М. М. ГЛУХОВ
В. П. ЕЛИЗАРОВ
А. А. НЕЧАЕВ

АЛГЕБРА

Издание второе,
исправленное и дополненное

РЕКОМЕНДОВАНО
ФГКОУ ВПО «Академия Федеральной службы безопасности РФ»
в качестве учебника для студентов вузов, обучающихся
по укрупненной группе направлений подготовки
и специальностей «Информационная безопасность»

ЛАНЬ®
САНКТ-ПЕТЕРБУРГ • МОСКВА • КРАСНОДАР
2015

ББК 22.14я73
Г 55

Глухов М. М., Елизаров В. П., Нечаев А. А.

Г 55 Алгебра: Учебник. — 2-е изд., испр. и доп. — СПб.: Издательство «Лань», 2015. — 608 с.: ил. — (Учебники для вузов. Специальная литература).

ISBN 978-5-8114-1961-6

В первой половине учебника излагается материал, содержащий основные понятия и теоремы современной алгебры, который может использоваться студентами, обучающимися по направлениям подготовки и специальностям математического и технического профиля. Последующие главы содержат такие важные для специалистов по защите информации разделы, как теория конечных полей, многочлены над конечными полями, группы подстановок, определяющие соотношения групп, линейные рекуррентные последовательности и др.

Содержание учебника полностью соответствует примерным программам учебных дисциплин алгебраического цикла при реализации федеральных государственных образовательных стандартов по направлениям подготовки и специальностям, входящим в укрупненную группу «Информационная безопасность».

ББК 22.14я73

Рецензенты:
В. Н. ЛАТЫШЕВ — доктор физико-математических наук, профессор, зав. кафедрой общей алгебры Московского государственного университета им. М. В. Ломоносова;
В. Н. ЧУБАРИКОВ — доктор физико-математических наук, профессор, декан механико-математического факультета Московского государственного университета им. М. В. Ломоносова;
В. Г. ЧИРСКИЙ — доктор физико-математических наук, и. о. зав. кафедрой теории чисел Московского педагогического государственного университета.

Обложка
Е. А. ВЛАСОВА

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ

В основу учебника положены лекции по курсу «Алгебра», читавшиеся авторами на протяжении ряда лет в Институте криптографии, связи и информатики для слушателей специальностей «Криптография» и «Компьютерная безопасность». В учебнике авторам удалось реализовать ряд оригинальных методических подходов к изложению материала. Вместе с тем, при подготовке учебника авторы использовали опыт изложения алгебраического материала другими авторами, а также свой опыт научно-исследовательской работы над математическими проблемами криптографии.

Современная криптография является одной из наиболее наукоемких областей естествознания. В частности, в ней находят применение практически все разделы современной алгебры. Именно этим объясняется тот факт, что «Алгебра» является одной из базовых дисциплин, широко используемых при изучении других дисциплин из федеральных государственных образовательных стандартов в области информационной безопасности.

Учитывая, что подлежащая криптографической защите информация обрабатывается, как правило, в дискретном виде, наиболее востребованными в криптографии являются знания по конечным алгебраическим объектам — конечным группам, полугруппам, кольцам, полям, векторным пространствам, функциям и многочленам над конечными полями и кольцами, группам подстановок и др. Авторы по возможности учитывали это при подготовке данного учебника. Усиленное внимание к конечным алгебраическим объектам является одной из особенностей предлагаемого учебника. Еще одна его особенность, также обусловленная практическими потребностями, заключается в алгоритмичности изложения материала, в стремлении к упрощению и четкому описанию алгоритмов решения рассматриваемых задач.

Первые двенадцать глав учебника содержат, главным образом, традиционный для математических специальностей алгебраический материал, который вполне может использоваться студентами математических факультетов университетов и педагогических вузов. В последующих главах продолжается изложение основных классических разделов курса: линейных пространств и их преобразований, квадратичных форм, групп, колец, полей. При этом изложение материала ориентируется на профессиональную деятельность специалистов в области защиты информации. Накопленная теоретическая база позволяет (в ряде случаев впервые) рассмотреть в рамках учебника такие специфические разделы из утвержденных программ по указанным выше специальностям, как линейные неравенства, стохастические матрицы, транзитивные, примитивные и кратно транзитивные группы подстановок, задание групп образую-

щими элементами и определяющими соотношениями, неприводимые многочлены над конечными полями, линейные рекуррентные последовательности над конечными полями и кольцами, графы линейных преобразований конечных пространств.

В учебнике авторы стремились выделять наиболее важные и законченные алгебраические результаты. Эти результаты оформлялись в виде теорем. Все остальные, более мелкие и вспомогательные факты, формулировались в виде лемм и утверждений.

Большинство рассматриваемых в учебном издании понятий и результатов иллюстрируется примерами. После каждой главы приводятся задачи для самоконтроля и на закрепление и углубление соответствующего материала.

Содержащиеся в учебнике параграфы, определения, теоремы, утверждения, леммы, примеры, замечания и формулы нумеруются по главам. В конце книги предлагаются списки использованной учебной и монографической литературы, а также перечень сборников задач по алгебре. Для удобства пользования учебником приведены именной и предметный указатели.

Данный учебник с определенным избытком охватывает также весь алгебраический материал по направлениям подготовки и специальностям укрупненной группы 10.00.00 «Информационная безопасность» и направлен на формирование соответствующих общепрофессиональных компетенций.

Предлагаемое второе издание учебника отличается от первого издания лишь исправлением опечаток, допущенных в первом издании, и добавлением двух новых параграфов, посвященных характерам конечных полей и их применению к распределению элементов на циклах линейных рекуррент.

Авторы выражают признательность В. Л. Куракину за качественное научное редактирование и подготовку электронной верстки учебника, О. В. Камловскому за предоставление материала по распределению элементов на циклах линейных рекуррент и Р. В. Богонатову за окончательную подготовку рукописи к печати.

Глава 1

ВВЕДЕНИЕ

§ 1. ПРЕДМЕТ АЛГЕБРЫ

Предмет и содержание алгебры претерпевали существенные изменения в ходе ее развития. До середины XIX века алгебраические исследования были связаны, в основном, с задачей нахождения корней многочленов, то есть решения уравнений вида

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0,$$

называемых теперь *алгебраическими уравнениями*. Также рассматривались уравнения и системы уравнений со многими неизвестными.

Термин «алгебра» происходит от названия сочинения узбекского математика IX века Мухаммеда ал-Хорезми «Альджебр аль-Мукабала», в котором были систематизированы сведения о правилах действий с числами и общих приемах решения задач, сводящихся к алгебраическим уравнениям 1-й и 2-й степеней. До XVI в. для записи уравнений применялись громоздкие словесные описания, что существенно сдерживало развитие алгебры. В XVI веке в алгебру постепенно проникает символический язык. Решающий вклад в его развитие внес французский математик Ф. Виет (1540–1603). Он первым стал обозначать буквами не только неизвестные, но и коэффициенты уравнений. Это позволило свойства уравнений и их корней записывать общими формулами. В частности, Виет вывел формулы, связывающие корни алгебраического уравнения с его коэффициентами. В XVII–XVIII в. исследованию алгебраических уравнений и их приложениям большое внимание уделяли такие крупные ученые, как французские математики Р. Декарт (1596–1650), П. Ферма (1601–1665), Ж. Л. Лагранж (1736–1813), английский физик и математик И. Ньютон (1643–1727), немецкий математик К. Ф. Гаусс (1777–1855) и др. Ферма и Декарт являются основоположниками аналитической геометрии. Они внесли значительный вклад в дальнейшее совершенствование алгебраического языка и в разработку алгебраических методов решения геометрических задач. Декарт широко применял алгебраические уравнения к классификации и изучению кривых на плоскости, разработал метод оценки числа действительных корней многочлена. Ферма занимался также решением уравнений в целых числах. В частности, он сформулировал утверждение о том, что уравнение $x^n + y^n = z^n$ не имеет целых (нетривиальных) решений при целом $n > 2$. Это утверждение, называемое *большой* (или великой) *теоремой Ферма*, удалось доказать лишь в 1993 г. Последний рубеж на пути к этому результату преодолели математики из США Э. Уайлс (A. Wiles) и Р. Тейлор (R. Taylor), однако основной вклад сделал

Э. Уайлс. Лагранж построил теорию исключения неизвестных из систем алгебраических уравнений, указал формулу для нахождения многочлена степени n по его значению в $n+1$ точках, разработал метод отделения действительных корней многочлена. Ньютон, основываясь на связи алгебраических уравнений с кривыми плоскости, указал метод приближенного вычисления корней уравнения. Гаусс установил связь между решением уравнения вида $x^n - 1 = 0$ и построением n-угольников с помощью циркуля и линейки. В частности, на этом пути ему удалось описать все значения n, при которых правильный n-угольник может быть построен с помощью циркуля и линейки. Оказалось, что такими являются все числа 2^m и $2^m p_1 \dots p_r$, где m — натуральное число, $p_1, \dots, p_r$ — различные простые числа вида $2^{2^k}+1$. В 1799 г. он впервые строго доказал, что любой многочлен с комплексными коэффициентами имеет хотя бы один корень. До сих пор эта теорема по традиции называется основной теоремой алгебры.

Среди различных задач об уравнениях центральной долгое время оставалась задача нахождения формул, выражающих корни уравнений через их коэффициенты с помощью основных арифметических операций и извлечения корней, по аналогии с известной из древности формулой для корней квадратных уравнений (проблема разрешимости уравнений в радикалах). Для уравнений 3-й и 4-й степеней эта задача была решена итальянскими математиками Н. Тарталья (1500–1557), Д. Кардано (1501–1576), Л. Феррари (1522–1565). Вот, к примеру, как выглядит формула для корней кубического уравнения вида $x^3 + px + q = 0$, называемая формулой Кардано:

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Много усилий было затрачено математиками на отыскание формул для корней уравнения 5-й степени и более высоких степеней. В 1799 г. итальянский математик П. Руффини (1765–1822) опубликовал теорему, утверждающую отсутствие общей формулы для корней уравнений степени $n \geqslant 5$. Однако доказательство Руффини содержало пробел. Впервые полное доказательство указанной теоремы было предложено в 1824 г. норвежским математиком Н. Х. Абелем (1802–1829). Теорема Руффини—Абеля и другие имеющиеся к тому времени результаты по теории уравнений помогли молодому французскому математику Э. Галуа (1811–1832) сформулировать более общую задачу — о разрешимости в радикалах произвольного конкретного алгебраического уравнения. Им же был найден и доказан критерий разрешимости. Этот результат Галуа имеет принципиальное значение не столько потому, что закрыл проблему о разрешимости уравнений в радикалах, сколько потому, что положил начало новому этапу развития алгебры. Дело в том, что для решения указанной проблемы Галуа развил зарождавшиеся к тому времени теорию групп и теорию полей. Позднее эти теории нашли глубокие приложения как в самой алгебре, так и в других областях науки (в геометрии, кристаллографии, физике, химии и др.). Так, например, в 1872 г. немецкий математик Ф. Х. Клейн (1849–1925) в работе, известной под названием «Эрлангенская программа», предложил новый подход к классификации и изучению геометрий, основанный на инвариантах групп, рассматриваемых в геометриях

преобразований пространств. В 1890 г. русский кристаллограф и геометр Е. С. Федоров (1853–1919), основываясь на свойствах групп преобразований, дал полную классификацию пространственных решеток кристаллов.

С современной точки зрения группы и поля являются типичными примерами множеств с операциями, или, как говорят, алгебраических структур. Общее определение операции сформировалось путем абстрагирования от известных операций сложения и умножения чисел. В соответствии с этим, под операцией f на произвольном множестве A понимают правило, по которому любым двум элементам из A, взятым в определенном порядке, сопоставляется элемент того же множества A. Точнее, так определенные операции называются *бинарными операциями*. Примерами бинарных операций являются операции сложения и умножения действительных чисел, операция сложения векторов плоскости (или пространства), операции сложения и умножения многочленов, операция композиции геометрических преобразований и др. По аналогии с бинарной операцией можно определить *n-арную операцию* на множестве A при любом натуральном n, как правило, сопоставляющее каждому упорядоченному набору $(a_1, a_2, \ldots, a_n)$ элементов из A вполне определенный элемент множества A. При $n = 1$ такие операции называются *унарными*. Задача исследования множеств с операциями остается главной задачей алгебры с XIX в. по настоящее время. В связи с этим современную алгебру называют *наукой о множествах с операциями*.

К развитию алгебры как науки о множествах с операциями привела также и задача исследования и решения систем линейных уравнений со многими неизвестными. А именно, построение общей теории систем линейных уравнений потребовало изучения таких алгебраических структур, как многомерные векторные пространства и кольца матриц.

В настоящее время основные алгебраические структуры — группы, полугруппы, квазигруппы, кольца, поля, модули, линейные алгебры, линейные пространства и др. используются и в таких сравнительно новых прикладных областях математики, как криптография, теория автоматов, теория графов, теория информации и т. д. Потребности этих и других наук служат, в свою очередь, главной движущей силой развития алгебры.

Развитие алгебры в дореволюционной России связано с именами таких выдающихся математиков, как Л. Эйлер (1707–1783), который жил и работал в Петербурге более 30 лет, Н. И. Лобачевский (1792–1856), П. Л. Чебышев (1821–1894), Д. А. Граве (1863–1939), Ф. Э. Молин (1861–1941) и др. Создателем первой отечественной алгебраической школы был ученик Д. А. Граве, известный математик, полярный исследователь и общественный деятель О. Ю. Шмидт (1891–1956). В 1916 г. в Киеве была издана его книга «Абстрактная теория групп», в которой впервые в мировой литературе основы теории групп излагались без предположения о конечности рассматриваемых групп. В 1939 г. О. Ю. Шмидт организовал при Московском университете семинар по теории групп, который со временем стал одним из основных центров деятельности российских алгебраистов. К настоящему времени крупные алгебраические школы сложились и в ряде других городов России: в Санкт-Петербурге, Новосибирске, Екатеринбурге и др.

§ 2. ПЕРВОНАЧАЛЬНЫЕ ПОНЯТИЯ И ОБОЗНАЧЕНИЯ ИЗ ТЕОРИИ МНОЖЕСТВ И МАТЕМАТИЧЕСКОЙ ЛОГИКИ

Непосредственно из трактовки современной алгебры как науки о множествах с операциями следует, что в алгебре не обойтись без использования основных понятий теории множеств. Само понятие *множества* считается в математике основным, неопределяемым понятием. Создатель теории множеств немецкий математик Г. Кантор (1845–1918) пояснил его следующим образом: «Под множеством понимают объединение в одно общее объектов, хорошо различаемых нашей интуицией или нашей мыслью». Говорят также, что множество — это совокупность (собрание, семейство) каких-либо реально существующих или мыслимых объектов, объединенных по некоторому признаку. Предполагается, что объекты, входящие в множество, попарно различны. Объекты, из которых составлено множество, называются его *элементами*. Множества и элементы множеств обозначаются различными буквами без индексов и с индексами. При этом, как правило, множества и элементы отождествляются с их обозначениями. Например, вместо фразы «элемент, обозначенный буквой a, содержится в множестве, обозначенном буквой A», говорят короче: «элемент a содержится в множестве A» (или «принадлежит множеству A») и пишут $a \in A$. Запись $a \notin A$ означает, что a не является элементом множества A. Множества A, B называют *равными*, что записывают в виде $A = B$, если каждый элемент множества A содержится в B, и, наоборот, каждый элемент множества B содержится в A. В противном случае говорят, что множества A и B не равны, и пишут $A \neq B$.

Множество обычно задают или перечислением всех его элементов, или указанием правила перечисления, или указанием каких-либо характеристических свойств его элементов. В первом случае множество обозначается в виде заключенного в фигурные скобки списка его элементов, например,

$$\{\text{а}, \text{в}, \text{г}\}, \quad \{5\}.$$

Во втором случае записывают в фигурных скобках несколько первых элементов с многоточием, например,

$$\{0, 2, 4, 6, \ldots\}.$$

Если же множество A задается системой свойств $P_1, \ldots, P_k$ его элементов, то пишут

$$A = \{a : P_1, \ldots, P_k\} \quad \text{или} \quad A = \{a \mid P_1, \ldots, P_k\}$$

и говорят, что A есть множество всех элементов a, обладающих свойствами $P_1, \ldots, P_k$.

Иногда приходится говорить о множестве, про которое неизвестно заранее, содержит ли оно хотя бы один элемент. Так, мы говорим о множестве решений уравнения, не решая его и, значит, не зная еще, имеет ли оно хотя бы одно решение. В связи с этим вводится множество, совсем не содержащее элементов. Оно называется *пустым* и обозначается символом $\varnothing$.

Для некоторых часто используемых ниже и известных из средней школы числовых множеств введем стандартные обозначения:

$\mathbb{N} = \{1, 2, 3, \ldots\}$ — множество натуральных чисел;

$\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$ — множество целых неотрицательных чисел;

$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ — множество целых чисел;

$\mathbb{Q}$ — множество рациональных чисел, т. е. чисел, представимых дробями вида $\frac{a}{b}$, где $a, b \in \mathbb{Z}$, $b \neq 0$;

$\mathbb{R}$ — множество действительных (или вещественных) чисел, т. е. чисел, представимых бесконечными десятичными дробями;

$\overline{m, n}$ для $m, n \in \mathbb{Z}$ есть $\{m, m+1, \ldots, n\}$, если $m < n$, и $\{m\}$, если $m = n$.

Если каждый элемент множества A является элементом множества B, то говорят, что A есть *подмножество* множества B (или A входит в B, или B включает A), и пишут $A \subset B$. В частности, подмножествами любого множества A являются A и $\varnothing$. Все остальные его подмножества называют *собственными*. Если хотят подчеркнуть, что подмножество A множества B не совпадает с B, то пишут $A \subsetneqq B$ и говорят, что B строго включает A.

Например, для указанных выше числовых множеств имеют место строгие включения

$$\mathbb{N} \subsetneqq \mathbb{N}_0 \subsetneqq \mathbb{Z} \subsetneqq \mathbb{Q} \subsetneqq \mathbb{R}.$$

В математике, а также на практике, часто приходится получать из одних множеств другие, используя различные операции над множествами. Определим четыре операции.

Определение 1. *Объединением множеств* A, B называется множество $A \cup B$, состоящее из всех тех элементов, каждый из которых принадлежит хотя бы одному из множеств A, B:

$$A \cup B = \{m : \ m \in A \text{ или } m \in B\}.$$

Определение 2. *Пересечением множеств* A, B называется множество $A \cap B$, состоящее из всех тех элементов, которые содержатся в обоих множествах A, B:

$$A \cap B = \{m : \ m \in A \text{ и } m \in B\}.$$

Заметим, что пересечение двух множеств может оказаться пустым множеством. В этом случае исходные множества называют *непересекающимися*.

Определение 3. *Декартовым произведением множеств* A, B называют множество $A \times B$, состоящее из всевозможных упорядоченных пар вида (a, b), где $a \in A$, $b \in B$:

$$A \times B = \{(a, b) : \ a \in A, \ b \in B\}.$$

Определение 4. *Разностью множеств* A, B называют множество $A \setminus B$, состоящее из всех элементов множества A, не содержащихся в B:

$$A \setminus B = \{m : \ m \in A, \ m \notin B\}.$$

В том случае, когда $B \subset A$, множество $A \setminus B$ называется *дополнением множества B до A*.

По аналогии с определениями 1, 2 можно определить объединение и пересечение произвольного семейства множеств $\{A_i : i \in I\}$ (здесь I — любое конечное или бесконечное множество индексов):

$$\bigcup_{i \in I} A_i = \{a : a \in A_i \text{ хотя бы для одного } i \in I\},$$

$$\bigcap_{i \in I} A_i = \{a : a \in A_i \text{ для всех } i \in I\}.$$

В частности, если $I = \{1, 2, \ldots, n\}$, то указанные множества записывают в виде $\bigcup\limits_{i=1}^{n} A_i$, $\bigcap\limits_{i=1}^{n} A_i$, или подробнее: $A_1 \cup \ldots \cup A_n$, $A_1 \cap \ldots \cap A_n$. Представление любого множества A в виде объединения непустых и попарно непересекающихся подмножеств называют *разбиением* множества A.

Определим еще декартово произведение n множеств:

$$A_1 \times \ldots \times A_n = \{(a_1, \ldots, a_n) : a_i \in A_i,\ i \in \overline{1, n}\}.$$

В том случае, когда $A_1 = \ldots = A_n = A$, мы получим n-ю *декартову степень* множества A:

$$A^n = \{(a_1, \ldots, a_n) : a_i \in A,\ i \in \overline{1, n}\}.$$

Таким образом, A^n есть множество всевозможных наборов длины n из элементов множества A. Подчеркнем, что в отличие от множества, в котором все элементы считаются различными по определению, набор $(a_1, \ldots, a_n)$ может содержать и одинаковые элементы. В дальнейшем упорядоченные наборы (не обязательно различных) элементов из A будут называться также *системами* элементов из A.

Важную роль в дальнейшем будет играть понятие отображения множеств.

Определение 5. Пусть A, B — произвольные множества. *Отображением множества A в множество B* называют всякое правило f, по которому каждому элементу множества A сопоставляется вполне определенный (единственный) элемент множества B.

Тот факт, что f есть отображение A в B, кратко записывают в виде

$$f : A \to B.$$

Если при этом элементу a из A сопоставлен элемент b из B, то b называют *образом* элемента a, а a — *прообразом* элемента b при отображении f, что записывается в виде $f(a) = b$.

Из определения отображения f следует, что у каждого элемента a из A существует единственный образ, однако, для элемента $b \in B$ прообразов может быть много, а может и вообще не быть. Множество всех прообразов элемента b из B называется его *полным прообразом* и обозначается через $f^{-1}(b)$. Таким образом, $f^{-1}(b) = \{a : a \in A,\ f(a) = b\}$, или, несколько короче, $f^{-1}(b) = \{a \in A : f(a) = b\}$. Естественным

путем определяется *образ* $f(A_1)$ *подмножества* A_1 из A и *полный прообраз* $f^{-1}(B_1)$ подмножества B_1 из B при отображении f:

$$f(A_1) = \bigcup_{a \in A_1} \{f(a)\} \quad \text{и} \quad f^{-1}(B_1) = \bigcup_{b \in B_1} f^{-1}(b).$$

Отображение множества A в B называют также *функцией*, заданной на множестве A со значениями в множестве B. При этом элемент $f(a)$ называют *значением функции* f *в точке* a, а множество всех пар вида (a, b) где $a \in A$, $b \in B$ и $f(a) = b$, — *графиком функции*, или отображения, f.

Замечание 1. Приведенное выше определение отображения не является математически строгим, поскольку в нем используется неопределенный термин «правило». Для строгого определения понятия отображения используется подход через график. А именно, отображение $f\colon A \to B$ отождествляется с его графиком, который уже определяется строго, как подмножество M декартова произведения $A \times B$, содержащее для каждого элемента $a \in A$ единственную пару с первым элементом a. При таком определении отображения f равенство $f(a) = b$ означает наличие в M пары (a, b).

В зависимости от свойств образов и прообразов различают отображения сюръективные, инъективные и биективные.

Определение 6. Отображение $f\colon A \to B$ называется *сюръективным*, если каждый элемент из B является образом хотя бы одного элемента из A, то есть $f(A) = B$.

Определение 7. Отображение $f\colon A \to B$ называется *инъективным*, если оно разные элементы множества A отображает в разные элементы множества B. Инъективные отображения называют также *вложениями*.

Определение 8. Отображение $f\colon A \to B$ называется *биективным*, или *взаимно однозначным* отображением A на B, если оно сюръективно и инъективно.

Пример 1. Определим отображение $f_1\colon \mathbb{Z} \to \mathbb{N}_0$, положив для $a \in \mathbb{Z}$

$$f_1(a) = |a|,$$

где $|a|$ — абсолютная величина числа a. Очевидно, что f_1 — сюръективное, но не инъективное отображение.

Пример 2. Отображение $f_2\colon \mathbb{Z} \to \mathbb{N}_0$, определенное равенством

$$f_2(a) = \begin{cases} 2a, & \text{если } a \geqslant 0, \\ |2a| - 1, & \text{если } a < 0, \end{cases}$$

является биективным отображением.

Примером биективного отображения множества A на себя является тождественное отображение ε_A, или просто ε, которое любой элемент из A отображает в себя: $\varepsilon_A(a) = a$.

Определение 9. *Композицией отображений* $f_1\colon B \to C$ и $f_2\colon A \to B$ называется отображение $f_1 \circ f_2\colon A \to C$, определенное условием

$$(f_1 \circ f_2)(a) = f_1(f_2(a)) \tag{1}$$

для любого элемента $a \in A$.

То же самое отображение называют еще *произведением отображений* f_2 и f_1 и обозначают в виде $f_2 \cdot f_1$, или $f_2 f_1$. Таким образом,

$$(f_2 f_1)(a) = f_1(f_2(a)).$$

Отметим некоторые свойства введенных операций.

Утверждение 1. *Если* $f_1\colon A \to B$, $f_2\colon B \to C$, $f_3\colon C \to D$, *то*

$$(f_3 \circ f_2) \circ f_1 = f_3 \circ (f_2 \circ f_1). \tag{2}$$

□ Найдем образ элемента a из A при действии отображений, записанных в левой и правой частях равенства (2). Из (1) имеем:

$$((f_3 \circ f_2) \circ f_1)(a) = (f_3 \circ f_2)(f_1(a)) = f_3(f_2(f_1(a))),$$
$$(f_3 \circ (f_2 \circ f_1))(a) = f_3((f_2 \circ f_1)(a)) = f_3(f_2(f_1(a))).$$

Отсюда и следует (2). □

С использованием операции умножения равенство (2) запишется в виде

$$f_1(f_2 f_3) = (f_1 f_2) f_3.$$

Утверждение 2. *Если отображения* $f_1\colon A \to B$, $f_2\colon B \to C$ *сюръективны, инъективны или биективны, то соответственно таким же будет и отображение* $\psi = f_2 \circ f_1 = f_1 f_2$.

□ Действительно, из сюръективности f_2 и f_1 следует соответственно: для любого $c \in C$ существует такой элемент $b \in B$, что $f_2(b) = c$, и такой элемент $a \in A$, что $f_1(a) = b$. Отсюда $\psi(a) = f_2(f_1(a)) = f_2(b) = c$, и отображение ψ сюръективно.

Если же f_1, f_2 инъективны и $a_1 \neq a_2$, то $f_1(a_1) \neq f_1(a_2)$ и $f_2(f_1(a_1)) \neq f_2(f_1(a_1))$, т. е. $\psi(a_1) \neq \psi(a_2)$, и ψ инъективно. □

Заметим, что обратные утверждения в общем случае неверны. Так, например, тождественное отображение $\varepsilon_{\mathbb{N}}$ представляется в виде композиции $\varepsilon_{\mathbb{N}} = f_2 \circ f_1$, где f_1 — не сюръективное отображение $\mathbb{N}$ в $\mathbb{N}$, определенное условием $f_1(x) = x + 1$, а f_2 — не инъективное отображение $\mathbb{N}$ в $\mathbb{N}$, определенное следующим образом:

$$f_2(x) = \begin{cases} x - 1, & \text{если } x \in \mathbb{N} \text{ и } x > 1, \\ 1, & \text{если } x = 1. \end{cases}$$

Вместе с тем, имеет место

Утверждение 3. *Пусть $\psi = f_1 \cdot f_2$. Тогда если ψ сюръективно, то f_2 сюръективно; если ψ инъективно, то f_1 инъективно.*

Утверждение 3 легко доказывается методом от противного (докажите в качестве упражнения).

Характерной особенностью биективных отображений является наличие для них обратных отображений.

Определение 10. Отображение $f\colon A \to B$ называется *обратимым*, если существует такое отображение $f'\colon B \to A$, что $ff' = \varepsilon_A$ и $f'f = \varepsilon_B$. При этом отображение f' называется *обратным* для f и обозначается через f^{-1}.

Докажите в качестве упражнения, что равенствами $ff' = \varepsilon_A$, $f'f = \varepsilon_B$ отображение f' определяется однозначно.

Имеет место следующий критерий обратимости.

Утверждение 4. *Отображение $f\colon A \to B$ обратимо тогда и только тогда, когда оно биективно.*

□ Если f обратимо, то его биективность (и биективность обратного к нему отображения f') следует из утверждения 3. Обратно, пусть отображение $f\colon A \to B$ биективно. Определим отображение $f'\colon B \to A$, положив для $b \in B$: $f'(b) = a$, если $f(a) = b$. Такое a найдется в силу сюръективности f, и это a единственно в силу инъективности f. Следовательно, отображение f' определено корректно. Очевидно, что оно является обратным для f. □

Определение 11. Множества A и B называют *равномощными* и пишут $|A| = |B|$, если существует биективное отображение $f\colon A \to B$.

Определение 12. Множество A называется *конечным*, если оно пусто или равномощно отрезку $\overline{1,n}$ натурального ряда $\mathbb{N}$. В последнем случае число n называют *мощностью множества* A, а само A — n-элементным множеством. Мощность пустого множества считается равной нулю. Все остальные множества называются *бесконечными*.

Мощность конечного множества A обозначается через $|A|$, тот факт, что A конечно, записывается в виде $|A| < \infty$.

Заметим, что в определении 12 конечного и бесконечного множества используется знание натурального ряда чисел. В принципе без этого можно обойтись, если воспользоваться следующим характеристическим свойством бесконечных множеств. Любое бесконечное множество равномощно некоторому своему собственному подмножеству. Однако мы не будем здесь вдаваться в тонкости теории множеств, а будем считать, что множества натуральных, целых, рациональных и действительных чисел читателю известны из средней школы.

Для отображений конечных множеств справедливо

Утверждение 5. *Если A, B — конечные и равномощные множества, то для любого отображения $f\colon A \to B$ эквивалентны условия*:

(а) f *сюръективно*;

(б) f *инъективно*;

(в) f *биективно.*

□ Из определений 6–8 видно, что для доказательства утверждения достаточно установить эквивалентность (а) и (б).

Пусть f сюръективно, т. е. $f(A) = B$. Тогда

$$|B| = |f(A)| = \Big|\bigcup_{a\in A}\{f(a)\}\Big|.$$

Так как $|\{f(a)\}| = 1$ при любом $a \in A$, то равенство $\Big|\bigcup\limits_{a\in A}\{f(A)\}\Big| = |A|$ возможно лишь в том случае, когда $f(a_1) \neq f(a_2)$ при любых значениях $a_1, a_2 \in A$. Это означает, что f инъективно. Обратно, пусть f инъективно. Тогда оно разные элементы отображает в разные, и поэтому $|f(A)| = \Big|\bigcup\limits_{a\in A}\{f(a)\}\Big| = |A|$. Отсюда и из условия $|A| = |B|$ имеем: $|f(A)| = |B|$. Теперь, учитывая включение $f(A) \subset B$ и конечность множества B, получаем: $f(A) = B$. Следовательно, f сюръективно. □

Наряду с понятиями теории множеств в современной математике широко используются язык и средства математической логики. Подробно они изучаются в отдельном курсе. Здесь же мы остановимся лишь на обозначениях основных логических операций и их использовании для сокращений записи утверждений.

Основным неопределяемым понятием математической логики является понятие *высказывания*. Обычно под высказыванием понимают любое утверждение, про которое можно сказать, что оно истинно или ложно, и не может быть одновременно истинным и ложным. Если высказывание a истинно (ложно), то говорят, что оно имеет значение «истина» («ложь») и пишут $a \equiv$ и ($a \equiv$ л).

Основными логическими операциями над высказываниями являются *конъюнкция* $\&$, *дизъюнкция* $\vee$, *импликация* $\Rightarrow$ и *отрицание* $\overline{\ }$. Первые три из них соответствуют в русском языке соединению двух утверждений союзами «и», «или», «если ..., то», отрицание соответствует вставке частицы «не». Значения получаемых таким образом высказываний определяются значениями исходных высказываний и соответствующими операциями на множестве {и, л}, которые определяются следующей таблицей:

a	b	$a \,\&\, b$	$a \vee b$	$a \Rightarrow b$	$\overline{a}$
л	л	л	л	и	и
л	и	л	и	и	и
и	л	л	и	л	л
и	и	и	и	и	л

Обратите особое внимание на импликацию $a \Rightarrow b$ высказываний a, b. Она является ложной лишь в том случае, когда a — истинное, а b — ложное высказывания.

В частности, если $a \equiv$ л, то высказывание $a \Rightarrow b$ истинно, но это не означает, что истинно высказывание b, оно может быть любым. В связи с этим говорят: «из лжи следует все, что угодно».

Кроме утверждений, имеющих вполне определенные значения — истину или ложь, в математике широко используются предложения, зависящие от переменных со значениями из заданных множеств и превращающиеся в высказывания при замене в них всех переменных любыми значениями из рассматриваемых множеств.

Такие утверждения называют *предикатами*. В целях общности к предикатам относят и высказывания. Примером предиката может служить неравенство «$x < y$» на множестве $\mathbb{R}$. Само оно не является высказыванием. Однако при замене x, y действительными числами становится высказыванием: «$2 < 3$» — истинное высказывание, «$5 < 1$» — ложное высказывание. К предикатам относятся, в частности, все уравнения с неизвестными на множестве $\mathbb{R}$ или любом его подмножестве M.

Заметим, что строго предикат p от n переменных на множестве A можно определить как отображение $p\colon A^n \to \{\text{и}, \text{л}\}$.

К предикатам, так же как и к высказываниям, можно применить операции конъюнкции, дизъюнкции, импликации и отрицания. В результате из заданных предикатов будут получаться новые, более сложные предикаты. Так, например, дизъюнкцией двух предикатов «$y < x$», «$x = y$» будет предикат «$(x < y) \vee (x = y)$», который короче записывается в виде «$x \leqslant y$».

Приведем для указанных операций над предикатами теоретико-множественную интерпретацию. Для простоты ограничимся рассмотрением предикатов от одного переменного x на фиксированном множестве A. Каждому такому предикату $p(x)$ сопоставим подмножество его истинности $A(p) = \{a \in A\colon\ p(a) \equiv \text{и}\}$.

Непосредственно из свойств логических и теоретико-множественных операций следуют соотношения:

$$
\begin{aligned}
&A(p_1 \,\&\, p_2) = A(p_1) \cap A(p_2),\\
&A(p_1 \vee p_2) = A(p_1) \cup A(p_2),\\
&A(p_1 \Rightarrow p_2) = A \setminus (A(p_1) \setminus A(p_2)),\\
&A(\overline{p}_1) = A \setminus A(p_1).
\end{aligned}
$$

Кроме указанных бинарных логических операций к предикатам часто применяются еще две унарные операции навешивания *кванторов*.

Пусть $p(x_1, \ldots, x_n)$ — предикат, зависящий от переменных x_1, …, x_n со значениями из множества A. Тогда из него можно построить новые предикаты:

«Для всякого $x_1 \in A$ имеет место $p(x_1, \ldots, x_n)$»,

«Существует $x_1 \in A$ такое, что $p(x_1, \ldots, x_n)$».

Говорят, что они получены из $p(x_1, \ldots, x_n)$ путем навешивания соответственно *квантора всеобщности* и *квантора существования* по переменному x_1. Кратко они обозначаются в виде

$$p(x_1, \ldots, x_n), \tag{3}$$

$$\exists\, x_1 \in A\colon\ p(x_1, \ldots, x_n). \tag{4}$$

Аналогично определяются операции навешивания кванторов по любому другому переменному x_i, $i \in \overline{2,n}$. Заменив в (3), (4) переменные $x_2, \ldots, x_n$ соответственно элементами $a_2, \ldots, a_n \in A$, получим высказывания

$$p(x_1, a_2, \ldots, a_n), \tag{5}$$

$$\exists\, x_1 \in A\colon\ p(x_1, a_2, \ldots, a_n). \tag{6}$$

Первое из них является истинным тогда и только тогда, когда высказывание $p(a_1, a_2, \ldots, a_n)$ является истинным при любом $a_1 \in A$. Второе истинно в том и только том случае, когда высказывание $p(a_1, a_2, \ldots, a_n)$ истинно хотя бы при одном a_1 из A. Таким образом, высказывания (5), (6) не зависят от переменного x_1, и потому (3), (4) являются предикатами от $n-1$ переменных $x_2, \ldots, x_n$. К ним можно применять операции навешивания кванторов по любому из переменных $x_2, \ldots, x_n$ и т. д.

Следует помнить, что истинность высказывания, полученного из предиката путем навешивания кванторов по разным переменным, в общем случае зависит от порядка следования кванторов. Так, например, высказывание «$\forall x \in \mathbb{N},\ \exists y \in \mathbb{N}\colon\ (x < y)$» истинно, а высказывание «$\exists y \in \mathbb{N},\ \forall x \in \mathbb{N}\colon\ (x < y)$» ложно.

С помощью логических операций $\&$, $\vee$, $\Rightarrow$, $\overline{\ }$, $\forall$, $\exists$ можно из заданных высказываний и предикатов естественным образом строить выражения или формулы, которые будут задавать новые высказывания и предикаты. Две формулы от одних и тех же переменных, принимающих значения из одного множества, называют *равносильными* или *эквивалентными*, если они принимают одинаковые значения (истину или ложь) при любых, одинаковых для обеих формул наборах значений переменных. Условимся равносильность формул обозначать знаком $\equiv$. С помощью равносильностей формул можно записать свойства логических операций над предикатами. Приведем примеры:

$$p \,\&\, p \equiv p, \qquad p \vee p \equiv p,$$

$$p \,\&\, q \equiv q \,\&\, p, \qquad p \vee q \equiv q \vee p,$$

$$(p \,\&\, q) \,\&\, r \equiv p \,\&\, (q \,\&\, r), \qquad (p \vee q) \vee r \equiv p \vee (q \vee r),$$

$$\overline{p \,\&\, q} \equiv \overline{p} \vee \overline{q}, \qquad \overline{p \vee q} \equiv \overline{p} \,\&\, \overline{q},$$

$$p \,\&\, (q \vee r) \equiv (p \,\&\, q) \vee (p \,\&\, r), \qquad p \vee (q \,\&\, r) \equiv (p \vee q) \,\&\, (p \vee r).$$

Обратим особое внимание на следующие равносильности, которые часто используют при доказательствах:

$$\overline{\forall x\, p(x)} \equiv \exists x\, \overline{p(x)}, \quad \overline{\exists x\, p(x)} \equiv \forall x\, \overline{p(x)}.$$

Справедливость выписанных равносильностей проверяется непосредственно с использованием определения логических операций.

Заметим, что логическая символика зачастую бывает полезной как в целях сокращения записи утверждений, так и с целью достижения их лучшей обозримости. Для примера запишем условия инъективности и сюръективности отображения $f\colon A \to B$:

$$\forall\, a_1, a_2 \in A\colon\ ((a_1 \neq a_2)\ \Rightarrow\ (f(a_1) \neq f(a_2))),$$

$$\forall\, b \in B,\ \exists\, a \in A\colon\ (f(a) = b).$$

§ 3. О МАТЕМАТИЧЕСКИХ УТВЕРЖДЕНИЯХ И МЕТОДАХ ИХ ДОКАЗАТЕЛЬСТВА

Типичной формой математического утверждения, или теоремы, является импликация

$$A \Rightarrow B, \tag{7}$$

которая читается как «из A следует B», или «если истинно A, то истинно B», или «A влечет B», или «A достаточно для B», или «B необходимо для A».

Напомним, что утверждение

$$B \Rightarrow A \tag{8}$$

называется *обратным к* (7), а утверждение

$$\overline{A} \Rightarrow \overline{B} \tag{9}$$

противоположным к (7).

В общем случае утверждения (8), (9) не равносильны утверждению (7). В частности, может оказаться, что импликация (7) истинна, в то время как импликации (8), (9) ложны. Иначе говоря, для заданной теоремы обратная и противоположная теоремы могут не иметь места. Приведите примеры. С другой стороны, из определений импликации и отрицания легко следует, что формула (7) равносильна формуле $\overline{B} \Rightarrow \overline{A}$. Значит, любая теорема равносильна противоположной к обратной ей теореме, и вместо доказательства импликации (7) можно доказывать импликацию

$$\overline{B} \Rightarrow \overline{A}.$$

Так зачастую и поступают.

В том случае, когда для теоремы (7) верной является и обратная теорема (8), их обычно объединяют в одно утверждение

$$(A \Rightarrow B) \ \& \ (B \Rightarrow A),$$

которое записывают в виде

$$A \Leftrightarrow B$$

и словесно читают в одной из следующих формулировок: «A имеет место тогда и только тогда, когда имеет место B»; «A выполняется в том и только в том случае, когда выполняется B»; «для выполнения A необходимо и достаточно выполнения B»; «для выполнения B необходимо и достаточно выполнения A» и т. п.

Доказать теорему (7) — значит установить истинность импликации (7). Подчеркнем, что в общем случае истинность импликации (7) не означает истинности B. Из определения операции импликации видно, что при ложном утверждении A импликация (7) истинна при любом (в частности, и при ложном) B, и в этом случае никакого доказательства не требуется. Значит, доказывать теорему (7) надо лишь в том случае, когда утверждение A истинно, и в этом случае для доказательства нужно установить истинность утверждения B.

Не вдаваясь в строгие логические формулировки, можно сказать, что любое математическое доказательство представляет собой конечную последовательность логических умозаключений, основанных на известных ранее математических фактах и логических правилах (законах логики). Приведем, для примера, некоторые широко используемые в доказательствах *правила логики*, позволяющие из истинности одних утверждений получать истинность других. Если при этом из истинности утверждений $A_1, \ldots, A_n$ получается истинность утверждения B, то будем записывать это в виде $(A_1, \ldots, A_n) \Rightarrow B$.

1. Правило заключения: $(A,\ A \Rightarrow B) \Rightarrow B$.
2. Правило силлогизма: $(A \Rightarrow B,\ B \Rightarrow C) \Rightarrow (A \Rightarrow C)$.
3. Правило контрапозиции: $(A \Rightarrow B) \Rightarrow (\overline{B} \Rightarrow \overline{A})$.
4. Правила двойного отрицания: $A \Rightarrow \overline{\overline{A}},\ \ \overline{\overline{A}} \Rightarrow A$.
5. Правило сложения посылок: $(A \Rightarrow C,\ B \Rightarrow C) \Rightarrow (A \vee B \Rightarrow C)$.
6. Правило умножения заключений:

$$(A \Rightarrow B,\ A \Rightarrow C) \Rightarrow (A \Rightarrow B \,\&\, C).$$

Отдельные методы доказательства явно выделяются своей спецификой. Укажем три типа таких доказательств.

1. Метод непосредственной проверки.

Этим методом обычно доказывают равенства или некоторые другие соотношения, а само доказательство заключается в осуществлении последовательности действий, существо и порядок которых определяются самой формулировкой доказываемого утверждения. Примером такого доказательства может служить доказательство формул сокращенного умножения. Так, для доказательства формулы $(a+b)(a-b) = a^2 - b^2$ достаточно перемножить многочлены $a+b$ и $a-b$, привести подобные члены и сравнить результат с выражением $a^2 - b^2$.

2. Метод доказательства «от противного».

Для доказательства этим методом некоторого утверждения A допускают, что утверждение A ложно, то есть истинно его отрицание $\overline{A}$. Далее, с использованием утверждения $\overline{A}$ доказывают некоторое заведомо ложное утверждение F и из этого делают вывод о том, что сделанное предположение о ложности A неверно, и поэтому A истинно. В основе этого метода лежит логическое правило $(\overline{A} \Rightarrow F,\ F \equiv \text{л}) \Rightarrow A$.

В том случае, когда доказываемое утверждение имеет вид $A \Rightarrow B$ и утверждение A истинно, в доказательстве методом «от противного» допускают, что верно утверждение $\overline{B}$, и из A и $\overline{B}$ выводят некоторое ложное утверждение F. Отсюда делают вывод о том, что из истинности A следует истинность B. В этом случае используется логическое правило:

$$(A \,\&\, \overline{B} \Rightarrow F,\ F \equiv \text{л}) \Rightarrow (A \Rightarrow B).$$

В некоторых случаях, исходя из A и $\overline{B}$, доказывают утверждение $\overline{A}$. В этой ситуации роль F играет ложное утверждение $A \,\&\, \overline{A}$.

В качестве примера доказательства методом «от противного» приведем известное утверждение о действительных числах: *произведение двух отличных от нуля действительных чисел отлично от нуля*.

Символически это утверждение можно записать так:

$$\forall\, x, y \in \mathbb{R}:\ ((x \neq 0)\ \&\ (y \neq 0) \Rightarrow (xy \neq 0)).$$

Для его доказательства нужно показать, что предикат

$$(x \neq 0\ \&\ y \neq\ 0) \Rightarrow (xy \neq 0)$$

принимает истинное значение при любых значениях x, y из $\mathbb{R}$. Допустим, что это не так, то есть при некоторых a, b ложна импликация

$$(a \neq 0)\ \&\ (b \neq 0) \Rightarrow (ab \neq 0).$$

Это означает, что ее посылка «$(a \neq 0)\ \&\ (b \neq 0)$» $= A$ истинна, а заключение «$(ab \neq 0)$» $= B$ ложно, т. е. $ab = 0$. Умножив обе части последнего равенства на число a^{-1}, обратное к a (которое существует в силу условия $a \neq 0$), и воспользовавшись известными свойствами умножения, получим равенство $b = 0$, которое свидетельствует об истинности утверждения $\overline{A}$. Таким образом, наше допущение о том, что утверждение теоремы неверно, привело нас к противоречию с условием A. Значит, такое допущение неверно, и тем самым наше утверждение доказано.

3. Метод полной математической индукции.

Этот метод применяют для доказательства таких утверждений, в формулировках которых участвует числовой параметр t, принимающий все значения из множества $\mathbb{N}$ натуральных чисел. По существу, такое утверждение $A(t)$ является предикатом от переменного t на множестве $\mathbb{N}$, а доказать требуется истинность формулы $\forall t\, A(t)$. Сам процесс доказательства методом полной математической индукции состоит из двух этапов.

1) Доказывают, что утверждение $A(t)$ истинно при $t = 1$ (это чаще всего удается сделать непосредственной проверкой).

2) Исходя из допущения, что утверждение $A(t)$ верно для произвольного фиксированного значения $t = n$, доказывают его истинность при $t = n + 1$.

После выполнения обоих этапов доказательства делается вывод об истинности утверждения $A(t)$ для всех значений t из множества $\mathbb{N}$.

Первый этап доказательства обычно называют началом или базисом индукции, второй — индуктивным шагом, или переходом от n к $n + 1$. С содержательной точки зрения метод полной математической индукции обычно не вызывает возражений. Интуитивно всем кажется ясным, что указанные два этапа метода вполне законно заменяют перебор бесконечного ряда значений параметра $t = 1, 2, 3, \ldots$. Теоретической основой метода является одна из аксиом натурального ряда чисел, называемая аксиомой полной математической индукции. Аксиоматическое построение арифметики натуральных чисел независимо было осуществлено в 1888 г. немецким математиком Р. Дедекиндом (1831–1916) и в 1889 г. итальянским математиком Д. Пеано (1858–1932). Натуральный ряд чисел Пеано определил как произвольное множество $\mathbb{N}$ с заданным на нем отношением «следовать за», удовлетворяющим аксиомам:

1. Существует элемент множества $\mathbb{N}$, не следующий ни за каким элементом из $\mathbb{N}$ (любой из них назовем единицей и обозначим символом 1);

2. Для каждого элемента $n \in \mathbb{N}$ существует единственный элемент, следующий за n (обозначим его через n');

3. Для каждого элемента $n \in \mathbb{N}$ существует не более одного элемента, за которым следует n;

4. (Аксиома полной математической индукции.) Пусть M — подмножество множества $\mathbb{N}$, удовлетворяющее условиям

а) $1 \in M$;

б) $\forall\, n \in \mathbb{N}:\ (n \in M \Rightarrow n' \in M)$.

Тогда $M = \mathbb{N}$.

В приведенном определении множества $\mathbb{N}$ ничего не говорится о природе его элементов. Она может быть какой угодно, лишь бы их совокупность удовлетворяла аксиомам 1–4. Выбирая в качестве $\mathbb{N}$ некоторое конкретное множество с определенным отношением «следовать за», удовлетворяющем аксиомам 1–4, мы получим интерпретацию, или модель множества натуральных чисел. В качестве стандартной модели обычно берут выработанный в процессе исторического развития человечества ряд символов $1, 2, 3, 4, \ldots$.

Используя аксиомы 1–4, можно определить операции сложения и умножения натуральных чисел, отношения «меньше», «больше» и др. на множестве натуральных чисел и доказать известные факты арифметики. Мы не будем здесь этим заниматься. Сделаем лишь отдельные замечания.

1) Операции сложения и умножения в $\mathbb{N}$ однозначно определяются равенствами $(\forall\, a, b \in \mathbb{N})$:

$$a + 1 = a', \qquad a \cdot 1 = a,$$
$$a + b' = (a + b)', \qquad a \cdot b' = ab + a.$$

2) Неравенства $<$ и $>$ для чисел $a, b \in \mathbb{N}$ определяются с использованием операции сложения:

$$a < b \ \Leftrightarrow\ b > a \ \Leftrightarrow\ \exists\, k \in \mathbb{N}:\ (b = a + k).$$

Подчеркнем, что, наряду с другими известными свойствами неравенств, из аксиом 1–4 следует свойство, называемое *аксиомой Архимеда* [1]:

$$\forall\, a, b \in \mathbb{N},\ \exists\, q \in \mathbb{N}:\ (a < bq).$$

3) Для обоснования изложенного выше метода доказательства утверждения $\forall t\, A(t)$ достаточно взять в качестве фигурирующего в аксиоме 4 множества M множество тех значений параметра t, при которых утверждение $A(t)$ истинно, и заметить, что $n' = n + 1$.

4) С помощью аксиом 1–4 можно обосновать и несколько более общий метод доказательства утверждений вида $\forall t\ A(t)$ с параметром t, принимающим все целые значения, начиная с некоторого целого числа n_0. А именно, можно доказать следующую теорему.

Если утверждение $A(t)$ истинно при некотором $t = n_0 \in \mathbb{Z}$ и для любого фиксированного целого числа $n \geqslant n_0$ из истинности $A(t)$ при всех значениях

[1] Архимед (287–212 до н. э.) — древнегреческий математик.

$t \in \overline{n_0, n}$ *следует истинность* $A(t)$ *при* $t = n + 1$, *то утверждение* $A(t)$ *истинно при всех целых* $t \geqslant n_0$.

Особо подчеркнем тот факт, что здесь допускать истинность доказываемого утверждения $A(t)$ можно не только для $t = n$, но и для всех t, удовлетворяющих неравенствам $n_0 \leqslant t \leqslant n$.

5) Используя аксиомы 1–4, можно доказать, что в любом непустом подмножестве M множества целых неотрицательных чисел $\mathbb{N}_0$ существует наименьшее число. Это утверждение в арифметике называют *принципом наименьшего числа*. Заметим, что, используя указанные выше аксиомы 1–3 и принцип наименьшего числа, можно доказать аксиому полной математической индукции. В этом смысле говорят, что принцип наименьшего числа эквивалентен принципу полной математической индукции.

В заключение данного параграфа приведем одну известную из средней школы теорему, доказываемую методом полной математической индукции.

Любое натуральное число, большее единицы, либо является простым, либо разлагается в произведение простых чисел. (Напомним, что натуральное число $p > 1$ называется *простым*, если оно делится лишь на 1 и на себя. В противном случае, оно называется *составным*. Единица не относится ни к простым, ни к составным числам.)

□ Докажем теорему методом полной математической индукции. При этом в качестве t выберем то самое число, которое фигурирует в формулировке данной теоремы. По условию оно может быть любым натуральным числом, начиная с числа 2.

Так как 2 — простое число, то для $t = 2$ утверждение теоремы верно. Допустим, что оно верно для всех $t \in \overline{2, n}$ при любом фиксированном натуральном $n \geqslant 2$, и докажем его истинность для $t = n + 1$. Если число $n + 1$ простое, то для него утверждение теоремы верно. Пусть $n+1$ — составное. Тогда оно делится на некоторое число a такое, что $1 < a < n + 1$. Следовательно, $n + 1 = ab$, где $1 < b < n + 1$. По предположению индукции каждое из чисел a, b или простое, или разлагается в произведение простых чисел, то есть имеем:

$$a = p_1 \dots p_k, \quad b = q_1 \dots q_l,$$

где $p_1, \dots, p_k$, $q_1, \dots, q_l$ — простые числа, $k, l \in \mathbb{N}$. Отсюда и из равенства $n + 1 = ab$ получаем разложение числа $n + 1$ в произведение простых чисел:

$$n + 1 = p_1 \dots p_k q_1 \dots q_l. \quad \square$$

ЗАДАЧИ

1. Выразите операцию объединения (пересечения) множеств через операции пересечения (объединения) и вычитания множеств.

2. Выразите операцию объединения (пересечения) подмножеств фиксированного множества A через операции пересечения (объединения) и дополнения.

3. Докажите равенства (для любых множеств A, B, C):

$$A \cap (A \cup B) = A \cup (A \cap B) = A,$$
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

4. Покажите, что из любого семейства n множеств с помощью операций пересечения и объединения можно построить лишь конечное число различных множеств.

5. Докажите, что для любых двух конечных множеств A, B справедливо равенство

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

6. Найдите мощность декартова произведения конечных множеств $A_1, \ldots, A_n$.

7. Сколько существует различных отображений $f\colon A \to B$, если A, B — конечные множества, $|A| = m$, $|B| = n$?

8. Пусть $f\colon M \to N$, $A_1, A_2 \subset M$, $B_1, B_2 \subset N$ и $* \in \{\cup, \cap, \setminus\}$. Выясните, какие из следующих равенств справедливы в любых случаях, а какие — не всегда:

$$f(A_1 * A_2) = f(A_1) * f(A_2),$$
$$f^{-1}(B_1 * B_2) = f^{-1}(B_1) * f^{-1}(B_2).$$

9. В обозначениях задачи 8 выясните условия, при которых справедливы равенства:

$$f^{-1}(f(A_1)) = A_1, \quad f(f^{-1}(B_1)) = B_1.$$

10. Пусть $f_1, f_2\colon A \to B$ и $\varphi_1, \varphi_2\colon B \to C$. Выясните, при каких условиях справедливы импликации

$$f_1\varphi_1 = f_1\varphi_2 \;\Rightarrow\; \varphi_1 = \varphi_2,$$
$$f_1\varphi_1 = f_2\varphi_1 \;\Rightarrow\; f_1 = f_2.$$

11. Докажите методом полной математической индукции следующие утверждения:

а) $\sum\limits_{i=1}^{n} i^2 = \dfrac{n(n+1)(2n+1)}{6}$;

б) $\sum\limits_{i=1}^{n} i^3 = \dfrac{(n(n+1))^2}{4}$;

в) если $M_1, \ldots, M_n$ — конечные множества, то

$$\Big|\bigcup_{i=1}^{n} M_i\Big| = \sum_{i=1}^{n} |M_i| - \sum_{1 \leqslant i_1 < i_2 \leqslant n} |M_{i_1} \cap M_{i_2}| +$$

$$+ \sum_{1 \leqslant i_1 < i_2 < i_3 \leqslant n} |M_{i_1} \cap M_{i_2} \cap M_{i_3}| - \ldots + (-1)^{n-1} |M_1 \cap M_2 \cap \ldots \cap M_n|.$$

Это равенство называется *формулой включения-исключения*.

12. Пользуясь аксиомами натурального ряда, докажите свойства ассоциативности и коммутативности операций сложения и умножения натуральных чисел.

Глава 2

ЭЛЕМЕНТЫ КОМБИНАТОРИКИ

Комбинаторика, или комбинаторный анализ, является большим самостоятельным разделом современной математики, играющим важную роль во всех других областях математики и ее приложениях. В комбинаторике, в частности, изучаются методы построения и перечисления различных комбинаций объектов, удовлетворяющих тем или иным условиям.

Простейшими комбинациями объектов некоторого множества являются его произвольные подмножества, его системы элементов, расположенных в определенном порядке, разбиения множества и др. При изучении алгебры часто возникает необходимость построения и подсчета числа различных комбинаций элементов, их упорядочиваний и группирований. В связи с этим приведем простейшие сведения комбинаторного характера.

§ 1. ОТНОШЕНИЯ НА МНОЖЕСТВАХ. ОТНОШЕНИЯ ЭКВИВАЛЕНТНОСТИ И ЧАСТИЧНОГО ПОРЯДКА

В теории и на практике обычно приходится иметь дело с такими множествами, между элементами которых существуют определенные связи, или отношения. Так, можно рассматривать в коллективах людей отношения родства, соседства, старшинства и др., на множестве прямых пространства — отношения параллельности, перпендикулярности и др., на множестве целых чисел — отношения равенства, делимости и др.

Попытаемся, исходя из знакомых примеров, сформулировать строгое определение понятия отношения на множестве. С этой целью проанализируем один пример подробнее. Рассмотрим отношение "a делит b" на множестве целых чисел $M = \{2, 3, 4, 5, 6, 7, 8\}$. Это отношение задается известным правилом, позволяющим выяснить, делится одно целое число на другое, или нет. Пользуясь этим правилом, из всех пар чисел (a, b) множества M выпишем все те пары, в которых число a делит b. Получим множество пар

$$(2,2),\ (2,4),\ (2,6),\ (2,8),\ (3,3),\ (3,6),$$
$$(4,4),\ (4,8),\ (5,5),\ (6,6),\ (7,7),\ (8,8).$$

Аналогично, множеством пар можно задать отношение «больше» на множестве M (перечислив все пары $\{a, b\}$, в которых $a, b \in M$ и $a > b$) и другие отношения. Эти примеры делают естественным

Определение 1. *Бинарным отношением на множестве* A называют любое подмножество ρ множества A^2 (т. е. декартова квадрата множества A).

По аналогии с этим, *n-арным отношением* на множестве A называют любое подмножество множества A^n. Ниже мы будем рассматривать лишь бинарные отношения и потому слово «бинарное» будем опускать.

Если ρ — отношение на A и $(a,b) \in \rho$, то говорят, что элемент a находится в отношении ρ к элементу b. Этот факт записывают также в виде $a \rho b$ (например, $a < b$, $a > b$, $a \parallel b$, $a \perp b$ и т. д.).

Отношения на множестве могут обладать различными свойствами. Наиболее важные свойства отношений выделяются следующим определением.

Определение 2. Отношение ρ на множестве A называется

1) *рефлексивным*, если $\forall\, a \in A\colon\ (a \rho a)$,
2) *симметричным*, если $\forall\, a, b \in A\colon\ (a \rho b \Rightarrow b \rho a)$,
3) *транзитивным*, если $\forall\, a, b, c \in A\colon\ (a \rho b,\ b \rho c \Rightarrow a \rho c)$,
4) *антисимметричным*, если $\forall\, a, b \in A\colon\ (a \rho b,\ b \rho a \ \Rightarrow\ a = b)$.

Например, отношение делимости и отношение «$\leqslant$» на множестве $\mathbb{N}$ рефлексивны, антисимметричны и транзитивны. Отношение параллельности прямых симметрично и транзитивно. Отношение перпендикулярности прямых симметрично и не обладает другими свойствами из 1–4.

Через свойства 1–4 определяются важнейшие для всей математики отношения эквивалентности и частичного порядка.

Определение 3. Бинарное отношение ρ на множестве A называется *отношением эквивалентности*, если оно рефлексивно, симметрично и транзитивно. При этом элементы, находящиеся в отношении ρ, называют эквивалентными (точнее, ρ-эквивалентными).

Значение отношений эквивалентности на множестве A определяется, главным образом, тем, что они индуцируют разбиения множества A на непересекающиеся классы эквивалентных элементов. А именно, имеет место

Теорема 1. *Если ρ — отношение эквивалентности на множестве A, то A распадается на непересекающиеся подмножества так, что для любых $a, b \in A$ элементы a, b содержатся в одном подмножестве в том и только том случае, когда $a \rho b$.*

□ Обозначим через $[a]_\rho$ подмножество элементов из A, эквивалентных a, т. е.

$$[a]_\rho = \{x \in A\colon\ x \rho a\},$$

и докажем, что

$$A = \bigcup_{a \in A} [a]_\rho \tag{1}$$

и

$$\forall\, a, b \in A:\ ([a]_\rho \cap [b]_\rho = \varnothing \ \text{ или } \ [a]_\rho = [b]_\rho). \tag{2}$$

Так как ρ рефлексивно, то $a \in [a]_\rho$ для любого $a \in A$, и равенство (1) верно. Вместо утверждения (2) докажем эквивалентное ему утверждение:

$$\forall\, a, b \in A:\ ([a]_\rho \cap [b]_\rho \neq \varnothing) \ \Rightarrow \ ([a]_\rho = [b]_\rho). \tag{3}$$

Пусть c — общий элемент множеств $[a]_\rho$, $[b]_\rho$ и x — любой элемент из $[a]_\rho$, т. е.

$$c \,\rho\, a,\ c \,\rho\, b,\ x \,\rho\, a.$$

Отсюда и из свойств симметричности и транзитивности отношения ρ следует, что $x \,\rho\, b$. Таким образом, для любого $x \in A$ справедлива импликация

$$x \,\rho\, a \Rightarrow x \,\rho\, b.$$

Это означает, что $[a]_\rho \subset [b]_\rho$. Аналогично получается и обратное включение. Следовательно, $[a]_\rho = [b]_\rho$, и утверждение (3) доказано.

Если в правой части равенства (1) оставить лишь все попарно различные множества, то получим искомое разложение множества A в объединение непустых и попарно непересекающихся подмножеств. □

Разложение (1) называют *разбиением* множества A, *индуцированным отношением эквивалентности* ρ. При этом подмножества $[a]_\rho$ называют *классами эквивалентности* отношения ρ. Легко показать что любое разбиение множества индуцируется подходящим отношением эквивалентности. Покажите, что разбиение $\bigcup_{i\in I} A_i$ множества A индуцируется следующим отношением эквивалентности ρ на A:

$$\forall\, a, b \in A:\ (a \,\rho\, b \ \Leftrightarrow \ \exists\, i \in I:\ a, b \in A_i).$$

Известными из средней школы примерами отношений эквивалентности являются: отношения равносильности уравнений с одним неизвестным x (ему соответствует разбиение множества всех уравнений от x на классы равносильных уравнений), отношение «параллельны или равны» на множестве прямых пространства (ему соответствует разбиение всех прямых на классы параллельных прямых), отношение подобия треугольников на плоскости (ему соответствует разбиение множества всех треугольников на классы подобных треугольников).

Определение 4. Бинарное отношение на множестве A называется *отношением частичного порядка*, если оно рефлексивно, транзитивно и антисимметрично. Множество с заданным на нем отношением частичного порядка называют *частично упорядоченным*.

Типичными примерами частичного порядка являются отношение теоретико-множественного включения на множестве всех подмножеств некоторого множества, отношение делимости на множестве $\mathbb{N}$, отношение $\leqslant$ на множестве $\mathbb{R}$ и др.

§ 2. СОЧЕТАНИЯ, РАЗМЕЩЕНИЯ И ПЕРЕСТАНОВКИ ЭЛЕМЕНТОВ КОНЕЧНОГО МНОЖЕСТВА

Определение 5. *Сочетанием* из n элементов множества $A=\{a_1,\dots,a_n\}$ по k называется любое k-элементное подмножество множества A.

Определение 6. *Размещением* из n элементов множества $A=\{a_1,\dots,a_n\}$ по k называется любой упорядоченный набор k различных элементов множества A. В частности, любой упорядоченный набор всех n элементов множества A, взятых по одному разу, называется *перестановкой* элементов множества A. Размещение из элементов множества A по k обычно записывают в виде

$$(a_{i_1}, a_{i_2}, \dots, a_{i_k}).$$

В дальнейшем нам наиболее часто придется встречаться с перестановками. В связи с этим для множества всех перестановок из элементов множества A введем специальное обозначение $P(A)$.

Найдем число различных сочетаний, размещений и перестановок из элементов множества A. Так как эти числа, очевидно, не зависят от природы элементов множества A, то можно взять

$$A=\{1,2,\dots,n\}=\overline{1,n}.$$

В этом случае говорят просто о сочетаниях и размещениях из n по k. Введем следующие обозначения:

C_n^k или $\binom{n}{k}$ — число различных сочетаний из n по k,

A_n^k или $(n)_k$ — число различных размещений из n по k,

$n!=1\cdot 2\cdot\ldots\cdot n$ (читается: n-факториал), $0!=1$.

Теорема 2. *Для любых натуральных чисел k и $n\geqslant k$ имеют место равенства*

$$A_n^k=\frac{n!}{(n-k)!}, \tag{4}$$

$$|P(\overline{1,n})|=n!, \tag{5}$$

$$C_n^k=\frac{n!}{k!(n-k)!}. \tag{6}$$

□ Сначала индукцией по k докажем утверждение (4) (для любого $n\geqslant k$). При $k=1$ оно проверяется непосредственно. Допустим, что оно верно для всех $k\leqslant m$, и докажем его для $k=m+1$. С этой целью укажем метод построения всех размещений из n по $m+1$, использующий размещения из n по m.

Возьмем любое размещение из n по m:

$$s=(i_1,i_2,\dots,i_m)$$

и будем поочередно добавлять к нему в конце по одному из оставшихся (т. е. не вошедших в s) элементов множества $\overline{1,n}$. Получим $n-m$ различных размещений

вида $(i_1, i_2, \ldots, i_m, j)$ из n по $m+1$. Если такую же процедуру провести, начав с другого размещения s' из n по m, то получим еще $n-m$ различных размещений из n по $m+1$, причем все они будут отличны от ранее полученных, поскольку различны s и s'. Отсюда видно, что, перебрав все размещения из n по m, получим ровно

$$A_n^m \cdot (n-m) \tag{7}$$

различных размещений из n по $m+1$. Заметим, что среди полученных размещений содержится любое размещение $(b_1, b_2, \ldots, b_{m+1})$ из n по $m+1$. Действительно, к размещению $(b_1, b_2, \ldots, b_m)$ из n по m мы добавляли в конце каждый из оставшихся элементов, а поэтому должны были добавить и элемент b_{m+1}. Таким образом, (7) есть в точности число всех размещений из n по $m+1$. Отсюда, используя предположение индукции, получим

$$A_n^{m+1} = A_n^m(n-m) = \frac{n!}{(n-m)!}(n-m) = \frac{n!}{(n-(m+1))!},$$

что и свидетельствует о справедливости утверждения (4) для $k = m+1$. Тем самым, по аксиоме полной математической индукции, равенство (4) доказано для любого k и любого $n \geqslant k$, или, что все равно, для любого n и любого $k \in \overline{1,n}$.

Формула (5) получается из формулы (4) при $k = n$. Докажем формулу (6). Для этого заметим, что, осуществляя всевозможные перестановки элементов в любом сочетании из n по k, мы получим из него $k!$ различных размещений. При этом размещения, получаемые из разных сочетаний, будут различными, и таким образом могут быть получены все размещения из n по k. Следовательно, число размещений из n по k в $k!$ раз больше числа сочетаний из n по k, т. е. $A_n^k = C_n^k \cdot k!$. Подставляя сюда значения A_n^k из формулы (4), получим формулу (6). $\square$

Замечание 1. В целях общности и в соответствии с содержательным смыслом числа A_n^k, C_n^k определяются также и для $k = 0$ при любом n, включая $n = 0$. А именно, при $n = 0$ или $k = 0$ они считаются равными 1. «Физический» смысл этого соглашения понятен: существует ровно одно сочетание и одно размещение из элементов пустого множества. Легко видеть, что формулы (4)–(6) остаются в силе и для этих значений n, k.

Числа C_n^k обладают рядом интересных и широко используемых в математике свойств. Так, непосредственной проверкой с учетом формулы (6) доказывается

Следствие. *Для любых чисел $k, n \in \mathbb{N}_0$, удовлетворяющих условиям $k \leqslant n$ или $1 \leqslant k < n$, выполняются соответственно равенства*

(а) $C_n^k = C_n^{n-k}$,

(б) $C_n^k = C_{n-1}^k + C_{n-1}^{k-1}$.

Теорема 3. *Для любого натурального числа n и любых чисел a, b справедливо равенство*

$$(a+b)^n = C_n^0 a^n + C_n^1 a^{n-1} b + \ldots + C_n^k a^{n-k} b^k + \ldots + C_n^n b^n. \tag{8}$$

□ Доказательство проведем методом полной математической индукции по числу n. При $n = 1$ равенство (8) очевидно. Допустим, что оно верно для $n = m$, где $m \in \mathbb{N}$, и докажем его справедливость для $n = m + 1$. Используя предположение индукции, получим

$$(a+b)^{m+1} = (a+b)(a+b)^m = (a+b)(C_m^0 a^m + C_m^1 a^{m-1}b + \ldots + C_m^m b^m).$$

Перемножив выражения в правой части последнего равенства и воспользовавшись равенством (б) для чисел C_n^k из следствия теоремы 2, будем иметь:

$$\begin{aligned}(a+b)^{m+1} &= C_m^0 a^{m+1} + (C_m^1 + C_m^0)a^m b + (C_m^2 + C_m^1)a^{m-1}b^2 + \ldots \\ &\ldots + (C_m^k + C_m^{k-1})a^{m+1-k}b^k + \ldots + (C_m^m + C_m^{m-1})ab^m + C_m^m b^{m+1} = \\ &= C_{m+1}^0 a^{m+1} + C_{m+1}^1 a^m b + \ldots + C_{m+1}^k a^{m+1-k}b^k + \ldots + C_{m+1}^{m+1} b^{m+1}.\end{aligned}$$

Отсюда видно, что формула (8) справедлива и для $n = m + 1$. □

Замечание 2. Формула (8) носит название *формулы бинома Ньютона*. Она позволяет находить в явном виде все натуральные степени двучлена, или бинома $a + b$. В связи с этим числа C_n^k называют *биномиальными коэффициентами*.

Следствие 1. *Для любого $n \in \mathbb{N}$ выполняются соотношения*:

(в) $C_n^0 + C_n^1 + \ldots + C_n^n = 2^n$;

(г) $C_n^0 - C_n^1 + C_n^2 - \ldots + (-1)^n C_n^n = 0$;

(д) $C_n^0 + C_n^2 + C_n^4 + \ldots = C_n^1 + C_n^3 + C_n^5 + \ldots = 2^{n-1}$.

□ Равенства (в), (г) получаются из формулы (8) соответственно при $a = 1$, $b = 1$ и $a = 1$, $b = -1$. Равенство (д) следует непосредственно из (в), (г). □

Если учесть, что C_n^k есть число k-элементных подмножеств n-элементного множества, то из (в) получим

Следствие 2. *Число всех подмножеств n-элементного множества равно 2^n.*

§ 3. ПЕРЕСТАНОВКИ И ИХ КЛАССИФИКАЦИЯ

Рассмотрим всевозможные перестановки множества $\overline{1,n}$.

Определение 7. Говорят, что в перестановке $s = (i_1, i_2, \ldots i_n)$ числа i_k, i_l образуют *инверсию* (или беспорядок), если большее из них расположено левее меньшего, т. е. $i_l > i_k$ и $l < k$ или $i_k > i_l$ и $k < l$.

Число инверсий в заданной перестановке $s \in P(\overline{1,n})$ можно найти, например, следующим образом. Сначала найдем, сколько чисел образуют инверсии с единицей, т. е. расположены в s левее единицы, затем — сколько чисел, отличных от 1, образуют инверсии с двойкой, т. е. расположены в s левее двойки, и т. д. Сумма полученных чисел и будет искомым числом инверсий.

Пример 1. В перестановке $(3,2,5,1,7,4,6)$ инверсии образуют следующие пары чисел:

$$\{3,1\},\ \{2,1\},\ \{5,1\},\ \{3,2\},\ \{5,4\},\ \{7,4\},\ \{7,6\}.$$

Следовательно, в ней 7 инверсий.

Определение 8. Перестановку называют *четной*, если она содержит четное число инверсий, и *нечетной* в противном случае.

Легко видеть, что при любом $n > 1$ среди всех перестановок из $P(\overline{1,n})$ имеются как четные, так и нечетные. Например, перестановка

$$(1,2,3,\ldots,n)$$

имеет 0 инверсий и, значит, является четной. Переставив в ней 1 и 2, мы получим перестановку с одной инверсией, то есть нечетную перестановку.

Определение 9. Преобразование перестановки, заключающееся в перемене местами каких-либо двух ее элементов, называется *транспозицией*.

Теорема 4. *Если перестановка s' получена из перестановки s с помощью одной транспозиции, то s и s' являются перестановками разной четности.*

□ Рассмотрим два случая.

1. Элементы i, j, меняющиеся местами при транспозиции, находятся в перестановке s рядом. Тогда условно перестановки s и s' можно записать в виде

$$s = (s_1, i, j, s_2), \quad s' = (s_1, j, i, s_2),$$

где s_1 и s_2 — перестановки чисел, расположенных в s соответственно левее i и правее j.

Пусть $\{a,b\}$ — любая пара чисел из перестановки s. Если $\{a,b\} \neq \{i,j\}$, то, очевидно, числа a,b образуют или не образуют инверсии одновременно как в s, так и в s'. Если же $\{a,b\} = \{i,j\}$, то ясно, что в одной из перестановок s, s' числа a,b образуют инверсию, а в другой — нет. Значит, число инверсий в перестановке s' отличается от числа инверсий в перестановке s ровно на 1 (в ту или другую сторону), и поэтому перестановки s, s' имеют разную четность.

2. Элементы i,j, меняющиеся местами при транспозиции, не находятся в перестановке s рядом, т. е.

$$s = (s_1, i, i_1, i_2, \ldots, i_k, j, s_2).$$

В этом случае транспозицию чисел i, j можно осуществить следующим образом. Сначала i поменяем последовательно местами с $i_1, i_2, \ldots, i_k$, а затем j поменяем местами последовательно с $i, i_k, \ldots, i_2, i_1$. При этом будет произведено $2k+1$ транспозиций соседних элементов, и, по доказанному в случае 1, четность при переходе от s к s' изменится $2k+1$ раз. Так как число $2k+1$ нечетное, то отсюда и следует, что перестановки s и s' имеют разную четность. □

Следствие. *Если $n > 1$, то число четных перестановок множества $\overline{1,n}$ равно числу нечетных перестановок этого множества и равно $n!/2$.*

□ Пусть A_0, A_1 — соответственно множества всех четных и всех нечетных перестановок из $P(\overline{1,n})$. Зафиксируем различные числа $k, l \in \overline{1,n}$ и в каждой перестановке $s \in P(\overline{1,n})$ поменяем местами элементы, расположенные на k-м и l-м местах. Этим задается отображение $\sigma\colon P(\overline{1,n}) \to P(\overline{1,n})$. Заметим, что σ разные перестановки s и s' переводит в разные. Действительно, если в s и s' на месте с номером r были разные элементы и $r \notin \{k,l\}$, то на r-м месте будут разными элементы и в перестановках $\sigma(s)$, $\sigma(s')$. Если же $r = k$ или $r = l$, то в перестановках $\sigma(s)$, $\sigma(s')$ разными будут элементы соответственно на l-м и k-м местах. Следовательно, отображение σ инъективно, и так как $P(\overline{1,n})$ — конечное множество, то по утверждению 5 главы 1 σ биективно. Из теоремы 4 следует, что σ переводит A_0 в A_1 и A_1 в A_0. Значит, $|A_0| \leqslant |A_1|$, $|A_1| \leqslant |A_0|$, и поэтому $|A_0| = |A_1| = n!/2$. □

Введем на множестве $P(\overline{1,n})$ *функцию четности*

$$\delta(s) = (-1)^{I(s)},$$

где $I(s)$ — число инверсий в перестановке s. Укажем некоторые свойства функции $\delta(s)$.

Утверждение 5. *Если $(i_1, i_2, \ldots, i_n)$ — перестановка множества $\overline{1,n}$ и таблица $A = \begin{pmatrix} j_1 & j_2 & \ldots & j_n \\ 1 & 2 & \ldots & n \end{pmatrix}$ получена из таблицы $B = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$ перестановкой столбцов, то*

$$\delta(j_1, j_2, \ldots, j_n) = \delta(i_1, i_2, \ldots, i_n). \tag{9}$$

□ С любой таблицей вида $C = \begin{pmatrix} r_1 & r_2 & \ldots & r_n \\ t_1 & t_2 & \ldots & t_n \end{pmatrix}$, в которой верхняя и нижняя строки являются перестановками множества $P(\overline{1,n})$, сопоставим число

$$\Delta(C) = \delta(r_1, r_2, \ldots, r_n) \cdot \delta(t_1, t_2, \ldots, t_n).$$

Пусть таблица $C' = \begin{pmatrix} r'_1 & r'_2 & \ldots & r'_n \\ t'_1 & t'_2 & \ldots & t'_n \end{pmatrix}$ получена из C перестановкой двух столбцов. Тогда перестановка $(r'_1, r'_2, \ldots, r'_n)$ получена из перестановки $(r_1, r_2, \ldots, r_n)$ с помощью одной транспозиции, и поэтому числа $I(r_1, r_2, \ldots, r_n)$, $I(r'_1, r'_2, \ldots, r'_n)$ имеют разную четность. По этой же причине числа $I(t_1, t_2, \ldots, t_n)$, $I(t'_1, t'_2, \ldots \ldots, t'_n)$ также имеют разную четность. Отсюда следует, что $\Delta(C) = \Delta(C')$. Так как таблицу B можно получить из таблицы A с помощью последовательности транспозиций столбцов, то $\Delta(A) = \Delta(B)$, то есть

$$\delta(j_1, j_2, \ldots, j_n) \cdot \delta(1, 2, \ldots, n) = \delta(1, 2, \ldots, n) \cdot \delta(i_1, i_2, \ldots, i_n).$$

Отсюда следует равенство (9). □

Замечание 3. Точно так же, как для перестановок чисел $1, 2, \ldots, n$, можно определить понятия инверсии, транспозиции, четности и нечетности, функции четности для перестановки любых попарно различных чисел $a_1, a_2, \ldots, a_n$. Ниже при необходимости мы будем без оговорок пользоваться этими понятиями.

Утверждение 6. *Если* $s = (i_1, \ldots, i_n) \in P(\overline{1,n})$ *и* $k \in \overline{1,n}$, *то*

$$\delta(s) = \delta(i_1, \ldots, i_k)\,\delta(i_{k+1}, \ldots, i_n)\,(-1)^r, \tag{10}$$

где $r = i_1 + \ldots + i_k - (1 + \ldots + k)$.

□ Из определения функции четности имеем равенство

$$\delta(s) = \delta(i_1, \ldots, i_k)\,\delta(i_{k+1}, \ldots, i_n)\,(-1)^r,$$

где r — число инверсий, которые образуют числа из множества $M_1 = \{i_1, \ldots, i_k\}$ с числами из множества $M_2 = \{i_{k+1}, \ldots, i_n\}$. Найдем число r. Выберем сначала наименьшее число из M_1, пусть это есть i_{α_1}. Чисел, меньших чем i_{α_1}, во множестве $\overline{1,n}$ существует ровно $i_{\alpha_1} - 1$ и все они лежат в M_2, поскольку в M_1 число i_{α_1} — наименьшее. Таким образом, число i_{α_1} из M_1 с числами из M_2 образует $i_{\alpha_1} - 1$ инверсий. Теперь возьмем в M число i_{α_2}, следующее по величине за i_{α_1}, и таким же образом найдем число инверсий, которые образует i_{α_2} с элементами из M_2. Так как все числа, меньшие его, кроме i_{α_1}, лежат в M_2, то указанное число инверсий равно $i_{\alpha_2} - 2$. Продолжая этот процесс, найдем:

$$r = (i_{\alpha_1} - 1) + (i_{\alpha_2} - 2) + \ldots + (i_{\alpha_k} - k) = (i_1 + \ldots + i_k) - (1 + \ldots + k). \quad \square$$

Утверждение 7. *Если в перестановке* $s \in P(\overline{1,n})$ *имеется* t *инверсий, то от нее можно перейти к перестановке* $s_0 = (1, \ldots, n)$ *с помощью последовательности из* t *транспозиций соседних элементов.*

Докажите это утверждение в качестве упражнения, используя указанный в начале параграфа способ подсчета числа инверсий.

ЗАДАЧИ

1. Сколько различных бинарных отношений можно задать на множестве из 5 элементов? Сколько среди них отношений эквивалентности?

2. Является ли бинарное отношение ρ отношением эквивалентности на множестве A:

а) $A = \mathbb{N} \setminus \{1\}$; $a \,\rho\, b \;\Leftrightarrow\; \exists\, d \in A :\; d \mid a,\; d \mid b$;

б) $A = \mathbb{R}$; $a \,\rho\, b \;\Leftrightarrow\; |a - b| \in \mathbb{Q}$;

в) $A = P(\overline{1,n})$; $s \,\rho\, s' \;\Leftrightarrow\; I(s) = I(s')$;

г) $A = P(\overline{1,n})$; $s \,\rho\, s' \;\Leftrightarrow\; \delta(s) = \delta(s')$.

3. На множестве A^4, где $A = \{0, 1\}$, заданы бинарные отношения ρ_1, ρ_2 так, что для $\alpha = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, $\beta = (\beta_1, \beta_2, \beta_3, \beta_4) \in A^4$:

$$\alpha \,\rho_1\, \beta \;\Leftrightarrow\; \exists\, i \in \overline{1,4}\colon\ \alpha_i \leqslant \beta_i, \quad \alpha \,\rho_2\, \beta \;\Leftrightarrow\; \forall\, i \in \overline{1,4}\colon\ \alpha_i \leqslant \beta_i.$$

Выясните, являются ли они отношениями частичного порядка?

4. Сколькими способами можно расставить на книжной полке книги n различных наименований, если имеется m_k экземпляров книг k-го наименования, $k \in \overline{1,n}$, при условии, что книги одного наименования неразличимы?

5. Сколько в множестве A^n существует наборов, содержащих не менее $n-1$, $n-2$ различных элементов, если $|A| = n$?

6. Сколько существует последовательностей из нулей и единиц, в которых встречается ровно p нулей и ровно q единиц? Сколько из них не содержат рядом стоящих единиц?

7. Сколькими способами, с учетом порядка слагаемых, можно представить натуральное число n в виде суммы k натуральных слагаемых?

8. Сколько существует различных инъективных, сюръективных и биективных отображений множества из m элементов в множество из n элементов?

9. Докажите равенства:

а) $\sum\limits_{i=0}^{k} C_m^i C_n^{k-i} = C_{m+n}^k$, $m, n, k \in \mathbb{N}$, $k \leqslant m$, $k \leqslant n$;

б) $\sum\limits_{i=0}^{n} i C_n^i = n \cdot 2^{n-1}$.

10. Пусть перестановки s_1, s_2 из $P(\overline{1,n})$ содержат соответственно t_1 и t_2 инверсий. Докажите, что от s_1 к s_2 можно перейти с помощью $t_1 + t_2$ транспозиций.

Глава 3

ОСНОВНЫЕ АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ

§ 1. БИНАРНЫЕ ОПЕРАЦИИ И ИХ СВОЙСТВА

Как было отмечено в § 1 главы 1, *бинарной операцией* на множестве A называют отображение A^2 в A.

Если $f\colon A^2 \to A$ — бинарная операция на A и $(a,b) \in A^2$, то образ пары (a,b) при отображении f называют *значением операции* f на элементах a, b, или *результатом применения операции* f к элементам a, b, и обозначают в виде $f(a,b)$ или afb (например, $a+b$, $a \cdot b$, $a \cup b$ и т. д.).

Особо подчеркнем, что значение операции определено однозначно для любых элементов a, b из A и обязательно принадлежит A.

Приведем примеры бинарных операций.

Пример 1. Известные из средней школы правила сложения и умножения чисел задают бинарные операции на любом из множеств $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.

Пример 2. Правило нахождения разности чисел задает бинарные операции на множествах $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и не задает операций на множествах $\mathbb{N}$ и $\mathbb{N}_0$.

Пример 3. Пусть f_1, f_2 — отображения множества $(\overline{1,n})^2$ в $\overline{1,n}$, определенные равенствами

$$f_1(a,b) = \max\{a,b\}, \qquad f_2(a,b) = \min\{a,b\}.$$

Так как для любых элементов a, b из $\overline{1,n}$ максимум и минимум однозначно определены и содержатся в $\overline{1,n}$, то отображения f_1, f_2, являются бинарными операциями на множестве $\overline{1,n}$.

Пример 4. Рассмотрим множество $\widetilde{M}$ всех подмножеств фиксированного множества M. Так как пересечение и объединение любых двух подмножеств из M являются вполне определенными подмножествами из M, то пересечение и объединение множеств являются бинарными операциями на $\widetilde{M}$.

Пример 5. Пусть $\Pi(M)$ — множество всех преобразований фиксированного непустого множества M (т. е. множество всевозможных отображений множества M в себя). Бинарными операциями на множестве $\Pi(M)$ являются введенные в § 2 главы 1 умножение и композиция отображений.

Пример 6. Обозначим через $B(M)$ множество всех бинарных отношений на непустом множестве M. Для каждой пары отношений ρ_1, ρ_2 из $B(M)$ определим отношение ρ, положив

$$\forall\, a, b \in M:\ \ (a\,\rho\, b\ \Leftrightarrow\ \exists\, c \in M:\ \ (a\,\rho_1\, c)\ \&\ (c\,\rho_2\, b)).$$

Отношение ρ называется *произведением отношений* ρ_1, ρ_2 и обозначается через $\rho_1\rho_2$. Умножение отношений есть бинарная операция на множестве $B(M)$.

Из приведенных примеров видно, сколь разнообразными по своей природе могут быть бинарные операции на множествах. В связи с этим для облегчения изучения множеств с операциями их классифицируют по свойствам операций.

Определение 1. Бинарная операция $*$ на множестве M называется *ассоциативной*, если для любых элементов $a, b, c \in M$ выполняется равенство

$$(a * b) * c = a * (b * c).$$

Ассоциативными являются все операции из примеров 1, 3, 4, 5, 6. Для операции примера 1 это известно из средней школы, для операции примеров 3, 4 это очевидно. Для операции примера 5 это следует из утверждения 1 главы 1. Для операции примера 6 это устанавливается ниже.

Утверждение 1. *Пусть M — произвольное непустое множество. Операция умножения бинарных отношений, определенных на множестве M, ассоциативна.*

□ Непосредственно из определения произведения бинарных отношений следует, что каждое из соотношений

$$a\,(\rho_1\rho_2)\rho_3\, b, \quad a\,\rho_1(\rho_2\rho_3)\, b,$$

выполняется тогда и только тогда, когда

$$\exists\, c, d \in M:\ \ a\,\rho_1\, c,\ \ c\,\rho_2\, d,\ \ d\,\rho_3\, b.$$

Следовательно, $(\rho_1\rho_2)\rho_3 = \rho_1(\rho_2\rho_3)$. □

Заметим, что операции примера 2 (вычитание на множествах чисел $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$) не ассоциативны.

Главная роль свойства ассоциативности заключается в том, что оно позволяет не расставлять скобки при оперировании со многими элементами.

Определение 2. Бинарная операция $*$ на множестве M называется *коммутативной*, если для любых элементов $a, b \in M$ выполняется равенство

$$a * b = b * a. \tag{1}$$

Легко видеть, что операции примеров 1, 3, 4 коммутативны. Операции примера 2 не коммутативны. Вопрос о коммутативности операций примеров 5, 6 решается в зависимости от мощности множества M.

Утверждение 2. *Операции умножения и композиции на множестве преобразований* $\Pi(M)$*, а также умножения на множестве бинарных отношений* $B(M)$*, коммутативны в том и только в том случае, когда* $|M| = 1$.

□ Если $|M| = 1$, то $|\Pi(M)| = 1$, $|B(M)| = 2$, и коммутативность указанных в утверждении операций очевидна. Пусть $|M| > 1$ и a_1, a_2 — различные элементы из M. Определим отображения $f_1, f_2 \colon M \to M$, положив $f_1(x) = a_1$, $f_2(x) = a_2$ для всех $x \in M$. Тогда

$$(f_1 \circ f_2)(a_1) = f_1(f_2(a_1)) = a_1, \quad (f_2 \circ f_1)(a_1) = f_2(f_1(a_1)) = a_2.$$

Следовательно, $f_1 \circ f_2 \neq f_2 \circ f_1$, а потому и $f_1 f_2 \neq f_2 f_1$.

Пример, показывающий некоммутативность умножения бинарных отношений на множестве M, постройте в качестве упражнения. □

Замечание 1. Для отдельных элементов $a, b \in M$ равенство (1) может выполняться и в том случае, когда операция $*$ не коммутативна. Такие элементы называются *перестановочными* (или *коммутирующими*) друг с другом. Так, например, любой элемент множества M перестановочен сам с собой при любой операции $*$.

Замечание 2. Свойства ассоциативности и коммутативности операций независимы, т. е. существуют операции, обладающие любым одним из этих свойств и не обладающие другим. Примеры ассоциативных, но не коммутативных операций уже встречались. Примером коммутативной, но не ассоциативной операции на множестве $\mathbb{R}$ может служить операция нахождения среднего арифметического для действительных чисел:

$$a * b = \frac{a + b}{2}.$$

В случае, когда на одном и том же множестве определены несколько операций, можно говорить о свойствах, связывающих различные операции.

Определение 3. Бинарная операция $*$ на множестве M называется *лево-* или *праводистрибутивной* относительно бинарной операции $\circ$, если для любых элементов из M выполняется соответственно равенство

$$a * (b \circ c) = (a * b) \circ (a * c) \quad \text{или} \quad (b \circ c) * a = (b * a) \circ (c * a).$$

Если выполняются оба этих свойства, то говорят просто о *дистрибутивности* операции $*$ относительно операции $\circ$. В частности, если операция $*$ коммутативна, то правая (левая) дистрибутивность совпадает с дистрибутивностью.

Так, из средней школы известно, что в числовых множествах операция умножения дистрибутивна относительно операции сложения. Заметим, что операция сложения чисел не дистрибутивна относительно умножения.

В примере 4 операция пересечения на множестве $\widetilde{M}$ дистрибутивна относительно операции объединения, а операция объединения дистрибутивна относительно операции пересечения.

В том случае, когда операция $*$ не коммутативна, свойства левой и правой дистрибутивности могут не совпадать. Так, например, на множестве $\widetilde{M}$ операция вычитания праводистрибутивна, но не леводистрибутивна относительно объединения. Покажите это в качестве упражнения.

§ 2. АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ С ОДНОЙ БИНАРНОЙ ОПЕРАЦИЕЙ

Алгебраической структурой или, просто, *алгеброй* называют множество, наделенное системой операций. Область алгебры, изучающая произвольные алгебраические структуры, называется универсальной или общей алгеброй. Несмотря на большую общность этого раздела, в нем имеется ряд интересных содержательных результатов о произвольных алгебраических структурах. Вместе с тем, в связи с потребностями развития математики и ее приложений, наиболее глубоко изучены отдельные узкие классы алгебраических структур, а именно, алгебраические структуры с одной и двумя бинарными операциями, удовлетворяющими определенным условиям. В этой главе будут рассмотрены простейшие свойства таких структур. Более обстоятельное их изучение будет проведено позже, после ознакомления с некоторыми важнейшими примерами таких структур.

Определение 4. Множество $G \neq \varnothing$ с одной бинарной операцией $*$ называют *группоидом* и обозначают через $(G; *)$.

Из определения 4 видно, что для задания группоида нужно задать множество G и то правило, по которому можно найти значение операции $*$ для любых двух элементов из G. В том случае, когда множество G конечно, всю эту информацию можно записать таблицей, в которой входной строкой и входным столбцом является список одинаково упорядоченных элементов множества G, а на пересечении строки с входом a и столбца с входом b располагается значение операции $a * b$.

Такая таблица называется *таблицей Кэли* группоида $(G; *)$ в честь английского математика А. Кэли (1821–1895). Если $G = \{a_1, \ldots, a_n\}$, то таблица Кэли для группоида $(G; *)$ имеет следующий вид:

	a_1	$\ldots$	a_j	$\ldots$	a_n
a_1			$\vdots$	$\ldots$	
$\vdots$			$\vdots$		$\vdots$
a_i	$\ldots$	$\ldots$	$a_i * a_j$	$\ldots$	
$\vdots$					$\vdots$
a_n		$\ldots$		$\ldots$	

Исходя из такого задания группоида, легко подсчитать, сколько различных операций можно определить на множестве G порядка n. В каждую из n^2 клеток таблицы

Кэли можно записать любой из n элементов множества G. Отсюда видно, что таблицу Кэли можно составить в n^{n^2} вариантах, то есть на множестве G из n элементов существует n^{n^2} различных группоидов.

Определение 5. Подмножество $G_1 \neq \varnothing$ группоида $(G;*)$ называется *замкнутым относительно операции* $*$, если выполнено условие

$$\forall\, a, b \in G:\ \ (a, b \in G_1\ \Rightarrow\ a * b \in G_1).$$

При этом группоид $(G_1;*)$ называют *подгруппоидом* в $(G;*)$.

Например, группоиды $(\mathbb{Z};+)$, $(\mathbb{N}_0;+)$, $(\mathbb{N};+)$ являются подгруппоидами группоида $(\mathbb{R};+)$.

Из всех группоидов особо выделяются группоиды с коммутативной операцией. Они называются *коммутативными*. Очевидно, что коммутативность группоида равносильна симметричности его таблицы Кэли относительно главной диагонали.

В некоторых группоидах могут существовать так называемые нейтральные элементы.

Определение 6. Элемент Λ группоида $(G;*)$ называют *нейтральным*, если для любого $a \in G$ выполняются равенства

$$a * \Lambda = \Lambda * a = a. \tag{2}$$

Так, в группоидах $(\mathbb{N}_0;\cdot)$, $(\mathbb{Q};\cdot)$ нейтральным элементом является единица, в группоидах $(\mathbb{N}_0;+)$, $(\mathbb{Q};+)$ — нуль, в группоидах $(\mathbb{Z};-)$, $(\mathbb{N};+)$ нейтральных элементов нет. В группоиде бинарных отношений $(B(M);\circ)$ нейтральным элементом является отношение равенства (проверьте).

Легко видеть, что элемент a_i конечного группоида является нейтральным в том и только в том случае, когда строка и столбец с входами a_i таблицы Кэли этого группоида совпадают соответственно с входной строкой и входным столбцом.

Утверждение 3. *Если в группоиде* $(G;*)$ *существует нейтральный элемент, то он единственный.*

□ Пусть Λ_1, Λ_2 — нейтральные элементы группоида $(G;*)$. Так как Λ_1 — нейтральный элемент, то $\Lambda_1 * \Lambda_2 = \Lambda_2$, а так как Λ_2 — нейтральный, то $\Lambda_1 * \Lambda_2 = \Lambda_1$. Следовательно, $\Lambda_1 = \Lambda_2$. □

В группоиде $(G;*)$ с нейтральным элементом Λ для элемента a могут существовать такие элементы a', что

$$a' * a = \Lambda, \quad a * a' = \Lambda. \tag{3}$$

Определение 7. Элемент a' группоида $(G;*)$ с нейтральным элементом Λ, удовлетворяющий равенствам (3), называют *симметричным для* a.

В общем случае в группоиде с нейтральным элементом Λ элемент a может не иметь симметричных элементов и может иметь один или несколько симметричных элементов. Постройте соответствующие примеры. Более определенно о числе симметричных элементов решается вопрос в группоидах с ассоциативной операцией.

Определение 8. Группоид $(G;*)$ с ассоциативной операцией называется *полугруппой*.

Примерами полугрупп могут служить группоиды, указанные в примерах 1, 3, 4, 5, 6 предыдущего параграфа. Все они являются полугруппами с нейтральным элементом.

Утверждение 4. *Если в полугруппе $(G;*)$ с нейтральным элементом Λ для элемента a существует симметричный элемент, то он единственный.*

□ Пусть a', a'' — симметричные элементы для элемента a. Тогда, используя равенства (2), (3) и ассоциативность операции $*$, получим:

$$a' = a' * \Lambda = a' * (a * a'') = (a' * a) * a'' = \Lambda * a'' = a''. \quad \square$$

Из всех группоидов наибольшую роль в математике играют группоиды, называемые группами.

Определение 9. Группоид $(G;*)$ называется *группой*, если выполнены условия:

1) операция $*$ ассоциативна;

2) в $(G;*)$ существует нейтральный элемент Λ;

3) для каждого элемента $a \in G$ существует симметричный элемент $a' \in G$.

Если, кроме того, выполняется еще условие коммутативности операции $*$, то группа $(G;*)$ называется *коммутативной*, или *абелевой* (в честь Н. Х. Абеля).

Приведем примеры групп. Из группоидов, рассмотренных выше, группами являются $(\mathbb{Z};+)$, $(\mathbb{Q};+)$, $(\mathbb{R};+)$. Все эти группы коммутативны, нейтральным элементом в них является число 0, а симметричным к числу a — противоположное ему число $-a$. Заметим, что группоиды $(\mathbb{Q};\cdot)$, $(\mathbb{R};\cdot)$ являются коммутативными полугруппами с нейтральным элементом 1, однако группами они не являются лишь из-за того, что для нуля не существует симметричного (в данном случае обратного) элемента. Удалив из $\mathbb{Q}$ и $\mathbb{R}$ число нуль, мы получим множества $\mathbb{Q}^*$, $\mathbb{R}^*$, которые являются группами относительно операции умножения. Легко видеть, что группами относительно умножения являются одноэлементное множество чисел $\{1\}$ и двухэлементное $\{1,-1\}$.

Приведем теперь пример некоммутативной группы. Из всех таких групп в дальнейшем особую роль будут играть группы подстановок.

Определение 10. *Подстановкой* непустого множества M называют любое биективное отображение множества M на себя.

Множество всех подстановок множества M обозначим через $S(M)$. Из утверждения 2 главы 1 следует, что множество $S(M)$ замкнуто относительно операций умножения $\cdot$ и композиции $\circ$ отображений. Следовательно, на множестве $S(M)$ определены два группоида $(S(M);\cdot)$ и $(S(M);\circ)$.

Теорема 5. *Группоиды $(S(M);\cdot)$ и $(S(M);\circ)$ являются группами. Эти группы коммутативны тогда и только тогда, когда $|M| \leqslant 2$.*

□ Ассоциативность операций $\cdot$ и $\circ$ на множестве $S(M)$ следует непосредственно из утверждения 1 главы 1. Нейтральным элементом в группоидах $(S(M);\cdot)$ и $(S(M);\circ)$ является тождественное отображение $\varepsilon\colon M \to M$. Симметричным для преобразования $g \in S(M)$ является преобразование g^{-1}, обратное для g. Его существование гарантируется утверждением 4 главы 1. Необходимо подчеркнуть, что отображение g^{-1}, обратное для подстановки g, также является подстановкой (т. е. $g^{-1} \in S(M)$). Это также обеспечивается утверждением 4 главы 1, поскольку равенства $gg^{-1} = g^{-1}g = \varepsilon$ означают не только обратимость g, но и обратимость g^{-1}. Итак, рассматриваемые группоиды являются группами. Рассмотрим вопрос о коммутативности этих групп.

Если $|M| = 1$ или $|M| = 2$, то $S(M)$ состоит соответственно из одной или двух подстановок и коммутативность рассматриваемых групп очевидна. Пусть $|M| > 2$, $a, b, c \in M$. Построим подстановки g_1, g_2 множества M следующим образом. Положим

$$g_1(a) = b,\ g_1(b) = a,\ g_1(x) = x \text{ для } x \in M \setminus \{a, b\};$$
$$g_2(b) = c,\ g_2(c) = b,\ g_2(x) = x \text{ для } x \in M \setminus \{b, c\}.$$

Так как

$$(g_1 \circ g_2)(a) = (g_1(g_2(a))) = g_1(a) = b,$$
$$(g_2 \circ g_1)(a) = (g_2(g_1(a))) = g_2(b) = c,$$

то $g_1 \circ g_2 \neq g_2 \circ g_1$, а поэтому и $g_1 g_2 \neq g_2 g_1$, т. е. рассматриваемые группы не коммутативны. □

Группу $(S(M);\cdot)$ условимся в дальнейшем называть *симметрической группой подстановок* множества M.

В том случае, когда множество M конечно, любую подстановку g из $S(M)$ можно задать таблицей из двух строк, выписав в первой строке все элементы множества M, а во второй записав под каждым элементом его образ при отображении g. Так, если $M = \{a_1, \ldots, a_n\}$ и $g(a_i) = a_{\alpha_i}$, $i \in \overline{1,n}$, то

$$g = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ a_{\alpha_1} & a_{\alpha_2} & \ldots & a_{\alpha_n} \end{pmatrix}.$$

В частности, тождественная подстановка имеет вид

$$\varepsilon = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix},$$

обратную подстановку для g можно записать в виде

$$g^{-1} = \begin{pmatrix} a_{\alpha_1} & a_{\alpha_2} & \ldots & a_{\alpha_n} \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}.$$

Вернемся к определению группы. Из него и утверждений 3, 4 получаем: в группе есть один нейтральный элемент и для каждого элемента a — один симметричный элемент a'. Кроме того, из равенства (3) видно, что $(a')' = a$, $(a * b)' = b' * a'$.

При изучении алгебр и в приложениях многие задачи сводятся к решению уравнений и систем уравнений в этих алгебрах. Поэтому вопросы об условиях разрешимости и методах решения уравнений являются важными в любых алгебраических структурах. В связи с этим, в дальнейшем при изучении конкретных группоидов и других алгебр мы, как правило, будем затрагивать и вопрос о решении простейших уравнений. В группах на этот вопрос отвечает

Теорема 6. *В любой группе* $(G;*)$ *для любых элементов* a, b *однозначно разрешимы уравнения*

$$a * x = b, \quad y * a = b. \tag{4}$$

□ Непосредственной проверкой легко убедиться, что уравнениям (4) удовлетворяют соответственно элементы $x = a' * b$ и $y = b * a'$, где a' — элемент, симметричный a. Остается доказать единственность этих решений. Пусть x_1, x_2 — любые решения уравнения $a * x = b$. Тогда имеем равенство

$$a * x_1 = a * x_2.$$

Умножив обе его части слева на элемент a', получим $x_1 = x_2$. Аналогично доказывается единственность решения и второго уравнения из (4). □

В заключение этого параграфа сделаем одно замечание по терминологии и обозначениям. Само собой разумеется, что свойства группоида не зависят от того, как названа и как обозначена его бинарная операция. В связи с этим, с целью избежания лишних значков и терминов, операции в группоидах обычно называют, как и для чисел, сложением и умножением и обозначают соответственно знаками $+$ и $\cdot$. Употребляемую при этом терминологию и форму записи называют соответственно *аддитивной* и *мультипликативной*.

Приведем сравнительную таблицу этих терминов и обозначений.

Название	Обознач.	Название	Обознач.	Название	Обознач.
Операция	$*$	Сложение	$+$	Умножение	$\cdot$
Результат операции	$a * b$	Сумма	$a + b$	Произведение	$a \cdot b$, ab
Нейтральный элемент	Λ	Нуль	0, θ	Единица	1, e, ε
Симметричный к элементу a	a'	Противоположный к a	$-a$	Обратный к a	a^{-1}
Решение уравнения $x * a = b$	$b * a'$	Разность	$b - a$	Правое частное	ba^{-1}
Решение уравнения $a * x = b$	$a' * b$	Разность	$-a + b$	Левое частное	$a^{-1}b$

Заметим, что аддитивная терминология чаще всего используется для коммутативных группоидов.

В дальнейшем, в основном, будут рассматриваться лишь ассоциативные группоиды. В них результат операций над несколькими элементами не зависит от расстановки скобок и сами скобки, указывающие порядок выполнения операций, чаще всего опускаются. В связи с этим корректной является запись вида

$$a_1 * a_2 * \ldots * a_n. \tag{5}$$

Если при этом $a_1 = a_2 = \ldots = a_n = a$, то вместо (5) пишут: a^n при мультипликативной форме и na при аддитивной форме записи. Элементы a^n и na называют соответственно *n-й степенью* и *n-кратным* элемента a. Непосредственно из определения элементов a^n и na легко следует

Утверждение 7. *Если $(G;\cdot)$ или $(G;+)$ — полугруппы, то для любого элемента $a \in G$ и любых натуральных чисел n_1, n_2 выполняются равенства*

$$a^{n_1} \cdot a^{n_2} = a^{n_1+n_2}, \qquad (a^{n_1})^{n_2} = a^{n_1 n_2}; \tag{6}$$

$$n_1 a + n_2 a = (n_1 + n_2)a, \qquad n_1(n_2 a) = (n_1 n_2)a. \tag{7}$$

Проверьте эти равенства в качестве упражнения.

Если группоид $(G;\cdot)$ или $(G;+)$ является группой, то понятия n-й степени и n-кратного элемента $a \in G$ можно распространить на любое $n \in \mathbb{Z}$, положив соответственно

$$a^0 = e, \qquad a^n = a^{-m} = (a^m)^{-1},$$
$$0a = \theta, \qquad na = (-m)a = -(ma)$$

для $n = -m < 0$. Нетрудно проверить, что в группе $(G;\cdot)$ (или $(G;+)$) равенства (6) (соответственно (7)) выполняются для любого $a \in G$ и любых $n_1, n_2 \in \mathbb{Z}$.

§ 3. КОЛЬЦА И ПОЛЯ

Определение 11. *Кольцом* называется множество R с бинарными операциями сложения $+$ и умножения $\cdot$, удовлетворяющими условиям:

1) $(R;+)$ — абелева группа,

2) $(R;\cdot)$ — полугруппа,

3) операция умножения дистрибутивна относительно сложения.

При этом группа $(R;+)$ называется *аддитивной группой кольца R*, а ее нейтральный элемент 0 — *нулем* кольца R.

Кольцо $(R;+)$ называется *коммутативным*, если операция умножения коммутативна, и кольцом *с единицей*, если $(R;\cdot)$ — полугруппа с единицей.

Примерами коммутативных колец с единицей являются числовые кольца:

$$(\mathbb{Z};+,\cdot), \quad (\mathbb{Q};+,\cdot), \quad (\mathbb{R};+,\cdot).$$

Примером коммутативного кольца без единицы может служить множество $2\mathbb{Z}$ всех четных чисел относительно обычных операций сложения и умножения.

Заметим, что любую абелеву группу $(G;+)$ можно сделать кольцом, задав на ней операцию умножения следующим образом:

$$\forall\, a, b \in G:\ \ (ab = 0).$$

Определение 12. Кольцо R, в котором произведение любых двух элементов равно нулевому элементу, называется *кольцом с нулевым умножением*.

Приведем еще один пример кольца.

Пример 7. Рассмотрим множество $\mathbb{R}^2$ упорядоченных пар действительных чисел:

$$\mathbb{R}^2 = \{(a, b):\ a, b \in \mathbb{R}\}.$$

Введем на множестве $\mathbb{R}^2$ операции сложения и умножения, положив

$$(a, b) + (c, d) = (a + c,\ b + d), \quad (a, b)(c, d) = (ac, bd).$$

Так как операции над парами производятся покомпонентно, то из свойств действительных чисел имеем: операции $+$ и $\cdot$ в $\mathbb{R}^2$ коммутативны и ассоциативны, а операция $\cdot$ дистрибутивна относительно $+$. Нулевым элементом является пара $(0, 0)$, единицей — пара $(1, 1)$, противоположной для пары (a, b) — пара $(-a, -b)$. Следовательно, $(\mathbb{R}^2; +, \cdot)$ является коммутативным кольцом с единицей.

В дальнейшем будет рассмотрено много других колец, в том числе и некоммутативных. Здесь же укажем на некоторые простейшие свойства, верные для любых колец и хорошо известные для чисел.

Теорема 8. *Для любых элементов a, b, c произвольного кольца R с нулем 0 справедливы равенства*:

(а) $a \cdot 0 = 0 \cdot a = 0$;
(б) $-(-a) = a$;
(в) $(-a)b = -(ab),\ \ a(-b) = -(ab)$;
(г) $(-a)(-b) = ab$;
(д) $a(b - c) = ab - ac$;
(е) $m(ab) = (ma)b = a(mb),\ m \in \mathbb{Z}$;
(ж) $(m_1 a)(m_2 b) = (m_1 m_2)(ab),\ m_1, m_2 \in \mathbb{Z}$.

□ (а) Так как $0 + 0 = 0$ по определению нулевого элемента кольца, то получим, что $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$. Прибавив к обеим частям полученного равенства $-(a \cdot 0)$, получим $a \cdot 0 = 0$. Аналогично доказывается равенство $0 \cdot a = 0$.

(б) Непосредственно из определения противоположного элемента получаем:

$$a + (-a) = (-a) + a = 0.$$

Из этих равенств видно, что если $-a$ — противоположный элемент для a, то a — противоположный для $-a$. Последнее означает, что $-(-a) = a$.

(в) Так как $-(ab)$ есть элемент, противоположный к ab, то в силу утверждения 4 для доказательства равенства $(-a)b = -(ab)$ достаточно показать, что $(-a)b$ также противоположен к ab, то есть выполняется равенство $ab + (-a)b = 0$. Используя свойство дистрибутивности умножения относительно сложения в кольце R и свойство (а), получим:

$$ab + (-a)b = (a + (-a))b = 0 \cdot b = 0.$$

Аналогично доказывается равенство $a(-b) = -(ab)$.

(г) Используя свойства (б), (в), получим:

$$(-a)(-b) = -(a(-b)) = -(-(ab)) = ab.$$

(д) $a(b - c) = a(b + (-c)) = ab + a(-c) = ab + (-(ac)) = ab - ac$.

(е) Для доказательства равенств из (е) достаточно воспользоваться определением m-кратного, а также свойством дистрибутивности при $m \in \mathbb{N}$, равенствами (а) при $m = 0$ и равенствами (в) при $m = -n$, где $n \in \mathbb{N}$.

(ж) Доказывается аналогично утверждению (е). □

Если $(R; +, \cdot)$ — кольцо с единицей e, то в нем для элемента $a \neq 0$ может не быть обратного элемента. Вместе с тем для некоторых элементов кольца R (например, для единицы e) обратные элементы существуют. Такие элементы играют в кольце особую роль.

Определение 13. Элемент a кольца R с единицей называется *обратимым*, если для него в R существует обратный элемент a^{-1}.

Множество всех обратимых элементов кольца R обозначают R^*.

Например, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{Z}^* = \{1, -1\}$. Обратимыми элементами кольца $(\mathbb{R}^2; +, \cdot)$ из примера 7 являются все пары вида (a, b), в которых $a \neq 0$ и $b \neq 0$, при этом $(a, b)^{-1} = (a^{-1}, b^{-1})$.

Заметим, что в рассмотренных примерах множества $\mathbb{Q}^*$, $\mathbb{Z}^*$, $(\mathbb{R}^2)^*$ являются группами относительно операции умножения. Этот факт не случаен.

Теорема 9. *Если R — кольцо с единицей, то множество всех его обратимых элементов замкнуто относительно операции умножения в R и является группой.*

□ Покажем сначала, что множество R^* замкнуто относительно операции умножения, определенной в кольце R. Пусть $a, b \in R^*$ и a^{-1}, b^{-1} — обратные к ним элементы. Тогда имеем:

$$(ab)(b^{-1}a^{-1}) = (a(bb^{-1}))a^{-1} = (ae)a^{-1} = aa^{-1} = e$$

и, аналогично, $(b^{-1}a^{-1})(ab) = e$. Следовательно, элемент $b^{-1}a^{-1}$ является обратным для ab, и потому $ab \in R^*$. Таким образом, R^* можно рассматривать как множество с операцией умножения (определенной на R). Эта операция на R^* ассоциативна, так как она ассоциативна на R. Единичный элемент e обратим, поскольку $ee = e$, и потому лежит в R^*. Очевидно, что e — единичный элемент группоида $(R^*; \cdot)$. Если $a \in R^*$ и a^{-1} — обратный элемент для a, то a является обратным для a^{-1}, и значит, $a^{-1} \in R^*$. Из всего сказанного и определения 9 следует, что $(R^*; \cdot)$ — группа. □

Определение 14. Группа $(R^*;\cdot)$ всех обратимых элементов кольца R с единицей называется *мультипликативной группой кольца* R.

Рассмотрим еще вопрос о решении уравнений

$$ax = b, \quad ya = b \tag{8}$$

в произвольном кольце R с единицей.

Утверждение 10. *В кольце R с единицей уравнения* (8) *разрешимы при любых $b \in R$ (и фиксированном $a \in R$) в том и только в том случае, когда $a \in R^*$. В последнем случае каждое из уравнений* (8) *имеет единственное решение.*

□ Если a обратим, то точно так же, как и в теореме 6, доказывается, что $x = a^{-1}b$, $y = ba^{-1}$ являются единственными решениями уравнений из (8). Обратно, пусть уравнения (8) разрешимы при любом b, и $x = a'$, $y = a''$ — их решения при $b = e$. Используя равенства $aa' = e$, $a''a = e$ и ассоциативность умножения, получим:

$$a'' = a''e = a''(aa') = (a''a)a' = ea' = a'.$$

Следовательно, $a' = a'' = a^{-1}$, т. е. a обратим. □

Определение 15. Пусть R — коммутативное кольцо и $a, b \in R$. Говорят, что элемент b *делится на* a, или a *делит* b, если существует такой элемент $c \in R$, что $b = ac$.

Тот факт, что a делит b, кратко записывают в виде $a \mid b$. Если $a \mid b$, то говорят также, что b *кратно* a, a *— делитель* b.

Заметим, что согласно определению 15 верно, что $0 \mid 0$.

Отношение делимости на коммутативном кольце обладает рядом свойств, сходных с известными из средней школы свойствами делимости целых чисел.

Утверждение 11. *Для любых элементов a, b, c коммутативного кольца R справедливы импликации*:

(а) $a \mid b,\ \ b \mid c \ \Rightarrow\ a \mid c$;

(б) $a \mid b,\ \ a \mid c \ \Rightarrow\ a \mid (b \pm c)$;

(в) $a \mid b \ \Rightarrow\ a \mid bc$.

Если R — коммутативное кольцо с единицей e, то оно обладает также свойствами:

(г) $\forall\, a \in R,\ \forall\, r \in R^* :\ (r \mid a,\ \ ar \mid a)$;

(д) $\forall\, a, b \in R,\ \forall\, r_1, r_2 \in R^* :\ (a \mid b \ \Leftrightarrow\ ar_1 \mid br_2)$.

□ Импликации (а), (б), (в) доказываются непосредственно на основании определения 15. Проделайте это в качестве упражнения. Свойство (г) следует из очевидных равенств $a = r(r^{-1}a),\ \ a = (ar)r^{-1}$. Докажем (д). Пусть $a, b \in R$, $r_1, r_2 \in R^*$. Если $a \mid b$, то $b = ac$ при некотором $c \in R$. Отсюда имеем равенство $br_2 = (ar_1)r_1^{-1}cr_2$, которое означает, что $ar_1 \mid br_2$. Обратная импликация доказывается аналогично. □

Заметим, что указанные в пункте (г) делители r и ar элемента a называются *несобственными*, или *тривиальными*.

Кроме обратимых элементов особую роль в кольцах играют элементы, называемые делителями нуля. В связи с термином «делитель нуля» необходимо сделать следующее замечание. В соответствии с определением 15 нуль делит нуль и потому нулевой элемент кольца следовало бы относить к делителям нуля. Однако в ряде случаев этого удобнее не делать. Поэтому здесь (как во многих других книгах по алгебре) термин «делитель нуля» будет использоваться только в смысле следующего определения.

Определение 16. *Делителем нуля* в произвольном кольце R называется любой его элемент $a \neq 0$, для которого в R существует элемент $b \neq 0$, удовлетворяющий условию: $ab = 0$ или $ba = 0$.

Для приведенных выше примеров колец имеем: в кольцах $\mathbb{Z}$, $2\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ делителей нуля нет; в кольце с нулевым умножением делителями нуля являются все ненулевые элементы; в кольце $(\mathbb{R}^2; +, \cdot)$ из примера 7 делителями нуля являются все пары (a, b), в которых $a = 0$, $b \neq 0$ или $a \neq 0$, $b = 0$.

Замечание 3. Если в коммутативном кольце R a делит b, то элемент c из условия $b = ac$ находится в общем случае неоднозначно. Однако, если $a \neq 0$ и a не является делителем нуля, то c находится однозначно, поскольку из равенства $ac_1 = ac_2$ следует $a(c_1 - c_2) = 0$, а потому и $c_1 - c_2 = 0$, т. е. $c_1 = c_2$. В этом случае однозначно определенный элемент c называют *частным от деления b на a* и обозначают в виде $\dfrac{b}{a}$.

Определение 17. Коммутативное кольцо с единицей и без делителей нуля называют *областью целостности*.

Примерами областей целостности являются кольца $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.

Из всех областей целостности особо выделяют поля.

Определение 18. *Полем* называют коммутативное кольцо с единицей, отличной от нуля, в котором каждый ненулевой элемент обратим.

Примерами полей являются кольца $\mathbb{Q}$ и $\mathbb{R}$. Их называют соответственно полем рациональных и полем действительных чисел. В качестве примера нечислового поля построим поле из двух элементов 0, e с операциями сложения и умножения, заданными следующими таблицами Кэли:

$+$	0	e
0	0	e
e	e	0

$\cdot$	0	e
0	0	0
e	0	e

Читателю предлагается проверить, что множество $\{0, e\}$ с указанными операциями является полем с нулем 0 и единицей e. Это поле называют *полем Галуа из двух элементов* и обозначают через $GF(2)$. В дальнейшем мы познакомимся со многими другими полями.

Так как поля являются кольцами, то они обладают всеми общими свойствами колец. Вместе с тем, поля обладают и некоторыми специфичными свойствами.

Утверждение 12. (а) *Если a, b — элементы поля P и $a \neq 0$, то уравнение $ax = b$ имеет единственное решение в P.*

(б) *В любом поле P отсутствуют делители нуля, т. е.*

$$\forall\, a, b \in P:\ (ab = 0 \ \Leftrightarrow\ a = 0 \text{ или } b = 0).$$

□ Свойство (а) следует непосредственно из утверждения 10, если учесть, что в поле все ненулевые элементы обратимы.

(б) Если $ab = 0$ и $a \neq 0$, то, умножив обе части равенства $ab = 0$ на a^{-1}, получим $a^{-1}(ab) = 0$, то есть $b = 0$. В другую сторону утверждение (б) следует из теоремы 8(а) для колец. □

Определение 19. Подмножество R_1 кольца $(R; +, \cdot)$ замкнутое относительно операций $+$, $\cdot$ в R и являющееся кольцом (полем) относительно этих операций, называют *подкольцом* (*подполем*) кольца R.

Из определения 19 следует, что кольцо $\mathbb{Z}$ является подкольцом кольца $\mathbb{Q}$, которое само является подкольцом и подполем поля $\mathbb{R}$.

§ 4. ИЗОМОРФИЗМ МНОЖЕСТВ С ОПЕРАЦИЯМИ

При изучении множества с операциями в алгебре обращают внимание лишь на те его свойства, которые обусловлены определенными на нем операциями, и не интересуются свойствами, обусловленными природой его элементов. Множества, устроенные одинаково с точки зрения определенных на них операций, называются изоморфными (т. е. имеющими одинаковое строение). Прежде чем дать этому понятию строгое определение, приведем простейший пример.

Рассмотрим группоид $G_1 = \{1, -1\}$ с обычной операцией умножения чисел. Его таблица Кэли имеет вид:

$\cdot$	1	-1
1	1	-1
-1	-1	1

Сравним группоид G_1 с другим группоидом G_2, состоящим из двух отображений множества $\mathbb{Z}$ в себя: тождественного отображения ε и отображения δ, определенного условием $\forall\, a \in \mathbb{Z}:\ \delta(a) = -a$. Легко видеть, что множество $G_2 = \{\varepsilon, \delta\}$ замкнуто относительно операции композиции отображений, и мы имеем группоид $(G_2; \circ)$ с таблицей Кэли

$\circ$	ε	δ
ε	ε	δ
δ	δ	ε

Сравнивая группоиды $(G_1; \cdot)$ и $(G_2; \circ)$, замечаем, что, заменив в таблице Кэли для G_1, элементы $1, -1$ соответственно на ε, δ, а операцию $\cdot$ на $\circ$, мы получим таблицу Кэли для группоида $(G_2; \circ)$. Таким образом, с точки зрения операций группоиды G_1

и G_2 отличаются лишь обозначением элементов и операций. Теперь заметим, что замена элементов 1, -1 на ε, δ есть биективное отображение φ множества G_1 на G_2, удовлетворяющее условию

$$\forall\, a, b, c \in G_1 :\ \ (ab = c \ \Leftrightarrow\ \varphi(a) \circ \varphi(b) = \varphi(c)).$$

Нетрудно видеть, что так записанное условие равносильно условию

$$\forall\, a, b \in G_1 :\ \ (\varphi(ab) = \varphi(a) \circ \varphi(b)).$$

Теперь должно быть понятным и естественным

Определение 20. Группоиды $(G; *)$ и $(H; \circ)$ называют *изоморфными*, если существует биективное отображение $\varphi\colon G \to H$ такое, что для любых элементов $a, b \in G$ выполняется равенство

$$\varphi(a * b) = \varphi(a) \circ \varphi(b). \tag{9}$$

При этом отображение φ называют *изоморфизмом* группоида $(G; *)$ на группоид $(H; \circ)$. Тот факт, что группоиды G и H изоморфны, записывается в виде $G \cong H$.

Легко видеть, что если φ — изоморфизм группоида $(G; *)$ на $(H; \circ)$, то отображение φ^{-1} является изоморфизмом группоида $(H; \circ)$ на $(G; *)$. Докажите это в качестве упражнения.

Понятие изоморфизма группоидов встречается и используется даже в школьной математике (без употребления слова изоморфизм). Так, отображение φ множества положительных чисел $\mathbb{R}^+$ во множество всех действительных чисел $\mathbb{R}$, определенное равенством $\varphi(a) = \lg a$, является изоморфизмом группоида $(\mathbb{R}^+; \cdot)$ на группоид $(\mathbb{R}; +)$. Условие (9) в данном случае записывается равенством

$$\lg(ab) = \lg a + \lg b.$$

Если в группоидах G, H операция обозначается одним и тем же символом, например $*$, то равенство (9) принимает вид

$$\varphi(a * b) = \varphi(a) * \varphi(b).$$

В этом случае говорят, что отображение φ является изоморфизмом относительно операции $*$.

В алгебре, изучающей множества лишь с точки зрения свойств операций, изоморфные группоиды попросту не различают, то есть изучают группоиды (да и другие множества с операциями) лишь с точностью до изоморфизма. Это объясняется тем, что операции в изоморфных группоидах обладают одними и теми же свойствами. Частично это утверждается в следующей теореме.

Теорема 13. *Пусть φ — изоморфизм группоида $(G; *)$ на группоид $(H; \circ)$. Тогда*

(а) *если группоид $(G; *)$ коммутативный или ассоциативный, то соответственно таким же является и $(H; \circ)$;*

(б) *если Λ — нейтральный элемент в $(G; *)$, то $\varphi(\Lambda)$ — нейтральный в $(H; \circ)$;*

(в) *если в $(G; *)$ элемент g' является симметричным для g, то в $(H; \circ)$ элемент $\varphi(g')$ — симметричный для $\varphi(g)$.*

□ (а) Пусть операция $*$ коммутативна и h_1, h_2 — любые элементы из H. Так как отображение φ сюръективно, то

$$\exists\, g_1, g_2 \in G:\ \varphi(g_1) = h_1,\ \varphi(g_2) = h_2.$$

Теперь, используя коммутативность операции $*$ и условие (9), получим:

$$h_1 \circ h_2 = \varphi(g_1) \circ \varphi(g_2) = \varphi(g_1 * g_2) = \varphi(g_2 * g_1) = \varphi(g_2) \circ \varphi(g_1) = h_2 \circ h_1.$$

Следовательно, операция $\circ$ также коммутативна. Аналогично доказывается утверждение (а) и для свойства ассоциативности.

(б) Пусть, как и в (а), $h_1 \in H$, $\varphi(g_1) = h_1$. Тогда

$$\varphi(\Lambda) \circ h_1 = \varphi(\Lambda) \circ \varphi(g_1) = \varphi(\Lambda * g_1) = \varphi(g_1) = h_1,$$

и аналогично $h_1 \circ \varphi(\Lambda) = h_1$. Следовательно, $\varphi(\Lambda)$ — нейтральный элемент в $(H;\circ)$.

(в) Из равенств $g * g' = g' * g = \Lambda$, учитывая, что φ — изоморфизм, получим:

$$\varphi(g) \circ \varphi(g') = \varphi(g') \circ \varphi(g) = \varphi(\Lambda). \tag{10}$$

Так как $\varphi(\Lambda)$ — нейтральный элемент в $(H;\circ)$ по доказанному в (б), то равенства (10) и означают, что $\varphi(g')$ — симметричный элемент для $\varphi(g)$. □

Следствие. *Если группоиды $(G;*)$, $(H;\circ)$ изоморфны и $(G;*)$ есть или полугруппа, или коммутативная полугруппа, или группа, то соответственно таким же является группоид $(H;\circ)$.*

В заключение данного параграфа докажем два утверждения о группах подстановок.

Утверждение 14. *Для любого множества $M \neq \varnothing$ группы $(S(M);\cdot)$ и $(S(M);\circ)$ изоморфны.*

□ Определим отображение $\varphi\colon S(M) \to S(M)$ следующим образом:

$$\forall\, g \in S(M):\ \varphi(g) = g^{-1},$$

где g^{-1} — обратный элемент для g в группе $(S(M);\cdot)$. Покажем, что φ — изоморфизм. Так как каждый элемент из $S(M)$ является обратным для обратного к нему, то φ сюръективно. Инъективность φ докажем от противного. Допустим, что $g_1^{-1} = g_2^{-1}$ для $g_1 \neq g_2$. Умножив обе части последнего равенства на g_1 слева и на g_2 справа, получим противоречащее условию равенство $g_2 = g_1$.

Итак, φ биективно, и осталось проверить условие (9). Оно проверяется с использованием известного равенства $(g_1 g_2)^{-1} = g_2^{-1} g_1^{-1}$:

$$\varphi(g_1 g_2) = (g_1 g_2)^{-1} = g_2^{-1} g_1^{-1} = \varphi(g_2)\,\varphi(g_1) = \varphi(g_1) \circ \varphi(g_2). \quad \square$$

Утверждение 15. *Если множества M, M' не пусты и равномощны, то*

$$(S(M);\,\cdot\,) \cong (S(M');\,\cdot\,).$$

□ По определению равномощности множеств существует биективное отображение $a\colon M \to M'$. Сопоставим каждой подстановке $g \in S(M)$ отображение $\varphi(g) = a^{-1}ga\colon M' \to M'$. Так как отображения a^{-1}, g, a биективны, то по утверждению 2 главы 1 биективным будет и их произведение. Следовательно, $\varphi(g) \in S(M')$. В итоге определено отображение $\varphi\colon S(M) \to S(M')$. Отображение φ сюръективно, поскольку в подстановку g' из $S(M')$ отобразится подстановка $ag'a^{-1}$ из $S(M)$. Действительно, по определению φ имеем:

$$\varphi(ag'a^{-1}) = a^{-1}(ag'a^{-1})a = (a^{-1}a)g'(a^{-1}a) = \varepsilon_M \cdot g' \cdot \varepsilon_{M'} = g'.$$

Отображение φ инъективно, так как из равенства образов $\varphi(g_1) = \varphi(g_2)$, т. е. $a^{-1}g_1a = a^{-1}g_2a$, следует, что $g_1 = g_2$. Таким образом, φ биективно, и остается проверить для φ условие (9):

$$\varphi(g_1g_2) = a^{-1}(g_1g_2)a = (a^{-1}g_1a)(a^{-1}g_2a) = \varphi(g_1)\,\varphi(g_2). \quad \square$$

Утверждения 14, 15 хорошо иллюстрируют значение понятия изоморфизма. Оказывается, для изучения групп $(S(M);\cdot)$, $(S(M);\circ)$ при всевозможных M достаточно из каждого бесконечного семейства равномощных множеств выбрать какое-либо одно и изучать лишь симметрическую группу подстановок этого множества (т. е. множество подстановок с операцией умножения). В конечных случаях в качестве таких множеств обычно выбираются множества $\overline{1,n}$, $n \in \mathbb{N}$. Группа подстановок множества $\overline{1,n}$ называется *симметрической группой подстановок степени* n и обозначается через S_n. Подстановки из S_n записывают обычно в виде

$$g = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix},$$

где i_s — образ элемента s при действии подстановки g.

Понятие изоморфизма группоидов естественным образом обобщается на алгебры со многими операциями. Здесь мы ограничимся лишь частным случаем, когда алгебры являются множествами с двумя бинарными операциями.

Определение 21. Алгебры $(R_1;+,\cdot)$, $(R_2;+,\cdot)$ с бинарными операциями сложения и умножения называют *изоморфными*, если существует такое биективное отображение $\varphi\colon R_1 \to R_2$, при котором для любых элементов $a, b \in R_1$ выполняются равенства

$$\varphi(a+b) = \varphi(a) + \varphi(b), \quad \varphi(ab) = \varphi(a)\,\varphi(b).$$

При этом отображение φ называют *изоморфизмом алгебры* $(R_1;+,\cdot)$ *на* $(R_2;+,\cdot)$.

Изоморфизм алгебр $(R_1;+,\cdot)$ и $(R_2;+,\cdot)$ обозначается тем же знаком $\cong$, что и изоморфизм группоидов.

В дальнейшем нам окажется полезной

Теорема 16. *Если алгебры* $(R_1;+,\cdot)$ *и* $(R_2;+,\cdot)$ *изоморфны и* $(R_1;+,\cdot)$ *— кольцо* (*поле*), *то* $(R_2;+,\cdot)$ *также является кольцом* (*полем*).

□ Выполнение всех аксиом кольца (поля), кроме дистрибутивности, для R_2 следует непосредственно из теоремы 13. Проверим условия дистрибутивности. Пусть φ — изоморфизм R_1 на R_2, и a, b, c — любые элементы из R_2. Так как φ сюръективно, то

$$\exists\, a_1, b_1, c_1 \in R_1 :\ \varphi(a_1) = a,\ \varphi(b_1) = b,\ \varphi(c_1) = c.$$

Применяя к обеим частям равенства $(a_1 + b_1)c_1 = a_1c_1 + b_1c_1$ отображение φ и учитывая, что φ — изоморфизм, получим соответственно:

$$\varphi((a_1 + b_1)c_1) = \varphi(a_1 + b_1)\,\varphi(c_1) = (\varphi(a_1) + \varphi(b_1))\,\varphi(c_1) = (a + b)c,$$

$$\varphi(a_1c_1 + b_1c_1) = \varphi(a_1c_1) + \varphi(b_1c_1) = \varphi(a_1)\,\varphi(c_1) + \varphi(b_1)\,\varphi(c_1) = ac + bc.$$

Следовательно, в R_2 операция $\cdot$ праводистрибутивна относительно $+$. Аналогично проверяется и свойство левой дистрибутивности. □

ЗАДАЧИ

1. Сколько различных бинарных операций можно определить на n-элементном множестве? В скольких случаях получатся группоиды:

а) коммутативные,

б) с нейтральным элементом,

в) с условием разрешимости любого уравнения вида $ax = b$,

г) с условием разрешимости любого уравнения вида $xa = b$?

2. Приведите пример множества с двумя бинарными операциями $*$ и $\circ$, из которых одна является леводистрибутивной, но не праводистрибутивной относительно другой.

3. Определите на множестве $\mathbb{R}^2$ операции

$$(a, b) + (c, d) = (a + c,\, b + d), \quad (a, b)(c, d) = (a, d).$$

Являются ли эти операции коммутативными, ассоциативными, лево(право)дистрибутивными одна относительно другой?

4. Найдите нейтральный элемент и опишите все обратимые элементы в полугруппе $B(M)$ всех бинарных отношений на конечном множестве M.

5. Докажите, что если g — подстановка конечного множества M и $a \in M$, то в последовательности a, $g(a)$, $g^2(a)$, ... первым из повторившихся элементов будет a.

6. Являются ли группами:

а) множество всех подстановок множества $M \neq \varnothing$, оставляющих на месте фиксированный элемент $a \in M$;

б) множество отношений эквивалентности на множестве $M \neq \varnothing$ относительно операции умножения;

в) множество всех подмножеств множества $M \neq \varnothing$ относительно операции $*$, где $A * B = (A \cup B) \setminus (A \cap B)$;

г) множество действительных чисел промежутка $[0, 1)$ с операцией $*$, где $a * b$ — дробная часть числа $a + b$?

7. Докажите, что если в группе $(G;\cdot)$ любой элемент a удовлетворяет условию $a^2 = e$, то G абелева.

8. Докажите, что все группы порядка 3 изоморфны между собой и существуют ровно две не изоморфные группы порядка 4.

9. Изоморфны ли группоиды:
а) $(\mathbb{N}_0;+)$ и $(\mathbb{N}_0;\cdot)$;
б) $(\mathbb{Z};+)$ и $(2\mathbb{Z};+)$;
в) $(\mathbb{Z};\cdot)$ и $(2\mathbb{Z};\cdot)$?

10. Являются ли кольцами (полями) относительно операций сложения и умножения чисел множества:
а) $\{a+b\sqrt{2}:\ a,b\in\mathbb{Z}\}$;
б) $\{a+b\sqrt{2}:\ a,b\in\mathbb{Q}\}$;
в) $\{a+b\sqrt[3]{2}:\ a,b\in\mathbb{Q}\}$?

11. Является ли кольцом (полем) множество $\mathbb{R}^2$ с операциями

$$(a,b)+(c,d)=(a+c,\ b+d);\quad (a,b)(c,d)=(ad+bc,\ bd)?$$

12. Докажите, что в любом кольце с единицей множества обратимых элементов и делителей нуля не пересекаются.

13. Докажите, что отношение изоморфизма является отношением эквивалентности на любом множестве группоидов.

14. Изоморфизм группоида G на себя называют *автоморфизмом группоида*. Докажите, что множество $\mathrm{Aut}(G)$ всех автоморфизмов группоида G является группой относительно операции умножения (композиции) отображений.

Глава 4

ЧИСЛОВЫЕ КОЛЬЦА И ПОЛЯ

§ 1. ОТНОШЕНИЕ ДЕЛИМОСТИ В КОЛЬЦЕ $\mathbb{Z}$. ДЕЛЕНИЕ ЦЕЛЫХ ЧИСЕЛ С ОСТАТКОМ

Кольцо целых чисел $\mathbb{Z}$ является одним из основных числовых колец. Методы решения многих задач в кольце $\mathbb{Z}$ нередко служат основой для аналогий при изучении других колец. Так, например, изложенный в данной главе материал по теории делимости в $\mathbb{Z}$ послужит в главе 9 основой для изучения сходных вопросов в кольцах многочленов.

Кольцо $\mathbb{Z}$ является коммутативным кольцом с единицей, и потому в нем отношение делимости обладает свойствами (а)–(д) из утверждения 11 главы 3. В дополнение к ним докажем

Утверждение 1. *Для любых* $a, b \in \mathbb{Z}$

(а) $a \mid b \;\Leftrightarrow\; \pm a \mid \pm b$;

(б) $a \mid b,\;\; b \neq 0 \;\Rightarrow\; |a| \leqslant |b|$;

(в) $a \mid b,\;\; b \mid a \;\Leftrightarrow\; |a| = |b|$.

□ (а) Свойство (а) является уточнением свойства (д) из утверждения 11 главы 3, поскольку обратимые элементы кольца $\mathbb{Z}$ исчерпываются числами 1, -1.

(б) Из условия $a \mid b$ следует, что $b = aq$ при некотором $q \in \mathbb{Z}$. Отсюда по свойству модулей чисел имеем: $|b| = |a| \cdot |q|$. Так как $b \neq 0$, то $|q| > 0$, т. е. $|q| = 1 + t$, где $t \in \mathbb{N}_0$. Следовательно, $|b| = |a|(1 + t) = |a| + k$, где $k = |a| \cdot t \geqslant 0$, и потому $|b| \geqslant |a|$.

(в) Пусть $a \mid b$ и $b \mid a$. Тогда числа a, b или оба равны нулю, или оба не равны нулю. В первом случае равенство $|a| = |b|$ очевидно, во втором оно следует из свойства (б). Обратная импликация следует из утверждения (а), если учесть, что $|a| = |b| \Rightarrow b = \pm a$. □

Заметим, что множество делителей любого целого числа a не пусто. Действительно, если $a = 0$, то его делителями являются все целые числа (включая и 0). Если же $a \neq 0$, то оно имеет, по крайней мере тривиальные делители ± 1, $\pm a$ (см. замечания к утверждению 11 главы 3).

Свойство (а) сводит описание всех делителей и всех кратных для данного числа к описанию лишь положительных (натуральных) делителей и кратных. Из свойства (б) следует конечность числа различных делителей у любого отличного от нуля целого числа, что дает принципиальную возможность нахождения всех делителей числа.

В том случае, когда одно натуральное число не делится на другое, алгоритм деления «уголком» приводит к неполному частному и остатку от деления. Оказывается, что понятие деления с остатком можно обобщить на любые целые числа.

Определение 1. *Разделить с остатком* целое число a на целое число b — это значит найти целые числа q и r, удовлетворяющие условиям

$$a = bq + r, \quad 0 \leqslant r < |b|. \tag{1}$$

Числа q и r, удовлетворяющие условиям (1), называют соответственно *неполным частным* и *остатком* от деления a на b.

Теорема 2. *Если $a, b \in \mathbb{Z}$ и $b \neq 0$, то a можно разделить на b с остатком, причем неполное частное и остаток определяются однозначно.*

□ Сначала докажем существование чисел q и r, удовлетворяющих условиям (1). Рассмотрим отдельно три случая.

1. $a \geqslant 0$, $b > 0$. По аксиоме Архимеда существует такое натуральное число k, что $a < bk$. Отсюда (согласно принципу наименьшего числа) следует существование такого целого неотрицательного числа q, что

$$bq \leqslant a < b(q+1), \quad \text{т. е.} \quad 0 \leqslant a - bq < b.$$

Следовательно, числа q и $r = a - bq$ удовлетворяют условиям (1).

2. $a < 0$, $b > 0$. Тогда $-a > 0$, и по доказанному в пункте 1 существуют такие числа q_1, r_1, что

$$-a = bq_1 + r_1, \quad 0 \leqslant r_1 < b.$$

Если $r_1 = 0$, то $a = b(-q_1)$, и условия (1) выполняются при $q = -q_1$, $r = 0$. Если же $r_1 \neq 0$, то

$$a = b(-q_1) - r_1 = b(-q_1 - 1) + (b - r_1) = bq + r,$$

где $q = -q_1 - 1$, $r = b - r_1$. Так как $0 < r_1 < b$, то $0 < r < b$, и для чисел q, r условия (1) выполнены.

3. a любое, $b < 0$. Тогда по доказанному в пунктах 1 и 2 найдутся такие числа q_1, r_1, что

$$a = (-b)q_1 + r_1, \quad 0 \leqslant r_1 < -b = |b|.$$

Отсюда имеем

$$a = b(-q_1) + r_1, \quad 0 \leqslant r_1 < |b|.$$

Таким образом, существование неполного частного и остатка доказано во всех случаях.

Докажем единственность. Пусть для целых чисел a, b, q, r, q_1, r_1 выполняются соотношения (1) и соотношения

$$a = bq_1 + r_1, \quad 0 \leqslant r_1 < |b|.$$

Тогда имеем $bq + r = bq_1 + r_1$, и потому

$$|b| \cdot |q - q_1| = |r_1 - r|.$$

Так как r, r_1 — неотрицательные числа, меньшие $|b|$, то $|r_1 - r| < |b|$. Однако, при $q \neq q_1$ из последнего равенства и утверждения 1(б) следует, что $|r_1 - r| \geqslant |b|$. Значит, $q = q_1$, а тогда и $r = r_1$. □

Ниже остаток от деления a на b будем обозначать через $r_b(a)$.

Сравнивая определение 15 главы 3 отношения делимости и определение 1 деления с остатком и учитывая единственность неполного частного и остатка, получим

Следствие. *Если* $a, b \in \mathbb{Z}$ *и* $b \neq 0$, *то* $b \mid a \Leftrightarrow r_b(a) = 0$.

§ 2. НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ И НАИМЕНЬШЕЕ ОБЩЕЕ КРАТНОЕ ЦЕЛЫХ ЧИСЕЛ

Определение 2. *Наибольшим общим делителем* (НОД) целых чисел $a_1, \ldots, a_n$ при $n \geqslant 2$ называют любое целое число d, удовлетворяющее условиям:

1) d есть общий делитель чисел $a_1, \ldots, a_n$, т. е.

$$d \mid a_1, \ \ldots, \ d \mid a_n;$$

2) d делится на любой общий делитель чисел $a_1, \ldots, a_n$, т. е.

$$\forall\, d_1 \in \mathbb{Z}\colon \ (d_1 \mid a_1, \ \ldots, \ d_1 \mid a_n \ \Rightarrow \ d_1 \mid d).$$

Множество всех наибольших общих делителей чисел $a_1, \ldots, a_n$, обозначим через НОД $\{a_1, \ldots, a_n\}$. Ниже мы докажем, что это множество не пусто при любых $a_1, \ldots, a_n \in \mathbb{Z}$. Пока же установим лишь более слабое

Утверждение 3. *Если* $n \geqslant 2$ *и* $a_1 = \ldots = a_n = 0$, *то для чисел* $a_1, \ldots, a_n$ *существует единственный НОД, равный* 0. *Если целые числа* $a_1, \ldots, a_n$ *не все равны* 0 *и для них существует хотя бы один НОД, то они имеют ровно два НОД, которые отличаются только знаком.*

□ При $a_1 = \ldots = a_n = 0$ число $d = 0$ удовлетворяет условиям определения 2, а число $d \neq 0$ удовлетворяет условию 1 и не удовлетворяет условию 2 определения, поскольку, например, $d + 1 \mid 0$, но $d + 1 \nmid d$. Следовательно, НОД $\{0, \ldots, 0\} = \{0\}$. Пусть теперь целые числа $a_1, \ldots, a_n$ не все равны 0, и $d \in$ НОД $\{a_1, \ldots, a_n\}$, т. е. d удовлетворяет условиям определения 2. Тогда $d \neq 0$, и из утверждения 1(а) следует, что этим условиям удовлетворяет также число $-d$.

Если целое число d_1 также является НОД чисел $a_1, \ldots, a_n$, то по условию 2 определения 2 выполнены соотношения $d_1 \mid d$ и $d \mid d_1$, а тогда по утверждению 1(в) имеем $|d_1| = |d|$, т. е. $d_1 = d$ или $d_1 = -d$. Таким образом, в рассматриваемом случае НОД $\{a_1, \ldots, a_n\} = \{-d, d\}$. □

Из утверждения 3 следует, что если множество НОД $\{a_1, \ldots, a_n\}$ не пусто, то в нем содержится единственное неотрицательное число. Условимся обозначать его через $(a_1, \ldots, a_n)$.

Для решения вопроса о существовании НОД чисел $a_1, \ldots, a_n$ ограничимся сначала рассмотрением случая $n = 2$. В этом случае для нахождения НОД существует известный алгоритм, описанный на геометрическом языке Евклидом[2].

Пусть даны два целых числа a, b. Если $b = 0$, то, очевидно, в множестве НОД $\{a, b\}$ содержится число a. Поэтому будем считать, что $b \neq 0$.

Алгоритм Евклида для целых чисел a, b при условии $b \neq 0$ заключается в следующем. Сначала делим с остатком a на b:

$$a = bq_1 + r_1, \quad 0 \leqslant r_1 < |b|.$$

Если $r_1 = 0$, то алгоритм окончен. В этом случае $b \mid a$, и, очевидно, $b \in$ НОД $\{a, b\}$. Если же $r_1 \neq 0$, то делим с остатком b на r_1:

$$b = r_1 q_2 + r_2, \quad 0 \leqslant r_2 < r_1.$$

Если $r_2 = 0$, то алгоритм окончен, в противном случае делим с остатком r_1 на r_2 и т. д. до тех пор, пока не получим остаток, равный нулю. Такой момент обязательно наступит, поскольку получающиеся остатки являются целыми неотрицательными числами и образуют строго убывающую цепочку чисел $r_1 > r_2 > \ldots$. Если остатки $r_1, \ldots, r_n$ отличны от нуля, а $r_{n+1} = 0$, то имеем следующую систему соотношений:

$$\begin{aligned}
&a = bq_1 + r_1, && 0 < r_1 < |b|,\\
&b = r_1 q_2 + r_2, && 0 < r_2 < r_1,\\
&r_1 = r_2 q_3 + r_3, && 0 < r_3 < r_2,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&r_{n-2} = r_{n-1} q_n + r_n, && 0 < r_n < r_{n-1},\\
&r_{n-1} = r_n q_{n+1}.
\end{aligned} \tag{2}$$

Прослеживая систему равенств из (2) снизу вверх, нетрудно заметить последовательно, что r_n делит числа r_{n-1}, r_{n-2}, $\ldots$, r_1, b, a. Следовательно, r_n есть общий делитель чисел a, b. Если d_1 — какой-либо другой их общий делитель, то, прослеживая систему равенств (2) сверху вниз, получим последовательно: d_1 делит $r_1, r_2, \ldots, r_n$. Следовательно, $r_n = (a, b)$. Отсюда, с учетом утверждения 3, можно сделать вывод о том, что справедлива

Теорема 4. *Для любых целых чисел a, b существует единственный неотрицательный наибольший общий делитель (a, b). При этом, если $a \mid b$ или $b \mid a$, то соответственно $(a, b) = a$ или $(a, b) = b$, в противном случае (a, b) совпадает с последним не равным нулю остатком в алгоритме Евклида для чисел a, b.*

Теорема 5. *Для любого натурального числа $n \geqslant 2$ и любых целых чисел $a_1, \ldots, a_n$ существует НОД, причем единственный неотрицательный НОД чисел $a_1, \ldots, a_n$ находится по формуле*

$$(a_1, \ldots, a_n) = ((\ldots((a_1, a_2), a_3), \ldots, a_{n-1}), a_n).$$

[2] Евклид (III век до н. э.) — древнегреческий математик, впервые осуществивший систематизацию и аксиоматическое изложение накопившихся геометрических знаний.

□ Докажем это утверждение индукцией по n. При $n = 2$ оно следует из теоремы 4. Допустим, что оно верно для $n = k \geqslant 2$ и докажем его для $n = k + 1$. По теореме 4

$$d_1 = ((\dots((a_1, a_2), a_3), \dots), a_k), \quad d_2 = ((\dots((a_1, a_2), a_3), \dots), a_{k+1})$$

являются вполне определенными числами из $\mathbb{N}_0$, и для доказательства теоремы достаточно показать, что $d_2 \in \text{НОД}\{a_1, \dots, a_k, a_{k+1}\}$. Из определения чисел d_1, d_2 и из предположения индукции получаем равенства:

$$d_2 = (d_1, a_{k+1}), \quad d_1 = (a_1, a_2, \dots, a_k). \tag{3}$$

Пользуясь равенствами (3), нетрудно проверить, что d_2 удовлетворяет обоим условиям определения НОД чисел $a_1, \dots, a_k, a_{k+1}$. Проверьте это самостоятельно. □

Используя алгоритм Евклида, нетрудно представить любой НОД чисел $a_1, \dots, a_m$ в виде целочисленной линейной комбинации этих чисел. Сделаем это сначала для $m = 2$.

Теорема 6. *Если $r_1, \dots, r_n$, $q_1, \dots, q_n$ — последовательности остатков и неполных частных в алгоритме Евклида для чисел a, b, то выполняются равенства*:

$$r_k = au_k + bv_k, \quad k \in \overline{1, n}, \tag{4}$$

где u_k, v_k — целые числа, определяемые рекуррентными соотношениями

$$u_k = u_{k-2} - u_{k-1}q_k, \quad v_k = v_{k-2} - v_{k-1}q_k \tag{5}$$

и начальными условиями

$$u_0 = 0,\ u_1 = 1,\ v_0 = 1,\ v_1 = -q_1. \tag{6}$$

□ Сначала заметим, что числа $u_1, \dots, u_n$, $v_1, \dots, v_n$ однозначно определяются условиями (5), (6). Теперь индукцией по k докажем, что они удовлетворяют соотношениям (4). При $k = 1$ равенство (4) имеет вид $r_1 = a - bq_1$ и легко получается из 1-й строки системы (2). Допустим, что соотношение (4) выполняется для $k \in \overline{1, m}$, где $1 \leqslant m < n$, и докажем его для $k = m + 1$. Из $(m + 1)$-го равенства системы соотношений (2), используя предположение индукции, получим при $m + 1 > 2$:

$$\begin{aligned} r_{m+1} &= r_{m-1} - r_m q_{m+1} = (au_{m-1} + bv_{m-1}) - (au_m + bv_m)q_{m+1} = \\ &= a(u_{m-1} - u_m q_{m+1}) + b(v_{m-1} - v_m q_{m+1}) = au_{m+1} + bv_{m+1}; \end{aligned}$$

при $m + 1 = 2$:

$$\begin{aligned} r_2 &= b - r_1 q_2 = b - (au_1 + bv_1)q_2 = a(-u_1 q_2) + b(1 - v_1 q_2) = \\ &= a(u_0 - u_1 q_2) + b(v_0 - v_1 q_2) = au_2 + bv_2. \quad \square \end{aligned}$$

Следствие. *Если $a, b \in \mathbb{Z}$ и $d = (a, b)$, то существуют такие целые числа u, v, что выполняется равенство*

$$au + bv = d. \tag{7}$$

□ Если $d = a$ или $d = b$, то утверждение очевидно. Если $d \neq a$, $d \neq b$, то по теореме 4 $d = r_n$, и искомыми целыми числами u, v могут служить числа u_n, v_n из равенства (4) при $k = n$. □

Процесс вычисления чисел u_k, v_k из (4) и, в частности, чисел u, v из (7) удобно проводить с помощью следующей таблицы.

k	0	1	2	...	m	...	n
q_k		q_1	q_2	...	q_m	...	q_n
u_k	0	1	$u_2 = u_0 - u_1 q_2$	...	$u_m = u_{m-2} - u_{m-1} q_m$	...	$u = u_n$
v_k	1	$-q_1$	$v_2 = v_0 - v_1 q_2$	...	$v_m = v_{m-2} - v_{m-1} q_m$	...	$v = v_n$

Используя теорему 5 и следствие теоремы 6, нетрудно индукцией по n доказать

Утверждение 7. *Пусть $a_1, \ldots, a_n \in \mathbb{Z}$, $n \geqslant 2$. Если $(a_1, \ldots, a_n) = d$, то существуют такие целые числа $u_1, \ldots, u_n$, что*

$$a_1 u_1 + \ldots + a_n u_n = d.$$

Заметим, что обратное утверждение в общем случае неверно. Приведите соответствующий пример.

Определение 3. Целые числа $a_1, \ldots, a_n$ называются *взаимно простыми* (в совокупности), если $(a_1, \ldots, a_n) = 1$.

Утверждение 8. *Целые числа $a_1, \ldots, a_n$ взаимно просты тогда и только тогда, когда существуют $u_1, \ldots, u_n \in \mathbb{Z}$ такие, что*

$$a_1 u_1 + \ldots + a_n u_n = 1. \tag{8}$$

□ Если $(a_1, \ldots, a_n) = 1$, то нужные числа $u_1, \ldots, u_n$ существуют по утверждению 7. Обратно, если при некоторых $u_1, \ldots, u_n$ выполняется равенство (8) и $d \mid a_1, \ldots, d \mid a_n$, то $d \mid 1$. Следовательно, $(a_1, \ldots, a_n) = 1$. □

Приведем наиболее часто используемые свойства взаимно простых чисел.

Теорема 9. *Для любых целых чисел a, b, c, справедливы утверждения*:
(а) $(a, b) = 1, \ (a, c) = 1 \ \Rightarrow \ (a, bc) = 1$;
(б) $a \mid bc, \ (a, b) = 1 \ \Rightarrow \ a \mid c$;
(в) $a \mid c, \ b \mid c, \ (a, b) = 1 \ \Rightarrow \ ab \mid c$;
(г) $(a, b) = c, \ c \neq 0 \ \Rightarrow \ \left(\frac{a}{c}, \frac{b}{c}\right) = 1$.

□ (а) Из условия и утверждения 8 следует существование целых чисел u_1, v_1, u_2, v_2, удовлетворяющих равенствам

$$au_1 + bv_1 = 1, \quad au_2 + cv_2 = 1.$$

Перемножив эти равенства почленно, получим: $au + (bc)v = 1$, где

$$u = au_1u_2 + bv_1u_2 + cu_1v_2, \quad v = v_1v_2.$$

Отсюда по утверждению 8 имеем $(a, bc) = 1$.

(б) По условию при подходящих $q, u, v \in \mathbb{Z}$ выполняются равенства $bc = aq$, $au + bv = 1$. Умножив последнее равенство на c и заменив после этого bc на aq, получим $a(cu) + a(qv) = c$ и $a(cu + qv) = c$. Следовательно, $a \mid c$.

(в) Как и в случае (б), имеем равенства

$$c = aq_1, \quad c = bq_2, \quad au + bv = 1 \quad (q_1, q_2, u, v \in \mathbb{Z}).$$

Умножив последнее равенство на c и учитывая два предыдущих равенства, получим: $abq_2u + abq_1v = c$. Отсюда видно, что $ab \mid c$.

(г) Из условия и утверждения 7 следует, что $c \mid a$, $c \mid b$ и существуют целые числа u, v, удовлетворяющие равенству $au + bv = c$. Отсюда имеем

$$\frac{a}{c}\,u + \frac{b}{c}\,v = 1, \quad \text{т. е.} \quad \left(\frac{a}{c},\ \frac{b}{c}\right) = 1. \quad \square$$

Определение 4. *Наименьшим общим кратным* (НОК) целых чисел $a_1, \ldots, a_n$ при $n \geqslant 2$ называется любое целое число k, удовлетворяющее условиям:

1) k есть общее кратное чисел $a_1, \ldots, a_n$, т. е. $a_1 \mid k$, $\ldots$, $a_n \mid k$;

2) k делит любое общее кратное чисел a_1, $\ldots$, a_n, т. е.

$$\forall\, k_1 \in \mathbb{Z}\colon\ (a_1 \mid k_1,\ \ldots,\ a_n \mid k_1\ \Rightarrow\ k \mid k_1).$$

Множество всех наименьших общих кратных чисел $a_1, \ldots, a_n$ обозначим через $\mathrm{НОК}\,\{a_1, \ldots, a_n\}$.

Утверждение 10. *Если $n \geqslant 2$ и хотя бы одно из целых чисел $a_1, \ldots, a_n$ равно 0, то для них существует единственное НОК, равное 0. Если целые числа $a_1, \ldots, a_n$ отличны от 0 и для них существует хотя бы одно НОК, то они имеют ровно два НОК, которые отличаются только знаком.*

Доказательство аналогично доказательству утверждения 3. Проведите его в качестве упражнения.

Из утверждения 10 видно, что если НОК чисел $a_1, \ldots, a_n$ существует, то их неотрицательное НОК определено однозначно. Будем обозначать его через $[a_1, \ldots, a_n]$. Следующие два утверждения решают вопрос о существовании НОК любых целых чисел и дают метод его нахождения.

Утверждение 11. *Если хотя бы одно из целых чисел a, b отлично от 0, то для них НОК существуют, и единственное неотрицательное НОК находится по формуле*

$$[a, b] = \frac{|ab|}{(a, b)}.$$

□ Обозначим $(a,b)=d$ и покажем, что число $\frac{ab}{d}$ удовлетворяет условиям определения 4. Так как $\frac{ab}{d}=a\frac{b}{d}=b\frac{a}{d}$, то $a \mid \frac{ab}{d}$ и $b \mid \frac{ab}{d}$. Пусть $k\in\mathbb{Z}$, $a \mid k$ и $b \mid k$. Тогда, очевидно, $d \mid k$, $\frac{a}{d} \mid \frac{k}{d}$ и $\frac{b}{d} \mid \frac{k}{d}$.

Отсюда по утверждениям (в)–(г) теоремы 9 имеем $\frac{ab}{d} \mid k$. Следовательно, $\frac{ab}{d} \in \text{НОК}\{a,b\}$. Тогда по утверждению 10 $\frac{|ab|}{d} \in \text{НОК}\{a,b\}$. А так как $\frac{|ab|}{d} \geqslant 0$, то $[a,b]=\frac{|ab|}{d}$. □

Теорема 12. *Для любого $n\geqslant 2$ и любых целых чисел $a_1,\ldots,a_n$ существует единственное неотрицательное НОК, которое находится по формуле*

$$[a_1,a_2,\ldots,a_n]=[\ldots[[a_1,a_2],a_3],\ldots,a_n].$$

Доказательство теоремы 12 проведите самостоятельно по аналогии с доказательством теоремы 5.

§ 3. ПРОСТЫЕ ЧИСЛА. ОСНОВНАЯ ТЕОРЕМА АРИФМЕТИКИ

Определение 5. Натуральное число $p\neq 1$ называется *простым*, если оно не имеет натуральных делителей, отличных от 1 и p, в противном случае оно называется *составным*. Число 1 не относится ни к простым, ни к составным числам.

Укажем некоторые свойства простых чисел.

Утверждение 13. *Пусть p — любое простое число. Тогда*
(а) $\forall\, a\in\mathbb{Z}:\ (p \mid a$ *или* $(a,p)=1)$;
(б) $\forall\, a,b\in\mathbb{Z}:\ (p \mid ab \ \Rightarrow\ (p \mid a$ *или* $p \mid b))$;
(в) *если q — также простое число, то $q=p$ или $(q,p)=1$.*

□ (а) Пусть $p \nmid a$. Тогда так как $(a,p)=d\in\{1,p\}$ и $d \mid a$, то $d=1$.

(б) Пусть $p \mid ab$. Если $p \nmid a$, то по свойству (а) $(a,p)=1$, и тогда по теореме 9(б) $p \mid b$.

(в) Если q — простое число и $q\neq p$, то по определению 5 $p \nmid q$, а тогда по свойству (а) $(q,p)=1$. □

Заметим, что свойство (б) можно обобщить на $n\geqslant 2$ сомножителей. Докажите это индукцией по n.

Роль простых чисел в арифметике во многом определяется следующим утверждением, называемым *основной теоремой арифметики*.

Теорема 14. *Всякое натуральное число $n\neq 1$ либо является простым, либо разлагается в произведение простых чисел, причем такое разложение единственно с точностью до перестановки сомножителей.*

Этой теореме, учитывая коммутативность кольца $\mathbb{Z}$, можно придать следующую, более компактную, форму.

Любое натуральное число $n \neq 1$ однозначно представляется в виде

$$n = p_1 \dots p_s, \tag{9}$$

где $s \geqslant 1$, $p_1, \dots, p_s$ — простые числа и $p_1 \leqslant \dots \leqslant p_s$.

□ Существование искомого разложения для числа n было доказано в § 3 главы 1 в порядке иллюстрации метода полной математической индукции. Единственность разложения (9) докажем индукцией по параметру $s(n)$, где $s(n)$ — наименьшее значение s по всем разложениям вида (9) для числа n. При $s(n) = 1$ это очевидно. Допустим, что это верно для всех n при $s(n) < s$ и любом фиксированном $s > 1$, и докажем для n при $s(n) = s$. Пусть наряду с (9) существует представление

$$n = q_1 \dots q_t, \tag{10}$$

где $q_1, \dots, q_t$ — простые числа и $q_1 \leqslant \dots \leqslant q_t$. Так как $p_1 \mid n$, то по обобщению свойства (б) утверждения 13 $p_1 \mid q_i$ при некотором $i \in \overline{1,t}$, и тогда по свойству (в) $p_1 = q_i$. Отсюда и из неравенства $q_1 \leqslant q_i$ получаем: $q_1 \leqslant p_1$. В силу симметрии имеем также $p_1 \leqslant q_1$. Следовательно, $p_1 = q_1$. Теперь из (9), (10), учитывая отсутствие делителей нуля в $\mathbb{Z}$, получаем два представления для числа $\dfrac{n}{p_1}$:

$$\frac{n}{p_1} = p_2 \dots p_s = q_2 \dots q_t.$$

По предположению индукции эти разложения совпадают, а потому совпадают и разложения (9), (10). □

Определение 6. Представление целого числа $n \neq 0$ в виде

$$n = \varepsilon\, p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}, \tag{11}$$

где $\varepsilon = \pm 1$, $s \geqslant 0$, $p_1, p_2, \dots, p_s$ — простые числа, $p_1 < p_2 < \dots < p_s$ и числа $\alpha_1, \alpha_2, \dots, \alpha_s \in \mathbb{N}$, называется *каноническим разложением числа n*. Считается, что при $s = 0$ равенство (11) имеет вид $n = \varepsilon$.

Из теоремы 14 очевидным образом получается

Следствие. *Для любого целого числа $n \neq 0$ существует каноническое разложение, и оно единственно.*

Каноническое разложение числа n дает хорошее представление о строении числа n и часто позволяет довольно легко решать многие вопросы, связанные с делимостью чисел.

В качестве примера приведем известный из средней школы способ нахождения НОД и НОК целых чисел a, b. С этой целью, добавляя, если надо, к их каноническим

разложениям в качестве сомножителей нулевые степени простых чисел, мы всегда сможем записать числа a, b в виде

$$a = \varepsilon_1 p_1^{\alpha_1} \dots p_s^{\alpha_s}, \quad b = \varepsilon_2 p_1^{\beta_1} \dots p_s^{\beta_s},$$

где $\varepsilon_1, \varepsilon_2 \in \{1, -1\}$, $\alpha_i \geqslant 0$, $\beta_i \geqslant 0$, $i \in \overline{1,s}$, $p_1 < \ldots < p_s$. Тогда нетрудно получить формулы

$$(a,b) = \prod_{i=1}^{s} p_i^{\min(\alpha_i,\beta_i)}, \quad [a,b] = \prod_{i=1}^{s} p_i^{\max(\alpha_i,\beta_i)}.$$

Докажите их в качестве упражнения.

В связи с большой ролью, которую играют простые числа в арифметике и особенно в таком ее разделе, как теория делимости, множество простых чисел издавна привлекало к себе внимание ученых. Изучением свойств этого множества занимались такие выдающиеся математики, как Евклид, Ферма, Эйлер, Лежандр[3], Чебышев и др. Многие вопросы из теории простых чисел очень легко формулируются, но чрезвычайно трудно решаются.

Особенно много вопросов, связанных с простыми числами, относится к их распределению в натуральном ряду. Непосредственно из имеющихся таблиц усматривается, что простые числа распределены в натуральном ряду весьма неравномерно. Так, например, в первой сотне насчитывается 25 простых чисел, во второй — 21, в сорок девятой — 8, в пятидесятой — 15. Однако, несмотря на неравномерность распределения, наблюдается общая тенденция к постепенному уменьшению количества простых чисел на все более удаленных отрезках натурального ряда одинаковой длины. При удалении по натуральному ряду в сторону возрастания чисел начинают появляться все более длинные промежутки, не содержащие простых чисел. В связи с этим можно отметить следующий интересный факт. Каково бы ни было натуральное число n, можно найти n составных чисел, непосредственно следующих друг за другом, например,

$$(n+1)!+2,\ (n+1)!+3,\ \ldots,\ (n+1)!+(n+1).$$

В связи с этим естественно возникает вопрос: не является ли множество простых чисел конечным? Отрицательный ответ на этот вопрос дал еще Евклид. Приведем доказательство этого факта.

Теорема 15. *Множество простых чисел бесконечно.*

□ Предположим, что множество простых чисел конечно. Выписав все их в порядке возрастания, получим ряд чисел:

$$2,\ 3,\ 5,\ \ldots,\ p_r. \tag{12}$$

Рассмотрим число $N = 2 \cdot 3 \cdot \ldots \cdot p_r + 1$. Так как каждое число из (12) делит число $2 \cdot 3 \cdot \ldots \cdot p_r$, но не делит 1, то число N не делится ни на одно из чисел (12), т. е. ни на одно простое число. А так как оно больше единицы, то это противоречит теореме 14. □

[3] А. М. Лежандр (1752–1833) — французский математик.

Обозначим через $\pi(x)$ число простых чисел, не превосходящих x. Тогда теорему 15 можно записать в следующем виде:

$$\text{если } x \to \infty, \text{ то } \pi(x) \to \infty.$$

Заметим, что теорема Евклида была обобщена немецким математиком П. Г. Л. Дирихле (1805–1859), который доказал, что любая арифметическая прогрессия, первый член и разность которой взаимно просты, содержит бесконечное множество простых чисел.

Ни теорема Евклида, ни теорема Дирихле ничего не говорят о порядке роста функции $\pi(x)$. Некоторое представление об этом дает следующая теорема, сформулированная впервые Эйлером:

$$\text{если } x \to \infty, \text{ то } \frac{\pi(x)}{x} \to 0.$$

Таким образом, хотя простых чисел «бесконечно много», однако встречаются они в натуральном ряду «бесконечно реже», чем натуральные.

В 1737 г. Эйлер доказал, что ряд чисел, обратных простым числам, т. е. ряд $1/2 + 1/3 + 1/5 + \ldots$, расходится. Из этой теоремы следует также, что простые числа расположены в натуральном ряду «гуще», чем числа, являющиеся квадратами, поскольку известно, что числовой ряд $1/1^2 + 1/2^2 + 1/3^2 + \ldots$ сходится.

В 1808 г. Лежандр опубликовал эмпирически найденную формулу

$$\pi(x) \approx \frac{x}{\ln x - 1,08366},$$

которая при больших значениях x давала приближенные значения для $\pi(x)$.

В 1848 г. П. Л. Чебышев доказал, что если предел отношения $\pi(x)$ к $x/\ln x$ при $x \to \infty$ существует, то он равен единице. Существование же этого предела было доказано в 1896 г. одновременно французским математиком Ж. Адамаром (1865–1963) и бельгийским математиком Ш. Ла Валле Пуссеном (1866–1962). Таким образом, было доказано асимптотическое равенство

$$\pi(x) \sim \frac{x}{\ln x}.$$

В ходе развития теории чисел математиками выделялись и изучались отдельные классы простых чисел. Так, например, Ферма, рассматривая числа вида $2^{2^n} + 1$, выдвинул гипотезу о том, что эти числа являются простыми при всех натуральных n (проверив ее лишь для $n \in \overline{1,4}$). Однако позднее Эйлер показал, что число $2^{2^5} + 1$ составное. Числа вида $2^{2^n} + 1$ называются *числами Ферма*. К настоящему времени известно много составных чисел Ферма и не найдено ни одного нового простого числа Ферма. Французский математик М. Мерсенн (1588–1648) особо интересовался простыми числами вида $2^n - 1$, называя их совершенными. Теперь они называются простыми *числами Мерсенна*. Большое внимание математиков привлекла *гипотеза Гольдбаха*[4]*—Эйлера* о возможности представления любого четного числа $n \geqslant 4$ в

[4] Х. Гольдбах (1690–1764) — немецкий математик. С 1725 г. жил в России, в 1725–1740 гг. был секретарем Петербургской академии наук.

виде суммы двух простых чисел, а любого нечетного $n \geqslant 7$ — в виде суммы трех простых чисел. Для нечетных чисел, больших некоторой константы, эта проблема была положительно решена советским академиком И. М. Виноградовым (1891–1983). Для четных чисел она остается открытой.

Приведенные здесь проблемы, как и многие другие проблемы теории чисел, носят, на первый взгляд, чисто познавательный характер. В действительности же результаты, полученные в ходе решения проблем теории чисел, не только отвечают на загадки натурального ряда, но и находят применение в самых различных областях науки и техники. Так, например, числа Мерсенна и алгоритмы разложения натуральных чисел на простые множители находят приложения в теории кодирования и в теории линейных рекуррентных последовательностей, метод тригонометрических сумм, созданный И. М. Виноградовым для решения проблемы Гольдбаха—Эйлера, применяется при вычислении неэлементарных интегралов, при исследовании статистических свойств последовательностей и т. д.

§ 4. ЧИСЛОВЫЕ ПОЛЯ. ПОЛЕ КОМПЛЕКСНЫХ ЧИСЕЛ

Поле (кольцо), элементами которого являются числа, а операциями — арифметические операции сложения и умножения, называют *числовым полем* (*кольцом*). Из приведенных ранее примеров полей числовыми полями являются $\mathbb{Q}$ и $\mathbb{R}$. Существует много других числовых полей. Так, например, нетрудно убедиться в том, что полем является множество чисел $\{a + b\sqrt{p} : \ a, b \in \mathbb{Q}\}$ из $\mathbb{R}$, где p — фиксированное простое число. Для читателей, знакомых с математикой лишь в объеме средней школы, поле $\mathbb{R}$ является самым широким числовым полем. Однако в математике и ее приложениях используются и не входящие в $\mathbb{R}$ числовые поля. Самым широким числовым полем (по определению) считают поле комплексных чисел. Это поле возникло в результате попыток построить поле, содержащее в качестве подполя поле действительных чисел $\mathbb{R}$ и лишенное известного недостатка поля $\mathbb{R}$ — неразрешимости в нем квадратных уравнений с отрицательными дискриминантами. Так как этот недостаток объясняется невозможностью извлекать в $\mathbb{R}$ квадратный корень из -1, то мы будем строить поле комплексных чисел, исходя из двух основных требований: оно *должно содержать подполе, изоморфное полю* $\mathbb{R}$*, и корень уравнения*

$$x^2 + 1 = 0. \tag{13}$$

В качестве исходного множества возьмем множество упорядоченных пар действительных чисел:

$$\mathbb{C} = \{(a, b) : \ a, b \in \mathbb{R}\}.$$

Подчеркнем, что две пары (a, b), (c, d) из $\mathbb{C}$ считаются равными в том и только том случае, когда $a = c$, $b = d$.

Определим на множестве $\mathbb{C}$ операции сложения и умножения, положив для любых пар (a, b), $(c, d) \in \mathbb{C}$:

$$(a, b) + (c, d) = (a + c, b + d), \tag{14}$$

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc). \tag{15}$$

Теорема 16. *Множество* $\mathbb{C}$ *с операциями сложения и умножения, определяемыми равенствами* (14) *и* (15)*, является полем. В нем содержится подполе, изоморфное* $\mathbb{R}$*, и разрешимо уравнение* (13).

□ Ассоциативность и коммутативность операции сложения в $\mathbb{C}$ следуют непосредственно из соответствующих свойств сложения в $\mathbb{R}$. Нулевым элементом группоида $(\mathbb{C};+)$ является пара $(0,0)$, а противоположным к (a,b) — пара $(-a,-b)$. Следовательно, $(\mathbb{C};+)$ — абелева группа. Ассоциативность и коммутативность умножения в $\mathbb{C}$, а также дистрибутивность умножения относительно сложения, доказываются непосредственной проверкой (которая предоставляется читателю). Тем же путем легко показать, что единицей кольца $(\mathbb{C};+;\cdot)$ является пара $(1,0)$, а элементом, обратным к $(a,b)\neq(0,0)$, — пара $(a/(a^2+b^2),\ -b/(a^2+b^2))$. Последняя находится из уравнения $(a,b)(x,y)=(1,0)$. Таким образом, $\mathbb{C}$ — поле.

Рассмотрим в $\mathbb{C}$ подмножество

$$\mathbb{C}_1=\{(a,0):\ a\in\mathbb{R}\}.$$

Нетрудно видеть, что множество $\mathbb{C}_1$ замкнуто относительно операций $+$, $\cdot$ в $\mathbb{C}$, а именно:

$$(a,0)+(b,0)=(a+b,0),\quad (a,0)\cdot(b,0)=(ab,0). \tag{16}$$

Отсюда следует, что отображение $\sigma\colon \mathbb{R}\to\mathbb{C}_1$, определенное условием $\forall\, a\in\mathbb{R}:\ \sigma(a)=(a,0)$, является изоморфизмом относительно операций $+$, $\cdot$. Следовательно, по теореме 16 главы 3 $\mathbb{C}_1$ есть поле, изоморфное полю $\mathbb{R}$. Для завершения доказательства теоремы остается заметить еще, что уравнению (13) удовлетворяет пара $(0,1)$. □

Определение 7. Построенное поле $\mathbb{C}$ называется *полем комплексных чисел*, а его элементы — *комплексными числами*.

Из равенств (16) видно, что операции над числами $(a,0)$, $(b,0)$, по существу, сводятся к соответствующим операциям над действительными числами a, b. В связи с этим естественно отождествить комплексное число $(a,0)$ с действительным числом a и тем самым включить множество $\mathbb{R}$ в $\mathbb{C}$. Заметим, что такой способ включения $\mathbb{R}$ в $\mathbb{C}$ является частным видом более общей конструкции (см. главу 22). Если теперь ввести обозначение $(0,1)=i$, то можно будет получить новое представление для любого комплексного числа:

$$(a,b)=(a,0)+(0,b)=(a,0)+(b,0)(0,1)=a+bi.$$

В такой форме чаще всего и используются комплексные числа на практике. При этом i называют *мнимой единицей*, a *— действительной частью* числа $a+bi$, b *— коэффициентом перед мнимой единицей*, bi *— мнимой частью* числа $a+bi$.

Заметим, что название «мнимая единица» за числом i сохранилось лишь в силу исторических традиций, поскольку символ i использовался вначале для обозначения «несуществующего» квадратного корня из -1.

В новых обозначениях равенства (14), (15), определяющие операции сложения и умножения комплексных чисел, примут вид

$$(a+bi)+(c+di)=(a+c)+(b+d)i,$$
$$(a+bi)(c+di)=(ac-bd)+(ad+bc)i.$$

Запишем в новой форме разность двух комплексных чисел и частное от деления на комплексное число, отличное от 0:

$$(a+bi)-(c+di)=(a-c)+(b-d)i,$$
$$\frac{a+bi}{c+di}=\frac{ac+bd}{c^2+d^2}+\frac{-ad+bc}{c^2+d^2}i. \tag{17}$$

ОПРЕДЕЛЕНИЕ 8. Комплексное число $a-bi$ называется *сопряженным* к числу $z=a+bi$ и обозначается через $\overline{z}$.

Утверждение 17. *Для любых комплексных чисел z, z_1 имеют место равенства*

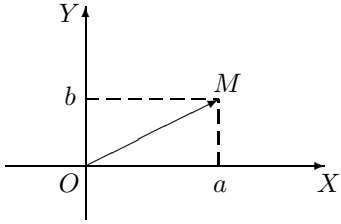
$$\overline{\overline{z}}=z, \qquad \overline{z+z_1}=\overline{z}+\overline{z}_1, \qquad \overline{zz_1}=\overline{z}\cdot\overline{z}_1.$$

Если $z\neq 0$, то выполняется также равенство $\overline{z}^{\,-1}=\overline{z^{-1}}$.

Утверждение доказывается непосредственной проверкой. Проделайте ее в качестве упражнения.

Наряду с представлением комплексных чисел в виде $a+bi$ в математике и ее приложениях часто используется их представление в тригонометрической форме. Для определения такого представления введем сначала геометрическую интерпретацию комплексных чисел.

Возьмем на плоскости декартову систему координат XOY и изобразим комплексное число $z=a+bi$ точкой плоскости XOY с координатами a, b (см. рисунок).



В итоге комплексному числу z будет сопоставлена точка M плоскости. Легко видеть, что это соответствие между комплексными числами и точками координатной плоскости XOY биективно, поэтому иногда множество комплексных чисел отождествляют с множеством точек координатной плоскости.

ОПРЕДЕЛЕНИЕ 9. Расстояние от точки O координатной плоскости XOY до точки M, изображающей комплексное число z, называют *модулем числа z* и обозначают в виде $|z|$. Наименьший угол, на который нужно повернуть ось OX против часовой стрелки до совпадения ее направления с направлением вектора OM, называется *аргументом числа $z\neq 0$* и обозначается в виде $\arg z$. Для $z=0$ аргумент не определяется.

Непосредственно из чертежа видно, что модуль числа $z = a + bi$ находится по формуле

$$|z| = \sqrt{a^2 + b^2},$$

где $\sqrt{a^2 + b^2}$ есть арифметический корень из неотрицательного действительного числа $a^2 + b^2$, а аргумент числа $z = a + bi \neq 0$ находится из соотношений

$$\cos(\arg z) = \frac{a}{\sqrt{a^2 + b^2}}, \quad \sin(\arg z) = \frac{b}{\sqrt{a^2 + b^2}}, \quad 0 \leqslant \arg z < 2\pi.$$

Отсюда видно также, что комплексное число $z = a + bi$ представимо в виде

$$z = |z|\,(\cos(\arg z) + i\sin(\arg z)). \tag{18}$$

Определение 10. *Тригонометрической формой комплексного числа* z называется любая его запись вида

$$z = \rho(\cos\varphi + i\sin\varphi), \tag{19}$$

где $\rho, \varphi \in \mathbb{R}$ и $\rho \geqslant 0$.

Утверждение 18. *Всякое комплексное число* z *представимо в тригонометрической форме. Если* $z \neq 0$ *и* (19) *есть представление его в тригонометрической форме, то* $\rho = |z|$, *а* $\varphi = \arg z + 2\pi k$, $k \in \mathbb{Z}$.

□ Из (18) и очевидного равенства $0 = 0(\cos 0 + i\sin 0)$ видно, что тригонометрическая форма существует для любого $z \in \mathbb{C}$. Пусть теперь $z \neq 0$ и выполняется равенство (19). Разделив обе части равенства (19) на соответствующие части равенства (18) (по формуле (17)), получим:

$$1 = \frac{\rho}{|z|}\cos(\varphi - \arg z) + i\frac{\rho}{|z|}\sin(\varphi - \arg z).$$

Отсюда имеем:

$$\frac{\rho}{|z|}\cos(\varphi - \arg z) = 1, \quad \frac{\rho}{|z|}\sin(\varphi - \arg z) = 0,$$

и потому $\rho = |z|$, $\varphi = \arg z + 2\pi k$, $k \in \mathbb{Z}$. □

Тригонометрическая форма комплексного числа полезна тем, что в ней проще, чем в алгебраической форме, осуществляется умножение, деление, возведение в степень комплексных чисел и извлечение корней из комплексного числа.

Теорема 19. *Для любых комплексных чисел* $z_1 = \rho_1(\cos\varphi_1 + i\sin\varphi_1)$, $z_2 = \rho_2(\cos\varphi_2 + i\sin\varphi_2)$ *справедливы равенства*:

(а) $z_1 z_2 = \rho_1\rho_2(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2))$;

(б) $z_1^m = \rho_1^m(\cos m\varphi_1 + i\sin m\varphi_1)$, $m \in \mathbb{N}$.

Если $z_2 \neq 0$, *то выполняется также равенство*

(в) $z_1/z_2 = \rho_1/\rho_2(\cos(\varphi_1 - \varphi_2) + i\sin(\varphi_1 - \varphi_2))$.

□ Равенства (а) и (в) проверяются непосредственно с использованием определения операций над комплексными числами. Проделайте это в качестве упражнения. Равенство (б) есть следствие равенства (а). □

Равенство (б) из теоремы 19 называют *формулой Муавра* в честь английского математика А. де Муавра (1667–1754). Наряду с этой формулой им же была выведена и формула извлечения корня n-й степени из комплексного числа $z = \rho(\cos\varphi + i\sin\varphi)$, т. е. формула нахождения всех корней уравнения

$$x^n = z \tag{20}$$

относительно неизвестного x. Как и для действительных чисел, множество всех *корней n-й степени* из комплексного числа z обозначают в виде $\sqrt[n]{z}$.

Пусть $\alpha = r(\cos\psi + i\sin\psi)$ есть решение уравнения (20). При $z = 0$ уравнению (20) удовлетворяет лишь число $x = 0$. Поэтому далее будем считать, что $z \neq 0$. Подставив в (20) числа α и z в тригонометрической форме и воспользовавшись формулой Муавра, получим:

$$r^n(\cos(n\psi) + i\sin(n\psi)) = \rho(\cos\varphi + i\sin\varphi).$$

Отсюда и из утверждения 18 имеем:

$$r^n = \rho, \quad n\psi = \varphi + 2\pi k,$$

или

$$r = \sqrt[n]{\rho}, \quad \psi = \frac{\varphi + 2\pi k}{n},$$

где k — некоторое целое число, $\sqrt[n]{\rho}$ — арифметический корень из действительного неотрицательного числа ρ. Таким образом, корнями n-й степени из числа z могут быть лишь числа

$$\alpha_k = \sqrt[n]{\rho}\left(\cos\frac{\varphi + 2\pi k}{n} + i\sin\frac{\varphi + 2\pi k}{n}\right), \quad k \in \mathbb{Z}. \tag{21}$$

Непосредственной проверкой, путем возведения в n-ю степень по формуле Муавра, легко убедиться в том, что число (21) при любом целом k является корнем n-й степени из числа z. Выясним, сколько среди чисел вида (21) различных.

По теореме 2 произвольное число k представляется в виде $k = nq + r$, где $r \in \{0, \ldots, n-1\}$. Отсюда и из очевидного равенства $\alpha_{nq+r} = \alpha_r$ получаем: $\sqrt[n]{z} \subset \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$. С другой стороны, из утверждения 18 следует, что числа $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ различны. Следовательно, $\sqrt[n]{z} = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$. В итоге доказана

Теорема 20. *Для любого $n \in \mathbb{N}$ корень n-й степени из комплексного числа*

$$z = \rho(\cos\varphi + i\sin\varphi) \neq 0$$

имеет ровно n различных значений, и все они находятся по формуле (21) *при* $k = 0, 1, \ldots, n-1$.

Следствие. *В поле комплексных чисел разрешимо любое квадратное уравнение* $ax^2 + bx + c = 0$*, и его корни находятся по формуле*

$$x = \frac{-b + \delta}{2a}, \quad \text{где} \quad \delta \in \sqrt{b^2 - 4ac}.$$

□ Доказательство проводится по аналогии с выводом формулы для корней квадратного уравнения в $\mathbb{R}$. Следует учесть, что здесь множество $\sqrt{b^2 - 4ac}$ всегда не пусто. □

Рассмотрим несколько подробнее множество Γ_n всех корней n-й степени из 1. При небольших значениях n, пользуясь формулой (21) при $z = 1 = \cos 0 + i \sin 0$, получим:

$$\Gamma_1 = \{1\}, \quad \Gamma_2 = \{1, -1\},$$

$$\Gamma_3 = \{1, \ -1/2 + i\sqrt{3/2}, \ -1/2 - i\sqrt{3/2}\}, \quad \Gamma_4 = \{1, -1, i, -i\}.$$

В общем случае

$$\Gamma_n = \{\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}\},$$

где

$$\varepsilon_k = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n}, \quad k \in \overline{0, n-1}. \tag{22}$$

Утверждение 21. *При любом натуральном* n *множество* Γ_n *всех корней* n*-й степени из* 1 *является группой относительно операции умножения комплексных чисел.*

□ Множество Γ_n замкнуто относительно умножения, поскольку

$$\varepsilon_s^n = 1, \ \varepsilon_t^n = 1 \ \Rightarrow \ (\varepsilon_s \varepsilon_t)^n = 1.$$

Γ_n содержит $1 = \varepsilon_0$ и вместе с каждым элементом ε_k — обратный ему элемент ε_{n-k}. Ассоциативность операции умножения в Γ_n следует из ее ассоциативности в $\mathbb{C}$. □

Следствие. *Для любого натурального числа* n *существует абелева группа из* n *элементов.*

Отметим одно замечательное свойство группы Γ_n. Из равенства (22) и формулы Муавра следует, что

$$\varepsilon_k = \varepsilon_1^k,$$

т. е. все элементы группы Γ_n являются степенями одного ее элемента ε_1. В связи с этим говорят, что группа Γ_n порождается элементом ε_1. Возникает вопрос, есть ли в Γ_n другие элементы, обладающие таким свойством? Прежде чем ответить на этот вопрос, докажем

Утверждение 22. *Для любого* $n \in \mathbb{N}$ *выполняется равенство*

$$\Gamma_n = \bigcup_{d|n} \Gamma_d,$$

где объединение множеств Γ_d *берется по всем делителям* $d \in \mathbb{N}$ *числа* n.

□ Обозначим $\bigcup_{d|n} \Gamma_d = K_n$. Включение $\Gamma_n \subset K_n$ следует из делимости $n \mid n$. Обратное включение доказывает импликация

$$\varepsilon^d = 1 \;\Rightarrow\; \varepsilon^n = 1,$$

которая, очевидно, истинна для любого делителя d числа n. □

Таким образом, среди всех корней n-й степени из 1 содержатся корни из 1 всех меньших степеней, являющихся делителями числа n. Например, $\Gamma_1 \subset \Gamma_2 \subset \Gamma_4$. В связи с этим естественно выделить из Γ_n корни собственно n-й степени из 1.

Определение 11. Корень n-й степени из 1 называется *примитивным*, или *первообразным*, если он не является корнем m-й степени из 1 при $m < n$.

Следующая теорема отвечает на поставленный выше вопрос и дает описание всех примитивных корней n-й степени из 1.

Теорема 23. *Следующие утверждения эквивалентны при любом $n \in \mathbb{N}$ и любом $k \in \{0, \ldots, n-1\}$:*

(а) *ε_k порождает группу Γ_n, т. е. $\Gamma_n = \{\varepsilon_k^0, \varepsilon_k^1, \ldots, \varepsilon_k^{n-1}\}$;*

(б) *ε_k — примитивный корень n-ой степени из 1;*

(в) *число k взаимно просто с n.*

□ Для доказательства достаточно установить истинность импликаций (а)⇒(б)⇒ ⇒(в)⇒(а).

(а)⇒(б) Если ε_k — не примитивный корень, то $\varepsilon_k^m = 1$ при некотором $m < n$ и $m > 0$. Следовательно, $\varepsilon_k \in \Gamma_m$, а потому $\varepsilon_k^l \in \Gamma_m$ при любом $l \in \mathbb{Z}$. Следовательно, ε_k не порождает Γ_n, и импликация (а)⇒(б) истинна.

(б)⇒(в) Если $(n, k) = d > 1$, то

$$\varepsilon_k^{n/d} = (\varepsilon_1^k)^{n/d} = (\varepsilon_1^n)^{k/d} = 1^{k/d} = 1,$$

и корень ε_k — не примитивный, что противоречит условию.

(в)⇒(а) Так как $(k, n) = 1$, то по следствию из теоремы 6 найдутся числа $u, v \in \mathbb{Z}$ такие, что $ku + nv = 1$, и потому $(ku + nv)s = s$ при любом $s \in \mathbb{Z}$. Следовательно, для любого $s \in \overline{0, n-1}$ имеем:

$$\varepsilon_s = \varepsilon_1^s = \varepsilon_1^{(ku+nv)s} = (\varepsilon_1^{ku})^s = (\varepsilon_1^k)^{us} = \varepsilon_k^{us}.$$

Таким образом, любой корень ε_s степени n из 1 является степенью корня ε_k, т. е. ε_k порождает группу Γ_n. □

В заключение укажем на связь корней n-й степени из любого числа z с корнями n-й степени из 1. Сравнивая формулы (21) и (22), получаем $\alpha_k = \alpha_0 \cdot \varepsilon_k$, $k \in \overline{0, n-1}$. Отсюда следует

Утверждение 24. *Все корни n-й степени из комплексного числа z получаются путем умножения одного из них на все корни n-й степени из 1.*

ЗАДАЧИ

1. Докажите, что при любом целом $k > 1$ и любом $n \in \mathbb{N}$ число $a \in \overline{0,\, k^n - 1}$ можно однозначно представить в виде

$$a = a_0 + a_1 k + a_2 k^2 + \ldots + a_{n-1} k^{n-1}, \text{ где } a_i \in \overline{0, k-1}.$$

Такое представление числа a называют *k-ичным*.

2. Докажите, что при любом $n \in \mathbb{N}$ каждое число $a \in \overline{0,\, (n+1)! - 1}$ можно однозначно представить в виде

$$a = a_1 \cdot 1! + a_2 \cdot 2! + \ldots + a_n \cdot n!,$$

где $a_i \in \overline{0, i}$. Такое представление числа называют *факториальным*.

3. Пусть $a, b, m \in \mathbb{Z}$ и $m \neq 0$. Докажите, что если числа a, b дают при делении на m одинаковые остатки, то $(a, m) = (b, m)$.

4. Докажите равенство (для любых целых чисел a_i, b_i):

$$(a_1, \ldots, a_n,\, b_1, \ldots, b_n) = ((a_1, b_1), \ldots, (a_n, b_n)).$$

5. Докажите, что если $a_1, \ldots, a_n, b \in \mathbb{Z}$, $n \geqslant 2$ и $(a_1, \ldots, a_n, b) = d$, то существуют такие $c_2, \ldots, c_n \in \mathbb{Z}$, что $(a_1 + c_2 a_2 + \ldots + c_n a_n,\, b) = d$.

6. Пусть $n \geqslant 2$, $a_1, \ldots, a_n$ — попарно взаимно простые натуральные числа и $b_i = \dfrac{a_1 a_2 \ldots a_n}{a_i}$. Докажите, что $(b_1, \ldots, b_n) = 1$.

7. По каноническому разложению натурального числа найдите число и сумму его положительных делителей.

8. В скольких вариантах можно восстановить пару натуральных чисел a, b по их НОД и НОК?

9. Пусть $n \geqslant 2$, $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$, $d \in \mathbb{N}$. Докажите, что следующие утверждения эквивалентны:

а) $(a_1, \ldots, a_n) = d$;

б) для чисел $a_1, \ldots, a_n$ число d является общим делителем вида $u_1 a_1 + \ldots + u_n a_n$, где $u_1, \ldots, u_n \in \mathbb{Z}$;

в) d — наименьшее натуральное число вида $u_1 a_1 + \ldots + u_n a_n$, где $u_1, \ldots, u_n \in \mathbb{Z}$;

г) d — максимальный общий делитель чисел $a_1, \ldots, a_n$.

10. Пусть $\exp_q(n)$ — показатель степени простого числа q в каноническом разложении числа n, и $[x]$ — целая часть числа $x \in \mathbb{R}$. Докажите, что

а) $\exp_q(n!) = \sum\limits_{i=1}^{[\log_q n]} \left[\dfrac{n}{q^i} \right]$,

б) $\exp_q(C_{q^n}^m) = n - \exp_q m$.

11. Докажите, что для любых чисел $a \in \mathbb{Z}$, $m, n \in \mathbb{N}$ справедливо равенство

$$(a^m - 1,\, a^n - 1) = a^{(m,n)} - 1.$$

(*Указание*: предварительно докажите равенство $(kq + r, k) = (r, k)$ для любых чисел $k, q, r \in \mathbb{Z}$.)

12. Пусть $a_1, \ldots, a_n \in \mathbb{N}$, $(a_1, \ldots, a_n) = d$,

$$M = \{a_1u_1 + \ldots + a_nu_n :\ u_1, \ldots, u_n \in \mathbb{N}_0\}.$$

Докажите, что тогда существует $q \in \mathbb{N}$ такое, что все числа из $\mathbb{N}$, кратные d и большие или равные qd, принадлежат M.

13. По аналогии с НОД чисел $a_1, \ldots, a_n$ определите НОД для бесконечного множества M целых чисел и докажите, что он совпадает с НОД некоторого конечного подмножества чисел из M.

14. Подкольцо $\mathbb{Z}[i] = \{a + bi :\ a, b \in \mathbb{Z}\}$ поля комплексных чисел $\mathbb{C}$ называется *кольцом целых гауссовых чисел*. Сформулируйте и докажите аналог теоремы о делении с остатком в кольце целых гауссовых чисел, определив предварительно в нем понятие деления с остатком (по аналогии с кольцом $\mathbb{Z}$).

15. Докажите, что отображение $\tau\colon \mathbb{C} \to \mathbb{C}$, определенное равенством $\tau(z) = \overline{z}$, является изоморфизмом поля $\mathbb{C}$ на себя.

16. Для корня ε_k n-й степени из 1 (см. (22)) найдите наименьшее натуральное m, при котором $\varepsilon_k \in \Gamma_m$.

Глава 5

КОЛЬЦА И ПОЛЯ ВЫЧЕТОВ

В данной главе будут построены бесконечные серии конечных колец и конечных полей, играющих важную роль в математике и ее приложениях.

§ 1. СРАВНЕНИЯ ЦЕЛЫХ ЧИСЕЛ ПО МОДУЛЮ

Зафиксируем натуральное число m, которое условимся называть модулем.

Определение 1. Два целых числа a, b называются *сравнимыми по модулю* m, если они при делении на m дают одинаковые остатки. Утверждение: «a сравнимо с b по модулю m» кратко записывается в виде соотношения

$$a \equiv b \,(\mathrm{mod}\, m),$$

называемого *сравнением*.

Теорема 1 (критерий сравнимости). *Для любых целых чисел a, b*

$$a \equiv b \,(\mathrm{mod}\, m) \;\Leftrightarrow\; m \mid a - b.$$

□ Разделим числа a, b с остатком на m:

$$a = mq_1 + r_1,\; b = mq_2 + r_2,\; 0 \leqslant r_i < m,\; i \in \overline{1,2}.$$

Если $a \equiv b \,(\mathrm{mod}\, m)$, то $r_1 = r_2$ и разность $a - b = m(q_1 - q_2)$ делится на m. Обратно, если $m \mid a - b$, то из равенства $a - b = m(q_1 - q_2) + (r_1 - r_2)$ следует, что $m \mid r_1 - r_2$. А так как $|r_1 - r_2| < m$, то по утверждению 1(б) главы 4 $r_1 - r_2 = 0$, т. е. $r_1 = r_2$, или $a \equiv b \,(\mathrm{mod}\, m)$. □

Теорема 2. (а) *Отношение сравнимости целых чисел по модулю m является отношением эквивалентности на $\mathbb{Z}$.*

(б) *Для любых $a, b, c, d \in \mathbb{Z}$*

$$a \equiv b \,(\mathrm{mod}\, m),\; c \equiv d \,(\mathrm{mod}\, m) \;\Rightarrow\; a * c \equiv b * d \,(\mathrm{mod}\, m),$$

где $*$ — любая из операций $+$, $-$, $\cdot$ (т. е. сравнения можно почленно складывать, вычитать и перемножать).

(в) *Если d — общий делитель чисел a, b, m из $\mathbb{Z}$, то*

$$a \equiv b \,(\mathrm{mod}\, m) \;\Leftrightarrow\; a/d \equiv b/d \,(\mathrm{mod}\, m/d)$$

(*т. е. обе части сравнения и модуль можно делить и умножать на одно и то же число*).

(г) *Если d — общий делитель чисел a, b и $(d, m) = 1$, то*

$$a \equiv b \,(\mathrm{mod}\, m) \;\Leftrightarrow\; a/d \equiv b/d \,(\mathrm{mod}\, m)$$

(*т. е. обе части сравнения можно умножать и делить на число, взаимно простое с модулем*).

□ (а) Непосредственно из определения 1 видно, что отношение сравнимости по модулю m рефлексивно, симметрично и транзитивно, т. е. является отношением эквивалентности.

(б) Из условия, согласно критерию сравнимости чисел, получаем, что $a - b = mq_1$ и $c - d = mq_2$, т. е. $a = b + mq_1$ и $c = d + mq_2$, где $q_1, q_2 \in \mathbb{Z}$. Складывая, вычитая и перемножая последние равенства, получим:

$$\begin{aligned} a + c &= b + d + m(q_1 + q_2), \\ a - c &= b - d + m(q_1 - q_2), \\ ac &= bd + m(q_1 d + bq_2 + mq_1 q_2). \end{aligned}$$

Отсюда видно, что разность $(a * c) - (b * d)$ делится на m при любой операции $* \in \{+, -, \cdot\}$. Следовательно, $a * c \equiv b * d \,(\mathrm{mod}\, m)$.

(в) Так как d — общий делитель чисел a, b, m, то существуют целые числа a_1, b_1, m_1, такие, что $a = a_1 d$, $b = b_1 d$, $m = m_1 d$. Отсюда и из определения делимости чисел, учитывая отсутствие делителей нуля в кольце $\mathbb{Z}$, получим:

$$m \mid a - b \;\Leftrightarrow\; m_1 d \mid (a_1 - b_1)d \;\Leftrightarrow\; m_1 \mid a_1 - b_1.$$

Теперь свойство (в) следует непосредственно из теоремы 1.

(г) Как и в случае (в), имеем:

$$m \mid a - b \;\Leftrightarrow\; m \mid (a_1 - b_1)d.$$

Так как числа m, d взаимно просты, то по теореме 9(б) главы 4

$$m \mid (a_1 - b_1)d \;\Rightarrow\; m \mid a_1 - b_1.$$

Обратная импликация следует из утверждения 11(в) главы 3. Теперь осталось применить теорему 1. □

Следствие 1. *Для любых целых чисел a, b, c и натурального k справедлива импликация*

$$a \equiv b \,(\mathrm{mod}\, m) \;\Rightarrow\; a * c \equiv b * c \,(\mathrm{mod}\, m),\; a^k \equiv b^k \,(\mathrm{mod}\, m),$$

где $*$ — любая из операций $+$, $-$, $\cdot$.

Приведенными свойствами сравнений можно воспользоваться для нахождения остатков от деления чисел на заданное число m.

Следствие 2. *Для любых целых чисел a, b и операции $* \in \{+, -, \cdot\}$ верно равенство*

$$r_m(a * b) = r_m(r_m(a) * r_m(b)). \tag{1}$$

□ Так как $a \equiv r_m(a) \pmod m$, $b \equiv r_m(b) \pmod m$, то по теореме 2(б)

$$a * b \equiv r_m(a) * r_m(b) \pmod m.$$

Отсюда по определению 1 имеем (1). □

Пример 1. Найдем остаток от деления числа $a = 128^{148} - 148^{129}$ на число 13. По следствию 2

$$r_{13}(a) = r_{13}(r_{13}(128^{148}) - r_{13}(148^{129})).$$

Поэтому найдем сначала остатки $r_{13}(128^{148})$, $r_{13}(148^{129})$. Заметим, что число $128 \equiv -2 \pmod{13}$. Отсюда последовательно находим:

$$\begin{aligned}
&128^2 \equiv (-2)^2 \pmod{13}, && \text{т. е. } 128^2 \equiv 4 \pmod{13},\\
&128^4 \equiv 4^2 \pmod{13}, && \text{т. е. } 128^4 \equiv 3 \pmod{13},\\
&128^6 \equiv 4 \cdot 3 \pmod{13}, && \text{т. е. } 128^6 \equiv -1 \pmod{13},\\
&128^{12} \equiv (-1)^2 \pmod{13}, && \text{т. е. } 128^{12} \equiv 1 \pmod{13}.
\end{aligned}$$

Так как $148 = 12 \cdot 12 + 4$, то $128^{148} = (128^{12})^{12} \cdot 128^4 \equiv 3 \pmod{13}$, и потому $r_{13}(128^{148}) = 3$. Аналогично найдем, что $r_{13}(148^{129}) = 5$. В итоге имеем искомый остаток:

$$r_{13}(a) = r_{13}(3 - 5) = r_{13}(-2) = 11.$$

§ 2. КЛАССЫ ВЫЧЕТОВ И ОПЕРАЦИИ НАД НИМИ

По теореме 2(а) отношение сравнимости по модулю m является отношением эквивалентности на $\mathbb{Z}$, и потому множество $\mathbb{Z}$ разбивается на непересекающиеся классы чисел, сравнимых по модулю m, т. е. дающих одинаковые остатки при делении на m (см. теорему 1 главы 2).

Определение 2. Класс всех целых чисел, сравнимых с числом a по модулю m, называют *классом вычетов по модулю m* и обозначают через $[a]_m$. Множество всех классов вычетов по модулю m обозначим через $\mathbb{Z}/m$.

Из определения 2 имеем:

$$\begin{aligned}
&[a]_m = \{x \in \mathbb{Z} \colon\ r_m(x) = r_m(a)\},\\
&[a]_m = [b]_m \ \Leftrightarrow\ a \equiv b \pmod m.
\end{aligned} \tag{2}$$

Так как различные остатки от деления целых чисел на m исчерпываются числами $0, 1, \ldots, m-1$, то число классов вычетов по модулю m равно m, и

$$\mathbb{Z}/m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}.$$

Определим на множестве $\mathbb{Z}/m$ операции сложения и умножения.

Определение 3. Для любых $[a]_m, [b]_m \in \mathbb{Z}/m$ положим:

$$[a]_m + [b]_m = [a+b]_m, \quad [a]_m \cdot [b]_m = [ab]_m.$$

Таким образом, чтобы сложить (перемножить) классы $[a]_m$, $[b]_m$, нужно выбрать из них по одному представителю, сложить (перемножить) их как числа и взять класс, содержащий полученное число. В определении 3 в качестве таких представителей выбраны числа a и b. Однако в классах $[a]_m$, $[b]_m$ содержится много других чисел, и мы заранее не уверены в том, что результат сложения (умножения) классов не зависит от выбора представителей. Если бы результат зависел от выбора представителей, то, складывая (перемножая) одни и те же классы, мы могли бы получать разные результаты. Это бы означало, что операции определены некорректно.

Докажем, что определение 3 корректно.

Действительно, пусть $a_1 \in [a]_m$, $b_1 \in [b]_m$. Тогда $a_1 \equiv a \pmod m$, $b_1 \equiv b \pmod m$, и по теореме 2 имеем:

$$a_1 + b_1 \equiv a + b \pmod m, \quad a_1 b_1 \equiv ab \pmod m,$$

т. е. $[a_1 + b_1]_m = [a+b]_m$, $[a_1 b_1]_m = [ab]_m$. Следовательно, результаты операций над классами не зависят от выбора представителей, т. е. операции определены корректно.

Теорема 3. *Множество $\mathbb{Z}/m$ всех классов вычетов по модулю m с определенными выше операциями сложения и умножения является коммутативным кольцом с единицей.*

□ Так как операции сложения и умножения над классами сводятся к соответствующим операциям над целыми числами, то обе они ассоциативны и коммутативны, кроме того, операция умножения дистрибутивна относительно сложения. Очевидно, что классы $[0]_m$ и $[1]_m$ являются в $\mathbb{Z}/m$ нейтральными элементами относительно операций соответственно $+$, $\cdot$, и для любого $[a]_m$ класс $[-a]_m$ является противоположным элементом, т. е. $-[a]_m = [-a]_m$. □

Кольцо $(\mathbb{Z}/m, +, \cdot)$ называется *кольцом классов вычетов по модулю m*, или, короче, *кольцом вычетов по модулю m*.

Следующее утверждение описывает в кольце $\mathbb{Z}/m$ обратимые элементы и делители нуля.

Теорема 4. *В кольце $\mathbb{Z}/m$ каждый элемент $[a]_m \neq [0]_m$ или обратим, или делитель нуля, причем*

(а) $[a]_m$ *обратим* $\Leftrightarrow$ $(a, m) = 1$,

(б) $[a]_m$ *— делитель нуля* $\Leftrightarrow$ $(a, m) \neq 1$.

□ Пусть $(a, m) = 1$. По следствию из теоремы 6 главы 4 существуют $u, v \in \mathbb{Z}$ такие, что $au + mv = 1$. Тогда $[au + mv]_m = [1]_m$, и согласно определению 3

$$[a]_m \cdot [u]_m + [m]_m \cdot [v]_m = [1]_m.$$

Отсюда и из равенства $[m]_m = [0]_m$ имеем: $[a]_m \cdot [u]_m = [1]_m$. Следовательно, элемент $[a]_m$ обратим, и $[a]_m^{-1} = [u]_m$.

Пусть $(a, m) = d > 1$. Тогда $a = da_1$, где $a_1 \in \mathbb{Z}$, и

$$[a]_m \cdot \left[\frac{m}{d}\right]_m = \left[\frac{a}{d}\, m\right]_m = [a_1 m]_m = [0]_m.$$

Так как $[a]_m \neq [0]_m$ по условию и $[\frac{m}{d}]_m \neq [0]_m$ в силу неравенства $d > 1$, то $[a]_m$ — делитель нуля.

Так как в любом кольце с единицей множества обратимых элементов и делителей нуля не пересекаются (задача 12 главы 3), то из доказанного следуют утверждения (а) и (б) теоремы. □

Из теорем 3 и 4 получаем

Следствие 1. *Порядок мультипликативной группы $(\mathbb{Z}/m)^*$ кольца $\mathbb{Z}/m$ равен количеству натуральных чисел, не превосходящих m и взаимно простых с m.*

Следствие 2. *Кольцо $\mathbb{Z}/m$ является полем тогда и только тогда, когда m — простое число.*

Если $m = p$ — простое число, то поле $(\mathbb{Z}/p, +, \cdot)$ называется *полем вычетов по модулю p*.

Рассмотрим вопрос о вычислении порядка группы $(\mathbb{Z}/m)^*$.

Определение 4. Отображение $\varphi\colon \mathbb{N} \to \mathbb{N}$, сопоставляющее каждому числу $m \in \mathbb{N}$ число $\varphi(m)$, равное количеству натуральных чисел $a \leqslant m$, взаимно простых с m, называется *функцией Эйлера*.

Пример 2. $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(10) = 4$, $\varphi(p) = p - 1$ для любого простого p.

Из определения 4 и следствия 1 теоремы 4 имеем:

$$|(\mathbb{Z}/m)^*| = \varphi(m).$$

Приведем формулу для вычисления $\varphi(m)$.

Теорема 5. *Если m — натуральное число, имеющее каноническое разложение $m = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$, то*

$$\varphi(m) = m\Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big) \dots \Big(1 - \frac{1}{p_s}\Big).$$

□ Найдем сначала $\varphi(p_i^{k_i})$. Так как p_i — простое число, то $(a, p_i^{k_i}) \neq 1$ в том и только том случае, когда $p_i \mid a$. Следовательно, написав ряд чисел от 1 до $p_i^{k_i}$ и удалив из него все числа, кратные p_i, получим:

$$\varphi(p_i^{k_i}) = p_i^{k_i} - p_i^{k_i-1} = p_i^{k_i}\Big(1 - \frac{1}{p_i}\Big).$$

Теперь для доказательства теоремы достаточно воспользоваться свойством *мультипликативности функции Эйлера*:

$$\forall\, m_1, m_2 \in \mathbb{N}\colon\ ((m_1, m_2) = 1 \ \Rightarrow\ \varphi(m_1 m_2) = \varphi(m_1)\,\varphi(m_2)),$$

которое мы пока примем без доказательства (оно будет получено попутно при изучении групп в § 5 главы 11). □

Докажем одно из замечательных свойств функции Эйлера.

Теорема 6. *Если $a \in \mathbb{Z}$, $m \in \mathbb{N}$ и числа a, m взаимно просты, то*

$$a^{\varphi(m)} \equiv 1 \,(\mathrm{mod}\, m). \tag{3}$$

□ Выпишем по одному представителю из каждого класса группы $(\mathbb{Z}/m)^*$:

$$a_1,\ a_2,\ \ldots,\ a_{\varphi(m)}.$$

Умножив все эти числа на a, получим ряд чисел:

$$a_1 a,\ a_2 a,\ \ldots,\ a_{\varphi(m)} a. \tag{4}$$

По теореме 9(а) главы 4 все числа из (4) взаимно просты с m. Кроме того, все они попарно несравнимы по модулю m, поскольку в силу теоремы 2(г)

$$a_i a \equiv a_j a \,(\mathrm{mod}\, m)\ \Rightarrow\ a_i \equiv a_j \,(\mathrm{mod}\, m).$$

Отсюда, учитывая, что $|(\mathbb{Z}/m)^*| = \varphi(m)$, получаем: (4) есть система представителей, взятых по одному из каждого класса множества $(\mathbb{Z}/m)^*$. Следовательно, имеет место система сравнений

$$\begin{gathered} a_1 a \equiv a_{i_1} \,(\mathrm{mod}\, m), \\ a_2 a \equiv a_{i_2} \,(\mathrm{mod}\, m), \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{\varphi(m)} a \equiv a_{i_{\varphi(m)}} \,(\mathrm{mod}\, m), \end{gathered}$$

где $i_1, i_2, \ldots, i_{\varphi(m)}$ — некоторая перестановка чисел $1, 2, \ldots, \varphi(m)$. Перемножив почленно эти сравнения и разделив обе части полученного сравнения на число $a_1 a_2 \ldots a_{\varphi(m)}$, которое взаимно просто с m, получим (3). □

Следствие. *Если p — простое число и $a \in \mathbb{Z}$, то*

(а) $a^{p-1} \equiv 1 \,(\mathrm{mod}\, p)$ *при* $(a, p) = 1$,

(б) $a^p \equiv a \,(\mathrm{mod}\, p)$ *при любом* a.

□ Для доказательства утверждения (а) достаточно заметить, что $\varphi(p) = p - 1$. Утверждение (б) при $(a, p) = 1$ следует из (а) и следствия 1 теоремы 2, а при $(a, p) \neq 1$ оно очевидно, поскольку в этом случае $a \equiv 0 \,(\mathrm{mod}\, p)$. □

Заметим, что утверждение (а) следствия впервые доказал Ферма, оно называется *малой теоремой Ферма*. Теорема 6 была позднее доказана Эйлером и носит название *теоремы Эйлера—Ферма*. Она находит широкое применение в математике и ее приложениях и, в частности, может оказаться полезной при нахождении остатков от деления степеней числа на заданное число, при решении сравнений с неизвестными и т. д.

Так, в примере 1 для нахождения остатка от деления числа 128^{148} на 13 мы нашли предварительно сравнение $128^{12} \equiv 1 \,(\mathrm{mod}\, 13)$. С учетом теоремы Эйлера–Ферма для его нахождения достаточно заметить, что $\varphi(13) = 12$.

Подчеркнем еще, что при любом простом p поле $\mathbb{Z}/p$ — не числовое, поскольку оно не является подполем поля комплексных чисел. Больше того, оно обладает рядом специфических свойств, не имеющих места в числовых полях. Приведем примеры таких свойств.

Утверждение 7. *Для любого элемента α поля $\mathbb{Z}/p$ выполняются равенства*:

(а) $p\alpha = \underbrace{\alpha + \ldots + \alpha}_{p} = \theta$, *где θ — нуль поля $\mathbb{Z}/p$*;

(б) $\alpha^p = \alpha$.

□ Равенство (а) очевидно, равенство (б) следует из утверждения (б) предыдущего следствия. □

Замечание 1. На практике в целях упрощения записей часто вместо кольца (поля) вычетов $\mathbb{Z}/m$ используют изоморфное ему кольцо (поле) $\mathbb{Z}_m$, элементами которого являются наименьшие неотрицательные представители $0, 1, \ldots, m - 1$ классов. При этом под операциями сложения и умножения понимают обычные арифметические операции над числами с последующей заменой результата остатком от его деления на m. Кольцо $\mathbb{Z}_m$ также называют *кольцом вычетов* по модулю m.

§ 3. РЕШЕНИЕ СРАВНЕНИЙ

Рассмотрим вопрос о решении в кольце $\mathbb{Z}/m$ простейшего уравнения

$$[a]_m \cdot [x]_m = [b]_m.$$

Из (2) и определения 3 следует, что задача описания всех решений этого уравнения в кольце $\mathbb{Z}/m$ эквивалентна задаче описания всех решений сравнения

$$ax \equiv b \,(\mathrm{mod}\, m) \tag{5}$$

в целых числах относительно неизвестного x.

Рассмотрим более общее сравнение по модулю m с неизвестным x:

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \equiv 0 \,(\mathrm{mod}\, m). \tag{6}$$

Определение 5. *Решением сравнения* (6) называется любое целое число x_0, при подстановке которого вместо x сравнение (6) становится верным числовым сравнением.

Определение 6. Два сравнения (по одному или по разным модулям) называются *равносильными*, если множества их решений совпадают.

Прежде чем решать сравнение (5), сделаем два общих замечания, следующих непосредственно из теоремы 2.

Замечание 2. Если в сравнении (6) любой из коэффициентов a_i заменить сравнимым с ним по модулю числом, то получится сравнение, равносильное исходному. Следовательно, сравнение (6) всегда можно привести к сравнению с коэффициентами из множества $\overline{0, m-1}$.

Замечание 3. Если целое число x_0 является решением сравнения (6), то его решениями являются все числа класса $[x_0]_m$. Все эти решения называют одинаковыми по модулю m. Решения же, не сравнимые по модулю m, называют различными по модулю m. Следовательно, для нахождения всех решений сравнения достаточно найти по одному представителю из каждого класса чисел по модулю m, удовлетворяющих данному сравнению. Число этих представителей называют *числом решений по модулю* m.

Вернемся к вопросу о решении сравнения (5). Исчерпывающий ответ на него дают две нижеследующие теоремы.

Теорема 8. *Если* $(a, m) = 1$*, то сравнение* (5) *имеет единственное решение по модулю* m*.*

□ Так как $(a, m) = 1$, то существуют такие $u, v \in \mathbb{Z}$, что

$$mu + av = 1. \tag{7}$$

Отсюда следует, что $av \equiv 1 \pmod m$, и потому

$$a(vb) \equiv b \pmod m.$$

Значит, число vb удовлетворяет сравнению (5), и сравнение (5) разрешимо. Пусть x_1, x_2 — решения сравнения (5). Тогда $ax_1 \equiv ax_2 \pmod m$, и в силу теоремы 2(г) $x_1 \equiv x_2 \pmod m$. Следовательно, сравнение (5) имеет единственное по модулю m решение vb:

$$x \equiv vb \pmod m. \quad \square \tag{8}$$

Теорема 9. *Если* $(a, m) = d$*, то сравнение* (5) *разрешимо в том и только том случае, когда* $d \mid b$*. При выполнении последнего условия сравнение* (5) *имеет ровно* d *решений по модулю* m*.*

□ Если сравнению удовлетворяет некоторое число x_0, то по теореме 1 $m \mid (ax_0 - b)$, и потому $d \mid (ax_0 - b)$. Отсюда и из условия $d \mid a$ следует, что $d \mid b$. Пусть теперь выполнено условие $d \mid b$. Тогда по теореме 2(в) сравнение (5) равносильно сравнению

$$a/d \cdot x \equiv b/d \,(\mathrm{mod}\, m/d). \tag{9}$$

Так как $(a/d, m/d) = 1$, то по теореме 8 сравнение (9) имеет единственное по модулю m/d решение x_0. Остается выяснить, сколько различных по модулю m чисел содержится в классе чисел $[x_0]_{m_1}$, где $m_1 = m/d$.

По определению классов вычетов

$$[x_0]_{m_1} = \{x + m_1 q : \ q \in \mathbb{Z}\}.$$

Покажем, что числа

$$x_0, \ x_0 + m_1, \ x_0 + 2m_1, \ \ldots, \ x_0 + (d-1)m_1 \tag{10}$$

попарно не сравнимы по модулю m и любое другое число из $[x_0]_{m_1}$ сравнимо с одним из чисел ряда (10). Действительно, если $x_0 + im_1 \equiv x_0 + jm_1 \,(\mathrm{mod}\, m)$, где $0 \leqslant i < j \leqslant d-1$, то $m \mid (j-i)m_1$, что невозможно, поскольку $0 < (j-i)m_1 < dm_1 = m$. Пусть теперь $x_0 + m_1 q$ — любое число из класса $[x_0]_{m_1}$. Разделив q на d с остатком, получим:

$$q = dq_1 + r, \quad 0 \leqslant r \leqslant d-1.$$

Тогда

$$x_0 + m_1 q = x_0 + m_1 dq_1 + rm_1 = x_0 + rm_1 + q_1 m \equiv x_0 + rm_1 \,(\mathrm{mod}\, m).$$

Таким образом, сравнение (5) в рассматриваемом случае имеет ровно d решений по модулю m:

$$x_k \equiv x_0 + km_1 \,(\mathrm{mod}\, m), \quad k = 0, 1, \ldots, d-1. \quad \square$$

Из доказательства теоремы 9 видно, что нахождение решений сравнения (5) сводится к случаю, когда $(a, m) = 1$. В этом случае решение сравнения (5) при небольших m можно найти перебором и непосредственной проверкой представителей из классов кольца (например, чисел $0, 1, \ldots, m-1$). В общем случае можно воспользоваться методом, указанным при доказательстве теоремы 8. С этой целью необходимо найти сначала целые числа u, v, удовлетворяющие равенству (7), после чего решение находится по формуле (8). При этом для нахождения числа v можно воспользоваться алгоритмом, указанным в § 2 главы 4. Напомним, что для этого нужно найти последовательность неполных частных $q_1, q_2, \ldots, q_n$ в алгоритме Евклида, примененном к числам m, a, а затем, положив $v_0 = 1$, $v_1 = -q_1$, найти по рекуррентной формуле $v_k = v_{k-2} - v_{k-1}q_k$ последовательность чисел $v_0, \ldots, v_n$. Последнее число v_n равно искомому v.

Пример 3. Решить сравнение

$$2775x \equiv 825 \,(\mathrm{mod}\, 624). \tag{11}$$

Заменив коэффициенты этого сравнения остатками от деления их на модуль 624, получим сравнение

$$279x \equiv 201 \,(\mathrm{mod}\, 624), \tag{12}$$

равносильное сравнению (11). Применяя к числам 624, 278 алгоритм Евклида, получим их НОД 3 и систему неполных частных:

$$q_1 = 2,\ q_2 = 4,\ q_3 = 4,\ q_4 = 2.$$

Так как 201 делится на 3, то сравнение (12) разрешимо, имеет ровно 3 решения по модулю 624 и равносильно сравнению

$$93x \equiv 67 \,(\mathrm{mod}\, 208). \tag{13}$$

Для решения этого сравнения нам нужна последовательность частных в алгоритме Евклида для чисел 208, 93. Однако легко видеть, что она будет той же, что и для чисел 624, 279. Для нахождения чисел $v_1, \ldots, v_4 = v$ удобно воспользоваться таблицей из § 2 главы 4.

k	0	1	2	3	4
q_k		2	4	4	2
v_k	1	-2	9	-38	85

Теперь по формуле (8) находим решение сравнения (13) по модулю 208:

$$x \equiv 79 \,(\mathrm{mod}\, 208).$$

Отсюда, пользуясь теоремой 9, найдем все три решения сравнения (11) по модулю 624:

$$x_1 = 79, \quad x_2 = 79 + 208 = 287, \quad x_3 = 79 + 208 \cdot 2 = 495.$$

Рассмотрим еще вопрос о решении простейшей системы сравнений.

Теорема 10 (китайская теорема об остатках). *Если натуральные числа $m_1, m_2, \ldots, m_k$ попарно взаимно просты, то система сравнений*

$$\begin{aligned} x &\equiv a_1 \,(\mathrm{mod}\, m_1) \\ x &\equiv a_2 \,(\mathrm{mod}\, m_2) \\ &\ldots\ldots\ldots\ldots \\ x &\equiv a_k \,(\mathrm{mod}\, m_k) \end{aligned} \tag{14}$$

имеет единственное решение по модулю $m = m_1 m_2 \ldots m_k$ при любых $a_1, a_2, \ldots, a_k \in \mathbb{Z}$.

□ Докажем теорему индукцией по k. При $k = 1$ ее утверждение верно. Пусть $k > 1$. По предположению индукции система, составленная из первых $k-1$ сравнений

системы (14), имеет единственное решение по модулю $m' = m_1 m_2 \dots m_{k-1}$. Пусть $x \equiv a \pmod{m'}$.

Так как класс $[a]_{m'}$ совпадает с множеством всех чисел вида

$$x = a + m'y, \tag{15}$$

где y — любое целое число, то для нахождения всех решений системы (14) остается найти те значения y, при которых числа вида (15) удовлетворяют последнему сравнению системы (14). С этой целью заменим в нем x на $a + m'y$ и решим полученное сравнение

$$m'y \equiv a_k - a \pmod{m_k}$$

относительно y. Так как $(m', m_k) = 1$, то по теореме 8 оно имеет единственное решение по модулю m_k. Пусть это будет класс $[b]_{m_k}$, т. е. множество чисел $\{b + m_k t : \ t \in \mathbb{Z}\}$. Отсюда и из (15) имеем: множество решений системы (14) совпадает с множеством чисел вида $a + bm' + mt$, т. е. с классом $[a + bm']_m$. □

Заметим, что из доказательства теоремы 10 виден и алгоритм решения системы (14):

1) из первого сравнения находим $x = a_1 + m_1 y$;

2) подставив во второе сравнение $a_1 + m_1 y$ вместо x и решив полученное сравнение относительно y, получим, $y = b_1 + m_2 z$, и потому $x = a_1 + m_1 b_1 + m_1 m_2 z$;

3) подставляем найденные значения x в третье сравнение системы и находим z, и т. д.

ЗАДАЧИ

1. Пусть ρ_1, ρ_2 — отношения сравнимости целых чисел по модулям m_1, m_2 соответственно. Выясните, являются ли отношениями сравнимости по подходящим модулям отношения $\rho_1 \cap \rho_2$, $\rho_1 \cup \rho_2$, $\rho_1 \cdot \rho_2$. В каком случае имеет место включение $\rho_1 \subset \rho_2$?

2. Покажите, что все натуральные числа любого класса вычетов $[a]_m$ образуют бесконечную арифметическую прогрессию. Найдите ее первый член и разность. Сколько чисел, попарно не сравнимых по модулю m_1, содержится в $[a]_m$ для любого $m_1 \in \mathbb{Z}$?

3. Элемент a любого кольца R называется *нильпотентным*, если существует такое $n \in \mathbb{N}$, что $a^n = 0$. Опишите все нильпотентные элементы кольца $\mathbb{Z}/m$ и выпишите формулу для нахождения числа таких элементов. При каком условии все необратимые элементы кольцам $\mathbb{Z}/m$ являются нильпотентными?

4. Найдите условия, при которых все элементы группы $(\mathbb{Z}/m; +)$ являются кратными одного ее элемента $[a]_m$. Сколько таких элементов существует в группе $(\mathbb{Z}/m; +)$?

5. Найдите наименьшее натуральное число k, которое удовлетворяет равенству $k[a]_m = [0]_m$, а также число классов $[a]_m \in \mathbb{Z}/m$, удовлетворяющих указанному равенству при данном значении k.

6. Выпишите группы обратимых элементов колец $\mathbb{Z}/16$ и $\mathbb{Z}/24$. Существуют ли в них элементы, степенями которых являются все элементы соответствующих групп? Изоморфны ли эти группы?

7. Выпишите все подкольца кольца $\mathbb{Z}/18$. Какие из них изоморфны кольцам вычетов по другим модулям?

8. В кольце $\mathbb{Z}/975$ найдите элементы, обратные к элементам $[13]_{975}$, $[223]_{975}$.

9. Докажите, что любое простое число p делит число $(p-1)!+1$. (Это утверждение называют в теории чисел *теоремой Вильсона* в честь английского математика Д. Вильсона (1741–1793).)

Глава 6

КОЛЬЦА МАТРИЦ

§ 1. МАТРИЦЫ НАД КОЛЬЦОМ И ОПЕРАЦИИ НАД НИМИ

Зафиксируем произвольное кольцо R.

Определение 1. *Матрицей* размеров $m \times n$ (или $m \times n$-матрицей) над кольцом R называют прямоугольную таблицу элементов кольца R, состоящую из m строк и n столбцов.

Условимся обозначать матрицы большими латинскими буквами, а их элементы — малыми латинскими буквами с двумя индексами; первый индекс всегда будет номером строки, а второй — номером столбца, в которых расположен рассматриваемый элемент.

Например, матрица A размеров $m \times n$ с элементами a_{ij} подробно запишется в виде

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

Иногда, ради краткости, эту матрицу будем обозначать $(a_{ij})_{m\times n}$.

Две матрицы считаются равными, если они имеют одинаковые размеры и одинаковые элементы на соответствующих местах.

Множество всех матриц размеров $m \times n$ над кольцом R будем обозначать через $R_{m,n}$.

Если строку и столбец с номером i матрицы A обозначить соответственно через $\vec{A}_i$, $A_i^{\downarrow}$, то можно записать:

$$A = \begin{pmatrix} \vec{A}_1 \\ \vec{A}_2 \\ \dots \\ \vec{A}_m \end{pmatrix}, \quad A = (A_1^{\downarrow}\, A_2^{\downarrow}\, \dots\, A_n^{\downarrow}).$$

Укажем некоторые названия и обозначения для отдельных частных видов матриц.

Матрицы размеров $n \times n$ называют *квадратными* матрицами порядка n. Матрицы размеров $1 \times n$ и $n \times 1$ называют соответственно *вектор-строками* и *вектор-столбцами*. Квадратные матрицы

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{nn} \end{pmatrix}, \quad \begin{pmatrix} a_{11} & 0 & \dots & 0 \\ a_{21} & a_{22} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \tag{1}$$

называют соответственно *верхне-* и *нижнетреугольными*; прямоугольные или квадратные матрицы

$$\begin{pmatrix} a_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_m & 0 & \dots & 0 \end{pmatrix}_{m \times n}, \quad \begin{pmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_n \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix}_{m \times n}$$

называют *диагональными* и обозначают в виде $\operatorname{diag}(a_1, a_2, \dots, a_t)_{m \times n}$, где $t = \min\{m, n\}$. К диагональным матрицам относятся, в частности, *нулевая* матрица $O_{m \times n}$ (все элементы которой равны нулю) и *скалярная* матрица $\operatorname{diag}(a, a, \dots, a)_{n \times n}$. Если R — кольцо с единицей e, то в $R_{n,n}$ среди скалярных матриц содержится матрица $\operatorname{diag}(e, e, \dots, e)_{n \times n}$. Она называется *единичной* и обозначается через $E_{n \times n}$. Матрицу из $R_{m,n}$, в которой элемент на месте (i, j) равен r, а остальные элементы — нули, обозначим через $E^{(i,j)}_{m \times n}(r)$ и, в частности, через $E^{(i,j)}_{m \times n}$ при $r = e$. Индексы m, n у матриц $E_{n \times n}$, $O_{m \times n}$, $E^{(i,j)}_{m \times n}$ зачастую опускаются.

Введем операции над матрицами.

Определение 2. *Суммой матриц* $A = (a_{ij})_{m \times n}$ и $B = (b_{ij})_{m \times n}$ называется матрица $C = (c_{ij})_{m \times n}$, в которой $c_{ij} = a_{ij} + b_{ij}$ для любых $i \in \overline{1, m}$, $j \in \overline{1, n}$. Обозначение: $A + B = C$.

Подчеркнем, что сложение определено лишь для матриц одних и тех же размеров над кольцом R.

Утверждение 1. *Для любого кольца R множество матриц $R_{m,n}$ с определенной выше операцией сложения является абелевой группой.*

□ Свойства ассоциативности и коммутативности сложения матриц следуют из соответствующих свойств сложения в R. Нейтральным элементом является нулевая матрица $O_{m \times n}$, а противоположной для матрицы $A = (a_{ij})_{m \times n}$ — матрица $-A = (-a_{ij})_{m \times n}$. □

Определение 3. *Транспонированием матрицы* $A = (a_{ij})_{m \times n}$ называется преобразование матрицы A в матрицу $A^T = (a^T_{ij})_{n \times m}$, в которой $a^T_{ij} = a_{ji}$, для любых $i \in \overline{1, n}$, $j \in \overline{1, m}$. При этом матрица A^T называется *транспонированной к* A.

Геометрически, транспонирование матрицы — это преобразование симметрии относительно главной диагонали (т. е. прямой линии, проходящей через элементы $a_{11}, a_{22}, \ldots$).

Определение 4. *Произведением матрицы $A = (a_{ij})_{m\times n}$ на элемент $r \in R$* называется матрица $B = (b_{ij})_{m\times n}$, в которой $b_{ij} = a_{ij}r$ для всех $i \in \overline{1,m}$, $j \in \overline{1,n}$. Матрицу B обозначают через $A \cdot r$ и называют также результатом умножения A на r справа. Аналогично определяется умножение матриц из $R_{m,n}$ на элемент $r \in R$ слева, результат обозначается через $r \cdot A$.

Если кольцо R коммутативное, то $Ar = rA$.

Заметим, что умножение матриц из R слева или справа на фиксированный элемент $r \in R$ является унарной операцией на множестве $R_{m,n}$.

Из определений 2–4 и свойств операций в кольце R легко следует

Утверждение 2. *Для любых элементов r_1, r_2 кольца R и матриц $A, B \in R_{m,n}$ выполняются равенства*:

$$
\begin{aligned}
&(r_1r_2)A = r_1(r_2A), && (r_1A)r_2 = r_1(Ar_2),\\
&A(r_1r_2) = (Ar_1)r_2, && O \cdot r_1 = r_1 \cdot O = 0 \cdot A = A \cdot 0 = O,\\
&(r_1 + r_2)A = r_1A + r_2A, && A(r_1 + r_2) = Ar_1 + Ar_2,\\
&r_1(A + B) = r_1A + r_1B, && (A + B)r_1 = Ar_1 + Br_1,\\
&(A + B)^T = A^T + B^T, && (r_1A)^T = r_1A^T.
\end{aligned}
$$

Проверьте эти равенства в качестве упражнения.

Используя операции сложения матриц и умножения матриц на элементы кольца R слева и справа, из заданных матриц $A_1, \ldots, A_k \in R_{m,n}$ можно получать матрицы вида

$$r_1A_1 + r_2A_2 + \ldots + r_kA_k, \quad A_1r_1 + A_2r_2 + \ldots + A_kr_k, \quad r_i \in R.$$

Такие матрицы называют *линейными комбинациями матриц* $A_1, \ldots, A_k$ над R (соответственно левыми и правыми).

Определение 5. *Произведением матрицы $A = (a_{ij})_{m\times n}$ на матрицу $B = (b_{ij})_{n\times k}$* называется матрица $C = (c_{ij})_{m\times k}$, в которой

$$c_{ij} = \sum_{s=1}^{n} a_{is}b_{sj}, \quad i \in \overline{1,m},\ j \in \overline{1,k}.$$

Обозначение: $A \cdot B = C$ или $AB = C$.

Таким образом, для нахождения элемента c_{ij} нужно все элементы i-й строки матрицы A умножить на соответствующие элементы j-го столбца матрицы B и результаты сложить, или короче, i-ю строку матрицы A умножить на j-й столбец матрицы B.

Если воспользоваться записями матриц через их строки и столбцы, то правило умножения матриц можно записать следующим образом:

$$AB = \begin{pmatrix} \vec{A}_1 \\ \vec{A}_2 \\ \dots \\ \vec{A}_m \end{pmatrix} (B_1^{\downarrow}\, B_2^{\downarrow}\, \dots\, B_k^{\downarrow}) = \begin{pmatrix} \vec{A}_1 B_1^{\downarrow} & \vec{A}_1 B_2^{\downarrow} & \dots & \vec{A}_1 B_k^{\downarrow} \\ \vec{A}_2 B_1^{\downarrow} & \vec{A}_2 B_2^{\downarrow} & \dots & \vec{A}_2 B_k^{\downarrow} \\ \dots & \dots & \dots & \dots \\ \vec{A}_m B_1^{\downarrow} & \vec{A}_m B_2^{\downarrow} & \dots & \vec{A}_m B_k^{\downarrow} \end{pmatrix}.$$

Из определения 5 видно, что умножать матрицу A на матрицу B можно лишь в том случае, когда число столбцов матрицы A равно числу строк матрицы B. Всюду далее в тех случаях, когда говорится о произведении матриц или записывается произведение матриц, указанное условие на размеры сомножителей предполагается выполненным.

Замечание 1. На первый взгляд, правило умножения матриц выглядит искусственным. В действительности к использованию именно такого правила умножения приводят многочисленные применения матриц в теории и на практике. О естественности определения 5 свидетельствует также

Теорема 3. *Для любых матриц A, B, C подходящих размеров над кольцом R выполняются равенства*:

(а) $(AB)C = A(BC)$,

(б) $A(B + C) = AB + AC$,

(в) $(A + B)C = AC + BC$.

Если кольцо R коммутативно, то выполняется также равенство

(г) $(AB)^T = B^T A^T$.

□ Доказываются свойства (а)–(г) непосредственной проверкой. А именно, находят и сравнивают элементы из i-й строки и j-го столбца матриц в левой и правой частях доказываемого равенства. Докажем для примера свойство (а). С этой целью введем обозначения:

$$A = (a_{ij})_{m\times n},\ B = (b_{ij})_{n\times k},\ C = (c_{ij})_{k\times l},\ AB = X = (x_{ij})_{m\times k},$$
$$XC = Y = (y_{ij})_{m\times l},\quad BC = U = (u_{ij})_{n\times l},\quad AU = V = (v_{ij})_{m\times l}.$$

Для доказательства равенства (а) достаточно доказать, что $y_{ij} = v_{ij}$ для любых $i \in \overline{1,m}$, $j \in \overline{1,l}$. Пользуясь определением 5 и свойствами операций в кольце R, находим:

$$y_{ij} = \sum_{s=1}^{k} x_{is}c_{sj} = \sum_{s=1}^{k}\left(\sum_{r=1}^{n} a_{ir}b_{rs}\right)c_{sj} = \sum_{s=1}^{k}\sum_{r=1}^{n}(a_{ir}b_{rs})c_{sj} =$$
$$= \sum_{r=1}^{n}\sum_{s=1}^{k} a_{ir}(b_{rs}c_{sj}) = \sum_{r=1}^{n} a_{ir}\left(\sum_{s=1}^{k} b_{rs}c_{sj}\right) = \sum_{r=1}^{k} a_{ir}u_{rj} = v_{ij}.$$

Свойства (б)–(г) докажите в качестве упражнения. □

Заметим, что произведение двух матриц из $R_{n,n}$ всегда определено и является матрицей из $R_{n,n}$. Следовательно, умножение матриц является бинарной операцией на $R_{n,n}$ при любом $n \in \mathbb{N}$. Из утверждения 1 и теоремы 3 следует

Теорема 4. *Множество $R_{n,n}$ квадратных матриц порядка n над кольцом R является кольцом относительно операций сложения и умножения матриц.*

В дальнейшем мультипликативная группа $(R_{n,n})^*$ кольца $R_{n,n}$ будет обозначаться через $R^*_{n,n}$.

Выясним, в каких случаях кольцо $(R_{n,n}; +, \cdot)$ обладает некоторыми дополнительными свойствами.

Теорема 5. (а) *Кольцо $(R_{n,n}; +, \cdot)$ коммутативно в том и только том случае, когда либо* 1) *$n = 1$ и R коммутативно, либо* 2) *$n > 1$ и R — кольцо с нулевым умножением.*

(б) *Кольцо $(R_{n,n}; +, \cdot)$ является кольцом с единицей в том и только в том случае, когда единица есть в кольце R.*

□ (а) Коммутативность кольца $R_{n,n}$ в случаях 1) и 2) очевидна. Докажем обратное утверждение. Пусть кольцо $R_{n,n}$ коммутативно. При $n = 1$ это равносильно коммутативности кольца R. Рассмотрим случай $n > 1$. Вычисляя и приравнивая произведения матриц

$$E^{(1,1)}_{n\times n}(a)\, E^{(1,2)}_{n\times n}(b) \quad \text{и} \quad E^{(1,2)}_{n\times n}(b)\, E^{(1,1)}_{n\times n}(a),$$

получим, что $ab = 0$ для любых $a, b \in R$. Следовательно, R — кольцо с нулевым умножением.

(б) Пусть кольцо $R_{n,n}$ имеет единицу — матрицу $\varepsilon = (e_{ij})_{n\times n}$. Тогда из равенства $E^{(1,1)}_{n\times n}(a)\varepsilon = \varepsilon E^{(1,1)}_{n\times n}(a)$ получим: $ae_{11} = e_{11}a = a$ для любого $a \in R$. Следовательно, e_{11} — единица кольца R. Обратно, пусть кольцо R имеет единицу e. Тогда в $R_{n,n}$ есть единичная матрица $E_{n\times n} = E$. Непосредственной проверкой нетрудно убедиться в том, что для любой матрицы A из $R_{n,n}$ выполняются равенства

$$AE = EA = A.$$

Следовательно, E есть единица кольца $R_{n,n}$. □

Легко проверить, что равенства

$$EA = A, \quad BE = B$$

выполняются вообще для любых матриц $A \in R_{n,k}$ и $B \in R_{m,n}$.

Замечание 2. Кольцо $R_{n,n}$ является полем лишь в том частном случае, когда $n = 1$ и R есть поле. В этом случае $R_{n,n}$, по существу, совпадает с R. Тот факт, что при $n > 1$ кольцо $R_{n,n}$ не является полем, следует непосредственно из теоремы 5. Однако в этом случае можно сказать больше. А именно, при $n > 1$ кольцо всегда имеет делители нуля: например, матрицы

$$E^{(1,2)}_{n\times n}(a),\ E^{(1,1)}_{n\times n}(b) \ \text{ при } a \neq 0,\ b \neq 0.$$

Найдем условия разрешимости простейших матричных уравнений $AX = C$ и $XB = C$, в которых A, B, C — известные матрицы над кольцом R соответственно размеров $m \times n$, $n \times k$, $m \times k$, а X — неизвестная матрица подходящих размеров. Для этого нам понадобится вспомогательное

Утверждение 6. *Для любых матриц $A = (a_{ij})_{m\times n}$, $B = (b_{ij})_{n\times k}$, $C = (c_{ij})_{m\times k}$ равенство $AB = C$ равносильно любой из следующих систем соотношений*:

$$\vec{C}_i = a_{i1}\vec{B}_1 + a_{i2}\vec{B}_2 + \ldots + a_{in}\vec{B}_n, \quad i \in \overline{1,m}; \tag{2}$$

$$C_j^{\downarrow} = A_1^{\downarrow}b_{1j} + A_2^{\downarrow}b_{2j} + \ldots + A_n^{\downarrow}b_{nj}, \quad j \in \overline{1,k}. \tag{3}$$

Доказывается утверждение 6 непосредственной проверкой. Проделайте ее в качестве упражнения.

Непосредственно из утверждения 6 следует

Теорема 7. *Для матриц над произвольным кольцом R уравнение $AX = C$ ($XB = C$) разрешимо в том и только том случае, когда столбцы (строки) матрицы C являются правыми (левыми) линейными комбинациями столбцов (строк) матрицы A (матрицы B).*

□ Уравнение $AX = C$ разрешимо тогда и только тогда, когда существует некоторая матрица $B = (b_{ij})_{n\times k}$, удовлетворяющая равенству $AB = C$. Последнее же равносильно существованию элементов $b_{ij} \in R$, удовлетворяющих системе соотношений (3). Для уравнения $XB = C$ рассуждения аналогичны, при этом вместо (3) используется (2). □

Замечание 3. Указанный в теореме 7 критерий разрешимости матричных уравнений носит больше теоретический характер и в общем случае не дает метода решения уравнений. Ниже такой метод будет указан для матриц над кольцом $\mathbb{Z}$ и для матриц над полями.

§ 2. ОПРЕДЕЛИТЕЛИ МАТРИЦ НАД КОММУТАТИВНЫМ КОЛЬЦОМ С ЕДИНИЦЕЙ

Зафиксируем произвольное *коммутативное* кольцо R с единицей e и будем рассматривать квадратные матрицы порядка n над кольцом R. Как было показано выше, кольцо $R_{n,n}$ таких матриц является кольцом с единицей E, и потому естественно ставить вопрос об описании обратимых элементов кольца $R_{n,n}$, т. е. обратимых $(n \times n)$-матриц над R. Для его решения введем понятие определителя квадратной матрицы порядка n, или, короче, определителя n-го порядка. С этой целью проанализируем сначала известное из аналитической геометрии понятие определителя матрицы 3-го порядка над полем действительных чисел:

$$\Delta = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} -$$

$$-a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}.$$

Рассматривая этот определитель, замечаем следующие факты.

1. Определитель Δ есть алгебраическая сумма 6 произведений вида

$$a_{1i_1}a_{2i_2}a_{3i_3}. \tag{4}$$

2. В произведениях (4) наборы вторых индексов (i_1, i_2, i_3) пробегают все 3! перестановок из чисел 1, 2, 3.

3. Произведение (4) берется со знаком «+», если (i_1, i_2, i_3) — четная перестановка, и со знаком «−» в противном случае.

Отмеченные факты и положим в основу определения определителя n-го порядка.

Определение 6. *Определителем квадратной матрицы* $A=(a_{ij})_{n\times n}$ порядка n над кольцом R называется элемент кольца R, равный алгебраической сумме $n!$ произведений вида

$$a_{1i_1}a_{2i_2}\dots a_{ni_n}, \tag{5}$$

соответствующих различным перестановкам $(i_1, i_2, \dots, i_n) \in P(\overline{1,n})$, в которую слагаемое (5) входит со знаком «+», если $(i_1, i_2, \dots, i_n)$ — четная перестановка, и со знаком «−» в противном случае.

Определитель матрицы A далее будем обозначать через $|A|$ или, подробнее,

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}.$$

Пользуясь введенной в § 3 главы 2 функцией четности δ на множестве перестановок, можно записать:

$$|A| = \sum_{(i_1,i_2,\dots,i_n)} \delta(i_1, i_2, \dots, i_n)\, a_{1i_1}a_{2i_2}\dots a_{ni_n}, \tag{6}$$

где суммирование ведется по всем перестановкам

$$(i_1, i_2, \dots, i_n) \in P(\overline{1,n}).$$

Правую часть равенства (6) называют *каноническим представлением определителя* $|A|$.

Заметим, что определением 6 охватывается и понятие определителя 2-го порядка:

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}.$$

Находить определитель матрицы можно непосредственно по формуле (6), однако такой способ сопряжен с большими трудностями. Так, уже для вычисления определителя 5-го порядка нам придется вычислить сначала $5! = 120$ произведений вида $a_{1i_1}a_{2i_2}a_{3i_3}a_{4i_4}a_{5i_5}$, а затем сложить их с нужными знаками. Однако в некоторых частных случаях определитель матрицы может быть легко вычислен непосредственно по определению 6.

Пример 1. Для треугольных матриц (1) произведение (5) может быть отличным от нуля лишь при $i_1 = 1$, $i_2 = 2$, ..., $i_n = n$ (проверьте). Отсюда следует, что определитель любой такой матрицы равен произведению элементов главной диагонали.

На практике часто вычисление определителя любой матрицы сводят к вычислению определителя треугольной матрицы с помощью свойств определителей.

Приведем ряд свойств определителей матриц над коммутативным кольцом с единицей.

Свойство 1. *Если матрица* $B = (b_{ij})_{n\times n}$ *получена из* $A = (a_{ij})_{n\times n}$ *умножением какой-либо строки на элемент* r *кольца* R, *то* $|B| = r \cdot |A|$.

Иначе это свойство формулируют так: *общий множитель всех элементов какой-либо строки матрицы можно вынести за знак определителя*.

□ Пусть B получена из A умножением s-й строки на r. Тогда, пользуясь определением 6 и свойствами коммутативности умножения и дистрибутивности умножения относительно сложения в кольце R, получим:

$$\begin{aligned}|B| &= \sum_{(i_1,\dots,i_n)} \delta(i_1,\dots,i_s,\dots,i_n)\, b_{1i_1}\dots b_{si_s}\dots b_{ni_n} = \\ &= \sum_{(i_1,\dots,i_n)} \delta(i_1,\dots,i_s,\dots,i_n)\, a_{1i_1}\dots ra_{si_s}\dots a_{ni_n} = \\ &= r\sum_{(i_1,\dots,i_n)} \delta(i_1,\dots,i_s,\dots,i_n)\, a_{1i_1}\dots a_{si_s}\dots a_{ni_n} = r\,|A|. \quad \square\end{aligned}$$

Свойство 2. *Если* s*-я строка* $\vec{A}_s$ *матрицы* A *представляется в виде суммы двух векторов-строк* $\vec{A}'_s + \vec{A}''_s$, *то определитель матрицы* A *равен сумме определителей матриц* A' *и* A'', *полученных из* A *заменой* s*-й строки соответственно векторами-строками* $\vec{A}'_s$ *и* $\vec{A}''_s$:

$$|A| = |A'| + |A''|.$$

□ Обозначим

$$\vec{A}'_s = (a'_{s1}, a'_{s2}, \dots, a'_{sn}), \quad \vec{A}''_s = (a''_{s1}, a''_{s2}, \dots, a''_{sn}).$$

Как и при доказательстве свойства 1, получим:

$$\begin{aligned}|A| &= \sum_{(i_1,\dots,i_n)} \delta(i_1,\dots,i_s,\dots,i_n)\, a_{1i_1}\dots a_{si_s}\dots a_{ni_n} = \\ &= \sum_{(i_1,\dots,i_n)} \delta(i_1,\dots,i_s,\dots,i_n)\, a_{1i_1}\dots (a'_{si_s} + a''_{si_s})\dots a_{ni_n} = \\ &= \sum_{(i_1,\dots,i_n)} \delta(i_1,\dots,i_s,\dots,i_n)\, a_{1i_1}\dots a'_{si_s}\dots a_{ni_n} + \\ &\quad + \sum_{(i_1,\dots,i_n)} \delta(i_1,\dots,i_s,\dots,i_n)\, a_{1i_1}\dots a''_{si_s}\dots a_{ni_n} = |A'| + |A''|. \quad \square\end{aligned}$$

Заметим, что свойство 2 очевидным образом обобщается на случай, когда s-я строка матрицы A представляется в виде суммы k векторов-строк при любом $k \in \mathbb{N}$. В этом случае определитель $|A|$ разложится в сумму k определителей.

Свойство 3. *Определитель матрицы с двумя одинаковыми строками равен нулю.*

□ Пусть в матрице $A = (a_{ij})_{n\times n}$ равны k-я и l-я строки, т. е. $a_{kj} = a_{lj}$, при всех $j \in \overline{1,n}$, и пусть, для определенности $k < l$. Представим определитель $|A|$ в виде суммы двух слагаемых:

$$|A| = \Delta_1 + \Delta_2,$$

где

$$\Delta_1 = \sum_{\substack{(i_1,\dots,i_n)\\ i_k<i_l}} \delta(i_1,\dots,i_n)\, a_{1i_1}\dots a_{ni_n},$$

$$\Delta_2 = \sum_{\substack{(i_1,\dots,i_n)\\ i_k>i_l}} \delta(i_1,\dots,i_n)\, a_{1i_1}\dots a_{ni_n}.$$

При доказательстве следствия теоремы 4 главы 2 было показано, что транспозиция элементов, расположенных на k-м и l-м местах в перестановках из $P(\overline{1,n})$, задает биективное отображение σ множества $P(\overline{1,n})$ на себя. По этому отображению можно построить взаимно однозначное соответствие между слагаемыми сумм Δ_1, Δ_2, сопоставив слагаемому

$$\delta(i_1,\dots,i_k,\dots,i_l,\dots,i_n)\, a_{1i_1}\dots a_{ki_k}\dots a_{li_l}\dots a_{ni_n}$$

из Δ_1 следующее слагаемое из Δ_2:

$$\delta(i_1,\dots,i_l,\dots,i_k,\dots,i_n)\, a_{1i_1}\dots a_{ki_l}\dots a_{li_k}\dots a_{ni_n}.$$

Так как по условию $a_{ki_k} = a_{li_k}$, $a_{li_l} = a_{ki_l}$ и кольцо R коммутативно, то в силу теоремы 4 главы 2 соответствующие слагаемые отличаются лишь знаком. Следовательно, $\Delta_2 = -\Delta_1$, и потому

$$|A| = \Delta_1 + \Delta_2 = 0. \quad \square$$

Свойство 4. *Если к какой-либо строке матрицы A прибавить другую ее строку, умноженную на любой элемент из R, то определитель полученной матрицы будет равен определителю матрицы A.*

□ Пусть матрица B получена из A прибавлением к j-й строке ее i-й строки, умноженной на r, и пусть, например, $i < j$. Тогда

$$B = \begin{pmatrix} \vec{A}_1 \\ \dots \\ \vec{A}_i \\ \dots \\ \vec{A}_j + r\vec{A}_i \\ \dots \\ \vec{A}_n \end{pmatrix}.$$

Применяя последовательно свойства 2, 1, 3, получим

$$|B| = \begin{vmatrix} \dots \\ \vec{A}_i \\ \dots \\ \vec{A}_j \\ \dots \end{vmatrix} + \begin{vmatrix} \dots \\ \vec{A}_i \\ \dots \\ r\vec{A}_i \\ \dots \end{vmatrix} = |A| + r \begin{vmatrix} \dots \\ \vec{A}_i \\ \dots \\ \vec{A}_i \\ \dots \end{vmatrix} = |A| + r \cdot 0 = |A|. \quad \square$$

Свойство 5. *Если в матрице A поменять местами две строки, то определитель полученной матрицы B будет лишь знаком отличаться от определителя матрицы A, т. е. $|B| = -|A|$.*

$\square$ Осуществим перестановку i-й и j-й строк матрицы A, пользуясь преобразованиями матриц, указанными в свойствах 1 и 4. На основании этих свойств получим:

$$|A| = \begin{vmatrix} \dots \\ \vec{A}_i \\ \dots \\ \vec{A}_j \\ \dots \end{vmatrix} = \begin{vmatrix} \dots \\ \vec{A}_i \\ \dots \\ \vec{A}_j + \vec{A}_i \\ \dots \end{vmatrix} = \begin{vmatrix} \dots \\ \vec{A}_i + (-\vec{A}_j - \vec{A}_i) \\ \dots \\ \vec{A}_j + \vec{A}_i \\ \dots \end{vmatrix} = \begin{vmatrix} \dots \\ -\vec{A}_j \\ \dots \\ \vec{A}_j + \vec{A}_i \\ \dots \end{vmatrix} =$$

$$= \begin{vmatrix} \dots \\ -\vec{A}_j \\ \dots \\ (\vec{A}_j + \vec{A}_i) + (-\vec{A}_j) \\ \dots \end{vmatrix} = \begin{vmatrix} \dots \\ -\vec{A}_j \\ \dots \\ \vec{A}_i \\ \dots \end{vmatrix} = - \begin{vmatrix} \dots \\ \vec{A}_j \\ \dots \\ \vec{A}_i \\ \dots \end{vmatrix} = -|B|. \quad \square$$

Свойство 5 допускает обобщение.

Свойство 6. *Если $A = (a_{ij})_{n\times n}$, $(\alpha_1, \dots, \alpha_n)$ — произвольная перестановка чисел $1, 2, \dots, n$ и*

$$A' = \begin{pmatrix} a_{\alpha_1 1} & \dots & a_{\alpha_1 n} \\ \dots & \dots & \dots \\ a_{\alpha_n 1} & \dots & a_{\alpha_n n} \end{pmatrix}, \tag{7}$$

то $|A'| = \delta(\alpha_1, \dots, \alpha_n)\,|A|$.

$\square$ Если перестановка $(\alpha_1, \dots, \alpha_n)$ имеет t инверсий, то по утверждению 7 главы 2 ее с помощью t транспозиций можно привести к виду $(1, \dots, n)$. Для матрицы A' этот факт означает, что ее с помощью t перестановок двух строк можно привести к матрице A. Теперь равенство (7) следует непосредственно из свойства 5. $\square$

Свойство 7. *Если какая-либо строка матрицы является линейной комбинацией других ее строк, то определитель матрицы равен нулю.*

$\square$ Пусть j-я строка матрицы A является линейной комбинацией ее строк с номерами $i_1, \dots, i_k$:

$$\vec{A}_j = \vec{A}_{i_1} c_1 + \dots + \vec{A}_{i_k} c_k, \quad j \notin \{i_1, \dots, i_k\}.$$

Тогда, прибавляя к j-й строке матрицы A ее строки $A_{i_1}, \dots, A_{i_k}$, умноженные соответственно на элементы $-c_1, \dots, -c_k$, получим матрицу B с нулевой j-й строкой. Ясно, что $|B| = 0$. С другой стороны, по свойству 4 $|B| = |A|$. Значит, $|A| = 0$. $\square$

Свойство 8. *Определитель матрицы, транспонированной к A, равен определителю матрицы A, т. е.* $|A^T| = |A|$.

$\square$ Обозначим $A = (a_{ij})_{n\times n}$ и $A^T = (b_{ij})_{n\times n}$. Тогда $b_{ij} = a_{ji}$ для $i, j \in \overline{1,n}$, и справедливо равенство

$$\begin{aligned} |A^T| &= \sum_{(i_1,\dots,i_n)} \delta(i_1,\dots,i_n)\, b_{1i_1}\dots b_{ni_n} = \\ &= \sum_{(i_1,\dots,i_n)} \delta(i_1,\dots,i_n)\, a_{i_1 1}\dots a_{i_n n}. \end{aligned} \tag{8}$$

В каждом произведении $a_{i_1 1}\dots a_{i_n n}$ переставим сомножители так, чтобы первые индексы расположились в порядке возрастания. Тогда их вторые индексы составят некоторую перестановку $(j_1,\dots,j_n) \in P(\overline{1,n})$, и ввиду коммутативности R получим равенство

$$a_{i_1 1}\dots a_{i_n n} = a_{1 j_1}\dots a_{n j_n}.$$

Кроме того, из утверждения 5 главы 2 следует, что $\delta(i_1,\dots,i_n) = \delta(j_1,\dots,j_n)$, поскольку таблица $\begin{pmatrix} j_1 & \dots & j_n \\ 1 & \dots & n \end{pmatrix}$ получена из таблицы $\begin{pmatrix} 1 & \dots & n \\ i_1 & \dots & i_n \end{pmatrix}$ с помощью некоторой перестановки столбцов. В итоге из (8) получим:

$$|A^T| = \sum_{(i_1,\dots,i_n)} \delta(j_1,\dots,j_n)\, a_{1 j_1}\dots a_{n j_n}. \tag{9}$$

Заметим, что отображение $\sigma\colon P(\overline{1,n}) \to P(\overline{1,n})$, сопоставляющее перестановке $s = (i_1,\dots,i_n)$ перестановку $\sigma(s) = (j_1,\dots,j_n)$ указанным выше образом, инъективно, а потому и биективно (см. утверждение 5 главы 1). Действительно, из определения отображения σ видно, что в перестановке $\sigma(s)$ число j_k есть номер места, на котором находится число k в перестановке s. Значит, если $s, s' \in P(\overline{1,n})$ и $s \neq s'$, то найдется такое число $k \in \overline{1,n}$, которое в s и s' расположено на разных местах, а тогда в перестановках $\sigma(s)$ и $\sigma(s')$ будут находиться различные элементы на месте с номером k, и $\sigma(s) \neq \sigma(s')$. Следовательно, отображение σ биективно, и потому в (9) суммирование по $s = (i_1,\dots,i_n)$ можно заменить суммированием по $\sigma(s) = (j_1,\dots,j_n)$. Произведя эту замену, получим:

$$|A^T| = \sum_{(j_1,\dots,j_n)} \delta(j_1,\dots,j_n)\, a_{1 j_1}\dots a_{n j_n} = |A|. \quad \square$$

Из свойства 8 следует, что все свойства определителей матриц, доказанные для строк, имеют место и для столбцов. В дальнейшем этим фактом будем пользоваться без оговорок.

Приведем пример на использование свойств определителей.

Пример 2. Вычислить определитель матрицы

$$A = \begin{pmatrix} a & b & b & \dots & b \\ b & a & b & \dots & b \\ b & b & a & \dots & b \\ \dots & \dots & \dots & \dots & \dots \\ b & b & b & \dots & a \end{pmatrix}_{n\times n}.$$

Прибавив к первому столбцу матрицы A все остальные ее столбцы и вынеся из первого столбца полученной матрицы общий множитель $a + b(n-1)$, будем иметь (в силу свойств 4 и 1):

$$|A| = (a + b(n-1))\,|B|, \quad B = \begin{pmatrix} 1 & b & b & \dots & b \\ 1 & a & b & \dots & b \\ 1 & b & a & \dots & b \\ \dots & \dots & \dots & \dots & \dots \\ 1 & b & b & \dots & a \end{pmatrix}.$$

Вычитая первую строку матрицы B из всех остальных ее строк, получим верхнетреугольную матрицу со следующей главной диагональю: $(1, a-b, a-b, \dots, a-b)$. Из свойства 4 с учетом примера 1 имеем: $|B| = (a-b)^{n-1}$, и потому

$$|A| = (a + b(n-1))(a-b)^{n-1}.$$

В заключение данного параграфа рассмотрим вопрос о вычислении определителя произведения квадратных матриц.

Теорема 8. *Определитель произведения двух квадратных матриц равен произведению определителей этих матриц*:

$$|AB| = |A| \cdot |B|.$$

□ Пусть $A = (a_{ij})_{n\times n}$, $B = (b_{ij})_{n\times n}$, $C = AB$. Из соотношений (2) имеем:

$$C = \begin{pmatrix} a_{11}\vec{B}_1 + a_{12}\vec{B}_2 + \dots + a_{1n}\vec{B}_n \\ a_{21}\vec{B}_1 + a_{22}\vec{B}_2 + \dots + a_{2n}\vec{B}_n \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ a_{n1}\vec{B}_1 + a_{n2}\vec{B}_2 + \dots + a_{nn}\vec{B}_n \end{pmatrix}.$$

Так как первая строка матрицы C есть сумма n векторов-строк, то, пользуясь обобщением свойства 2 определителей, разложим определитель $|C|$ в сумму n определителей для матриц вида

$$\begin{pmatrix} a_{1i_1}\vec{B}_{i_1} \\ a_{21}\vec{B}_1 + a_{22}\vec{B}_2 + \dots + a_{2n}\vec{B}_n \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ a_{n1}\vec{B}_1 + a_{n2}\vec{B}_2 + \dots + a_{nn}\vec{B}_n \end{pmatrix}, \quad i_1 \in \overline{1,n}.$$

Определитель каждой из этих матриц снова можно разложить в сумму n определителей по 2-й строке, и т. д. В итоге определитель $|C|$ будет представлен в виде суммы n^n определителей:

$$|C| = \sum_{i_1,\dots,i_n \in \overline{1,n}} \begin{vmatrix} a_{1i_1}\vec{B}_{i_1} \\ a_{2i_2}\vec{B}_{i_2} \\ \dots\dots \\ a_{ni_n}\vec{B}_{i_n} \end{vmatrix} = \sum_{i_1,\dots,i_n \in \overline{1,n}} a_{1i_1}a_{2i_2}\dots a_{ni_n} \begin{vmatrix} \vec{B}_{i_1} \\ \vec{B}_{i_2} \\ \dots \\ \vec{B}_{i_n} \end{vmatrix}.$$

Здесь каждый индекс i_s, $s \in \overline{1,n}$, независимо от остальных индексов пробегает все множество чисел $\overline{1,n}$. Заметим, что в последней сумме многие слагаемые равны нулю. А именно, всякое слагаемое, соответствующее набору индексов $i_1, i_2, \dots, i_n$, содержащему хотя бы два одинаковых элемента, равно нулю по свойству 3 определителей. Поэтому в последней сумме можно оставить лишь те слагаемые, которые соответствуют наборам различных индексов, т. е. перестановкам из $P(\overline{1,n})$:

$$|C| = \sum_{(i_1,\dots,i_n)} a_{1i_1}\dots a_{ni_n} \begin{vmatrix} \vec{B}_{i_1} \\ \vec{B}_{i_2} \\ \dots \\ \vec{B}_{i_n} \end{vmatrix}.$$

Отсюда по свойству 6 имеем:

$$|C| = \sum_{(i_1,\dots,i_n)} a_{1i_1}\dots a_{ni_n}\delta(i_1,\dots,i_n)\,|B| =$$
$$= \left(\sum_{(i_1,\dots,i_n)} \delta(i_1,\dots,i_n)a_{1i_1}\dots a_{ni_n}\right)|B| = |A|\cdot|B|. \quad \square$$

Замечание 4. Все изложенные в этом параграфе свойства определителей (включая теорему 8) справедливы и для матриц над коммутативным кольцом R без единицы. Выясните, в каких из приведенных здесь доказательств появятся дополнительные трудности, и постарайтесь преодолеть их.

§ 3. ПОДМАТРИЦЫ МАТРИЦ. МИНОРЫ И ИХ АЛГЕБРАИЧЕСКИЕ ДОПОЛНЕНИЯ

В данном параграфе будет показано, как вычисление определителя n-го порядка можно свести к вычислению определителей меньших порядков. При этом матрицы будут рассматриваться над произвольным коммутативным кольцом R.

Определение 7. *Подматрицей* матрицы A называется любая матрица, полученная из A удалением некоторых ее строк и столбцов. Подматрицу, полученную из A удалением всех строк, кроме строк с номерами $i_1 < \dots < i_k$, и всех столбцов, кроме столбцов с номерами $j_1 < \dots < j_l$, будем обозначать через

$$A\begin{pmatrix} i_1,\dots,i_k \\ j_1,\dots,j_l \end{pmatrix}.$$

Определение 8. Определитель квадратной подматрицы $A\binom{i_1,\ldots,i_k}{j_1,\ldots,j_k}$ матрицы A называется *минором k-го порядка* матрицы A и обозначается

$$M_A\begin{pmatrix} i_1,\ldots,i_k \\ j_1,\ldots,j_k \end{pmatrix}. \tag{10}$$

Про этот минор говорят также, что он находится в строках с номерами $i_1,\ldots,i_k$ и в столбцах с номерами $j_1,\ldots,j_k$ матрицы A.

Из определения 8 видно, что для $A=(a_{ij})_{m\times n}$

$$M_A\begin{pmatrix} i_1,\ldots,i_k \\ j_1,\ldots,j_k \end{pmatrix} = \begin{vmatrix} a_{i_1j_1} & a_{i_1j_2} & \ldots & a_{i_1j_k} \\ a_{i_2j_1} & a_{i_2j_2} & \ldots & a_{i_2j_k} \\ \ldots & \ldots & \ldots & \ldots \\ a_{i_kj_1} & a_{i_kj_2} & \ldots & a_{i_kj_k} \end{vmatrix}.$$

Укажем каноническое представление этого минора.

Утверждение 9. *Пусть $A=(a_{ij})_{m\times n}$, $1\leqslant i_1<\ldots<i_k\leqslant n$ и $1\leqslant j_1<\ldots<j_k\leqslant n$. Тогда*

$$M_A\begin{pmatrix} i_1,\ldots,i_k \\ j_1,\ldots,j_k \end{pmatrix} = \sum_{(t_1,\ldots,t_k)\in P(j_1,\ldots,j_k)} \delta(t_1,\ldots,t_k)\, a_{i_1t_1}\ldots a_{i_kt_k}. \tag{11}$$

□ Введя обозначение $a_{i_rj_s}=b_{rs}$ для $r,s\in\overline{1,k}$ и воспользовавшись формулой (6), получим:

$$\begin{aligned} M_A\begin{pmatrix} i_1,\ldots,i_k \\ j_1,\ldots,j_k \end{pmatrix} &= \sum_{(s_1,\ldots,s_k)\in P(\overline{1,k})} \delta(s_1,\ldots,s_k)\, b_{1s_1}\ldots b_{ks_k} = \\ &= \sum_{(s_1,\ldots,s_k)\in P(\overline{1,k})} \delta(s_1,\ldots,s_k)\, a_{i_1j_{s_1}}\ldots a_{i_kj_{s_k}}. \end{aligned}$$

Так как $j_1<\ldots<j_k$, то неравенство $j_a<j_b$ равносильно неравенству $a<b$. Следовательно, в перестановках $(s_1,\ldots,s_k)$ и $(j_{s_1},\ldots,j_{s_k})$ содержится одно и то же число инверсий, и потому

$$\delta(s_1,\ldots,s_k)=\delta(j_{s_1},\ldots,j_{s_k}).$$

Кроме того, соответствие $(s_1,\ldots,s_k)\to(j_{s_1},\ldots,j_{s_k})$ задает биективное отображение $\varphi\colon P(\overline{1,k})\to P(j_1,\ldots,j_k)$. Следовательно, в последней сумме вместо суммирования по всем перестановкам из $P(\overline{1,k})$ можно суммировать по всем перестановкам множества $\{j_1,\ldots,j_k\}$, и потому

$$M_A\begin{pmatrix} i_1,\ldots,i_k \\ j_1,\ldots,j_k \end{pmatrix} = \sum_{(j_{s_1},\ldots,j_{s_k})\in P(j_1,\ldots,j_k)} \delta(j_{s_1},\ldots,j_{s_k})\, a_{i_1j_{s_1}}\ldots a_{i_kj_{s_k}}.$$

Теперь осталось заметить, что правая часть последнего равенства отличается от правой части равенства (11) лишь обозначениями индексов суммирования. □

Определение 9. *Дополнительным минором* для минора (10) квадратной матрицы A называется определитель подматрицы, полученной из A удалением строк с номерами $i_1, \ldots, i_k$ и столбцов с номерами $j_1, \ldots, j_k$. Этот минор будем обозначать

$$CM_A\begin{pmatrix} i_1, \ldots, i_k \\ j_1, \ldots, j_k \end{pmatrix}.$$

Определение 10. *Алгебраическим дополнением для минора* (10) квадратной матрицы A называется его дополнительный минор, умноженный на $(-1)^{i_1+\ldots+i_k+j_1+\ldots+j_k}$. Обозначение:

$$\overline{CM}_A\begin{pmatrix} i_1, \ldots, i_k \\ j_1, \ldots, j_k \end{pmatrix}.$$

Таким образом,

$$\overline{CM}_A\begin{pmatrix} i_1, \ldots, i_k \\ j_1, \ldots, j_k \end{pmatrix} = (-1)^{i_1+\ldots+i_k+j_1+\ldots+j_k} CM_A\begin{pmatrix} i_1, \ldots, i_k \\ j_1, \ldots, j_k \end{pmatrix}.$$

Приведем формулу, выражающую определитель матрицы A через ее миноры k-го порядка и их алгебраические дополнения.

Теорема 10 (Лаплас).[5] *Для любых фиксированных натуральных чисел $k < n$, $i_1 < \ldots < i_k \leqslant n$ определитель квадратной матрицы $A = (a_{ij})_{n\times n}$ над кольцом R равен сумме произведений всех ее миноров порядка k, содержащихся в строках с номерами $i_1, \ldots, i_k$, на их алгебраические дополнения, т. е.*

$$|A| = \sum_{1\leqslant j_1<\ldots<j_k\leqslant n} M_A\begin{pmatrix} i_1, \ldots, i_k \\ j_1, \ldots, j_k \end{pmatrix} \overline{CM}_A\begin{pmatrix} i_1, \ldots, i_k \\ j_1, \ldots, j_k \end{pmatrix}. \tag{12}$$

□ 1. Рассмотрим сначала случай, когда $i_1 = 1, \ldots, i_k = k$. Обозначим в этом случае правую часть равенства (12) через Δ и будем вычислять ее, пользуясь определениями миноров и их алгебраических дополнений:

$$\begin{aligned}\Delta &= \sum_{1\leqslant j_1<\ldots<j_k\leqslant n} M_A\begin{pmatrix} 1, \ldots, k \\ j_1, \ldots, j_k \end{pmatrix} \overline{CM}_A\begin{pmatrix} 1, \ldots, k \\ j_1, \ldots, j_k \end{pmatrix} = \\ &= \sum_{1\leqslant j_1<\ldots<j_k\leqslant n} \left(\left(\sum_{(s_1,\ldots,s_k)\in P(j_1,\ldots,j_k)} \delta(s_1, \ldots, s_k)\, a_{1s_1} \ldots a_{ks_k} \right) \times \right. \\ &\times \left. \left((-1)^{1+\ldots+k+j_1+\ldots+j_k} \sum_{(s_{k+1},\ldots,s_n)\in P(\overline{1,n}\setminus\{j_1,\ldots,j_k\})} \delta(s_{k+1}, \ldots, s_n)\, a_{k+1s_{k+1}} \ldots a_{ns_n} \right) \right).\end{aligned}$$

[5] П. С. Лаплас (1749–1827) — французский математик и физик.

Перемножая в скобках 1-ю сумму на 2-ю почленно и пользуясь свойствами операций в кольце R, получим

$$\Delta = \sum_{1\leqslant j_1<\ldots<j_k\leqslant n}\Bigg(\sum_{\substack{(s_1,\ldots,s_k)\in P(j_1,\ldots,j_k)\\(s_{k+1},\ldots,s_n)\in P(\overline{1,n}\setminus\{j_1,\ldots,j_k\})}}\delta(s_1,\ldots,s_k)\,\delta(s_{k+1},\ldots,s_n)\times$$
$$\times(-1)^{1+\ldots+k+j_1+\ldots+j_k}a_{1s_1}\ldots a_{ks_k}a_{k+1s_{k+1}}\ldots a_{ns_n}\Bigg). \quad (13)$$

Запишем полученную сумму сумм в виде одной суммы. Заметим, что число слагаемых во внутренней сумме равно $k!(n-k)!$, а во внешней — C_n^k. Значит, общее число слагаемых в сумме равно $k!(n-k)!C_n^k = n!$, т. е. числу всех перестановок из $P(\overline{1,n})$. Заметим теперь, что наборы индексов $(s_1,\ldots,s_k,s_{k+1},\ldots,s_n)$, соответствующие слагаемым суммы (13), являются перестановками множества $\overline{1,n}$, и любая перестановка из $P(\overline{1,n})$ может быть представлена в виде такого набора индексов при подходящем выборе подмножества $\{j_1,\ldots,j_k\}\subset\overline{1,n}$ и перестановок $(s_1,\ldots,s_k)\in P(j_1,\ldots,j_k)$, $(s_{k+1},\ldots,s_n)\in P(\overline{1,n}\setminus\{j_1,\ldots,j_k\})$. Следовательно, в результате суммирование будет производиться по всем перестановкам $(s_1,\ldots,s_n)$ из $P(\overline{1,n})$ Отсюда, с учетом утверждения 6 главы 2, получим:

$$\Delta = \sum_{(s_1,\ldots,s_k,s_{k+1},\ldots,s_n)\in P(\overline{1,n})}\delta(s_1,\ldots,s_k,s_{k+1},\ldots,s_n)\,a_{1s_1}\ldots a_{ks_k}a_{k+1s_{k+1}}\ldots a_{ns_n} = |A|,$$

и равенство (12) в рассматриваемом случае доказано.

2. Пусть теперь $i_1,\ \ldots,\ i_k$ — любые числа из множества $\overline{1,n}$, удовлетворяющие условию $1\leqslant i_1<\ldots<i_k\leqslant n$. Сведем этот случай к первому. Для этого осуществим в матрице A следующую перестановку строк. Переставляя i_1-ю строку поочередно со всеми предыдущими, поставим ее на 1-е место, затем i_2-ю строку таким же образом поставим на 2-е место, и т. д., и, наконец, поставим i_k-ю строку на k-е место. В итоге получим некоторую матрицу B. Так как для перехода от A к B мы произвели $(i_1-1)+(i_2-2)+\ldots+(i_k-k)$ перестановок строк, то по свойству 5 определителей

$$|A| = (-1)^{1+\ldots+k+i_1+\ldots+i_k}|B|. \quad (14)$$

По доказанному в случае 1 имеем:

$$|B| = \sum M_B\begin{pmatrix}1,\ \ldots,\ k\\ j_1,\ldots,j_k\end{pmatrix}\overline{CM}_B\begin{pmatrix}1,\ \ldots,\ k\\ j_1,\ldots,j_k\end{pmatrix}. \quad (15)$$

Непосредственно из построения матрицы B следует, что

$$M_B\begin{pmatrix}1,\ \ldots,\ k\\ j_1,\ldots,j_k\end{pmatrix} = M_A\begin{pmatrix}i_1,\ldots,i_k\\ j_1,\ldots,j_k\end{pmatrix},$$

$$CM_B\begin{pmatrix}1,\ \ldots,\ k\\ j_1,\ldots,j_k\end{pmatrix} = CM_A\begin{pmatrix}i_1,\ldots,i_k\\ j_1,\ldots,j_k\end{pmatrix}.$$

Из последнего равенства, используя определение алгебраического дополнения, получим:

$$\overline{CM}_B\begin{pmatrix}1,\ldots,k\\ j_1,\ldots,j_k\end{pmatrix}=(-1)^{1+\ldots+k+j_1+\ldots+j_k}CM_A\begin{pmatrix}i_1,\ldots,i_k\\ j_1,\ldots,j_k\end{pmatrix}=$$

$$=(-1)^{1+\ldots+k+j_1+\ldots+j_k}(-1)^{i_1+\ldots+i_k+j_1+\ldots+j_k}\overline{CM}_A\begin{pmatrix}i_1,\ldots,i_k\\ j_1,\ldots,j_k\end{pmatrix}=$$

$$=(-1)^{1+\ldots+k+i_1+\ldots+i_k}\overline{CM}_A\begin{pmatrix}i_1,\ldots,i_k\\ j_1,\ldots,j_k\end{pmatrix}.$$

Из найденных соотношений между минорами и алгебраическими дополнениями матриц A, B и равенств (14), (15) легко следует равенство (12). □

Замечание 5. Ясно, что теорема Лапласа останется верной, если вместо k выделенных строк матрицы взять k столбцов.

В качестве отдельного утверждения выделим один практически важный частный случай теоремы Лапласа, когда $k=1$. В этом случае минор $M_A\binom{r}{s}$ матрицы $A=(a_{ij})_{n\times n}$ совпадает с ее элементом a_{rs}, и потому его алгебраическое дополнение называют *алгебраическим дополнением элемента* a_{rs} и обозначают также через A_{rs}. По определению 9 для нахождения A_{rs} нужно удалить из A r-ю строку и s-й столбец, вычислить определитель полученной матрицы и умножить его на $(-1)^{r+s}$.

Следствие 1. *Определитель матрицы $A=(a_{ij})_{n\times n}$ равен сумме произведений всех элементов любой строки (любого столбца) матрицы A на их алгебраические дополнения*:

$$|A|=\sum_{j=1}^{n}a_{ij}A_{ij},\quad i\in\overline{1,n};\qquad |A|=\sum_{i=1}^{n}a_{ij}A_{ij},\quad j\in\overline{1,n}. \tag{16}$$

Правые части равенств (16) называются *разложениями определителя матрицы A* соответственно *по i-й строке и j-му столбцу*.

Следствие 2. *Сумма произведений всех элементов любой строки (любого столбца) квадратной матрицы на алгебраические дополнения соответствующих элементов другой строки (другого столбца) этой же матрицы равна нулю, т. е. для $A=(a_{ij})_{n\times n}$*

$$\sum_{j=1}^{n}a_{kj}A_{ij}=0\quad \textit{при } i,k\in\overline{1,n},\ i\neq k; \tag{17}$$

$$\sum_{i=1}^{n}a_{ij}A_{ik}=0\quad \textit{при } j,k\in\overline{1,n},\ j\neq k. \tag{18}$$

□ Рассмотрим вспомогательную матрицу $B = (b_{ij})_{n\times n}$, которая получается заменой в A i-й строки ее k-й строкой (при сохранении неизменными остальных строк). Разложим $|B|$ по i-й строке. По следствию 1 получим:

$$|B| = \sum_{j=1}^{n} b_{ij} B_{ij}.$$

Так как в матрице B есть две равные строки, то $|B| = 0$, и поэтому выполняется равенство

$$\sum_{j=1}^{n} b_{ij} B_{ij} = 0. \tag{19}$$

Теперь заметим, что $b_{ij} = a_{kj}$, $B_{ij} = A_{ij}$, для всех $i, j \in \overline{1,n}$. Произведя в равенстве (19) указанную замену, получим равенство (17). Аналогично доказывается равенство (18). □

§ 4. ОБРАТИМЫЕ МАТРИЦЫ. КРИТЕРИЙ ОБРАТИМОСТИ

Рассмотрим кольцо $R_{n,n}$ квадратных матриц порядка n над коммутативным кольцом R с единицей e и найдем все его обратимые элементы.

Теорема 11. *Матрица $A \in R_{n,n}$ обратима в кольце $R_{n,n}$ тогда и только тогда, когда ее определитель $|A|$ является обратимым элементом кольца R.*

□ Пусть матрица A обратима в кольце $R_{n,n}$, т. е. для нее существует матрица A^{-1}, удовлетворяющая условию

$$AA^{-1} = A^{-1}A = E,$$

где E — единичная матрица из $R_{n,n}$. Отсюда и из теоремы 8 имеем:

$$|A| \cdot |A^{-1}| = |A^{-1}| \cdot |A| = e.$$

Эти равенства означают, что $|A^{-1}|$ есть обратный элемент для $|A|$, т. е. $|A|$ обратим в R и $|A|^{-1} = |A^{-1}|$.

Обратно, пусть $|A|$ — обратимый элемент кольца R. Построим матрицу $A^* = (c_{ij})_{n\times n}$, в которой $c_{ij} = A_{ji}$. Непосредственным перемножением матриц с использованием следствий 1 и 2 из теоремы Лапласа, получим:

$$AA^* = A^*A = \begin{pmatrix} |A| & 0 & \dots & 0 \\ 0 & |A| & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & |A| \end{pmatrix}.$$

Отсюда следует, что $A \cdot (|A|^{-1} \cdot A^*) = (|A|^{-1} \cdot A^*) \cdot A = E$, т. е. матрица $|A|^{-1} \cdot A^*$ является обратной для A, и матрица A обратима. □

Матрицу A^* называют *взаимной* к A.

В доказательстве теоремы указан и алгоритм нахождения обратной матрицы для A: сначала надо в A каждый элемент заменить на его алгебраическое дополнение, затем полученную матрицу транспонировать и в полученной таким образом матрице A^* каждый элемент умножить на $|A|^{-1}$.

В следующей главе для матриц над полем будет указан более простой алгоритм нахождения обратной матрицы.

Следствие. *Если $A, B \in R_{n,n}$ и $AB = E$, то $B = A^{-1}$.*

□ Так как $AB = E$, то по теореме 8 $|A| \cdot |B| = e$, а потому и $|B| \cdot |A| = e$ (в силу коммутативности кольца R). Значит, элемент $|A|$ обратим в R, а тогда по теореме 11 обратима и матрица A, т. е. существует $A^{-1} \in R_{n,n}$. Умножив обе части равенства $AB = E$ слева на A^{-1}, получим искомое равенство $B = A^{-1}$. □

§ 5. ЭЛЕМЕНТАРНЫЕ ПРЕОБРАЗОВАНИЯ МАТРИЦ. ЭКВИВАЛЕНТНЫЕ МАТРИЦЫ

Определение 11. *Элементарными преобразованиями строк* матрицы $A \in R_{m,n}$ называют:

1) умножение любой ее строки на обратимый элемент кольца R;

2) прибавление к любой ее строке другой строки, умноженной на произвольный элемент кольца R.

Аналогично определяются *элементарные преобразования столбцов* матрицы A. *Элементарными преобразованиями матрицы* называют элементарные преобразования ее строк и столбцов.

Покажем, что элементарные преобразования строк (столбцов) матрицы можно осуществить путем умножения ее слева (справа) на подходящие квадратные обратимые матрицы.

Утверждение 12. (а) *Умножение i-й строки (i-го столбца) матрицы $A \in R_{m,n}$ на r равносильно умножению A слева (справа) на матрицу*

$$D_m^{(i)}(r) \quad (D_n^{(i)}(r)), \quad \textit{где} \quad D_k^{(i)}(r) = \operatorname{diag}(e, \ldots, \overset{i}{r}, \ldots, e)_{k\times k}.$$

(б) *Прибавление к i-й строке (i-му столбцу) матрицы $A \in R_{m,n}$ произведения ее j-й строки (j-го столбца) на $r \in R$ при $j \neq i$ равносильно умножению A слева (справа) на матрицу*

$$T_m^{(i,j)}(r) \quad (T_n^{(j,i)}(r)), \quad \textit{где} \quad T_k^{(s,t)}(r) = E_{k\times k} + E_{k\times k}^{(s,t)}(r).$$

Доказывается утверждение непосредственной проверкой.

Определение 12. Матрицы $D_k^{(i)}(r)$ при $r \in R^*$ и $T_k^{(i,j)}(c)$ при любом $c \in R$ и $i \neq j$ называются *элементарными матрицами*.

Легко видеть, что матрицы $D_k^{(i)}(r)$ и $T_k^{(i,j)}(c)$ получаются путем соответствующих элементарных преобразований единичной матрицы $E_{k\times k}$ (проверьте).

Так как $|D_k^{(i)}(r)| = r$, $|T_k^{(i,j)}(c)| = e$ и элемент r обратим, то элементарные матрицы обратимы. Легко видеть, что обратные для них матрицы также являются элементарными, а именно (проверьте):

$$D_k^{(i)}(r)^{-1} = D_k^{(i)}(r^{-1}), \quad T_k^{(i,j)}(c)^{-1} = T_k^{(i,j)}(-c).$$

Определение 13. Матрица $B \in R_{m,n}$, называется *эквивалентной* матрице $A \in R_{m,n}$, если она может быть получена из A с помощью конечной последовательности элементарных преобразований. Обозначение: $B \sim A$.

Из определения 13 видно, что эквивалентные матрицы имеют одни и те же размеры. Следовательно, отношение $\sim$ является бинарным отношением на множестве $R_{m,n}$. Укажем простейшие свойства этого отношения.

Утверждение 13. (а) *Отношение $\sim$ является отношением эквивалентности на множестве $R_{m,n}$.*

(б) *Если матрица B получена из A перестановкой строк или столбцов, то $B \sim A$.*

(в) *Если $A, B \in R_{m,n}$ и $A \sim B$, то существуют матрицы $U \in R^*_{m,m}$, $V \in R^*_{n,n}$ такие, что $B = UAV$.*

(г) *Если матрицы A и B квадратные и $A \sim B$, то $|B| = r|A|$, где r — некоторый обратимый элемент кольца R.*

□ (а) Свойства рефлексивности и транзитивности отношения $\sim$ очевидны. Для доказательства симметричности достаточно заметить, что если матрица B получена из A одним элементарным преобразованием, то и A из B можно получить одним элементарным преобразованием (проверьте).

(б) Для доказательства достаточно осуществить с помощью элементарных преобразований перестановку любых двух строк (столбцов) матрицы A (поскольку с помощью транспозиций можно перейти от любой перестановки к любой другой). Для строк это сделано при доказательстве свойства 5 определителей, для столбцов делается аналогично.

(в) Так как $A \sim B$, то в соответствии с определением 11 и утверждением 12 существуют такие элементарные матрицы $U_1, \ldots, U_k \in R^*_m$ и $V_1, \ldots, V_l \in R^*_n$, что $B = U_k \ldots U_1 A V_1 \ldots V_l$. Тогда искомыми матрицами являются $U = U_k \ldots U_1$ и $V = V_1 \ldots V_l$.

(г) Из утверждения (в) следует, что $B = UAV$ для некоторых обратимых матриц U, V. Отсюда, используя теорему 8 и коммутативность кольца R, получим:

$$|B| = |U| \cdot |A| \cdot |V| = |U| \cdot |V| \cdot |A| = r \cdot |A|,$$

где $r = |U| \cdot |V|$ — обратимый элемент кольца R. □

В дальнейшем нам неоднократно понадобится

Теорема 14 (о минорах эквивалентных матриц). *Если $A, B \in R_{m,n}$, $A \sim B$, и все миноры k-го порядка матрицы A кратны элементу $c \in R$, то все миноры k-го порядка матрицы B также кратны c.*

□ Утверждение теоремы достаточно доказать для случая, когда B получена из A одним элементарным преобразованием.

1. Пусть i-й столбец матрицы A умножен на обратимый элемент r. Тогда любой минор матрицы B или совпадает с минором матрицы A, или отличается от него лишь множителем r (по свойству 1 определителей), и утверждение верно.

2. Пусть к l-му столбцу матрицы A прибавлен ее s-й столбец, умноженный на $r \in R$. Рассмотрим любой минор k-го порядка матрицы B:

$$M_B\begin{pmatrix} i_1, \dots, i_k \\ j_1, \dots, j_k \end{pmatrix} = M_B.$$

Если $l \notin \{j_1, \dots, j_k\}$ или $l, s \in \{j_1, \dots, j_k\}$, то, очевидно, имеет место равенство

$$M_B = M_A\begin{pmatrix} i_1, \dots, i_k \\ j_1, \dots, j_k \end{pmatrix}.$$

Пусть $l \in \{j_1, \dots, j_k\}$, например $l = j_t$, $1 \leqslant t \leqslant k$, и $s \notin \{j_1, \dots, j_k\}$. Обозначим через $\tilde{A}_1^{\downarrow}, \dots, \tilde{A}_n^{\downarrow}$ столбцы подматрицы $A\begin{pmatrix} i_1, \dots, i_k \\ 1, \dots, n \end{pmatrix}$. Тогда минор M_B можно записать в виде

$$M_B = \big|\tilde{A}_{j_1}^{\downarrow} \dots \tilde{A}_{j_{t-1}}^{\downarrow} (\tilde{A}_{j_t}^{\downarrow} + r\tilde{A}_s^{\downarrow})\, \tilde{A}_{j_{t+1}}^{\downarrow} \dots \tilde{A}_{j_k}^{\downarrow}\big|.$$

По свойству 2 определителей имеем: $M_B = M_1 + M_2 \cdot r$, где

$$M_1 = \big|\tilde{A}_{j_1}^{\downarrow} \dots \tilde{A}_{j_{t-1}}^{\downarrow} \tilde{A}_{j_t}^{\downarrow}\, \tilde{A}_{j_{t+1}}^{\downarrow} \dots \tilde{A}_{j_k}^{\downarrow}\big|, \quad M_2 = \big|\tilde{A}_{j_1}^{\downarrow} \dots \tilde{A}_{j_{t-1}}^{\downarrow} \tilde{A}_s^{\downarrow}\, \tilde{A}_{j_{t+1}}^{\downarrow} \dots \tilde{A}_{j_k}^{\downarrow}\big|.$$

Отсюда видно, что M_1 — минор матрицы A, а M_2 — минор матрицы A, если $j_{t-1} < s < j_{t+1}$, и может не быть минором матрицы A в противном случае. В последнем случае, переставив в M_2 столбцы так, чтобы их индексы расположились в порядке возрастания, мы получим минор матрицы A, которой, согласно свойству 5 определителей, будет равен M_2 или $-M_2$.

Таким образом, во всех возможных подслучаях случая 2 минор M_B или совпадает с минором k-го порядка матрицы A, или равен алгебраической сумме двух ее миноров k-го порядка. Отсюда и из условия следует, что минор M_B кратен c, и утверждение теоремы верно. Для элементарных преобразований строк доказательство проводится или аналогичным образом, или переходом к транспонированным матрицам. □

Следствие. *Если $A, B \in R_{m,n}$, $A \sim B$ и все миноры k-го порядка матрицы A равны нулю, то все миноры k-го порядка матрицы B также равны нулю.*

Ниже, при изучении матриц и при решении систем линейных уравнений особую роль будут играть элементарные преобразования строк матрицы. В связи с этим сформулируем

Определение 14. Матрица B называется *строчно эквивалентной матрице* $A \in R_{m,n}$, если она может быть получена из A с помощью конечной последовательности элементарных преобразований строк. Обозначение: $B \overset{c}{\sim} A$.

Для введенного отношения $\overset{c}{\sim}$ имеет место аналогичное утверждению 13

Утверждение 15. (а) *Отношение $\overset{c}{\sim}$ является отношением эквивалентности на множестве матриц $R_{m,n}$.*

(б) *Если матрица B получена перестановкой строк в матрице A, то $B \overset{c}{\sim} A$.*

(в) *Если $A, B \in R_{m,n}$ и $A \overset{c}{\sim} B$, то существует обратимая матрица $U \in R^*_{m,m}$ такая, что $B = UA$.*

(г) *Если матрицы A, B квадратные и $A \overset{c}{\sim} B$, то $|B| = r|A|$, где r — некоторый обратимый элемент кольца R.* □

В некоторых случаях элементарные преобразования строк матриц могут помочь найти обратную матрицу для заданной обратимой матрицы из $R_{n,n}$.

Утверждение 16. *Пусть A — обратимая, а E — единичная матрица из $R_{n,n}$. Если матрица $B = (A, E)$ строчно эквивалентна матрице $B' = (E, A')$, то $A' = A^{-1}$.*

□ Из условия и утверждения 15(в) получаем, что $B' = U(A, E)$, где $U \in R^*_{n,n}$. Так как $U(A, E) = (UA, UE)$, то $UA = E$ и $U = A'$. Отсюда и из следствия теоремы 11 получим $A' = A^{-1}$. □

Таким образом, для нахождения матрицы A^{-1} достаточно уметь обратимую матрицу A элементарными преобразованиями строк приводить к единичной матрице.

Заметим, что для решения последней задачи в общем случае (т. е. для матриц над произвольным кольцом R) алгоритм неизвестен. То же самое относится и к задаче распознавания эквивалентности матриц. Вместе с тем, для матриц над $\mathbb{Z}$ алгоритмы решения указанных задач известны. В частности, алгоритм распознавания эквивалентности матриц над $\mathbb{Z}$ основан на преобразовании матриц к определенным каноническим матрицам. В главе 7 эта же идея будет использована для матриц над полями.

§ 6. КАНОНИЧЕСКИЕ МАТРИЦЫ НАД КОЛЬЦОМ $\mathbb{Z}$

Определение 15. *Канонической матрицей* над кольцом $\mathbb{Z}$ называется диагональная матрица

$$\operatorname{diag}(\delta_1, \ldots, \delta_t)_{m \times n}, \tag{20}$$

в которой $\delta_1, \ldots, \delta_t \in \mathbb{N}_0$ и $\forall\, i \in \overline{1, t-1}:\ \delta_i \mid \delta_{i+1}$.

Матрицу (20) называют также *матрицей в нормальной форме Смита* в честь английского математика Г. Смита (1826–1889).

Пример 3. Из трех матриц

$$\operatorname{diag}(1, 2, 4, 0), \quad \operatorname{diag}(1, 0, 2, 4), \quad \operatorname{diag}(1, -2, 4, 0)$$

первая — каноническая, две другие — нет. Нулевая матрица — каноническая.

Теорема 17 (Смит, 1861). *Для любой матрицы $A = (a_{ij})_{m\times n}$ над $\mathbb{Z}$ существует эквивалентная ей каноническая матрица.*

Предварительно введем обозначение $\mu(X)$ для минимального по модулю ненулевого элемента любой целочисленной матрицы $X \neq O$ и докажем вспомогательное утверждение.

Лемма. *Для любой ненулевой матрицы $A = (a_{ij})_{m\times n}$ над $\mathbb{Z}$ существует эквивалентная ей матрица $B = (b_{ij})_{m\times n}$, удовлетворяющая условию*

$$\forall\, i \in \overline{1,m},\ \forall\, j \in \overline{1,n}:\ \ \mu(B) \mid b_{ij}. \tag{21}$$

□ Докажем лемму индукцией по $|\mu(A)|$. Если $|\mu(A)| = 1$, то утверждение очевидно. Допустим, что оно верно при $|\mu(A)| < d$ и пусть $|\mu(A)| = d$, где $d \in \mathbb{N}$ и $d > 1$. Выберем в A элемент $a_{kl} = \mu(A)$ и рассмотрим три случая.

1. $\exists\, s \in \overline{1,n}:\ \ a_{kl} \nmid a_{ks}$. Разделим a_{ks} на a_{kl} с остатком: $a_{ks} = a_{kl}q + r$, $0 < r < |a_{kl}|$. Прибавив к s-му столбцу матрицы A ее l-й столбец, умноженный на $-q$, получим матрицу A' с элементом r на месте (k,s). Так как $0 < r < |a_{kl}|$, то $|\mu(A')| < |\mu(A)|$, и по предположению индукции существует матрица B со свойством (21), эквивалентная A', а потому и A.

2. $\exists\, t \in \overline{1,m}:\ \ a_{kl} \nmid a_{tl}$. В этом случае рассуждения аналогичны, вместо преобразования столбцов используются преобразования строк.

3. $\forall\, s \in \overline{1,n},\ \forall\, t \in \overline{1,m}:\ \ a_{kl} \mid a_{ks},\ a_{kl} \mid a_{tl}$. Допустим, что $a_{kl} \nmid a_{pq}$. Прибавим k-ю строку матрицы A, умноженную на $-a_{pl}/a_{kl}$, к ее p-й строке, а затем p-ю строку полученной матрицы — к ее k-й строке:

$$A = \begin{pmatrix} \dots & \dots & \dots & \dots & \dots \\ \dots & a_{kl} & \dots & a_{kq} & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \dots & a_{pl} & \dots & a_{pq} & \dots \\ \dots & \dots & \dots & \dots & \dots \end{pmatrix} \sim \begin{pmatrix} \dots & \dots & \dots & \dots & \dots \\ \dots & a_{kl} & \dots & a_{kq} & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \dots & 0 & \dots & a'_{pq} & \dots \\ \dots & \dots & \dots & \dots & \dots \end{pmatrix} \sim \begin{pmatrix} \dots & \dots & \dots & \dots & \dots \\ \dots & a'_{kl} & \dots & a'_{kq} & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \dots & 0 & \dots & a'_{pq} & \dots \\ \dots & \dots & \dots & \dots & \dots \end{pmatrix}.$$

В итоге получим матрицу $A' = (a'_{ij})$, в которой

$$a'_{kl} = a_{kl}, \quad a'_{kq} = a_{pq} + a_{kq}(1 - a_{pl}/a_{kl}) \quad \text{и} \quad a'_{kl} \nmid a'_{kq},$$

поскольку $a'_{kl} \mid a_{kq}$ и $a'_{kl} \nmid a_{pq}$. Следовательно, для матрицы A' выполнено одно из условий: или $|\mu(A')| < |\mu(A)|$, или $\mu(A') = \mu(A)$ и тогда $\mu(A') = a'_{kl}$ и $a'_{kl} \nmid a'_{kq}$. Отсюда видно, что для матрицы A', а потому и для A, искомая матрица B существует или по предположению индукции, или по доказанному в случае 1. □

□ Теперь докажем теорему 17 индукцией по $m + n$. Заметим, что для нулевой матрицы A утверждение верно. Поэтому далее будем считать, что $A \neq 0$.

Если $m + n = 2$, то $m = n = 1$, и утверждение теоремы очевидно. Допустим, что оно верно при $m + n < k$, и пусть $m + n = k$, где $k \in \mathbb{N}$ и $k > 1$. По лемме существует матрица B со свойством (21), эквивалентная A. Не теряя общности, можно считать, что $|\mu(B)| = b_{11}$, ибо этого можно добиться перестановками строк и столбцов (что, согласно утверждению 13, осуществимо с помощью элементарных преобразований)

и умножением 1-й строки на -1. Прибавив к i-й строке матрицы B ее 1-ю строку, умноженную на $-b_{i1}/b_{11}$ для всех $i \in \overline{2,m}$, а затем к j-му столбцу 1-й столбец, умноженный на $-b_{1j}/b_{11}$ для всех $j \in \overline{2,n}$, получим матрицу вида

$$B_1 = \begin{pmatrix} b_{11} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & B' & \\ 0 & & & \end{pmatrix}, \quad \text{где} \quad B' = \begin{pmatrix} b'_{22} & \dots & b'_{2n} \\ \dots & \dots & \dots \\ b'_{m2} & \dots & b'_{mn} \end{pmatrix}.$$

При этом $B_1 \sim A$, и по теореме 14 $b_{11} \mid b'_{ij}$ для всех $i \in \overline{2,m}$, $j \in \overline{2,n}$. По предположению индукции матрицу B' можно элементарными преобразованиями привести к канонической матрице $\operatorname{diag}(\delta_2, \dots, \delta_t)_{(m-1)\times(n-1)}$. Осуществляя соответствующие преобразования над строками и столбцами матрицы B_1, получим матрицу $\operatorname{diag}(b_{11}, \delta_2, \dots, \delta_t)_{m\times n} = D$, удовлетворяющую по теореме 14 условию $b_{11} \mid \delta_i$, где $i \in \overline{2,t}$. А так как $D \sim A$, то матрица D — искомая. □

Заметим, что доказательство теоремы 17 конструктивно. Из него легко извлекается алгоритм нахождения канонической матрицы, эквивалентной A. Алгоритм этот допускает вариации, связанные с неоднозначным выбором минимального по модулю элемента и не делящихся на него элементов в промежуточных матрицах. Вместе с тем, ниже будет доказано принципиально важное утверждение о единственности канонической матрицы, эквивалентной A. Для этого понадобятся некоторые вспомогательные факты.

Определение 16. Пусть $A \in \mathbb{Z}_{m,n}$, $t = \min(m,n)$ и $k \in \overline{1,t}$. *Инвариантным делителем k-го порядка*, или k-м инвариантным делителем, матрицы A называется число $d_k(A)$, равное неотрицательному НОД всех миноров k-го порядка матрицы A.

Заметим, что в силу следствия 1 теоремы Лапласа числа $d_i(A)$ удовлетворяют условию $\forall\, i \in \overline{1,t-1}:\ d_i(A) \mid d_{i+1}(A)$ (докажите).

Оказывается, набор чисел $(d_1(A), \dots, d_t(A))$ является инвариантом класса всех матриц, эквивалентных A, а именно, справедливо

Утверждение 18. *У эквивалентных матриц над $\mathbb{Z}$ инвариантные делители одинаковых порядков равны.*

□ Пусть $A \sim B$, $d_k(A) = d$, $d_k(B) = d'$. Тогда по теореме 14 имеем: $d \mid d'$ и $d' \mid d$. Отсюда, учитывая, что $d \geqslant 0$, $d' \geqslant 0$, получим $d = d'$. □

Утверждение 19. *Если $D = \operatorname{diag}(\delta_1, \dots, \delta_t)$ — каноническая матрица над $\mathbb{Z}$, то для любого $k \in \overline{1,t}$ справедливо равенство*

$$d_k(D) = \delta_1 \dots \delta_k. \tag{22}$$

□ Легко видеть, что среди всех миноров k-го порядка матрицы D не равными нулю могут быть лишь миноры $M_D\binom{i_1, \dots, i_k}{i_1, \dots, i_k} = \delta_{i_1} \dots \delta_{i_k}$. Отсюда и из условия $\delta_i \mid \delta_{i+1}$ для $i \in \overline{1,t-1}$ следуют соотношения $\delta_1 \dots \delta_k \mid \delta_{i_1} \dots \delta_{i_k}$, а потому и равенство (22). □

Теперь может быть доказана

Теорема 20 (Смит). *Каждая целочисленная матрица A эквивалентна единственной канонической матрице.*

□ Если A эквивалентна канонической матрице (20), то по утверждению 19 для любого $k \in \overline{1,t}$ справедливо равенство (22). Отсюда и из утверждения 16 имеем $\delta_1 = d_1(A)$, и для $k \in \overline{2,t}$:

$$\delta_k = \begin{cases} d_k(A)/d_{k-1}(A), & \text{если } d_{k-1}(A) \neq 0, \\ 0, & \text{если } d_{k-1}(A) = 0. \end{cases}$$

Таким образом, элементы матрицы D однозначно определяются матрицей A. □

Из теорем 17, 20 следует, что корректно

Определение 17. Каноническая матрица $\operatorname{diag}(\delta_1, \ldots, \delta_t)_{m\times n}$, эквивалентная матрице $A \in \mathbb{Z}_{m,n}$, называется *канонической формой или нормальной формой Смита матрицы* A и обозначается через $\mathcal{K}(A)$. Элемент δ_k этой матрицы называется *k-м инвариантным множителем матрицы* A и обозначается через $\delta_k(A)$, $k \in \overline{1,t}$.

Таким образом,

$$\mathcal{K}(A) = \operatorname{diag}(\delta_1(A), \ldots, \delta_t(A))_{m\times n}. \tag{23}$$

Следствие 1. *Матрица $A \in \mathbb{Z}_{n,n}$ обратима тогда и только тогда, когда она представляется в виде произведения элементарных матриц.*

□ Пусть матрица A обратима. Так как $A \sim \mathcal{K}(A)$, то существуют элементарные матрицы $U_1, \ldots, U_k$, $V_1, \ldots, V_l$ такие, что

$$A = U_1 \ldots U_k \mathcal{K}(A) V_1 \ldots V_l.$$

По теореме 11 $|A| = \varepsilon \in \{1, -1\}$. Так как $|\mathcal{K}(A)| > 0$, то $|\mathcal{K}(A)| = 1$. Отсюда следует, что $\mathcal{K}(A) = E$, и потому $A = U_1 \ldots U_k V_1 \ldots V_l$. Если же матрица A есть произведение элементарных матриц, то ясно, что она обратима. □

Следствие 2. *Любая обратимая над $\mathbb{Z}$ матрица A строчно эквивалентна единичной матрице E.*

□ Из доказанного в следствии 1 имеем: $A = U_1 \ldots U_k V_1 \ldots V_l E$. Это и означает, что $A \overset{c}{\sim} E$. □

Заметим, что следствие 2 делает возможным нахождение матрицы A^{-1} с использованием утверждения 16.

Следствие 3. *Для любых матриц $A, B \in \mathbb{Z}_{m,n}$ равносильны утверждения*:

(а) $A \sim B$;

(б) *существуют обратимые матрицы U, V над $\mathbb{Z}$ такие, что*

$$B = UAV; \tag{24}$$

(в) $\mathcal{K}(A) = \mathcal{K}(B)$;

(г) $d_k(A) = d_k(B)$ *для всех* $k = 1, \ldots, \min\{m, n\}$;

(д) $\delta_k(A) = \delta_k(B)$ *для всех* $k = 1, \ldots, \min\{m, n\}$.

□ Эквивалентность утверждений (а), (в), (г), (д) следует из существования и единственности канонической формы для любой матрицы над $\mathbb{Z}$ и равенств (22), (23). Импликация (а)⇒(б) доказана утверждением 13, и остается доказать импликацию (б)⇒(а). Пусть $B = UAV$, где U, V — обратимые матрицы. Тогда по следствию 1 U и V представляются произведениями элементарных матриц. Отсюда и из утверждения 12 следует, что от A к B можно перейти с помощью конечной последовательности элементарных преобразований. Значит, $A \sim B$. □

Следствие 4. *Существует алгоритм, позволяющий для любых матриц A, B над $\mathbb{Z}$ выяснять, эквивалентны они или нет, и в случае положительного ответа находить обратимые матрицы U, V, удовлетворяющие условию* (24).

□ Для распознавания эквивалентности матриц A, B достаточно найти и сравнить их канонические формы. Для нахождения матриц U, V из (24) при условии $A \sim B$ найдем сначала матрицы U_1, V_1, U_2, V_2, удовлетворяющие равенствам

$$U_1 A V_1 = \mathcal{K}(A), \quad U_2 B V_2 = \mathcal{K}(B).$$

Отсюда с учетом равенства $\mathcal{K}(A) = \mathcal{K}(B)$ получим: $B = U_2^{-1} U_1 A V_1 V_2^{-1}$, и потому условию (24) удовлетворяют матрицы $U = U_2^{-1} U_1$, $V = V_1 V_2^{-1}$. Таким образом, задача нахождения матриц U, V из (24) сводится к случаю, когда $B = \mathcal{K}(A)$. В этом случае U и V можно найти путем перемножения элементарных матриц, соответствующих элементарным преобразованиям, осуществляемым при переходе от A к $\mathcal{K}(A)$. Однако процесс этот можно формализовать, если воспользоваться следующим легко проверяемым равенством:

$$\begin{pmatrix} U_{m\times m} & O_{m\times n} \\ O_{n\times m} & E_{n\times n} \end{pmatrix} \begin{pmatrix} A_{m\times n} & E_{m\times m} \\ E_{n\times n} & O_{n\times m} \end{pmatrix} \begin{pmatrix} V_{n\times n} & O_{n\times m} \\ O_{m\times n} & E_{m\times m} \end{pmatrix} = \begin{pmatrix} UAV & U \\ V & O \end{pmatrix}.$$

Из него следует, что для нахождения матриц U, V достаточно к матрице

$$\begin{pmatrix} A_{m\times n} & E_{m\times m} \\ E_{n\times n} & O_{n\times m} \end{pmatrix}$$

применить те элементарные преобразования первых m строк и первых n столбцов, которые переводят A в $\mathcal{K}(A)$. В итоге получим матрицу $\begin{pmatrix} \mathcal{K}(A) & U \\ V & O \end{pmatrix}$ и тем самым найдем U, V. □

Заметим, что приведенным выше алгоритмом можно воспользоваться и для нахождения обратной матрицы для A, если она обратима. Действительно, в этом случае $\mathcal{K}(A) = E$, и из равенства $UAV = \mathcal{K}(A)$ следует, что $A^{-1} = VU$.

Канонические формы матриц могут оказаться полезными и при решении простейших матричных уравнений над $\mathbb{Z}$.

Пример 4. Решить уравнение

$$AX = B, \tag{25}$$

где $A \in \mathbb{Z}_{m,n}$, $B \in \mathbb{Z}_{m,k}$. Найдем для A каноническую форму и обратимые матрицы U, V такие, что $A = U\mathcal{K}(A)V$. Умножив обе части уравнения (25) слева на матрицу U^{-1}, получим уравнение

$$\mathcal{K}(A)VX = U^{-1}B, \tag{26}$$

равносильное (25), т. е. имеющее с (25) одно и то же множество решений. Так как V — обратимая матрица, то для решения уравнения (26) достаточно найти все решения уравнения

$$\mathcal{K}(A)Y = U^{-1}B, \tag{27}$$

а затем по формуле $X = V^{-1}Y$ найти все решения уравнения (25). Таким образом, решение уравнения (25) сведено к решению значительно более простого уравнения (27), для которого нетрудно указать как критерий разрешимости, так и способ нахождения всех решений, в случае их наличия.

Утверждение 21. *Пусть* $\mathcal{K}(A) = \operatorname{diag}(\delta_1, \ldots, \delta_t)_{m\times n}$, *где* $\delta_1, \ldots, \delta_s$ *отличны от* 0, *а* $\delta_{s+1} = \ldots = \delta_t = 0$, $U^{-1}B = C = (c_{ij})_{m\times k}$. *Тогда уравнение* (27) *имеет решение в том и только том случае, когда все элементы* i*-й строки матрицы* C *делятся на* δ_i *при* $i \in \overline{1,s}$ *и равны нулю при* $i > s$. *Если уравнение* (27) *разрешимо, то все его решения исчерпываются матрицами* $Y = (y_{ij})_{m\times k}$, *где*

$$y_{ij} = \begin{cases} c_{ij}/\delta_i, & \text{если } i \in \overline{1,s}, \\ \text{любое целое число}, & \text{если } i \in \overline{s+1,n}. \end{cases}$$

Проверьте это утверждение самостоятельно.

ЗАДАЧИ

1. Пусть R — кольцо с единицей. Докажите, что для любой матрицы $A = (a_{ij})_{m\times n} \in R_{m,n}$ выполняются равенства:

а) $A = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}E_{m\times n}^{(i,j)}$,

б) $E_{m\times m}^{(i,l)}AE_{n\times n}^{(t,j)} = a_{lt}E_{m\times n}^{(i,j)}$,

в) $E_{m\times n}^{(i,j)}E_{n\times r}^{(k,l)} = \delta_{jk}E_{m\times r}^{(i,l)}$, где $\delta_{jk} = \begin{cases} 0, & \text{если } j \neq k, \\ 1, & \text{если } j = k \end{cases}$ (δ_{jk} — *символ Кронекера*).

2. Докажите, что матрицы, перестановочные со всеми $(n \times n)$-матрицами над коммутативным кольцом R с единицей $e \neq 0$, исчерпываются скалярными матрицами, т. е. матрицами вида aE.

3. Являются ли подкольцами кольца матриц $R_{n,n}$ (над коммутативным кольцом R с единицей):

а) множество всех скалярных матриц;

б) множество всех диагональных матриц;

в) множество всех верхне-, нижнетреугольных матриц;

г) множество всех матриц с заданным определителем;

д) множество всех матриц, в которых первые r строк нулевые, $1 \leqslant r \leqslant n$?

4. Докажите, что множество матрицы вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ над полем $\mathbb{R}$ образует поле, изоморфное полю $\mathbb{C}$.

5. Является ли полем множество матриц вида $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ над $\mathbb{R}$?

6. Докажите, что для любой обратимой матрицы A над коммутативным кольцом с единицей выполняется равенство $(A^T)^{-1} = (A^{-1})^T$.

7. Докажите равенство

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ a_1 & a_2 & \dots & a_n \\ a_1^2 & a_2^2 & \dots & a_n^2 \\ \dots & \dots & \dots & \dots \\ a_1^{n-1} & a_2^{n-1} & \dots & a_n^{n-1} \end{vmatrix} = \prod_{1 \leqslant i < j \leqslant n} (a_j - a_i).$$

Данный определитель называют *определителем Вандермонда*.[6] *Указание*: примените метод полной математической индукции по n. Для перехода от n к $n+1$ следует вычесть из каждой строки предыдущую, умноженную на a_1.

8. Докажите, что для любых матриц $A \in R_{m,n}$, $B \in R_{n,k}$ и натуральных чисел r, $s_1, \dots, s_r$, $t_1, \dots, t_r$, удовлетворяющих неравенствам $r \leqslant \min\{m, n, k\}$, $1 \leqslant s_1 < \dots < s_r \leqslant m$, $1 \leqslant t_1 < \dots < t_r \leqslant n$, справедлива формула, называемая *формулой Бине—Коши*[7]:

$$M_{AB}\begin{pmatrix} s_1, \dots, s_r \\ t_1, \dots, t_r \end{pmatrix} = \sum_{1 \leqslant i_1 < \dots < i_r \leqslant n} M_A\begin{pmatrix} s_1, \dots, s_r \\ i_1, \dots, i_r \end{pmatrix} M_B\begin{pmatrix} i_1, \dots, i_r \\ t_1, \dots, t_r \end{pmatrix}.$$

9. Докажите, что если в матрице $A_{n \times n}$ есть нулевая подматрица размеров $k \times l$ и $k + l > n$, то $|A| = 0$.

10. Найдите сумму произведений всех миноров порядка k матрицы $A_{n \times n}$ на их алгебраические дополнения, $1 \leqslant k < n$.

11. Докажите, что матрицы $A_{n \times n}$, $B_{n \times n}$ обратимы тогда и только тогда, когда обратима матрица $C = AB$. При этом $C^{-1} = B^{-1}A^{-1}$.

12. Даны матрицы над $\mathbb{Z}$:

$$A_1 = \begin{pmatrix} -2 & 2 & 3 & -3 \\ -4 & 1 & 4 & 2 \\ -3 & 2 & 4 & 5 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 2 & 3 & 4 & 5 \\ -3 & -4 & 2 & -6 \\ 3 & 5 & 14 & 9 \end{pmatrix},$$

$$B = \begin{pmatrix} 1 & 2 & 1 & 3 \\ 4 & -3 & 2 & -5 \\ -2 & 1 & 3 & 4 \end{pmatrix}.$$

[6] А. Т. Вандермонд (1735–1796) — французский математик.

[7] Ж. Ф. М. Бине (1786–1856), О. Л. Коши (1789–1857) — французские математики.

а) Найдите канонические формы матриц A_1, A_2 и такие обратимые над $\mathbb{Z}$ матрицы U_i, V_i, что $U_iA_iV_i = \mathcal{K}(A_i)$, $i = 1, 2$.

б) Решите матричные уравнения $A_iX = B$, $i = 1, 2$, над $\mathbb{Z}$.

13. Являются ли обратимыми матрицы над $\mathbb{Z}$:

$$A_1 = \begin{pmatrix} -3 & -4 & 3 & 4 \\ 3 & 5 & -2 & -3 \\ 5 & 8 & -3 & -5 \\ -4 & -4 & 3 & 5 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 2 & 3 & 4 & -2 \\ 3 & -2 & 2 & -3 \\ 1 & -5 & -2 & -1 \\ 3 & 1 & 2 & 4 \end{pmatrix}?$$

В случае положительного ответа найдите соответствующую обратную матрицу.

Глава 7

МАТРИЦЫ НАД ПОЛЕМ

В данной главе мы более подробно изучим матрицы над произвольным полем P. Обратимость всех ненулевых элементов поля P дает возможность найти сравнительно простые алгоритмы решения таких задач о матрицах, для которых в общем случае (т. е. над произвольным коммутативным кольцом с единицей) алгоритмы решения или неизвестны или более сложны. Так, например, для матриц над полем можно указать несложный алгоритм распознавания их эквивалентности, в то время как в общем случае алгоритм решения такой задачи неизвестен.

Полученные здесь результаты о матрицах будут применены в следующей главе к исследованию и решению произвольных систем линейных уравнений над полем. В качестве основного средства изучения матриц над полем будут использоваться элементарные преобразования систем их строк и столбцов.

Вектор-строки и вектор-столбцы над полем P (т. е. матрицы размеров $1 \times n$ и $n \times 1$ соответственно) условимся обозначать латинскими буквами с горизонтальной и вертикальной стрелками, например,

$$\vec{A} = (a_1, a_2, \ldots, a_n), \quad b^{\downarrow} = \begin{pmatrix} a_1 \\ a_2 \\ \ldots \\ a_n \end{pmatrix}.$$

Элементы векторов будем также называть их *координатами*. Множество всех векторов-строк (столбцов) длины n над полем P обозначим через P^n ($P^{(n)}$). Для векторов из P^n ($P^{(n)}$), как для матриц, определены операции покоординатного сложения и умножения на элементы поля P.

Определение 1. Множество векторов-строк P^n (векторов-столбцов $P^{(n)}$) с операциями сложения векторов и умножения векторов на элементы поля P называют *n-мерным арифметическим пространством над полем P*.

Понятие n-мерного арифметического пространства является естественным обобщением понятия трехмерного пространства D^3, изучаемого в школе и в аналитической геометрии. Действительно, при фиксированной системе координат каждый вектор из D^3 определяется упорядоченной тройкой действительных чисел (координат) и потому D^3 можно отождествить с множеством $\mathbb{R}^3$. При этом соответствующие

операции сложения векторов из $\mathbb{R}^3$ и их умножения на числа из $\mathbb{R}$ осуществляются также покоординатно. Этой связью P^n с D^3 объясняется проникновение в алгебру геометрических терминов «вектор», «пространство» и др.

§ 1. РАНГ МАТРИЦЫ

Зафиксируем произвольное поле P и будем рассматривать матрицы над полем P. В этом случае обратимыми в кольце матриц $P_{n,n}$ будут все матрицы с отличными от нуля определителями. Они называются также *невырожденными*. Матрицы с определителем, равным нулю, называют *вырожденными*.

В ряде задач и, в частности, в задаче исследования и решения систем линейных уравнений важную роль играют невырожденные подматрицы данной матрицы. Наибольший порядок таких подматриц называют *рангом матрицы*. Приведем более традиционное

Определение 2. *Рангом* ненулевой матрицы A называется наибольший из порядков отличных от нуля миноров матрицы A. Ранг нулевой матрицы считается равным нулю. Обозначение ранга матрицы A: $\operatorname{rang} A$.

Пример 1. Очевидно, что ранг матрицы $E^{(ij)}$ равен единице, ранг любой невырожденной матрицы из $P_{n,n}$ равен n, ранг диагональной матрицы $\operatorname{diag}(a_1, \ldots, a_t)_{m\times n}$, где $t = \min\{m, n\}$, равен числу ее ненулевых элементов.

Определение 3. Подматрица наибольшего порядка среди всех невырожденных подматриц матрицы A называется ее *ранговой подматрицей*.

Заметим, что во всех матрицах предыдущего примера существует единственная ранговая подматрица. В общем же случае их в заданной матрице может быть много.

Пример 2. Легко проверить, что ранг матрицы

$$A = \begin{pmatrix} 2 & 4 & 3 & 4 \\ 1 & 2 & -1 & 3 \\ 1 & 2 & 4 & 1 \end{pmatrix}$$

равен 2 и число ее ранговых подматриц равно 15 (проверьте).

Способ вычисления ранга матрицы, основанный непосредственно на определении 2, связан с перебором и вычислением большого числа миноров. Естественно возникает мысль: нельзя ли предварительно как-то упростить матрицу, не изменяя ранга, а затем найти ранг полученной матрицы? Эта идея приводит к более простому методу вычисления ранга.

Теорема 1. *Если матрицы A и B эквивалентны, то их ранги равны.*

□ Пусть матрицы A и B эквивалентны и $\operatorname{rang} A = k$. Согласно определению 2 в матрице A для любого $l > k$ или совсем нет миноров порядка l, или все они равны нулю. Тогда по следствию теоремы 14 главы 6 то же самое верно и для матрицы B.

Следовательно, $\operatorname{rang} B \leqslant k$, т. е. $\operatorname{rang} B \leqslant \operatorname{rang} A$. Так как отношение эквивалентности матриц симметрично, то имеем также неравенство $\operatorname{rang} A \leqslant \operatorname{rang} B$. Следовательно, $\operatorname{rang} A = \operatorname{rang} B$. □

Следствие 1. *Ранг произведения матриц не превосходит рангов матриц-сомножителей.*

□ Действительно, если $C = AB$, то, согласно утверждению 6 главы 6, строки матрицы C являются линейными комбинациями строк матрицы B. Поэтому элементарными преобразованиями строк матрицу $\begin{pmatrix} B \\ C \end{pmatrix}$ можно привести к виду $\begin{pmatrix} B \\ 0 \end{pmatrix}$. Используя этот факт и очевидные соотношения между рангами матриц, получим:

$$\operatorname{rang} C \leqslant \operatorname{rang} \begin{pmatrix} B \\ C \end{pmatrix} = \operatorname{rang} \begin{pmatrix} B \\ 0 \end{pmatrix} = \operatorname{rang} B.$$

Аналогично из соотношений (3) главы 6 для столбцов матрицы C получим: $\operatorname{rang} C \leqslant \operatorname{rang} A$. □

Следствие 2. *Если $C = AB$ или $C = BA$, где A — квадратная невырожденная матрица, то* $\operatorname{rang} C = \operatorname{rang} B$.

□ По следствию 1 $\operatorname{rang} C \leqslant \operatorname{rang} B$. А так как $B = A^{-1}C$ или $B = CA^{-1}$, то снова по следствию 1 $\operatorname{rang} B \leqslant \operatorname{rang} C$. Значит, $\operatorname{rang} C = \operatorname{rang} B$. □

Определение 4. Ненулевая матрица $S = (s_{ij})_{m\times n}$ называется *ступенчатой матрицей* типа $S(i_1, \ldots, i_r)$, где $r \in \overline{1,m}$, $1 \leqslant i_1 < \ldots < i_r \leqslant n$, если

1) $s_{1i_1},\ s_{2i_2},\ \ldots,\ s_{ri_r} \neq 0$,
2) $s_{lt} = 0$ при $l > r$, $t \in \overline{1,n}$ и при $l \in \overline{1,r}$, $t < i_l$.

Нулевая матрица также считается ступенчатой.

В подробной записи ступенчатая матрица типа $S(i_1, \ldots, i_r) \in P_{m,n}$ имеет вид

$$S = \begin{pmatrix} 0\ldots0 & s_{1i_1} & *\ldots* & * & *\ldots* & * & *\ldots* \\ 0\ldots0 & 0 & 0\ldots0 & s_{2i_2} & *\ldots* & * & *\ldots* \\ \ldots\ldots & \ldots & \ldots\ldots & \ldots & \ldots\ldots & \ldots & \ldots\ldots \\ 0\ldots0 & 0 & 0\ldots0 & 0 & 0\ldots0 & s_{ri_r} & *\ldots* \\ 0\ldots0 & 0 & 0\ldots0 & 0 & 0\ldots0 & 0 & 0\ldots0 \\ \ldots\ldots & \ldots & \ldots\ldots & \ldots & \ldots\ldots & \ldots & \ldots\ldots \\ 0\ldots0 & 0 & 0\ldots0 & 0 & 0\ldots0 & 0 & 0\ldots0 \end{pmatrix}, \tag{1}$$

где $s_{1i_1},\ s_{2i_2},\ \ldots,\ s_{ri_r} \neq 0$, а на местах звездочек могут находиться любые элементы поля P. Из приведенной записи матрицы S видно, что ее минор $M_S\left(\begin{smallmatrix} 1, \ldots, r \\ i_1, \ldots, i_r \end{smallmatrix}\right)$ отличен от нуля, а все миноры более высоких порядков, если они существуют, равны нулю. Следовательно, ранг ступенчатой матрицы равен числу ее ненулевых строк.

Теорема 2. *Любую матрицу A над полем P можно элементарными преобразованиями строк привести к ступенчатой матрице.*

□ Докажем теорему индукцией по числу m строк матрицы A. При $m = 1$ матрица A сама ступенчатая, и утверждение теоремы верно. Допустим, что оно верно для любой матрицы, состоящей из m строк, и докажем его для матрицы $A \in P_{m+1,n}$.

Если A — нулевая матрица, то она ступенчатая и утверждение верно. Пусть $A \neq 0$ и $A^{\downarrow}_{i_1}$ — самый левый ненулевой столбец матрицы A. Переставляя (если нужно) строки матрицы A, мы, согласно утверждению 15(б) главы 6, получим строчно эквивалентную A матрицу B вида

$$B = \begin{pmatrix} 0 & \dots & 0 & b_{1i_1} & * & \dots & * \\ 0 & \dots & 0 & b_{2i_1} & * & \dots & * \\ & & & \dots\dots\dots & & & \\ 0 & \dots & 0 & b_{m+1\,i_1} & * & \dots & * \end{pmatrix},$$

в которой $b_{1i_1} \neq 0$. Прибавляя к l-й строке матрицы B для каждого $l \in \overline{2, m+1}$ ее 1-ю строку, умноженную на $-b_{li_1}b_{1i_1}^{-1}$, получим матрицу

$$B' = \begin{pmatrix} 0 & \dots & 0 & b_{1i_1} & * & \cdots\cdots & * \\ 0 & \dots & 0 & 0 & \multicolumn{3}{c}{\multirow{3}{*}{A_1}} \\ \dots\dots & & \dots & \vdots & & & \\ 0 & \dots & 0 & 0 & & & \end{pmatrix}.$$

Так как число строк матрицы A_1 равно m, то по предположению индукции она строчно эквивалентна ступенчатой матрице. Произведя соответствующие преобразования строк матрицы B', мы приведем A_1 к ступенчатому виду, не изменив 1-ю строку и первые i_1 столбцов матрицы B'. В итоге B' преобразуется в искомую ступенчатую матрицу. □

Теорема 2 делает содержательным и полезным для нахождения ранга матриц

Утверждение 3. *Ранг произвольной матрицы над полем равен числу ненулевых строк в любой эквивалентной ей ступенчатой матрице.*

□ Справедливость утверждения 3 следует непосредственно из теоремы 1 и совпадения ранга ступенчатой матрицы с числом ее ненулевых строк. □

§ 2. КАНОНИЧЕСКАЯ ФОРМА МАТРИЦЫ

Определение 5. *Каноническими матрицами* над полем P называются нулевая матрица и все матрицы вида

$$\operatorname{diag}(e, \dots, e, 0, \dots, 0)_{m\times n}.$$

Заметим, что каноническая матрица является ступенчатой и ее ранг равен числу единиц на главной диагонали.

Теорема 4. *Для любой матрицы A над полем P существует единственная эквивалентная ей каноническая матрица.*

□ Если A — нулевая матрица, то она уже каноническая. Пусть теперь матрица A отлична от нулевой. Приведем сначала матрицу A элементарными преобразованиями строк к ступенчатой матрице. Пусть при этом получилась матрица (1). Умножив ее l-ю строку на $s_{li_l}^{-1}$ для всех $l \in \overline{1,r}$, получим матрицу с единицами на местах

$$(1,i_1),\ (2,i_2),\ \ldots,\ (r,i_r).$$

Вычитая последовательно ее строки с номерами $2,\ldots,r$, умноженные на подходящие элементы, из предыдущих строк, получим матрицу

$$C = \begin{array}{c} \begin{array}{cccccccccccccc} & & & i_1 & & & & & & i_2 & & & & i_r & \\ \end{array} \\ \begin{pmatrix} 0 & \ldots & 0 & e & * & \ldots & * & 0 & * & \ldots & * & 0 & * & \ldots & * \\ 0 & \ldots & 0 & 0 & 0 & \ldots & 0 & e & * & \ldots & * & 0 & * & \ldots & * \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 & e & * & \ldots & * \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 \end{pmatrix} \end{array}. \tag{2}$$

Теперь, вычитая столбцы с номерами $i_1,\ i_2,\ \ldots,\ i_r$, умноженные на подходящие элементы, из последующих столбцов, отличных от столбцов с номерами $i_1, i_2, \ldots, i_r$, заменим нулями все элементы, обозначенные в (2) звездочками. После этого перестановкой столбцов, поставив столбец с номером i_l на l-е место для $l = 1, \ldots, r$, получим каноническую матрицу K, эквивалентную исходной матрице A. Единственность такой матрицы следует из совпадения числа единиц на ее главной диагонали с рангом матрицы A. □

Единственная каноническая матрица, эквивалентная матрице A, называется *канонической формой* матрицы A и обозначается через $\mathcal{K}(A)$.

Определение 6. Матрицу вида (2) назовем *специальной ступенчатой матрицей* типа $S(i_1, \ldots, i_r)$.

Из доказательств теоремы 4 получаем

Следствие 1. *Любая ненулевая матрица над полем строчно эквивалентна специальной ступенчатой матрице.*

Выделим в виде самостоятельного утверждения важный частный случай следствия 1.

Следствие 2. *Любая квадратная невырожденная матрица над полем строчно эквивалентна единичной матрице.*

Наличие алгоритма приведения невырожденной матрицы к единичной путем элементарных преобразований строк делает возможным применение метода нахождения обратной матрицы, указанного в утверждении 16 главы 6, к любой невырожденной матрице над полем.

Точно так же, как и следствие 1 теоремы 20 главы 6, доказывается

Следствие 3. *Квадратная матрица над полем обратима тогда и только тогда, когда она представляется в виде произведения элементарных матриц.*

Используя теоремы 1–4, нетрудно получить ряд критериев эквивалентности матриц над полем P, некоторые из которых сходны с критериями эквивалентности матриц над $\mathbb{Z}$ (см. следствие 3 теоремы 20 главы 6).

Теорема 5. *Для любых матриц $A, B \in P_{m,n}$ равносильны следующие утверждения*:
(а) $A \sim B$;
(б) *существуют невырожденные матрицы $U \in P_{m,m}$ и $V \in P_{n,n}$ такие, что*

$$B = UAV; \tag{3}$$

(в) $\operatorname{rang} A = \operatorname{rang} B$;
(г) $\mathcal{K}(A) = \mathcal{K}(B)$.

□ Для доказательства теоремы достаточно доказать цепочку импликаций

$$\text{(а)} \Rightarrow \text{(б)} \Rightarrow \text{(в)} \Rightarrow \text{(г)} \Rightarrow \text{(а)}.$$

Импликации (а)⇒(б), (б)⇒(в), (г)⇒(а) следуют соответственно из утверждения 13 главы 6, следствия 2 теоремы 1, теоремы 4. Импликация (в)⇒(г) следует из существования канонических форм и совпадения ранга матрицы с числом единиц в ее канонической форме. □

Одно из принципиально важных приложений канонических форм матриц указывает

Утверждение 6. *Существует алгоритм, позволяющий для любых матриц A, B над полем P выяснять, эквивалентны они или нет, и в случае положительного ответа находить невырожденные матрицы U, V, удовлетворяющие условию* (3).

Доказывается утверждение 6 точно так же, как и следствие 4 теоремы 20 главы 6.

§ 3. ЛИНЕЙНАЯ ЗАВИСИМОСТЬ ВЕКТОРОВ. БАЗИС И РАНГ СИСТЕМЫ ВЕКТОРОВ

В аналитической геометрии при изучении плоскости D^2 и пространства D^3 важную роль играют понятия коллинеарности и компланарности векторов. Так, например, пары неколлинеарных векторов и только они являются базисами пространства D^2. Обобщением понятий коллинеарности и компланарности векторов в n-мерных арифметических пространствах является одно из важнейших для всей математики понятий — понятие линейной зависимости векторов.

Многие результаты из теории линейной зависимости векторов излагаются сходным образом для пространств P^n и $P^{(n)}$. В связи с этим при изложении общих вопросов о линейной зависимости мы будем говорить просто о системах векторов длины n, подразумевая под этим либо системы векторов-строк, либо системы векторов-столбцов длины n. При этом вместо латинских букв со стрелками будем использовать

малые греческие буквы без стрелок. Вектор, все координаты которого нулевые, будем называть нулевым вектором и обозначать буквой θ. Нулевые вектор-строка и вектор-столбец будут обозначаться соответственно через $\vec{0}$ и $0^{\downarrow}$. Пусть

$$\alpha_1, \ldots, \alpha_k \tag{4}$$

— произвольная система векторов длины n над полем P.

Определение 7. Если для некоторых элементов поля P выполняется равенство

$$\alpha_1 c_1 + \alpha_2 c_2 + \ldots + \alpha_k c_k = \theta, \tag{5}$$

то говорят, что для векторов системы (4) выполняется (имеет место) *линейное соотношение* (5). Это соотношение называется *тривиальным*, если все коэффициенты $c_1, \ldots, c_k$ нулевые, и *нетривиальным* в противном случае.

Очевидно, что тривиальное линейное соотношение выполняется для векторов любой системы, наличие же нетривиальных линейных соотношений существенно зависит от заданной системы векторов.

Пример 3. Рассмотрим две системы векторов из P^n:
а) $\vec{e}_1, \ldots, \vec{e}_n$;
б) $\vec{e}_1, \ldots, \vec{e}_n, \vec{a}$, где $\vec{e}_i = (0, \ldots, 0, \overset{i}{1}, 0, \ldots, 0)$, $i \in \overline{1,n}$, $\vec{a} = (a_1, \ldots, a_n)$.
Из определения операций в пространстве P^n имеем:

$$\forall\, c_1, \ldots, c_n \in R\colon\ \vec{e}_1 c_1 + \ldots + \vec{e}_n c_n = (c_1, \ldots, c_n).$$

Следовательно, соотношение

$$\vec{e}_1 c_1 + \ldots + \vec{e}_n c_n = \theta$$

выполняется лишь в том случае, когда $c_1 = \ldots = c_n = 0$, т. е. для векторов системы а) выполняется только тривиальное линейное соотношение. Для векторов же системы б) наряду с тривиальным выполняется и нетривиальное линейное соотношение

$$\vec{e}_1 a_1 + \ldots + \vec{e}_n a_n + \vec{a}(-1) = \theta.$$

Определение 8. Система векторов (4) называется *линейно зависимой*, если для ее векторов выполняется хотя бы одно нетривиальное линейное соотношение. В противном случае она называется *линейно независимой*. Пустая система векторов по определению считается *линейно независимой*.

Более подробно: система векторов (4) называется линейно зависимой, если существуют такие *не все равные нулю* элементы $c_1, \ldots, c_k \in P$, что выполняется равенство (5). Система (4) называется линейно независимой, если для ее векторов равенство (5) выполняется только при

$$c_1 = \ldots = c_k = 0.$$

В примере 3 система векторов а) линейно независима, а система б) линейно зависима при любом векторе $\vec{a}$.

Рассмотрим некоторые свойства линейной зависимости. Напомним, что вектор β называется *линейной комбинацией векторов* системы (4), если существуют такие элементы $r_1, \ldots, r_k \in P$, что $\beta = \alpha_1 r_1 + \ldots + \alpha_k r_k$.

В этом случае говорят также, что вектор β *линейно выражается* через векторы $\alpha_1, \ldots, \alpha_k$.

Теорема 7 (критерий линейной зависимости).

(а) *Система векторов* (4) *при* $k > 1$ *линейно зависима тогда и только тогда, когда хотя бы один ее вектор линейно выражается через остальные векторы.*

(б) *Система, состоящая из одного вектора, линейно зависима тогда и только тогда, когда этот вектор нулевой.*

□ (а) Если $k > 1$ и система (4) линейно зависима, то по определению 8 найдутся не все равные нулю элементы $c_1, \ldots, c_k \in P$, при которых выполняется равенство (5). Пусть, например, $c_i \neq 0$. Так как P — поле, то в P существует элемент c_i^{-1}. Умножив обе части равенства (5) на c_i^{-1} и перенеся все слагаемые, кроме α_i, в правую сторону, мы выразим вектор α_i линейно через остальные векторы системы (4). Обратно, пусть некоторый вектор α_j системы (4) линейно выражается через остальные ее векторы:

$$\alpha_j = \alpha_1 r_1 + \ldots + \alpha_{j-1} r_{j-1} + \alpha_{j+1} r_{j+1} + \ldots + \alpha_k r_k.$$

Тогда имеем нетривиальное линейное соотношение

$$\alpha_1 r_1 + \ldots + \alpha_{j-1} r_{j-1} + \alpha_j (-e) + \alpha_{j-1} r_{j-1} + \ldots + \alpha_k r_k = \theta,$$

и потому система (4) линейно зависима.

(б) Пусть система (4) состоит из одного вектора α_1. Если $\alpha_1 = \theta$, то выполнено нетривиальное линейное соотношение $\alpha_1 e = \theta$, и система $\{\alpha_1\}$ линейно зависима. Если же $\alpha_1 \neq 0$, то равенство $\alpha_1 c = \theta$ может выполняться лишь при $c = 0$, поскольку умножение α_1 на c производится покоординатно и в поле отсутствуют делители нуля. Следовательно, система $\{\alpha_1\}$ линейно независима. □

Обратите внимание на то, что в линейно зависимой системе не обязательно каждый вектор выражается через остальные. Примером может служить система векторов α, θ, где $\alpha \neq \theta$. В ней вектор θ выражается через α (а именно, $\theta = \alpha \cdot 0$), а вектор α через θ не выражается.

Следствие. *Система из двух векторов* α, β *линейно зависима тогда и только тогда, когда эти векторы пропорциональны* (*т. е.* $\alpha = \beta c$ *или* $\beta = \alpha c$ *при некотором* $c \in P$).

Утверждение 8. *Если некоторая подсистема системы векторов линейно зависима, то и вся система линейно зависима, т. е. любая подсистема линейно независимой системы линейно независима.*

□ Справедливость утверждения 8 следует непосредственно из определения 8, поскольку любое нетривиальное линейное соотношение для части векторов системы можно дополнить слагаемыми с нулевыми коэффициентами до нетривиального соотношения для всех векторов системы. □

Утверждение 9. *Если в системе векторов* (4) $k > 1$ *и первый вектор ненулевой, то она линейно зависима тогда и только тогда, когда хотя бы один ее вектор линейно выражается через предыдущие векторы.*

□ Если какой-либо вектор системы (4) линейно выражается через предыдущие, то система (4) линейно зависима по теореме 7. Обратно, пусть система (4) линейно зависима и (5) есть нетривиальное линейное соотношение для ее векторов. Выберем максимальное $j \in \overline{1,k}$ такое, что $c_j \neq 0$. Так как $\alpha_1 \neq \theta$, то $j > 1$, и из соотношения (5) вектор α_j выразится через предыдущие векторы $\alpha_1, \ldots, \alpha_{j-1}$. □

Выделим особо один практически важный случай утверждения 9.

Утверждение 10. *Если система векторов* (4) *линейно независима, то система векторов* $\alpha_1, \ldots, \alpha_k, \beta$ *линейно зависима тогда и только тогда, когда вектор* β *линейно выражается через векторы системы* (4).

Утверждение 11. *Если система векторов* (4) *линейно независима и вектор* β *линейно выражается через векторы системы* (4)*, то его представление в виде линейной комбинации векторов из* (4) *единственно.*

□ Пусть выполняются равенства $\beta = \alpha_1 c_1 + \ldots + \alpha_k c_k$, $\beta = \alpha_1 c'_1 + \ldots + \alpha_1 c'_1$. Вычитая почленно из первого равенства второе, получим $\alpha_1(c_1 - c'_1) + \ldots + \alpha_k(c_k - c'_k) = \theta$. Отсюда и из линейной независимости системы (4) получаем $c_i = c'_i$, $i \in \overline{1,k}$. □

Определение 9. Подсистема T системы векторов (4) называется ее *максимальной линейно независимой подсистемой*, или *базисом*, если

а) система T линейно независима,

б) добавление к системе T любого вектора из системы (4) приводит к линейно зависимой системе.

Пример 4. Нетрудно видеть, что максимальными линейно независимыми подсистемами системы векторов

$$\vec{\alpha}_1 = (0,0,0), \quad \vec{\alpha}_2 = (1,0,0), \quad \vec{\alpha}_3 = (0,1,1), \quad \vec{\alpha}_4 = (1,1,1)$$

будут подсистемы $(\vec{\alpha}_2, \vec{\alpha}_3)$, $(\vec{\alpha}_2, \vec{\alpha}_4)$, $(\vec{\alpha}_3, \vec{\alpha}_4)$, $(\vec{\alpha}_3, \vec{\alpha}_2)$, $(\vec{\alpha}_4, \vec{\alpha}_2)$, $(\vec{\alpha}_4, \vec{\alpha}_3)$.

Пример 5. Базисом системы нулевых векторов $\theta, \theta, \ldots, \theta$ является пустая система векторов.

Непосредственно из теоремы 7 и утверждения 10 следует

Утверждение 12. *Если система* (4) *содержит хотя бы один ненулевой вектор, то совокупность условий* а)–б) *определения* 9 *эквивалентна совокупности условий* а) *и*

б′) *любой вектор системы* (4) *линейно выражается через векторы системы* T.

Утверждение 13. *Любая конечная система векторов имеет базис. Более того, любую ее линейно независимую подсистему можно дополнить до базиса.*

□ Пусть (4) — любая система векторов и T — любая ее линейно независимая подсистема (возможно, и пустая).

Рассмотрим всевозможные линейно независимые подсистемы векторов системы (4), содержащие T, и выберем среди них подсистему с наибольшим числом векторов. Очевидно, что она удовлетворяет условиям а)–б) определения 9, и потому является базисом системы (4), содержащим T. □

В связи с изучением линейной зависимости систем векторов из P^n ($P^{(n)}$) естественно возникают следующие задачи алгоритмического характера.

1. Выяснить, является заданная система векторов линейно зависимой или нет?

2. Выяснить, выражается заданный вектор линейно через векторы заданной системы или нет?

3. В случае положительного ответа на вопрос 2, найти представление указанного вектора в виде линейной комбинации векторов заданной системы.

4. Найти базис заданной системы векторов.

5. Выяснить, является ли базисом системы векторов заданная ее подсистема.

6. Дополнить заданную линейно независимую подсистему системы векторов до ее базиса.

В принципе все эти задачи разрешимы и сводятся, по существу, к решению систем линейных уравнений над полем P, которые мы научимся исследовать и решать в следующей главе. Вместе с тем, для решения задач 1–6 можно указать более простые алгоритмы, основанные на использовании алгоритма приведения любой матрицы к ступенчатой или специальной ступенчатой матрице. С этой целью докажем предварительно две теоремы.

Теорема 14. *Если матрицы* A, B *из* $P_{m,n}$ *строчно эквивалентны, то между столбцами матрицы* A *и между столбцами матрицы* B *выполняются одни и те же линейные соотношения, т. е.*

$$\forall\, c_1, \ldots, c_n \in P\colon\ (A_1^{\downarrow}c_1 + \ldots + A_n^{\downarrow}c_n = 0^{\downarrow}) \ \Leftrightarrow\ (B_1^{\downarrow}c_1 + \ldots + B_n^{\downarrow}c_n = 0^{\downarrow}).$$

В частности, система столбцов матрицы A *линейно зависима тогда и только тогда, когда линейно зависима соответствующая система столбцов матрицы* B.

□ По условию и утверждению 15 главы 6 существует такая невырожденная матрица $U \in P_{m,m}$, что $UA = B$, т. е. $UA_i^{\downarrow} = B_i^{\downarrow}$, $i \in \overline{1,m}$. Отсюда, пользуясь свойствами

операций над матрицами, получим:

$$A_1^{\downarrow}c_1 + \ldots + A_n^{\downarrow}c_n = 0^{\downarrow} \;\Leftrightarrow\; U(A_1^{\downarrow}c_1 + \ldots + A_n^{\downarrow}c_n) = U0^{\downarrow} \;\Leftrightarrow$$
$$\Leftrightarrow\; (UA_1^{\downarrow})c_1 + \ldots + (UA_n^{\downarrow})c_n = 0^{\downarrow} \;\Leftrightarrow\; B_1^{\downarrow}c_1 + \ldots + B_n^{\downarrow}c_n = 0^{\downarrow}.$$

Заметим, что в первой из выписанных равносильностей использовано условие невырожденности матрицы U, в этом случае переход справа налево можно осуществить путем умножения на матрицу U^{-1}. □

Теорема 15. *Пусть ненулевая матрица A из $P_{m,n}$ строчно эквивалентна ступенчатой матрице $S = (s_{ij})_{m\times n}$ типа $S(i_1, \ldots, i_r)$. Тогда справедливы следующие утверждения*:

(а) *столбец $A_j^{\downarrow}$ матрицы A является ненулевым и не представляется в виде линейной комбинации ее предыдущих столбцов тогда и только тогда, когда $j \in \{i_1, \ldots, i_r\}$*;

(б) *если S — специальная ступенчатая матрица, то*

$$\forall\, j \in \overline{1,n}: \quad A_j^{\downarrow} = \sum_{k=1}^{r} A_{i_k}^{\downarrow} s_{kj}. \tag{6}$$

□ Согласно теореме 14, утверждения (а), (б) достаточно доказать для соответствующих столбцов матрицы S. В этом же случае они легко усматриваются непосредственно из строения матрицы S. □

Из этой, по существу очевидной, теоремы можно получить очень важные следствия и, в частности, алгоритмы решения перечисленных выше задач 1–6.

Следствие 1. *Если матрица A строчно эквивалентна ступенчатой матрице S типа $S(i_1, \ldots, i_r)$, то система столбцов*

$$A_{i_1}^{\downarrow},\ \ldots,\ A_{i_r}^{\downarrow} \tag{7}$$

матрицы A является базисом системы всех ее столбцов.

□ Не теряя общности, можно считать, что S — специальная ступенчатая матрица. Тогда в силу теоремы 15(а) и утверждения 9 система (7) линейно независима. Кроме того, из (6) следует, что все столбцы матрицы A линейно выражаются через векторы системы (7). □

Следствие 2. *Все ступенчатые матрицы, строчно эквивалентные A, имеют один и тот же тип и среди них существует единственная специальная ступенчатая матрица.*

□ Если $A \overset{c}{\sim} S$ и S — ступенчатая матрица типа $S(i_1, \ldots, i_r)$, то по теореме 15(а) числа $i_1, \ldots, i_r$ однозначно определяются матрицей A: это номера тех ее ненулевых столбцов, которые не выражаются через предыдущие столбцы. Если, кроме того, S —

специальная ступенчатая матрица, то по теореме 15(б) ее элементы являются коэффициентами в линейных выражениях столбцов матрицы A через линейно независимую систему ее столбцов (7) и по утверждению 11 однозначно определяются столбцами матрицы A. □

Следствие 3 (критерий линейной независимости). *Система векторов-столбцов*

$$A_1^{\downarrow}, \ldots, A_m^{\downarrow} \tag{8}$$

длины n над полем P линейно независима тогда и только тогда, когда ранг матрицы $A = (A_1^{\downarrow} \ldots A_m^{\downarrow})$ равен m.

□ По теореме 15(а) условие линейной независимости системы (8) равносильно тому, что ступенчатая матрица, строчно эквивалентная A, имеет тип $S(1, 2, \ldots, m)$. Тому же самому по утверждению 3 равносильно и условие $\operatorname{rang} A = m$. □

Из следствия 3 и определения ранга матрицы получаем

Следствие 4. *Любая линейно независимая система векторов длины n содержит не более n векторов.*

Мы можем также доказать следующий *критерий равенства нулю определителя матрицы*.

Следствие 5. *Определитель квадратной матрицы $A_{n\times n}$ над полем равен нулю тогда и только тогда, когда система ее столбцов (строк) линейно зависима.*

□ Если система столбцов или строк матрицы A линейно зависима, то $|A| = 0$ по теореме 7 и свойству 7 определителей (или его аналогу для строк). Обратно, пусть $|A| = 0$. Тогда по определению 2 $\operatorname{rang} A < n$ и по следствию 3 система ее столбцов линейно зависима. Для доказательства линейной зависимости системы ее строк достаточно те же рассуждения провести для транспонированной матрицы. □

Следствие 6. *Любые два базиса произвольной конечной системы векторов-столбцов (строк) состоят из одного и того же числа векторов, которое для непустой системы равно рангу матрицы, составленной из столбцов (строк) этой системы.*

□ Для пустой системы векторов и системы, состоящей из нулевых векторов, утверждение следствия очевидно. Рассмотрим произвольную непустую систему, содержащую ненулевые векторы-столбцы. Пусть это есть система (8), и (7) — любой ее базис. Допишем к системе (7) все остальные векторы системы (8) в произвольном порядке и из полученной системы столбцов составим матрицу

$$A' = (A_{i_1}^{\downarrow} \ \ldots \ A_{i_r}^{\downarrow} \ A_{i_{r+1}}^{\downarrow} \ \ldots \ A_{i_m}^{\downarrow}).$$

Так как (7) есть базис системы столбцов матрицы A', то ступенчатая матрица S', строчно эквивалентная A', имеет тип $S(1, \ldots, r)$, и по утверждению 3 $\operatorname{rang} A' = r$.

Однако матрица A' эквивалентна матрице $A = (A_1^{\downarrow} \dots A_m^{\downarrow})$, и тогда по теореме 1 $\operatorname{rang} A' = \operatorname{rang} A$. Для доказательства утверждения о системе векторов-строк достаточно путем транспонирования перейти к системе векторов-столбцов и учесть, что ранг матрицы равен рангу транспонированной к ней матрицы. □

В силу следствия 6 корректно

Определение 10. *Рангом* произвольной конечной системы векторов называется число элементов любого ее базиса.

Пользуясь понятием ранга системы векторов, следствие 6 можно сформулировать короче:

Следствие 7 (теорема о ранге матрицы). *Ранг матрицы равен рангу системы ее строк и рангу системы ее столбцов.*

В заключение укажем алгоритмы решения перечисленных выше задач 1–6 для произвольной системы векторов-столбцов (8).

1. Для решения задачи 1 о системе векторов (8) достаточно найти ранг матрицы $A = (A_1^{\downarrow} \dots A_m^{\downarrow})$ и воспользоваться следствием 3.

2. Чтобы выяснить, выражается ли линейно вектор-столбец $A_{m+1}^{\downarrow}$ длины n через векторы системы (8), найдем ступенчатую матрицу S'', строчно эквивалентную матрице $A'' = (A_1^{\downarrow} \dots A_m^{\downarrow} A_{m+1}^{\downarrow})$. Если она имеет тип $S(j_1, \dots, j_t)$, то по теореме 15(а) вектор $A_{m+1}^{\downarrow}$ линейно выражается через систему (8) тогда и только тогда, когда $j_t < m + 1$.

3. Если, в обозначениях пункта 2, $j_t < m + 1$, то для решения задачи 3 матрицу S'' следует элементарными преобразованиями строк привести к специальной ступенчатой матрице. По теореме 15(б) первые t элементов последнего столбца полученной матрицы и будут коэффициентами линейного выражения вектора $A_{m+1}^{\downarrow}$ через векторы $A_{j_1}^{\downarrow}, \dots, A_{j_t}^{\downarrow}$.

4. Для нахождения базиса системы векторов (8) достаточно найти ступенчатую матрицу, строчно эквивалентную A, и воспользоваться следствием 1.

5. Чтобы выяснить, является ли система (7) базисом системы (8), составим матрицу по схеме $A' = (A_{i_1}^{\downarrow} \dots A_{i_r}^{\downarrow} A_{i_{r+1}}^{\downarrow} \dots A_{i_m}^{\downarrow})$, указанной в доказательстве следствия 6, и найдем ступенчатую матрицу S', строчно эквивалентную A'. По теореме 15 система (7) является базисом системы (8) тогда и только тогда, когда S' имеет тип $S(1, 2, \dots, r)$.

6. Для того, чтобы дополнить произвольную линейно независимую подсистему векторов (7) до базиса системы (8), воспользуемся алгоритмом пункта 5. В силу линейной независимости системы (7) полученная при этом матрица S' будет иметь тип $S(1, \dots, r, t_1, \dots, t_l)$ при некоторых $t_1, \dots, t_l \in \overline{r+1, m}$. Согласно следствию 1, система столбцов $A_{i_1}^{\downarrow}, \dots, A_{i_r}^{\downarrow}, A_{i_{t_1}}^{\downarrow}, \dots, A_{i_{t_l}}^{\downarrow}$ и будет одним из искомых базисов системы (8).

Решение задач 1–6 для векторов-строк сводится к решению соответствующих задач для векторов-столбцов, транспонированных к исходным векторам-строкам.

§ 4. ПОДПРОСТРАНСТВА АРИФМЕТИЧЕСКИХ ПРОСТРАНСТВ

Пусть P — поле и L_n — любое из арифметических пространств P^n, $P^{(n)}$.

Определение 11. *Подпространством пространства* L_n назовем любое непустое подмножество $K \subset L_n$, замкнутое относительно операций сложения векторов и умножения их на элементы поля P, т. е. удовлетворяющее условиям:

1) $\forall\, \alpha, \beta \in K:\ (\alpha + \beta \in K)$,

2) $\forall\, \alpha \in K,\ \forall\, c \in P:\ (\alpha c \in K)$.

Обозначение: $K < L_n$.

Примерами подпространств в L_n могут служить нулевое подпространство, состоящее из одного нулевого вектора θ, само пространство L_n, множество векторов вида

$$\{\alpha_1 c_1 + \ldots + \alpha_m c_m :\ c_1, \ldots, c_m \in P\},$$

где $\alpha_1, \ldots, \alpha_m$ — произвольная фиксированная система векторов из L_n (проверьте это в качестве упражнения).

Как и для конечных систем векторов, для подпространств из L_n можно определить понятие базиса.

Определение 12. *Базисом* ненулевого подпространства K пространства L_n называется любая его конечная система векторов

$$\beta_1, \ldots, \beta_t, \tag{9}$$

удовлетворяющая условиям:

1) система (9) линейно независима,

2) любой вектор из K линейно выражается через векторы системы (9).

Базисом нулевого подпространства считается пустая система векторов.

Теорема 16. *Любое подпространство K пространства L_n имеет базисы, и любые два его базиса равномощны.*

□ По следствию 4 теоремы 15 любая конечная линейно независимая система векторов из K содержит не более n векторов. Следовательно, в K существуют конечные линейно независимые системы с наибольшим числом векторов. Из утверждения 10 следует, что любая из них является базисом K. Пусть система (9) и система векторов

$$\gamma_1, \ldots, \gamma_s \tag{10}$$

являются базисами K. Тогда очевидно, что каждая из них является базисом конечной системы векторов

$$\gamma_1, \ldots, \gamma_s, \beta_1, \ldots, \beta_t. \tag{11}$$

Отсюда и из следствия 6 теоремы 15 имеем: $s = t$. □

Из доказанной теоремы следует, что корректно

Определение 13. Число элементов в любом из базисов подпространства K пространства L_n называется *размерностью подпространства* K и обозначается через $\dim K$.

Следующее утверждение описывает все базисы подпространства K из L_n.

Утверждение 17. *Если $K < L_n$ и $\dim K = t$, то любая конечная линейно независимая система векторов из K содержит не более t векторов, и любая такая система из t векторов является базисом подпространства K.*

□ Пусть (9) есть базис K и (10) — любая линейно независимая система векторов из K. Рассмотрим систему векторов (11). По утверждению 13 систему (10) можно дополнить до базиса системы (11), который, согласно следствию 6 теоремы 15, состоит из t векторов. Следовательно, $s \leqslant t$ и при $s = t$ система векторов (10) есть базис системы (11). Остается заметить, что любой базис системы (11) является базисом пространства K. □

В заключение рассмотрим вопрос о числе векторов и различных базисов в пространствах из L_n над конечным полем.

Утверждение 18. *Пусть P — конечное поле из q элементов, K — подпространство из L_n и $\dim K = t > 0$. Тогда*

(а) $|K| = q^t$;

(б) *число различных базисов пространства K равно*

$$\prod_{i=0}^{t-1}(q^t - q^i).$$

□ (а) Пусть (9) есть базис пространства K. Из определения базиса и утверждения 11 следует, что любой вектор α из K однозначно представляется в виде $\alpha{=}\beta_1 c_1{+}\ldots{+}\beta_t c_t$. С другой стороны, из определения 11 видно, что $\beta_1 c_1{+}\ldots{+}\beta_t c_t{\in}K$ при любых $c_1, \ldots, c_t \in P$. Следовательно, число векторов в K равно числу различных наборов $(c_1, \ldots, c_t)$ элементов поля P, которое, очевидно, равно q^t.

(б) Укажем алгоритм построения всех базисов пространства K. Так как $\dim K > 0$, то в K существуют ненулевые векторы. Возьмем любой из них α_1. Если $t = 1$, то процесс окончен. В противном случае, в K есть векторы, не выражающиеся линейно через α_1. Возьмем любой из таких векторов α_2. Продолжим этот процесс до тех пор, пока не получим систему из t векторов $\alpha_1, \alpha_2, \ldots, \alpha_t$. По утверждению 9 любая такая система линейно независима и по утверждению 17 является базисом K. Легко видеть также, что указанным способом может быть получен любой базис пространства K. Теперь заметим, что при любой уже выбранной системе $\alpha_1, \ldots, \alpha_r$ из r векторов $(r+1)$-й вектор может быть выбран в

$$|K \setminus \{\alpha_1 c_1 + \ldots + \alpha_r c_r : \ c_1, \ldots, c_r \in P\}| \tag{12}$$

вариантах. По утверждению (а) $|K| = q^t$, а из утверждения 11 следует равенство $|\{\alpha_1 c_1 + \ldots + \alpha_r c_r : \ c_1, \ldots, c_r \in P\}| = q^r$. Значит, в описанном выше процессе $(r+1)$-й вектор может быть выбран в $q^t - q^r$ вариантах. Отсюда и следует утверждение (б). □

Следствие. *Число невырожденных матриц размера $n \times n$ над конечным полем из q элементов равно $\prod_{i=0}^{n-1}(q^n - q^i)$.*

□ На основании следствия 5 теоремы 15 и утверждения 17 имеем: матрица A из $P_{n,n}$ тогда и только тогда невырождена, когда система ее строк является базисом пространства P^n. Далее остается применить утверждение 18(б) при $t = n$. □

ЗАДАЧИ

1. Подсчитайте число подматриц порядка r в матрице размеров $m \times n$.

2. Докажите, что ранг матрицы вида $\begin{pmatrix} A_{k\times k} & 0 \\ 0 & B_{l\times l} \end{pmatrix}$ равен сумме рангов матриц A, B.

3. Решите матричное уравнение $AXA = A$, где A — заданная матрица размеров $m \times n$. Сколько решений имеет это уравнение над полем из q элементов. (*Указание*: воспользоваться канонической формой матрицы A.)

4. Оцените сверху число сомножителей в произведениях элементарных матриц, которыми можно представить все невырожденные матрицы размеров $n \times n$.

5. Найдите число векторов из P^n, представимых в виде линейных комбинаций m заданных векторов, если P — конечное поле из q элементов.

6. Опишите конечные системы векторов с единственным базисом.

7. Опишите матрицы, имеющие единственную ранговую подматрицу.

8. Докажите, что ранг суммы матриц не превосходит суммы рангов исходных матриц.

9. Сколько линейно независимых систем по r векторов существует в пространстве P^n над конечным полем P из q элементов? Сколько в нем существует подпространств размерности r?

10. Две конечные системы векторов из P^n называются *эквивалентными*, если все векторы каждой из них являются линейными комбинациями векторов другой системы. Докажите, что определенное таким образом отношение для систем векторов из P^n является отношением эквивалентности. Покажите, что произвольная система векторов эквивалентна своему базису.

11. Докажите, что матрицы A, B одинаковых размеров строчно эквивалентны тогда и только тогда, когда системы векторов-строк этих матриц также эквивалентны (в смысле определения из задачи 10).

12. Пусть $S_{m\times n}$ — специальная ступенчатая матрица. Докажите, что для любой матрицы $A_{k\times m}$ матрица AS является специальной ступенчатой в том и только том случае, когда A — специальная ступенчатая матрица. Найти тип матрицы AS по типам матриц A, S.

13. Докажите, что в кольце матриц $P_{n,n}$ над полем P делители нуля исчерпываются ненулевыми вырожденными матрицами.

Глава 8

СИСТЕМЫ ЛИНЕЙНЫХ УРАВНЕНИЙ

На важность задачи решения уравнений и систем уравнений в любых алгебрах указывалось в § 2 главы 3. Для колец и полей в общем случае эта задача является очень сложной, а иногда и неразрешимой в принципе. Вместе с тем, для одного частного вида систем уравнений над полями, называемых системами линейных уравнений, указанная задача решается сравнительно просто. Общий подход к исследованию и решению таких систем уравнений основан на использовании матричного аппарата и применим к системам уравнений над произвольным коммутативным кольцом с единицей. Для систем уравнений над полями он приводит к наиболее законченным результатам и, в частности, к алгоритмам распознавания разрешимости и нахождения всех решений.

§ 1. СИСТЕМЫ ЛИНЕЙНЫХ УРАВНЕНИЙ НАД КОММУТАТИВНЫМ КОЛЬЦОМ С ЕДИНИЦЕЙ. ТЕОРЕМА КРАМЕРА

Зафиксируем произвольное коммутативное кольцо R с единицей.

Определение 1. Отображение $f\colon R^n \to R$ называется *аффинной функцией* от n переменных над кольцом R, если существуют такие элементы $a_0, a_1, \ldots, a_n \in R$, что

$$\forall\, r_1, \ldots, r_n \in R\colon \ f(r_1, \ldots, r_n) = a_0 + a_1 r_1 + \ldots + a_n r_n.$$

В частности, при $a_0 = 0$ функция f называется *линейной*.

Используя символы переменных $x_1, \ldots, x_n$, указанную аффинную функцию f можно записать в виде

$$f(x_1, \ldots, x_n) = a_0 + a_1 x_1 + \ldots + a_n x_n.$$

Для аффинных функций от переменных $x_1, \ldots, x_n$ над R естественным образом определяются операции сложения и умножения на элементы из R:

$$\begin{aligned}(a_0 + a_1 x_1 + \ldots + a_n x_n) + (b_0 + b_1 x_1 + \ldots + b_n x_n) = \\ = (a_0 + b_0) + (a_1 + b_1) x_1 + \ldots + (a_n + b_n) x_n;\end{aligned}$$

$$r(a_0 + a_1 x_1 + \ldots + a_n x_n) = (r a_0) + (r a_1) x_1 + \ldots + (r a_n) x_n.$$

Определение 2. *Системой линейных уравнений* с неизвестными $x_1, \ldots, x_n$ над кольцом R называется любая система уравнений вида

$$\begin{aligned} &f_1(x_1, \ldots, x_n) = g_1(x_1, \ldots, x_n), \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &f_m(x_1, \ldots, x_n) = g_m(x_1, \ldots, x_n), \end{aligned} \tag{1}$$

где $m \geqslant 1$, а $f_1, \ldots, f_m$, $g_1, \ldots, g_m$ — аффинные функции над R.

Определение 3. *Решением системы уравнений* (1) называется упорядоченный набор $\gamma = (c_1, \ldots, c_n)$ элементов из R при подстановке которых в уравнения вместо соответственно неизвестных $x_1, \ldots, x_n$ все уравнения системы (1) превращаются в верные равенства между элементами кольца R. В этом случае говорят также, что набор, или вектор, γ удовлетворяет системе уравнений (1).

Определение 4. Система уравнений над R называется *совместной*, или *разрешимой*, если она имеет хотя бы одно решение, *определенной*, если имеет ровно одно решение, и *неопределенной*, если имеет более одного решения. Система уравнений, не имеющая ни одного решения, называется *несовместной*.

Исследовать систему уравнений — значит выяснить, совместна она или нет, и если совместна, то — определена или нет. Решить систему — значит найти все ее решения.

Определение 5. Две системы уравнений над R с одними и теми же неизвестными называются *равносильными*, если множества их решений совпадают.

Для нахождения решений системы обычно стремятся предварительно преобразовать ее к какой-либо более простой системе, равносильной исходной системе. Так, например, очевидно, что, прибавив к обеим частям любого уравнения системы (1) произвольную аффинную функцию, мы получим систему, равносильную системе (1). Пользуясь такими преобразованиями, можно переносить слагаемые из одной части уравнения в другую (с изменением знака) и, в частности, привести любую систему линейных уравнений над R к равносильной ей системе уравнений вида

$$\begin{aligned} &a_{11}x_1 + \ldots + a_{1n}x_n = b_1, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &a_{m1}x_m + \ldots + a_{mn}x_n = b_m, \end{aligned} \tag{2}$$

где $a_{ij}, b_i \in R$ для всех $i \in \overline{1,m}$, $j \in \overline{1,n}$. Используя обозначения

$$A = (a_{ij})_{m\times n}, \quad \beta^{\downarrow} = \begin{pmatrix} b_1 \\ \ldots \\ b_m \end{pmatrix}, \quad x^{\downarrow} = \begin{pmatrix} x_1 \\ \ldots \\ x_n \end{pmatrix},$$

систему (2) записывают в матричной форме:

$$Ax^{\downarrow} = \beta^{\downarrow}. \tag{3}$$

При этом матрицы A и $B = (A, \beta^{\downarrow})$ называют соответственно *основной* и *расширенной матрицами* системы уравнений (3), а вектор $\beta^{\downarrow}$ — столбцом свободных членов. В связи с использованием матричной формы записи решение $\gamma = (c_1, \ldots, c_n)$ удобнее записывать в виде столбца и обозначать через $\gamma^{\downarrow}$.

В дальнейшем оказывается полезной следующая теорема о равносильности систем линейных уравнений.

Теорема 1. *Если U — обратимая $(m \times m)$-матрица над R, то система уравнений* (3) *равносильна системе*

$$(UA)x^{\downarrow} = U\beta^{\downarrow}. \tag{4}$$

□ Пусть $\gamma^{\downarrow}$ есть решение системы (3). Тогда $A\gamma^{\downarrow} = \beta^{\downarrow}$ — верное равенство. Умножив обе его части слева на матрицу U, получим верное равенство $(UA)\gamma^{\downarrow} = U\beta^{\downarrow}$, свидетельствующее о том, что $\gamma^{\downarrow}$ — решение системы (4). Таким образом, всякое решение системы (3) является решением системы (4). Аналогично, используя умножение на матрицу U^{-1}, можно доказать и обратное утверждение. Следовательно, системы (3) и (4) равносильны. □

Следствие. *Если матрицы $(A, \beta^{\downarrow})$ и $(C, \delta^{\downarrow})$ строчно эквивалентны, то система уравнений* (3) *равносильна системе*

$$Cx^{\downarrow} = \delta^{\downarrow}.$$

Применим теорему 1 к решению системы (3) в одном частном случае, когда $m = n$ и матрица A обратима.

Теорема 2 (Крамер).[8] *Если* (3) *есть система n линейных уравнений с n неизвестными над R и ее основная матрица A обратима, то система* (3) *имеет единственное решение $\gamma = (c_1, \ldots, c_n)$, где*

$$c_i = |A|^{-1}|A_i|, \quad i \in \overline{1, n}, \tag{5}$$

A_i — матрица, полученная из A заменой i-го столбца столбцом свободных членов $\beta^{\downarrow}$.

□ По теореме 1 система уравнений (3) в рассматриваемом случае равносильна системе

$$x^{\downarrow} = A^{-1}\beta^{\downarrow}, \tag{6}$$

которая, очевидно, имеет единственное решение. Найдем каждое неизвестное x_i отдельно. Для этого запишем равенство (6) более подробно, с использованием правила нахождения матрицы A^{-1}, указанного в доказательстве теоремы 11 главы 6:

$$\begin{pmatrix} x_1 \\ x_2 \\ \ldots \\ x_n \end{pmatrix} = |A|^{-1} \begin{pmatrix} A_{11} & A_{21} & \ldots & A_{n1} \\ A_{12} & A_{22} & \ldots & A_{n2} \\ \ldots & \ldots & \ldots & \ldots \\ A_{1n} & A_{2n} & \ldots & A_{nn} \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \ldots \\ b_n \end{pmatrix}. \tag{7}$$

[8] Г. Крамер (1704–1752) — швейцарский математик.

(Напомним, что здесь A_{ij} есть алгебраическое дополнение элемента a_{ij} матрицы A.) Приравнивая координаты векторов-столбцов из левой и правой частей равенства (7), получим:

$$x_i = |A|^{-1}(b_1A_{1i} + b_2A_{2i} + \ldots + b_nA_{ni}) = |A|^{-1}\Delta_i, \quad i \in \overline{1,n}.$$

Сравнивая Δ_i с разложением определителя матрицы A по ее i-му столбцу (см. следствие 1 теоремы 10 главы 6):

$$|A| = a_{1i}A_{1i} + a_{2i}A_{2i} + \ldots + a_{ni}A_{ni},$$

замечаем, что Δ_i есть определитель матрицы A_i. □

Равенства (5) называют *формулами Крамера*.

Таким образом, для нахождения решения системы (3) в рассматриваемом случае можно воспользоваться или формулами (5), для чего понадобится вычислить определители $n+1$ матриц n-го порядка, или формулой (6), для чего понадобится найти матрицу, обратную к A. Оба метода при достаточно больших n являются весьма сложными. В связи с этим теорема Крамера имеет, в основном, теоретическое значение.

§ 2. СИСТЕМЫ ЛИНЕЙНЫХ УРАВНЕНИЙ НАД ПОЛЕМ

Рассмотрим один из наиболее распространенных на практике методов решения систем линейных уравнений над полем, называемый *методом Гаусса*.

Пусть дана система уравнений (3) над произвольным полем. Если $A = O_{m\times n}$, то система совместна только при $\beta^{\downarrow} = 0^{\downarrow}$. При выполнении этого условия любой вектор из $P^{(n)}$ является ее решением. Далее считаем, что A — ненулевая матрица. Приведем расширенную матрицу $B = (A, \beta^{\downarrow})$ к специальному ступенчатому виду с помощью элементарных преобразований строк, что можно сделать согласно следствию 1 из теоремы 4 главы 7. Пусть при этом получилась матрица $C = (c_{ij})_{m\times(n+1)}$ типа $S(i_1, \ldots, i_r)$. Тогда по следствию из теоремы 1 система (3) равносильна системе уравнений

$$C'x^{\downarrow} = \gamma^{\downarrow}, \tag{8}$$

где $C' = (c_{ij})_{m\times n}$, а $\gamma^{\downarrow}$ — последний столбец матрицы C. В зависимости от значений параметров $r, i_1, \ldots, i_r$ возможны следующие три принципиально различных случая.

1. $i_r = n+1$. В этом случае по теореме 15 главы 7 столбец $\beta^{\downarrow}$ матрицы B не выражается линейно через столбцы матрицы A, и по теореме 7 главы 6 система уравнений (3) несовместна.

2. $i_r \leqslant n$, $r = n$. В этом случае матрица C имеет тип $S(1, 2, \ldots, n)$, а тогда по теореме 15 главы 7 и ее следствию 1 имеем:

$$\beta^{\downarrow} = A_1^{\downarrow}c_{1\,n+1} + \ldots + A_n^{\downarrow}c_{n\,n+1}$$

и система столбцов $A_1^{\downarrow}, \ldots, A_n^{\downarrow}$ линейно независима. Отсюда и из утверждения 11 главы 7 следует, что столбец $\gamma^{\downarrow}$ является единственным решением системы уравнений (3). Следовательно, в рассматриваемом случае система (3) совместна и определена.

3. $i_r \leqslant n$, $r < n$. Рассмотрим в этом случае подробнее систему уравнений (8). Удалив из нее все уравнения вида

$$0x_1 + \ldots + 0x_n = 0 \tag{9}$$

(если такие есть) и перенеся в оставшихся уравнениях все слагаемые, кроме $x_{i_1}, \ldots, x_{i_r}$ в правую часть, получим систему уравнений

$$\begin{aligned} x_{i_1} &= c_{1n+1} - c_{1i_{r+1}}x_{i_{r+1}} - \ldots - c_{1i_n}x_{i_n}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_{i_r} &= c_{rn+1} - c_{ri_{r+1}}x_{i_{r+1}} - \ldots - c_{ri_n}x_{i_n}, \end{aligned} \tag{10}$$

где $\{i_{r+1}, \ldots, i_n\} = \overline{1,n} \setminus \{i_1, \ldots, i_r\}$. Эта система, очевидно, равносильна системе (8). Подставляя в (10) вместо $x_{i_{r+1}}, \ldots, x_{i_n}$ произвольные элементы $a_{i_{r+1}}, \ldots, a_{i_n}$ поля P, мы однозначно определим значения $a_{i_1}, \ldots, a_{i_r}$ остальных неизвестных $x_{i_1}, \ldots, x_{i_r}$ так, что набор $(a_1, \ldots, a_n)$ будет решением системы (10). Нетрудно заметить, что каждое решение системы (10) можно получить указанным способом. Так как $r < n$, то система (10) (а потому и (3)) имеет в рассматриваемом случае более одного решения.

Анализируя случаи 1–3, нетрудно заметить, что они характеризуются следующими условиями:

1. $\operatorname{rang} C' < \operatorname{rang} C$,
2. $\operatorname{rang} C' = \operatorname{rang} C = n$,
3. $\operatorname{rang} C' = \operatorname{rang} C < n$.

Так как матрицы C' и C строчно эквивалентны соответственно матрицам A и $B = (A, \beta^{\downarrow})$, то, учитывая теорему 1 главы 7, можно сделать следующий вывод. При решении системы уравнений (3) методом Гаусса логически возможны следующие взаимно исключающие случаи:

1. $\operatorname{rang} A \neq \operatorname{rang} B$, система несовместна;
2. $\operatorname{rang} A = \operatorname{rang} B = n$, система совместна и определена;
3. $\operatorname{rang} A = \operatorname{rang} B < n$, система совместна и неопределена (при этом все ее решения однозначно определяются наборами значений лишь некоторых $n - r$ фиксированных неизвестных).

Отсюда получаем ответы на все основные вопросы, связанные с исследованием систем линейных уравнений над полем P.

Теорема 3 (критерий совместности). *Система линейных уравнений над полем совместна тогда и только тогда, когда ранг ее основной матрицы равен рангу расширенной матрицы.*

Эту теорему называют *теоремой Кронекера–Капелли* в честь немецкого математика Л. Кронекера (1823–1891) и итальянского математика А. Капелли (1855–1910).

Теорема 4 (критерий определенности). *Система линейных уравнений над полем имеет единственное решение тогда и только тогда, когда ранги основной и расширенной матриц системы равны числу ее неизвестных.*

Теорема 5. *Совместная и неопределенная система линейных уравнений над полем P имеет бесконечно много решений при бесконечном поле P и q^{n-r} решений при $|P| = q$, где n — число неизвестных, а r — ранг основной (и расширенной) матрицы системы.*

Рассмотрим еще метод решения систем линейных уравнений над полем, основанный на использовании ранговых подматриц матриц этих систем.

Пусть дана система (3) с основной матрицей A и расширенной матрицей $B = (A, \beta^{\downarrow})$ и известно, что $\operatorname{rang} A = \operatorname{rang} B = r$. Выберем в матрице A произвольную ранговую подматрицу

$$A' = A \begin{pmatrix} i_1, \ldots, i_r \\ j_1, \ldots, j_r \end{pmatrix}.$$

Так как $\operatorname{rang} B = r$ и A есть подматрица матрицы B, то A' является ранговой подматрицей и для матрицы B. Отсюда и из следствий 3 и 6 теоремы 15 главы 7 легко получить, что система строк $\vec{B}_{i_1}, \ldots, \vec{B}_{i_r}$ является базисом системы всех строк матрицы B. Поэтому матрицу B элементарными преобразованиями строк можно привести к матрице вида

$$B' = \begin{pmatrix} \vec{B}_{i_1} \\ \ldots \\ \vec{B}_{i_r} \\ \vec{0} \\ \ldots \\ \vec{0} \end{pmatrix} = \begin{pmatrix} a_{i_1 1} & \ldots & a_{i_1 n} & b_{i_1} \\ \ldots & \ldots & \ldots & \ldots \\ a_{i_r 1} & \ldots & a_{i_r n} & b_{i_r} \\ 0 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & 0 \end{pmatrix}.$$

Тогда по следствию теоремы 1 система (3) равносильна системе уравнений

$$A' x^{\downarrow} = \beta'^{\downarrow}, \tag{11}$$

где $\beta'^{\downarrow}$ — последний столбец матрицы B', а A' получена из B' удалением столбца $\beta'^{\downarrow}$. Удалив из системы (11) последние $m - r$ уравнений вида (9) и перенеся в оставшихся уравнениях в правые части все слагаемые, не содержащие неизвестных $x_{j_1}, \ldots, x_{j_r}$, получим систему из r уравнений, равносильную системе (3):

$$\begin{aligned} &a_{i_1 j_1} x_{j_1} + \ldots + a_{i_1 j_r} x_{j_r} = b_{i_1} - a_{i_1 j_{r+1}} x_{j_{r+1}} - \ldots - a_{i_1 j_n} x_{j_n}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &a_{i_r j_1} x_{j_1} + \ldots + a_{i_r j_r} x_{j_r} = b_{i_r} - a_{i_r j_{r+1}} x_{j_{r+1}} - \ldots - a_{i_r j_n} x_{j_n}, \end{aligned} \tag{12}$$

в которой $\{j_{r+1}, \ldots, j_n\} = \overline{1, n} \setminus \{j_1, \ldots, j_r\}$.

Подставив в (12) вместо $x_{j_{r+1}}, \ldots, x_{j_n}$ произвольные элементы из P, мы получим систему из r уравнений с r неизвестными $x_{j_1}, \ldots, x_{j_r}$, которая по теореме Крамера имеет единственное решение $x_{j_1} = a_{j_1}, \ \ldots, \ x_{j_r} = a_{j_r}$. В итоге мы найдем решение $(a_1, \ldots, a_n)$ системы (12) (а потому и системы (3)). Легко видеть, что таким образом можно получить все решения системы (12). Действительно, если $\gamma = (c_1, \ldots, c_n)$ — любое решение системы (12), то, заменив в (12) x_i на c_i при всех $i \in \overline{1, n}$, получим систему верных равенств, которая свидетельствует о том, что $c_{j_1}, \ldots, c_{j_r}$ есть решение системы, полученной из (12) заменой $x_{j_{r+1}}, \ldots, x_{j_n}$ соответственно элементами $c_{j_{r+1}}, \ldots, c_{j_n}$.

Замечание 1. Вместо того, чтобы решать методом Крамера все системы уравнений, получаемые из (12) заменой $x_{j_{r+1}}, \ldots, x_{j_n}$ всевозможными элементами поля P, можно решить методом Крамера саму систему (12), считая $x_{j_{r+1}}, \ldots, x_{j_n}$ параметрами со значениями из поля P. В итоге неизвестные $x_{j_1}, \ldots, x_{j_r}$ будут представлены в виде аффинных функций от переменных $x_{j_{r+1}}, \ldots, x_{j_n}$. Придавая последним произвольные значения из P и вычисляя соответствующие значения неизвестных $x_{j_1}, \ldots, x_{j_r}$, получим все решения системы (12), а значит и системы (3).

Замечание 2. Набор неизвестных $x_{j_{r+1}}, \ldots, x_{j_n}$ из правых частей уравнений системы (12) называют *системой свободных неизвестных* системы уравнений (3). В общем случае система свободных неизвестных для системы (3) находится неоднозначно и определяется выбором ранговой подматрицы в матрице A.

§ 3. СИСТЕМЫ ЛИНЕЙНЫХ ОДНОРОДНЫХ УРАВНЕНИЙ

Определение 6. Система линейных уравнений называется *системой линейных однородных уравнений*, если ее столбец свободных членов является нулевым вектором.

Произвольной системе линейных уравнений (3) можно поставить в соответствие систему линейных однородных уравнений

$$Ax^{\downarrow} = 0^{\downarrow}, \tag{13}$$

заменив в (3) столбец свободных членов $\beta^{\downarrow}$ нулевым столбцом $0^{\downarrow}$. Полученная система (13) называется *ассоциированной* с системой (3).

Заметим, что любая система линейных однородных уравнений совместна, поскольку имеет нулевое решение $0^{\downarrow} = (0, \ldots, 0)^T$.

В теории систем линейных уравнений системы однородных уравнений играют важную роль вследствие особых свойств их решений и существующей простой связи между решениями произвольной системы линейных уравнений и ассоциированной с ней системы линейных однородных уравнений.

Теорема 6. *Множество M решений системы линейных однородных уравнений* (13) *с n неизвестными над полем P является подпространством пространства $P^{(n)}$ и* $\dim M = n - \operatorname{rang} A$.

□ Если $\alpha^{\downarrow}, \beta^{\downarrow} \in M$, то $A\alpha^{\downarrow} = 0^{\downarrow}$, $A\beta^{\downarrow} = 0^{\downarrow}$ — верные равенства. Отсюда получаем:

$$A(\alpha^{\downarrow} + \beta^{\downarrow}) = A\alpha^{\downarrow} + A\beta^{\downarrow} = 0^{\downarrow} + 0^{\downarrow} = 0^{\downarrow},$$
$$A(\alpha^{\downarrow} r) = (A\alpha^{\downarrow}) \cdot r = 0^{\downarrow} \cdot r = 0^{\downarrow}, \quad r \in P.$$

Следовательно, $\alpha^{\downarrow} + \beta^{\downarrow}$, $\alpha^{\downarrow} \cdot r \in M$, и, согласно определению 11 главы 7, M — подпространство пространства $P^{(n)}$. Найдем базис пространства M. Если $\operatorname{rang} A = n$, то по теореме 4 система (13) имеет единственное решение — нулевое, и базисом пространства M является пустая система векторов. Следовательно, в этом случае $\dim M = 0 = n - \operatorname{rang} A$, и утверждение теоремы 6 о размерности пространства M

верно. Если же $\operatorname{rang} A = r < n$, то, как и в общем случае, решая систему (13) с помощью ранговых подматриц, получим равносильную ей систему уравнений вида (12) при $b_{i_1} = \ldots = b_{i_r} = 0$. Все решения системы (12) находятся известным способом. Придадим ее свободным неизвестным $x_{j_{r+1}}, \ldots, x_{j_n}$ произвольные значения из P:

$$x_{j_{r+1}} = c_{j_{r+1}},\ \ldots,\ x_{j_n} = c_{j_n},$$

и по ним однозначно найдем значения остальных неизвестных:

$$x_{j_1} = c_{j_1},\ \ldots,\ x_{j_r} = c_{j_r}.$$

Расположив элементы $c_{j_1}, \ldots, c_{j_n}$ так, чтобы их индексы шли в порядке возрастания, получим решение системы (12): $\gamma^{\downarrow} = (c_1, \ldots, c_n)^T$. Подчеркнем особо, что все координаты вектора $\gamma^{\downarrow}$, как и любого решения системы (12), однозначно определяются значениями свободных неизвестных $x_{j_{r+1}}, \ldots, x_{j_n}$. Найдем указанным образом $n - r$ решений, придавая поочередно одному из свободных неизвестных значение e, а остальным — нуль. Значения неизвестных $x_1, \ldots, x_n$ (т. е. координаты) в полученных решениях

$$\gamma_1^{\downarrow},\ \gamma_2^{\downarrow},\ \ldots,\ \gamma_{n-r}^{\downarrow} \tag{14}$$

запишем в следующую таблицу:

Решения	Значения неизвестных						
	x_{j_1}	$\ldots$	x_{j_r}	$x_{j_{r+1}}$	$x_{j_{r+2}}$	$\ldots$	x_{j_n}
$\gamma_1^{\downarrow}$	c_{1j_1}	$\ldots$	c_{1j_r}	e	0	$\ldots$	0
$\gamma_2^{\downarrow}$	c_{2j_1}	$\ldots$	c_{2j_r}	0	e	$\ldots$	0
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$		$\ldots$	
$\gamma_{n-r}^{\downarrow}$	$c_{n-r\,j_1}$	$\ldots$	$c_{n-r\,j_r}$	0	0	$\ldots$	e

Из таблицы видно, что в матрице C, составленной из столбцов (14), минор $M_C\binom{j_{r+1}, \ldots,\ j_n}{1,\ \ldots, n-r}$ отличен от 0. Тогда по следствию 3 из теоремы 15 главы 7 система векторов (14) линейно независима. Покажем, что она является базисом пространства M. Для этого остается показать, что любой вектор из M является линейной комбинацией векторов (14). Пусть $\alpha^{\downarrow} = (a_1, a_2, \ldots, a_n)^T \in M$, т. е. $\alpha^{\downarrow}$ — решение системы (12). Рассмотрим следующую линейную комбинацию векторов (14):

$$\gamma^{\downarrow} = \gamma_1^{\downarrow} a_{j_{r+1}} + \gamma_2^{\downarrow} a_{j_{r+2}} + \ldots + \gamma_{n-r}^{\downarrow} a_{j_n}.$$

Так как M — пространство и $\gamma_1^{\downarrow}, \ldots, \gamma_{n-r}^{\downarrow} \in M$, то $\gamma^{\downarrow} \in M$, т. е. $\gamma^{\downarrow}$ — решение системы (12). Из таблицы видно, что в решении $\gamma^{\downarrow}$ значения неизвестных $x_{j_{r+1}}, \ldots, x_{j_n}$ равны соответственно $a_{j_{r+1}}, \ldots, a_{j_n}$. Таким образом, в решениях $\alpha^{\downarrow}$ и $\gamma^{\downarrow}$ системы (12) значения свободных неизвестных одни и те же. А так как значения свободных неизвестных однозначно определяют решения, то $\alpha^{\downarrow} = \gamma^{\downarrow}$, и значит, $\alpha^{\downarrow}$ есть линейная комбинация системы векторов (14). $\square$

Определение 7. Система решений системы линейных однородных уравнений называется ее *фундаментальной системой решений* (ФСР), если она является базисом пространства всех ее решений.

Так, например, (14) является фундаментальной системой решений системы уравнений (13). В общем случае ФСР находится неоднозначно. Даже в указанном выше способе нахождения ФСР системы уравнений (13) имеется большой произвол. Он связан и с выбором ранговой подматрицы матрицы A, а значит, и системы свободных неизвестных, и с выбором значений для свободных неизвестных. Вместе с тем, из теоремы 6 и теоремы 16 главы 7 имеем

Следствие 1. *Любая система линейных однородных уравнений имеет ФСР, и любая ее ФСР содержит ровно $n - r$ векторов, где n — число неизвестных, а r — ранг основной матрицы заданной системы уравнений.*

Следствие 2. *Если $\alpha_1^{\downarrow}, \ldots, \alpha_{n-r}^{\downarrow}$ — любая ФСР системы линейных однородных уравнений, то множество всех решений системы совпадает с множеством векторов*

$$M = \{\alpha_1^{\downarrow} c_1 + \ldots + \alpha_{n-r}^{\downarrow} c_{n-r} : \ c_1, \ldots, c_{n-r} \in P\}.$$

При этом выражение

$$\alpha_1^{\downarrow} c_1 + \ldots + \alpha_{n-r}^{\downarrow} c_{n-r} \tag{15}$$

называют *общим решением системы* (13).

Теорема 7. *Множество M всех решений произвольной совместной системы линейных уравнений представляется в виде*

$$M = \alpha^{\downarrow} + M_0,$$

где $\alpha^{\downarrow}$ — любое одно ее решение, а M_0 — множество всех решений ассоциированной с ней системы линейных однородных уравнений.

□ Пусть $\alpha^{\downarrow}$ — любое решение, M — множество всех решений системы (3), M_0 — множество всех решений ассоциированной с ней системы (13). Докажем включения

$$\alpha^{\downarrow} + M_0 \subset M, \quad M \subset \alpha^{\downarrow} + M_0.$$

Пусть $\gamma^{\downarrow} \in \alpha^{\downarrow} + M_0$, т. е. $\gamma^{\downarrow} = \alpha^{\downarrow} + \delta^{\downarrow}$, где $\delta^{\downarrow}$ — подходящий вектор из M_0. Тогда имеем

$$A\gamma^{\downarrow} = A(\alpha^{\downarrow} + \delta^{\downarrow}) = A\alpha^{\downarrow} + A\delta^{\downarrow} = \beta^{\downarrow} + 0^{\downarrow} = \beta^{\downarrow}.$$

Значит, $\gamma^{\downarrow} \in M$, и потому $\alpha^{\downarrow} + M_0 \subset M$.

Пусть $\gamma^{\downarrow} \in M$, т. е. $A\gamma^{\downarrow} = \beta^{\downarrow}$. Тогда

$$A(\gamma^{\downarrow} - \alpha^{\downarrow}) = A\gamma^{\downarrow} - A\alpha^{\downarrow} = \beta^{\downarrow} - \beta^{\downarrow} = 0^{\downarrow},$$

и потому $\gamma^{\downarrow} - \alpha^{\downarrow} \in M_0$. Следовательно, $\gamma^{\downarrow} \in \alpha^{\downarrow} + M_0$ и $M \subset \alpha^{\downarrow} + M_0$. □

Если $\alpha^{\downarrow}$ — решение системы (3), а (15) есть общее решение ассоциированной с ней системы (13), то, как следует из теоремы 7, множество M всех решений системы (3) можно записать в виде

$$M = \{\alpha^{\downarrow} + \alpha_1^{\downarrow}c_1 + \ldots + \alpha_{n-r}^{\downarrow}c_{n-r} : \ c_1, \ldots, c_{n-r} \in P\}.$$

В связи с этим выражение

$$\alpha^{\downarrow} + \alpha_1^{\downarrow}c_1 + \ldots + \alpha_{n-r}^{\downarrow}c_{n-r}$$

называют *общим решением* системы (3).

ЗАДАЧИ

1. Уравнение с неизвестными $x_1, \ldots, x_n$ называют *следствием совместной системы уравнений* с теми же неизвестными, если ему удовлетворяют все решения этой системы. Докажите, что уравнение $a_1x_1 + \ldots + a_nx_n = b$ является следствием совместной системы $Ax^{\downarrow} = \beta^{\downarrow}$ тогда и только тогда, когда вектор $(a_1, \ldots, a_n, b)$ является линейной комбинацией строк матрицы $(A, \beta^{\downarrow})$. Сформулируйте основанный на этом утверждении критерий равносильности систем уравнений.

2. Докажите, что совместные системы уравнений

$$A_{m\times n}x^{\downarrow} = \beta^{\downarrow}, \quad C_{m\times n}x^{\downarrow} = \delta^{\downarrow}$$

равносильны тогда и только тогда, когда матрицы $(A, \beta^{\downarrow})$ и $(C, \delta^{\downarrow})$ строчно эквивалентны.

3. Приведите примеры систем линейных уравнений, в которых одно из переменных:

а) не может быть включено ни в какую систему свободных неизвестных;

б) входит в любую систему свободных неизвестных;

в) входит в одну систему свободных неизвестных и не входит в какую-либо другую систему свободных неизвестных.

4. Сколько решений может иметь система из $n-1$ линейных уравнений с n неизвестными над полем $GF(2)$?

5. Дайте геометрическую интерпретацию для системы трех линейных уравнений с тремя неизвестными над полем $\mathbb{R}$ и множества ее решений при всех возможных значениях рангов основной и расширенной матриц.

6. Оцените сверху сложность решения системы n линейных уравнений с n неизвестными над полем P методом Гаусса, понимая под сложностью число всех арифметических операций над элементами поля P.

7. Докажите следующее обобщение теоремы Кронекера–Капелли: матричная система уравнений $AX = B$ совместна тогда и только тогда, когда $\operatorname{rang}(A, B) = \operatorname{rang} A$.

8. Сколько фундаментальных систем решений имеет система линейных уравнений $A_{m\times n}x^{\downarrow} = 0^{\downarrow}$ над полем P, если $\operatorname{rang} A = r$, и как все их найти?

9. Пусть $\alpha^{\downarrow}$ — решение системы линейных уравнений $Ax^{\downarrow} = \beta^{\downarrow}$, где $\beta^{\downarrow} \neq 0^{\downarrow}$, и $\alpha_1^{\downarrow}, \ldots, \alpha_r^{\downarrow}$ — ФСР системы уравнений $Ax^{\downarrow} = 0^{\downarrow}$. Докажите, что система векторов $\alpha, \alpha_1^{\downarrow}, \ldots, \alpha_r^{\downarrow}$ линейно независима.

10. Докажите, что любое подпространство M пространства $P^{(n)}$ совпадает с множеством всех решений подходящей системы однородных линейных уравнений.

11. Докажите, что для любой линейно независимой системы векторов $\alpha, \alpha_1^{\downarrow}, \ldots, \alpha_r^{\downarrow}$ из $P^{(n)}$ существуют матрица $A_{(n-r)\times n}$ ранга $n - r$ и вектор $\beta^{\downarrow} \in P^{(n)}$ такие, что $\alpha^{\downarrow} + \alpha_1^{\downarrow} c_1 + \ldots + \alpha_r^{\downarrow} c_r$ есть общее решение системы уравнений $Ax^{\downarrow} = \beta^{\downarrow}$.

Глава 9

МНОГОЧЛЕНЫ

Как читатель уже заметил, один из основных методов алгебры состоит в том, что решение какой-либо задачи для данного алгебраического объекта сводится к решению более простой задачи для другого алгебраического объекта, определенным образом построенного из исходного. Например, решение системы линейных уравнений над кольцом R сводится к решению простейшего уравнения над кольцом матриц $R_{n,n}$, решение сравнения над $\mathbb{Z}$ сводится к решению уравнения над кольцом вычетов $\mathbb{Z}_m$. В связи с этим, в алгебре много внимания уделяется различным способам конструирования из данных алгебраических объектов новых объектов и изучению свойств последних.

В этой главе изучается еще одна важная конструкция подобного типа — кольцо многочленов над данным кольцом. К необходимости использования и изучения понятия многочлена приводят многие алгебраические задачи. Простейшая (по формулировке) и древнейшая из них — задача о решении уравнения вида

$$a_n x^n + \ldots + a_1 x + a_0 = 0$$

над данным кольцом. Этим, однако, далеко не исчерпывается область приложений многочленов в алгебре. Как читатель увидит далее, с помощью многочленов описываются преобразования колец и полей, изучаются свойства матриц, из исходных полей строятся различные новые поля с заданными свойствами и решаются многие другие задачи.

Читатель уже знаком с понятием многочлена из средней школы. Однако мы начнем изложение теории многочленов с их формального определения, которое, на первый взгляд, может показаться неестественным и неудобным, но в действительности позволяет наиболее экономным способом добиться нужной строгости и перейти к общепринятой терминологии.

§ 1. КОЛЬЦО МНОГОЧЛЕНОВ НАД КОЛЬЦОМ С ЕДИНИЦЕЙ

1. Пусть R — произвольное кольцо с единицей e.

Определение 1. *Многочленом* над R назовем любую бесконечную последовательность

$$(a_i) = (a_0, a_1, \ldots, a_n, \ldots) \tag{1}$$

элементов $a_i \in R$, $i \in \mathbb{N}_0$, в которой все a_i, за исключением конечного их числа, равны нулю. Элементы a_i назовем *коэффициентами* многочлена (1). Многочлен $(0) = (0, 0, \ldots)$ назовем *нулевым*. Обозначим через $M(R)$ множество всех таких последовательностей.

Определение 2. а) *Суммой многочленов* (a_i), $(b_i) \in M(R)$ называют последовательность

$$(c_i) = (a_i) + (b_i), \tag{2}$$

в которой $c_i = a_i + b_i$ для каждого $i \in \mathbb{N}_0$.

б) *Произведением многочленов* (a_i) и (b_i) называют последовательность

$$(d_i) = (a_i) \cdot (b_i), \tag{3}$$

в которой $d_i = \sum\limits_{k=0}^{i} a_k b_{i-k}$ для всех $i \in \mathbb{N}_0$.

в) *Произведением многочлена* $(a_i) \in M(R)$ *на элемент* $r \in R$ слева или справа называют, соответственно, последовательность

$$r(a_i) = (ra_0, ra_1, \ldots) \quad \text{или} \quad (a_i)r = (a_0 r, a_1 r, \ldots). \tag{4}$$

г) *Суммой элемента* $r \in R$ *и многочлена* $(a_i) \in M(R)$ называют последовательность

$$r + (a_i) = (a_i) + r = (a_0 + r, a_1, \ldots, a_n, \ldots). \tag{5}$$

Нетрудно видеть, что в последовательностях (2)–(5), так же как и в исходных последовательностях, все коэффициенты, за исключением конечного их числа, равны нулю, и потому эти последовательности принадлежат $M(R)$.

Замечание 1. Операции сложения, введенные в пунктах а) и г) определения 2, различны, хотя для удобства и обозначаются одним и тем же символом $+$. Последнее обстоятельство не может вызвать путаницы, поскольку природа суммируемых элементов ясно указывает на то, какая из операций имеется в виду. Кроме того, различие между этими операциями имеет, по существу, лишь формальный характер, поскольку операция из пункта г) легко выражается через операцию из пункта а):

$$r + (a_i) = (r, 0, \ldots, 0, \ldots) + (a_i).$$

Используя заданные на $M(R)$ операции, можно следующим образом перейти к традиционной форме записи многочленов. Введем обозначения:

$$x = (0, e, 0, \ldots, 0, \ldots), \tag{6}$$

$$x^i = (\overbrace{0, \ldots, 0}^{i \text{ нулей}}, e, 0, \ldots) \quad \text{для } i \in \mathbb{N}_0. \tag{7}$$

Заметим, что ввиду определения 2 б) для любых $i, k \in \mathbb{N}_0$ выполняются равенства

$$x^i x^k = (\overbrace{0, \ldots, 0}^{i}, e, 0, \ldots) \cdot (\overbrace{0, \ldots, 0}^{k}, e, 0, \ldots) = (\overbrace{0, \ldots, 0}^{i+k}, e, 0, \ldots) = x^{i+k}.$$

Поэтому для любых $i, j, k \in \mathbb{N}_0$ верны равенства

$$(x^i \cdot x^j) \cdot x^k = x^{i+j+k} = x^i \cdot (x^j \cdot x^k), \tag{8}$$

т. е. операция умножения на множестве $X = \{x^i : i \in \mathbb{N}_0\}$ ассоциативна, и для $i \in \mathbb{N}$ символ x^i обозначает не что иное, как i-ю степень элемента x:

$$x^i = x \cdot x \cdot \ldots \cdot x.$$

Пользуясь определением 2 в), получаем, что для любых $a \in R$ и $i \in \mathbb{N}_0$ верны равенства

$$ax^i = (0, \ldots, 0, a, 0, \ldots) = x^i a,$$

и поэтому любой многочлен $(a_i) = (a_0, \ldots, a_n, 0, \ldots) \in M(R)$ может быть записан в виде суммы:

$$(a_i) = (a_0, 0, \ldots) + (0, a_1, 0, \ldots) + \ldots + (0, \ldots, 0, a_n, 0, \ldots) =$$
$$= a_0 x^0 + a_1 x^1 + \ldots + a_n x^n = \sum_{i=0}^{n} a_i x^i.$$

Пользуясь замечанием 1 и обозначением (6), последнюю запись многочлена (a_i) можно еще упростить, записав его в общепринятом виде:

$$a(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n. \tag{9}$$

Определение 3. При введенных обозначениях многочлен (9) называют *многочленом от x над кольцом R*, а элементы $a_i \in R$ называют его коэффициентами. Говорят, что a_i — *коэффициент многочлена* $a(x)$ при x^i, а a_0 — его *свободный член*. Множество $M(R)$ называют множеством *многочленов от одного переменного* x над кольцом R и обозначают

$$M(R) = R[x].$$

Замечание 2. Подчеркнем, что многочлен $a(x) \in R[x]$ вида (9) имеет бесконечно много коэффициентов a_i, $i \in \mathbb{N}_0$, а равенство (9) означает, что $a_{n+1} = a_{n+2} = \ldots = 0$. При этом возможно, что и $a_n = 0$. Согласно определениям 1 и 3, многочлен (9) равен многочлену

$$b(x) = b_0 + b_1 x + \ldots + b_m x^m \tag{10}$$

тогда и только тогда, когда $a_i = b_i$ для всех $i \in \mathbb{N}_0$.

Определение 4. *Степенью многочлена* $a(x) \in R[x]$ называют параметр $\deg a(x)$, равный наибольшему из номеров i его ненулевых коэффициентов a_i, если $a(x) \neq 0$, и равный $-\infty$, если $a(x) = 0$. Если $\deg a(x) = n \in \mathbb{N}_0$, то коэффициент a_n многочлена $a(x)$ называют его *старшим коэффициентом*, а слагаемое $a_n x^n$ — *старшим членом* многочлена $a(x)$ и обозначают через $\mathrm{Ст}(a(x))$: $a_n x^n = \mathrm{Ст}(a(x))$.

Как нетрудно увидеть из определений 2 а), б), сумма и произведение многочленов (9) и (10) могут быть записаны следующим образом:

$$a(x)+b(x)=\sum_{i=0}^{t}(a_i+b_i)\,x^i,\quad t=\max\{m,n\};$$
$$a(x)\cdot b(x)=a_0b_0+(a_0b_1+a_1b_0)\,x+\ldots+(a_{n-1}b_m+a_nb_{m-1})\,x^{m+n-1}+a_nb_mx^{m+n}.$$

Отсюда легко следует (проверьте)

Утверждение 1. *Для любых многочленов* $a(x),b(x)\in R[x]$:

(а) $\deg(a(x)+b(x))\leqslant\max\{\deg a(x),\deg b(x)\}$, *причем последнее неравенство является строгим тогда и только тогда, когда*

$$\mathrm{Ст}(a(x))=-\,\mathrm{Ст}(b(x));$$

(б) $\deg(a(x)\cdot b(x))\leqslant\deg a(x)+\deg b(x)$, *причем последнее неравенство обращается в равенство тогда и только тогда, когда либо один из многочленов* $a(x)$, $b(x)$ *равен* $0x^0$, *либо произведение их старших коэффициентов отлично от нуля*;

(в) *если в кольце* R *нет делителей нуля (в частности, если* R *— поле), то*

$$\deg(a(x)\cdot b(x))=\deg a(x)+\deg b(x).$$

Иногда, при проведении формальных выкладок, многочлен $a(x)$ вида (9) удобно бывает записывать в виде следующей формально бесконечной суммы:

$$a(x)=\sum_{i\geqslant0}a_ix^i=\sum_{i=0}^{\infty}a_ix^i.$$

При этом надо лишь помнить, что в действительности выписанная сумма конечна, поскольку для некоторого $n\in\mathbb{N}_0$ все ее слагаемые a_ix^i с номерами $i>n$ есть нулевые многочлены. При такой форме записи сумма и произведение многочленов $a(x)=\sum_{i\geqslant0}a_ix^i$ и $b(x)=\sum_{i\geqslant0}b_ix^i$ имеют более простой вид:

$$a(x)+b(x)=\sum_{i\geqslant0}(a_i+b_i)\,x^i,\quad a(x)\cdot b(x)=\sum_{i\geqslant0}\left(\sum_{k=0}^{i}a_kb_{i-k}\right)x^i.\tag{11}$$

2. Докажем основной результат данного параграфа.

Теорема 2. *Алгебра* $(R[x],+,\cdot)$ *многочленов над кольцом* R *с единицей есть кольцо с единицей. Кольцо* $R[x]$ *коммутативно тогда и только тогда, когда кольцо* R *коммутативно, и содержит делители нуля тогда и только тогда, когда* R *содержит делители нуля.*

□ Так как $(R,+)$ — абелева группа, то, пользуясь определением 2 а), легко проверить, что $(R[x],+)$ — абелева группа с нулем $0x^0$, в которой противоположным для элемента $a(x)=\sum_{i\geqslant 0}a_ix^i$ является элемент

$$-a(x)=\sum_{i\geqslant 0}(-a_i)\,x^i.$$

Докажем дистрибутивность умножения относительно сложения на $R[x]$. Пусть $c(x)=a(x)\cdot b(x)$ и $b(x)=f(x)+g(x)$. Тогда $b_k=f_k+g_k$ для $k\in\mathbb{N}_0$, и для коэффициентов многочлена $c(x)$ из (11) следуют равенства

$$c_i=\sum_{k=0}^{i}a_{i-k}b_k=\sum_{k=0}^{i}a_{i-k}f_k+\sum_{k=0}^{i}a_{i-k}g_k.$$

Поэтому, если $a(x)f(x)=\sum_{i\geqslant 0}u_ix^i$ и $a(x)g(x)=\sum_{i\geqslant 0}v_ix^i$, то $c_i=u_i+v_i$ для всех $i\in\mathbb{N}_0$, т. е. $a(x)\cdot(f(x)+g(x))=a(x)\cdot f(x)+a(x)\cdot g(x)$.

Левая дистрибутивность доказана. Правая дистрибутивность доказывается аналогично.

С использованием свойств дистрибутивности и соотношений (8), ассоциативность умножения в $R[x]$ доказывается следующим образом. Если $a(x)$, $b(x)$, $c(x)\in R[x]$, то

$$(a(x)\,b(x))\,c(x)=\left(\sum_{i\geqslant 0}a_ix^i\cdot\sum_{j\geqslant 0}b_jx^j\right)\sum_{k\geqslant 0}c_kx^k=\sum_{i\geqslant 0}\sum_{j\geqslant 0}\sum_{k\geqslant 0}(a_ib_j)c_kx^{i+j+k}.$$

Так как $(a_ib_j)c_k=a_i(b_jc_k)$ ввиду ассоциативности умножения в R, то последнюю сумму можно переписать следующим образом:

$$\begin{aligned}(a(x)\,b(x))\,c(x)&=\sum_{i\geqslant 0}\sum_{j\geqslant 0}\sum_{k\geqslant 0}a_i(b_jc_k)x^{i+j+k}=\\&=\sum_{i\geqslant 0}a_ix^i\left(\sum_{j\geqslant 0}\sum_{k\geqslant 0}b_jc_kx^{j+k}\right)=\\&=\sum_{i\geqslant 0}a_ix^i\left(\sum_{j\geqslant 0}b_jx^j\cdot\sum_{k\geqslant 0}c_kx^k\right)=a(x)\,(b(x)\,c(x)).\end{aligned}$$

Таким образом, $(R[x],+,\cdot)$ — кольцо.

Единицей в $R[x]$, очевидно, является многочлен x^0. Если кольцо R коммутативно, то коммутативность $R[x]$ доказывают равенства

$$a(x)\cdot b(x)=\sum a_ib_jx^{i+j}=\sum b_ja_ix^{j+i}=b(x)\cdot a(x).$$

Если же $ab\neq ba$ для некоторых $a,b\in R$, то в $R[x]$ не коммутируют многочлены ax^0 и bx^0.

Если в R нет делителей нуля, то по утверждению 1(в) для любых ненулевых многочленов $a(x),b(x)\in R[x]$ справедливы соотношения

$$\deg(a(x)\cdot b(x))=\deg a(x)+\deg b(x)\geqslant 0$$

и потому $a(x) \cdot b(x) \neq 0x^0$. Наоборот, если $a, b \in R \setminus \{0\}$ таковы, что $ab = 0$, то ax^0 и bx^0 — делители нуля в $R[x]$. $\square$

В дальнейшем нуль и единицу в кольце $R[x]$ мы, для краткости, будем обозначать теми же символами, которые приняты для их обозначения в кольце R, т. е. положим

$$0x^0 = 0, \quad x^0 = e.$$

Замечание 3. Последнее соглашение позволяет, по сути дела, отождествить произвольный элемент $r = re$ из кольца R с многочленом $rx^0 = (r, 0, 0, \ldots)$. Такое отождествление весьма естественно, поскольку очевидно, что множество $\overline{R} = \{rx^0 : r \in R\}$ есть подкольцо в $R[x]$, изоморфное кольцу R, и изоморфизм $R \to \overline{R}$ задается как раз соответствием $r \to rx^0$. Таким образом, везде, где это удобно, можно считать, что кольцо R есть подкольцо в кольце $R[x]$. Строгая формальная конструкция, позволяющая рассматривать R как подкольцо в $R[x]$, будет изложена позже в § 8 главы 20.

§ 2. ДЕЛИМОСТЬ МНОГОЧЛЕНОВ. ТЕОРЕМА О ДЕЛЕНИИ С ОСТАТКОМ

Определение 5. Говорят, что элемент a кольца S *делится на элемент* $b \in S$ *слева* (*справа*), если в S разрешимо уравнение

$$bx = a \quad (yb = a).$$

Как уже отмечалось, если S — кольцо с единицей и элемент b обратим в S, то каждое из этих уравнений имеет единственное решение: $b^{-1}a$ и ab^{-1} соответственно. Если же $b \notin S^*$, то даже нет алгоритма, позволяющего проверить разрешимость этих уравнений для произвольного бесконечного кольца S.

Однако если $S = R[x]$ — кольцо многочленов над кольцом R с единицей, то в S можно ввести понятие делимости с остатком (которое уже встречалось читателю при изучении кольца целых чисел) и предложить алгоритм, который во многих важных случаях позволяет проверить, делится один многочлен на другой или нет.

Определение 6. Говорят, что в кольце $R[x]$ *многочлен* $a(x)$ *делится на многочлен* $b(x)$ *справа с остатком*, если существуют многочлены $q_{\text{П}}(x)$, $r_{\text{П}}(x) \in R[x]$ со свойствами

$$a(x) = q_{\text{П}}(x)b(x) + r_{\text{П}}(x), \quad \deg r_{\text{П}}(x) < \deg b(x). \tag{12}$$

При этом многочлены $q_{\text{П}}(x)$ и $r_{\text{П}}(x)$ называют, соответственно, *неполным правым частным* и *правым остатком* от деления $a(x)$ на $b(x)$. Аналогично определяются понятие *делимости* $a(x)$ *на* $b(x)$ *слева с остатком* и *неполное левое частное* $q_{\text{Л}}(x)$ и *левый остаток* $r_{\text{Л}}(x)$ как многочлены, удовлетворяющие соотношениям

$$a(x) = b(x)q_{\text{Л}}(x) + r_{\text{Л}}(x), \quad \deg r_{\text{Л}}(x) < \deg b(x).$$

Иногда, для краткости, многочлен $q_{\text{П}}(x)$ ($q_{\text{Л}}(x)$) называют просто правым (левым) частным от деления с остатком $a(x)$ на $b(x)$.

Замечание 4. Вообще говоря, деление с остатком в $R[x]$ не всегда возможно, а когда возможно, то не всегда однозначно. Например, если $R = P_{2\times 2}$ — кольцо 2×2-матриц над полем P, то многочлен $a(x) = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)x + \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) \in P[x]$ можно разделить справа с остатком на многочлен $b(x) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)x + \left(\begin{smallmatrix} 0 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ по крайней мере двумя способами:

$$a(x) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot b(x) + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad a(x) = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \cdot b(x) + \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}.$$

При этом $a(x)$ нельзя разделить на $b(x)$ с остатком слева (докажите).

Однако отмеченная неопределенность исчезает при некоторых ограничениях на многочлен $b(x)$.

Теорема 3. *Если старший коэффициент многочлена $b(x) \in R[x] \setminus \{0\}$ обратим в кольце R, то любой многочлен $a(x) \in R[x]$ можно разделить справа (слева) с остатком на $b(x)$. При этом правые (левые) неполное частное и остаток определяются однозначно.*

□ Если $\deg a(x) < \deg b(x)$, то соотношения (12) выполняются при $q_{\text{П}}(x) = 0$, $r_{\text{П}}(x) = a(x)$. Пусть $\text{Ст}(a(x)) = a_m x^m$, $\text{Ст}(b(x)) = b_n x^n$ и $m \geqslant n$. Так как по условию $b_n \in R^*$, то в $R[x]$ существует многочлен $a_m b_n^{-1} x^{m-n} \cdot b(x)$. Нетрудно видеть, что его старший член равен $a_m x^m$. Поэтому многочлен

$$a_1(x) = a(x) - a_m b_n^{-1} x^{m-n} b(x)$$

имеет степень $m_1 < m$. Если $m_1 < n$, то мы уже разделили $a(x)$ на $b(x)$ с остатком справа:

$$a(x) = (a_m b_n^{-1} x^{m-n}) \cdot b(x) + a_1(x).$$

Если же $m_1 \geqslant n$ и $\text{Ст}(a_1(x)) = a_{m_1}^{(1)} x^{m_1}$, то строим многочлен

$$a_2(x) = a_1(x) - a_{m_1}^{(1)} b_n^{-1} x^{m_1-n} b(x).$$

Ясно, что $\deg a_2(x) = m_2 < m_1$, и справедливо соотношение

$$a(x) = \big(a_m b_n^{-1} x^{m-n} + a_{m_1}^{(1)} b_n^{-1} x^{m_1-n}\big) b(x) + a_2(x).$$

Продолжая аналогично далее, мы за конечное число k шагов придем к равенству

$$\begin{aligned} a(x) = \big(a_m b_n^{-1} x^{m-n} + a_{m_1}^{(1)} b_n^{-1} x^{m_1-n} + \ldots \\ \ldots + a_{m_k}^{(k)} b_n^{-1} x^{m_k-n}\big) b(x) + a_{k+1}(x), \end{aligned} \tag{13}$$

в котором $m > m_1 > \ldots > m_k \geqslant n > \deg a_{k+1}(x)$. Но это и означает, что мы разделили $a(x)$ с остатком на $b(x)$ справа.

Докажем теперь однозначность деления с остатком при условии теоремы. Пусть

$$a(x) = q_{\Pi}(x)b(x) + r_{\Pi}(x), \quad \deg r_{\Pi}(x) < \deg b(x),$$
$$a(x) = \overline{q}_{\Pi}(x)b(x) + \overline{r}_{\Pi}(x), \quad \deg \overline{r}_{\Pi}(x) < \deg b(x).$$

В таком случае верно равенство $r_{\Pi}(x) - \overline{r}_{\Pi}(x) = (\overline{q}_{\Pi}(x) - q_{\Pi}(x))b(x)$. Если $\overline{q}_{\Pi}(x) - q_{\Pi}(x) \neq 0$, то по утверждению 1(б) в правой части этого равенства находится многочлен степени не меньшей, чем $\deg b(x)$, а по утверждению 1(а) степень многочлена в левой его части строго меньше, чем $\deg b(x)$, что невозможно. Следовательно, $\overline{q}_{\Pi}(x) = q_{\Pi}(x)$, а тогда и $r_{\Pi}(x) = \overline{r}_{\Pi}(x)$.

Доказательство возможности и однозначности деления $a(x)$ на $b(x)$ с остатком слева проводится совершенно аналогично. □

Очевидно, что если R — коммутативное кольцо (в частности, если R — поле), то левые неполное частное и остаток от деления $a(x)$ на $b(x)$ (в случае их существования) являются также правым неполным частным и остатком. В этом случае говорят просто о делении $a(x)$ на $b(x)$ с остатком.

Следствие 1. *Если P — поле и $b(x) \in P[x] \setminus \{0\}$, то любой многочлен $a(x) \in P[x]$ можно разделить с остатком на $b(x)$ и притом единственным способом.*

□ Достаточно заметить, что старший коэффициент $b(x)$ отличен от нуля и потому обратим в P. □

Следствие 2. *В условиях теоремы многочлен $b(x)$ делит $a(x)$ в кольце $R[x]$ справа (слева) тогда и только тогда, когда при делении с остатком $a(x)$ на $b(x)$ справа (слева) остаток равен нулю.*

□ Если в (12) $r_{\Pi}(x) \neq 0$, то равенство $a(x) = q(x)b(x) + 0$ невозможно ни при каком $q(x) \in R[x]$ ввиду доказанной единственности правого остатка. □

Полезно заметить, что предложенный в доказательстве теоремы 3 метод деления $a(x)$ на $b(x)$ с остатком справа есть хорошо известный метод деления «уголком», который осуществляется по следующей схеме:

$$\begin{array}{l|l} a(x) = a_m x^m + \ldots & b(x) = b_n x^n + \ldots \\ \hline a_m b_n^{-1} x^{m-n} b(x) = a_m b_n^{-1} b_n x^m + \ldots & a_m b_n^{-1} x^{m-n} + \ldots + a_{m_k}^{(k)} b_n^{-1} x^{m_k - n} = q_{\Pi}(x) \end{array}$$

$$\begin{array}{l} a_1(x) = a_{m_1}^{(1)} x^{m_1} + \ldots \\ \hline a_{m_1}^{(1)} b_n^{-1} x^{m_1 - n} b(x) = a_{m_1}^{(1)} b_n^{-1} b_n x^{m_1} + \ldots \end{array}$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\begin{array}{l} a_k(x) = a_{m_k}^{(k)} x^{m_k} + \ldots \\ \hline a_{m_k}^{(k)} b_n^{-1} x^{m_k - n} b(x) = a_{m_k}^{(1)} b_n^{-1} b_n x^{m_k} + \ldots \\ \hline a_{k+1}(x) = r_{\Pi}(x) \end{array}$$

§ 3. ЗНАЧЕНИЕ И КОРЕНЬ МНОГОЧЛЕНА. ТЕОРЕМА БЕЗУ. МНОГОЧЛЕН КАК ФУНКЦИЯ

ОПРЕДЕЛЕНИЕ 7. *Значением многочлена* $a(x) = a_0 + a_1x + \ldots + a_nx^n$ *из* $R[x]$ *в точке* $\alpha \in R$ называют элемент кольца R

$$a(\alpha) = a_0 + a_1\alpha + \ldots + a_n\alpha^n.$$

Говорят, что α — *корень многочлена* $a(x)$, если $a(\alpha) = 0$.

Очевидно, что значение суммы двух многочленов в любой точке $\alpha \in R$ равно сумме их значений. Для произведения многочленов аналогичное утверждение верно не всегда. Например, если элементы $\alpha, b \in R$ не перестановочны, то значение в точке α произведения $a(x) \cdot b(x)$ многочленов $a(x) = x$ и $b(x) = b$ не равно $a(\alpha) \cdot b(\alpha)$ (проверьте). Однако, справедлива

Лемма 4. *Если* $a(x), b(x) \in R[x]$, $c(x) = a(x) \cdot b(x)$ *и элемент* α *перестановочен со всеми коэффициентами правого множителя* $b(x)$, *то* $c(\alpha) = a(\alpha) \cdot b(\alpha)$.

□ При сформулированном условии верны равенства

$$a(\alpha) \cdot b(\alpha) = \sum_{i\geqslant 0}\sum_{j\geqslant 0} a_i\alpha^i b_j\alpha^j = \sum_{i\geqslant 0}\sum_{j\geqslant 0} a_ib_j\alpha^{i+j} = c(\alpha). \quad \square$$

Важную связь между понятием делимости и понятием корня многочлена устанавливает

Теорема 5 (Безу).[9] *Остаток от деления справа многочлена* $a(x) \in R[x]$ *на двучлен* $x - \alpha \in R[x]$ *равен* $a(\alpha)$. *В частности, элемент* α *кольца* R *является корнем многочлена* $a(x) \in R[x]$ *тогда и только тогда, когда* $a(x)$ *делится справа на* $x - \alpha$.

□ По теореме 3 многочлен $a(x)$ можно разделить справа с остатком на $x - \alpha$:

$$a(x) = q(x)(x - \alpha) + r(x), \quad \deg r(x) < 1.$$

Тогда $r(x) = rx^0$, где $r \in R$, и $r(\alpha) = r$. По лемме 4 для многочлена $c(x) = q(x)(x-\alpha)$ верно равенство $c(\alpha) = q(\alpha)(\alpha - \alpha) = 0$, откуда

$$a(\alpha) = c(\alpha) + r(\alpha) = 0 + r = r.$$

В частности, равенство $a(\alpha) = 0$ эквивалентно равенству $r = 0$, а последнее по следствию 2 теоремы 3 эквивалентно тому, что $x - \alpha$ делит справа $a(x)$. □

Определение 7 позволяет поставить в соответствие каждому многочлену $a(x) \in R[x]$ функцию $a_R\colon R \to R$, определяемую условием

$$\forall\, \alpha \in R\colon \ a_R(\alpha) = a(\alpha).$$

[9] Э. Безу (1730–1783) — французский математик.

При этом, вообще говоря, для различных многочленов $a(x), b(x) \in R[x]$ функции a_R и b_R могут совпадать. Например, если R — конечное коммутативное кольцо, состоящее из элементов $r_1, \ldots, r_n$, то для любого многочлена $a(x) \in R[x]$ и любого многочлена вида

$$b(x) = a(x) + (x - r_1) \ldots (x - r_n)\, c(x)$$

в силу теоремы Безу верно равенство $a_R = b_R$. С другой стороны, на произвольном кольце R не любую функцию $\varphi\colon R \to R$ можно задать в виде $\varphi = a_R$ для подходящего $a(x) \in R[x]$.

Определение 8. Отображение φ кольца R в себя называют *полиномиальным*, если для некоторого $a(x) \in R[x]$ выполняется равенство $\varphi = a_R$. В этом случае говорят, что φ *задается многочленом* (*полиномом*) $a(x)$.

Позже читатель сможет показать, что если R — коммутативное кольцо, то любое отображение $\varphi\colon R \to R$ полиномиально в том и только в том случае, когда R — конечное поле. Полиномиальность любого преобразования конечного поля вытекает из следующего общего результата.

Теорема 6. *Если в поле P есть n попарно различных элементов $\alpha_1, \ldots, \alpha_n$, то для любых $\beta_1, \ldots, \beta_n \in P$ существует единственный многочлен $a(x) \in P[x]$ со свойствами*

$$a(\alpha_i) = \beta_i \quad \textit{для} \quad i \in \overline{1,n}, \quad \deg a(x) < n. \tag{14}$$

□ Многочлен $a(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} \in P[x]$ удовлетворяет условиям (14) тогда и только тогда, когда вектор $(a_0, a_1, \ldots, a_{n-1})$ есть решение системы линейных уравнений

$$\begin{pmatrix} e & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ e & \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{n-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ e & \alpha_n & \alpha_n^2 & \ldots & \alpha_n^{n-1} \end{pmatrix} X^{\downarrow} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \cdots \\ \beta_n \end{pmatrix}. \tag{15}$$

Определитель основной матрицы этой системы есть определитель Вандермонда, он равен $\prod_{1 \leqslant i < j \leqslant n} (\alpha_j - \alpha_i)$ и отличен от нуля по условию. Следовательно, система имеет единственное решение. □

Замечание 5. Для построения многочлена со свойствами (14) вовсе не обязательно решать систему (15), так как он, очевидно, описывается формулой

$$a(x) = \sum_{i=1}^{n} \frac{\beta_i}{(\alpha_i - \alpha_1) \ldots (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}) \ldots (\alpha_i - \alpha_n)} \times \\ \times (x - \alpha_1) \ldots (x - \alpha_{i-1})(x - \alpha_{i+1}) \ldots (x - \alpha_n),$$

называемой *интерполяционной формулой Лагранжа*.

Следствие 1. *Многочлен степени $n > 0$ над полем P имеет в этом поле не более n различных корней.*

□ В противном случае он принимает нулевое значение в $n+1$ точках из P и по теореме совпадает с многочленом $0+0x+\ldots+0x^n$. □

Из этого результата, в частности, следует, что для комплексного числа z в поле $\mathbb{C}$ существует не более n различных корней степени n из z, так как все они — корни многочлена x^n-z (см. теорему 20 главы 4). Отсюда же следует, что если P — бесконечное поле, то обязательно существуют не полиномиальные отображения $\varphi\colon P\to P$. Например, таково отображение φ, принимающее значение 0 на бесконечном множестве точек из P, но не равное тождественно нулю (докажите).

Следствие 2. *Если P — бесконечное поле, то многочлены $a(x)$ и $b(x)$ из $P[x]$ равны в том и только в том случае, когда равны функции a_P и b_P.*

§ 4. КОЛЬЦО МНОГОЧЛЕНОВ НАД ПОЛЕМ. НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ И НАИМЕНЬШЕЕ ОБЩЕЕ КРАТНОЕ

В этом и следующем параграфах излагается теория делимости в кольце $P[x]$ многочленов над произвольным полем P, аналогичная теории, изложенной в главе 4 для кольца целых чисел $\mathbb{Z}$.

Основное сходство между кольцами $P[x]$ и $\mathbb{Z}$ состоит в том, что, согласно теореме 2 и следствию 1 теоремы 3, кольцо $P[x]$, как и $\mathbb{Z}$, есть коммутативное кольцо с единицей и без делителей нуля, в котором определено понятие деления с остатком и любой элемент можно разделить с остатком на любой ненулевой элемент единственным способом.

Для дальнейшего описания свойств кольца $P[x]$ и сравнения их со свойствами кольца $\mathbb{Z}$ введем

Определение 9. Элементы a и b коммутативного кольца S с единицей называются *ассоциированными*, если $b=ua$ для некоторого обратимого элемента $u\in S$.

Читатель без труда проверит, что отношение ассоциированности элементов есть отношение эквивалентности на S. Очевидно, что ассоциированность чисел $a,b\in\mathbb{Z}$ эквивалентна равенству $|a|=|b|$, которое, в свою очередь, эквивалентно условию: $a\mid b$ и $b\mid a$. Эти результаты переносятся на кольцо $P[x]$ следующим образом.

Утверждение 7. *В кольце $P[x]$ обратимы все многочлены нулевой степени и только они. Для многочленов $a(x),b(x)\in P[x]$ следующие утверждения эквивалентны*:
(а) *$a(x)$ и $b(x)$ ассоциированы*;
(б) *$a(x)\mid b(x)$ и $b(x)\mid a(x)$*;
(в) *$a(x)\mid b(x)$ и $\deg a(x)=\deg b(x)$*.

□ Если $u(x)\in P[x]$ и $u(x)v(x)=e$, то по утверждению 1(в) верно равенство $\deg u(x)+\deg v(x)=0$, откуда $\deg u(x)=0$. Обратимость $u(x)$ при условии $\deg u(x)=0$ очевидна.

Импликация (а)⇒(б) очевидна. Импликация (б)⇒(в) легко получается с использованием утверждения 1(в). Наконец, при условии (в) справедливы равенства $b(x)=u(x)a(x)$, $\deg u(x)=0$. Следовательно, $u(x)\in P[x]^*$ и (в)⇒(а). □

В кольце $\mathbb{Z}$ особую роль играют натуральные числа: множество $\mathbb{N}$ замкнуто относительно умножения и с каждым ненулевым целым числом ассоциировано единственное натуральное. Подмножество с аналогичными свойствами можно выделить и в $P[x]$.

Определение 10. Ненулевой многочлен со старшим коэффициентом, равным единице, называют *унитарным*.

Очевидно, что множество всех унитарных многочленов из $P[x]$ замкнуто относительно операции умножения, и, так как $P[x]^* = P^*$, то с любым ненулевым многочленом $f(x) \in P[x]$ ассоциирован единственный унитарный многочлен, который мы будем обозначать символом $f^*(x)$.

Однако, аналогия между унитарными многочленами и натуральными числами имеет ограниченную область применения. В частности, если целое a делится с остатком на $b \in \mathbb{Z} \setminus \{0\}$, то остаток r есть либо нуль, либо натуральное число. Если же многочлен $a(x) \in P[x]$ делится с остатком на $b(x) \in P[x] \setminus \{0\}$ и остаток $r(x)$ отличен от нуля, то $r(x)$ — не обязательно унитарный многочлен. Аналогия между r и $r(x)$ здесь состоит в том, что r удовлетворяет условию $0 \leqslant r < |b|$, а $r(x)$ — условию $\deg r(x) < \deg b(x)$.

Ниже все результаты о многочленах из $P[x]$ формулируются по аналогии с результатами о целых числах и излагаются практически без доказательств, которые читателю предлагается восстановить самостоятельно по доказательствам соответствующих результатов из главы 4.

Определение 11. *Наибольшим общим делителем* (НОД) *многочленов* $a_1(x), \ldots, a_n(x) \in P[x]$ называют многочлен $d(x) \in P[x]$ такой, что

1) $d(x)$ есть общий делитель многочленов $a_1(x), \ldots, a_n(x)$;

2) $d(x)$ делится на любой другой общий делитель этих многочленов.

Совокупность всех НОД указанных многочленов обозначают следующим образом: НОД $\{a_1(x), \ldots, a_n(x)\}$.

Прежде чем доказывать существование наибольшего общего делителя для любого набора многочленов, покажем, что для описания НОД $\{a_1(x), \ldots, a_n(x)\}$ достаточно найти один его элемент.

Утверждение 8. (а) *Если* $a_1(x) = \ldots = a_n(x) = 0$, *то*

$$\text{НОД}\,\{a_1(x), \ldots, a_n(x)\} = \{0\}.$$

(б) *Если хотя бы один из многочленов* $a_1(x), \ldots, a_n(x)$ *не равен нулю и* НОД $\{a_1(x), \ldots, a_n(x)\} \neq \varnothing$, *то для любого* $d(x) \in$ НОД $\{a_1(x), \ldots, a_n(x)\}$ *верно равенство*

$$\text{НОД}\,\{a_1(x), \ldots, a_n(x)\} = \{ud(x) :\ u \in P^*\},$$

и существует единственный унитарный НОД этих многочленов.

□ Утверждение (а) очевидно. Докажем (б). Из определения 11 следует, что многочлен $d(x) \neq 0$ и $ud(x) \in \text{НОД}\{a_1(x), \ldots, a_n(x)\}$ для любого $u \in P^*$. Наоборот, если $f(x) \in \text{НОД}\{a_1(x), \ldots, a_n(x)\}$, то по свойству 2 определения 11 $f(x) \mid d(x)$ и $d(x) \mid f(x)$, т. е. по утверждению 7 $f(x) = ud(x)$ для некоторого $u \in P^*$. □

Теорема 9. *Если среди многочленов $a_1(x), \ldots, a_n(x) \in P[x]$ есть ненулевые, то для них в $P[x]$ существует единственный унитарный наибольший общий делитель.*

□ По утверждению 8(б) достаточно доказать существование одного НОД рассматриваемых многочленов. Это делается так же, как и для целых чисел, индукцией по параметру $n \geqslant 2$. При $n = 2$ доказательство проводится с помощью *алгоритма Евклида*, который для многочленов $a_1(x) = a(x)$ и $a_2(x) = b(x) \neq 0$ реализуется следующим образом. Если $b(x) \mid a(x)$, то $b(x) \in \text{НОД}\{a(x), b(x)\}$. Если $b(x) \nmid a(x)$, то строится цепочка соотношений:

$$\begin{aligned} a(x) &= b(x)q_1(x) + r_1(x), \quad 0 \leqslant \deg r_1(x) < \deg b(x); \\ b(x) &= r_1(x)q_2(x) + r_2(x), \quad 0 \leqslant \deg r_2(x) < \deg r_1(x); \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ r_{k-2}(x) &= r_{k-1}(x)q_k(x) + r_k(x), \quad 0 \leqslant \deg r_k(x) < \deg r_{k-1}(x). \end{aligned} \tag{16}$$

Эта цепочка при некотором $k \in \mathbb{N}$ обязательно обрывается соотношением

$$r_{k-1}(x) = r_k(x)q_{k+1}(x), \quad r_{k+1}(x) = 0, \tag{17}$$

поскольку степени остатков в (16) образуют строго убывающий ряд чисел из $\mathbb{N}_0$:

$$\deg b(x) > \deg r_1(x) > \ldots > \deg r_k(x),$$

и по аксиоме индукции этот ряд не может быть бесконечным, а в случае, когда $r_{k+1}(x) \neq 0$, к этому ряду можно приписать справа еще один член. При условиях (16), (17) так же, как и в теореме 4 главы 4, доказывается, что $r_k(x) \in \text{НОД}\{a(x), b(x)\}$. □

Теорема 10. *Если $d(x) \in \text{НОД}\{a_1(x), \ldots, a_n(x)\}$, то существуют многочлены $u_1(x), \ldots, u_n(x) \in P[x]$ такие, что*

$$d(x) = u_1(x)a_1(x) + \ldots + u_n(x)a_n(x).$$

□ Индукция по $n \geqslant 2$. При $n = 2$ нужные многочлены находятся из соотношений (16), (17) точно так же, как это делается в следствии теоремы 6 главы 4 для целых чисел. □

Пример 1. Пусть $P = \mathbb{Z}_3$ — поле вычетов по модулю 3 и требуется найти НОД многочленов $a(x) = x^5 + 2x^4 + 2x^3 + x^2 + x + 2$ и $b(x) = x^5 + x^3 + x$ и представить этот НОД в виде линейной комбинации $a(x)$ и $b(x)$ над $P[x]$. Выполняя цепочку последовательных делений с остатком, получаем:

$$
\begin{array}{rl|l}
 & a(x) = x^5 + 2x^4 + 2x^3 + x^2 + x + 2 & x^5 + x^3 + x = b(x) \\
- & \underline{x^5 \qquad + x^3 \qquad + x} & \hline
 & & 1 = q_1(x)
\end{array}
$$

$$
\begin{array}{rl|l}
 & b(x) = x^5 \qquad + x^3 + x & 2x^4 + x^3 + x^2 \qquad + 2 = r_1(x) \\
- & \underline{x^5 + 2x^4 + 2x^3 + x} & \hline
 & & 2x + 2 = q_2(x)
\end{array}
$$

$$
\begin{array}{rl}
 & x^4 + 2x^3 \\
- & \underline{x^4 + 2x^3 + \quad 2x^2 + 1}
\end{array}
$$

$$
\begin{array}{rl|l}
 & r_1(x) = 2x^4 + x^3 + x^2 + 2 & x^2 + 2 = r_2(x) \\
- & \underline{2x^4 \qquad + x^2} & \hline
 & & 2x^2 + 2 = q_3(x)
\end{array}
$$

$$
\begin{array}{rl}
 & x^3 \qquad + 2 \\
- & \underline{x^3 + 2x} \qquad\qquad
\end{array}
$$

$$
\begin{array}{rl|l}
 & r_2(x) = x^2 + 2 & x + 2 = r_3(x) \\
- & \underline{x^2 + 2x} & \hline
 & & x + 1 = q_4(x)
\end{array}
$$

$$
\begin{array}{rl}
 & \underline{x \quad + 2} \\
 & 0 \;=\; r_4(x)
\end{array}
$$

Таким образом, $r_3(x) = x + 2 \in \text{НОД}\,\{a(x), b(x)\}$, и для построения многочленов $u(x), v(x) \in P[x]$, для которых $x + 2 = u(x)a(x) + v(x)b(x)$, нужно по правилам, изложенным в § 2 главы 4, построить последовательность пар многочленов $u_t(x)$, $v_t(x)$, $t \in \overline{1,3}$, удовлетворяющих соотношениям $u_t(x)a(x) + v_t(x)b(x) = r_t(x)$. Тогда $u(x) = u_3(x)$, $v(x) = v_3(x)$. Строим таблицу, аналогичную таблице из § 2 главы 4:

t	0	1	2	3
q_t		1	$2x + 2$	$2x^2 + 2$
$u_t(x)$	0	1	$x + 1$	$x^3 + 2x + 1$
$v_t(x)$	1	-1	$2x$	$x^3 + x^2 + 2$

Отсюда имеем: $(x^3 + 2x + 1)\,a(x) + (x^3 + x^2 + 2)\,b(x) = x + 2$.

Для многочленов $a_1(x), \ldots, a_n(x) \in P[x]$, не все из которых равны нулю, единственный унитарный наибольший общий делитель обозначим через $(a_1(x), \ldots, a_n(x))$. В случае $a_1(x) = \ldots = a_n(x) = 0$ положим $(a_1(x), \ldots, a_n(x)) = 0$.

Определение 12. Многочлены $a_1(x), \ldots, a_n(x) \in P[x]$ называют *взаимно простыми* (*в совокупности*), если

$$(a_1(x), \ldots, a_n(x)) = e.$$

Утверждение 11. *Многочлены $a_1(x), \ldots, a_n(x) \in P[x]$ взаимно просты тогда и только тогда, когда существуют многочлены $u_1(x), \ldots, u_n(x) \in P[x]$ такие, что $u_1(x)a_1(x) + \ldots + u_n(x)a_n(x) = e$.*

□ См. доказательство утверждения 8 главы 4. □

Теорема 12. *Для любых многочленов $a(x), b(x), c(x) \in P[x]$ справедливы утверждения*:

(а) *если* $(a(x), b(x)) = e$ *и* $(a(x), c(x)) = e$, *то* $(a(x),\, b(x)c(x)) = e$;

(б) *если* $(a(x), b(x)) = e$ *и* $a(x) \mid b(x)c(x)$, *то* $a(x) \mid c(x)$;

(в) *если* $(a(x), b(x)) = e$, $a(x) \mid c(x)$ *и* $b(x) \mid c(x)$, *то* $a(x)b(x) \mid c(x)$;

(г) *если* $(a(x), b(x)) = c(x) \neq 0$, *то* $\left(\dfrac{a(x)}{c(x)}\,,\, \dfrac{b(x)}{c(x)}\right) = e$.

□ См. доказательство теоремы 9 главы 4. □

Определение 13. *Наименьшим общим кратным* (НОК) многочленов $a_1(x), \ldots, a_n(x) \in P[x]$ называют многочлен $k(x) \in P[x]$ со свойствами:

1) $k(x)$ — общее кратное многочленов $a_1(x), \ldots, a_n(x)$;

2) если $k_1(x)$ — любое общее кратное многочленов $a_1(x), \ldots, a_n(x)$, то $k(x) \mid k_1(x)$.

Совокупность всех описанных многочленов $k(x)$ обозначают следующим образом: $\text{НОК}\{a_1(x), \ldots, a_n(x)\}$.

Очевидно, что если среди многочленов $a_1(x), \ldots, a_n(x)$ есть нулевой, то $\text{НОК}\,\{a_1(x), \ldots, a_n(x)\} = \{0\}$. В противном случае справедлива

Теорема 13. *Если $a_1(x), \ldots, a_n(x) \in P[x] \setminus \{0\}$, то существует единственный унитарный многочлен $k(x) \in \text{НОК}\,\{a_1(x), \ldots, a_n(x)\}$ и справедливо равенство*

$$\text{НОК}\,\{a_1(x), \ldots, a_n(x)\} = \{uk(x) \colon\, u \in P^*\}.$$

□ Существование НОК указанных многочленов доказывается индукцией по параметру n. При $n = 2$ так же, как и при доказательстве утверждения 11 главы 4, показывается, что

$$\frac{a_1(x)\, a_2(x)}{(a_1(x), a_2(x))} \in \text{НОК}\,\{a_1(x), a_2(x)\},$$

а затем доказывается, что если $n > 2$ и $f_1(x) \in \text{НОК}\,\{a_1(x), \ldots, a_{n-1}(x)\}$, $f(x) \in \text{НОК}\,\{f_1(x), a_n(x)\}$, то $f(x) \in \text{НОК}\,\{a_1(x), \ldots, a_n(x)\}$. Если $k(x) = f^\star(x)$ — унитарный многочлен, ассоциированный с $f(x)$, то он также удовлетворяет определению 13, т. е. $k(x) \in \text{НОК}\,\{a_1(x), \ldots, a_n(x)\}$. Последняя часть теоремы легко доказывается с помощью того же определения. □

Унитарный многочлен $k(x)$, являющийся наименьшим общим кратным многочленов $a_1(x), \ldots, a_n(x) \in P[x] \setminus \{0\}$, обозначают $k(x) = [a_1(x), \ldots, a_n(x)]$.

Теперь результаты теоремы 13 можно коротко записать так:

$$[a_1(x), a_2(x)] = \frac{a_1^*(x)\, a_2^*(x)}{(a_1(x), a_2(x))},$$

$$[a_1(x), \ldots, a_n(x)] = [\,[a_1(x), \ldots, a_{n-1}(x)],\, a_n(x)].$$

§ 5. НЕПРИВОДИМЫЕ МНОГОЧЛЕНЫ НАД ПОЛЕМ. КАНОНИЧЕСКОЕ РАЗЛОЖЕНИЕ МНОГОЧЛЕНА

1. Понятие неприводимого многочлена в кольце $P[x]$ есть аналог понятия простого числа в кольце $\mathbb{Z}$.

Определение 14. *Делитель* $d(x) \in P[x]$ многочлена $f(x) \in P[x]$ называется *собственным*, если $0 < \deg d(x) < \deg f(x)$, и *несобственным* в противном случае. Многочлен $f(x) \in P[x]$ называется *неприводимым над полем* P (или *неприводимым в кольце* $P[x]$), если $\deg f(x) > 0$ и $f(x)$ не имеет собственных делителей в кольце $P[x]$. Если многочлен $f(x)$ имеет собственный делитель в кольце $P[x]$, то он называется *приводимым*.

Многочлены нулевой степени (т. е. обратимые элементы $P[x]$) и нулевой многочлен не являются ни приводимыми, ни неприводимыми многочленами.

Так как по утверждению 1(в) степень произведения любых двух многочленов из $P[x]$ равна сумме их степеней, то очевидно

Утверждение 14. *Многочлен* $f(x) \in P[x]$ *приводим тогда и только тогда, когда его можно представить в виде произведения двух многочленов, степени которых строго меньше, чем* $\deg f(x)$.

Очевидно, что в кольце $P[x]$ неприводимы все многочлены первой степени, однако могут существовать неприводимые многочлены более высоких степеней.

Понятно, что если $f(x)$ — неприводимый многочлен из $P[x]$ степени $n \geqslant 2$, то он не имеет корней в P (в противном случае по теореме Безу он имеет собственный делитель степени 1). Обратное утверждение в общем случае (при $n \geqslant 4$) неверно, однако справедливо

Утверждение 15. *Многочлен* $f(x) \in P[x]$ *степени* 2 *или* 3 *тогда и только тогда неприводим над* P*, когда он не имеет корней в* P.

□ Достаточно заметить, что если $f(x)$ приводим, то он имеет унитарный делитель степени 1, и воспользоваться теоремой Безу. □

Пример 2. Если $P = \mathbb{Z}_2$ — поле из двух элементов, то в $P[x]$ неприводимы многочлены x^2+x+1, x^3+x+1, x^3+x^2+1, так как они не имеют в P корней. Многочлен x^4+x^2+1 также не имеет корней в P, но он приводим: $x^4+x^2+1 = (x^2+x+1)^2$.

Иногда один и тот же многочлен приходится рассматривать как многочлен над разными полями. Например, многочлен $x^2-2 \in \mathbb{Q}[x]$ можно рассматривать и как многочлен над $\mathbb{R}$. В связи с этим следует подчеркнуть, что неприводимость многочлена это не просто свойство самого многочлена, а свойство многочлена по отношению к тому полю, над которым он рассматривается. Так, многочлен x^2-2 неприводим над $\mathbb{Q}$, поскольку его корни иррациональны, но приводим над $\mathbb{R}$: $x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$.

2. Для описания свойств многочленов, связанных с их разложением на множители, нужно сначала описать свойства неприводимых многочленов. По аналогии с утверждением 13 главы 4 доказывается

Утверждение 16. *Пусть $f(x) \in P[x]$ — неприводимый многочлен. Тогда для любых многочленов $a(x), b(x) \in P[x]$ справедливы следующие утверждения*:

(а) $f(x) \mid a(x)$ *или* $(f(x), a(x)) = e$;

(б) *если* $f(x) \mid a(x)b(x)$, *то* $f(x) \mid a(x)$ *или* $f(x) \mid b(x)$;

(в) *если* $g(x) \in P[x]$ *— неприводимый многочлен, то либо* $(f(x), g(x)) = e$, *либо многочлены* $f(x)$ *и* $g(x)$ *ассоциированы.* □

Замечание 6. Задача о разложении произвольного многочлена из $P[x]$ на множители легко сводится к аналогичной задаче для унитарного многочлена, поскольку для любых $f(x), a(x), b(x) \in P[x] \setminus \{0\}$ многочлен $f(x)$ неприводим над P тогда и только тогда, когда $f^*(x)$ неприводим, а равенство $f(x) = a(x)b(x)$ влечет равенство $f^*(x) = a^*(x)\, b^*(x)$. Переход к унитарным многочленам оказывается весьма удобным, поскольку существенно упрощает формулировки теорем и их доказательства. Например, если $f(x)$, $g(x)$ — унитарные неприводимые многочлены, то для них утверждение 16(в) имеет вид: либо $(f(x), g(x)) = e$, либо $f(x) = g(x)$.

Для многочленов над полем справедлив следующий аналог основной теоремы арифметики.

Теорема 17. *Любой унитарный многочлен $a(x) \in P[x]$ ненулевой степени либо неприводим над P, либо раскладывается в произведение унитарных неприводимых над P многочленов, причем это разложение однозначно с точностью до перестановки сомножителей.*

□ См. доказательство теоремы 14 главы 4. □

Из первого утверждения теоремы 17 следует, что любой многочлен $f(x) \in P[x]$ степени $n > 0$ можно представить в виде

$$f(x) = f_n \cdot p_1(x)^{k_1} \cdot \ldots \cdot p_r(x)^{k_r}, \tag{18}$$

где f_n — старший коэффициент $f(x)$; $p_1(x), \ldots, p_r(x)$ — унитарные, неприводимые, попарно различные (т. е. попарно взаимно простые) многочлены из $P[x]$ и $k_1, \ldots, k_r \in \mathbb{N}$.

Определение 15. Представление многочлена $f(x)$ в виде (18) называют его *каноническим разложением над полем P*. Каждый многочлен $p_i(x)$ называют *неприводимым делителем* $f(x)$, а показатель k_i — *кратностью* $p_i(x)$ в каноническом разложении $f(x)$. Многочлены $p_i(x)^{k_i}$ называют *примарными компонентами* многочлена $f(x)$.

Из второго утверждения теоремы получаем

Следствие. *Каноническое разложение многочлена $f(x) \in P[x]$ степени $n > 0$ определено однозначно, с точностью до перестановки примарных компонент: если $f(x) = f_n \cdot g_1(x)^{l_1} \cdot \ldots \cdot g_s(x)^{l_s}$ — другое каноническое разложение $f(x)$, то $r = s$ и существует перестановка $(i_1, \ldots, i_r) \in P(\overline{1,r})$ такая, что для $m \in \overline{1,r}$ выполняются равенства $g_m(x)^{l_m} = p_{i_m}(x)^{k_{i_m}}$, т. е. $g_m(x) = p_{i_m}(x)$ и $l_m = k_{i_m}$.*

Отметим, что по каноническим разложениям двух многочленов из $P[x]$ с помощью формул, которые приведены в § 3 главы 4, легко находятся их НОД и НОК.

В частности, с использованием понятий канонического разложения и неприводимого многочлена часто удается просто доказывать взаимную простоту многочленов. В основе таких доказательств лежит очевидное

Утверждение 18. *Многочлены $a_1(x), \dots, a_n(x) \in P[x]$ взаимно просты тогда и только тогда, когда они не имеют общего неприводимого делителя.*

В качестве примера использования этого утверждения докажем

Утверждение 19. *Если ненулевые многочлены $a_1(x)$, $\dots$, $a_t(x)$ из $P[x]$ попарно взаимно просты и*

$$\widehat{a}_i(x) = a_1(x) \dots a_{i-1}(x)\, a_{i+1}(x) \dots a_t(x) \quad \textit{для} \quad i \in \overline{1,t},$$

то $(\widehat{a}_1(x), \dots, \widehat{a}_t(x)) = e$.

□ Пусть утверждение неверно. Тогда по утверждению 18 существует неприводимый многочлен $f(x) \in P[x]$ такой, что $f(x) \mid \widehat{a}_i(x)$ для $i \in \overline{1,t}$. В частности, $f(x) \mid \widehat{a}_1(x)$. Отсюда по утверждению 16(б) получаем, что $f(x) \mid a_j(x)$ для некоторого $j \in \overline{2,t}$. Последнее противоречит утверждению 18, так как $f(x) \mid \widehat{a}_j(x)$, а в силу теоремы 12(а) $(a_j(x), \widehat{a}_j(x)) = e$. □

С использованием теоремы 17 доказывается аналогичная теореме Евклида (теорема 15 главы 4)

Теорема 20. *Для любого поля P множество унитарных неприводимых многочленов в кольце $P[x]$ бесконечно.*

Ясно, что это утверждение нетривиально лишь для конечных полей и в этом случае из теоремы вытекает очевидное

Следствие. *Если P — конечное поле, то для каждого натурального m в кольце $P[x]$ существует неприводимый многочлен степени $n \geqslant m$.*

Более подробно со свойствами неприводимых многочленов над конечными полями читатель познакомится в главе 22. Здесь мы отметим лишь, что в современной прикладной математике весьма важными являются задачи разработки алгоритмов, позволяющих с помощью ЭВМ быстро строить неприводимые многочлены больших степеней над конечными полями и раскладывать многочлены над такими полями на неприводимые множители.

§ 6. КОРНИ МНОГОЧЛЕНОВ НАД ПОЛЕМ

1. Напомним, что, согласно теореме Безу, элемент $\alpha \in P$ есть корень многочлена $f(x) \in P[x]$ тогда и только тогда, когда $x - \alpha \mid f(x)$. В алгебре и ее приложениях широко используется следующая классификация корней многочленов.

Определение 16. *Кратностью корня* $\alpha \in P$ многочлена $f(x) \in P[x]$ называют число $k \in \mathbb{N}$ со свойствами

$$(x-\alpha)^k \mid f(x), \quad (x-\alpha)^{k+1} \nmid f(x).$$

Говорят, что α — *простой корень* $f(x)$, если $k=1$, и α — *кратный корень* $f(x)$, если $k>1$.

Очевидно, что кратность корня α многочлена $f(x)$ совпадает с кратностью многочлена $x-\alpha$ в каноническом разложении $f(x)$ над P.

Следующий результат существенно усиливает следствие 1 теоремы 6.

Теорема 21. *Многочлен $f(x)$ степени $n>0$ над полем P имеет в этом поле не более n корней с учетом их кратностей, т. е. если $\alpha_1, \ldots, \alpha_m$ — различные корни $f(x)$ в поле P и их кратности равны соответственно $k_1, \ldots, k_m$, то верно неравенство $k_1 + \ldots + k_m \leqslant n$.*

□ Так как по теореме 12(а) многочлены $(x-\alpha_1)^{k_1}$, $\ldots$, $(x-\alpha_m)^{k_m}$ попарно взаимно просты и каждый из них делит $f(x)$, то по теореме 12(в)

$$(x-\alpha_1)^{k_1} \ldots (x-\alpha_m)^{k_m} \mid f(x).$$

Отсюда по утверждению 1(в) $n \geqslant k_1 + \ldots + k_m$. □

2. Удобный способ различения простых и кратных корней многочлена в поле связан с понятием производной многочлена. В алгебре это понятие вводится формально, по аналогии с известным из курса математического анализа описанием производной многочлена в $\mathbb{R}[x]$. Напомним, что элементы поля P как элементы абелевой группы $(P,+)$ можно умножать на целые числа так, как это делалось в § 2 главы 3. Ниже используются сформулированные там законы ассоциативности и дистрибутивности такого умножения.

Определение 17. *Производной многочлена* $a(x) = a_0 + a_1 x + \ldots + a_n x^n \in P[x]$ называют многочлен

$$a'(x) = a_1 + 2a_2 x + \ldots + n a_n x^{n-1}.$$

Несмотря на столь формальное определение, производная сохраняет свойства, известные из курса математического анализа.

Теорема 22. *Для любых многочленов $a(x), b(x) \in P[x]$ справедливы равенства*:

$$(a(x)+b(x))' = a'(x) + b'(x), \tag{19}$$

$$(a(x)\,b(x))' = a'(x)\,b(x) + a(x)\,b'(x). \tag{20}$$

□ Равенство (19) легко следует из определения 17. Равенство (20) очевидно, если один из многочленов является константой. Рассмотрим теперь следующий случай, когда $a(x) = a \cdot x^k$, $b(x) = b \cdot x^l$, $k, l \in \mathbb{N}$. По определению

$$(a(x) \cdot b(x))' = (abx^{k+l})' = (k+l)abx^{k+l-1},$$

т. е. в этом случае равенство (20) верно.

Наконец, в общей ситуации, пользуясь равенством (19) и доказанными выше соотношениями, получаем

$$(a(x)\,b(x))' = \sum_{k\geqslant 0}\sum_{l\geqslant 0}((a_kx^k)(b_lx^l))' = \sum_{k\geqslant 0}\sum_{l\geqslant 0}((a_kx^k)'(b_lx^l) + (a_kx^k)(b_lx^l)') =$$
$$= \sum_{k\geqslant 0}(a_kx^k)'\sum_{l\geqslant 0}b_lx^l + \sum_{k\geqslant 0}a_kx^k\sum_{l\geqslant 0}(b_lx^l)' = a'(x)b(x) + a(x)b'(x). \quad \square$$

Следствие 1. *Для любых многочленов $a_1(x),\dots,a_n(x) \in P[x]$ справедливо равенство*

$$(a_1(x)\dots a_n(x))' = a_1'(x)a_2(x)\dots a_n(x) + a_1(x)a_2'(x)a_3(x)\dots a_n(x) + \dots$$
$$\dots + a_1(x)\dots a_{n-1}(x)a_n'(x).$$

Доказательство легко проводится индукцией по n.

Из следствия 1 очевидным образом получаем

Следствие 2. *Для любых $a(x) \in P[x]$ и $k \in \mathbb{N}$ справедливо равенство*

$$(a(x)^k)' = k\cdot a(x)^{k-1}\cdot a'(x).$$

Замечание 7. Совершенно аналогично производную можно определить для многочленов над любым (не обязательно коммутативным) кольцом с единицей. При этом остаются справедливыми теорема 22 и ее следствия, доказательства которых проводятся дословно так же (проверьте). Следствие 2 верно для многочленов над коммутативным кольцом.

Теорема 23. *Корень $\alpha \in P$ многочлена $f(x) \in P[x]$ является простым тогда и только тогда, когда α не является корнем его производной $f'(x)$.*

$\square$ Пусть k — кратность корня α. Тогда $f(x) = (x-\alpha)^k g(x)$, где $g(\alpha) \neq 0$. Отсюда по теореме 22 имеем:

$$f'(x) = k(x-\alpha)^{k-1}g(x) + (x-\alpha)^k g'(x).$$

Если $k = 1$, то $f'(\alpha) = g(\alpha) \neq 0$. Если $k > 1$, то

$$f'(\alpha) = k(\alpha-\alpha)^{k-1}g(\alpha) + (\alpha-\alpha)^k g'(\alpha) = 0,$$

т. е. из условия $f'(\alpha) \neq 0$ следует, что $k = 1$. $\square$

Следствие 1. *Множество кратных корней в поле P многочлена $f(x) \in P[x]$ совпадает с множеством всех корней в поле P многочлена $d(x) = (f(x), f'(x))$.*

$\square\ \forall\,\alpha \in P\colon \big(f(\alpha) = f'(\alpha) = 0\big) \Leftrightarrow \big(x-\alpha \mid f(x) \text{ и } x-\alpha \mid f'(x)\big) \Leftrightarrow \big(x-\alpha \mid d(x)\big) \Leftrightarrow$
$\Leftrightarrow \big(d(\alpha) = 0\big)$. $\square$

Определение 18. Поле P называется *полем разложения многочлена* $f(x) \in P[x]$ степени $n > 0$, если $f(x)$ раскладывается над P в произведение линейных множителей, т. е. если каноническое разложение $f(x)$ над P имеет вид

$$f(x) = f_n(x - \alpha_1)^{k_1} \dots (x - \alpha_r)^{k_r}.$$

Пример 3. Для многочлена $x^2 + 1 \in \mathbb{R}[x]$ поле $\mathbb{C}$ является полем разложения, а поле $\mathbb{R}$ — нет.

Пример 4. Для любого простого $p \in \mathbb{N}$ поле $\mathbb{Z}_p$ вычетов по модулю p есть поле разложения многочлена $x^p - x$ (докажите!):

$$x^p - x = x \cdot (x - 1) \cdot \ldots \cdot (x - (p - 1)).$$

Следствие 2. *Если P — поле разложения многочлена $f(x) \in P[x]$, то $f(x)$ не имеет кратных корней в P тогда и только тогда, когда $(f(x), f'(x)) = e$.*

□ Многочлен $d(x) = (f(x), f'(x))$ делит $f(x)$, поэтому, если $\deg d(x) > 0$, то по условию теоремы $d(x)$ раскладывается над P на линейные множители и имеет в P корень. В рассматриваемой ситуации отсутствие у $f(x)$ кратных корней в поле P согласно следствию 1 равносильно условию $\deg d(x) = 0$. □

Замечание 8. Если P не является полем разложения для многочлена $f(x)$, то условие $(f(x), f'(x)) = e$ является достаточным для отсутствия кратных корней многочлена $f(x)$ в поле P, но не является необходимым (докажите).

Полученные результаты можно использовать не только для отыскания кратных корней многочлена, но и для разложения его на множители в случае наличия у него таких корней.

Пример 5. Найти кратные корни в поле $\mathbb{Z}_5$ многочлена

$$f(x) = x^4 - 2x^3 + 2x^2 - 2x + 1 \in \mathbb{Z}_5[x].$$

Вычисляя наибольший общий делитель $f(x)$ и $f'(x) = 4x^3 - x^2 + 4x - 2$, получаем: $(f(x), f'(x)) = x - 1$. Следовательно, 1 — кратный корень $f(x)$, и $(x - 1)^2 \mid f(x)$. Выполняя деление, находим: $f(x) = (x - 1)^2(x^2 + 1)$. Непосредственной проверкой убеждаемся, что многочлен $x^2 + 1$ имеет в поле $\mathbb{Z}_5$ корни 2 и 3. Таким образом, $f(x) = (x - 1)^2(x - 2)(x - 3)$.

3. Пусть F — произвольное поле. Напомним, что подполем поля F называется подмножество $P \subset F$, замкнутое относительно операций сложения и умножения на F и являющееся полем относительно этих операций. В этой ситуации говорят также, что поле F есть *расширение поля P*. В главе 21 будет показано, что для любого поля P и любого многочлена $f(x) \in P[x]$ существует расширение F поля P, которое является полем разложения для $f(x)$.

В действительности, справедливо даже более сильное утверждение.

Определение 19. Поле F называется *алгебраически замкнутым*, если оно является полем разложения для любого многочлена $f(x) \in F[x]$, $\deg f(x) > 0$.

Теорема 24 (Штейниц).[10] *Для любого поля P существует расширение F, которое является алгебраически замкнутым.*

Доказательство этого результата выходит за рамки нашего курса. Мы ограничимся здесь лишь указанием одного очень важного примера.

Теорема 25 (Гаусс). *Любой многочлен ненулевой степени над полем $\mathbb{C}$ комплексных чисел имеет в этом поле корень* (*другими словами, поле $\mathbb{C}$ алгебраически замкнуто*).

Эта теорема, долгое время называвшаяся *основной теоремой алгебры*, не имеет чисто алгебраического доказательства и будет выведена как следствие из более общих результатов при изучении теории функций комплексного переменного. Мы, однако, уже сейчас будем широко использовать эту теорему. В частности, теперь может быть коротко доказано следующее утверждение (см. теорему 20 главы 4).

Следствие. *Для любого ненулевого комплексного числа z и любого $n \in \mathbb{N}$ в поле $\mathbb{C}$ существует ровно n различных корней степени n из z.*

□ По теореме 25 многочлен $x^n - z$ раскладывается на линейные множители над $\mathbb{C}$, а по следствию 2 теоремы 23 он не имеет кратных корней в $\mathbb{C}$, т. е. в поле $\mathbb{C}$ у него есть ровно n различных корней. □

§ 7. МНОГОЧЛЕНЫ НАД ЧИСЛОВЫМИ ПОЛЯМИ

Здесь приводятся полное описание неприводимых многочленов над полями $\mathbb{C}$ и $\mathbb{R}$, некоторые важные достаточные условия неприводимости многочленов над $\mathbb{Q}$ и способы вычисления рациональных корней многочленов из $\mathbb{Q}[x]$.

1. Описание неприводимых многочленов над полем $\mathbb{C}$ легко следует из теоремы Гаусса.

Утверждение 26. *Над полем комплексных чисел неприводимы все многочлены первой степени и только они.*

Эта теорема позволяет также описать все неприводимые многочлены над $\mathbb{R}$. Напомним, что дискриминантом многочлена $f(x) = ax^2 + bx + c \in \mathbb{R}[x]$, $a \neq 0$, называется число $\Delta(f) = b^2 - 4ac$, и $f(x)$ не имеет корней в $\mathbb{R}$ тогда и только тогда, когда $\Delta(f) < 0$.

Теорема 27. *В кольце $\mathbb{R}[x]$ неприводимыми являются все многочлены первой степени, многочлены второй степени с отрицательными дискриминантами и только они.*

[10] Э. Штейниц (1871–1928) — немецкий математик.

□ Неприводимость указанных многочленов очевидна (см. утверждение 15). Покажем, что других неприводимых многочленов в $\mathbb{R}[x]$ нет.

Пусть $f(x) = f_0 + f_1x + \ldots + f_nx^n \in \mathbb{R}[x]$ — неприводимый многочлен степени $n > 1$. Тогда он не имеет корней в $\mathbb{R}$, но по теореме 25 имеет корень $\beta \in \mathbb{C}$. В таком случае число β не совпадает с сопряженным к нему числом $\overline{\beta}$ (т. к. $\beta \notin \mathbb{R}$), и $\overline{\beta}$ — также корень $f(x)$, поскольку в силу утверждения 17 главы 4

$$f(\overline{\beta}) = \sum f_i\overline{\beta}^i = \sum \overline{f}_i\overline{\beta}^i = \overline{\sum f_i\beta^i} = \overline{f(\beta)} = \overline{0} = 0.$$

По теореме Безу многочлен $f(x)$ делится в кольце $\mathbb{C}[x]$ на два взаимно простых многочлена: $x - \beta$ и $x - \overline{\beta}$. Следовательно, по теореме 12(в) он делится на многочлен $g(x) = (x - \beta)(x - \overline{\beta})$. Так как $g(x) = x^2 - (\beta + \overline{\beta})x + \beta\overline{\beta}$ — также многочлен из $\mathbb{R}[x]$, то $g(x)$ делит $f(x)$ в $\mathbb{R}[x]$ (докажите). Поскольку у $f(x)$ нет собственных делителей в $\mathbb{R}[x]$, то $f(x)$ ассоциирован с $g(x)$. Следовательно, $f(x)$ — многочлен степени 2, и так как его корни в $\mathbb{C}$ не принадлежат $\mathbb{R}$, то $\Delta(f) < 0$. □

Следствие. *Любой многочлен нечетной степени из* $\mathbb{R}[x]$ *имеет корень в* $\mathbb{R}$.

2. Значительно более сложно устроены неприводимые многочлены в кольце $\mathbb{Q}[x]$. Полного их описания не существует, но можно указать некоторые достаточно большие классы таких многочленов. Один из основных методов изучения возможностей разложения многочленов из $\mathbb{Q}[x]$ на множители состоит в сведении задачи к разложению многочленов в кольце $\mathbb{Z}[x]$.

Определение 20. Многочлен $c(x) = c_0 + c_1x + \ldots + c_nx^n$ степени $n \geqslant 0$ с целыми коэффициентами назовем *примитивным* (по Гауссу), если $c_n > 0$ и $(c_0, c_1, \ldots, c_n) = 1$, в случае $n = 0$ имеется в виду равенство $c_0 = 1$.

Утверждение 28. *Для каждого ненулевого многочлена* $f(x) \in \mathbb{Q}[x]$ *в кольце* $\mathbb{Z}[x]$ *существует единственный ассоциированный с ним примитивный многочлен* $f^\star(x)$.

□ Если $\deg f(x) = n$, то $f(x)$ можно представить в виде

$$f(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1}\,x + \ldots + \frac{a_n}{b_n}\,x^n, \quad \text{где} \quad a_i \in \mathbb{Z},\ b_i \in \mathbb{N} \text{ для } i \in \overline{0,n}.$$

Пусть $q = [b_0, b_1, \ldots, b_n]$, тогда $q \cdot f(x) = g_0 + g_1x + \ldots + g_nx^n$ — многочлен с целыми коэффициентами, и если $d = (g_0, g_1, \ldots, g_n)$, то по теореме 9(г) главы 4 искомый многочлен имеет вид $f^\star(x) = \pm\frac{q}{d}\,f(x)$ (где знак определяется знаком коэффициента g_n). Если $h(x)$ — еще один примитивный многочлен из $\mathbb{Z}[x]$, ассоциированный с $f(x)$, то он ассоциирован и с $f^\star(x)$, и $h(x) = \frac{u}{v}\,f^\star(x)$, где $u, v \in \mathbb{N}$. Тогда $vh(x) = uf^\star(x)$, и так как НОД коэффициентов многочленов $uf^\star(x)$ и $vh(x)$ равны, соответственно, u и v, то из последнего равенства следует, что $u = v$, т. е. $h(x) = f^\star(x)$. □

Теорема 29. *Если* $a(x),\ b(x),\ c(x) \in \mathbb{Q}[x] \setminus \{0\}$ *и выполняется равенство* $a(x) = b(x)\,c(x)$, *то* $a^\star(x) = b^\star(x)\,c^\star(x)$.

□ Основное содержание доказательства составляет

Лемма 30 (Гаусс). *Произведение примитивных многочленов $b^\star(x)$ и $c^\star(x)$ есть примитивный многочлен.*

□ Пусть $b^\star(x) = \sum\limits_{i\geqslant 0} \beta_i x^i$, $c^\star(x) = \sum\limits_{i\geqslant 0} \gamma_i x^i$ и $b^\star(x)\cdot c^\star(x) = \sum\limits_{i\geqslant 0} \delta_i x^i$. Достаточно доказать, что для любого простого $p \in \mathbb{N}$ хотя бы один из коэффициентов δ_i не делится на p. Так как $b^\star(x)$ и $c^\star(x)$ — примитивные многочлены, то можно выбрать наименьшее $k \in \mathbb{N}_0$ такое, что $p \nmid \beta_k$, и наименьшее $l \in \mathbb{N}_0$ такое, что $p \nmid \gamma_l$. Тогда δ_{k+l} не делится на p, поскольку

$$\delta_{k+l} = \underline{\beta_0\gamma_{k+l} + \ldots + \beta_{k-1}\gamma_{l+1}} + \beta_k\gamma_l + \underline{\beta_{k+1}\gamma_{l-1} + \ldots + \beta_{k+l}\gamma_0}$$

и все подчеркнутые слагаемые в последней сумме делятся на p, а слагаемое $\beta_k\gamma_l$ по утверждению 13(б) главы 4 на p не делится. □

Теперь доказательство теоремы 29 завершается следующим образом. Так как $b^\star(x)$ и $c^\star(x)$ — примитивные многочлены, ассоциированные, соответственно, с $b(x)$ и $c(x)$, то $b^\star(x)\,c^\star(x)$ — примитивный многочлен, ассоциированный с $b(x)\,c(x) = a(x)$. □

Следствие 1. *Многочлен $a(x) \in \mathbb{Z}[x]$ положительной степени неприводим в кольце $\mathbb{Q}[x]$ тогда и только тогда, когда он неприводим в кольце $\mathbb{Z}[x]$ (т. е. не раскладывается в $\mathbb{Z}[x]$ на множители меньших степеней).*

□ Достаточно заметить, что $a(x) = ka^\star(x)$, где $k \in \mathbb{Z}$. □

Следствие 2. *Пусть $a(x)$ — многочлен степени $n > 0$ из $\mathbb{Q}[x]$ и $a^\star(x) = a_n^\star x^n + \ldots + a_1^\star x + a_0^\star$ — ассоциированный с $a(x)$ примитивный многочлен. Тогда если число $\alpha = \dfrac{u}{v} \in \mathbb{Q}$, где $u \in \mathbb{Z}$, $v \in \mathbb{N}$, $(u, v) = 1$, является корнем $a(x)$, то*

$$u \mid a_0^\star, \quad v \mid a_n^\star, \quad mv - u \mid a^\star(m) \ \text{ для любого } m \in \mathbb{Z},$$

в частности, $v - u \mid a^\star(1)$, $v + u \mid a^\star(-1)$.

□ Достаточно заметить, что $a^\star(x) = (x-\alpha)^\star\, c^\star(x)$ для подходящего примитивного $c^\star(x) \in \mathbb{Z}[x]$, и $(x-\alpha)^\star = vx - u$. □

Напомним, что для любых $m \in \mathbb{N}$ и $c \in \mathbb{Z}$ через $r_m(c)$ обозначается остаток от деления c на m, который можно рассматривать как элемент кольца $\mathbb{Z}_m$. Операции в этом кольце и кольце многочленов $\mathbb{Z}_m[x]$ обозначим символами $\oplus$ и $\otimes$. Для любого многочлена $a(x) = \sum a_i x^i \in \mathbb{Z}[x]$ через $r_m(a(x))$ обозначим многочлен из $\mathbb{Z}_m[x]$ вида $\sum r_m(a_i)x^i$. Используя свойства отношения сравнимости в $\mathbb{Z}$ (см. следствие 2 теоремы 2 главы 5), легко получить, что для любых многочленов $b(x), c(x) \in \mathbb{Z}[x]$ выполняется соотношение $r_m(b(x)\cdot c(x)) = r_m(b(x)) \otimes r_m(c(x))$.

Следствие 3. *Если $a(x) \in \mathbb{Q}[x]$ — приводимый многочлен степени n и $\mathrm{Ст}(a^\star(x)) = a_n^\star x^n$, то для каждого простого $p \in \mathbb{N}$, не делящего $a_n^\star$, многочлен $r_p(a^\star(x))$ приводим в кольце $\mathbb{Z}_p[x]$.*

□ Если $a(x) = b(x)\,c(x)$, где $\deg b(x) = k \in \overline{1, n-1}$, то выполняется равенство $r_p(a^\star(x)) = r_p(b^\star(x)) \otimes r_p(c^\star(x))$, причем ввиду условия $p \nmid a_n^\star$ можно утверждать, что $p \nmid b_k^\star$ и $\deg r_p(a^\star(x)) = n$, $\deg r_p(b^\star(x)) = k$. □

Полученные результаты можно использовать для перечисления рациональных корней и проверки неприводимости многочленов из $\mathbb{Q}[x]$.

Пример 6. Найти рациональные корни многочлена

$$a(x) = x^3 - \frac{3}{2}\,x - \frac{3}{2}.$$

Заметим, что $a^\star(x) = 2x^3 - 3x - 3$, и если элемент $\alpha = \dfrac{u}{v} \in \mathbb{Q}$, где $u \in \mathbb{Z}$, $v \in \mathbb{N}$, $(u, v) = 1$, есть корень $a(x)$, то по следствию 2 $u \mid 3$ и $v \mid 2$, т. е. $\alpha \in \{\pm 3, \pm 1, \pm\frac{1}{2}, \pm\frac{3}{2}\}$. Кроме того, должны выполняться соотношения $v - u \mid a^\star(1) = -4$ и $v + u \mid a^\star(-1) = -2$, поэтому остается лишь один кандидат в корни $a(x)$ — число $\alpha = -3$. Но $a(-3) = -24 \neq 0$, и потому многочлен $a(x)$ не имеет корней в $\mathbb{Q}$. Отсюда по утверждению 15 следует также, что $a(x)$ неприводим над $\mathbb{Q}$.

Пример 7. Проверить, является ли неприводимым многочлен

$$a(x) = x^4 + \frac{3}{7}\,x^3 + 3x^2 + \frac{4}{7}\,x + 5 \in \mathbb{Q}[x].$$

Воспользуемся следствием 3. Получаем:

$$a^\star(x) = 7x^4 + 3x^3 + 21x^2 + 4x + 35.$$

Будем перебирать простые числа $p \neq 7$. Если $p = 2$, то

$$r_2(a^\star(x)) = x^4 + x^3 + x^2 + 1 = (x + 1) \otimes (x^3 + x + 1)$$

— приводимый многочлен в $\mathbb{Z}_2[x]$. Для $p = 3$ получаем: $r_3(a^\star(x)) = x^4 + x + 2 \in \mathbb{Z}_3[x]$. Этот многочлен неприводим над $\mathbb{Z}_3$, так как он не имеет корней в $\mathbb{Z}_3$ и не делится ни на один из трех существующих в $\mathbb{Z}_3[x]$ неприводимых унитарных многочленов второй степени: $x^2 + 1$, $x^2 + x + 2$, $x^2 + 2x + 2$ (непосредственная проверка). Следовательно, многочлен $a(x)$ неприводим над $\mathbb{Q}$. Для доказательства неприводимости $a(x)$ можно и не убеждаться в неприводимости $r_3(a(x))$, а заметить лишь, что $r_3(a(x))$ не имеет корней в $\mathbb{Z}_3$, поскольку из рассмотрения многочлена $r_2(a(x))$ следует, что если $a(x)$ приводим, то он имеет делитель первой степени.

Замечание 9. Вытекающий из следствия 3 метод проверки неприводимости многочленов из $\mathbb{Q}[x]$ не является универсальным в том смысле, что существуют унитарные неприводимые многочлены $a(x) \in \mathbb{Z}[x]$ такие, что для любого простого $p \in \mathbb{N}$ многочлен $r_p(a(x))$ приводим над $\mathbb{Z}_p$. Например, таков многочлен $x^4 - 10x^2 + 1$.

В заключение докажем один широко используемый признак неприводимости многочленов над $\mathbb{Q}$.

Теорема 31 (Эйзенштейн).[11] *Пусть* $a(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$, $n > 0$, *и для некоторого простого* $p \in \mathbb{N}$ *выполняются условия*

$$p \nmid a_n; \tag{21}$$

$$p \mid a_i, \quad i \in \overline{0,\, n-1}; \tag{22}$$

$$p^2 \nmid a_0. \tag{23}$$

Тогда многочлен $a(x)$ *неприводим над* $\mathbb{Q}$.

□ Если многочлен $a(x)$ приводим в $\mathbb{Q}[x]$, то по следствию 1 теоремы 29 существуют многочлены $b(x), c(x) \in \mathbb{Z}[x]$ такие, что

$$a(x) = b(x)\,c(x), \quad \deg b(x) = k \in \overline{1,n}, \quad \deg c(x) = l \in \overline{1,n}, \quad k + l = n.$$

Следовательно, $r_p(a(x)) = r_p(b(x)) \otimes r_p(c(x))$ в $\mathbb{Z}_p[x]$. Из (21), (22) следует, что многочлен $r_p(a(x)) \in \mathbb{Z}_p[x]$ имеет вид $r_p(a(x)) = r_p(a_n)x^n$, $r_p(a_n) \neq 0$. Отсюда получаем: $r_p(b(x)) = r_p(b_k)x^k$, $r_p(c(x)) = r_p(c_l)x^l$. Так как $k, l \geqslant 1$, то из последних равенств следует, что $p \mid b_0$ и $p \mid c_0$. Но тогда $p^2 \mid a_0$, поскольку $a_0 = b_0c_0$, что противоречит условию (23). □

Важное значение этой теоремы состоит не только в том, что она позволяет просто доказывать неприводимость некоторых многочленов, но и в том, что она дает возможность их легко строить. В частности, из нее получается следующий результат, показывающий принципиальное различие между свойствами множества неприводимых многочленов над полем $\mathbb{Q}$ и множеств неприводимых многочленов над полями $\mathbb{R}$ и $\mathbb{C}$.

Следствие. *Над полем* $\mathbb{Q}$ *существуют неприводимые многочлены любой натуральной степени* n.

□ Например, для любого простого $p \in \mathbb{N}$ многочлен $x^n - p$ неприводим над $\mathbb{Q}$. □

Заметим, что приведенный пример существенно усиливает известное из средней школы утверждение об иррациональности числа $\sqrt[n]{p}$, эквивалентное лишь тому, что многочлен $x^n - p$ не имеет корней в $\mathbb{Q}$.

В книге Лидл Р., Нидеррайтер Г. «Конечные поля» (том 1, с. 61, см. раздел Научная литература) изложен метод Кронекера, позволяющий за конечное число шагов определить, приводим или нет многочлен над $\mathbb{Q}$ и, в случае приводимости, получить его каноническое разложение.

§ 8. КОЛЬЦО МНОГОЧЛЕНОВ ОТ НЕСКОЛЬКИХ ПЕРЕМЕННЫХ

1. Пусть R — кольцо с единицей e и $R[x]$ — кольцо многочленов от одного переменного x над R, построенное в § 1. Так как по теореме 2 $R_1 = R[x]$ есть кольцо с единицей ex^0, то над ним можно так же, как делалось в § 1, построить

[11] Ф. Г. М. Эйзенштейн (1823–1852) — немецкий математик.

кольцо многочленов $R_1[y]$ от переменного y. Элементами кольца $R_1[y]$ являются все последовательности вида

$$(a_0(x), a_1(x), \dots, a_n(x), \dots), \quad a_i(x) \in R_1, \tag{24}$$

в каждой из которых все многочлены, за исключением конечного их числа, равны $0x^0$, а переменное y определяется равенством

$$y = (0x^0,\, ex^0,\, 0x^0, \dots). \tag{25}$$

Операции сложения и умножения в $R_1[y]$ вводятся определением 2 а), б). Определением 2 в), г) задаются операция умножения последовательностей вида (24) на элементы $a(x) \in R_1$ и операция прибавления к таким последовательностям элементов $a(x) \in R_1$. С использованием этих операций любой элемент (24) кольца $R_1[y]$ может быть записан в виде суммы

$$a_0(x) + a_1(x)y + \dots + a_n(x)y^n, \tag{26}$$

где $n \in \mathbb{N}_0$ выбирается так, что в (24) $a_i(x) = 0$ для всех $i > n$. Используя каноническую запись каждого из многочленов $a_j(x)$:

$$a_j(x) = a_{0j} + a_{1j}x + \dots + a_{mj}x^m, \quad a_{ij} \in R,\ a_{ij} = 0 \text{ для } i > m,$$

и очевидные свойства дистрибутивности операции умножения последовательностей вида (24) на элементы из R_1, сумму (26), обозначая ее через $a(x, y)$, можно записать в виде

$$a(x,y) = \sum_{j=0}^{n}\sum_{i=0}^{m} a_{ij}x^iy^j = \sum_{i=0}^{m}\sum_{j=0}^{n} a_{ij}x^iy^j, \tag{27}$$

или в виде бесконечной суммы

$$a(x,y) = \sum_{i\geqslant 0}\sum_{j\geqslant 0} a_{ij}x^iy^j = \sum_{(i,j)} a_{ij}x^iy^j, \tag{28}$$

где суммирование производится по всем наборам $(i, j) \in \mathbb{N}_0 \times \mathbb{N}_0$. Представляя последовательности (24) в виде (28), подразумевают, что для некоторых $m, n \in \mathbb{N}_0$, при $i > m$, $j > n$ выполняются равенства $a_{ij} = 0$, т. е. $a_{ij}x^iy^j = 0x^iy^j = 0x^0y^0$ — нуль кольца $R_1[y]$, и в действительности, (28) — конечная сумма вида (27) (поэтому порядок суммирования в ней не важен).

Определение 21. Кольцо $R_1[y] = R[x][y]$ называют *кольцом многочленов от двух переменных* x и y над кольцом R и обозначают через $R[x, y]$. Элементы этого кольца называют *многочленами от двух переменных*, а выражение (27) (или (28)) — *канонической записью многочлена* $a(x, y)$. Элементы $a_{ij} \in R$ в канонической записи многочлена $a(x, y)$ называют его *коэффициентами*.

Таким образом, как и в случае многочленов от одного переменного, каждый многочлен $a(x, y)$ имеет бесконечно много коэффициентов $a_{ij} \in R$, и равенство многочлена (28) многочлену $b(x, y) = \sum_{(i,j)} b_{ij}x^iy^j$ из $R[x, y]$ означает, что $a_{ij} = b_{ij}$ для всех $i \geqslant 0$, $j \geqslant 0$.

Результаты операций над многочленами из $R[x,y]$, записанными в канонической форме, представляются следующим образом:

$$a(x,y)+b(x,y)=\sum_{(i,j)}a_{ij}x^iy^j+\sum_{(i,j)}b_{ij}x^iy^j=\sum_{(i,j)}(a_{ij}+b_{ij})\,x^iy^j,$$

$$a(x,y)\cdot b(x,y)=\sum_{(i,j)}\left(\sum_{r=0}^{i}\sum_{s=0}^{j}a_{rs}b_{i-r,j-s}\right)x^iy^j.$$

Первое из этих равенств очевидно, а второе легко следует из равенства

$$a(x,y)\cdot b(x,y)=\sum_{(i_1,j_1)}\sum_{(i_2,j_2)}a_{i_1j_1}\cdot b_{i_2j_2}\,x^{i_1+i_2}\cdot y^{j_1+j_2},$$

которое, в свою очередь, выводится из дистрибутивности умножения и равенств $a_{i_1j_1}x^{i_1}y^{j_1}\cdot b_{i_2j_2}x^{i_2}y^{j_2}=a_{i_1j_1}b_{i_2j_2}x^{i_1+i_2}y^{j_1+j_2}$, вытекающих из определения операции умножения в кольце $R_1[y]$.

Замечание 10. Использование канонической записи многочленов из $R[x,y]$ существенно облегчает выполнение операций над ними. Для наглядности достаточно заметить, что переход к первоначальному представлению многочленов в виде последовательностей превращает сумму (28) в сумму последовательностей вида

$$a_{ij}x^iy^j=(\overbrace{(0,\dots,0,\dots),\ \dots,\ (0,\dots,0,\dots)}^{j\text{ нулевых последовательностей}},\ (\underbrace{0,\dots,0}_{i\text{ нулей}},a_{ij},0,\dots),\ (0,\dots,0,\dots),\ \dots).$$

2. Аналогично, индуктивным методом, строится кольцо многочленов от произвольного конечного числа переменных.

Определение 22. Если $R[x_1,\dots,x_{n-1}]$ — кольцо многочленов от $n-1$ переменных $x_1,\dots,x_{n-1}$ над кольцом R с единицей, то кольцо многочленов

$$R[x_1,\dots,x_n]=R[x_1,\dots,x_{n-1}][x_n]$$

называют *кольцом многочленов от n переменных* $x_1,\dots,x_n$ над кольцом R.

Таким образом, кольцо $R[x_1,\dots,x_n]$ есть множество всех последовательностей вида

$$(a_0(x_1,\dots,x_{n-1}),\ \dots,\ a_i(x_1,\dots,x_{n-1}),\ \dots),$$
$$a_i(x_1,\dots,x_{n-1})\in R[x_1,\dots,x_{n-1}],$$

в которых все члены $a_i(x_1,\dots,x_{n-1})$, за исключением конечного числа, равны нулю, а переменное x_n есть последовательность

$$x_n=(0x_1^0\dots x_{n-1}^0,\ ex_1^0\dots x_{n-1}^0,\ 0x_1^0\dots x_{n-1}^0,\ \dots).$$

Операции на $R[x_1,\dots,x_n]$ вводятся определением 2. С использованием этих операций каждый элемент $a(x_1,\dots,x_n)\in R[x_1,\dots,x_n]$ может быть представлен в виде суммы

$$a(x_1,\dots,x_n)=\sum_{i_1=0}^{m_1}\dots\sum_{i_n=0}^{m_n}a_{i_1,\dots,i_n}x_1^{i_1}\dots x_n^{i_n},\quad a_{i_1,\dots,i_n}\in R \tag{29}$$

или в виде формально бесконечной суммы

$$a(x_1,\dots,x_n)=\sum_{(i_1,\dots,i_n)}a_{i_1,\dots,i_n}x_1^{i_1}\dots x_n^{i_n}, \tag{30}$$

в которой символ $\sum\limits_{(i_1,\dots,i_n)}$ означает суммирование по всем различным наборам $(i_1,\dots,i_n)\in\mathbb{N}_0^n$, но подразумевается, что все слагаемые, за исключением конечного их числа, равны нулю (т. е. равны нулю соответствующие коэффициенты $a_{i_1,\dots,i_n}$).

Определение 23. Элементы кольца $R[x_1,\dots,x_n]$ называются *многочленами от n переменных* $x_1,\dots,x_n$ над R. Представление многочлена $a(x_1,\dots,x_n)\in R[x_1,\dots,x_n]$ в виде (29) или в виде (30) называют его *канонической записью*, элементы $a_{i_1,\dots,i_n}$ в этой записи называют *коэффициентами* многочлена $a(x_1,\dots,x_n)$, а слагаемые $a_{i_1,\dots,i_n}x_1^{i_1}\dots x_n^{i_n}$ — *одночленами*, или *мономами*, из его канонической записи.

Каноническая запись (30) многочлена из $R[x_1,\dots,x_n]$ однозначна с точностью до перестановки слагаемых: если

$$b(x_1,\dots,x_n)=\sum_{(i_1,\dots,i_n)}b_{i_1,\dots,i_n}x_1^{i_1}\dots x_n^{i_n}\in R[x_1,\dots,x_n],$$

то $b(x_1,\dots,x_n)=a(x_1,\dots,x_n)$ тогда и только тогда, когда $b_{i_1,\dots,i_n}=a_{i_1,\dots,i_n}$ для всех $(i_1,\dots,i_n)\in\mathbb{N}_0^n$. Результаты операций над многочленами в канонической записи представляются следующим образом:

$$a(x_1,\dots,x_n)+b(x_1,\dots,x_n)=\sum_{(i_1,\dots,i_n)}\left(a_{i_1,\dots,i_n}+b_{i_1,\dots,i_n}\right)x_1^{i_1}\dots x_n^{i_n},$$

$$a(x_1,\dots,x_n)\cdot b(x_1,\dots,x_n)=$$
$$=\sum_{(i_1,\dots,i_n)}\left(\sum_{r_1=0}^{i_1}\dots\sum_{r_n=0}^{i_n}a_{r_1,\dots,r_n}b_{i_1-r_1,\dots,i_n-r_n}\right)x_1^{i_1}\dots x_n^{i_n}.$$

Последнее равенство получается из равенства

$$a(x_1,\dots,x_n)\cdot b(x_1,\dots,x_n)=$$
$$=\sum_{(r_1,\dots,r_n)}\sum_{(s_1,\dots,s_n)}a_{r_1,\dots,r_n}b_{s_1,\dots,s_n}x_1^{r_1+s_1}\dots x_n^{r_n+s_n}, \tag{31}$$

которое выводится из дистрибутивности умножения и из соотношений $x_ib=bx_i$, $x_ix_j=x_jx_i$, справедливых для любых $b\in R$ и $i,j\in\overline{1,n}$.

3. Кольцо $R[x_1,\dots,x_n]$, как и кольцо многочленов от одного переменного, сохраняет некоторые свойства исходного кольца R.

Теорема 32. *Кольцо $R[x_1,\dots,x_n]$ коммутативно тогда и только тогда, когда коммутативно кольцо R, и содержит делители нуля тогда и только тогда, когда R содержит делители нуля.*

□ При $n=1$ это — теорема 2. Доказательство в общем случае легко проводится индукцией по n с использованием определения 22. □

Замечание 11. Нулем и единицей кольца $R[x_1,\dots,x_n]$ являются, соответственно, многочлены $0x_1^0\dots x_n^0$ и $ex_1^0\dots x_n^0$. Как и в кольце многочленов от одного переменного, для краткости будем обозначать их теми же символами, которыми обозначаются нуль и единица в R, т. е. положим

$$0x_1^0\dots x_n^0=0,\quad ex_1^0\dots x_n^0=e.$$

При этом, по сути дела, исходное кольцо R отождествляется с изоморфным ему подкольцом $\overline{R}=\{rx_1^0\dots x_n^0:\ r\in R\}$ кольца $R[x_1,\dots,x_n]$ (см. замечание 3). Более того, каждое кольцо $R[x_1,\dots,x_m]$, $m\in\overline{1,n-1}$, отождествляется с изоморфным ему подкольцом

$$\overline{R[x_1,\dots,x_m]}=\{a(x_1,\dots,x_m)\cdot x_{m+1}^0\dots x_n^0:\ a(x_1,\dots,x_m)\in R[x_1,\dots,x_m]\}$$

кольца $R[x_1,\dots,x_n]$ (ввиду равенств $a(x_1,\dots,x_m)=a(x_1,\dots,x_m)\cdot e=$ $=(a(x_1,\dots,x_m)\,ex_1^0\dots x_m^0)\cdot x_{m+1}^0\dots x_n^0=a(x_1,\dots,x_m)\,x_{m+1}^0\dots x_n^0)$).

И наоборот, это соглашение позволяет употреблять компактную запись многочленов из $R[x_1,\dots,x_n]$ в каноническом виде, опуская в одночленах из (29) сомножители $x_s^{i_s}$, для которых $i_s=0$, т. е. используя равенства типа

$$x_1^{i_1}\dots x_m^{i_m}\cdot x_{m+1}^0\dots x_n^0=x_1^{i_1}\dots x_m^{i_m}\cdot ex_1^0\dots x_n^0=x_1^{i_1}\dots x_m^{i_m}\cdot e=x_1^{i_1}\dots x_m^{i_m}.$$

Например, многочлен из $R[x_1,\dots,x_n]$

$$f(x_1,\dots,x_n)=ax_1^0x_2^0\dots x_n^0+bx_1^2x_2^0\dots x_n^0+cx_1^0\dots x_{n-3}^0x_{n-2}^1x_{n-1}^3x_n^0$$

может быть записан в виде

$$f(x_1,\dots,x_n)=a+bx_1^2+cx_{n-2}x_{n-1}^3.$$

Понятие степени многочлена обобщается на многочлены от нескольких переменных следующим образом:

Определение 24. *Степенью одночлена* $ax_1^{i_1}\dots x_n^{i_n}$ из $R[x_1,\dots,x_n]$ называют параметр

$$\deg ax_1^{i_1}\dots x_n^{i_n}=\begin{cases}-\infty, & \text{если } a=0;\\ i_1+\dots+i_n, & \text{если } a\neq 0.\end{cases}$$

Степенью указанного одночлена *по переменному* x_s называют параметр

$$\deg_{x_s} ax_1^{i_1}\dots x_n^{i_n}=\begin{cases}-\infty, & \text{если } a=0,\\ i_s, & \text{если } a\neq 0.\end{cases}$$

Степенью произвольного многочлена (30) и его *степенью по переменной* x_s называют, соответственно

$$\deg a(x_1,\dots,x_n)=\max\{\deg a_{i_1,\dots,i_n}x_1^{i_1}\dots x_n^{i_n}:\ (i_1,\dots,i_n)\in\mathbb{N}_0^n\},$$

$$\deg_{x_s} a(x_1,\dots,x_n)=\max\{\deg_{x_s} a_{i_1,\dots,i_n}x_1^{i_1}\dots x_n^{i_n}:\ (i_1,\dots,i_n)\in\mathbb{N}_0^n\}.$$

Если $\deg_{x_s} a(x_1,\dots,x_n)\leqslant 0$, то говорят, что многочлен $a(x_1,\dots,x_n)$ не зависит от переменного x_s (или, что он зависит от x_s лишь формально). Последнее равносильно тому, что любой одночлен $a_{i_1,\dots,i_n}x_1^{i_1}\dots x_n^{i_n}$ из (30) удовлетворяет условию: если $a_{i_1,\dots,i_n}\neq 0$, то $i_s=0$.

В дальнейшем, если ясно (или неважно), о каком числе n переменных идет речь, кольцо $R[x_1,\dots,x_n]$ и его элементы $a(x_1,\dots,x_n)$, для краткости будем обозначать через $R[\vec{x}]$ и $a(\vec{x})$, где $\vec{x}=(x_1,\dots,x_n)$.

Непосредственно из определения следует, что для любых многочленов $a(\vec{x})$, $b(\vec{x})\in R[\vec{x}]$ верны соотношения

$$\deg a(\vec{x})\leqslant\sum_{s=1}^{n}\deg_{x_s} a(\vec{x}),$$

$$\deg(a(\vec{x})+b(\vec{x}))\leqslant\max\{\deg a(\vec{x}),\deg b(\vec{x})\},$$

$$\deg a(\vec{x})\,b(\vec{x})\leqslant\deg a(\vec{x})+\deg b(\vec{x}).$$

Каждое из этих соотношений может быть, в зависимости от выбора многочленов $a(\vec{x})$ и $b(\vec{x})$, как строгим неравенством, так и равенством (соответствующие примеры читателю предлагается привести самостоятельно). Ниже будет доказано, что последнее соотношение является равенством для любых многочленов $a(\vec{x})$ и $b(\vec{x})$ из $R[\vec{x}]$, если R — кольцо без делителей нуля. Однако доказательство этого факта проводится несколько сложнее, чем в кольце многочленов от одного переменного, поскольку в канонической записи (29) многочлена $a(\vec{x})$ может содержаться несколько различных одночленов степени $\deg a(\vec{x})$.

Определение 25. Ненулевой многочлен (29) называют *формой степени* k, если степени всех его ненулевых одночленов равны k. Формы степеней 1, 2, 3 называют, соответственно, *линейными*, *квадратичными* и *кубическими*.

Очевидно, что любой многочлен $a(\vec{x})\in R[\vec{x}]\setminus\{0\}$ степени k может быть однозначно представлен в виде суммы

$$a(\vec{x})=a^{(0)}(\vec{x})+a^{(1)}(\vec{x})+\ldots+a^{(k)}(\vec{x}),\tag{32}$$

где $a^{(r)}(\vec{x})$ для $r\in\overline{1,k}$ — либо нулевой многочлен, либо форма степени r, и $a^{(k)}(\vec{x})\neq 0$.

Определение 26. Равенство (32) назовем *представлением многочлена* $a(\vec{x})$ *в виде суммы форм*.

Из определения произведения многочленов следует, что произведение двух ненулевых форм степеней k и l есть либо нуль, либо форма степени $k+l$.

Теорема 33. *Если R — кольцо с единицей без делителей нуля, то для любых $a(\vec{x}), b(\vec{x}) \in R[\vec{x}]$ верно равенство*

$$\deg a(\vec{x})\, b(\vec{x}) = \deg a(\vec{x}) + \deg b(\vec{x}).$$

□ Нетривиален лишь случай, когда $\deg a(\vec{x}) = k > 0$, $\deg b(\vec{x}) = l$. В этой ситуации пусть представления многочленов $a(\vec{x})$ и $b(\vec{x})$ в виде суммы форм имеют вид соответственно (32) и

$$b(\vec{x}) = b^{(0)}(\vec{x}) + b^{(1)}(\vec{x}) + \ldots + b^{(l)}(\vec{x}). \tag{33}$$

Перемножая равенства (32) и (33) почленно, получаем следующее представление $a(\vec{x})\, b(\vec{x})$ в виде суммы форм:

$$a(\vec{x})\, b(\vec{x}) = [a^{(0)}(\vec{x})\, b^{(0)}(\vec{x})] + [a^{(0)}(\vec{x})\, b^{(1)}(\vec{x}) + a^{(1)}(\vec{x})\, b^{(0)}(\vec{x})] + \ldots$$
$$\ldots + [a^{(k-1)}(\vec{x})\, b^{(l)}(\vec{x}) + a^{(k)}(\vec{x})\, b^{(l-1)}(\vec{x})] + a^{(k)}(\vec{x})\, b^{(l)}(\vec{x}).$$

Так как по теореме 32 в $R[\vec{x}]$ нет делителей нуля, то в полученной сумме $a^{(k)}(\vec{x})\, b^{(l)}(\vec{x})$ — форма степени $k+l$, а каждое выражение в квадратных скобках есть либо нуль, либо форма степени строго меньшей, чем $k+l$. Следовательно, $\deg a(\vec{x})\, b(\vec{x}) = k+l$. □

4. Каждый многочлен $a(\vec{x}) \in R[x_1, \ldots, x_n]$ задает некоторую функцию на множестве $R^n = R \times \ldots \times R$ со значениями в R.

Определение 27. *Значением многочлена $a(\vec{x})$* вида (30) *в точке $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n) \in R^n$* называется следующий элемент кольца R:

$$a(\vec{\alpha}) = \sum_{(i_1, \ldots, i_n)} a_{i_1 \ldots i_n} \alpha_1^{i_1} \ldots \alpha_n^{i_n}.$$

Функцию $a_R\colon R^n \to R$, определяемую условием

$$\forall\, \vec{\alpha} \in R^n :\ a_R(\vec{\alpha}) = a(\vec{\alpha}),$$

называют *полиномиальной функцией, определяемой многочленом $a(\vec{x})$*.

Очевидно, что значение суммы двух многочленов из $R[x_1, \ldots, x_n]$ в любой точке $\vec{\alpha} \in R^n$ равно сумме их значений в этой точке. Кроме того, справедливо

Утверждение 34. *Если кольцо R коммутативно и $c(\vec{x}) = a(\vec{x})\, b(\vec{x})$, где $a(\vec{x}), b(\vec{x}) \in R[\vec{x}]$, то для любого $\vec{\alpha} \in R^n$ справедливо равенство $c(\vec{\alpha}) = a(\vec{\alpha})\, b(\vec{\alpha})$.*

□ Доказательство проводится с использованием равенства (31) и предоставляется читателю. □

Из многочисленных результатов, связанных с представлением функций на кольце полиномами, мы приведем лишь следующий важный в прикладном аспекте результат.

Теорема 35. *Если P — конечное поле из q элементов, то для любой функции $\varphi\colon P^n \to P$ существует единственный многочлен $a(\vec{x}) \in P[x_1, \ldots, x_n]$, имеющий по каждому переменному степень не выше, чем $q-1$, и такой, что $\varphi = a_R$.*

□ По теореме 6 для каждого элемента $\beta \in P$ существует многочлен $\delta_\beta \in P[x]$, имеющий степень не выше, чем $q-1$, и такой, что

$$\forall\, \alpha \in P\colon\ \delta_\beta(\alpha) = \begin{cases} e, & \text{если } \alpha = \beta, \\ 0, & \text{если } \alpha \neq \beta. \end{cases}$$

Этот многочлен имеет вид $\delta_\beta(x) = e - (x-\beta)^{q-1}$ (докажите). Тогда, используя утверждение 34, нетрудно проверить, что многочлен

$$a(x_1, \ldots, x_n) = \sum_{(\beta_1, \ldots, \beta_n) \in P^n} \varphi(\beta_1, \ldots, \beta_n) \cdot \delta_{\beta_1}(x_1) \ldots \delta_{\beta_n}(x_n)$$

удовлетворяет условиям: $\varphi = a_R$,

$$\deg_{x_s} a(\vec{x}) \leqslant q-1 \quad \text{для } \ s \in \overline{1,n}. \tag{34}$$

Докажем его единственность. Любой многочлен $a(\vec{x}) \in R[\vec{x}]$ со свойством (34) имеет вид

$$a(\vec{x}) = \sum_{i_1=0}^{q-1} \ldots \sum_{i_n=0}^{q-1} a_{i_1, \ldots, i_n} x_1^{i_1} \ldots x_n^{i_n}, \tag{35}$$

и число его ненулевых коэффициентов не превосходит q^n. Следовательно, общее количество таких многочленов равно $|P|^{q^n} = q^{q^n}$. Но количество различных отображений $\varphi\colon P^n \to P$ также равно q^{q^n}, и поскольку каждое такое отображение представляется многочленом вида (35), а разные отображения представляются разными многочленами, то это представление однозначно. □

5. Мы уже отмечали, что кольцо $R[x_1, \ldots, x_n]$ можно рассматривать как расширение кольца R (см. замечание 11). Следующий принципиально важный результат показывает, что это расширение является «универсальным» в том смысле, что оно позволяет описать большой класс других расширений кольца R.

Теорема 36. *Пусть R' — коммутативное кольцо с единицей e и R — его подкольцо с той же единицей. Тогда для любых $\alpha_1, \ldots, \alpha_n \in R'$ множество $R[\alpha_1, \ldots, \alpha_n]$ всех элементов $r' \in R'$, представимых в виде $r' = a(\alpha_1, \ldots, \alpha_n)$, $a(\vec{x}) \in R[\vec{x}]$, есть подкольцо кольца R'.*

□ Очевидно, что подмножество $R[\alpha_1, \ldots, \alpha_n]$ замкнуто относительно заданных на R' операций сложения и умножения (см. утверждение 34) и $(R[\alpha_1, \ldots, \alpha_n], +)$ — группа. Всем остальным аксиомам кольца алгебра $(R[\vec{\alpha}], +, \cdot)$ удовлетворяет ввиду того, что им удовлетворяет алгебра $(R', +, \cdot)$. □

Нетрудно увидеть, что кольцо $R[\alpha_1, \ldots, \alpha_n]$ содержит подкольцо R и элементы $\alpha_1, \ldots, \alpha_n$, и $R[\alpha_1, \ldots, \alpha_n]$ — наименьшее подкольцо в R' с этими свойствами (докажите самостоятельно). Его называют *расширением подкольца R кольца R' элементами $\alpha_1, \ldots, \alpha_n \in R'$*.

§ 9. ИНВАРИАНТНЫЕ ПОДКОЛЬЦА. СИММЕТРИЧЕСКИЕ МНОГОЧЛЕНЫ

Один из способов изучения свойств многочленов кольца $R[x_1,\dots,x_n]$ состоит в описании таких многочленов, которые не изменяются при различных преобразованиях этого кольца. Ниже рассматривается важный частный класс таких преобразований.

Каждой подстановке $\pi = \begin{pmatrix} 1 & \dots & n \\ \pi(1) & \dots & \pi(n) \end{pmatrix}$ можно поставить в соответствие отображение $\hat{\pi}\colon R[x_1,\dots,x_n] \to R[x_1,\dots,x_n]$, определяемое правилом

$$\forall\, a(\vec{x}) \in R[\vec{x}]:\ \hat{\pi}(a(\vec{x})) = \sum_{(i_1,\dots,i_n)} a_{i_1,\dots,i_n} x_{\pi(1)}^{i_1} \dots x_{\pi(n)}^{i_n}. \tag{36}$$

Утверждение 37. *Отображение $\hat{\pi}$ есть изоморфизм кольца $R[\vec{x}]$ на себя.*

□ Непосредственно из (36) нетрудно увидеть, что $\hat{\pi}$ — биекция. Кроме того, если $a(\vec{x}), b(\vec{x}) \in R[\vec{x}]$, то верны равенства

$$\begin{aligned}\hat{\pi}(a(\vec{x}) + b(\vec{x})) &= \sum_{(i_1,\dots,i_n)} (a_{i_1,\dots,i_n} + b_{i_1,\dots,i_n})\, x_{\pi(1)}^{i_1} \dots x_{\pi(n)}^{i_n} = \\ &= \sum_{(i_1,\dots,i_n)} a_{i_1,\dots,i_n} x_{\pi(1)}^{i_1} \dots x_{\pi(n)}^{i_n} + \sum_{(i_1,\dots,i_n)} b_{i_1,\dots,i_n} x_{\pi(1)}^{i_1} \dots x_{\pi(n)}^{i_n} = \\ &= \hat{\pi}(a(\vec{x})) + \hat{\pi}(b(\vec{x})).\end{aligned}$$

Отсюда, используя (31), получаем также, что

$$\begin{aligned}\hat{\pi}(a(\vec{x}) \cdot b(\vec{x})) &= \sum_{(r_1,\dots,r_n)} \sum_{(s_1,\dots,s_n)} \hat{\pi}(a_{r_1,\dots,r_n} b_{s_1,\dots,s_n} x_1^{r_1+s_1} \dots x_n^{r_n+s_n}) = \\ &= \sum_{(r_1,\dots,r_n)} \sum_{(s_1,\dots,s_n)} a_{r_1,\dots,r_n} b_{s_1,\dots,s_n} x_{\pi(1)}^{r_1+s_1} \dots x_{\pi(n)}^{r_n+s_n} = \hat{\pi}(a(\vec{x})) \cdot \hat{\pi}(b(\vec{x})).\end{aligned}$$

Следовательно, $\hat{\pi}$ — изоморфизм колец. □

Определение 28. Многочлен $a(\vec{x}) \in R[x_1,\dots,x_n]$ называется *инвариантным относительно подстановки* $\pi \in S$, если $\hat{\pi}(a(\vec{x})) = a(\vec{x})$.

Пример 8. Многочлен $x_1 + x_2 \in R[x_1,\dots,x_n]$ инвариантен относительно подстановки $\begin{pmatrix} 1\ 2\ 3\ \dots\ n \\ 2\ 1\ 3\ \dots\ n \end{pmatrix}$, но при $n > 2$ он не инвариантен относительно подстановки $\begin{pmatrix} 1\ 2\ \dots\ n{-}1\ n \\ 2\ 3\ \dots\ \ n\ \ \ 1 \end{pmatrix}$. Для любой подстановки $\pi \in S$ многочлен $x_1 + x_2^2 + \dots + x_n^n$ не инвариантен относительно π, а многочлен $x_1^k + \dots + x_n^k$, $k \in \mathbb{N}$, инвариантен относительно π.

Любому подмножеству $G \subset S_n$ можно поставить в соответствие подмножество $I_{R[\vec{x}]}(G) = I(G)$ многочленов из $R[x_1,\dots,x_n]$, инвариантных относительно каждой подстановки $\pi \in G$:

$$I(G) = \{a(\vec{x}) \in R[x]:\ \forall\, \pi \in G\ (\pi(a(\vec{x})) = a(\vec{x}))\}.$$

Заметим, что подмножество $I(G)$ всегда непусто, поскольку содержит нуль и все многочлены нулевой степени.

Утверждение 38. *Подмножество $I(G)$ есть подкольцо кольца $R[\vec{x}]$.*

□ Замкнутость $I(G)$ относительно каждой операции $* \in \{+, \cdot\}$ следует из утверждения 37, поскольку для любой подстановки $\pi \in G$ и многочленов $a(\vec{x}), b(\vec{x}) \in I(G)$

$$\hat{\pi}(a(\vec{x}) * b(\vec{x})) = \hat{\pi}(a(\vec{x})) * \hat{\pi}(b(\vec{x})) = a(\vec{x}) * b(\vec{x}).$$

Так как операция $+$ на $I(G)$ ассоциативна, $0 \in I(G)$ и для каждого $a(\vec{x}) \in I(G)$ многочлен $-a(\vec{x})$, очевидно, также принадлежит $I(G)$, то $(I(G), +)$ — абелева группа. Ассоциативность умножения на $I(G)$ и его дистрибутивность относительно сложения следуют из того, что $R[\vec{x}]$ — кольцо. □

Определение 29. Подкольцо $I(G)$ называется *подкольцом инвариантов* кольца $R[\vec{x}]$ относительно множества подстановок G.

Ниже дается описание подкольца $I(G)$ в важном частном случае, когда $G = S_n$.

Определение 30. Многочлен $a(\vec{x}) \in R[x_1, \ldots, x_n]$ называется *симметрическим*, если он инвариантен относительно любой подстановки $\pi \in S_n$ (т. е. если $a(\vec{x}) \in I(S_n)$). Подкольцо $I(S_n) = I_{R[\vec{x}]}(S_n)$ кольца $R[\vec{x}]$ называется *кольцом симметрических многочленов* от n переменных над R и обозначается через $\Sigma_R[x_1, \ldots, x_n]$.

Прежде всего приведем основные примеры симметрических многочленов.

Определение 31. *Элементарными симметрическими многочленами* называются многочлены

$$\begin{aligned}
&\sigma_1(\vec{x}) = x_1 + x_2 + \ldots + x_n,\\
&\sigma_2(\vec{x}) = x_1x_2 + x_1x_3 + \ldots + x_1x_n + x_2x_3 + \ldots + x_{n-1}x_n,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&\sigma_k(\vec{x}) = \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant n} x_{i_1}x_{i_2}\ldots x_{i_k}, \quad 1 \leqslant k \leqslant n,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&\sigma_n(\vec{x}) = x_1x_2\ldots x_n.
\end{aligned}$$

Очевидно, что $\sigma_k(\vec{x})$ есть форма степени k из $\Sigma_R[x_1, \ldots, x_n]$.

Интерес к элементарным симметрическим многочленам обусловлен, прежде всего, следующим классическим результатом.

Теорема 39 (Виет). *Если P — поле разложения унитарного многочлена $f(x) \in P[x]$ степени n и $\alpha_1, \ldots, \alpha_n$ — все корни $f(x)$ в P (с учетом их кратностей), то*

$$f(x) = x^n - \sigma_1(\vec{\alpha})\, x^{n-1} + \sigma_2(\vec{\alpha})\, x^{n-2} + \ldots + (-1)^n\sigma_n(\vec{\alpha}),$$

где $\sigma_k(\vec{x})$ — элементарный симметрический многочлен степени k из $\Sigma_R[\vec{x}]$ и $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$.

□ Нужное равенство легко получается из разложения

$$f(x) = (x - \alpha_1) \dots (x - \alpha_n). \quad \square$$

Главное свойство элементарных симметрических многочленов, к доказательству которого мы приступаем, состоит в том, что любой симметрический многочлен может быть выражен через них с помощью конечного числа операций сложения и умножения. Получим предварительно несколько вспомогательных результатов представляющих также самостоятельный интерес.

Определение 32. Говорят, что ненулевой одночлен $ax_1^{i_1} \dots x_n^{i_n}$ *старше* одночлена $bx_1^{j_1} \dots x_n^{j_n}$, и пишут $ax_1^{i_1} \dots x_n^{i_n} \succ bx_1^{j_1} \dots x_n^{j_n}$, если либо $b = 0$, либо положительна первая ненулевая из разностей

$$(i_1 + \dots + i_n) - (j_1 + \dots + j_n), \quad i_1 - j_1, \ \dots, \ i_n - j_n.$$

Одночлены вида $ax_1^{i_1} \dots x_n^{i_n}$ и $bx_1^{i_1} \dots x_n^{i_n}$ называют *подобными*.

Старший одночлен из канонической записи (30) ненулевого многочлена $a(\vec{x}) \in R[\vec{x}]$ называют *старшим членом* многочлена $a(\vec{x})$ и обозначают через $\mathrm{Ст}(a(\vec{x}))$.

Таким образом, согласно определению, одночлен большей степени старше одночлена меньшей степени. Если степени двух ненулевых одночленов равны, то старше тот из них, у которого степень x_1 больше. В случае равенства степеней переменного x_1 в этих одночленах, старше тот, у которого больше степень переменного x_2, и т. д. Очевидно, что отношение $\prec$ позволяет строго упорядочить все слагаемые в канонической записи многочлена $a(\vec{x})$ (такое упорядочение называют *лексикографическим*), и поэтому определение старшего члена многочлена $a(\vec{x})$ корректно.

Пример 9. В кольце $R[x_1, x_2]$ справедливы соотношения

$$0 \prec e \prec x_2 \prec x_1 \prec x_2^2 \prec x_1x_2 \prec x_1^2 \prec x_2^3 \prec x_1x_2^2 \prec x_1^2x_2 \prec x_1^3 \prec \dots \ .$$

Теорема 40. *Если произведение старших членов многочленов $a(\vec{x})$, $b(\vec{x}) \in R[\vec{x}]$ не равно нулю, то справедливо равенство*

$$\mathrm{Ст}(a(\vec{x}) \cdot b(\vec{x})) = \mathrm{Ст}(a(\vec{x})) \cdot \mathrm{Ст}(b(\vec{x})).$$

□ Пусть $\mathrm{Ст}(a(\vec{x})) = ax_1^{\alpha_1} \dots x_n^{\alpha_n}$, $\mathrm{Ст}(b(\vec{x})) = bx_1^{\beta_1} \dots x_n^{\beta_n}$. Выберем произвольно ненулевые одночлены из канонических записей многочленов $a(\vec{x})$ и $b(\vec{x})$, соответственно: $u(\vec{x}) = a'x_1^{r_1} \dots x_n^{r_n}$ и $v(\vec{x}) = b'x_1^{s_1} \dots x_n^{s_n}$. Ввиду равенства (31), очевидно, достаточно показать, что если $u(\vec{x}) \prec \mathrm{Ст}(a(\vec{x}))$ или $v(\vec{x}) \prec \mathrm{Ст}(b(\vec{x}))$, то

$$\begin{aligned} u(\vec{x}) \cdot v(\vec{x}) = a'b'x_1^{r_1+s_1} \dots x_n^{r_n+s_n} \prec \mathrm{Ст}(a(\vec{x})) \cdot \mathrm{Ст}(b(\vec{x})) = \\ = abx_1^{\alpha_1+\beta_1} \dots x_n^{\alpha_n+\beta_n}. \end{aligned} \tag{37}$$

Рассмотрим последовательности

$$A_0 = \sum_{i=1}^{n} \alpha_i - \sum_{i=1}^{n} r_i, \quad A_1 = \alpha_1 - r_1, \ \dots, \ A_n = \alpha_n - r_n$$

и

$$B_0 = \sum_{i=1}^{n} \beta_i - \sum_{i=1}^{n} s_i, \quad B_1 = \beta_1 - s_1, \ \ldots, \ B_n = \beta_n - s_n.$$

Согласно сделанным предположениям, в каждой из этих последовательностей первое ненулевое число (если оно есть) положительно и хотя бы одна из этих последовательностей ненулевая. В таком случае последовательность

$$A_0 + B_0 = \sum_{i=1}^{n}(\alpha_i + \beta_i) - \sum_{i=1}^{n}(r_i + s_i),$$
$$A_1 + B_1 = (\alpha_1 + \beta_1) - (r_1 + s_1), \ \ldots, \ A_n + B_n = (\alpha_n + \beta_n) - (r_n + s_n)$$

содержит ненулевые числа и первое из них положительно. Это в совокупности с условием $ab \neq 0$ и доказывает соотношение (37). □

Обратите внимание на то, что теорема 40 усиливает теорему 33.

Лемма 41. *Если* $\tau(x_1, \ldots, x_n)$ *— ненулевой симметрический многочлен и* $\mathrm{Ст}(\tau(\vec{x})) = ux_1^{\alpha_1} \ldots x_n^{\alpha_n}$, *то* $\alpha_1 \geqslant \alpha_2 \geqslant \ldots \geqslant \alpha_n$.

□ Предположим, что $\alpha_i < \alpha_{i+1}$ для некоторого $i \in \overline{1, n-1}$. Рассмотрим подстановку $\pi = \begin{pmatrix} 1 & 2 & \ldots & i & i{+}1 & \ldots & n \\ 1 & 2 & \ldots & i{+}1 & i & \ldots & n \end{pmatrix}$. Так как $\hat{\pi}(\tau(\vec{x})) = \tau(\vec{x})$, то одночлен

$$\hat{\pi}(\mathrm{Ст}(\tau(\vec{x}))) = ux_1^{\alpha_1} \ldots x_{i-1}^{\alpha_{i-1}} x_i^{\alpha_{i+1}} x_{i+1}^{\alpha_i} x_{i+2}^{\alpha_{i+2}} \ldots x_n^{\alpha_n}$$

входит слагаемым в каноническую запись многочлена $\tau(\vec{x})$. Но он при условии $\alpha_i < \alpha_{i+1}$ старше одночлена $\mathrm{Ст}(\tau(\vec{x}))$, что невозможно. □

Теорема 42. *Если* R *— кольцо с единицей, то для любого многочлена* $\tau(\vec{x}) \in \Sigma_R[x_1, \ldots, x_n]$ *существует такой многочлен* $a(\vec{x}) \in R[\vec{x}]$, *что*

$$\tau(\vec{x}) = \sum_{(i_1, \ldots, i_n)} a_{i_1, \ldots, i_n} \sigma_1(\vec{x})^{i_1} \ldots \sigma_n(\vec{x})^{i_n} = a(\sigma_1(\vec{x}), \ldots, \sigma_n(\vec{x})).$$

□ Если $\tau(\vec{x}) = 0$, то утверждение очевидно. Пусть $\tau(\vec{x}) \neq 0$. Обозначим через $\partial(\tau(\vec{x}))$ количество одночленов $ex_1^{i_1} \ldots x_n^{i_n} \in R[\vec{x}]$, которые младше, чем $\mathrm{Ст}(\tau(\vec{x}))$, и будем вести доказательство индукцией по $\partial(\tau(\vec{x}))$. Если $\partial(\tau(\vec{x})) = 0$, то $\tau(\vec{x}) = ux_1^0 \ldots x_n^0$ и утверждение очевидно ($a(\vec{x}) = \tau(\vec{x})$).

Предположим, что $m > 0$ и теорема верна при условии $\partial(\tau(\vec{x})) < m$. Докажем ее в случае, когда $\partial(\tau(\vec{x})) = m$. Пусть $\mathrm{Ст}(\tau(\vec{x})) = ux_1^{\alpha_1} \ldots x_n^{\alpha_n}$. Тогда по лемме 41 $\alpha_1 \geqslant \ldots \geqslant \alpha_n$. Рассмотрим многочлен

$$f_1(\vec{x}) = \sigma_1(\vec{x})^{\alpha_1 - \alpha_2} \cdot \sigma_2(\vec{x})^{\alpha_2 - \alpha_3} \cdot \ldots \cdot \sigma_1(\vec{x})^{\alpha_n} \in \Sigma_R[\vec{x}].$$

Применяя несколько раз теорему 40, получаем:

$$\begin{aligned} \mathrm{Ст}(f_1(\vec{x})) &= \mathrm{Ст}(\sigma_1(\vec{x}))^{\alpha_1 - \alpha_2} \cdot \mathrm{Ст}(\sigma_2(\vec{x}))^{\alpha_2 - \alpha_3} \cdot \ldots \cdot \mathrm{Ст}(\sigma_1(\vec{x}))^{\alpha_n} = \\ &= x_1^{\alpha_1 - \alpha_2} \cdot (x_1 x_2)^{\alpha_2 - \alpha_3} \cdot \ldots \cdot (x_1 \ldots x_{n-1})^{\alpha_{n-1} - \alpha_n} \cdot (x_1 \ldots x_n)^{\alpha_n} = \\ &= x_1^{\alpha_1} \ldots x_n^{\alpha_n}. \end{aligned}$$

Тогда для многочлена $\tau_1(\vec{x}) = \tau(\vec{x}) - uf_1(\vec{x})$ выполняется соотношение $\mathrm{Ст}(\tau_1(\vec{x})) \prec \mathrm{Ст}(\tau(\vec{x}))$, и потому $\partial(\tau(\vec{x})) < m$.

По предположению индукции существует многочлен $a_1(\vec{x}) \in R[x]$ такой, что $\tau_1(\vec{x}) = a_1(\sigma_1(\vec{x}), \ldots, \sigma_n(\vec{x}))$. Но тогда

$$\tau(\vec{x}) = uf_1(\vec{x}) + \tau_1(\vec{x}) = u\sigma_1(\vec{x})^{\alpha_1-\alpha_2} \ldots \sigma_n(\vec{x})^{\alpha_n} + a_1(\sigma_1(\vec{x}), \ldots, \sigma_n(\vec{x})). \quad \square$$

Заметим, что доказательство теоремы 42 дает практический способ выражения симметрического многочлена $\tau(\vec{x})$ через элементарные симметрические многочлены.

Следствие. *Пусть F — поле разложения унитарного многочлена*

$$f(x) = x^n + c_{n-1}x^{n-1} + \ldots + c_0 \in F[x]$$

и $\alpha_1, \ldots, \alpha_n$ — все корни $f(x)$ в F с учетом их кратностей. Тогда если P — подполе поля F, содержащее все коэффициенты многочлена $f(x)$, то для любого симметрического многочлена $\tau(\vec{x}) \in P[x_1, \ldots, x_n]$ элемент $\tau(\alpha_1, \ldots, \alpha_n)$ тоже принадлежит подполю P.

$\square$ По теореме 42 существует многочлен $a(x_1, \ldots, x_n)$, для которого $\tau(\vec{x}) = a(\sigma_1(\vec{x}), \ldots, \sigma_n(\vec{x}))$. Тогда ввиду утверждения 34 и теоремы 39 справедливы соотношения

$$\tau(\vec{\alpha}) = a(\sigma_1(\vec{\alpha}), \ldots, \sigma_n(\vec{\alpha})) = a(-c_{n-1},\, c_{n-2},\, \ldots,\, (-1)^n c_0) \in P. \quad \square$$

ЗАДАЧИ

1. Докажите, что если в кольце R нет делителей нуля, то мультипликативная группа $R[x]^*$ кольца $R[x]$ совпадает с R^*.

2. Докажите, что группа $\mathbb{Z}_4[x]^*$ состоит из всех многочленов с обратимыми свободными членами и четными коэффициентами при остальных степенях x.

3. Докажите, что множество делителей нуля кольца $\mathbb{Z}_4[x]$ состоит из всех многочленов с четными коэффициентами.

4. Опишите обратимые элементы и делители нуля в кольце многочленов $\mathbb{Z}_{p^n}[x]$ при простом $p \in \mathbb{N}$.

5. Может ли кольцо многочленов быть полем?

6. В условиях теоремы 3 приведите пример кольца R и многочленов $a(x)$, $b(x) \in R[x]$ таких, что при делении $a(x)$ на $b(x)$ с остатком справа и слева получаются разные остатки.

7. Докажите, что если в кольце R нет делителей нуля и многочлен $a(x) \in R[x]$ делится на не нулевой многочлен $b(x) \in R[x]$ с остатком справа, то частное и остаток определены однозначно. Приведите пример, когда такое деление невозможно.

8. Приведите пример, показывающий, что если R некоммутативное кольцо, то в теореме 5 условие $a(\alpha) = 0$ не равносильно условию: $a(x)$ делится на $x - \alpha$ слева.

9. Для любых $a(x), b(x) \in R[x]$ над коммутативным кольцом R положим $a(b(x)) = \sum_{i \geqslant 0} a_i b(x)^i$. Докажите равенство

$$a(b(x))' = a'(b(x)) \cdot b'(x).$$

10. Пусть $a_1(x), \ldots, a_n(x)$ — ненулевой набор многочленов над полем P. Докажите, что для унитарного многочлена $d(x) \in P[x]$ следующие утверждения эквивалентны:

а) $d(x) = (a_1(x), \ldots, a_n(x))$;

б) $d(x)$ — общий делитель многочленов $a_1(x), \ldots, a_n(x)$ наибольшей степени;

в) $d(x)$ — общий делитель многочленов $a_1(x), \ldots, a_n(x)$, имеющий вид $d(x) = u_1(x)a_1(x) + \ldots + u_n(x)a_n(x)$;

г) $d(x)$ — многочлен наименьшей степени среди ненулевых многочленов вида $c_1(x)a_1(x) + \ldots + c_n(x)a_n(x)$, $c_1(x), \ldots, c_n(x) \in P[x]$.

11. Пусть $a_0(x)$, $a_1(x)$ — ненулевые неассоциированные многочлены над полем P, $\deg a_0(x) > 0$, и $d(x) = (a_0(x), a_1(x))$. Докажите, что существуют единственные многочлены $u_0(x), u_1(x) \in P[x]$ такие, что

$$u_0(x)a_0(x) + u_1(x)a_1(x) = d(x)$$

и $\deg u_i(x) < \deg a_{1-i}(x) - \deg d(x)$, для $i \in \overline{0,1}$. (Рассмотрите сначала случай, когда $d(x) = e$ и поделите $u_i(x)$ с остатком на $a_{1-i}(x)$.)

12. Покажите, что если многочлены $a(x), b(x) \in P[x]$ взаимно просты, то для любого многочлена $c(x) \in P[x]$ многочлены $a(c(x))$ и $b(c(x))$ также взаимно просты.

13. Докажите, что если многочлен $f(x) \in P[x]$ взаимно прост со своей производной, то кратность каждого его неприводимого делителя в каноническом разложении над P равна единице.

14. Составьте таблицы неприводимых многочленов второй степени над полями $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$, третьей степени над полями $\mathbb{Z}_2$, $\mathbb{Z}_3$, четвертой и пятой степеней над полем $\mathbb{Z}_2$.

15. Пусть $f(x)$, $g(x)$ — многочлены над полем P, F — расширение поля P и $d_P(x)$, $d_F(x)$ — унитарные наибольшие общие делители многочленов $f(x)$ и $g(x)$ соответственно в $P[x]$ и $F[x]$. Докажите, что $d_P(x) = d_F(x)$.

16. Докажите, что если F — поле разложения многочлена $f(x) \in P[x]$ над полем P, то $f(x)$ не имеет кратных корней в F тогда и только тогда, когда $(f(x), f'(x)) = e$.

17. Пусть $a(x) \in \mathbb{Z}[x]$ — многочлен степени $n > 0$ и для каждого $k \in \overline{1, n-1}$ существует простое $p \in \mathbb{N}$ такое, что $p \nmid a_n$ и $r_p(a(x))$ не имеет в $\mathbb{Z}_p[x]$ делителей степени k. Докажите, что $a(x)$ неприводим над $\mathbb{Q}$.

18. Докажите, что если $a(x) \in P[x]$ — приводимый многочлен и $b(x) \in P[x] \setminus P$, то многочлен $a(b(x))$ приводим, а если $\deg b(x) = 1$, то верно и обратное утверждение.

19. Докажите, что для любого простого $p \in \mathbb{N}$ многочлен $x^{p-1} + \ldots + x + 1$ над полем $\mathbb{Q}$ неприводим (сделайте замену $x = y+1$ и используйте признак Эйзенштейна).

20. Докажите, что для любого простого $p \in \mathbb{N}$ и любого натурального k многочлен $x^{p^{k-1}(p-1)} + x^{p^{k-1}(p-2)} + \ldots + x^{p^{k-1}} + 1 \in \mathbb{Q}[x]$ неприводим, а его корнями в поле $\mathbb{C}$ являются в точности все примитивные корни степени p^k из единицы.

21. Пусть P — поле из q элементов. Докажите, что многочлен x^{q-1} задает на P функцию, равную e во всех ненулевых точках. (*Указание*: пусть $P^* = \{\alpha_1, \ldots, \alpha_{q-1}\}$ и $\alpha \in P^*$. Сравните произведения $\alpha_1 \ldots \alpha_{q-1}$ и $(\alpha\alpha_1)\ldots(\alpha\alpha_{q-1})$.)

22. В условиях предыдущей задачи докажите, что любая функция $\varphi\colon P^n \to P$ представляется многочленом

$$a(x_1, \ldots, x_n) = \sum_{(c_1,\ldots,c_n)\in P^n} \varphi(c_1, \ldots, c_n) \cdot (e - (x_1 - c_1)^{q-1}) \cdot \ldots \cdot (e - (x_n - c_n)^{q-1}).$$

23. Докажите, что если P — поле порядка q, то все его элементы — корни многочлена $x^q - x \in P[x]$.

24. Докажите, что если P — поле из q элементов и многочлен $f(x) = f_0 + f_1 x + \ldots + f_{q-1}x^{q-1} \in P[x]$ задает на P подстановку, то $f_{q-1} = 0$. (Покажите, что для любого $k \in \overline{1, q-2}$ верно равенство $\sum_{\alpha\in P} \alpha^k = 0$, и просуммируйте все значения подстановки $f(x)$.)

25. Опишите все многочлены, задающие подстановки на поле $\mathbb{Z}_3$.

26. Найдите многочлен степени большей, чем 1, задающий подстановку на поле $\mathbb{Z}_5$.

27. Выразите через элементарные симметрические многочлены следующие симметрические многочлены из $P[x_1, x_2, x_3]$:

а) $x_1^2 + x_1^2 + x_3^2$;

б) $x_1^3 + x_1^3 + x_3^3$;

в) $x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_2^2x_3 + x_1x_3^2 + x_2x_3^2$;

г) $x_1^4 + x_2^4 + x_3^4$.

28. Пусть $f(x) \in P[x]$, F — поле разложения многочлена $f(x)$ над полем P и $\alpha_1, \ldots, \alpha_n \in F$ — все корни $f(x)$ с учетом их кратностей. *Дискриминантом* многочлена $f(x)$ называют следующий элемент поля F:

$$\Delta(f) = \prod_{1\leqslant i<j\leqslant n} (\alpha_i - \alpha_j)^2.$$

Докажите, что $\Delta(f) \in P$ и $\Delta(f)$ не зависит от выбора поля F.

29. Найдите дискриминанты многочленов $x^2 + bx + c$ и $x^3 + bx + c$ над данным полем P.

Глава 10

ГРУППОИДЫ И ПОЛУГРУППЫ

Основными понятиями, связанными с изучением алгебр, являются понятия подалгебры, гомоморфизма алгебр, конгруэнции на алгебре, факторалгебры, системы образующих алгебры. Все эти понятия можно определить для произвольной универсальной алгебры, т. е. для множества с любым набором операций. Однако ради простоты изложения и восприятия, мы в данной главе введем указанные понятия для алгебр с одной бинарной операцией, т. е. для группоидов. При этом в общих рассуждениях будет использоваться в основном мультипликативная терминология.

Заметим, что в неассоциативных группоидах при записи произведения более двух элементов необходимо расставлять все скобки, определяющие порядок выполнения операций. Это обстоятельство в некоторых случаях значительно усложняет изложение. В связи с этим, мы будем особое внимание уделять ассоциативным группоидам, т. е. полугруппам (в которых произведение любого набора элементов можно записывать без скобок).

§ 1. ПОДГРУППОИДЫ И ПОДПОЛУГРУППЫ

Напомним (см. определение 5 главы 3), что подгруппоидом группоида $G = (G; \cdot)$ называется любое его непустое подмножество G_1, замкнутое относительно операции $\cdot$ и рассматриваемое как множество с этой операцией.

В частности, подгруппоидом любого группоида является сам этот группоид. Если группоид содержит нейтральный элемент, то последний один образует подгруппоид. Приведем и менее тривиальные примеры подгруппоидов.

Пример 1. Подгруппоидами группоида $(\mathbb{N}_0; \cdot)$ будут его подмножества

$$p^{t\mathbb{N}} = \{p^{tn} : n \in \mathbb{N}\}, \quad p^{t\mathbb{N}_0} = \{p^{tn} : n \in \mathbb{N}_0\},$$

где p — простое число, $t \in \mathbb{N}$.

Если G_1 — подгруппоид в G и G — полугруппа, то G_1 — также полугруппа. Ее называют подполугруппой полугруппы G. Заметим, что подгруппоид G_1 группоида G может быть ассоциативным и в том случае, когда G неассоциативен. В связи с этим имеет смысл

Определение 1. Подгруппоид G_1 группоида G, являющийся полугруппой, называется *подполугруппой группоида* G.

Утверждение 1. *Если* $\{G_i : i \in I\}$ *— семейство подгруппоидов группоида* G *и* $H = \bigcap\limits_{i\in I} G_i$*, то либо* $H = \varnothing$*, либо* H *— подгруппоид группоида* G*.*

□ Достаточно доказать, что если $H \neq \varnothing$, то H замкнуто относительно операции $\cdot$ в G. Пусть $h_1, h_2 \in H$, т. е. $h_1, h_2 \in G_i$ для всех $i \in I$. Так как G_i — подгруппоиды в G, то $h_1h_2 \in G_i$ при всех $i \in I$, и потому $h_1h_2 \in H$. Следовательно, H — подгруппоид группоида G. □

Заметим, что каждый из вариантов ($H = \varnothing$ и H — подгруппоид) для множества H из утверждения 1 возможен.

Пример 2. Для подгруппоидов полугруппы $(\mathbb{N}_0; \cdot)$ примера 1 имеем:
$p^{2\mathbb{N}} \cap p^{3\mathbb{N}} = p^{6\mathbb{N}}$ — подгруппоид,
$p^{\mathbb{N}} \cap q^{\mathbb{N}} = \varnothing$ при различных простых p и q.

Используя операцию пересечения подгруппоидов, укажем один из широко используемых в алгебре способов задания группоидов и, в частности, полугрупп.

Пусть G — группоид и $\varnothing \neq M \subset G$. Если подмножество M не является группоидом, то естественно поставить задачу о наиболее экономном пополнении M элементами из G до группоида. Для этого необходимо добавить к M все элементы из G вида ab, если $a, b \in M$ и $ab \notin M$. Затем то же самое проделать с полученным множеством и т. д. до тех пор, пока не получится замкнутое, относительно операции $\cdot$ множество. Оно и будет искомым подгруппоидом. Формально и более строго этот группоид определяется следующим образом.

Определение 2. *Подгруппоидом* группоида G, *порожденным* непустым *подмножеством* $M \subset G$, называется подгруппоид $[M\rangle$, являющийся пересечением всех подгруппоидов из G, содержащих M. При этом множество M называется *системой образующих* группоида $[M\rangle$ (и самого группоида G в случае $[M\rangle = G$).

Если обозначить через $\{G_i : i \in I\}$ семейство всех группоидов из G, содержащих множество M, то можно будет записать

$$[M\rangle = \bigcap_{i\in I} G_i. \tag{1}$$

Из утверждения 1 следует, что определение 2 корректно. Следующее утверждение дает описание элементов из $[M\rangle$.

Утверждение 2. *Подгруппоид* $[M\rangle$ *группоида* G *совпадает с множеством* H *всех элементов группоида* G*, которые или содержатся в* M *или представляются в виде произведений элементов из* M*.*

□ Из определения множества H видно, что H — подгруппоид из G, содержащий множество M. Тогда из (1) получаем: $[M\rangle \subset H$. С другой стороны, каждый подгруппоид G_i из (1) содержит M и, будучи замкнутым относительно умножения, содержит H. Следовательно, $H \subset [M\rangle$. В итоге имеем: $H = [M\rangle$. □

В случае когда группоид G является полугруппой, произведения элементов записываются сравнительно просто, и мы из утверждения 1 получаем

Следствие. *Если $(G;\cdot)$ — полугруппа и $\varnothing \neq M \subset G$, то ее подполугруппа, порожденная множеством M, состоит из всех элементов, представимых в виде*

$$m_1 \cdot \ldots \cdot m_k,$$

где $k \in \mathbb{N}$, а $m_1, \ldots, m_k$ — произвольные, не обязательно различные, элементы из M.

Пример 3. Пользуясь следствием, нетрудно проверить, что в полугруппе $(\mathbb{N}_0;\cdot)$ из примера 1 ее подполугруппы $p^{t\mathbb{N}}$, $p^{t\mathbb{N}_0}$ порождаются соответственно множествами $\{p^t\}$, $\{1, p^t\}$. Сама полугруппа $(\mathbb{N}_0;\cdot)$ в силу основной теоремы арифметики (см. теорему 14 главы 4) порождается множеством $\Pi \cup \{1\}$, где Π — множество всех простых чисел.

Определение 3. Группоид G называется *конечно порожденным*, если он имеет конечную систему образующих, и *циклическим*, если порождается некоторым одним элементом.

Пример 4. Из примера 3 видно, что полугруппы $p^{t\mathbb{N}}$, $p^{t\mathbb{N}_0}$ конечно порождены. Полугруппа же $(\mathbb{N}_0;\cdot)$ не является конечно порожденной. Докажите это в качестве упражнения, пользуясь теоремой Евклида о бесконечности множества простых чисел (см. теорему 15 главы 4).

Для систем образующих конечно порожденных группоидов справедливо

Утверждение 3. *Если группоид G конечно порожден, то в любой его бесконечной системе образующих содержится некоторая его конечная система образующих.*

□ По условию $G = [R\rangle$ для некоторого конечного множества R. Пусть также $G = [M\rangle$, где $|M| = \infty$. Из утверждения 2 следует, что каждый элемент из R или принадлежит M или представляется в виде произведения конечного числа элементов из M. Зафиксируем по одному такому представлению для каждого элемента $R \setminus M$ и обозначим через M_1 объединение множества всех входящих в эти представления элементов и множества $R \cap M$. Так как $|R| < \infty$, то $|M_1| < \infty$. По определению 2 $[M_1\rangle \subset G$. С другой стороны, $R \subset [M_1\rangle$, и потому $[R\rangle \subset [M_1\rangle$, т. е. $G \subset [M_1\rangle$. Следовательно, $G = [M_1\rangle$. □

§ 2. ГОМОМОРФИЗМЫ ГРУППОИДОВ

В § 4 главы 3 было определено понятие изоморфизма группоида $(G;\cdot)$ на группоид $(H;\circ)$ как биективного отображения $\varphi\colon G \to H$, удовлетворяющего условию

$$\forall\, a, b \in G:\ \ \varphi(ab) = \varphi(a) \circ \varphi(b). \tag{2}$$

Естественным обобщением понятия изоморфизма является понятие гомоморфизма группоидов.

Определение 4. *Гомоморфизмом* группоида $(G;\cdot)$ в группоид $(H;\circ)$ называется любое отображение $\varphi\colon G \to H$, удовлетворяющее условию (2). При этом множество $\varphi(G) \subset H$ называется *гомоморфным образом* группоида G.

В том случае, когда отображение φ сюръективно или инъективно, гомоморфизм φ называют соответственно *эпиморфизмом* или *мономорфизмом* (мономорфизм G в H называют также *изоморфным вложением* G в H).

Если φ — гомоморфизм группоидов с одинаково обозначенной операцией, то говорят также, что φ — гомоморфизм относительно этой операции.

При гомоморфизме группоида (в отличие от изоморфизма) сохраняются не все свойства операций, однако некоторые из них сохраняются. Об этом свидетельствует

Теорема 4. *Пусть φ — гомоморфизм группоида $(G;\cdot)$ в группоид $(H;\circ)$. Тогда множество $\varphi(G)$ замкнуто относительно операции $\circ$ в H, т. е. является группоидом. Если при этом группоид G является полугруппой, коммутативной полугруппой, полугруппой с единицей, группой, то соответственно таким же является и его гомоморфный образ $(\varphi(G);\circ)$. Кроме того, при гомоморфизме φ единица группоида G (если существует) переходит в единицу группоида $\varphi(G)$ и обратный элемент для a (если он существует) переходит в обратный элемент для $\varphi(a)$, т. е. $\varphi(a^{-1}) = \varphi(a)^{-1}$.*

□ Из определения образа $\varphi(G)$ множества G имеем:

$$\forall\, b_1, b_2 \in \varphi(G),\ \exists\, a_1, a_2 \in G\colon\ \varphi(a_1) = b_1,\ \varphi(a_2) = b_2.$$

Отсюда и из условия (2) для φ получаем:

$$\varphi(a_1 a_2) = \varphi(a_1) \circ \varphi(a_2) = b_1 \circ b_2.$$

Следовательно, $b_1 \circ b_2 \in \varphi(G)$, т. е. $\varphi(G)$ замкнуто относительно операции $\circ$. Остальные утверждения теоремы 4 доказываются точно так же, как соответствующие утверждения теоремы 13 главы 3 об изоморфизме φ, поскольку при доказательстве последних условие инъективности отображения φ не использовалось. □

Приведем ряд примеров гомоморфизмов полугрупп.

Пример 5. Рассмотрим отображение $\varphi\colon \mathbb{Z} \to \mathbb{Z}/m$, при котором $\forall\, r \in \mathbb{Z}\colon\ \varphi(r) = [r]_m$. Из определения операций в $\mathbb{Z}/m$:

$$[r_1]_m + [r_2]_m = [r_1 + r_2]_m, \quad [r_1]_m \cdot [r_2]_m = [r_1 r_2]_m$$

видно, что φ есть гомоморфизм полугрупп $(\mathbb{Z};+)$ и $(\mathbb{Z};\cdot)$ на полугруппы соответственно $(\mathbb{Z}/m;+)$, $(\mathbb{Z}/m;\cdot)$. Действительно, если $*$ — любая из операций $+$, $\cdot$, то

$$\varphi(r_1 * r_2) = [r_1 * r_2]_m = [r_1]_m * [r_2]_m = \varphi(r_1) * \varphi(r_2).$$

Очевидно, что этот гомоморфизм является эпиморфизмом.

Пример 6. Пусть P — поле. Отображение $\varphi_r\colon P[x] \to P$, определенное при любом фиксированном $r \in P$ формулой

$$\forall\, a(x) \in P[x]:\ \varphi_r(a(x)) = a(r),$$

является гомоморфизмом относительно операций $+$ и $\cdot$. Это следует из леммы 4 главы 9. Так как

$$a(r) = b(r) \ \Leftrightarrow\ c(r) = 0 \text{ для } c(x) = a(x) - b(x),$$

то φ_r — не мономорфизм.

Пример 7. Известное свойство определителей квадратных матриц над коммутативным кольцом R: $|AB| = |A|\cdot|B|$ свидетельствует о том, что отображение $\varphi\colon R_{n,n} \to R$, при котором $\varphi(A) = |A|$, есть гомоморфизм полугруппы $(R_{n,n};\cdot)$ в полугруппу $(R;\cdot)$. Здесь в случае $n > 1$ видно, что при гомоморфизме φ некоммутативная полугруппа может переходить в коммутативную.

Обратим особое внимание на примеры 5–6, в которых рассматриваемые отображения являются гомоморфизмами относительно двух операций. В такой ситуации представляется интересным вопрос о сохранении при гомоморфизме φ тех свойств, которые связывают разные операции, например, свойства дистрибутивности одной операции, относительно другой. На этот вопрос отвечает

Утверждение 5. *Пусть $(G;*,\circ)$, $(H;*,\circ)$ — алгебры с двумя бинарными операциями и отображение $\varphi\colon G \to H$ является эпиморфизмом относительно каждой из операций $*,\circ$. Тогда из правой (левой) дистрибутивности операции $*$ относительно $\circ$ в алгебре G следует выполнение соответствующего свойства в алгебре H.*

□ Доказывается этот факт точно так же, как и в теореме 16 главы 3 для изоморфизма φ. □

Из теоремы 4 и утверждения 5 получаем

Следствие. *Пусть $(G;+,\cdot)$, $(H;+,\cdot)$ — алгебры с двумя бинарными операциями и отображение $\varphi\colon G \to H$ есть эпиморфизм относительно каждой из указанных операций. Тогда, если $(G;+,\cdot)$ — кольцо, коммутативное кольцо, кольцо с единицей или поле, то соответственно то же самое верно и для алгебры $(H;+,\cdot)$.*

§ 3. КОНГРУЭНЦИИ НА ГРУППОИДАХ И ФАКТОРГРУППОИДЫ

Из результатов предыдущего параграфа видно, что сохранение определенных свойств операций при гомоморфизме алгебр позволяет использовать гомоморфизмы для сведения изучения одних алгебр к изучению других алгебр. Кроме того, гомоморфизмы используются и для построения алгебр. Так, например, имея некоторую полугруппу, мы можем строить новые полугруппы — гомоморфные образы исходной. Все это делает актуальной задачу описания всех гомоморфных образов заданной

алгебры, в частности, полугруппы. Для решения этой задачи в классе группоидов введем понятие конгруэнции на группоиде.

В § 1 главы 2 было показано, что любое отношение эквивалентности ρ на произвольном множестве G индуцирует разбиение множества G на непересекающиеся классы эквивалентности, т. е. на классы вида

$$[a]_\rho = \{x \in G : \ x \,\rho\, a\}.$$

Множество всех этих классов называют *факторомножеством* множества G по отношению ρ и обозначают через G/ρ. Переход от множества G к множеству G/ρ называют факторизацией множества G. В данном параграфе нас будет интересовать случай, когда факторизуемое множество является группоидом. В этом случае по операции на G можно попытаться определить операцию на факторомножестве G/ρ. Самый естественный путь определения операции над классами заключается в сведении ее к имеющейся операции над представителями классов. Именно так ранее мы определяли операции над классами $\mathbb{Z}/m$. Если следовать этой идее, то надо положить по определению

$$\forall\, [a]_\rho, [b]_\rho \in G/\rho : \ \ [a]_\rho \cdot [b]_\rho = [a \cdot b]_\rho. \tag{3}$$

Однако, такое определение будет некорректно, если результат операции над классами $[a]_\rho$, $[b]_\rho$ окажется зависящим от выбора представителей a, b. Легко видеть, что определение корректно в том и только в том случае, когда отношение ρ удовлетворяет условию

$$\forall\, a, b, a_1, b_1 \in G : \ \ ((a \,\rho\, a_1) \,\&\, (b \,\rho\, b_1) \ \Rightarrow \ (ab) \,\rho\, (a_1 b_1)). \tag{4}$$

Определение 5. Отношение эквивалентности ρ на группоиде $(G;\cdot)$, удовлетворяющее условию (4), называется *согласованным с операцией* в G, или *конгруэнцией* на группоиде G.

Если ρ — конгруэнция на группоиде G, то определение операции на классах эквивалентности с помощью формулы (3) корректно, и потому корректно

Определение 6. Факторомножество G/ρ группоида G по конгруэнции ρ с операцией, определенной формулой (3), называется *факторгруппоидом группоида* G по конгруэнции ρ. При этом об операции на G/ρ говорят, что она индуцирована операцией на G.

Утверждение 6. *Если ρ — конгруэнция на группоиде $(G;\cdot)$, то отображение $\varphi_\rho : G \to G/\rho$, при котором*

$$\forall\, a \in G : \ \ \varphi_\rho(a) = [a]_\rho,$$

является эпиморфизмом $(G;\cdot)$ на $(G/\rho;\cdot)$.

□ Отображение φ_ρ сюръективно, поскольку в класс $[a]_\rho$ отображается элемент $a \in G$ (и все остальные элементы класса $[a]_\rho$). Кроме того, из определений отображения φ_ρ и операции на G/ρ имеем:

$$\forall\, a, b \in G : \ \ \varphi_\rho(ab) = [ab]_\rho = [a]_\rho \cdot [b]_\rho = \varphi(a) \cdot \varphi(b).$$

Следовательно, φ_ρ — эпиморфизм. □

Отображение φ_ρ, определенное в утверждении 6, обычно называют *естественным*, или *каноническим гомоморфизмом* группоида $(G;\cdot)$ на факторгруппоид $(G/\rho;\cdot)$.

Из утверждения 6 и теоремы 4 получаем

Следствие. *Если G — полугруппа, коммутативная полугруппа, полугруппа с единицей, группа, а ρ — конгруэнция на G, то факторполугруппа G/ρ является соответственно полугруппой, коммутативной полугруппой, полугруппой с единицей, группой.*

Таким образом, по конгруэнции ρ на группоиде G можно построить новый группоид G/ρ, который наследует многие свойства группоида G.

Заметим, что на каждом группоиде G имеются две тривиальные конгруэнции, а именно, отношение равенства ρ_1:

$$\forall\, a, b \in G:\ \ (a\,\rho_1\, b\ \Leftrightarrow\ a = b)$$

и так называемое универсальное бинарное отношение ρ_0:

$$\forall\, a, b \in G:\ \ (a\,\rho_0\, b).$$

Очевидно, что при любом $a \in G$ класс $[a]_{\rho_1}$ содержит единственный элемент a, а класс $[a]_{\rho_0}$ — все элементы из G. Отсюда и из утверждения 6 следует, что группоид G/ρ_1 изоморфен G, а группоид G/ρ_0 одноэлементный.

Приведем примеры нетривиальных конгруэнций на полугруппах.

Пример 8. Отношение сравнимости целых чисел по модулю m является конгруэнцией на каждой из полугрупп $(\mathbb{Z};+)$, $(\mathbb{Z};\cdot)$. Свойство (4) для этих конгруэнций (означающее, что сравнения можно почленно складывать и перемножать) доказано ранее, см. теорему 2 главы 5. Соответствующими факторполугруппами являются $(\mathbb{Z}/m;+)$ и $(\mathbb{Z}/m;\cdot)$.

Пример 9. Рассмотрим отношения σ_1 на множестве комплексных чисел $\mathbb{C}$ и σ_2 на множестве $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$, определенные формулами

$$\forall\, a, b \in \mathbb{C}:\ \ (a\,\sigma_1\, b\ \Leftrightarrow\ |a| = |b|),$$

$$\forall\, a, b \in \mathbb{C}^*:\ \ (a\,\sigma_2\, b\ \Leftrightarrow\ \arg a = \arg b).$$

Из свойств умножения комплексных чисел в тригонометрической форме легко следует, что σ_1, σ_2 — конгруэнции соответственно на полугруппах $(\mathbb{C};\cdot)$ и $(\mathbb{C}^*;\cdot)$ (проверьте). Геометрически, при изображении комплексных чисел точками плоскости с прямоугольной системой координат, элементы факторполугрупп $(\mathbb{C}/\sigma_1;\cdot)$ и $(\mathbb{C}^*/\sigma_2;\cdot)$ изображаются соответственно концентрическими кругами с центром в начале координат O и лучами, выходящими из точки O (без самой точки O).

По утверждению 6 факторполугруппа G/ρ полугруппы G по конгруэнции ρ является гомоморфным образом полугруппы G. Естественно, возникает вопрос: не исчерпываются ли все гомоморфные образы любого группоида его факторгруппоидами по конгруэнциям? Положительный ответ на этот вопрос дает

Теорема 7 (об эпиморфизме группоидов). *Пусть φ — эпиморфизм группоида $(G;\cdot)$ на группоид $(H;\cdot)$. Тогда*

(а) *отношение ρ на G, определенное формулой*

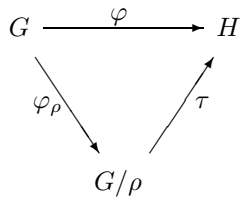
$$\forall\, a, b \in G\colon\ (a\,\rho\, b\ \Leftrightarrow\ \varphi(a) = \varphi(b)), \tag{5}$$

является конгруэнцией на группоиде G;

(б) *группоиды H и G/ρ изоморфны, причем существует единственный изоморфизм $\tau\colon G/\rho \to H$, удовлетворяющий условию*

$$\varphi = \varphi_\rho \cdot \tau. \tag{6}$$

Замечание. Для наглядности гомоморфизмы φ, φ_ρ, τ представляют диаграммой



(7)

и вместо слов «выполняется равенство (6)» говорят: «Диаграмма (7) коммутативна».

□ (а) Из (5) следует, что отношение ρ рефлексивно, симметрично и транзитивно, т. е. является отношением эквивалентности на G. Проверим для ρ свойство (4). Используя определение ρ и тот факт, что φ — гомоморфизм, получим (для любых $a, b, a_1, b_1 \in G$):

$$a\,\rho\, a_1,\ b\,\rho\, b_1\ \Rightarrow\ (\varphi(a) = \varphi(a_1),\ \varphi(b) = \varphi(b_1))\ \Rightarrow$$
$$\Rightarrow\ (\varphi(a)\varphi(b) = \varphi(a_1)\varphi(b_1))\ \Rightarrow\ (\varphi(ab) = \varphi(a_1 b_1))\ \Rightarrow\ (ab)\,\rho\,(a_1 b_1).$$

Следовательно, ρ — конгруэнция.

(б) Определим отображение $\tau\colon G/\rho \to H$, положив

$$\forall\, [a]_\rho \in G/\rho\colon\ \tau([a]_\rho) = \varphi(a).$$

Это определение корректно, т. е. образ класса $[a]_\rho$ не зависит от выбора представителя a, поскольку для любого $a_1 \in G$ имеем:

$$[a_1]_\rho = [a]_\rho\ \Leftrightarrow\ a_1\,\rho\, a\ \Leftrightarrow\ \varphi(a_1) = \varphi(a)\ \Leftrightarrow\ \tau([a_1]_\rho) = \tau([a]_\rho).$$

Отсюда следует также, что отображение τ инъективно. Сюръективность τ следует из сюръективности отображения φ. Следовательно, τ — биекция. Наконец, τ — гомоморфизм, поскольку для любых элементов $[a]_\rho, [b]_\rho \in G/\rho$ верны равенства

$$\tau([a]_\rho \cdot [b]_\rho) = \tau([ab]_\rho) = \varphi(ab) = \varphi(a)\cdot\varphi(b) = \tau([a]_\rho)\cdot\tau([b]_\rho).$$

Итак, τ — гомоморфизм. Проверим условие (6). По определению естественного гомоморфизма φ_ρ и изоморфизма τ для любого $a \in G$ имеем:

$$(\varphi_\rho\tau)(a) = \tau(\varphi_\rho(a)) = \tau([a]_\rho) = \varphi(a), \quad \text{т. е.} \quad \varphi_\rho\tau = \varphi.$$

Докажем единственность τ. Пусть наряду с τ существует изоморфизм $\tau_1 \colon G/\rho \to H$, удовлетворяющий условию $\varphi_\rho\tau_1 = \varphi$. Тогда для любого элемента $[a]_\rho \in G/\rho$ имеем:

$$\tau([a]_\rho) = \varphi(a) = (\varphi_\rho\tau_1)(a) = \tau_1(\varphi_\rho(a)) = \tau_1([a]_\rho).$$

Следовательно, $\tau_1 = \tau$. $\square$

Замечание. Заменив в доказательстве теоремы 7 всюду слово группоид словом полугруппа, мы получим утверждение, называемое *теоремой об эпиморфизме полугрупп*. Ее доказательство полностью совпадает с доказательством теоремы 7, т. е. она является частным случаем теоремы 7.

Теорема 7 и утверждение 6 сводят задачу описания всех гомоморфных образов группоида G к нахождению всех конгруэнций на G. Последняя задача, будучи в общем случае сложной, имеет принципиальное преимущество перед первой, поскольку для ее решения нужно использовать лишь сам группоид G, а не искать его гомоморфные образы в классе всех группоидов.

Пример 10. Найти все конгруэнции на полугруппе $(\mathbb{N}_0; +)$.

Пусть ρ — любая нетривиальная конгруэнция на полугруппе $(\mathbb{N}_0; +)$. Опишем классы $[a]_\rho$. Пусть k — наименьшее число из $\mathbb{N}_0$, удовлетворяющее условию $|[k]_\rho| > 1$, d — минимальная положительная разность чисел из $[k]_\rho$ и a, $a + d \in [k]_\rho$. Тогда из соотношений $a\,\rho\,(a + d)$, $k\,\rho\,a$, используя свойства конгруэнции, легко получить последовательно соотношения

$$a\,\rho\,(a + dt), \quad (k + dt)\,\rho\,(a + dt), \quad k\,\rho\,(k + dt)$$

для любого $t \in \mathbb{N}_0$. Отсюда, с учетом условий выбора чисел k, d, получаем равенство: $[k]_\rho = \{k+dt : \ t \in \mathbb{N}_0\}$, т. е. $[k]_\rho$ — класс неотрицательных вычетов по модулю d, больших или равных k. В связи с этим, обозначим класс $[k]_\rho$ через $[k]'_d$. Теперь, используя импликацию $a\,\rho\,b \ \Rightarrow \ (a+1)\,\rho\,(b+1)$, найдем и остальные неодноэлементные классы: $[k+1]'_d, \ \ldots, \ [k+d-1]'_d$. Таким образом, классы эквивалентности по конгруэнции ρ исчерпываются классами

$$\{0\}, \ \{1\}, \ \ldots, \ \{k-1\}, \ [k]'_d, \ \ldots, \ [k+d-1]'_d$$

и полностью определяются парой чисел k, d, где $k \in \mathbb{N}_0$, $d \in \mathbb{N}$. Перебирая все такие пары (k, d), мы получим все конгруэнции полугруппы $(\mathbb{N}_0; +)$, а в силу теоремы 7 и все ее гомоморфные образы.

Отметим еще, что теорема об эпиморфизме группоидов может быть использована для установления изоморфизма различных группоидов и для построения изоморфных образов группоидов.

Пример 11. По теореме 36 главы 9 множество $\mathbb{Q}[\pi]$ значений всех многочленов из $\mathbb{Q}[x]$ при $x = \pi = 3,14\ldots$ является кольцом относительно операций сложения и умножения в $\mathbb{R}$. Следовательно, имеет смысл говорить о полугруппах $(\mathbb{Q}[\pi];+)$ и $(\mathbb{Q}[\pi];\cdot)$. Попытаемся заменить их изоморфными и более знакомыми полугруппами.

С этой целью рассмотрим отображение $\varphi_\pi\colon \mathbb{Q}[x] \to \mathbb{Q}[\pi]$, определенное формулой

$$\forall\, a(x) \in \mathbb{Q}[x]:\ \ \varphi_\pi(a(x)) = a(\pi).$$

Отображение φ_π сюръективно и, как следует из леммы 4 главы 9, является гомоморфизмом относительно операций сложения и умножения. Значит, по теореме 7 существуют такие конгруэнции ρ_1, ρ_2 соответственно на полугруппах $(\mathbb{Q}[x];+)$ и $(\mathbb{Q}[x];\cdot)$, что

$$(\mathbb{Q}[x];+)/\rho_1 \cong (\mathbb{Q}[\pi];+), \quad (\mathbb{Q}[x];\cdot)/\rho_2 \cong (\mathbb{Q}[\pi];\cdot).$$

Из формулировки теоремы 7 видно, что конгруэнции ρ_1, ρ_2 не зависят от операций, а однозначно определяются отображением φ_π. Следовательно, $\rho_1 = \rho_2 = \rho$, где ρ определено условием

$$\forall\, a(x), b(x) \in \mathbb{Q}[x]:\ \ a(x)\,\rho\, b(x) \ \Leftrightarrow\ a(\pi) = b(\pi).$$

Заметим, что

$$a(\pi) = b(\pi) \ \Leftrightarrow\ a(\pi) - b(\pi) = 0 \ \Leftrightarrow\ c(\pi) = 0,$$

где $c(x) = a(x) - b(x)$. Теперь воспользуемся известным в математике фактом о трансцендентности числа π, т. е. об отсутствии ненулевого многочлена из $\mathbb{Q}[x]$ с корнем π. В итоге получим:

$$\forall\, a(x), b(x) \in \mathbb{Q}[x]:\ \ a(x)\,\rho\, b(x) \ \Leftrightarrow\ a(x) = b(x),$$

т. е. ρ — отношение равенства. Отсюда и из теоремы 7 легко следует, что отображение φ_π является изоморфизмом относительно обеих операций $+$, $\cdot$. Следовательно, φ_π есть изоморфизм кольца $(\mathbb{Q}[x];+,\cdot)$ на кольцо $(\mathbb{Q}[\pi];+,\cdot)$.

§ 4. ПОЛУГРУППЫ ПРЕОБРАЗОВАНИЙ

Определение 7. *Полугруппой преобразований* множества Ω называется любая подполугруппа полугруппы $\Pi(\Omega)$ всех преобразований множества Ω относительно операции умножения преобразований.

Особая роль полугрупп преобразований в теории полугрупп связана с наличием следующего утверждения.

Теорема 8. *Любая полугруппа $(G;\cdot)$ изоморфна некоторой полугруппе преобразований подходящего множества Ω.*

□ Доказательство разбивается на два случая.

1. Полугруппа G имеет единицу e. Тогда возьмем в качестве Ω саму полугруппу G и определим отображение $\varphi\colon G \to \Pi(G)$, положив для $g \in G$: $\varphi(g) = \widehat{g}$, где $\widehat{g}$ — преобразование множества G, определяемое формулой

$$\forall\, x \in G:\ \ \widehat{g}(x) = x \cdot g. \tag{8}$$

Отображение φ инъективно, поскольку для любых $g_1, g_2 \in G$

$$g_1 \neq g_2 \;\Rightarrow\; e \cdot g_1 \neq e \cdot g_2 \;\Rightarrow\; \widehat{g}_1(e) \neq \widehat{g}_2(e) \;\Rightarrow\; \widehat{g}_1 \neq \widehat{g}_2.$$

Докажем, что

$$\forall\, g_1, g_2 \in G\colon\ \varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2), \quad \text{т. е.} \quad \forall\, g_1, g_2 \in G\colon\ \widehat{g_1 g_2} = \widehat{g}_1 \cdot \widehat{g}_2.$$

Последнее утверждение доказывается следующей цепочкой очевидных равенств:

$$\widehat{g_1 g_2}(x) = x \cdot (g_1 g_2) = (x g_1) g_2 = \widehat{g}_1(x) \cdot g_2 = \widehat{g}_2(\widehat{g}_1(x)) = \widehat{g}_1 \widehat{g}_2(x).$$

Получим, что φ — мономорфизм, и потому полугруппа G изоморфна подполугруппе $\varphi(G) < \Pi(G)$.

2. G — полугруппа без единицы. Тогда добавим к G новый элемент e и доопределим операцию умножения на множестве $G_1 = G \cup \{e\}$, положив

$$\forall\, g \in G\colon\ eg = ge = g \quad \text{и} \quad e \cdot e = e.$$

В итоге получим полугруппу G_1 с единицей e. Взяв ее в качестве множества Ω, мы точно так же, как и в случае 1, построим мономорфизм $\varphi_1\colon G \to \Pi(G_1)$. $\square$

В приложениях особый интерес представляют полугруппы преобразований конечных множеств. Поэтому далее мы ограничимся этим случаем. Заметим еще, что если множества Ω_1, Ω_2 равномощны, то полугруппы $\Pi(\Omega_1)$, $\Pi(\Omega_2)$ изоморфны. (Доказательство этого факта сходно с доказательством утверждения 15 главы 3, проведите его в качестве упражнения.) В связи с этим можно ограничиться изучением лишь полугруппы $\Pi(\Omega)$ при $\Omega = \overline{1,n}$.

Определение 8. Полугруппа всех преобразований множества $\overline{1,n}$ называется *симметрической полугруппой* преобразований степени n. Обозначим ее через Π_n.

Заметим, что порядок полугруппы Π_n равен n^n, она некоммутативна при всех $n > 1$ (см. теорему 5 главы 3) и содержит в качестве подполугруппы симметрическую группу подстановок S_n. Любое преобразование $g \in \Pi_n$, как и подстановку из S_n, можно записать таблицей:

$$g = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix},$$

где $i_s = g(s)$ для $s \in \overline{1,n}$. Однако здесь, в отличие от подстановок, в нижней строке таблицы некоторые элементы из $\overline{1,n}$ могут повторяться несколько раз, а некоторых может и не быть совсем. В связи с этим для преобразований из Π_n можно ввести следующие параметры.

Определение 9. Для преобразования $g \in \Pi_n$ параметры $|g(\overline{1,n})|$ и $n - |g(\overline{1,n})|$ называются соответственно *рангом* и *дефектом* преобразования g и обозначаются через $\operatorname{rang}(g)$ и $\operatorname{def}(g)$.

Очевидно, что ранги преобразований из Π_n могут принимать значения от 1 до n, а дефекты — значения от 0 до $n-1$. В частности, подстановки из Π_n — это преобразования ранга n и дефекта 0.

Непосредственно из определения произведения преобразований (см. § 2 главы 1) следует

Утверждение 9. *Для любых преобразований* $g_1, g_2 \in \Pi_n$

$$\operatorname{rang}(g_1 g_2) \leqslant \min\{\operatorname{rang}(g_1), \operatorname{rang}(g_2)\}, \tag{9}$$

и соотношение (9) *является равенством, если* $g_1 \in S_n$ *или* $g_2 \in S_n$.

Следствие 1. *Для любого* $k \in \overline{1,n}$ *множество*

$$\Pi_n^{(k)} = \{g \in \Pi_n : \ \operatorname{rang}(g) \leqslant k\}$$

является подполугруппой полугруппы Π_n*, и все такие подполугруппы образуют цепочку*:

$$\Pi_n^{(1)} \subset \Pi_n^{(2)} \subset \ldots \subset \Pi_n^{(n)} = \Pi_n.$$

Следствие 2. *Если* M *есть система образующих элементов полугруппы* Π_n*, то множество* M' *всех подстановок из* M *порождает ее подполугруппу* S_n.

Таким образом, по следствию 2 любая система образующих полугруппы Π_n содержит систему образующих группы S_n. В связи с этим естественно возникает вопрос: какие преобразования следует добавить к S_n, чтобы получить систему образующих полугруппы Π_n? На этот вопрос отвечает

Теорема 10. *Множество* $A = M \cup S_n$ *из* Π_n *тогда и только тогда порождает полугруппу* Π_n*, когда* M *содержит хотя бы одно преобразование ранга* $n-1$.

□ Если в A нет преобразований ранга $n-1$, то в любом произведении $g_1 \ldots g_m = g$ преобразований $g_i \in A$, $i \in \overline{1,m}$, или все сомножители — подстановки или есть сомножитель ранга $r < n-1$. В первом случае g — подстановка, во втором — $\operatorname{rang}(g) < n-1$. Следовательно, в полугруппе $[A\rangle$ нет преобразований ранга $n-1$, и потому $[A\rangle \neq \Pi_n$.

Обратно, пусть $g_0 \in A$ и $\operatorname{rang}(g_0) = n-1$. Докажем, что $[A\rangle = \Pi_n$. Для этого достаточно доказать импликацию

$$g \in \Pi_n \ \Rightarrow \ g \in [A\rangle. \tag{10}$$

Докажем ее индукцией по $\operatorname{def}(g)$. Если $\operatorname{def}(g) = 0$, то $g \in S_n$, и утверждение (10) очевидно. Предположим, что оно верно для любого $g \in \Pi_n$ при условии $\operatorname{def}(g) < k$, где $k \in \overline{1, n-1}$, и рассмотрим случай, когда $\operatorname{def}(g) = k$. Так как $k > 0$, то существуют такие $s, t, j \in \overline{1,n}$, что $s \neq t$, $g(s) = g(t)$, $j \notin g(\overline{1,n})$. Возьмем из Π_n следующее преобразование g':

$$g'(x) = g(x), \ \text{если } x \neq t, \ \text{и } g'(t) = j. \tag{11}$$

Так как $\operatorname{def}(g') = \operatorname{def}(g) - 1 = k-1$, то по предположению индукции $g' \in [A\rangle$. Теперь найдем такое $g'' \in [A\rangle$, что $g''g' = g$. Для этого воспользуемся содержащимися в A

подстановками из S_n и преобразованием g_0. Так как $\operatorname{rang}(g_0) = n-1$, то существуют такие $u, v \in \overline{1,n}$, что $u \neq v$ и $g_0(u) = g_0(v)$. Домножив g_0 слева на подстановку h_1 со свойством $h_1(s) = u$, $h_1(t) = v$, получим преобразование $g_1 = h_1 g_0$ такое, что $g_1(s) = g_1(t)$. Кроме того, по утверждению 11 $\operatorname{rang}(g_1) = n-1$, и потому существует лишь один элемент $r \in \overline{1,n} \setminus g_1(\overline{1,n})$. Следовательно, преобразование

$$h_2 = \begin{pmatrix} g_1(1) & g_1(2) & \dots & g_1(s) & \dots & g_1(t-1) & r & g_1(t+1) & \dots & g_1(n) \\ 1 & 2 & \dots & s & \dots & t-1 & t & t+1 & \dots & n \end{pmatrix}$$

является подстановкой из S_n, и для $g'' = g_1 h_2$ имеем:

$$g''(x) = x, \text{ если } x \neq t, \text{ и } g''(t) = s. \tag{12}$$

Теперь из (12) и (11) находим: $(g''g')(x) = g(x)$ для любого $x \in \overline{1,n}$, т. е. $g''g' = g$, или, подробнее, $h_1 g_0 h_2 g' = g$. Так как $h_1, g_0, h_2, g' \in [A\rangle$ и $[A\rangle$ — полугруппа, то $g \in [A\rangle$. □

§ 5. ПОЛУГРУППЫ БИНАРНЫХ ОТНОШЕНИЙ

Рассмотрим множество $B(\Omega)$ всех бинарных отношений на фиксированном множестве Ω. В § 1 главы 3 была определена операция умножения бинарных отношений $\rho_1\rho_2$:

$$\forall\, a, b \in \Omega:\ \ (a\,(\rho_1\rho_2)\,b \ \Leftrightarrow\ \exists\, c \in \Omega:\ \ a\,\rho_1\,c,\ c\,\rho_2\,b),$$

и показано, что эта операция ассоциативна. Следовательно, $(B(\Omega);\cdot)$ — полугруппа. Очевидно, что эта полугруппа конечна (и имеет порядок $2^{|\Omega|^2}$), если $|\Omega| < \infty$, и бесконечна в противном случае. В полугруппе $B(\Omega)$ есть единичный элемент, им является отношение равенства (проверьте).

Укажем на связь полугруппы $B(\Omega)$ с рассмотренной в § 4 полугруппой $\Pi(\Omega)$.

Утверждение 11. *Полугруппа* $(\Pi(\Omega);\cdot)$ *всех преобразований множества* Ω *изоморфно вложима в полугруппу* $(B(\Omega);\cdot)$.

□ Зададим отображение $\varphi\colon \Pi(\Omega) \to B(\Omega)$, сопоставив каждому преобразованию $g \in \Pi(\Omega)$ отношение ρ_g, определенное следующим образом:

$$\forall\, a, b \in \Omega:\ \ (a\,\rho_g\,b \ \Leftrightarrow\ g(a) = b).$$

Покажем, что φ — мономорфизм. Во-первых, отображение φ инъективно. Действительно, если $g, h \in \Pi(\Omega)$ и $g \neq h$, то существуют такие $a, b \in \Omega$, что $g(a) = b \neq h(a)$. Следовательно, $(a,b) \in \rho_g$ и $(a,b) \notin \rho_h$, т. е. $\rho_g \neq \rho_h$. Во-вторых, φ — гомоморфизм, т. е. для любых g, h из $\Pi(\Omega)$ выполняется равенство

$$\varphi(gh) = \varphi(g)\varphi(h), \text{ или } \rho_{gh} = \rho_g\rho_h.$$

Справедливость последнего равенства доказывает следующая последовательность равносильностей:

$$\begin{aligned} a\,\rho_{gh}\,b \ \Leftrightarrow\ (gh)(a) = b \ &\Leftrightarrow\ \exists\, c \in \Omega:\ \ g(a) = c,\ h(c) = b \ \Leftrightarrow \\ &\Leftrightarrow\ \exists\, c \in \Omega:\ \ (a\,\rho_g\,c,\ c\,\rho_h\,b) \ \Leftrightarrow\ a\,(\rho_g\rho_h)\,b. \quad \square \end{aligned}$$

Из утверждения 11 и теоремы 8 получаем

Следствие. *Любая полугруппа изоморфно вложима в полугруппу бинарных отношений $B(\Omega)$ на подходящем множестве Ω.*

Рассмотрим еще ряд других используемых на практике операций над бинарными отношениями. Так как $B(\Omega)$ есть множество всех подмножеств декартова квадрата $\Omega \times \Omega$, то на $B(\Omega)$ определены ассоциативные бинарные операции пересечения $\cap$ и объединения $\cup$. Следовательно, имеем еще две полугруппы бинарных отношений на множестве $B(\Omega)$: $(B(\Omega);\cap)$ и $(B(\Omega);\cup)$. Обе эти полугруппы коммутативны и имеют нейтральные элементы — соответственно универсальное отношение $\Omega \times \Omega$ и пустое отношение $\varnothing$.

В том случае, когда множество Ω конечно, с полугруппами $(B(\Omega);\cap)$ и $(B(\Omega);\cup)$ естественным образом связаны изоморфные им полугруппы матриц над $\mathbb{Z}_2 = \{0,1\}$.

Определение 10. *Матрицей инцидентности* бинарного отношения ρ на множестве $\Omega = \{\omega_1, \ldots, \omega_n\}$ называется матрица $A_\rho = (a_{ij})_{n\times n}$, в которой для любых $i, j \in \overline{1,n}$

$$a_{ij} = \begin{cases} 1, & \text{если } (\omega_i, \omega_j) \in \rho, \\ 0, & \text{если } (\omega_i, \omega_j) \notin \rho. \end{cases}$$

Заметим, что матрица A_ρ зависит от упорядочивания элементов множества Ω, однако при фиксированном порядке соответствие $\rho \to A_\rho$ задает биективное отображение σ множества $B(\Omega)$ на множество B_n всех $(n \times n)$-матриц над $\mathbb{Z}_2$, или булевых матриц порядка n.

Выясним, как матрицы инцидентности отношений $\rho_1\rho_2$, $\rho_1 \cap \rho_2$, $\rho_1 \cup \rho_2$ выражаются через матрицы A_{ρ_1}, A_{ρ_2}. С этой целью введем сначала на множестве матриц B_n три новые операции. При их определении элементы 1, 0 рассматриваются как истина и ложь в математической логике, и потому становится возможным использование логических операций конъюнкции $\&$ и дизъюнкции $\vee$ (см. § 2 главы 1). Далее для $a, b \in \{1,0\}$ вместо $a \,\&\, b$ будем писать ab.

Определение 11. Пусть $A = (a_{ij})_{n\times n}$ и $B = (b_{ij})_{n\times n}$ — две матрицы с элементами из множества $\{1,0\}$. *Пересечением, объединением* и *логическим* (или *булевым*) *произведением* матриц A, B называются соответственно матрицы

$$A \wedge B = (c_{ij})_{n\times n}, \quad A \vee B = (d_{ij})_{n\times n}, \quad A \,\&\, B = (s_{ij})_{n\times n},$$

где для всех $i, j \in \overline{1,n}$

$$c_{ij} = a_{ij}b_{ij}, \quad d_{ij} = a_{ij} \vee b_{ij}, \quad s_{ij} = \bigvee_{k=1}^{n} a_{ik}b_{kj}.$$

Очевидно, что введенные операции на множестве B_n ассоциативны, и мы имеем три полугруппы матриц:

$$(B_n;\wedge), \quad (B_n;\vee), \quad (B_n;\,\&).$$

Теорема 12. *Если* $\Omega = \{\omega_1, \ldots, \omega_n\}$, *то отображение* $\sigma\colon B(\Omega) \to B_n$, *определенное формулой*

$$\forall\, \rho \in B(\Omega):\ \ \sigma(\rho) = A_\rho,$$

является изоморфизмом полугрупп $(B(\Omega); \cap)$, $(B(\Omega); \cup)$, $(B(\Omega), \cdot)$ *бинарных отношений соответственно на полугруппы матриц* $(B_n; \wedge)$, $(B_n; \vee)$ *и* $(B_n; \&)$.

□ Выше уже отмечалось, что отображение σ биективно. Чтобы показать, что σ является гомоморфизмом в каждом из трех случаев, достаточно для любых отношений $\rho_1, \rho_2 \in B(\Omega)$ доказать равенства

$$A_{\rho_1 \cap \rho_2} = A_{\rho_1} \wedge A_{\rho_2}, \quad A_{\rho_1 \cup \rho_2} = A_{\rho_1} \vee A_{\rho_2}, \quad A_{\rho_1 \rho_2} = A_{\rho_1} \,\&\, A_{\rho_2}. \tag{13}$$

Доказываются эти равенства сходным образом. Докажем для примера последнее равенство.

Пусть $A_{\rho_1} = (a_{ij})_{n\times n}$, $A_{\rho_2} = (b_{ij})_{n\times n}$, $A_{\rho_1\rho_2} = (c_{ij})_{n\times n}$. Используя определения, получим цепочку эквивалентностей

$$c_{ij} = 1 \ \Leftrightarrow\ \omega_i\,(\rho_1\rho_2)\,\omega_j \ \Leftrightarrow\ \exists \omega_k \in \Omega:\ \ (\omega_i\,\rho_1\,\omega_k,\ \omega_k\,\rho_2\,\omega_j) \ \Leftrightarrow$$

$$\Leftrightarrow\ \exists\, k \in \overline{1,n}:\ \ (a_{ik} = 1,\ b_{kj} = 1) \ \Leftrightarrow\ \bigvee_{s=1}^{n} a_{is} b_{sj} = 1.$$

Таким образом,

$$\forall\, i, j \in \overline{1,n}:\ \ c_{ij} = \bigvee_{s=1}^{n} a_{is} b_{sj}, \quad \text{т. е.} \quad A_{\rho_1\rho_2} = A_{\rho_1} \,\&\, A_{\rho_2}. \quad \square$$

ЗАДАЧИ

1. Будут ли подполугруппами полугруппы $(P_{n,n}; \cdot)$ всех $(n \times n)$-матриц над полем P множества:

а) всех матриц ранга r;

б) всех матриц рангов, не превосходящих r (r — любое число из множества $\overline{0,n}$)?

2. Пусть R — коммутативное кольцо с единицей и $R_1 \subset R$. При каком условии множество всех матриц из $R_{n,n}$ с определителями из R_1 образует подполугруппу полугруппы $(R_{n,n}; \cdot)$?

3. Найдите все элементы подполугруппы $[A\rangle$ полугруппы $(\mathbb{Z}; +)$, если

а) $A = \{3, 5\}$; б) $A = \{4, 6, 10\}$; в) $A = \{2, -3\}$.

4. Пусть $\mathbb{E}$ — множество всех элементарных матриц размеров $n \times n$ над полем P. Докажите:

а) $\mathbb{E}$ порождает полугруппу $(P^*_{n,n}; \cdot)$, при любых $n \in \mathbb{N}$ и P;

б) $\mathbb{E}$ порождает полугруппу $(P_{n,n}; +)$ тогда и только тогда, когда $P \neq GF(2)$ или $P = GF(2)$, $n = 1$;

в) подмножество $M = \mathbb{E} \cup \mathbb{F}$ из $P_{n,n}$ порождает полугруппу $(P_{n,n}; \cdot)$ тогда и только тогда, когда в $\mathbb{F}$ содержится хотя бы одна матрица ранга $n - 1$.

5. Докажите, что для любых $a, b, a_1, \ldots, a_t \in \mathbb{Z}_m$ в полугруппе $(\mathbb{Z}_m; +)$ справедливы утверждения:

а) $[a\rangle \subset [b\rangle \;\Leftrightarrow\; (b, m) \mid (a, m)$;

б) $[a\rangle = [b\rangle \;\Leftrightarrow\; (b, m) = (a, m)$;

в) $[a_1, \ldots, a_t\rangle = [d_1\rangle = [d\rangle$, где $d_1 = (a_1, \ldots, a_t)$, $d = (a_1, \ldots, a_t, m)$.

6. Опишите все подполугруппы полугруппы $(\mathbb{Z}_m; +)$ при $m = p$, p^n, 100, где p — простое число.

7. Опишите с точностью до изоморфизма все циклические полугруппы.

8. Является ли отображение $\varphi\colon \mathbb{C} \to \mathbb{C}$ гомоморфизмом полугруппы $(\mathbb{C}; *)$ в себя, если $*$ есть $+$ или $\cdot$, а φ определяется одним из следующих равенств (при любом $z = a + bi \in \mathbb{C}$ и фиксированном $n \in \mathbb{N}$):

а) $\varphi(z) = |z|$; б) $\varphi(z) = \arg z$; в) $\varphi(z) = nz$;

г) $\varphi(z) = z^n$; д) $\varphi(z) = a$; е) $\varphi(z) = a - bi$?

9. Пусть $R[x]$ — кольцо многочленов над кольцом R. Является ли отображение $\varphi\colon R[x] \to R$ гомоморфизмом полугруппы $(R[x]; *)$ в полугруппу $(R; *)$, если $*$ есть $+$ или $\cdot$, а φ определяется одним из следующих способов (при любом $a(x) \in R[x]$ и фиксированном $n \in \mathbb{N}$):

а) $\varphi(a(x))$ есть свободный член $a(x)$;

б) $\varphi(a(x))$ есть старший коэффициент $a(x)$, если $a(x) \neq 0$, и 0 если $a(x) = 0$;

в) $\varphi(a(x)) = a(r)$, для некоторого фиксированного $r \in R$?

10. Является ли гомоморфизмом полугруппы $(R_{n,n}; *)$ на себя отображение $\varphi\colon R_{n,n} \to R_{n,n}$, если R — любое кольцо, $*$ есть $+$ или $\cdot$, а φ каждую матрицу A отображает в транспонированную к ней матрицу A^T?

11. Являются ли конгруэнциями отношения:

а) «иметь равные действительные части» на полугруппах $(\mathbb{C}; +)$ и $(\mathbb{C}; \cdot)$;

б) «иметь равные ранги» на полугруппе матриц $(P_{n,n}; \cdot)$ над полем P;

в) «иметь одно и то же множество простых делителей» на полугруппе $(\mathbb{N}; \cdot)$;

г) «иметь равные значения в фиксированной точке r из кольца R» на полугруппах многочленов $(R[x]; +)$, $(R[x]; \cdot)$;

д) «иметь равные дефекты» на полугруппе $(\Pi_n; \cdot)$?

12. Опишите все обратимые элементы в полугруппах бинарных отношений $(B(M); \cdot)$, $(B(M); \cap)$, $(B(M); \cup)$ при $M = \overline{1, n}$.

13. Опишите все конгруэнции и все гомоморфные образы полугрупп $(\mathbb{Z}_{p^n}; +)$ и $(\mathbb{Z}_{p^n}; \cdot)$ при простом p.

14. Будут ли подполугруппами в полугруппе $(B(M); *)$, где $*$ — одна из операций $\cap$, $\cup$, $\cdot$, подмножества:

а) всех рефлексивных отношений;

б) всех симметричных отношений;

в) всех транзитивных отношений;

г) всех конгруэнций?

Глава 11

ОСНОВЫ ТЕОРИИ ГРУПП

Понятие группы является одним из основных понятий современной математики, широко используемым в различных областях науки и техники. Как уже отмечалось во введении, понятие группы появилось в связи с исследованиями по проблеме разрешимости алгебраических уравнений над полем в радикалах. Эти исследования завершились созданием теории Галуа. При этом рассматривались лишь группы подстановок. По существу, такие группы использовались до Галуа в работах Ж. Л. Лагранжа (1771), П. Руффини (1799), Н. Х. Абеля (1824). Однако термин «группа» ввел Э. Галуа в 1832 г. Небольшие и кратко написанные работы Галуа долгое время оставались мало доступными. Существенное развитие теория групп получила в опубликованном в 1870 г. «Трактате о подстановках» французского математика К. Жордана (1838–1922). Эта книга (объемом 667 страниц), названная Жорданом комментариями к работам Галуа, привлекла всеобщее внимание математиков к теории групп. Далее, в конце XIX в. и в начале XX в. теорию групп успешно развивали такие крупные математики как У. Бернсайд[12], Ф. Х. Клейн, А. Кэли, С. Ли[13] и др. Благодаря их работам постепенно сформировалось понятие абстрактной группы. Определенные итоги развития групп на этом этапе были подведены в книгах У. Бернсайда «Теория групп конечного порядка» (1897) и О. Ю. Шмидта «Абстрактная теория групп» (1916). В данной главе будут изложены основы общей теории групп.

§ 1. ОПРЕДЕЛЯЮЩИЕ СВОЙСТВА ГРУПП

Введенная в предыдущей главе терминология позволяет определить группу как полугруппу с нейтральным элементом, в которой для каждого элемента есть обратный. Ниже будет показано, что класс всех групп можно выделить из класса всех полугрупп и некоторыми другими наборами свойств (каждый такой набор свойств называют определяющим).

Определение 1. Элемент $e_{\text{П}}$ ($e_{\text{Л}}$) группоида $(M, *)$ называют *правым* (*левым*) *нейтральным*, если

$$\forall\, m \in M:\ \ m * e_{\text{П}} = m \quad (\forall\, m \in M:\ \ e_{\text{Л}} * m = m).$$

[12] У. Бернсайд (1852–1927) — английский математик.
[13] С. М. Ли (1842–1899) — норвежский математик.

Ясно, что если в группоиде $(M,*)$ есть нейтральный элемент, то он — левый и правый нейтральный. Наоборот, если в $(M,*)$ имеются левый $e_{\text{Л}}$ и правый $e_{\text{П}}$ нейтральные элементы, то они совпадают:

$$e_{\text{Л}} = e_{\text{Л}} * e_{\text{П}} = e_{\text{П}},$$

следовательно, в $(M,*)$ есть нейтральный элемент. Читателю предлагается самостоятельно привести примеры полугрупп, в которых есть один или несколько правых нейтральных элементов и нет ни одного левого.

Определение 2. Если в группоиде $(M,*)$ есть правый нейтральный элемент $e_{\text{П}}$, то *правым обратным* для элемента $m \in M$ (относительно правого нейтрального $e_{\text{П}}$) называют элемент $m'_{\text{П}}$ со свойством $m * m'_{\text{П}} = e_{\text{П}}$.

Теорема 1. *Для полугруппы $(H,*)$ следующие утверждения эквивалентны*:

(а) $(H,*)$ — *группа*;

(б) *для любых $g,h \in H$ каждое из уравнений*

$$g * x = h, \qquad y * g = h \tag{1}$$

однозначно разрешимо в H;

(в) *для любых $g,h \in H$ уравнения* (1) *разрешимы в H*;

(г) *в $(H,*)$ существует правый нейтральный элемент $e_{\text{П}}$, относительно которого для каждого $h \in H$ существует правый обратный элемент $h'_{\text{П}} \in H$.*

□ Импликация (а)⇒(б) — это теорема 6 главы 3.

Импликация (б)⇒(в) очевидна.

(в)⇒(г) Зафиксируем $g \in H$ и обозначим через e_g решение уравнения $g * x = g$. Тогда $e_g = e_{\text{П}}$ — правый нейтральный элемент в $(H,*)$, поскольку для любого $h \in H$ существует $y_h \in H$ со свойством $h = y_h * g$ и справедливы равенства

$$h * e_g = (y_h * g) * e_g = y_h * (g * e_g) = y_h * g = h.$$

Правым обратным для h относительно $e_{\text{П}}$ является решение уравнения $h * x = e_{\text{П}}$.

(г)⇒(а) Для произвольного элемента $h \in H$, пользуясь равенством $e_{\text{П}} = h'_{\text{П}} * (h'_{\text{П}})'_{\text{П}}$, получаем

$$\begin{aligned} h'_{\text{П}} * h &= (h'_{\text{П}} * h) * e_{\text{П}} = (h'_{\text{П}} * h) * (h'_{\text{П}} * (h'_{\text{П}})'_{\text{П}}) = \\ &= h'_{\text{П}} * (h * h'_{\text{П}}) * (h'_{\text{П}})'_{\text{П}} = (h'_{\text{П}} * e_{\text{П}}) * (h'_{\text{П}})'_{\text{П}} = e_{\text{П}}. \end{aligned} \tag{2}$$

Отсюда, пользуясь равенством $e_{\text{П}} = h * h'_{\text{П}}$, получаем

$$e_{\text{П}} * h = h * h'_{\text{П}} * h = h * e_{\text{П}} = h.$$

Следовательно, $e_{\text{П}}$ — нейтральный элемент в $(H,*)$. Но тогда в силу (2) $h'_{\text{П}}$ — обратный для h элемент, т. е. $(H,*)$ — группа. □

Полезно заметить, что эквивалентность утверждений (а) и (г) теоремы позволяет производить «в два раза меньше» выкладок при проверке того, является ли данная

полугруппа группой. Эквивалентность утверждений (а), (б), (в) объясняет важную роль понятия «группа» в математике.

В дальнейшем, для обозначения групповой операции используются традиционные символы $+$ и $\cdot$, соответствующие аддитивной и мультипликативной формам записи. Употребляемые при этом обозначения и терминология приведены в § 2 главы 3. Аддитивная форма используется ниже только для коммутативных операций, мультипликативная — для произвольной групповой операции.

§ 2. ПОРЯДКИ ЭЛЕМЕНТОВ И ЭКСПОНЕНТА ГРУППЫ

Определение 3. *Порядком элемента* g группы $(G, \cdot)$ называют наименьшее из чисел $n \in \mathbb{N}$ со свойством $g^n = e$, если такие n существуют, и бесконечность — в противном случае. Порядок g обозначают через $\operatorname{ord} g$ и пишут, соответственно, $\operatorname{ord} g = n$ или $\operatorname{ord} g = \infty$.

Естественно, в группе $(G, +)$ при определении порядка элемента условие $g^n = e$ заменяется на $ng = \theta$.

Пример 1. В группе $(\mathbb{Z}, +)$ все ненулевые элементы имеют бесконечный порядок.

Пример 2. В группе $(\mathbb{Z}_m, +)$, $m \in \mathbb{N}$, каждый элемент имеет конечный порядок:

$$\forall\, d \in \mathbb{Z}_m \ (md = 0).$$

Пример 3. В группе $(\mathbb{C}^*, \cdot)$ обратимых элементов поля $\mathbb{C}$ комплексных чисел есть как элементы конечного порядка (все корни конечных степеней из 1), так и элементы бесконечного порядка (все остальные числа).

Очевидно условию $\operatorname{ord} g = 1$ удовлетворяет лишь нейтральный элемент группы.

Определение 4. Группа G, состоящая из конечного числа n элементов, называется *группой порядка* n или, просто, *конечной группой*. Пишут $|G| = n$ или $|G| < \infty$.

Утверждение 2. *Порядок любого элемента g конечной группы G конечен.*

□ Если $|G| = n$, то среди элементов $g^0 = e$, g^1, $\ldots$, g^n есть одинаковые. Следовательно, существуют $k, l \in \mathbb{N}_0$ такие, что $0 \leqslant k < l \leqslant n$ и $g^k = g^l$. Умножая обе части последнего равенства на g^{-k}, получаем $g^{l-k} = e$, $l - k \in \mathbb{N}$. □

Пример 3 показывает, что в бесконечной группе порядки элементов не обязательно бесконечны. Более того, существуют бесконечные группы, в которых все элементы имеют конечный порядок (т. е. обращение утверждения 2 неверно).

Пример 4. Для простого $p \in \mathbb{N}$ множество

$$\mathbb{C}(p^\infty) = \{\xi \in \mathbb{C} \colon\ \exists\, k \in \mathbb{N}\ (\xi^{p^k} = 1)\}$$

замкнуто относительно операции умножения. $\mathbb{C}(p^\infty)$ — группа, в которой каждый элемент имеет конечный порядок.

Основные свойства функции $\operatorname{ord} g$ описывает

Теорема 3. *Пусть g — элемент конечного порядка m в группе $(G,\cdot)$. Тогда*
(а) *элемент g^{-1} равен неотрицательной степени элемента g, а именно, верно равенство $g^{-1}=g^{m-1}$;*
(б) $\forall\, k\in\mathbb{Z}\ \ (g^k=e)\Leftrightarrow(m\mid k)$;
(в) $\forall\, k\in\mathbb{Z}\ \ \operatorname{ord} g^k=\dfrac{m}{(m,k)}$;
(г) *если $h\in G$ — элемент порядка n, $(m,n)=1$ и $gh=hg$, то верны равенства* $\operatorname{ord} gh=\operatorname{ord} g\cdot\operatorname{ord} h=mn$.

□ (а) Равенство $g^{-1}=g^{m-1}$ доказывается умножением равенства $e=g^m$ на g^{-1}.
(б) Разделим k на m с остатком: $k=qm+r,\ 0\leqslant r<m$. Тогда $g^k=(g^m)^q\cdot g^r$, и так как $r<m=\operatorname{ord} g$, то

$$(g^k=e)\ \Leftrightarrow\ (g^r=e)\ \Leftrightarrow\ (r=0)\ \Leftrightarrow\ (m\mid k).$$

(в) Пусть $h=g^k$ и $n\in\mathbb{N}$. Тогда, пользуясь утверждением (б) и теоремой 9(б) главы 4, получаем:

$$(h^n=e)\Leftrightarrow(g^{kn}=e)\Leftrightarrow(m\mid kn)\Leftrightarrow\Big(\frac{m}{(m,k)}\ \Big|\ \frac{kn}{(m,k)}\Big)\Leftrightarrow\Big(\frac{m}{(m,k)}\ \Big|\, n\Big).$$

Таким образом, $\operatorname{ord} h<\infty$ и наименьшее $n\in\mathbb{N}$ со свойством $h^n=e$ есть $n=\dfrac{m}{(m,k)}$.
(г) Так как $(gh)^{mn}=(g^m)^n(h^n)^m=e$, то $\operatorname{ord} gh<\infty$ и согласно (б) $\operatorname{ord} gh=k$, где $k\mid mn$. С другой стороны, так как $(gh)^k=g^kh^k=e$, то $g^k=h^{-k}$ и $\operatorname{ord} g^k=\operatorname{ord} h^{-k}$. Отсюда по утверждению (в) получаем равенство $\dfrac{m}{(m,k)}=\dfrac{n}{(n,k)}$, а так как $(m,n)=1$, то $\dfrac{m}{(m,k)}=\dfrac{n}{(n,k)}=1$. Следовательно, $m\mid k$ и $n\mid k$, а потому $mn\mid k$. Таким образом, $mn=k$. □

Определение 5. *Экспонентой группы* $(G,\cdot)$ называют наименьшее из чисел $m\in\mathbb{N}$ со свойством

$$\forall\, g\in G\ (g^m=e),$$

если такие m существуют, и бесконечность — в противном случае. Экспоненту группы G обозначают через $\exp G$ и пишут, соответственно, $\exp G=m$ или $\exp G=\infty$.

Пример 5. $\exp(\mathbb{Z},+)=\infty,\ \ \exp(\mathbb{Z}_m,+)=m,\ \ \exp\mathbb{C}(p^\infty)=\infty$.

Утверждение 4. *Экспонента конечной группы $G=\{g_1,\dots,g_n\}$ конечна и удовлетворяет равенству*

$$\exp G=[\operatorname{ord} g_1,\dots,\operatorname{ord} g_n]. \tag{3}$$

При этом если G — абелева группа, то существует элемент $g\in G$ со свойством $\operatorname{ord} g=\exp G$.

□ Пусть $k = [\operatorname{ord} g_1, \ldots, \operatorname{ord} g_n]$. Ввиду теоремы 3(б) для любого $g \in G$ верно равенство $g^k = e$, и потому $\exp G \leqslant k$. Пусть $\exp G = m$. Тогда по определению $g_i^m = e$ и по теореме 3(б) $\operatorname{ord} g_i \mid m$, $i \in \overline{1,n}$. Следовательно, $k \mid m$, и так как $m \leqslant k$, то $k = m$, т. е. верно (3).

Пусть $(G, \cdot)$ — абелева группа и число $m = \exp G$ имеет каноническое разложение $m = p_1^{k_1} \ldots p_t^{k_t}$. Тогда из (3) следует, что для каждого $j \in \overline{1,t}$ существует элемент $h_j \in G$ со свойством $p_j^{k_j} \mid \operatorname{ord} h_j$ (иначе не выполнялось бы условие $p_j^{k_j} \mid m$). Пусть $\operatorname{ord} h_j = p_j^{k_j} \cdot n_j$. Положим $f_j = h_j^{n_j}$. Тогда по теореме 3(в) $\operatorname{ord} f_j = p_j^{k_j}$, $j \in \overline{1,t}$, и по теореме 3(г) $g = f_1 \ldots f_t$ — искомый элемент порядка m. □

Очевидно, что вторая часть утверждения 4 справедлива для любой абелевой группы с конечной экспонентой. Пример группы $(\mathbb{Z}_2)^*_{2,2}$ показывает, что в этой части утверждения нельзя отказаться от условия коммутативности. Полезно заметить также, что если $\exp G = \infty$, то в группе G не обязательно есть элемент бесконечного порядка, даже если она коммутативна. Пример тому — группа $\mathbb{C}(p^\infty)$.

В § 4 будут получены дополнительные соотношения между порядком конечной группы, ее экспонентой и порядками ее элементов.

§ 3. ПОДГРУППЫ. ПОДГРУППА, ПОРОЖДЕННАЯ ПОДМНОЖЕСТВОМ

1. Введем одно из основных понятий теории групп.

Определение 6. Непустое подмножество H группы $(G, \cdot)$ называют ее *подгруппой*, если H замкнуто относительно групповой операции и является группой относительно этой операции. В этом случае пишут $H < (G, \cdot)$ или $H < G$. Если $H \notin \{G, \{e\}\}$, то подгруппу H называют *собственной*.

Очевидно, что всякая подгруппа в $(G, \cdot)$ является подполугруппой, но обратное неверно, как показывает пример подполугруппы $\mathbb{N}$ в $(\mathbb{Z}, +)$. Ясно также, что если $H < (G, \cdot)$, $M < (H, \cdot)$, то $M < (G, \cdot)$.

Пример 6. Для каждого $m \in \mathbb{Z}$ множество $m\mathbb{Z} = \{mk \colon k \in \mathbb{Z}\}$ есть подгруппа в $(\mathbb{Z}, +)$.

Пример 7. Пусть Γ — множество всех комплексных чисел с модулем 1, $\Gamma_{\mathbb{N}}$ — множество всех элементов конечного порядка из $\mathbb{C}^*$, Γ_m — множество всех корней степени $m \in \mathbb{N}$ из единицы в $\mathbb{C}$. Тогда

$$(\Gamma_m, \cdot) < (\Gamma_{\mathbb{N}}, \cdot) < (\Gamma, \cdot) < (\mathbb{C}^*, \cdot);$$

для каждого простого $p \in \mathbb{N}$ и каждого $n \in \mathbb{N}$

$$(\Gamma_{p^n}, \cdot) < (\mathbb{C}(p^\infty), \cdot) < (\Gamma_{\mathbb{N}}, \cdot).$$

Пример 8. Для любой группы $(G, \cdot)$ множество

$$C(G) = \{g \in G \colon \forall\, h \in G\ (gh = hg)\},$$

называемое *центром группы* G, есть подгруппа в $(G, \cdot)$ (докажите).

Пример 9. Для любой абелевой группы G множество $T(G)$ всех ее элементов конечного порядка есть подгруппа в G (докажите). Эта подгруппа называется *подгруппой кручения* группы G. В частности, $T(\mathbb{C}^*) = \Gamma_{\mathbb{N}}$, $T(\mathbb{R}^*) = \{1, -1\}$.

Утверждение 5. *Если H — подгруппа группы $(G, \cdot)$, то ее нейтральный элемент e_H совпадает с e_G и для каждого $h \in H$ обратный к h элемент в H совпадает с обратным к h элементом в G.*

□ Равенство $e_H = e_G$ следует из равенств $e_H e_H = e_H$ и $e_G e_H = e_H$ ввиду теоремы 1(б). Последняя часть утверждения теперь следует из единственности решения в G уравнения $hx = e_G$. □

При проверке свойства «быть подгруппой» полезно

Утверждение 6. *Непустое подмножество H группы $(G, \cdot)$ является ее подгруппой тогда и только тогда, когда*

$$\forall\, g, h \in H\ (gh^{-1} \in H). \tag{4}$$

□ Если $H < (G, \cdot)$, то (4) следует из определения подгруппы и утверждения 5. Пусть верно (4). Так как $H \neq \varnothing$, то существует $g \in H$ и в силу (4) $e = g \cdot g^{-1} \in H$. Тогда для любых $g, h \in H$ справедливы соотношения $h^{-1} = eh^{-1} \in H$ и $gh = g(h^{-1})^{-1} \in H$. Следовательно, подмножество H замкнуто относительно групповой операции на G, и так как эта операция ассоциативна, то H удовлетворяет всем условиям определения 6, т. е. $H < (G, \cdot)$. □

Следствие 1. *Конечное непустое подмножество H группы G является ее подгруппой тогда и только тогда, когда*

$$\forall\, g, h \in H\ (gh \in H), \tag{5}$$

т. е. тогда и только тогда, когда H — подполугруппа в $(G, \cdot)$.

□ Пусть $h \in H$. Тогда при условии (5) $h^n \in H$ для любого $n \in \mathbb{N}$. Отсюда ввиду конечности H так же, как и при доказательстве утверждения 2, получаем, что порядок элемента h конечен и по теореме 3(а) $h^{-1} \in H$. Теперь видно, что из (5) следует (4). □

Следствие 2. *Пусть $\varphi\colon (G, \cdot) \to (K, \cdot)$ — гомоморфизм групп. Тогда*
(а) *если $H < G$, то $\varphi(H) < K$;*
(б) *если $L < K$, то $\varphi^{-1}(L) < G$.*

□ (а) Для любых элементов $\alpha, \beta \in \varphi(H)$ существуют $a, b \in H$ такие, что $\varphi(a) = \alpha$ и $\varphi(b) = \beta$. Так как $ab^{-1} \in H$ и $\varphi(b^{-1}) = \varphi(b)^{-1}$, то

$$\alpha\beta^{-1} = \varphi(a)\,\varphi(b)^{-1} = \varphi(ab^{-1}) \in \varphi(H).$$

(б) Если $a, b \in \varphi^{-1}(L)$, то $\varphi(a)$, $\varphi(b) \in L$. Отсюда следует, что

$$\varphi(ab^{-1}) = \varphi(a)\,\varphi(b)^{-1} \in L,$$

т. е. $ab^{-1} \in \varphi^{-1}(L)$. □

2. Один из основных способов описания подгрупп группы G связан со следующим их свойством.

Утверждение 7. *Пересечение любого семейства* $\{G_\alpha : \alpha \in A\}$ *подгрупп группы* $(G, \cdot)$ *есть ее подгруппа.*

□ Пусть $H = \bigcap\limits_{\alpha \in A} G_\alpha$. Тогда для любых $g, h \in G$

$$(g, h \in H) \Rightarrow (\forall\, \alpha \in A\ (g, h \in G_\alpha)) \Rightarrow \forall\, \alpha \in A\ (gh^{-1} \in G_\alpha) \Rightarrow (gh^{-1} \in H),$$

и по утверждению 6 $H < (G, \cdot)$. □

Из утверждения 7 следует, что корректно

Определение 7. *Подгруппой* группы G, *порожденной подмножеством* $S \subset G$, называется подгруппа $\langle S \rangle$, равная пересечению всех подгрупп $H < (G, \cdot)$, содержащих S:

$$\langle S \rangle = \bigcap_{S \subset H < (G, \cdot)} H.$$

Если при этом $\langle S \rangle = G$ (т. е. G — единственная подгруппа в G, содержащая S), то говорят, что S — *система образующих группы* G, или что группа G *порождается множеством* S.

Разумеется, всегда $G = \langle G \rangle$. Однако при изучении свойств данной группы G зачастую важно найти для нее систему образующих, содержащую как можно меньше элементов. Например, можно написать $(\mathbb{Z}, +) = \langle \mathbb{N} \rangle$, а можно — $(\mathbb{Z}, +) = \langle 1 \rangle$.

Определение 8. Группу G называют *конечно порожденной*, если она имеет конечную систему образующих, и *циклической*, если она может быть порождена каким-либо одним элементом.

Важный результат, позволяющий строить различные системы образующих группы, состоит в следующем описании элементов группы $\langle S \rangle$. Очевидно, что $\langle \varnothing \rangle = \{e\}$.

Теорема 8. *Для любого непустого подмножества* S *группы* $(G, \cdot)$ *подгруппа* $\langle S \rangle$ *состоит из всех элементов* $g \in G$ *вида* $g = s_1^{c_1} \cdot \ldots \cdot s_n^{c_n}$, *где* $n \in \mathbb{N}$, $s_i \in S$, $c_i \in \mathbb{Z}$ *для* $i \in \overline{1, n}$, *т. е.*

$$\langle S \rangle = \{g \in G :\ g = s_1^{c_1} \ldots s_n^{c_n},\ \text{где } n \in \mathbb{N},\ s_i \in S,\ c_i \in \mathbb{Z},\ i \in \overline{1, n}\}. \tag{6}$$

□ Обозначим через $\overline{S}$ множество из правой части доказываемого равенства (6). Тогда $\overline{S} \subset \langle S \rangle$. Действительно, так как $S \subset \langle S \rangle$ и $\langle S \rangle$ — подгруппа в $(G, \cdot)$, то $\langle S \rangle$ содержит все конечные произведения элементов из S и обратных к ним, т. е. все элементы из $\overline{S}$.

Для доказательства обратного включения заметим, что $\overline{S} < (G, \cdot)$. Действительно, если $g, h \in \overline{S}$, то $g = \alpha_1^{a_1} \cdot \ldots \cdot \alpha_m^{a_m}$, $h = \beta_1^{b_1} \cdot \ldots \cdot \beta_n^{b_n}$ для некоторых $m, n \in \mathbb{N}$, $\alpha_i, \beta_j \in S$, $a_i, b_j \in \mathbb{Z}$ ($i \in \overline{1, m}$, $j \in \overline{1, n}$), и потому $gh^{-1} = \alpha_1^{a_1} \cdot \ldots \cdot \alpha_m^{a_m} \cdot \beta_n^{-b_n} \cdot \ldots \cdot \beta_1^{-b_1}$ — элемент из $\overline{S}$. Остается заметить, что так как $S \subset \overline{S}$, то по определению 7 $\langle S \rangle \subset \overline{S}$. □

Следствие 1. *В условиях теоремы* 8 *подгруппа* $\langle S \rangle$ *коммутативна тогда и только тогда, когда элементы множества* S *попарно перестановочны.*

Следствие 2. *В условиях теоремы* 8 *справедливо равенство* $\langle S\rangle = [S \cup S^{-1}\rangle$, *где* $S^{-1} = \{s^{-1} : s \in S\}$, *а если* G *— конечная группа, то* $\langle S\rangle = [S\rangle$.

□ Достаточно воспользоваться утверждением 2 главы 10 и теоремой 3(а). □

Следствие 3. *Если* $\varphi\colon G \to H$ *— гомоморфизм групп и* $G = \langle S\rangle$, *то* $\varphi(G) = \langle\varphi(S)\rangle$.

Пример 10. Группа $G = P^*_{n,n}$ всех обратимых $(n \times n)$-матриц над полем P порождается множеством S всех элементарных матриц (см. следствие 3 теоремы 4 главы 7).

Пример 11. Группа $(\mathbb{Q}, +)$ порождается множеством S всех дробей вида $\frac{1}{p^k}$, где p пробегает множество всех простых чисел, а k — множество $\mathbb{N}$. Если S' получено из S удалением конечного множества элементов, то равенство $\mathbb{Q} = \langle S'\rangle$ сохраняется (докажите).

Замечание 1. Если $S = \{g_1, \ldots, g_t\}$ — конечная система попарно перестановочных элементов группы G, то элементы порождаемой ею подгруппы допускают существенно более простое описание:

$$\langle g_1, \ldots, g_t\rangle = \{g \in G : g = g_1^{c_1} \cdot \ldots \cdot g_t^{c_t}, \text{ где } c_1, \ldots, c_t \in \mathbb{Z}\}$$

при мультипликативной форме записи групповой операции и

$$\langle g_1, \ldots, g_t\rangle = \{g \in G : g = c_1 g_1 + \ldots + c_t g_t, \text{ где } c_1, \ldots, c_t \in \mathbb{Z}\}$$

при аддитивной форме записи. Первое из этих равенств легко получается из (6) перегруппировкой сомножителей в представлении элементов $g \in G$ в виде $g = s_1^{c_1} \cdot \ldots \cdot s_n^{c_n}$, а второе — его аддитивный аналог.

3. Теорема 8 позволяет описать все циклические группы и их подгруппы.

Теорема 9. *Пусть* $(G, \cdot) = \langle g\rangle$ *— циклическая группа. Тогда*

(а) *если* $\operatorname{ord} g = m < \infty$, *то* $(G, \cdot) \cong (\mathbb{Z}_m, \oplus)$ *и*

$$G = \{e = g^0, g^1, \ldots, g^{m-1}\}; \tag{7}$$

(б) *если* $\operatorname{ord} g = \infty$, *то* $(G, \cdot) \cong (\mathbb{Z}, +)$ *и*

$$G = \{\ldots, g^{-m}, \ldots, g^{-1}, e, g, \ldots, g^n, \ldots\}; \tag{8}$$

(в) *если* $H < (G, \cdot)$, *то* H *— циклическая группа.*

□ Легко видеть, что отображение $\varphi\colon \mathbb{Z} \to G$, определенное правилом $\forall\, c \in \mathbb{Z}\colon\ \varphi(c) = g^c$, есть гомоморфизм группы $(\mathbb{Z}, +)$ в группу $(G, \cdot)$. Так как по теореме 8 любой элемент из G имеет вид g^c при подходящем $c \in \mathbb{Z}$, то φ — эпиморфизм. Тогда по теореме 7 главы 10 группа $(G, \cdot)$ изоморфна факторгруппе $(\mathbb{Z}/\rho, +)$, где ρ — конгруэнция на $(\mathbb{Z}, +)$, определяемая условием

$$\forall\, a, b \in \mathbb{Z}\ (a\,\rho\, b \ \Leftrightarrow\ g^a = g^b).$$

(а) Если $\operatorname{ord} g = m$, то, пользуясь теоремой 3(б), получаем:

$$\forall\, a, b \in \mathbb{Z}\ (g^a = g^b) \ \Leftrightarrow\ (g^{a-b} = e) \ \Leftrightarrow\ (a \equiv b \,(\operatorname{mod} m)).$$

В этом случае ρ есть отношение сравнимости по модулю m, $(\mathbb{Z}/\rho, +) \cong (\mathbb{Z}_m, \oplus)$ (см. § 2 главы 5, замечание 1), и очевидно, что все различные элементы группы G описываются равенством (7).

(б) Если $\operatorname{ord} g = \infty$, то

$$\forall\, a, b \in \mathbb{Z}\colon\ g^a = g^b \ \Leftrightarrow\ a = b,$$

т. е. ρ есть отношение равенства на $\mathbb{Z}$, и $(\mathbb{Z}/\rho, +) \cong (\mathbb{Z}, +)$. В этом случае группа G описывается равенством (8).

(в) Пусть $H < G$. Если $H = \{e\}$, то $H = \langle e \rangle$ — циклическая группа. Если $H \neq \{e\}$, то существуют числа $k \in \mathbb{Z} \setminus \{0\}$ такие, что $g^k \in H$. Выберем среди них наименьшее по абсолютной величине число c. Пусть $g^c = h$. Покажем, что $H = \langle h \rangle$.

Включение $\langle h \rangle \subset H$ очевидно. Наоборот, для любого $h_1 \in H$ существует $k \in \mathbb{Z}$ такое, что $h_1 = g^k$. Разделим k на c с остатком: $k = qc + r$, $0 \leqslant r < |c|$. Заметим, что $g^r = g^k g^{-qc} = h_1 h^{-q} \in H$, поэтому условие $r \neq 0$ противоречит выбору c. Следовательно, $r = 0$, $k = q \cdot c$ и $h_1 = h^q \in \langle h \rangle$, т. е. $H \subset \langle h \rangle$. □

Следствие. *Две циклические группы изоморфны тогда и только тогда, когда их порядки равны. Бесконечная циклическая группа изоморфна любой ее собственной подгруппе.*

Из теоремы 9(в) следует, в частности, что примером 6 описаны все подгруппы группы $(\mathbb{Z}, +)$. Описание всех подгрупп конечной циклической группы будет дано в § 4.

§ 4. СМЕЖНЫЕ КЛАССЫ. ТЕОРЕМА ЛАГРАНЖА. ПОДГРУППЫ ЦИКЛИЧЕСКОЙ ГРУППЫ

Каждая подгруппа H группы $(G, \cdot)$ задает на G следующие два бинарных отношения.

Определение 9. Говорят, что элементы a, b группы G *сравнимы по подгруппе H справа* (*слева*), и пишут $a \equiv b\,(H)_{\text{П}}$ ($a \equiv b\,(H)_{\text{Л}}$), если $ab^{-1} \in H$ ($a^{-1}b \in H$).

Если G — абелева группа, то отношения сравнимости по H справа и слева совпадают, поскольку

$$ab^{-1} \in H \ \Leftrightarrow\ (ab^{-1})^{-1} \in H \ \Leftrightarrow\ ba^{-1} \in H \ \Leftrightarrow\ a^{-1}b \in H.$$

В этом случае говорят просто об отношении сравнимости по подгруппе H и пишут $a \equiv b\,(H)$. При аддитивной форме записи групповой операции отношение сравнимости по подгруппе H группы $(G, +)$ задается условием $a \equiv b\,(H) \ \Leftrightarrow\ a - b \in H$.

Эта запись позволяет легко увидеть, что в предыдущих главах мы уже встречали отношения на группах, являющиеся отношениями сравнимости по подгруппам.

Пример 12. На $(\mathbb{Z},+)$ отношение сравнимости по модулю m есть отношение сравнимости по подгруппе $\langle m\rangle = m\mathbb{Z}$:

$$\forall\, a,b\in\mathbb{Z}\ (a\equiv b\,(\mathrm{mod}\,m))\ \Leftrightarrow\ (a\equiv b\,(m\mathbb{Z})).$$

Пример 13. На мультипликативной группе $(\mathbb{C}^*,\cdot)$ поля $\mathbb{C}$ равенство аргументов чисел эквивалентно сравнимости чисел по подгруппе $(\mathbb{R}_{>0},\cdot)$ а равенство модулей — сравнимости по подгруппе $(\Gamma,\cdot)$ (см. пример 7).

Все приведенные в качестве примеров отношения являются отношениями эквивалентности, и это, как мы сейчас покажем, неслучайно.

Определение 10. *Правым* (*левым*) *смежным классом группы* $(G,\cdot)$ по ее подгруппе H с представителем $g\in G$ называется множество Hg (множество gH).

Теорема 10. *Пусть H — подгруппа группы $(G,\cdot)$. Тогда*

(а) *отношение сравнимости на G по подгруппе H справа есть отношение эквивалентности*;

(б) *для любого $g\in G$ класс элементов, сравнимых с g по H справа, есть Hg. Любые два правых смежных класса группы G по подгруппе H либо не пересекаются, либо совпадают. Группа G распадается на непересекающиеся правые смежные классы по подгруппе H.*

Аналогичные утверждения верны для левых смежных классов группы G по подгруппе H и отношения сравнимости по H слева.

□ (а) Обозначим, для краткости, отношение сравнимости на G по H справа через ρ, т. е. положим

$$\forall\, a,b\in G\colon\ a\,\rho\, b\ \Leftrightarrow\ a\equiv\ b\,(H)_{\Pi}\ \Leftrightarrow\ ab^{-1}\in H.$$

Отношение ρ рефлексивно, так как $e\in H$, и симметрично, так как в H существует обратный для каждого элемента из H. Наконец, ρ транзитивно, так как если $a\,\rho\, b$ и $b\,\rho\, c$, то $ab^{-1}\in H$, $bc^{-1}\in H$, и потому $ac^{-1}=(ab^{-1})(bc^{-1})\in H$, т. е. $a\,\rho\, c$.

(б) Для каждого $g\in H$ класс $[g]_\rho$ всех элементов, ρ-эквивалентных g, имеет вид

$$[g]_\rho=\{a\in G\colon\ ag^{-1}=h,\ h\in H\}=\{a\in G\colon\ a=hg,\ h\in H\}=Hg.$$

Теперь из общих свойств отношений эквивалентности (теорема 1 главы 2) следует, что для любых $g_1,g_2\in G$ классы $Hg_1=[g_1]_\rho$ и $Hg_2=[g_2]_\rho$ либо не пересекаются, либо совпадают, и если $\{Hg_\alpha\colon\ \alpha\in A\}$ — множество всех различных правых смежных классов G по H, то

$$G=\bigcup_{\alpha\in A}Hg_\alpha.\quad\square \tag{9}$$

Определение 11. Представление (9) группы G в виде объединения попарно непересекающихся правых смежных классов по подгруппе H называется *разложением G на правые смежные классы по H*.

Полезно заметить, что в (9) один из смежных классов G по H есть $H = He$.

Следующий результат по эффективности его использования в теории групп является одним из основополагающих.

Теорема 11. (а) *Любые два правых (левых) смежных класса группы G по подгруппе H равномощны. В частности, в конечной группе G для любого $g \in G$ верны равенства $|H| = |Hg| = |gH|$.*

(б) *Множество $\mathfrak{R}$ правых смежных классов G по H равномощно множеству $\mathfrak{L}$ левых смежных классов G по H.*

□ (а) Достаточно заметить, что отображение $\varphi\colon H \to Hg$, определяемое для элемента $h \in H$ формулой $\varphi(h) = hg$, есть биекция. Следовательно, все смежные классы G по H равномощны H.

(б) По теореме 10 и определению 9 для любых $g_1, g_2 \in G$ справедливы импликации

$$Hg_1 = Hg_2 \;\Leftrightarrow\; g_1 g_2^{-1} \in H \;\Leftrightarrow\; (g_1^{-1})^{-1} g_2^{-1} \in H \;\Leftrightarrow\; g_1^{-1} H = g_2^{-1} H.$$

Отсюда следует, что отображение $\psi\colon \mathfrak{R} \to \mathfrak{L}$, определяемое на $Hg \in \mathfrak{R}$ условием $\psi(Hg) = g^{-1}H$, задано корректно и является инъективным. Его сюръективность очевидна. Таким образом, ψ — биекция. □

Определение 12. *Индексом подгруппы H* в группе G называют число правых (левых) смежных классов G по H, если это число конечно, и бесконечность — в противном случае. Индекс H в G обозначают через $|G : H|$.

Очевидно, что если $H < G$, то $H = G \;\Leftrightarrow\; |G : H| = 1$.

Пример 14. $|\mathbb{Z} : \{0\}| = \infty$. Если $m \in \mathbb{N}$, то $|\mathbb{Z} : m\mathbb{Z}| = m$ и

$$\mathbb{Z} = m\mathbb{Z} \cup (1 + m\mathbb{Z}) \cup \ldots \cup (m - 1 + m\mathbb{Z}).$$

Пример 15. Если $m, k \in \mathbb{N}$ и $n = mk$, то при условии $\Gamma_n = \langle \xi \rangle$ справедливо равенство $\Gamma_n = \Gamma_m \cup \xi\Gamma_m \cup \ldots \cup \xi^{k-1}\Gamma_m$.

Следствие 1 (теорема Лагранжа). *Порядок подгруппы H конечной группы G делит порядок G и*

$$|G| = |G : H| \cdot |H|.$$

□ Разложение G на правые смежные классы по подгруппе H имеет вид $G = Hg_1 \cup \ldots \cup Hg_k$, где $k = |G : H|$. Отсюда $|G| = |Hg_1| + \ldots + |Hg_k|$ и, ввиду утверждения (а) теоремы 11, $|G| = k\,|H|$. □

Следствие 2. *Если $G > H > K$ — цепочка подгрупп конечной группы G, то $|G : K| = |G : H| \cdot |H : K|$. Если при этом $|G : K| = p$ — простое число, то либо $H = G$, либо $H = K$.*

□ $|G : K| = \dfrac{|G|}{|K|} = \dfrac{|G|}{|H|} \cdot \dfrac{|H|}{|K|} = |G : H| \cdot |H : K|$. □

Следствие 3. *Порядок любого элемента g конечной группы G делит $|G|$, в частности, $g^{|G|} = e$.*

□ По утверждению 2 порядок элемента g конечен, и по теореме 9(а) подгруппа $H = \langle g \rangle$ имеет порядок $|H| = \operatorname{ord} g$. Теперь соотношение $\operatorname{ord} g \mid |G|$ следует из теоремы Лагранжа. □

Следствие 4. *Если G — конечная группа, то* $\exp G \mid |G|$.

□ Достаточно воспользоваться утверждением 4 и предыдущим следствием. □

Следствие 5. *Любая группа G простого порядка p — циклическая.*

□ Пусть $g \in G \setminus \{e\}$. Тогда $\operatorname{ord} g > 1$, $\operatorname{ord} g \mid p$, и так как p — простое, то $\operatorname{ord} g = p$ и $|\langle g \rangle| = p = |G|$. Следовательно, $G = \langle g \rangle$. □

В общем случае для конечной группы G *обращение теоремы Лагранжа*, т. е. обращение импликации

$$(\exists\, H < G\ (|H| = d)) \ \Rightarrow\ (d \mid |G|),$$

неверно. Соответствующий пример будет построен позже (пример 29). Однако для конечных абелевых групп обращение теоремы Лагранжа верно. В полном объеме это будет доказано в § 14, а пока докажем это, и даже более сильное утверждение для циклических групп.

Теорема 12. *В циклической группе $G = \langle g \rangle$ порядка m для любого натурального делителя d числа m существует единственная подгруппа H порядка d: $H = \langle g^l \rangle$, где $l = m/d$.*

□ Подгруппа $H = \langle g^l \rangle$ имеет порядок d, так как по теореме 3(в) $\operatorname{ord} g^l = d$. Если $H_1 < G$ и $|H_1| = d$, то по теореме 9(в) H_1 — циклическая группа, т. е. $H_1 = \langle g^k \rangle$ для некоторого $k \in \overline{1, m-1}$. Тогда по теореме 9(а) $\operatorname{ord} g^k = |H_1| = d$ и по теореме 3(в) $d = \dfrac{m}{(m,k)}$, т. е. $\dfrac{m}{d} = (m,k)$. Поэтому $l = \dfrac{m}{d} \mid k$ и $g^k \in \langle g^l \rangle = H$, т. е. $H_1 \subset H$, а так как $|H_1| = |H|$, то $H_1 = H$. □

§ 5. ПРОИЗВЕДЕНИЯ ГРУПП И ПОДГРУПП

1. При описании строения групп используют различные способы, позволяющие из некоторой группы или совокупности групп строить другие группы. Один такой способ — факторизация — читателю уже знаком по главе 10 и еще будет подробно изучаться ниже. Другой, более простой, но также очень важный способ дает

Определение 13. *Прямым* (внешним) *произведением групп* $(G_1, \cdot)$, …, $(G_t, \cdot)$ называют группоид $(G, \cdot)$, где $G = G_1 \times \ldots \times G_t$ — декартово произведение множеств $G_1, \ldots, G_t$, а операция $\cdot$ на G задается условием

$$\forall\, g = (g_1, \ldots, g_t) \in G,\ \forall\, h = (h_1, \ldots, h_t) \in G\colon\ gh = (g_1 h_1, \ldots, g_t h_t).$$

Для этого группоида используют обозначение

$$G = G_1 \otimes \ldots \otimes G_t = \prod_{i=1}^{t} \otimes\, G_i.$$

Утверждение 13. *Пусть $G = G_1 \otimes \ldots \otimes G_t$ — прямое произведение групп. Тогда*

(а) *группоид $(G, \cdot)$ есть группа*;

(б) *группа G абелева тогда и только тогда, когда группы $G_1, \ldots, G_t$ абелевы*;

(в) *элемент $g = (g_1, \ldots, g_t) \in G$ имеет конечный порядок тогда и только тогда, когда конечные порядки имеют элементы g_1, ..., g_t, и в этом случае* $\operatorname{ord} g = [\operatorname{ord} g_1, \ldots, \operatorname{ord} g_t]$;

(г) *экспонента группы G конечна тогда и только тогда, когда конечны экспоненты групп G_1, ..., G_t, и при этом верно равенство* $\exp G = [\exp G_1, \ldots, \exp G_t]$.

□ Утверждения (а) и (б) очевидны, если заметить, что нейтральный элемент в $(G, \cdot)$ есть $e = (e_1, \ldots, e_t)$, где e_i — единица $(G_i, \cdot)$ для $i \in \overline{1,t}$, а обратный для $g = (g_1, \ldots, g_t) \in G$ есть $g^{-1} = (g_1^{-1}, \ldots, g_t^{-1})$.

(в) Для любого $k \in \mathbb{N}$ справедливо равенство $g^k = (g_1^k, \ldots, g_t^k)$ и потому верно $(g^k = e) \Leftrightarrow (g_1^k = e_1, \ldots, g_t^k = e_t)$. Остается воспользоваться теоремой 3(б).

(г) Заметим, что число $k \in \mathbb{N}$ удовлетворяет условию

$$\forall\, g_i \in G_i \ (g_i^k = e_i)$$

тогда и только тогда, когда $\exp G_i \mid k$. Теперь утверждение об экспонентах групп G и G_1, ..., G_t, легко следует из предыдущих рассуждений и определения экспоненты группы. □

Следствие 1. *Пусть G_1, ..., G_t — конечные циклические группы порядков, соответственно, $m_1, \ldots, m_t$, и $G = G_1 \otimes \ldots \otimes G_t$. Тогда следующие утверждения эквивалентны*:

(а) *G — циклическая группа*;

(б) *числа $m_1, \ldots, m_t$ попарно взаимно просты.*

□ Из условия следует, что $|G_s| = \exp G_s = m_s$ для $s \in \overline{1,t}$. Следовательно, $|G| = m_1 \ldots m_t$ и по утверждению 13(г) $\exp G = [m_1, \ldots, m_t]$. Поэтому из (а) следует равенство $[m_1, \ldots, m_t] = m_1 \ldots m_t$, которое эквивалентно (б). Наоборот, по условию для каждого $s \in \overline{1,t}$ в группе G_s можно выбрать элемент g_s порядка m_s. Тогда в силу утверждения 13(б) $g = (g_1, \ldots, g_t)$ — элемент группы G порядка $[m_1, \ldots, m_t]$. Если верно (б), то $\operatorname{ord} g = |G|$ и справедливо (а). □

Теперь может быть доказано свойство мультипликативности функции Эйлера (см. определение 4 главы 5).

Следствие 2. *Если $m_1, \ldots, m_t$ — натуральные попарно взаимно простые числа и $m = m_1 \ldots m_t$, то $\varphi(m) = \varphi(m_1) \ldots \varphi(m_t)$.*

□ Пусть $G_1, \ldots, G_t$ — группы из следствия 1. Тогда по теоремам 3(в) и 9(а) число элементов порядка m_s в группе G_s равно $\varphi(m_s)$ и число элементов порядка m в циклической группе $G = G_1 \otimes \ldots \otimes G_t$ равно $\varphi(m)$. Остается заметить, что ввиду условия $m_1 \ldots m_t = m$ для произвольного элемента $g = (g_1, \ldots, g_t) \in G$ справедливы импликации

$$(\operatorname{ord} g = m) \;\Leftrightarrow\; (\operatorname{ord} g_1 = m_1,\; \ldots,\; \operatorname{ord} g_t = m_t)$$

(докажите). □

При аддитивной форме записи операций в группах $G_1, \ldots, G_t$ будем говорить не о прямом произведении, а о прямой сумме этих групп. В этом случае групповую операцию на $G = G_1 \times \ldots \times G_t$ определим равенством $(g_1, \ldots, g_t) + (h_1, \ldots, h_t) = (g_1 + h_1,\; \ldots,\; g_t + h_t)$ и группу $(G, +)$ обозначим через $G_1 \oplus \ldots \oplus G_t$ или $\sum\limits_{i=1}^{t} \oplus\, G_i$.

2. Простота описания свойств произведения групп $G_1 \otimes \ldots \otimes G_t$ через свойства сомножителей G_i делает естественным правило: при изучении произвольной группы H в качестве одного из первых шагов выяснить, не изоморфна ли она некоторому прямому произведению групп? Методика решения этого вопроса опирается на следующие общие понятия и результаты, представляющие значительный самостоятельный интерес.

Определение 14. *Произведением непустых подмножеств A и B группы $(G, \cdot)$* называют подмножество $AB = \{ab\colon\ a \in A,\ b \in B\}$.

Если групповая операция записывается аддитивно, то вместо произведения аналогичным образом определяется сумма $A + B$. Очевидно, операция произведения на множестве непустых подмножеств группы G ассоциативна и справедливо

Утверждение 14. *Если A — непустое подмножество группы $(G, \cdot)$ и множество $A^{-1} = \{a^{-1}\colon\ a \in A\}$, то*

$$A < (G, \cdot) \;\Leftrightarrow\; (A^{-1} = A \text{ и } A^2 \subset A) \;\Leftrightarrow\; (AA^{-1} \subset A).$$

Отметим, что даже если A и B — подгруппы группы $(G, \cdot)$, то множество AB, вообще говоря, не является подгруппой в G. Например, в группе S_3 (см. § 4 главы 3) произведение любых двух различных подгрупп порядка 2 — не подгруппа (проверьте). Однако, верна

Теорема 15. *Произведение AB подгрупп A и B группы $(G, \cdot)$ есть подгруппа в $(G, \cdot)$ тогда и только тогда, когда подгруппы A и B перестановочны, т. е. $AB = BA$.*

□ Пользуясь утверждением 14, из условия $AB < G$ получаем равенства $AB = (AB)^{-1} = B^{-1}A^{-1} = BA$. Наоборот, из равенства $AB = BA$ получим:

$$(AB)(AB)^{-1} = ABB^{-1}A^{-1} = ABBA = AABB = AB.$$

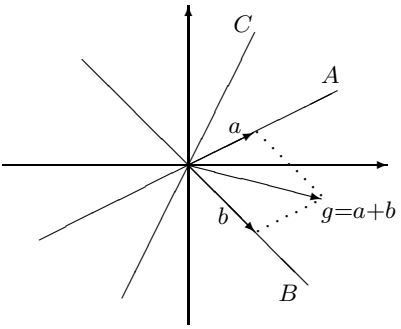
Следовательно, $AB < G$. □

Замечание 2. Если для подгрупп A и B группы G множество AB есть подгруппа, то это — наименьшая подгруппа, содержащая A и B, т. е. $AB = \langle A \cup B \rangle$ (докажите).

Следствие. *Сумма* (*произведение*) *любого конечного семейства* $A_1, \ldots, A_t$ *подгрупп абелевой группы* $(G, +)$ (*абелевой группы* $(G, \cdot)$) *есть подгруппа группы* G.

В дальнейшем произведение $A_1 \cdot \ldots \cdot A_t$ подмножеств группы $(G, \cdot)$ будем коротко записывать в виде $\prod_{i=1}^{t} A_i$, а сумму подмножеств группы $(G, +)$ — в виде $\sum_{i=1}^{t} A_i$. Представление какой-либо группы в виде суммы (произведения) ее подгрупп — один из важнейших способов описания различных классов групп.

Пример 16. В группе $(D^2, +)$ всех векторов декартовой плоскости, выходящих из начала координат, с операцией $+$ сложения векторов по правилу параллелограмма, подмножество A всех векторов, концы которых лежат на фиксированной прямой, проходящей через начало координат, есть подгруппа. Если B — любая другая подгруппа того же типа и $A \neq B$, то $D^2 = A + B$. Последнее равенство иллюстрируется следующим рисунком



Замечание 3. Операция пересечения подгрупп группы $(G, +)$ не дистрибутивна относительно операции сложения подгрупп: если $A, B, C < (G, +)$, то

$$C \cap (A + B) \supset (C \cap A) + (C \cap B),$$

однако левая и правая части этого соотношения, вообще говоря, не равны. Например, из рисунка к примеру 16 видно, что $A+B = D^2$ и $C \cap (A+B) = C$, но $C \cap A = C \cap B = 0$ и $(C \cap A) + (C \cap B) = 0$.

Пример 17. Пусть $G = G_1 \otimes \ldots \otimes G_t$ — прямое произведение групп и e_i — единица группы G_i для $i \in \overline{1,t}$. Для каждого $g_i \in G_i$ через $\overline{g}_i$ обозначим элемент группы G вида $\overline{g}_i = (e_1, \ldots, e_{i-1}, g_i, e_{i+1}, \ldots, e_t)$ и положим $\overline{G}_i = \{\overline{g}_i : g_i \in G_i\}$. Тогда очевидно, что $\overline{G}_1, \ldots, \overline{G}_t$ — попарно перестановочные подгруппы группы G, $\overline{G}_i \cong G_i$ и $G = \overline{G}_1 \cdot \ldots \cdot \overline{G}_t$. Более того, каждый элемент $g = (g_1, \ldots, g_t) \in G$ единственным способом представляется в виде $g = \xi_1 \ldots \xi_t$, где $\xi_1 \in \overline{G}_1$, $\ldots$, $\xi_t \in \overline{G}_t$ (это представление имеет вид $g = \overline{g}_1 \ldots \overline{g}_t$), и подгруппы $\overline{G}_i$ и $\overline{G}_j$ при $i \neq j$ не просто перестановочны, но *перестановочны поэлементно*, т. е. если $\xi_i \in \overline{G}_i$ и $\xi_j \in \overline{G}_j$, то $\xi_i \xi_j = \xi_j \xi_i$.

3. Теперь можно ответить на вопрос: при каких условиях группа H изоморфна прямому произведению групп?

Определение 15. Группа $(H,\cdot)$ называется *прямым произведением своих подгрупп* $H_1,\dots,H_t$, если

1) каждый элемент $h\in H$ однозначно представляется в виде

$$h=h_1\dots h_t,\quad \text{где}\quad h_1\in H_1,\ \dots,\ h_t\in H_t;$$

2) для любых $i,j\in\overline{1,t}$, $i\neq j$, группы H_i и H_j поэлементно перестановочны, т. е.

$$(h_i\in H_i,\ h_j\in H_j)\ \Rightarrow\ (h_ih_j=h_jh_i).$$

В этом случае пишут $H=H_1\dot\times\dots\dot\times H_t$.

Пример 18. В обозначениях примера 17 справедливо равенство $G=\overline{G}_1\dot\times\dots\dot\times\overline{G}_t$. Более того, если для некоторой группы H существует изоморфизм $\varphi\colon G_1\otimes\dots\otimes G_t\to H$, то $H_1=\varphi(\overline{G}_1)$, $\dots$, $H_t=\varphi(\overline{G}_t)$ — подгруппы группы H и $H=H_1\dot\times\dots\dot\times H_t$.

Пример 19. Если $k,l\in\mathbb{N}$, $(k,l)=1$, то $\Gamma_{kl}=\Gamma_k\dot\times\Gamma_l$.

Пример 20. $\mathbb{C}^*=\Gamma\dot\times\mathbb{R}_{>0}$, где $(\mathbb{R}_{>0},\cdot)$ — группа всех положительных действительных чисел.

Пример 21. Пусть $k,n\in\mathbb{N}$, $1\leqslant k<n$, и $(H,\cdot)$ — группа всех подстановок h множества $\overline{1,n}$, обладающих свойством: $h(\overline{1,k})=\overline{1,k}$. Тогда в H есть подгруппы $H_1=\{h\in H:\ h(i)=i$ для $i\in\overline{1,k}\}$, $H_2=\{h\in H:\ h(j)=j$ для $j\in\overline{k+1,n}\}$, и $H=H_1\dot\times H_2$.

Утверждение 16. *Пусть группа H раскладывается в прямое произведение подгрупп: $H=H_1\dot\times\dots\dot\times H_t$. Тогда*

(а) $H\cong\widehat{H}=H_1\otimes\dots\otimes H_t$;

(б) *если $h=h_1\dots h_t$, где $h_1\in H_1$, $\dots$, $h_t\in H_t$, то* $\operatorname{ord}h=[\operatorname{ord}h_1,\dots,\operatorname{ord}h_t]$, *если порядки элементов $h_1,\dots,h_t$ конечны, и* $\operatorname{ord}h=\infty$ *в противном случае*;

(в) *если подгруппы $H_1,\dots,H_t$ конечны, то*

$$|H|=|H_1|\cdot\ldots\cdot|H_t|,\quad \exp H=[\exp H_1,\ \dots,\ \exp H_t].$$

□ (а) Определим отображение $\varphi\colon\widehat{H}\to H$ следующим правилом: $\varphi((h_1,\dots,h_t))=h_1\dots h_t$. Тогда, ввиду условия 1 определения 15, φ — биекция, а ввиду условия 2 φ — гомоморфизм:

$$\begin{aligned}\varphi((h_1,\dots,h_t)\cdot(h'_1,\dots,h'_t))&=\varphi((h_1h'_1,\dots,h_th'_t))=h_1h'_1\cdot h_2h'_2\cdot\ldots\cdot h_th'_t=\\&=h_1\dots h_t\cdot h'_1\dots h'_t=\varphi((h_1,\dots,h_t))\cdot\varphi((h'_1,\dots,h'_t)).\end{aligned}$$

Утверждения (б) и (в) следуют теперь, соответственно, из утверждений 13(в) и 13(г). □

Замечание 4. Если группа $(H,\cdot)$ абелева, то для любых ее подгрупп $H_1,\dots,H_t$ условие 2 определения 15 выполняется автоматически, и равенство $H = H_1 \dot\times \dots \dot\times H_t$ эквивалентно условию 1 этого определения.

Замечание 5. Если H — абелева группа с аддитивной формой записи операции, то в определении 15 мультипликативная терминология также заменяется аддитивной: группу $(H,+)$ называют *прямой суммой* своих подгрупп $H_1,\dots,H_t$ и пишут $H = H_1 \dot+ \dots \dot+ H_t$, если любой элемент $h \in H$ однозначно представляется в виде $h = h_1 + \dots + h_t$, где $h_1 \in H_1$, …, $h_t \in H_t$.

Пример 22. В обозначениях примера 16 $D^2 = A \dot+ B$.

4. Следующий критерий важен для многих последующих разделов курса.

Теорема 17. *Пусть $H_1,\dots,H_t$ — подгруппы группы $(H,\cdot)$, удовлетворяющие условию 2 определения 15, и $H = H_1 \cdot \dots \cdot H_t$. Тогда следующие утверждения эквивалентны*:

(а) $H = H_1 \dot\times \dots \dot\times H_t$;

(б) *если* $e = h_1 \dots h_t$, *где* $h_i \in H_i$, $i \in \overline{1,t}$, *то* $h_1 = \dots = h_t = e$;

(в) *для каждого* $i \in \overline{1,t}$

$$H_i \cap (H_1 \cdot \dots \cdot H_{i-1} \cdot H_{i+1} \cdot \dots \cdot H_t) = \{e\}.$$

□ Импликация (а)⇒(б) следует из свойства 1 прямого произведения подгрупп и соотношений $e = e \cdot \dots \cdot e$, $e \in H_i$, $i \in \overline{1,t}$.

(б)⇒(в) Пусть элемент $h \in H_i \cap (H_1 \dots H_{i-1} H_{i+1} \dots H_t)$. Тогда $h = h_i$ и $h = h_1 \dots h_{i-1} h_{i+1} \dots h_t$, где $h_j \in H_j$ для $j \in \overline{1,t}$. Отсюда ввиду условия 2 получаем $e = h \cdot h^{-1} = h_1 \dots h_{i-1} h_i^{-1} h_{i+1} \dots h_t$ и согласно (б) $h_i^{-1} = e$. Следовательно, $h = h_i = e$.

(в)⇒(а) Пусть $h \in H$ и $h = h_1 \dots h_t = h'_1 \dots h'_t$, где $h_i, h'_i \in H_i$, $i \in \overline{1,t}$. Достаточно доказать, что $h_i = h'_i$ для $i \in \overline{1,t}$. Допустим, что, например, $h_1 \neq h'_1$. Тогда, пользуясь условием 2, получаем $e = h^{-1}h = h_1^{-1}h'_1 \cdot \dots \cdot h_t^{-1}h'_t$ и

$$(h_1^{-1}h'_1)^{-1} = h_2^{-1}h'_2 \cdot \dots \cdot h_t^{-1}h'_t \in H_1 \cap (H_2 \dots H_t), \quad h_1^{-1}h'_1 \neq e,$$

что противоречит утверждению (в) при $i = 1$. □

Следствие. *Если $H_1,\dots,H_t$ — конечные подгруппы абелевой группы $(G,+)$, имеющие попарно взаимно простые порядки, и $H = H_1 + \dots + H_t$, то $H = H_1 \dot+ \dots \dot+ H_t$.*

□ Пусть $|H_i| = m_i$ для $i \in \overline{1,t}$. Ввиду коммутативности групповой операции, достаточно доказать, что если $g \in H_1 \cap (H_2 + \dots + H_t)$, то $g = \theta$. По теореме Лагранжа из включений $g \in H_1$ и $g \in H_2 + \dots + H_t$ следуют, соответственно, равенства $m_1 g = \theta$ и $m_2 \dots m_t g = \theta$. Отсюда и из условия $(m_1, m_2 \dots m_t) = 1$ по теореме 3(б) следует, что $\operatorname{ord} g = 1$, т. е. $g = \theta$. □

5. Один из естественных подходов к описанию групп связан со следующим определением.

Определение 16. Группа $(G,\cdot)$ называется *разложимой*, если она представляется в виде прямого произведения двух собственных подгрупп. В противном случае, группа G называется *неразложимой*.

Очевидно, что задача описания (с точностью до изоморфизма) всех конечных групп сводится к описанию всех конечных неразложимых групп. Однако в классе некоммутативных групп вторая задача не легче первой. Качественно иная картина наблюдается в классе конечных абелевых групп. Здесь удается описать все неразложимые группы и дать полную классификацию конечных абелевых групп (см. главу 12). Первый шаг в этом направлении состоит в следующем.

Определение 17. Группа порядка p^n, где p — простое число, называется *p-группой*, или *примарной группой*.

Теорема 18. *Циклическая группа $(G,+)$ неразложима тогда и только тогда, когда она бесконечна или примарна. Любая конечная циклическая не примарная группа однозначно, с точностью до перестановки слагаемых, раскладывается в прямую сумму примарных циклических подгрупп.*

□ Если G — бесконечная группа, то она изоморфна группе $(\mathbb{Z},+)$, которая неразложима по теореме 17, поскольку любые две ее ненулевые подгруппы $m\mathbb{Z}$ и $n\mathbb{Z}$ имеют ненулевое пересечение: $m\mathbb{Z}\cap n\mathbb{Z}\ni mn\neq 0$.

Если $|G|=p^m$, то в G также любые две ненулевые подгруппы A и B имеют ненулевое пересечение. Действительно, по теореме 9(в) A и B — циклические группы, и по теореме Лагранжа они — p-группы. Тогда по теореме 12 в каждой из них есть подгруппа порядка p: $A_1<A$, $B_1<B$, $|A_1|=|B_1|=p$. Но по той же теореме в G есть лишь одна подгруппа порядка p. Поэтому $A_1=B_1\subset A\cap B$ и $A\cap B\neq\{0\}$. Таким образом, примарная циклическая группа неразложима.

Пусть, наконец, $|G|=n>1$, и каноническое разложение числа n имеет вид $n=p_1^{m_1}\ldots p_t^{m_t}$, где $t>1$. Тогда для каждого $i\in\overline{1,t}$ в G есть единственная подгруппа H_i порядка $p_i^{m_i}$ (теорема 12). Рассмотрим подгруппу $H=H_1+\ldots+H_t$. По следствию теоремы 17 $H=H_1\dot{+}\ldots\dot{+}H_t$. Но тогда по утверждению 16(в) выполняются равенства $|H|=|H_1|\cdot\ldots\cdot|H_t|=|G|$, и

$$G=H_1\dot{+}\ldots\dot{+}H_t$$

есть искомое разложение группы G в прямую сумму примарных циклических подгрупп. Единственность такого разложения с точностью до перестановки слагаемых следует из теоремы 12. □

В действительности теорема 18 описывает все неразложимые группы в классе абелевых конечно порожденных групп. Для конечных абелевых групп это будет доказано в главе 12 (теорема 1). Среди абелевых групп, не имеющих конечных систем образующих, есть другие неразложимые группы, например, группа $(\mathbb{Q},+)$ (докажите ее неразложимость).

§ 6. КЛАССЫ СОПРЯЖЕННЫХ ЭЛЕМЕНТОВ. НОРМАЛИЗАТОРЫ. ЦЕНТР p-ГРУППЫ

При изучении некоммутативных групп весьма полезным оказывается следующее бинарное отношение.

Определение 18. Элементы a и b группы $(G,\cdot)$ называют *сопряженными* и пишут $a \approx b$, если для некоторого элемента $g \in G$ выполняется равенство $g^{-1}ag = b$.

Очевидно, отношение сопряженности есть бинарное отношение на G, которое является тривиальным (совпадает с отношением равенства) в том и только в том случае, когда G — абелева группа.

Утверждение 19. *Отношение сопряженности на любой группе G есть отношение эквивалентности. Группа G разбивается на непересекающиеся классы сопряженных элементов.*

□ Так как $a = e^{-1}ae$ для любого $a \in G$, то отношение $\approx$ рефлексивно. Если $a \approx b$, то $b = g^{-1}ag$ для некоторого $g \in G$, а тогда $a = (g^{-1})^{-1}bg^{-1}$ и $b \approx a$, т. е. отношение $\approx$ симметрично. Если $a \approx b$ и $b \approx c$, то $b = g^{-1}ag$ и $c = h^{-1}bh$ для подходящих $g, h \in G$, а тогда $c = (gh)^{-1}a(gh)$, т. е. $a \approx c$, и отношение $\approx$ транзитивно.

Пусть $[a]_{\approx}$ — класс элементов группы G, сопряженных с a, и пусть множество всех таких различных классов есть $\{[a]_{\approx} :\ a \in A\}$. Тогда по общему свойству эквивалентности любые два различных класса из этого множества не пересекаются, и имеет место равенство

$$G = \bigcup_{a \in A} [a]_{\approx}\,. \quad \square \tag{10}$$

Определение 19. Равенство (10) называют *разложением группы G на классы сопряженных элементов*.

Замечание 6. В отличие от отношения сравнимости по подгруппе, отношение сопряженности разбивает любую некоммутативную группу G на классы разных мощностей. В частности, если $C(G)$ — центр группы, то

$$\forall\, a \in G \ \ (\,|[a]_{\approx}| = 1) \ \Leftrightarrow\ (a \in C(G))$$

(докажите).

Общий подход к описанию мощностей классов в разложении (10) основан на следующем понятии.

Определение 20. *Нормализатором подмножества M* группы G называется множество

$$N_G(M) = \{g \in G :\ gM = Mg\}.$$

Нормализатором элемента $a \in G$ называется множество $N_G(a) = N_G(\{a\})$.

Теорема 20. *Нормализатор подмножества M группы G есть подгруппа в G. Для любого элемента $a \in G$ справедливо равенство*

$$|[a]_{\approx}| = |G : N_G(a)|.$$

□ Пусть $x, y \in N_G(M)$. Тогда $xM = Mx$, $yM = My$, и $My^{-1} = y^{-1}M$. Отсюда следуют равенства $xy^{-1}M = xMy^{-1} = Mxy^{-1}$, доказывающие включение $xy^{-1} \in N_G(M)$. Следовательно, по утверждению 6 $N_G(M) < G$.

Класс $[a]_{\approx}$ состоит из всех различных элементов вида $x^{-1}ax$, $x \in G$. Заметим, что для любых $x, y \in G$ справедливы соотношения

$$(x^{-1}ax = y^{-1}ay) \Leftrightarrow (axy^{-1} = xy^{-1}a) \Leftrightarrow (xy^{-1} \in N_G(a)) \Leftrightarrow (N_G(a)x = N_G(a)y).$$

Таким образом, элементы $x^{-1}ax$ и $y^{-1}ay$ различны в том и только в том случае, если различны смежные классы $N_G(a)x$ и $N_G(a)y$. Следовательно, $|[a]_{\approx}| = |G : N_G(a)|$. □

Полученный результат оказывается весьма полезным при доказательстве различных классификационных теорем в теории групп. Одна из них

Теорема 21. *Для простого p центр любой p-группы не равен $\{e\}$. Любая группа порядка p^2 коммутативна.*

□ Пусть $|G| = p^n$, $n > 0$. Предположим, что $C(G) = \{e\}$. Тогда по замечанию 6 если $a \in G \setminus \{e\}$, то $|[a]_{\approx}| > 1$, и так как число $|[a]_{\approx}| = |G : N_G(a)|$ делит p^n, то $p \mid [a]_{\approx}$. В таком случае в разложении группы G на классы сопряженных элементов есть один класс мощности 1 — класс $[e]_{\approx}$, а мощности остальных классов кратны p:

$$G = [e]_{\approx} \cup [a_2]_{\approx} \cup \ldots \cup [a_t]_{\approx}, \quad |[a_i]| = pk_i, \quad i \in \overline{2,t}.$$

Поскольку в этом разложении классы не пересекаются, то $|G| = |[e]|+|[a_2]|+\ldots+|[a_t]|$, т. е. $p^n = 1 + p(k_2 + \ldots + k_t)$, что, очевидно, невозможно при $n > 0$. Следовательно, $C(G) \neq \{e\}$.

Пусть теперь $|G| = p^2$. По доказанному $C(G) \neq \{e\}$, и можно выбрать элемент $c \in C(G) \setminus \{e\}$. Если при этом $G = \langle c \rangle$, то коммутативность G доказана. Если $G \neq \langle c \rangle$, то $|G : \langle c \rangle| = p$, и можно выбрать элемент $g \in G \setminus \langle c \rangle$. Рассмотрим в G подгруппу $H = \langle c, g \rangle$. По построению справедливы соотношения $\langle c \rangle \lneqq H < G$. Отсюда по следствию 2 теоремы 11 $G = H = \langle c, g \rangle$, и так как $cg = gc$, то по следствию 1 теоремы 8 G — коммутативная группа. □

§ 7. ГРУППЫ ПОДСТАНОВОК. ОРБИТЫ И СТАБИЛИЗАТОРЫ. ЛЕММА БЕРНСАЙДА

1. В параграфах 2 и 4 главы 3 читатель уже познакомился с понятием подстановки на множестве Ω, операцией умножения подстановок, симметрической группой $(S(\Omega), \cdot)$ всех подстановок на Ω и симметрической группой $S_n = S(\overline{1,n})$ всех подстановок степени n.

Определение 21. Подгруппы группы $S(\Omega)$ называются *группами подстановок множества* Ω, а подгруппы S_n — *группами подстановок степени* n.

Следует отметить, что класс групп подстановок исторически — один из первых классов изучавшихся групп (в связи с задачей о разрешимости уравнений в радикалах). Более того, именно изучение свойств операции умножения на множестве S_n в значительной степени способствовало формированию абстрактного понятия группы. В современной алгебре группы подстановок продолжают играть важную роль как при решении задач классификации групп, так и в многочисленных прикладных вопросах. Ниже, в параграфах 7–9, изучаются лишь некоторые основные, первичные понятия теории групп подстановок, и на этих группах иллюстрируются результаты, полученные в предыдущих параграфах.

Особое положение теории групп подстановок в общей теории групп проясняет

Теорема 22 (Кэли). *Произвольная группа $(G,\cdot)$ изоморфна некоторой подгруппе группы $(S(G),\cdot)$.*

□ Поставим в соответствие каждому элементу $g \in G$ отображение $\widehat{g}\colon G \to G$, определяемое условием

$$\forall\, x \in G\colon\ \widehat{g}(x) = xg.$$

Покажем, что $\widehat{g} \in S(G)$. Действительно, $\widehat{g}$ сюръективно, так как для любого $y \in G$ верно равенство $\widehat{g}(yg^{-1}) = y$; $\widehat{g}$ инъективно, так как

$$\forall\, x, y \in G\ \ (\widehat{g}(x) = \widehat{g}(y)\ \Leftrightarrow\ xg = yg\ \Leftrightarrow\ x = y).$$

Таким образом, $\widehat{g} = \begin{pmatrix} x \\ xg \end{pmatrix}$ — подстановка на G.

Теперь покажем, что отображение $\Psi\colon G \to S(G)$, определяемое правилом

$$\forall\, g \in G\colon\ \Psi(g) = \widehat{g},$$

есть мономорфизм. Это отображение инъективно, так как если $\Psi(g_1) = \Psi(g_2)$ для $g_1, g_2 \in G$, то $\widehat{g}_1 = \widehat{g}_2$, а тогда $g_1 = \widehat{g}_1(e) = \widehat{g}_2(e) = g_2$. Наконец, Ψ — гомоморфизм группы $(G,\cdot)$ в группу $(S(G),\cdot)$, так как для любых $g, h \in G$ и для любого $x \in G$ справедливы соотношения $\Psi(gh) = \widehat{gh}$,

$$\widehat{gh}(x) = xgh = (xg)h = \widehat{g}(x)h = \widehat{h}(\widehat{g}(x)) = (\widehat{g}\cdot\widehat{h})(x),$$

доказывающие равенство $\Psi(gh) = \Psi(g)\Psi(h)$.

Итак, Ψ — мономорфизм G в $S(G)$, и по теореме 4 главы 10 $\Psi(G)$ — подгруппа группы $S(G)$, изоморфная G. □

Заметим, что для каждого $n \in \mathbb{N}$ класс всех групп порядка n разбивается отношением изоморфизма на непересекающиеся классы изоморфных групп. Число таких классов очевидно конечно (так как конечно число таблиц Кэли на множестве из n элементов). Более точную оценку этого числа дает

Следствие. *Любая группа G порядка n изоморфна некоторой подгруппе группы S_n. Число классов изоморфных групп порядка n равно числу классов изоморфных подгрупп порядка n в S_n.*

□ Достаточно заметить, что $S(G) \cong S_n$ (утверждение 15 главы 3), и потому G изоморфна подгруппе в S_n. □

Пример 23. Рассмотрим теорему Кэли в применении к циклической группе $(\mathbb{Z}_m, \oplus)$. Соответствующая ей группа $\widehat{\mathbb{Z}}_m$ есть группа подстановок на множестве $\overline{0, m-1}$. При этом циклическому образующему 1 группы $\mathbb{Z}_m$ по правилу, определенному теоремой 22, ставится в соответствие подстановка $t = \widehat{1} = \begin{pmatrix} 0 & 1 & \dots & x & \dots & m-1 \\ 1 & 2 & \dots & x \oplus 1 & \dots & 0 \end{pmatrix}$, и $\widehat{\mathbb{Z}}_m = \langle t \rangle$ — циклическая подгруппа в $S(\overline{0, m-1})$. Произвольному элементу $g \in \mathbb{Z}_m$ соответствует подстановка $\psi(g) = \widehat{g}$ вида

$$\widehat{g} = \begin{pmatrix} 0 & 1 & \dots & x & \dots \\ g & 1 \oplus g & \dots & x \oplus g & \dots \end{pmatrix} = t^g = \widehat{1}^g.$$

2. Теорема Кэли дает универсальный алгоритм, позволяющий представить любую конечную группу как группу подстановок. Правда, этот алгоритм, вообще говоря, не является ни единственно возможным, ни наиболее «экономным» (например, с его помощью сама группа S_n представляется группой подстановок степени не n, а $n!$). Однако важность теоремы Кэли определяется не только ее универсальностью, но и тем, что она — первый результат, открывший в теории групп новое направление — теорию представлений групп. В связи с этим уместно привести

Определение 22. *Подстановочным представлением* группы G на множестве Ω называется любой гомоморфизм $\sigma\colon G \to S(\Omega)$. Это представление называется *точным*, если σ — мономорфизм. При этом саму группу $\sigma(G)$ также иногда называют подстановочным представлением группы G. Если $|\Omega| = n$, то говорят, что $\sigma(G)$ — представление степени n (при этом уже не обязательно $|G| = n$).

В этих терминах теорема Кэли указывает точное подстановочное представление степени n группы G порядка n, называемое *правым регулярным представлением* G. Для любой группы $(G, \cdot)$ определяется и *левое регулярное представление*, при котором элементу $g \in G$ ставится в соответствие подстановка $\sigma(g) = \begin{pmatrix} x \\ g^{-1}x \end{pmatrix} \in S(G)$. (Докажите самостоятельно, что $\sigma\colon G \to S(G)$ — мономорфизм групп.)

Приведем еще некоторые важные примеры групп подстановок и подстановочных представлений.

Пример 24. Пусть R — произвольное кольцо с единицей e, $R^{(m)}$ — множество векторов-столбцов длины m над R. Поставим в соответствие каждой обратимой матрице $A \in R_{m,m}$ преобразование $\varphi_A\colon R^{(m)} \to R^{(m)}$, определяемое правилом

$$\forall\, x^{\downarrow} \in R^{(m)}\colon\ \varphi_A(x^{\downarrow}) = Ax^{\downarrow}.$$

Тогда φ_A — подстановка на $R^{(m)}$, называемая *линейной*, а множество $GL(m, R)$ всех линейных подстановок на $R^{(m)}$ есть подгруппа группы $S(R^{(m)})$, называемая *полной линейной группой* размерности m над кольцом R (доказательство сформулированных утверждений предоставляется читателю). Несложно проверить, что

отображение $\sigma\colon R^*_{m,m} \to GL(m,R)$ по правилу $\sigma(A) = \varphi_A^{-1} = \varphi_{A^{-1}}$ есть изоморфизм групп. Таким образом, если R — конечное кольцо, то $GL(m,R)$ — точное подстановочное представление степени $|R|^m$ группы $R^*_{m,m}$, имеющей порядок, значительно больший, чем $|R|^m$. В случае, если R — конечное поле из q элементов, вместо $GL(m,R)$ пишут $GL(m,q)$. По следствию утверждения 18 главы 7 $|GL(m,q)| = (q^m-1)(q^m-q)\dots(q^m-q^{m-1})$.

Пример 25. При обозначениях из примера 24 каждой матрице $A \in R^*_{m,m}$ и каждому вектору $b^{\downarrow} \in R^{(m)}$ поставим в соответствие преобразование $\psi_{A,b^{\downarrow}}\colon R^{(m)} \to R^{(m)}$, определяемое правилом

$$\forall\, x^{\downarrow} \in R^{(m)}:\ \psi_{A,b^{\downarrow}}(x^{\downarrow}) = Ax^{\downarrow} + b^{\downarrow}.$$

Тогда $\psi_{A,b^{\downarrow}}$ — подстановка на $R^{(m)}$, называемая *аффинной*, а множество

$$AGL(m,R) = \{\psi_{A,b^{\downarrow}}:\ A \in R^*_{m,m},\ b^{\downarrow} \in R^{(m)}\}$$

есть подгруппа в $S(R^{(m)})$, называемая *полной аффинной группой* размерности m над R. Если R — поле из q элементов, то вместо $AGL(m,R)$ пишут $AGL(m,q)$.

Как уже упоминалось, абстрактное понятие группы сформировалось в математике, в частности, и под воздействием геометрии. Здесь источник и область применения понятия группы можно проиллюстрировать следующим образом.

Пример 26. Пусть в трехмерном евклидовом пространстве D^3 помещен многогранник (или плоский многоугольник) M с n вершинами. Назовем *движением* (или инвариантным преобразованием) многогранника M любое его перемещение в пространстве, в результате которого он будет занимать ту же область, которую он занимал первоначально (два движения считаются равными, если они равны как отображения множества точек M в множество D^3).

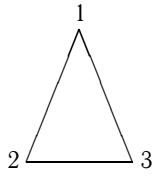
Пусть $D(M)$ — множество всех движений многогранника M. Перенумеруем точки пространства, в которых расположены его вершины, числами $1,2,\dots,n$. Тогда каждому движению $\varphi \in D(M)$ однозначно соответствует подстановка $\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$, где i_k — номер точки пространства, в которую в результате движения φ переместилась вершина из k-й точки, $k \in \overline{1,n}$. Так как M — «твердая» фигура, то указанной подстановкой однозначно определяется все движение φ. Поэтому в дальнейшем мы будем отождествлять движение φ с соответствующей ему подстановкой и писать $\varphi = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$. Таким образом, $D(M) \subset S_n$. Нетрудно заметить, что если к многограннику M применить сначала движение φ, а потом движение $\psi = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}$, то результатом выполнения этих двух движений будет также движение, которое описывается подстановкой $\varphi\psi = \begin{pmatrix} 1 & 2 & \dots & n \\ j_{i_1} & j_{i_2} & \dots & j_{i_n} \end{pmatrix}$. Следовательно, $D(M) < S_n$.

Определение 23. Группа $(D(M),\cdot)$ подстановок на множестве номеров вершин многогранника (многоугольника) M, соответствующих его движениям в трехмерном пространстве, называется *группой движений многогранника* M.

В этом определении мы, по сути дела, отождествили группу движений многогранника M с n вершинами и ее точное подстановочное представление степени n, описанное выше.

Геометрический смысл группы $D(M)$ состоит в том, что она — мера симметрии многогранника M: чем он симметричнее, тем больше его группа движений.

Пример 27. Если M — треугольник, все стороны которого имеют разные длины, то $D(M)=\{\varepsilon\}$ — единичная группа. Если M — равнобедренный треугольник,



то $D(M)=\{\varepsilon,\ \left(\begin{smallmatrix}1&2&3\\1&3&2\end{smallmatrix}\right)\}$ — группа порядка 2. Если M — равносторонний треугольник, то $D(M)=S_3$.

3. При изучении различных свойств групп подстановок весьма важными оказываются следующие результаты.

Определение 24. Для группы $G<S(\Omega)$ элементы $\alpha,\beta\in\Omega$ называют *G-эквивалентными* и пишут $\alpha\underset{G}{\sim}\beta$ (или просто $\alpha\sim\beta$), если $g(\alpha)=\beta$ для некоторого $g\in G$.

Теорема 23. *Пусть $G<S(\Omega)$. Тогда*

(а) *отношение $\underset{G}{\sim}$ на Ω есть отношение эквивалентности. Множество Ω разбивается на непересекающиеся классы G-эквивалентных элементов, называемые* областями транзитивности *группы G*;

(б) *подмножество $\Delta\subset\Omega$ есть область транзитивности группы G тогда и только тогда, когда*

1) $\forall\, g\in G\ (g(\Delta)\subset\Delta)$;

2) $\forall\,\alpha,\beta\in\Delta,\ \exists\, g\in G\ (g(\alpha)=\beta)$.

□ (а) Так как для любого $\alpha\in\Omega$ верно равенство $\varepsilon(\alpha)=\alpha$ и $\varepsilon\in G$, то $\alpha\sim\alpha$, т. е. отношение $\sim$ рефлексивно. Если $\alpha\sim\beta$, то $\beta=g(\alpha)$ для некоторого $g\in G$. Но тогда $\alpha=g^{-1}(\beta)$, $g^{-1}\in G$. Поэтому $\beta\sim\alpha$, т. е. отношение $\sim$ симметрично. Если $\alpha\sim\beta$, $\beta\sim\gamma$, то $\beta=g(\alpha)$, $\gamma=h(\beta)$ для подходящих $g,h\in G$. В таком случае $gh(\alpha)=h(g(\alpha))=\gamma$, $gh\in G$, и $\alpha\sim\gamma$, т. е. отношение $\sim$ транзитивно. Утверждение о разбиении множества Ω на области транзитивности теперь очевидно.

(б) Если Δ — область транзитивности G, $\alpha\in\Delta$ и $g\in G$, то $\alpha\sim g(\alpha)$, и потому $g(\alpha)\in\Delta$, т. е. $g(\Delta)\subseteq\Delta$, и верно утверждение 1). Утверждение 2) в этом случае очевидно.

Наоборот, если для $\Delta \subset \Omega$ выполнены утверждения 1) и 2), то ввиду утверждения 2) Δ есть подмножество некоторого класса G-эквивалентных элементов. Кроме того, если $\alpha \in \Delta$, $\beta \in \Omega$ и $\alpha \sim \beta$, то $\beta = g(\alpha)$ для некоторого $g \in G$ и ввиду утверждения 1) $\beta \in \Delta$, т. е. Δ — в точности класс G-эквивалентных элементов (область транзитивности группы G). □

Определение 25. Группа $G < S(\Omega)$ называется *транзитивной*, если Ω — ее область транзитивности, т. е.

$$\forall\, \alpha, \beta \in \Omega,\ \exists\, g \in G\ (g(\alpha) = \beta),$$

в противном случае, группа G называется *интранзитивной*.

Транзитивными группами являются, например, группа S_n, ее подгруппа

$$\left\langle \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \end{pmatrix} \right\rangle,$$

группа $AGL(m, R)$. Пример интранзитивной группы — $GL(m, R)$. В частности, группа $GL(m, q)$ имеет ровно две области транзитивности (докажите).

Очевидно, что группа $D(M)$ движений правильного многогранника M транзитивна, однако обратное утверждение неверно. Например, если M — плоский шестиугольник, у которого любые два несмежных ребра равны, то группа его движений в трехмерном пространстве транзитивна (покажите).

При изучении областей транзитивности группы подстановок полезно

Определение 26. *Орбитой* элемента $\alpha \in \Omega$ относительно группы $G < S(\Omega)$ называется множество

$$G(\alpha) = \{\beta \in \Omega :\ \beta = g(\alpha),\ g \in G\}.$$

Теорема 24. *Если Δ — область транзитивности группы $G < S(\Omega)$, то $\Delta = G(\alpha)$ для любого $\alpha \in \Delta$.*

□ Так как все элементы из $G(\alpha)$ G-эквивалентны α, то $G(\alpha) \subset \Delta$. Если $\beta \in \Delta$, то $\beta \underset{G}{\sim} \alpha$, т. е. $\beta = g(\alpha)$ для некоторого $g \in G$ и $\beta \in G(\alpha)$. □

Теперь можно вывести следующее важное соотношение между порядком группы подстановок и порядками ее областей транзитивности.

Определение 27. *Стабилизатором* элемента $\alpha \in \Omega$ в группе $G < S(\Omega)$ называется множество подстановок

$$G_\alpha = \{g \in G :\ g(\alpha) = \alpha\}.$$

Теорема 25 (лемма Бернсайда). *Стабилизатор любого элемента $\alpha \in \Omega$ в группе $G < S(\Omega)$ есть подгруппа в G, и $|G| = |G_\alpha| \cdot |G(\alpha)|$.*

□ Если $g, h \in G_\alpha$, то $(gh^{-1})(\alpha) = h^{-1}(g(\alpha)) = \alpha$, т. е. $gh^{-1} \in G_\alpha$, и $G_\alpha < G$. Заметим теперь, что для любых подстановок $x, y \in G$ справедливы соотношения

$$x \equiv y(G_\alpha)_\Pi \;\Leftrightarrow\; xy^{-1} \in G_\alpha \;\Leftrightarrow\; (xy^{-1})(\alpha) = \alpha \;\Leftrightarrow\; x(\alpha) = y(\alpha).$$

Следовательно, число различных элементов вида $x(\alpha)$, $x \in G$, равно числу правых смежных классов G по G_α, т. е.

$$|G(\alpha)| = |G : G_\alpha|.$$

Отсюда по теореме Лагранжа получаем утверждение теоремы 25. □

Следствие 1. *Если $|\Omega| = n$ и G — транзитивная группа подстановок на Ω, то $n \mid |G|$ и $|G| = n \cdot |G_\alpha|$ для любого $\alpha \in \Omega$.*

□ Для любого $\alpha \in \Omega$ верны равенства $G(\alpha) = \Omega$ и $|G(\alpha)| = n$. □

Следствие 2. *Если M — правильный многогранник (многоугольник) с n вершинами, в котором каждая вершина имеет k соседних вершин, то порядок его группы движений $D(M)$ равен nk.*

□ Воспользуемся терминологией и обозначениями из примера 26, и, для краткости, вершину многогранника, расположенную в точке пространства с номером α, будем называть просто вершиной α.

Зафиксируем некоторую вершину α многогранника M. Так как M — правильный многогранник, то по следствию 1 $|D(M)| = n \cdot |D(M)_\alpha|$. Остается подсчитать число движений многогранника M, оставляющих на месте α. Пусть $\alpha_1, \ldots, \alpha_k$ — все вершины, смежные с α. Очевидно, любое движение $\varphi \in D(M)_\alpha$ есть поворот вокруг оси симметрии, проходящей через точку α, и φ однозначно задается указанием образа $\varphi(\alpha_1)$ элемента α_1. Более того, если $\varphi \in D(M)_\alpha$, то вершина $\varphi(\alpha_1) \in \{\alpha_1, \ldots, \alpha_k\}$, так как $\varphi(\alpha_1)$ остается смежной вершиной для α. Наконец, для любой смежной с α вершины α_i существует движение $\varphi \in D(M)_\alpha$ такое, что $\varphi(\alpha_1) = \alpha_i$. Таким образом, $|D(M)_\alpha| = k$, и потому $|D(M)| = nk$. □

Определение 28. Группа движений правильного плоского n-угольника называется *группой диэдра степени n* и обозначается через D_n.

Из следствия 2 леммы Бернсайда имеем $|D_n| = 2n$. В частности, $|D_3| = 6$, и потому $D_3 = S_3$, $|D_4| = 8$, и D_4 — пример некоммутативной группы порядка p^3 (сравните с теоремой 21).

§ 8. ЦИКЛОВАЯ СТРУКТУРА И ЧЕТНОСТЬ ПОДСТАНОВКИ. ЗНАКОПЕРЕМЕННАЯ ГРУППА

1. Всюду далее Ω — произвольное множество мощности n. В теории групп подстановок большое количество результатов основывается на следующем способе представления подстановки в виде произведения подстановок более простого вида.

Определение 29. Элемент $\alpha \in \Omega$ назовем *мобильным элементом подстановки* $g \in S(\Omega)$, если $g(\alpha) \neq \alpha$, и *неподвижным* — в противном случае. Множество мобильных элементов подстановки g обозначим через $\operatorname{mob} g$: $\operatorname{mob} g = \{\alpha \in \Omega : g(\alpha) \neq \alpha\}$. Подстановки $g, h \in S(\Omega)$ назовем *независимыми*, если $\operatorname{mob} g \cap \operatorname{mob} h = \varnothing$.

Например, в S_5 подстановки $g = \begin{pmatrix} 1&2&3&4&5 \\ 3&2&1&4&5 \end{pmatrix}$ и $h = \begin{pmatrix} 1&2&3&4&5 \\ 1&4&3&2&5 \end{pmatrix}$ независимы. Тождественная подстановка ε независима с любой подстановкой из $S(\Omega)$. Очевидны следующие свойства множества мобильных элементов подстановки:

$$\alpha \in \operatorname{mob} g \;\Leftrightarrow\; g(\alpha) \in \operatorname{mob} g, \quad \operatorname{mob} g^{-1} = \operatorname{mob} g, \quad \operatorname{mob} g = \varnothing \;\Leftrightarrow\; g = \varepsilon.$$

Доказательство перечисляемых ниже простейших свойств независимых подстановок предоставляется читателю.

Утверждение 26. *Если g, h — независимые подстановки из $S(\Omega)$, то*
(а) *для любых $\alpha \in \operatorname{mob} g$, $\beta \in \operatorname{mob} h$ верны равенства*

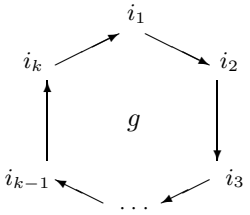
$$(gh)(\alpha) = g(\alpha), \quad (gh)(\beta) = h(\beta);$$

(б) $\operatorname{mob} gh = \operatorname{mob} g \cup \operatorname{mob} h$;
(в) $gh = hg$;
(г) $gh = \varepsilon \;\Leftrightarrow\; g = h = \varepsilon$;
(д) $g = h \;\Leftrightarrow\; g = h = \varepsilon$;
(е) *для любых $s, t \in \mathbb{Z}$ подстановки g^s, h^t независимы*;
(ж) $\operatorname{ord} gh = [\operatorname{ord} g, \operatorname{ord} h]$.

Определение 30. Подстановку $g \in S_n$ называют *циклом*, если $g \neq \varepsilon$ и существует перестановка $(i_1, \ldots, i_n)$ элементов множества Ω такая, что g имеет вид

$$g = \begin{pmatrix} i_1 & i_2 & \ldots & i_{k-1} & i_k & i_{k+1} & \ldots & i_n \\ i_2 & i_3 & \ldots & i_k & i_1 & i_{k+1} & \ldots & i_n \end{pmatrix}, \tag{11}$$

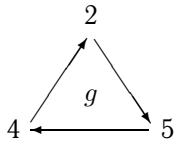
т. е. мобильные элементы подстановки g переставляются ею «по циклу»:



При этом число $k = |\operatorname{mob} g|$ называется *длиной цикла* g.

Например, подстановка $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 2 & 4 \end{pmatrix}$ является циклом длины 3, так как, упорядочив элементы $1, 2, \ldots, 5$ следующим образом: $2, 5, 4, 1, 3$, получаем

$$g = \begin{pmatrix} 2 & 5 & 4 & 1 & 3 \\ 5 & 4 & 2 & 1 & 3 \end{pmatrix}$$



Вместо записи (11) для цикла g употребляют значительно более компактную формальную запись:

$$g = (i_1, i_2, \ldots, i_k). \tag{12}$$

Отметим, что из (12) нельзя однозначно определить степень подстановки g и, в случае необходимости, эту степень нужно указывать отдельно.

Полезно иметь ввиду, что цикл g длины k может быть записан ровно k различными способами в форме (12):

$$\begin{aligned} g &= (i_1, i_2, \ldots, i_{k-1}, i_k) = (i_2, i_3, \ldots, i_k, i_1) = \\ &= (i_3, i_4, \ldots, i_k, i_1, i_2) = \ldots = (i_k, i_1, \ldots, i_{k-1}). \end{aligned} \tag{13}$$

Теорема 27. *Произвольная неединичная подстановка $g \in S(\Omega)$ либо является циклом, либо раскладывается в произведение некоторого числа попарно независимых циклов. Такое разложение однозначно с точностью до перестановки сомножителей.*

□ Существование нужного разложения для g доказывается индукцией по параметру $m = |\operatorname{mob} g|$. Если $m = 2$, т. е. $\operatorname{mob} g = \{\alpha_1, \alpha_2\}$, то очевидно, что $g = (\alpha_1, \alpha_2)$ — цикл длины 2. Пусть $s > 2$ и первое утверждение теоремы верно для всех $g \in S(\Omega)$ таких, что $2 \leqslant m < s$. Предположим, что $m = s$.

Выберем элемент $\alpha \in \operatorname{mob} g$ и рассмотрим последовательность элементов

$$\alpha \xrightarrow{g} g(\alpha) \xrightarrow{g} \ldots \xrightarrow{g} g^i(\alpha) \xrightarrow{g} \ldots \ . \tag{14}$$

Так как все элементы этой последовательности принадлежат Ω, то в ней есть лишь конечное число различных элементов, и можно утверждать, что для некоторого $k \in \overline{1, n}$ элементы $\alpha, g(\alpha), \ldots, g^{k-1}(\alpha)$ различны, а $g^k(\alpha)$ совпадает с одним из них. При этом $k > 1$, так как $g(\alpha) \neq \alpha$. Покажем, что $g^k(\alpha) = \alpha$. Если это не так, т. е. $g^k(\alpha) = g^l(\alpha)$, где $k > l > 0$, то, применяя к обеим частям последнего равенства подстановку g^{-1}, получаем $g^{k-1}(\alpha) = g^{l-1}(\alpha)$, $k - 1 > l - 1 \geqslant 0$. Это противоречит выбору параметра k. Следовательно, $g^k(\alpha) = \alpha$, и последовательность элементов (14) имеет вид

$$\alpha \xrightarrow{g} g(\alpha) \xrightarrow{g} \ldots \xrightarrow{g} g^{k-1}(\alpha) \xrightarrow{g} \alpha \xrightarrow{g} g(\alpha) \xrightarrow{g} \ldots \ .$$

Отсюда следует, что элементы множества $\Delta_1 = \{\alpha, g(\alpha), \ldots, g^{k-1}(\alpha)\}$ преобразуются подстановкой g точно так же, как и циклом

$$h_1 = (\alpha, g(\alpha), \ldots, g^{k-1}(\alpha)).$$

Следовательно, все эти элементы неподвижны относительно подстановки $g_1 = h_1^{-1}g$, причем $\operatorname{mob} g_1 = \operatorname{mob} g \setminus \Delta_1$. Если $\operatorname{mob} g_1 = \varnothing$, то $g_1 = \varepsilon$ и $g = h_1$ — цикл. Если $\operatorname{mob} g_1 \neq \varnothing$, то $|\operatorname{mob} g_1| = m - k < s$ и по предположению индукции подстановка g_1 или является циклом h_2, или раскладывается в произведение попарно независимых нееединичных циклов: $g_1 = h_2 \dots h_t$. В таком случае подстановка g следующим образом раскладывается в произведение циклов:

$$g = h_1 h_2 \dots h_t. \tag{15}$$

При $t > 1$ циклы в этом разложении попарно независимы, так как по утверждению 26(б)

$$\operatorname{mob} h_i \subset \operatorname{mob} g_1, \quad i \in \overline{2,t},$$

а поскольку $\operatorname{mob} h_1 = \Delta_1$ и $\Delta_1 \cap \operatorname{mob} g_1 = \varnothing$, то $\operatorname{mob} h_1 \cap \operatorname{mob} h_i = \varnothing$ для $i \in \overline{2,t}$. Первое утверждение теоремы доказано.

Допустим теперь, что, наряду с разложением (15), подстановка g имеет еще одно разложение:

$$g = f_1 \dots f_s, \tag{16}$$

в котором либо $s = 1$ и $g = f_1$ — цикл, либо $s > 1$ и $f_1, \dots, f_s$ — попарно независимые циклы. Выберем элемент $\alpha \in \operatorname{mob} h_1$. По утверждению 26(б) $\alpha \in \operatorname{mob} g$ и $\alpha \in \operatorname{mob} f_i$ для некоторого $i \in \overline{1,s}$. Переставив, если надо, сомножители в разложении (16) (это можно сделать по утверждению 26(в)), считаем, что $\alpha \in \operatorname{mob} f_1$. Таким образом, $\alpha \in \operatorname{mob} h_1 \cap \operatorname{mob} f_1$. Покажем, что $h_1 = f_1$. В силу утверждения 26(а) справедливы равенства

$$h_1(\alpha) = g(\alpha) = f_1(\alpha).$$

Но тогда опять верны включения

$$g(\alpha) = h_1(\alpha) \in \operatorname{mob} h_1 \cap \operatorname{mob} f_1,$$

и, применяя то же утверждение, получаем цепочку равенств:

$$h_1^2(\alpha) = h_1(g(\alpha)) = g(g(\alpha)) = f_1(g(\alpha)) = f_1^2(\alpha).$$

Продолжая аналогично далее, получаем:

$$h_1^i(\alpha) = f_1^i(\alpha) \text{ для всех } i \in \mathbb{N}. \tag{17}$$

Так как $h_1 = (\alpha, h_1(\alpha), \dots, h_1^{k-1}(\alpha))$ и $f_1 = (\alpha, f_1(\alpha), \dots, f_1^{l-1}(\alpha))$ для некоторых $k, l \in \mathbb{N}$, то из (17) следует, что $k = l$, поскольку

$$h_1^i(\alpha) = \alpha \;\Leftrightarrow\; f_1^i(\alpha) = \alpha,$$

и мы приходим к равенству $h_1 = f_1$. Отсюда видно, что если в (15) $t = 1$, то в (16) $s = 1$, так как иначе выполнялось бы равенство $\varepsilon = f_2 \dots f_s$, которое, по утверждению 26(г), невозможно, ввиду попарной независимости нееединичных подстановок $f_2, \dots, f_s$. Если же $t > 1$, то и $s > 1$, и справедливо равенство $h_2 \dots h_t = f_2 \dots f_s$. Теперь доказательство совпадения разложений (15) и (16) легко завершить индукцией по $s + t$, приняв за первый шаг индукции случай, когда $s + t = 2$, т. е. $s = t = 1$. $\square$

В качестве примера приведем разложение:

$$\begin{pmatrix} 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9 \\ 1\ 5\ 9\ 8\ 6\ 2\ 4\ 7\ 3\ 0 \end{pmatrix} = (0,1,5,2,9)\cdot(3,8)\cdot(4,6). \tag{18}$$

Допустим, что разложение подстановки $g \in S(\Omega)$ в произведение попарно независимых циклов имеет вид

$$g = (\alpha_1,\ldots,\alpha_k)\cdot(\beta_1,\ldots,\beta_l)\cdot\ldots\cdot(\gamma_1,\ldots,\gamma_t), \tag{19}$$

и $\delta_1,\ldots,\delta_r$ — все неподвижные элементы относительно подстановки g. Для того чтобы подчеркнуть, что подстановка g действует и на этих элементах, не указанных в разложении (19), их называют *единичными циклами* подстановки g, и подстановку g записывают в виде

$$g = (\alpha_1,\ldots,\alpha_k)\cdot(\beta_1,\ldots,\beta_l)\cdot\ldots\cdot(\gamma_1,\ldots,\gamma_t)\cdot(\delta_1)\cdot\ldots\cdot(\delta_r). \tag{20}$$

Определение 31. Представление подстановки $g \in S(\Omega)$ в виде (19) или (20) называют ее *разложением на независимые циклы*.

Например, подстановка (18) раскладывается на независимые циклы следующим образом:

$$\begin{pmatrix} 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9 \\ 1\ 5\ 9\ 8\ 6\ 2\ 4\ 7\ 3\ 0 \end{pmatrix} = (0,1,5,2,9)\cdot(3,8)\cdot(4,6)\cdot(7).$$

Согласно теореме 27 разложение (20) для подстановки g однозначно, с точностью до перестановки сомножителей, и потому корректно.

Определение 32. *Цикловой структурой подстановки* g называется таблица

$$[g] = [l_1^{k_1},\, l_2^{k_2},\, \ldots,\, l_m^{k_m}],$$

указывающая, что разложение подстановки g в виде (20) в произведение независимых циклов (включая единичные) состоит из k_1 циклов длины l_1, k_2 циклов длины $l_2,\ldots,k_m$ циклов длины l_m.

Например, цикловая структура подстановки (18) есть $[1^1, 2^2, 5^1]$.

Для любой подстановки $g \in S(\Omega)$ по ее цикловой структуре легко вычислить ее порядок.

Теорема 28. *Порядок цикла равен его длине. Порядок произвольной подстановки $g \in S(\Omega)$ равен наименьшему общему кратному длин циклов в ее разложении на независимые циклы.*

□ Если $g = (\alpha_0, \alpha_1, \ldots, \alpha_{k-1})$ — цикл длины k, то для $i \in \overline{0, k-1}$ справедливы соотношения $g(\alpha_i) = \alpha_{i\oplus 1}$, где $\oplus$ — сложение в $\mathbb{Z}_k$. Отсюда индукцией легко получить, что для любых $i \in \overline{0, k-1}$ и $m \in \mathbb{N}$ верно соотношение

$$g^m(\alpha_i) = \alpha_{i\oplus r_k(m)} = \alpha_{r_k(i+m)},$$

где $r_k(m)$ — остаток от деления m на k. Теперь очевидно, что

$$(g^m = \varepsilon) \;\Leftrightarrow\; (r_k(m) = 0),$$

т. е. $\operatorname{ord} g = k$.

Если разложение g в произведение попарно независимых циклов имеет вид (15), где $t > 1$, то, ввиду попарной перестановочности циклов $h_1, \ldots, h_t$ (утверждение 26(в)), для любого $s \in \mathbb{N}$ верно равенство $g^s = h_1^s \cdot \ldots \cdot h_t^s$. Так как по утверждению 26(е) подстановки h_1^s, ..., h_t^s попарно независимы, то по утверждению 26(г)

$$(g^s = \varepsilon) \;\Leftrightarrow\; (h_1^s = \ldots = h_t^s = \varepsilon).$$

Теперь очевидно, что $\operatorname{ord} g = [\operatorname{ord} h_1, \ldots, \operatorname{ord} h_t]$. □

Например, порядок подстановки (18) равен $[5, 2, 2] = 10$.

2. Другой способ представления подстановок в виде произведения циклов (возможно зависимых) тесно связан со следующей классификацией подстановок, которую мы, для простоты изложения, введем сначала в S_n.

Определение 33. Подстановку $g = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix} \in S_n$ называют *четной*, если перестановка $(i_1, i_2, \ldots, i_n)$ четная, и *нечетной* в противном случае.

Определение 34. *Транспозицией* в S_n называют любой цикл длины 2.

Лемма 29. *Если $g, h \in S_n$ и h — транспозиция, то четности подстановок g и gh противоположны.*

□ Пусть $g = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$ и $h = (i_k, i_l)$, $k < l$. Тогда

$$gh = \begin{pmatrix} 1 & \ldots & k & \ldots & l & \ldots & n \\ i_1 & \ldots & i_k & \ldots & i_l & \ldots & i_n \end{pmatrix} \begin{pmatrix} 1 & \ldots & i_k & \ldots & i_l & \ldots & n \\ 1 & \ldots & i_l & \ldots & i_k & \ldots & n \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & \ldots & k{-}1 & k & k{+}1 & \ldots & l{-}1 & l & l{+}1 & \ldots & n \\ i_l & \ldots & i_{k-1} & i_l & i_{k+1} & \ldots & i_{l-1} & i_k & i_{l+1} & \ldots & n \end{pmatrix}.$$

Остается заметить, что перестановки

$$(i_1 \ldots i_k \ldots i_l \ldots i_n) \quad \text{и} \quad (i_1 \ldots i_{k-1}\, i_l\, i_{k+1} \ldots i_l\, i_k\, i_{l+1} \ldots i_n)$$

различаются транспозицией и их четности противоположны. □

Теорема 30. *Всякая подстановка $g \in S_n$ раскладывается в произведение транспозиций, причем в любом таком разложении число сомножителей четно, если подстановка g четна, и нечетно в противном случае.*

□ Если $g = \varepsilon$, то $g = (1,2)\cdot(1,2)$. Если $g = (a_1, \ldots, a_k)$ — цикл, то

$$g = (a_1, \ldots, a_k) = (a_1, a_2)\cdot(a_1, a_3)\cdot \ldots \cdot (a_1, a_k). \tag{21}$$

Теперь первая часть теоремы следует из теоремы 27. Пусть подстановка $g \in S_n$ и $g = t_1 t_2 \ldots t_s$ — произведение s транспозиций. Тогда $g = \varepsilon \cdot t_1 t_2 \ldots t_s$, т. е. g получается из четной подстановки ε s-кратным умножением на транспозиции. Отсюда, применяя лемму 29, получаем: g — четная подстановка тогда и только тогда, когда число s четно. □

Следствие 1. *Цикл длины k является четной подстановкой тогда и только тогда, когда число k нечетно.*

□ См. (21). □

Следствие 2 (теорема о декременте). *Если подстановка $g \in S_n$ каким-либо способом представлена в виде произведения m циклов длин $l_1, \ldots, l_m$, то она четна тогда и только тогда, когда число $l_1 + \ldots + l_m - m$ четно.*

□ Цикл длины l_i раскладывается в произведение $l_i - 1$ транспозиций (см. (21)), поэтому g раскладывается в произведение $l_1 + \ldots + l_m - m$ транспозиций. □

Если в условиях следствия 2 циклы попарно независимы, то число $d(g)$, равное $d(g) = l_1 + \ldots + l_m - m$, называют *декрементом* подстановки g.

Следствие 3. *Множество A_n всех четных подстановок из S_n образует подгруппу группы S_n индекса 2.*

□ Если $g, h \in A_n$, то по теореме каждая из подстановок g, h есть произведение четного числа транспозиций. Тогда и gh — произведение четного числа транспозиций, т. е. по теореме $gh \in A_n$. Отсюда по следствию 1 утверждения 6 получаем: $A_n < S_n$. Заметим, что $S_n \setminus A_n = A_n \cdot (1,2)$, так как $A_n \cdot (1,2) \subset S_n \setminus A_n$ и $(S_n \setminus A_n)\cdot(1,2) \subset A_n$. Следовательно, $S_n = A_n \cup A_n \cdot (1,2)$ и $|S_n : A_n| = 2$. □

Определение 35. Подгруппу A_n всех четных подстановок группы S_n называют *знакопеременной группой* степени n.

Знакопеременная группа играет в теории групп подстановок, и вообще в теории групп, роль не менее важную, чем сама симметрическая группа. Она очень часто встречается в приложениях.

Пример 28. Если M — тетраэдр, то $D(M) = A_4$. Действительно, $D(M) < S_4$ и по следствию 2 теоремы 25 $|D(M)| = 12 = |A_4|$. Остается заметить, что $A_4 \subset D(M)$, так как $A_4 \setminus \{\varepsilon\}$ состоит из подстановок вида $g = (a,b)(c,d)$ и $h = (\alpha, \beta, \gamma)$: подстановка g осуществляет вращение тетраэдра вокруг оси симметрии, проходящих через середины противоположных ребер $\overline{ab}$ и $\overline{cd}$, а подстановка h — вращение вокруг оси симметрии, проходящей через вершину.

Теперь можно показать, что обращение теоремы Лагранжа для конечных групп неверно.

Пример 29. В группе A_4 (имеющей порядок 12) нет подгруппы порядка 6. Из теоремы о декременте и теоремы 28 следует, что любой элемент из $A_4 \setminus \{\varepsilon\}$ имеет порядок 2 или 3. Если $G < A_4$ и $|G| = 6$, то $|G \setminus \{\varepsilon\}| = 5$. Множество $G \setminus \{\varepsilon\}$ не может состоять только из элементов порядка 2, так как A_4 содержит всего три таких элемента, и не может состоять только из элементов порядка 3, так как их количество в любой конечной группе четно (докажите). Следовательно, в G есть подстановки вида $g = (a, b)(c, d)$, $\{a, b\} \cap \{c, d\} = \varnothing$, и $h = (\alpha, \beta, \gamma)$. Остается заметить, что $\langle g, h\rangle = A_4$ (докажите).

Замечание 7. Если Ω — произвольное конечное множество, то для подстановок из $S(\Omega)$ также можно ввести понятие четности и получить результаты, аналогичные теореме 30 и ее следствиям. Упорядочим каким-либо образом элементы множества Ω: $\Omega = \{\alpha_1, \ldots, \alpha_n\}$. Тогда каждой подстановке $g \in S(\Omega)$ соответствует единственная перестановка $(i_1, \ldots, i_n) \in P(\overline{1, n})$ такая, что $g = \begin{pmatrix} \alpha_1 & \ldots & \alpha_n \\ \alpha_{i_1} & \ldots & \alpha_{i_n} \end{pmatrix}$. Подстановка g называется *четной*, если $(i_1, \ldots, i_n)$ — четная перестановка, и *нечетной* в противном случае. При таком определении для подстановок из $S(\Omega)$ практически так же, как и для подстановок из S_n, доказывается лемма 29, и дословно так же — теорема 30 и ее следствия. Из теоремы 30 следует, что четность подстановки $g \in S(\Omega)$ определяется лишь четностью числа транспозиций в ее разложении и не зависит от способа первоначального упорядочения множества Ω. Подгруппа всех четных подстановок из $S(\Omega)$ обозначается через $A(\Omega)$ и называется *знакопеременной группой подстановок* множества Ω.

§ 9. СИСТЕМЫ ОБРАЗУЮЩИХ СИММЕТРИЧЕСКОЙ И ЗНАКОПЕРЕМЕННОЙ ГРУПП

Для упрощения обозначений мы будем рассматривать лишь группы S_n и A_n. Предварительно докажем вспомогательное утверждение, позволяющее по заданному разложению на независимые циклы подстановки $g \in S_n$ быстро вычислять такое же разложение для любой подстановки $f^{-1}gf$, где $f \in S_n$.

Лемма 31. *Пусть подстановка g представлена в виде произведения циклов*:

$$g = (a_1, a_2, \ldots, a_k) \cdot (b_1, b_2, \ldots, b_l) \cdot \ldots \cdot (c_1, c_2, \ldots, c_m). \tag{22}$$

Тогда верно равенство

$$f^{-1}gf = (f(a_1),\, f(a_2),\, \ldots,\, f(a_k)) \cdot (f(b_1),\, \ldots,\, f(b_l)) \cdot \ldots \\ \ldots \cdot (f(c_1),\, \ldots,\, f(c_m)). \tag{23}$$

□ Пусть $\alpha \in \overline{1, n}$ и $\beta = g(\alpha)$. Тогда

$$f(\beta) = f(g(\alpha)) = f(g(f^{-1}(f(\alpha)))) = (f^{-1}gf)(f(\alpha)).$$

Таким образом, подстановка g переводит α в β тогда и только тогда, когда подстановка $f^{-1}gf$ переводит $f(\alpha)$ в $f(\beta)$. В частности, отсюда следует, что

$$\operatorname{mob}(f^{-1}gf) = f(\operatorname{mob} g),$$

и если $g = (a_1, \ldots, a_k)$ — цикл, то $f^{-1}gf = (f(a_1), \ldots, f(a_k))$. Теперь (23) следует из (22) ввиду равенства

$$f^{-1}gf = f^{-1}(a_1, \ldots, a_k)f \cdot f^{-1}(b_1, \ldots, b_l)f \cdot \ldots \cdot f^{-1}(c_1, \ldots, c_m)f. \quad \square$$

Отметим, что в условии леммы 31 не требуется, чтобы циклы в разложении (22) были независимы. Но, разумеется, если в (22) циклы независимы, то они независимы и в (23).

Большие возможности для упражнений в применении леммы 31 дает читателю доказательство следующей теоремы.

Теорема 32. *Группа S_n порождается*:

1) *множеством всех транспозиций*;
2) *множеством всех транспозиций вида* $(1, \alpha)$, $\alpha \in \overline{2, n}$;
3) *множеством всех транспозиций вида* $(\alpha, \alpha + 1)$, $\alpha \in \overline{1, n-1}$;
4) *транспозицией* $(1, 2)$ *и полным циклом* $(1, 2, \ldots, n)$.

$\square$ Для $i \in \overline{1, 4}$ обозначим через H_i подгруппу в S_n, порожденную множеством подстановок, описанном в пункте i) теоремы. Наша задача — доказать равенства $H_i = S_n$, $i \in \overline{1, 4}$. Мы сделаем это, доказав цепочку соотношений $S_n = H_1 \subset H_2 \subset \subset H_3 \subset H_4$.

По теореме 30 каждая подстановка из S_n раскладывается в произведение транспозиций, т. е. принадлежит H_1. Следовательно $H_1 = S_n$.

Подгруппа $H_2 = \langle (1, 2), (1, 3), \ldots, (1, n) \rangle$ из S_n содержит любую транспозицию $(\alpha, \beta) \in S_n$. Действительно, если $\alpha = 1$ или $\beta = 1$, то включение $(\alpha, \beta) \in H_2$ вытекает непосредственно из определения H_2, а если $\alpha \neq 1$ и $\beta \neq 1$, то $(1, \alpha), (1, \beta) \in H_2$ и $(\alpha, \beta) = (1, \alpha)(1, \beta)(1, \alpha) \in H_2$. Следовательно, $H_1 \subset H_2$.

Подгруппа $H_3 = \langle (1, 2), (2, 3), \ldots, (n-1, n) \rangle$ содержит все транспозиции $(1, \alpha)$, так как $(1, 2) \in H_3$ и если $(1, \alpha - 1) \in H_3$, то $(1, \alpha) = (\alpha, \alpha - 1)(1, \alpha - 1)(\alpha - 1, \alpha) \in H_3$. Следовательно, $H_2 \subset H_3$.

Наконец, подгруппа H_4 содержит все транспозиции $(\alpha, \alpha+1)$, так как $(\alpha, \alpha+1) = = (1, 2, \ldots, n)^{-\alpha}(1, 2)(1, 2, \ldots, n)^{\alpha} \in H_4$. Следовательно, $H_3 \subset H_4$. $\square$

В § 3 были описаны, с точностью до изоморфизма, все конечные группы с одним образующим. В связи с этим возникает естественное желание получать дальнейшие классификационные результаты в теории конечных групп, описывая все группы с r образующими для $r = 2, 3, \ldots$. Однако теперь можно отметить, что уже в случае $r = 2$ эта задача будет мало отличаться от задачи классификации всех конечных групп, поскольку справедливо

Следствие. *Любая конечная группа изоморфна подгруппе группы с двумя образующими.*

□ Достаточно использовать теорему Кэли и утверждение 4) теоремы 32. □

Теорема 33. *Знакопеременная группа A_n степени $n \geqslant 3$ порождается всеми циклами длины* 3.

□ По следствию 1 теоремы 30 все циклы длины 3 из S_n принадлежат A_n. С другой стороны, любая подстановка $h \in A_n$ представляется по теореме 30 в виде произведения четного числа транспозиций:

$$h = t_1 \cdot t_2 \cdot \ldots \cdot t_{2k-1} \cdot t_{2k}.$$

Теперь достаточно доказать, что любое произведение $(\alpha, \beta)(\gamma, \delta)$ двух транспозиций представляется в виде произведения циклов длины 3. Для этого рассмотрим все возможные соотношения между множествами $\{\alpha, \beta\}$ и $\{\gamma, \delta\}$.

Если $\{\alpha, \beta\} = \{\gamma, \delta\}$, то $(\alpha, \beta)(\gamma, \delta) = \varepsilon = (1, 2, 3)^3$.

Если $\{\alpha, \beta\} \cap \{\gamma, \delta\} = \{\alpha\}$, то можно считать, что $\gamma = \alpha$, и тогда выполняются равенства $(\alpha, \beta)(\gamma, \delta) = (\alpha, \beta)(\alpha, \delta) = (\alpha, \beta, \delta)$.

Если $\{\alpha, \beta\} \cap \{\gamma, \delta\} = \varnothing$, то $(\alpha, \beta)(\gamma, \delta) = (\beta, \alpha, \gamma)(\gamma, \beta, \delta)$. □

Отметим, что в системе образующих группы A_n, указанной в теореме 33, есть много «лишних» элементов. Читателю предлагается самостоятельно доказать, что верно равенство

$$A_n = \langle (1, 2, 3),\ (1, 2, 4),\ \ldots,\ (1, 2, n) \rangle.$$

В частности, если M — тетраэдр, то вместо $D(M) = \langle (1, 2, 3),\ (1, 2, 4), (1, 3, 4) \rangle$ (см. пример 28) можно написать $D(M) = \langle (1, 2, 3),\ (1, 2, 4) \rangle$.

§ 10. СОПРЯЖЕННЫЕ ЭЛЕМЕНТЫ В СИММЕТРИЧЕСКОЙ ГРУППЕ. УРАВНЕНИЕ КОШИ

Цикловая форма записи подстановок позволяет описать классы сопряженных элементов в группе S_n и предложить методику решения уравнений вида

$$x^{-1} g x = h \tag{24}$$

в этой группе, называемого *уравнением Коши*. Заметим, что по определению 18 сопряженность подстановок $g, h \in S_n$ в группе S_n равносильна разрешимости уравнения (24).

Теорема 34. *Подстановки $g, h \in S_n$ сопряжены в S_n тогда и только тогда, когда они имеют одинаковую цикловую структуру.*

□ Допустим, что разложение подстановки g на независимые циклы, включая единичные циклы, имеет вид

$$g = (a_1, \ldots, a_k) \cdot (b_1, \ldots, b_l) \cdot \ldots \cdot (c_1, \ldots, c_m), \quad k + l + \ldots + m = n. \tag{25}$$

Тогда если h — подстановка, сопряженная с g, и f есть решение уравнения (24), то по лемме 31 справедливо равенство

$$h = (f(a_1),\ \ldots,\ f(a_k)) \cdot (f(b_1),\ \ldots,\ f(b_l)) \cdot \ldots \cdot (f(c_1),\ \ldots,\ f(c_m)), \tag{26}$$

представляющее собой разложение подстановки h также на независимые циклы. Таким образом, подстановка h имеет ту же цикловую структуру, что и g.

Наоборот, допустим, что h — произвольная подстановка с той же цикловой структурой, что и g. Тогда для подходящей перестановки

$$(\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_l, \ldots, \gamma_1, \ldots, \gamma_m)$$

множества $\overline{1,n}$ разложение h на независимые циклы имеет вид

$$h = (\alpha_1, \ldots, \alpha_k) \cdot (\beta_1, \ldots, \beta_l) \cdot \ldots \cdot (\gamma_1, \ldots, \gamma_m). \tag{27}$$

Пользуясь разложениями (25) и (27), составим подстановку

$$f = \begin{pmatrix} a_1 & \ldots & a_k & b_1 & \ldots & b_l & \ldots & c_1 & \ldots & c_m \\ \alpha_1 & \ldots & \alpha_k & \beta_1 & \ldots & \beta_l & \ldots & \gamma_1 & \ldots & \gamma_m \end{pmatrix}. \tag{28}$$

Ввиду леммы 31 очевидно, что f — решение уравнения (24), т. е. подстановки g и h сопряжены. □

Помимо критерия разрешимости уравнения (24) теорема 34 дает способ построения его решения в виде (28). Более того, эта теорема дает способ описания всех решений уравнения (24). Действительно, сравним разложение (26) подстановки h на независимые циклы, построенное по произвольному решению f уравнения (24), и произвольное разложение (27) подстановки h на независимые циклы при том же упорядочении длин циклов, что и в разложении подстановки g. Видно, что каждая запись (26) совпадает с некоторой записью (27) и, значит, любое решение f уравнения (24) может быть представлено в виде (28) при подходящем выборе записи h в виде (27). При этом очевидно, что запись (25) подстановки g можно зафиксировать. Таким образом, нами доказано

Следствие 1. *Пусть разложение подстановки g на независимые циклы имеет вид* (25)*, где $k \geqslant l \geqslant \ldots \geqslant m$, и h — подстановка из S_n с той же цикловой структурой, что и g. Тогда множество всех решений уравнения* (24) *есть множество всех подстановок вида* (28)*, соответствующих различным способам* (27) *разложения подстановки h на независимые циклы длин $k \geqslant l \geqslant \ldots \geqslant m$.*

Рассмотрим один наглядный и важный с теоретической точки зрения пример. Пусть

$$g = h = (a_0, a_1, \ldots, a_{n-1})$$

— *полный цикл* из S_n. Тогда множество решений уравнения (24) есть $N_{S_n}(g)$ — нормализатор элемента g в группе S_n, и по следствию 1 $N_{S_n}(g)$ есть множество подстановок вида

$$f = \begin{pmatrix} a_0 & a_1 & \ldots & a_{n-i-1} & a_{n-i} & \ldots & a_{n-1} \\ a_i & a_{i+1} & \ldots & a_{n-1} & a_0 & \ldots & a_{i-1} \end{pmatrix}, \quad i \in \overline{0,\, n-1}.$$

Выписанная подстановка f есть ни что иное, как g^i. Таким образом, число решений уравнения (24) в рассматриваемом случае равно n, и нами доказано

Следствие 2. *Если g — полный цикл из S_n, то $N_{S_n}(g) = \langle g \rangle$.*

Если подстановка g распадается на несколько независимых циклов, число решений уравнения (24) в случае его совместности может значительно превысить n.

Пример 30. Если $g = (a,b)(c,d)$, $h = (\alpha,\beta)(\gamma,\delta)$ — подстановки из S_4, то число решений уравнения (24) равно 8, и множество его решений f описывается следующей таблицей:

Верхняя строка подстановки f	a	b	c	d
Варианты нижних строк подстановки f	α	β	γ	δ
	β	α	γ	δ
	α	β	δ	γ
	β	α	δ	γ
	γ	δ	α	β
	δ	γ	α	β
	γ	δ	β	α
	δ	γ	β	α

В общем случае решения уравнения (24) и их число описывает

Теорема 35. *Пусть g — подстановка из S_n с цикловой структурой*

$$[g] = [l_1^{k_1}, l_2^{k_2}, \ldots, l_r^{k_r}]. \tag{29}$$

Тогда справедливы следующие утверждения:

(а) *группа $N_{S_n}(g)$ имеет порядок*

$$|N_{S_n}(g)| = \prod_{i=1}^{r} (k_i)! \cdot l_i^{k_i}; \tag{30}$$

(б) *если h — подстановка с той же цикловой структурой* (29) *и f — произвольное решение уравнения* (24)*, то множество всех решений уравнения* (24) *есть правый смежный класс $N_{S_n}(g) \cdot f$ и его мощность описывается формулой* (30).

□ (а) Как уже отмечалось, $N_{S_n}(g)$ есть множество всех решений уравнения

$$x^{-1}gx = g, \tag{31}$$

которое может быть построено по правилу, описанному следствием 1 теоремы 34. Для подсчета мощности этого множества введем рабочий термин: *нормальная запись подстановки*. Так мы будем называть разложение подстановки g на независимые циклы вида

$$g = g_1 g_2 \ldots g_s; \quad g_i = (a_1^{(i)}, \ldots, a_{m_i}^{(i)}), \quad i \in \overline{1,s}, \quad m_1 \geqslant m_2 \geqslant \ldots \geqslant m_s \geqslant 1. \tag{32}$$

В этой терминологии для описания всех решений уравнения (31) нужно:

1. Зафиксировать какую-либо нормальную запись (32) подстановки g.

2. Перебрать все возможные нормальные записи подстановки g:

$$g = g'_1 g'_2 \dots g'_s; \quad g'_i = (\alpha_1^{(i)}, \dots, \alpha_{m_i}^{(i)}), \quad i \in \overline{1,s}, \quad m_1 \geqslant m_2 \geqslant \dots \geqslant m_s \geqslant 1. \tag{33}$$

3. Для каждого варианта (33) нормальной записи подстановки g построить решение f уравнения (31) в виде

$$f = \begin{pmatrix} a_1^{(1)} & \dots & a_{m_1}^{(1)} & a_1^{(2)} & \dots & a_1^{(s)} & \dots & a_{m_s}^{(s)} \\ \alpha_1^{(1)} & \dots & \alpha_{m_1}^{(1)} & \alpha_1^{(2)} & \dots & \alpha_1^{(s)} & \dots & \alpha_{m_s}^{(s)} \end{pmatrix}.$$

По следствию 1 теоремы 34 таким способом будут описаны в точности все разные решения уравнения (31).

Из приведенного алгоритма следует, что число решений уравнения (31) равно числу различных нормальных записей подстановки g. Остается заметить, что для получения из нормальной записи (32) подстановки g всех ее нормальных записей (33) нужно:

1. Всеми способами переставить между собой циклы одинаковых длин (для k_j циклов длины l_j это, согласно (29), можно сделать $(k_j)!$ способами).

2. Для каждого варианта расстановки циклов перебрать все возможные способы записи каждого цикла (согласно (13), для k_j циклов длины l_j это можно проделать $l_j^{k_j}$ способами).

Теперь формула (30) очевидна.

(б) Заметим, что если f — какое-либо решение уравнения (24), то все подстановки из смежного класса $N_{S_n}(g)f$, очевидно, также будут решениями уравнения (24). Допустим теперь, что f_1 — еще одно решение уравнения (24). Тогда $f_1^{-1} g f_1 = f^{-1} g f = h$, и, следовательно, $(f_1 f^{-1})^{-1} \cdot g \cdot f_1 f^{-1} = g$, т. е. $f_1 f^{-1} \in N_{S_n}(g)$ и $f_1 \in N_{S_n}(g) f$. $\square$

Следствие. *Число подстановок в S_n, цикловая структура которых описывается таблицей* (29)*, равно*

$$\frac{n!}{\prod\limits_{i=1}^{r} (k_i)! \cdot l_i^{k_i}}.$$

$\square$ По теореме 34 совокупность указанных подстановок есть в точности класс $[g]_{\approx}$ элементов из S_n, сопряженных с подстановкой g из условия теоремы. Остается заметить, что согласно теореме 20 справедливы равенства

$$|[g]_{\approx}| = |S_n : N_{S_n}(g)| = \frac{|S_n|}{|N_{S_n}(g)|}. \quad \square$$

Замечание 8. Приведенный в доказательстве теоремы 35 алгоритм описания всех решений уравнения (31) пригоден для описания всех решений любого разрешимого уравнения (24) — достаточно лишь заменить в (33) подстановку g подстановкой h.

Полезно обратить внимание на сходство утверждения (б) теоремы 35 с теоремой 7 главы 8 о связи между множествами решений неоднородной и ассоциированной однородной систем линейных уравнений. Если уравнение (31) рассматривать как однородное, ассоциированное с (24), а систему линейных уравнений рассматривать как матричное уравнение, то в обоих случаях множество решений однородного уравнения — подгруппа, а множество решений неоднородного уравнения — смежный класс по ней, порожденный любым решением.

§ 11. ГОМОМОРФИЗМЫ ГРУПП И НОРМАЛЬНЫЕ ДЕЛИТЕЛИ

Читатель уже знаком с понятием гомоморфизма группоидов и с примерами гомоморфизмов, которые, в действительности, почти все строились в классе групп. Выше отмечалась и иллюстрировалась (см., например, доказательство теоремы 9) важная роль, которую играют гомоморфизмы при получении разного рода классификационных теорем и описании свойств алгебраических объектов.

В данном параграфе изучаются основные свойства гомоморфизмов групп и связанных с ними понятий.

1. Теорема 7 главы 10 (об эпиморфизме) сводит описание гомоморфных образов произвольного группоида к описанию его конгруэнций и факторгруппоидов. Однако для произвольного группоида (и даже полугруппы) это — задача весьма сложная. Если же группоид G является группой, то можно установить связь между конгруэнциями и некоторыми подгруппами G и значительно упростить описание классов конгруэнтных элементов.

Определение 36. Подгруппу H группы $(G, \cdot)$ называют *нормальной* или *нормальным делителем* группы G, если для любого $g \in G$ выполняется равенство $gH = Hg$ (т. е. множество левых смежных классов G по H совпадает с множеством правых смежных классов). В таком случае вместо $H < (G, \cdot)$ пишут $H \lhd (G, \cdot)$.

В любой неединичной группе G всегда есть два нормальных делителя: $H = G$ и $H = \{e\}$, называемых *несобственными*. Остальные нормальные делители группы называют *собственными*.

Пример 31. В абелевой группе все подгруппы являются нормальными делителями.

Пример 32. В любой группе $(G, \cdot)$ ее центр $C(G)$ (см. пример 8) — нормальный делитель (докажите).

Пример 33. Для любой группы G, если $H < G$ и $|G : H| = 2$, то $H \lhd G$ (в этом случае любой смежный класс G по H совпадает с H или с $G \setminus H$). В частности, для любого $n \in \mathbb{N}$, $A_n \lhd S_n$.

Пример 34. В группе S_4 подмножество

$$K_4 = \{\varepsilon,\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3)\}$$

есть абелева подгруппа и нормальный делитель (докажите). Группа K_4 называется *группой Клейна* или четверной группой.

Пример 35. Не являются нормальными подгруппа $\langle(1,2)\rangle$ в S_3 и любая циклическая неединичная подгруппа в S_n при $n \geqslant 4$ (докажите).

Следующие утверждения показывают, насколько свойство нормальности подгруппы устойчиво и делает подгруппу похожей на подгруппу абелевой группы.

Утверждение 36. *Пусть $(G,\cdot)$ — произвольная группа, тогда*
(а) *если $A < G$ и $H \lhd G$, то $A \cap H \lhd A$ и $AH < G$;*
(б) *если $K \lhd G$ и $H \lhd G$, то $K \cap H \lhd G$ и $KH \lhd G$.*

□ (а) Очевидно, что $A \cap H < A$. Кроме того, для любого $a \in A$ верны равенства $aH = Ha$ и

$$a(A \cap H) = aA \cap aH = A \cap Ha = Aa \cap Ha = (A \cap H)a,$$

т. е. $A \cap H \lhd A$. Наконец,

$$AH = \bigcup_{a \in A} aH = \bigcup_{a \in A} Ha = HA,$$

и в силу теоремы 15 $AH < G$.

(б) Если $K \lhd G$ и $H \lhd G$, то нормальность в G подгрупп $K \cap H$ и KH следует из того, что для любого $g \in G$ верны равенства

$$g(K \cap H) = gK \cap gH = Kg \cap Hg = (K \cap H)g,$$
$$g(KH) = (gK)H = (Kg)H = K(gH) = K(Hg) = (KH)g. \quad \square$$

2. Важнейшие определяющие свойства нормальных делителей в классе подгрупп перечисляет

Теорема 37. *Для подгруппы H группы G следующие утверждения эквивалентны*:
(а) $H \lhd G$;
(б) $N_G(H) = G$, *т. е.* $g^{-1}hg \in H$ *для любых* $g \in G$, $h \in H$;
(в) *отношения* "$\equiv (H)_{\text{П}}$" *и* "$\equiv (H)_{\text{Л}}$" *на G совпадают*;
(г) *отношение* "$\equiv (H)_{\text{П}}$" *есть конгруэнция на G*;
(д) *отношение* "$\equiv (H)_{\text{Л}}$" *есть конгруэнция на G.*

□ Эквивалентность утверждений (а) и (б) следует непосредственно из определений нормализатора и нормального делителя. Докажем теперь цепочку импликаций (а)⇒(в)⇒(г)⇒(а).

(а)⇒(в) Так как $Hg = gH$ для всех $g \in G$, то в силу теоремы 10 разбиение группы G, порождаемое отношением эквивалентности "$\equiv (H)_{\text{П}}$", совпадает с разбиением, порождаемым отношением "$\equiv (H)_{\text{Л}}$".

(в)⇒(г) Пусть $a \equiv b\,(H)_{\text{П}}$ и $c \equiv d\,(H)_{\text{П}}$. Тогда $ab^{-1} \in H$, $acc^{-1}b^{-1} \in H$, и, следовательно, $ac \equiv bc\,(H)_{\text{П}}$. Кроме того, в силу утверждения (в) $c \equiv d\,(H)_{\text{Л}}$ и справедливы соотношения $c^{-1}d \in H$, $c^{-1}b^{-1}bd \in H$, т. е. $bc \equiv bd\,(H)_{\text{Л}}$. Отсюда, опять по утверждению (в), имеем $bc \equiv bd\,(H)_{\text{П}}$, и, так как $ac \equiv bc\,(H)_{\text{П}}$, то $ac \equiv bd\,(H)_{\text{П}}$.

(г)⇒(а) Так как для любого $h \in H$ верно соотношение $h \equiv e\,(H)_\Pi$ и для любого $g \in G$ верны соотношения $g \equiv g\,(H)_\Pi$, $g^{-1} \equiv g^{-1}\,(H)_\Pi$, то, пользуясь согласованностью отношения "$\equiv (H)_\Pi$" с групповой операцией, получим последовательно $hg \equiv g\,(H)_\Pi$, $g^{-1}hg \equiv g^{-1}g\,(H)_\Pi$, $g^{-1}hg \equiv e\,(H)_\Pi$.

Следовательно, для любых $g \in G$ и $h \in H$ имеется включение $g^{-1}hg \in H$, т. е. $g^{-1}Hg \subset H$ и $Hg \subset gH$. Заменяя здесь g на g^{-1}, получаем $gHg^{-1} \subset H$ и $gH \subset Hg$. Следовательно, $Hg = gH$ для всех $g \in G$, т. е. $H \lhd G$.

Таким образом, доказана эквивалентность первых четырех утверждений теоремы. Теперь их эквивалентность утверждению (д) очевидна в силу соображений симметрии. (Читателю предлагается самостоятельно доказать импликации (в)⇒(д)⇒(а).) □

3. Покажем теперь, что теоремой 37 в действительности описаны все конгруэнции на группе G. Заметим, что если H — нормальный делитель в G, то можно говорить просто об отношении сравнимости по H и писать $a \equiv b\,(H)$, поскольку отношения "$\equiv (H)_\Pi$" и "$\equiv (H)_\Lambda$" совпадают.

Определение 37. Если $\varphi\colon (G,\cdot) \to (K,\cdot)$ — гомоморфизм групп, то его *ядром* называют множество

$$\operatorname{Ker}\varphi = \{g \in G\colon\ \varphi(g) = e_K\} = \varphi^{-1}(e_K),$$

где e_K — единица группы K.

Теорема 38. *Для любого гомоморфизма групп $\varphi\colon (G,\cdot) \to (K,\cdot)$ его ядро $\operatorname{Ker}\varphi$ есть нормальная подгруппа в G. Если ρ — произвольная конгруэнция на G, то ρ есть отношение сравнимости по подгруппе $\operatorname{Ker}\varphi_0$, где $\varphi_0\colon G \to G/\rho$ — канонический эпиморфизм. При этом $\operatorname{Ker}\varphi_0 = \{g \in G\colon\ g\,\rho\,e_G\} = [e_G]_\rho$.*

□ Пусть $\varphi\colon (G,\cdot) \to (K,\cdot)$ — произвольный гомоморфизм, тогда для любых элементов $a, b \in \operatorname{Ker}\varphi$ верны соотношения

$$\varphi(ab^{-1}) = \varphi(a)\cdot\varphi(b)^{-1} = e_K \cdot e_K^{-1} = e_K.$$

Следовательно, $ab^{-1} \in \operatorname{Ker}\varphi$ и $\operatorname{Ker}\varphi < G$. Кроме того, для любого $g \in G$ верны соотношения

$$\varphi(g^{-1}ag) = \varphi(g)^{-1}\varphi(a)\,\varphi(g) = \varphi(g)^{-1}\varphi(g) = e_K,$$

т. е. $g^{-1}ag \in \operatorname{Ker}\varphi$. Следовательно, $N_G(\operatorname{Ker}\varphi) = G$, и по теореме 37 $\operatorname{Ker}\varphi \lhd G$.

Пусть ρ — произвольная конгруэнция на $(G,\cdot)$. Рассмотрим факторгруппу G/ρ, состоящую из всех различных классов $[g]_\rho = \{a \in G\colon\ a\,\rho\,g\}$, с операцией $[g_1]_\rho \cdot [g_2]_\rho = [g_1g_2]_\rho$. По утверждению 6 главы 10 отображение $\varphi_0\colon G \to G/\rho$ по правилу $\varphi_0(g) = [g]_\rho$ есть гомоморфизм групп, связанный с отношением ρ следующим образом:

$$\forall\, g_1, g_2 \in G\colon\ g_1\,\rho\,g_2 \ \Leftrightarrow\ \varphi_0(g_1) = \varphi_0(g_2).$$

Но выше уже доказано соотношение

$$g_1 \equiv g_2\,(\operatorname{Ker}\varphi_0) \ \Leftrightarrow\ \varphi_0(g_1) = \varphi_0(g_2).$$

Следовательно, отношение ρ есть отношение сравнимости по $\operatorname{Ker}\varphi_0$. Остается заметить, что нейтральный элемент в группе G/ρ есть $[e_G]_\rho$, поэтому ядро канонического гомоморфизма φ_0 имеет вид:

$$\operatorname{Ker}\varphi_0 = \{g \in G:\ \varphi_0(g) = [e_G]_\rho\} = \{g \in G:\ \varphi_0(g) = \varphi_0(e_G)\} = \\ = \{g \in G:\ g\,\rho\,e_G\}. \quad \square$$

Следствие. *Гомоморфизм групп $\varphi\colon G \to K$ является мономорфизмом тогда и только тогда, когда* $\operatorname{Ker}\varphi = \{e_G\}$.

$\square$ Достаточно воспользоваться соотношением

$$\varphi(a) = \varphi(b) \ \Leftrightarrow\ a \equiv b\,(\operatorname{Ker}\varphi). \quad \square$$

4. Теоремы 37, 38 позволяют по новому, в более удобной и наглядной форме, сформулировать для групп теорему об эпиморфизме полугрупп.

Определение 38. Если $H \lhd G$, то *факторгруппой группы G по подгруппе H* называют факторгруппу группы G по отношению "$\equiv (H)$". Эту факторгруппу обозначают G/H. Таким образом, $G/H = G/\equiv(H)$.

Из общего определения факторгруппы очевидно, что элементами группы G/H являются классы элементов G, сравнимых по подгруппе H, т. е. по теореме 10 — смежные классы $gH = Hg$ группы G по H. При этом операция на элементах группы G/H задается следующим образом:

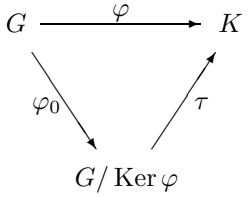
$$g_1H \cdot g_2H = g_1g_2H,$$

а канонический эпиморфизм $\varphi_0\colon G \to G/H$ задается равенством $\varphi_0(g) = gH$.

Заметим, что при аддитивной форме записи групповой операции элементы факторгруппы G/H записываются в виде $g + H$, а операция задается равенством

$$(g_1 + H) + (g_2 + H) = (g_1 + g_2) + H.$$

Теорема 39 (об эпиморфизме групп). *Если $\varphi\colon (G,\cdot) \to (K,\cdot)$ — эпиморфизм групп, то $G/\operatorname{Ker}\varphi \cong K$, и существует единственный изоморфизм $\tau\colon G/\operatorname{Ker}\varphi \to K$ такой, что коммутативна диаграмма*

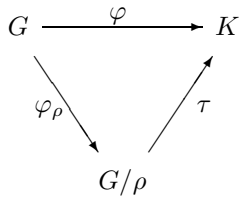


где $\varphi_0\colon G \to G/\operatorname{Ker}\varphi$ — канонический эпиморфизм. Изоморфизм τ задается равенством $\tau(g \cdot \operatorname{Ker}\varphi) = \varphi(g)$.

□ Из теоремы об эпиморфизме полугрупп (глава 10) следует, что если ρ — конгруэнция на G, определяемая условием

$$g_1 \,\rho\, g_2 \;\Leftrightarrow\; \varphi(g_1) = \varphi(g_2),$$

и $\varphi_0 \colon G \to G/\rho$ — канонический эпиморфизм, то существует единственный изоморфизм $\tau \colon G/\rho \to K$, дающий коммутативную диаграмму



При этом $\tau([g]_\rho) = \varphi(g)$. Остается заметить, что по теореме 38 ρ есть отношение сравнимости по $\operatorname{Ker}\varphi$, $G/\rho = G/\operatorname{Ker}\varphi$ и $[g]_\rho = g \cdot \operatorname{Ker}\varphi$. □

Эта теорема широко используется в теории групп для доказательства соотношений типа $G/H \cong K$ путем подбора эпиморфизма $\varphi \colon G \to K$ с ядром $\operatorname{Ker}\varphi = H$.

Пример 36. Имеет место изоморфизм групп $(\mathbb{R}/\mathbb{Z}, +) \cong (\Gamma, \cdot)$. Для доказательства достаточно заметить, что можно задать эпиморфизм $\varphi \colon (\mathbb{R}, +) \to (\Gamma, \cdot)$ по правилу $\varphi(r) = \cos 2\pi r + i \sin 2\pi r$, и при этом $\operatorname{Ker}\varphi = \mathbb{Z}$. Аналогично можно доказать, что $(\mathbb{R}/m\mathbb{Z}, +) \cong (\Gamma, \cdot)$ для любого $m \in \mathbb{N}$.

5. Следствие 2 утверждения 6 можно теперь дополнить.

Теорема 40. *Пусть* $\varphi \colon (G, \cdot) \to (K, \cdot)$ *— гомоморфизм групп. Тогда*
(а) $A < G \;\Rightarrow\; \varphi^{-1}(\varphi(A)) = A \cdot \operatorname{Ker}\varphi$;
(б) $B \lhd K \;\Rightarrow\; \varphi^{-1}(B) \lhd G$.
Если к тому же φ *— эпиморфизм, то*
(в) $B < K \;\Rightarrow\; \varphi(\varphi^{-1}(B)) = B$;
(г) $A \lhd G \;\Rightarrow\; \varphi(A) \lhd K$.

□ (а) Пусть $A < G$. По следствию 2 утверждения 6 $\varphi(A) < K$ и

$$A < \varphi^{-1}(\varphi(A)) < G. \tag{34}$$

Так как $e_K \in \varphi(A)$, то

$$\operatorname{Ker}\varphi = \varphi^{-1}(e_K) \subset \varphi^{-1}(\varphi(A)). \tag{35}$$

Из соотношений (34), (35) следует, что $A \cdot \operatorname{Ker}\varphi < \varphi^{-1}(\varphi(A))$. Наоборот, если элемент $\alpha \in \varphi^{-1}(\varphi(A))$, то $\varphi(\alpha) = \varphi(a)$ для подходящего $a \in A$, и

$$e_K = \varphi(a)^{-1} \cdot \varphi(\alpha) = \varphi(a^{-1} \cdot \alpha).$$

Следовательно, $a^{-1}\alpha \in \operatorname{Ker}\varphi$ и $\alpha \in a \operatorname{Ker}\varphi \subset A \cdot \operatorname{Ker}\varphi$, т. е. $\varphi^{-1}(\varphi(A)) < A \cdot \operatorname{Ker}\varphi$.

(б) Пусть $B \lhd K$. Тогда для любых $h \in \varphi^{-1}(B)$ и $g \in G$ справедливы соотношения $\varphi(h) \in B$ и $\varphi(g^{-1}hg) = \varphi(g)^{-1}\varphi(h)\varphi(g) \in B$. Следовательно, $g^{-1}hg \in \varphi^{-1}(B)$ и по теореме 37, с учетом следствия 2 утверждения 6, $\varphi^{-1}(B) \lhd G$.

(в) Для любого сюръективного отображения $\varphi\colon G \to K$ и любого $B \subset K$ верно равенство $\varphi(\varphi^{-1}(B)) = B$.

(г) Пусть φ — эпиморфизм и $A \lhd G$. Тогда для любого $k \in K$ существует $g \in G$ со свойством $k = \varphi(g)$, и, так как $gA = Ag$, то

$$k\varphi(A) = \varphi(g)\varphi(A) = \varphi(gA) = \varphi(Ag) = \varphi(A)\varphi(g) = \varphi(A)k.$$

Следовательно, $\varphi(A) \lhd K$. □

Замечание 9. Если операция в группе G записывается аддитивно, то утверждение (а) имеет вид $\varphi^{-1}(\varphi(A)) = A + \operatorname{Ker}\varphi$.

Читателю рекомендуется самому подобрать примеры, показывающие, что утверждения (в) и (г) теоремы 40 неверны, если φ — не эпиморфизм.

Теорему 40 вместе со следствием 2 утверждения 6 называют *теоремой об образах и полных прообразах* при гомоморфизме групп. Следующий результат принято называть *теоремой о соответствии* при эпиморфизме групп.

Для любой подгруппы H группы G обозначим через $L(H, G)$ множество всех подгрупп $F < G$, содержащих H (множество $L(H, G)$ содержит G и H).

Теорема 41. *Пусть $\varphi\colon (G, \cdot) \to (K, \cdot)$ — эпиморфизм групп. Тогда существует биекция*

$$\mu\colon L(\operatorname{Ker}\varphi, G) \to L(e, K)$$

такая, что для любых $F, T \in L(\operatorname{Ker}\varphi, G)$

(а) $F \subset T \;\Leftrightarrow\; \mu(F) \subset \mu(T)$;

(б) $T \lhd G \;\Leftrightarrow\; \mu(T) \lhd K$.

□ Нужное отображение μ задается правилом

$$\forall\, F \in L(\operatorname{Ker}\varphi, G) \quad \mu(F) = \varphi(F).$$

Проверка того, что μ — отображение, удовлетворяющее указанным в формулировке условиям, осуществляется с использованием теоремы 40 и следствия 2 утверждения 6 и предоставляется читателю. □

§ 12. ТЕОРЕМЫ ОБ ИЗОМОРФИЗМЕ

При получении многих теоретико-групповых результатов весьма эффективным инструментом оказываются следующие две теоремы.

Теорема 42 (первая теорема об изоморфизме). *Если $\varphi\colon (G, \cdot) \to (K, \cdot)$ — гомоморфизм групп и $A < G$, то*

$$(A \cap \operatorname{Ker}\varphi) \lhd A, \quad \varphi(A) \cong A/A \cap \operatorname{Ker}\varphi.$$

□ Так как $\operatorname{Ker}\varphi \lhd G$ (теорема 38), то $(A \cap \operatorname{Ker}\varphi) \lhd A$ (утверждение 36(а)). Зададим отображение $\psi\colon A \to K$, положив

$$\forall\, a \in A\ (\psi(a) = \varphi(a)).$$

Нетрудно видеть, что ψ — гомоморфизм группы $(A,\cdot)$ в $(K,\cdot)$ и $\psi(A) = \varphi(A)$, т. е. ψ — эпиморфизм $(A,\cdot)$ на $(\varphi(A),\cdot)$. Следовательно, по теореме об эпиморфизме для групп $\varphi(A) \cong A/\operatorname{Ker}\psi$. Остается заметить, что справедливы равенства

$$\operatorname{Ker}\psi = \{a \in A\colon\ \psi(a) = e_K\} = \{a \in G\colon\ \varphi(a) = e_K,\ a \in A\} = A \cap \operatorname{Ker}\varphi. \quad \square$$

Следствие. *Если H — нормальный делитель и A — подгруппа группы G, то верны соотношения*

$$H \lhd AH, \quad A \cap H \lhd A, \quad AH/H \cong A/A \cap H.$$

□ Рассмотрим канонический эпиморфизм $\varphi\colon G \to G/H$. Тогда $\operatorname{Ker}\varphi = H$ и по теореме 40(а) справедливы равенства

$$\varphi^{-1}(\varphi(A)) = A \cdot \operatorname{Ker}\varphi = A \cdot H. \tag{36}$$

Так как $\varphi(\varphi^{-1}(\varphi(A))) = \varphi(A)$ (докажите), то из (36) следует равенство $\varphi(A) = \varphi(AH)$. Теперь, дважды применяя теорему, получаем:

$$\varphi(A) \cong A/A \cap \operatorname{Ker}\varphi = A/A \cap H,$$
$$\varphi(A) \cong AH/AH \cap \operatorname{Ker}\varphi = AH/AH \cap H = AH/H. \quad \square$$

Замечание 10. При аддитивной форме записи групповой операции следствие теоремы 42 утверждает: если A, H — произвольные подгруппы абелевой группы $(G,+)$, то

$$A/A \cap H \cong (A+H)/H. \tag{37}$$

Последнее соотношение имеет весьма интересную арифметическую интерпретацию.

Пример 37. Нетрудно проверить, что для любых $a, m \in \mathbb{N}$ имеет место изоморфизм $(a\mathbb{Z}/am\mathbb{Z},+) \cong (\mathbb{Z}_m,+)$. Пусть A и H — подгруппы в $(\mathbb{Z},+)$. Тогда для подходящих $a, h \in \mathbb{N}$ верны равенства $A = a\mathbb{Z}$, $H = h\mathbb{Z}$, $A + H = (a,h)\mathbb{Z}$, $A \cap H = [a,h]\mathbb{Z}$, и имеют место изоморфизмы:

$$(A+H)/H = (a,h)\mathbb{Z}/h\mathbb{Z} \cong \mathbb{Z}_{h/(a,h)},$$
$$A/A \cap H = a\mathbb{Z}/[a,h]\mathbb{Z} \cong \mathbb{Z}_{[a,h]/a}.$$

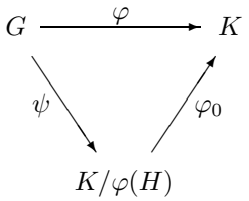
Теперь видно, что изоморфизм (37) обобщает известное арифметическое соотношение $\dfrac{h}{(a,h)} = \dfrac{[a,h]}{a}$.

Теорема 43 (вторая теорема об изоморфизме). *Если* $\varphi\colon (G,\cdot) \to (K,\cdot)$ *— эпиморфизм групп и* $H \lhd G$*, то*

$$\varphi(H) \lhd K \quad \textit{и} \quad K/\varphi(H) \cong G/(H \cdot \operatorname{Ker}\varphi),$$

т. е. $\varphi(G)/\varphi(H) \cong G/(H \cdot \operatorname{Ker}\varphi)$.

□ Условие $\varphi(H) \lhd K$ следует из теоремы 40(г). Рассмотрим канонический эпиморфизм $\varphi_0\colon K \to K/\varphi(H)$ и зададим отображение $\psi\colon G \to K/\varphi(H)$ условием $\psi(g) = \varphi_0(\varphi(g)) = \varphi(g)\cdot\varphi(H)$, т. е. так, чтобы была коммутативна следующая диаграмма



Очевидно, что ψ — эпиморфизм G на $K/\varphi(H)$, так как $\psi = \varphi_0 \circ \varphi$ — композиция двух эпиморфизмов. Следовательно, по теореме об эпиморфизме $K/\varphi(H) \cong G/\operatorname{Ker}\psi$.

Остается доказать равенство $\operatorname{Ker}\psi = H \cdot \operatorname{Ker}\varphi$.

Так как нейтральным элементом в группе $K/\varphi(H)$ является класс $\varphi(H)$ и $\psi(g) = \varphi(g)\cdot\varphi(H)$ для любого $g \in G$, то верны соотношения

$$g \in \operatorname{Ker}\psi \;\Leftrightarrow\; \varphi(g)\cdot\varphi(H) = \varphi(H) \;\Leftrightarrow\; \varphi(g) \in \varphi(H) \;\Leftrightarrow$$
$$\Leftrightarrow\; g \in \varphi^{-1}(\varphi(H)) = H\operatorname{Ker}\varphi. \quad \square$$

Следствие. *Если* N*,* H *— нормальные подгруппы группы* G *и* $N \subset H$*, то* $H/N \lhd G/N$ *и*

$$G/H \cong (G/N)/(H/N). \tag{38}$$

□ Факторгруппа H/N есть образ нормального делителя H группы G при каноническом гомоморфизме $\varphi\colon G \to G/N$, так как по определению H/N есть множество разных смежных классов вида gN, где $g \in H$. Тогда в силу теоремы 43 имеем:

$$(G/N)/\varphi(H) = (G/N)/(H/N) \cong G/H \cdot \operatorname{Ker}\varphi.$$

Остается заметить, что $\operatorname{Ker}\varphi = N \subset H$, и поэтому $H \cdot \operatorname{Ker}\varphi = H$. □

Доказанное следствие имеет еще более простую арифметическую интерпретацию.

Пример 38. Пусть $G = \mathbb{Z} > H > N \neq 0$. Тогда $N = n\mathbb{Z}$, $H = h\mathbb{Z}$ и $n = mh$, где $m, n, h \in \mathbb{N}$. Отсюда имеем $G/H = \mathbb{Z}/h\mathbb{Z} \cong \mathbb{Z}_h$, $G/N \cong \mathbb{Z}_n$, $H/N = h\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_m$, и H/N — подгруппа порядка m в $\mathbb{Z}_n$, порожденная делителем h. Поскольку все выписанные группы циклические, а изоморфизм таких групп эквивалентен равенству их порядков, то изоморфизм (38) в рассматриваемом случае есть эквивалент равенства $h = \dfrac{mh}{m}$.

§ 13. ПРОСТЫЕ ГРУППЫ

1. Изучение группы путем ее «упрощения» с помощью гомоморфизмов или факторизации возможно лишь в тех случаях, когда она имеет собственные нормальные делители. Однако этим свойством обладает не любая группа.

Определение 39. Неединичную группу G, не имеющую собственных нормальных делителей, называют *простой*.

Описание всех простых групп — один из основных и самых сложных разделов современной теории конечных групп. Простые абелевы группы, т. е. абелевы группы, не имеющие собственных подгрупп, описываются очень легко.

Теорема 44. *Неединичная абелева группа $(G, \cdot)$ является простой тогда и только тогда, когда она — конечная группа простого порядка.*

□ Если $|G| = p$ — простое число, то по теореме Лагранжа G не имеет собственных подгрупп. Пусть, наоборот, G — простая абелева группа. Выберем любой элемент $g \in G \backslash \{e\}$. Тогда $\langle g \rangle$ — неединичная подгруппа в G, и так как G не имеет собственных подгрупп, то $G = \langle g \rangle$ — циклическая группа. Но в таком случае по теореме 9 либо $G \cong \mathbb{Z}$, либо $G \cong \mathbb{Z}_m$. Если $G \cong \mathbb{Z}$ или $G \cong \mathbb{Z}_m$, где m — не простое число, то в G легко указать собственную подгруппу. Следовательно, $G \cong \mathbb{Z}_p$, где p — простое. □

2. Первую серию конечных простых неабелевых групп открыл еще Э. Галуа. Его результат можно сформулировать следующим образом.

Теорема 45. *Знакопеременные группы A_n просты при всех $n \geqslant 3$ за исключением случая $n = 4$.*

□ $A_3 = \langle (1, 2, 3) \rangle$ — простая абелева группа порядка 3.

A_4 — не простая (не абелева) группа, ее собственным нормальным делителем является подгруппа Клейна (см. пример 34).

Докажем простоту A_n при $n \geqslant 5$.

Лемма 46. *При $n \geqslant 5$ любые два цикла длины 3: $g = (a_1, a_2, a_3)$ и $h = (\alpha_1, \alpha_2, \alpha_3)$ сопряжены в A_n.*

□ Уравнение $x^{-1} g x = h$ имеет в S_n решение вида

$$f = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & \dots & a_n \\ \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \dots & \alpha_n \end{pmatrix}.$$

Но тогда, очевидно, подстановка

$$f' = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & \dots & a_n \\ \alpha_1 & \alpha_2 & \alpha_3 & \alpha_5 & \alpha_4 & \dots & \alpha_n \end{pmatrix}$$

— также решение этого уравнения. Так как f и f' — подстановки разной четности, то одна из них принадлежит A_n. □

Пусть G — неединичный нормальный делитель в A_n. Покажем, что $G = A_n$. Среди элементов G выберем неединичную подстановку g с наименьшим числом мобильных элементов. Достаточно показать, что g — цикл длины 3, так как тогда по лемме 46 в G лежат все циклы длины 3 и по теореме 33 $G \supset A_n$.

Покажем сначала, что в разложении подстановки g в произведение независимых циклов все неединичные циклы имеют одинаковую длину. Действительно, если в этом разложении есть циклы длин k и m, и $1 < k < m$, то $g^k \in G \setminus \{\varepsilon\}$, причем $|\operatorname{mob} g^k| < |\operatorname{mob} g|$, что противоречит выбору подстановки g. Следовательно, разложение g на независимые неединичные циклы имеет вид

$$g = (a_1, \ldots, a_k) \cdot (b_1, \ldots, b_k) \cdot \ldots \cdot (c_1, \ldots, c_k), \quad k \geqslant 2. \tag{39}$$

Допустим, что число циклов в разложении (39) равно t. Наша задача — доказать, что $k = 3$, $t = 1$.

Заметим, что для любой подстановки $f \in A_n$ подстановки $f^{-1}gf$ и $g' = g^{-1}f^{-1}gf$ принадлежат H. Покажем, что если $k \neq 3$ или $t > 1$, то можно подобрать подстановку $f \in A_n$ так, что $|\operatorname{mob} g'| < |\operatorname{mob} g|$ и $g' \neq \varepsilon$, а это противоречит выбору g.

Если $k > 3$, то, выбирая $f = (a_1, a_k, a_2)$, получаем

$$f \in A_n, \quad \operatorname{mob} g' \subset \operatorname{mob} g \tag{40}$$

и $g' = (a_k, a_{k-1}, \ldots, a_2, a_1) \cdot (a_k, a_1, a_3, \ldots, a_{k-1}, a_2) = (a_1) \cdot (a_2, a_3, a_k) \cdot \ldots$. Следовательно,

$$g' \neq \varepsilon, \quad g'(a_1) = a_1 \quad \text{и} \quad |\operatorname{mob} g'| < |\operatorname{mob} g|. \tag{41}$$

Если $k = 3$, но $t > 1$, то для $f = (a_2, b_2, b_1)$ выполняются условия (40) и

$$g' = (b_3, b_2, b_1)(a_3, a_2, a_1)(a_1, b_2, a_3)(a_2, b_1, b_3) = (a_1)(a_2, b_2, \ldots),$$

откуда также следует (41).

Если $k = 2$, то t четно, поскольку $g \in A_n$. При этом если $t = 2$, т. е. $g = (a_1, a_2)(b_1, b_2)$, то, ввиду условия $n \geqslant 5$, существует элемент $d \in \overline{1, n} \setminus \{a_1, a_2, b_1, b_2\}$. Тогда условия (40) и (41) выполняются для $f = (b_1, b_2, d)$, поскольку в этом случае

$$g' = (b_2, b_1)(a_2, a_1)(a_1, a_2)(b_2, d) = (b_1, d, b_2).$$

Наконец, если $k = 2$, $t \geqslant 4$, то $|\operatorname{mob} g| \geqslant 8$, и, выбирая $f = (a_1, b_1, c_1)$, получаем

$$g' = (c_2, c_1)(b_2, b_1)(a_2, a_1)(b_1, a_2)(c_1, b_2)(a_1, c_2) = (a_1, b_1, c_1)(a_2, c_2, b_2).$$

Следовательно, $|\operatorname{mob} g'| = 6 < |\operatorname{mob} g|$.

Таким образом, разложение (39) имеет вид $g = (a_1, a_2, a_3)$, и потому $H = A_n$. $\square$

3. Еще одна важная серия простых групп, найденная К. Жорданом, — это проективные специальные линейные группы. Пусть F — поле и $m \in \mathbb{N}$. Подгруппа полной линейной группы $GL(m, F)$, состоящая из всех преобразований φ_A (см. пример 24), для которых $|A| = e$, называется *специальной линейной группой* и обозначается $SL(m, F)$. Центр $C(SL(m, F))$ группы $SL(m, F)$ состоит из всех принадлежащих

ей скалярных матриц (докажите). Факторгруппа $SL(m,F)/C(SL(m,F))$ называется *проективной специальной линейной группой* и обозначается $PSL(m,F)$. Если F — поле из q элементов, то употребляется обозначение $PSL(m,q)$.

Приведем без доказательства следующий результат.

Теорема Жордана–Диксона.[14] *Для конечного поля F группа $PSL(m,F)$ проста, за исключением случаев $PSL(2,2)$ и $PSL(2,3)$.*

Приведем еще два важных результата (которые, однако, далеко не полно характеризуют настоящее состояние теории).

Теорема Бернсайда. *Любая группа порядка p^aq^b, где p, q — простые, не проста.*

Теорема Фейта–Томпсона.[15] *Любая конечная неабелева группа нечетного порядка не проста.*

Полезно иметь в виду, что первое опубликованное доказательство последней теоремы занимает несколько сотен страниц — целый выпуск математического журнала.

Таким образом, порядок любой конечной простой неабелевой группы делится на 2 и еще на два нечетных простых числа. Самая маленькая простая неабелева группа есть группа A_5 порядка 60.

Выдвинута гипотеза (называемая S-гипотезой) о том, что классификация конечных простых групп завершена, т. е. что список уже найденных простых конечных групп, небольшая часть которых приведена выше, содержит все существующие простые группы. Эта гипотеза, однако, до сих пор окончательно не подтверждена.

§ 14. СИЛОВСКИЕ ПОДГРУППЫ

Выше уже отмечалось, что обращение теоремы Лагранжа (см. замечание перед теоремой 12) в общей форме для конечных групп неверно (пример 29). Однако такое обращение справедливо для любой конечной группы в одном важном случае.

Определение 40. Подгруппу H конечной группы G называют *p-подгруппой*, или *примарной подгруппой*, если $|H| = p^k$, где p — простое число, $k \in \mathbb{N}$. Если при этом p^k есть наибольшая степень числа p, делящая $|G|$, то H называют *силовской p-подгруппой группы G*.

Следующие результаты, полученные более ста лет назад П. Л. Силовым[16], по своей фундаментальности и многообразию приложений сравнимы с самой теоремой Лагранжа.

Теорема 47 (первая теорема Силова). *Если $(G,\cdot)$ — группа порядка n, p — простой делитель n и $p^t \mid n$, то в G существует подгруппа порядка p^t. В частности, в G существует силовская p-подгруппа.*

[14] Л. Е. Диксон (1874–1954) — американский математик.
[15] У. Фейт, Дж. Томпсон — современные американские математики.
[16] П. Л. Силов (1832–1918) — норвежский математик.

Докажем сначала следующее вспомогательное утверждение.

Лемма 48 (Коши). *Если $(A,\cdot)$ — абелева группа порядка m и p — простой делитель m, то в A существует подгруппа порядка p.*

□ Индукция по m. Если m — простое число, то лемма очевидна. Пусть $N>1$, и лемма верна для всех групп A таких, что $m<N$. Докажем ее для $m=N$. Очевидно, достаточно доказать, что в A есть элемент порядка p. Выберем произвольно $b\in A\setminus\{e\}$. Если $\operatorname{ord} b=r$ и $p\mid r$, то нужный элемент есть b^k, $k=\dfrac{r}{p}$. Пусть $p\nmid r$, т. е. $(p,r)=1$. Рассмотрим подгруппу $B=\langle b\rangle$ группы A и факторгруппу A/B. Так как $|B|=r$, то $|A/B|=\dfrac{m}{r}$, и $p\mid\dfrac{m}{r}$, поскольку $(p,r)=1$. Так как $\dfrac{m}{r}<N$, то, ввиду предположения индукции, в группе A/B существует некоторый элемент $a\cdot B$ порядка p.

Остается заметить, что $\operatorname{ord}(aB)\mid\operatorname{ord} a$, поскольку из условия $a^t=e$ следует, что $(aB)^t=e=B$. Следовательно, $p\mid\operatorname{ord} a$. □

□ Доказательство теоремы 47 проведем индукцией по порядку $n\in\mathbb{N}$ группы G. Если n — простое, то теорема очевидна. Пусть $N>1$ и теорема верна для любой группы порядка n при $n<N$. Предположим, что $n=N$.

Если в группе G существует собственная подгруппа H такая, что $(|G:H|,p)=1$, то, очевидно, $p^t\mid|H|$. По предположению индукции в H существует подгруппа порядка p^t, и она будет нужной p-подгруппой в G.

Допустим теперь, что для любой собственной подгруппы $H<G$ выполняется условие $p\mid|G:H|$. Покажем сначала, что в этом случае центр $C(G)$ группы G нетривиален, и $p\mid|C(G)|$.

Пусть $[g_1]_{\approx}$, …, $[g_s]_{\approx}$ — все различные классы сопряженных элементов группы G, имеющие мощность, большую единицы. Тогда, ввиду замечания 6, множество G следующим образом представляется в виде объединения непересекающихся подмножеств:

$$G=C(G)\cup[g_1]_{\approx}\cup\ldots\cup[g_s]_{\approx}.$$

Следовательно,

$$|G|=|C(G)|+|[g_1]_{\approx}|+\ldots+|[g_s]_{\approx}|. \tag{42}$$

По теореме 20 $|[g_i]_{\approx}|=|G:N_G(g_i)|$, и, в соответствии со сделанными предположениями об индексах подгрупп в G, можно утверждать, что

$$p\mid|[g_i]_{\approx}|\text{ для }i\in\overline{1,s}. \tag{43}$$

Так как по условию $p\mid|G|$, то из (42) и (43) следует нужное соотношение: $p\mid|C(G)|$.

В таком случае, по лемме Коши в группе $C(G)$ есть подгруппа H порядка p. Если $t=1$, то H — искомая p-подгруппа в G. Допустим, что $t>1$. Поскольку H — подгруппа центра группы G, то $H\lhd G$, и можно рассмотреть факторгруппу G/H и канонический эпиморфизм $\varphi\colon G\to G/H$.

Так как $|G/H|=\dfrac{n}{p}<N$ и $p^{t-1}\mid|G/H|$, то по предположению индукции в G/H существует подгруппа S' порядка p^{t-1}. Пусть $S=\varphi^{-1}(S')$. Тогда $S\supset H=\operatorname{Ker}\varphi$,

и по теореме 40(в) $\varphi(S) = S'$. Следовательно, по первой теореме об изоморфизме (теорема 42) $S' \cong S/H$. Но тогда выполняются равенства $|S| = |S'| \cdot |H| = p^t$, и S — искомая подгруппа в G. □

Теперь можно доказать обращение теоремы Лагранжа для конечных абелевых групп.

Следствие. *Если $(G,+)$ — абелева группа порядка n и $d \mid n$, $d \in \mathbb{N}$, то в G существует подгруппа H порядка d.*

□ Индукция по d. При $d = 1$ утверждение очевидно. Пусть $m > 1$ и утверждение верно для $d < m$. Докажем его для $d = m$. Пусть p — простой делитель d и $d = p^t k$, где $(k,p) = 1$. Тогда $k < m$ и по предположению индукции в группе G существует подгруппа A порядка k, а по первой теореме Силова в G существует подгруппа B порядка p^t. В таком случае, по следствию теоремы 17, $H = A + B$ — искомая подгруппа в G порядка d. □

Анализируя доказательство первой теоремы Силова, нетрудно увидеть, что она может быть дополнена также следующим утверждением: *любая p-подгруппа конечной группы лежит в некоторой ее силовской p-подгруппе.*

Приведем еще две теоремы о силовских p-подгруппах.

Вторая теорема Силова. *Любые две силовских p-подгруппы конечной группы G сопряжены в G.*

Третья теорема Силова. *Число s_p силовских p-подгрупп в группе G удовлетворяет условиям*: $s_p \equiv 1 \pmod p$, $s_p \mid |G|$.

Мы докажем эти теоремы лишь в частном случае — для коммутативной группы. Здесь справедливо даже более сильное утверждение.

Теорема 49. *Пусть $(G,+)$ — конечная абелева группа порядка n, и для некоторого простого p верны соотношения*: $n = p^k m$, $k > 0$, $(p,m) = 1$. *Тогда в G существует единственная силовская p-подгруппа $G^{(p)}$ и справедливы равенства*

$$G^{(p)} = \{g \in G : \ \operatorname{ord} g \mid p^k\}, \tag{44}$$

$$G^{(p)} = mG = \{mg : \ g \in G\}. \tag{45}$$

□ Обозначим через G_1 и G_2 множества из правых частей равенств соответственно (44) и (45). Пользуясь коммутативностью группы G, легко проверить, что $G_i < G$, $i \in \overline{1,2}$ (докажите). По первой теореме Силова в группе G существует силовская p-подгруппа: $S < G$, $|S| = p^k$. Теперь очевидно, достаточно доказать равенства $S = G_1$, $G_1 = G_2$.

Включение $S \subset G_1$ очевидно. С другой стороны, G_1 — p-подгруппа в G, так как иначе число $|G_1|$ делится на некоторое простое q, отличное от p, и тогда по лемме Коши в G_1 существует подгруппа и элемент порядка q, что противоречит определению G_1. Следовательно, $|G_1| = p^l$, $p^l \mid n$, и, ввиду условия, $l \leqslant k$. Отсюда $|G_1| < |S|$, и так как $S \subset G_1$, то $S = G_1$.

Докажем равенство $G_1 = G_2$. Так как для любого $g \in G$ выполняется равенство $p^k(mg) = 0$, то $mg \in G_1$, т. е. $G_2 \subset G_1$. С другой стороны, для любого $g \in G_1$ из условия $(m, p) = 1$ следует, что $(\operatorname{ord} g, m) = 1$, и потому $\operatorname{ord} mg = \operatorname{ord} g$, т. е. $\langle mg \rangle = \langle g \rangle$ и $g \in \langle mg \rangle \subset G_2$. Следовательно, $G_1 \subset G_2$ и $G_1 = G_2$. □

Следствие. *Конечная непримарная абелева группа $(G, +)$ порядка $n \in \mathbb{N}$, имеющего каноническое разложение $n = p_1^{k_1} \dots p_t^{k_t}$, раскладывается в прямую сумму своих силовских подгрупп*:

$$G = G^{(p_1)} \dotplus \ldots \dotplus G^{(p_t)}. \tag{46}$$

Любое другое разложение группы G в прямую сумму примарных подгрупп попарно взаимно простых порядков отличаются от (46) *лишь перестановкой слагаемых.*

□ Пусть $H = G^{(p_1)} + \ldots + G^{(p_t)}$. Тогда по следствию из теоремы 17 имеем, что $H = G^{(p_1)} \dotplus \ldots \dotplus G^{(p_t)}$ и $|H| = |G^{(p_1)}| \cdot \ldots \cdot |G^{(p_t)}| = n = |G|$. Следовательно, $G = H$, и справедливо (46).

Если $G = H_1 + \ldots + H_s$, где $H_1, \ldots, H_s$ — примарные подгруппы попарно взаимно простых порядков $q_1^{l_1}, \ldots, q_s^{l_s}$, соответственно, то $|G| = |H_1| \cdot \ldots \cdot |H_s|$, и каноническое разложение числа $n = |G|$ можно записать в виде $n = q_1^{l_1} \dots q_s^{l_s}$. Отсюда по основной теореме арифметики следует, что $s = t$ и $(q_1^{l_1}, \ldots, q_s^{l_s})$ — перестановка чисел $p_1^{k_1}, \ldots, p_t^{k_t}$. Следовательно, $H_1, \ldots, H_t$ — силовские подгруппы группы G. Так как по теореме для каждого p_i, $i \in \overline{1,t}$, силовская p_i-подгруппа в G единственна, то $(H_1, \ldots, H_t)$ — перестановка набора $(G^{(p_1)}, \ldots, G^{(p_t)})$. □

Обратите внимание на то, что доказанное следствие есть обобщение второй части теоремы 18 на конечные абелевы группы.

ЗАДАЧИ

1. Докажите, что если в полугруппе с нейтральным элементом для некоторого элемента есть правый и левый обратные, то они совпадают.

2. Опишите возможные порядки элементов и экспоненты групп $\mathbb{Z}_4^*$, $\mathbb{Z}_8^*$, $\mathbb{Z}_{2^n}^*$, S_2, S_3, S_4.

3. Докажите, что в конечной группе $(G, \cdot)$ для любого $k > 2$ число элементов порядка k четно (воспользуйтесь тем, что $\operatorname{ord} g = \operatorname{ord} g^{-1}$).

4. Докажите, что если в группе есть перестановочные элементы порядков $m, n \in \mathbb{N}$, то в ней есть элемент порядка $[m, n]$.

5. Приведите пример конечной группы G, в которой нет элемента $g \in G$ со свойством $\operatorname{ord} g = \exp G$.

6. Докажите, что если $\varphi\colon G \to H$ — гомоморфизм групп, то для любого $g \in G$ верно соотношение $\operatorname{ord} \varphi(g) \mid \operatorname{ord} g$, а если φ — мономорфизм, то $\operatorname{ord} \varphi(g) = \operatorname{ord} g$.

7. Пусть P — поле с единицей e. Докажите, что в группе $(P, +)$ либо $\operatorname{ord} e = \infty$, либо $\operatorname{ord} e = p$ — простое число, и для любого $g \in P \setminus \{0\}$ верны равенства $\operatorname{ord} g = \operatorname{ord} e = \exp(P, +)$.

8. Опишите элементы конечных порядков в группах $(\mathbb{Q},+)$ и $(\mathbb{Q}^*,\cdot)$ и покажите, что эти группы не изоморфны.

9. Докажите, что центр группы $P^*_{n\times n}$ всех обратимых матриц над полем P состоит из всех ненулевых скалярных матриц.

10. Покажите, что для любых подмножеств A и B группы G справедливо соотношение

$$\langle A\rangle < \langle B\rangle \;\Leftrightarrow\; A\subset\langle B\rangle.$$

11. Докажите, что группы $(\mathbb{Q},+)$, $(\mathbb{C}(p^\infty),\cdot)$, $(\Gamma_{\mathbb{N}},\cdot)$ не имеют конечных систем образующих.

12. Докажите, что если S — система образующих группы $\mathbb{C}(p^\infty)$, то для любого $s\in S$ множество $S\setminus\{s\}$ — также система образующих $\mathbb{C}(p^\infty)$. Верно ли аналогичное утверждение для группы $(\mathbb{Q},+)$?

13. Пусть $a_1,\ldots,a_t\in\mathbb{Z}$, $d=(a_1,\ldots,a_t)$, $h=[a_1,\ldots,a_t]$. Докажите соотношения:

$$\langle a_1\rangle\subset\langle a_2\rangle \;\Leftrightarrow\; a_2\mid a_1;\quad \langle a_1,\ldots,a_t\rangle=\langle d\rangle;\quad \langle a_1\rangle\cap\ldots\cap\langle a_t\rangle=\langle h\rangle.$$

14. Докажите, что для конечной группы G следующие утверждения эквивалентны:

а) $\exists\, g\in G:\ \operatorname{ord} g=|G|$;

б) G — циклическая группа;

в) G — абелева группа и $\exp G=|G|$.

Покажите, что в пункте в) нельзя отказаться от первого условия.

15. Пусть $G=\langle g\rangle$ — циклическая группа порядка m. Докажите, что для любых $a,b\in\mathbb{Z}$

$$g^b\in\langle g^a\rangle \;\Leftrightarrow\; \text{разрешимо сравнение } ax\equiv b\,(\operatorname{mod} m).$$

16. Пусть $A_i=\langle S_i\rangle$, $i\in\overline{1,t}$, — подгруппы абелевой группы $(G,+)$. Докажите равенство $A_1+\ldots+A_t=\langle S_1\cup\ldots\cup S_t\rangle$.

17. Докажите, что если $A,B<(G,\cdot)$, то

$$(AB<(G,\cdot)) \;\Leftrightarrow\; (AB=\langle A\cup B\rangle).$$

18. Докажите, что для подгрупп A,B,C абелевой группы $(G,+)$ верно включение $A\cap(B+C)\supset(A\cap B)+(A\cap C)$, и, если $A\supset B$, то оно превращается в равенство.

19. Покажите, что для любых подгрупп A,B,C группы $(\mathbb{Z},+)$ верно равенство $A\cap(B+C)=A\cap B+A\cap C$.

20. Если $m_1,m_2\in\mathbb{N}$ и $m=m_1m_2$, то в группе Γ_m лежат подгруппы Γ_{m_1}, Γ_{m_2}. Докажите, что

$$\Gamma_m=\Gamma_{m_1}\cdot\Gamma_{m_2} \;\Leftrightarrow\; (m_1,m_2)=1.$$

21. Докажите, что если A,B — конечные подгруппы группы $(G,\cdot)$, то $|AB|=\dfrac{|A|\cdot|B|}{|A\cap B|}$ (покажите, что число различных смежных классов вида aB, $a\in A$, равно $|A:(A\cap B)|$).

22. Используя теорему Лагранжа, докажите *теорему Эйлера*:

$$\forall\, a \in \mathbb{Z},\ \forall\, m \in \mathbb{N}:\ (a,m)=1\ \Rightarrow\ a^{\varphi(m)} \equiv 1 \,(\mathrm{mod}\, m).$$

23. Используя теорему Лагранжа, покажите, что если P — поле из q элементов, то все элементы из P^* — корни многочлена $x^{q-1}-e$, а все элементы из P — корни $x^q - x$.

24. Докажите, что в мультипликативной группе P^* произвольного поля P любая конечная подгруппа — циклическая, в частности если $|P| < \infty$, то P^* — циклическая группа (воспользуйтесь результатом задачи 14).

25. Докажите, что непустое подмножество K группы $(G,\cdot)$ является смежным классом по некоторой ее подгруппе тогда и только тогда, когда

$$\forall\, a,b,c \in K\ (ab^{-1}c \in K).$$

Опишите подгруппы, по которым K является правым и левым смежным классом.

26. Пусть H_1, H_2 — подгруппы группы $(G,\cdot)$ и $g_1, g_2 \in G$. Докажите:

а) $H_1 g_1 \cap H_2 g_2 \neq \varnothing\ \Leftrightarrow\ g_1 g_2^{-1} \in H_1 \cdot H_2$;

б) $g \in (H_1 g_1 \cap H_2 g_2)\ \Rightarrow\ H_1 g_1 \cap H_2 g_2 = (H_1 \cap H_2)g$;

в) $H_1 g_1 \subset H_2 g_2\ \Leftrightarrow\ H_1 \subset H_2,\ g_1 g_2^{-1} \in H_2$;

г) $H_1 g_1 = H_2 g_2\ \Leftrightarrow\ H_1 = H_2,\ g_1 g_2^{-1} \in H_2$.

27. Пусть $G = \langle g \rangle$ — группа порядка m и $H = \langle g_1, \ldots, g_t \rangle$, где $g_1, \ldots, g_t \in G$. Докажите:

а) если $\mathrm{ord}\, g_i = m_i$, $i \in \overline{1,t}$, то $H = \langle g^{\left(\frac{m}{m_1}, \ldots, \frac{m}{m_t}\right)} \rangle$ и $|H| = [m_1, \ldots, m_t]$;

б) если $g_i = g^{k_i}$, $i \in \overline{1,t}$, то $H = \langle g^{(k_i, \ldots, k_t)} \rangle = \langle g^{(k_1, \ldots, k_t, m)} \rangle$.

28. Докажите, что в циклической группе порядка m для каждого натурального числа d, делящего m, существует ровно $\varphi(d)$ элементов порядка d ($\varphi(d)$ — функция Эйлера, $\varphi(1)=1$). Выведите *тождество Гаусса*: $\sum_{d|m} \varphi(d) = m$.

29. Пусть G — группа порядка m, в которой для каждого $d \mid m$ существует не более одной подгруппы порядка d. Докажите, что G — циклическая группа. (Покажите, что число $\psi(d)$ элементов порядка d в G не превосходит $\varphi(d)$, и воспользуйтесь предыдущей задачей.)

30. Пусть $(G,+)$ — конечная группа, и сумма всех ее элементов порядка $m \in \mathbb{N}$ есть σ. Покажите, что $2\sigma = 0$; если $m > 2$, то $\sigma = 0$; а если $m = 2$ и G — циклическая группа, то $\mathrm{ord}\, \sigma = 2$.

31. Пусть $G_1, \ldots, G_t$ — абелевы группы порядков, соответственно $m_1, \ldots, m_t \in \mathbb{N}$. Докажите, что $G_1 \otimes \ldots \otimes G_t$ — циклическая группа тогда и только тогда, когда $G_1, \ldots, G_t$ — циклические группы и числа $m_1, \ldots, m_t$ попарно взаимно просты.

32. Пусть $\rho(G)$ — минимальное число образующих группы G. Покажите, что если $\rho(G_i) = m_i$, $i \in \overline{1,t}$, то $\rho(G_1 \otimes \ldots \otimes G_t) \leqslant m_1 + \ldots + m_t$, и последнее неравенство может быть строгим и может обращаться в равенство. Если $G_1, \ldots, G_t$ — конечные группы попарно взаимно простых порядков, то $\rho(G_1 \otimes \ldots \otimes G_t) = \max\{m_1, \ldots, m_t\}$.

33. Докажите, что если p — минимальный простой делитель порядка конечной группы G, то $\rho(G) \leqslant \log_p |G|$, и указанная оценка достижима.

34. Докажите, что сопряженные элементы группы имеют одинаковые порядки, но обратное утверждение неверно.

35. Покажите, что центр конечной неабелевой группы есть подгруппа не простого индекса.

36. Опишите все конечные группы, разбивающиеся на 2 класса сопряженных элементов.

37. Подгруппы A и B группы $(G, \cdot)$ называются *сопряженными*, если $B = g^{-1}Ag$ для некоторого $g \in G$. Докажите, что число подгрупп группы G, сопряженных с A, равно $|G : N_G(A)|$.

38. Докажите, что группа диэдра D_n порождается подстановками

$$g = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \end{pmatrix} \quad \text{и} \quad h = \begin{pmatrix} 1 & 2 & \dots & n \\ n & n-1 & \dots & 1 \end{pmatrix}$$

и не коммутативна. Покажите, что $D_3 = S_3$, а D_4 содержит подгруппу Клейна K_4.

39. Докажите, что группа G движений тетраэдра есть A_4, и опишите движения, составляющие в G подгруппу Клейна K_4.

40. Докажите, что группы движений куба и октаэдра изоморфны.

41. Опишите возможные порядки элементов и экспоненты групп S_n, $n \leqslant 6$, перечислите их классы сопряженных элементов.

42. Пусть $g = (a_0, a_1, \dots, a_{k-1})$ — цикл длинны k, $m \in \mathbb{N}$ и $d = (m, k)$. Докажите, что g^m есть произведение d независимых циклов длины $l = k/d$:

$$g = \prod_{s=0}^{d-1} (a_s, a_{r_k(s+m)}, \dots, a_{r_k(s+(l-1)m)}),$$

где $r_k(x)$ — остаток от деления x на k.

43. Докажите, что для подстановки $g \in S_n$, имеющей цикловую структуру $[1^{t_1}, 2^{t_2}, \dots, n^{t_n}]$, и для любого простого $p \in \mathbb{N}$ уравнение $x^p = g$ разрешимо в S_n тогда и только тогда, когда

$$\forall\, k \in \overline{1,n}: \;\; p \mid k \;\; \Rightarrow \;\; p \mid t_k.$$

44. Докажите, что $A_n = \langle (1,2,3), (1,2,4), \dots, (1,2,n) \rangle$.

45. Покажите, что если в группе $G < S_n$ есть нечетная подстановка, то множество H всех ее четных подстановок есть подгруппа индекса 2.

46. Пусть C_k — множество всех циклов длины $k > 1$ в S_n. Найдите $|C_k|$. Покажите, что $\langle C_k \rangle = A_n$, если k нечетно, и $\langle C_k \rangle = S_n$, если k четно.

47. В условиях предыдущей задачи покажите, что для некоторого $l \in \mathbb{N}$ выполняется равенство $S_n = C_2^1 \cup C_2^2 \cup \ldots \cup C_2^l$, и найдите наименьшее l с этим свойством.

48. Докажите, что подстановки $g = (0, 1, \ldots, n-1)$ и $h = (0, a)$ на множестве $\overline{0, n-1}$ порождают группу $S(\overline{0, n-1})$ тогда и только тогда, когда $(a, n) = 1$. (При условии $(a, n) = m > 1$ покажите, что любая подстановка $f \in \langle g, h\rangle$ обладает свойством

$$\forall\, \alpha, \beta \in \mathbb{Z}_n \ (\alpha \equiv \beta \,(\mathrm{mod}\, m) \ \Rightarrow \ f(\alpha) \equiv f(\beta) \,(\mathrm{mod}\, m)).)$$

49. Опишите с точностью до изоморфизма все группы порядков 2–7.

50. Пусть $g = (0, 1, \ldots, n-1)$ — подстановка на кольце $\mathbb{Z}_n$. Докажите, что нормализатор подгруппы $G = \langle g\rangle$ в группе $S(\mathbb{Z}_n)$ есть $AGL(1, \mathbb{Z}_n)$.

51. Пусть $g \in S_n$ и $\operatorname{ord} g = m$. Докажите равенство $|N_{S_n}(\langle g\rangle)| = \varphi(m) \cdot |N_{S_n}(g)|$. Для этого докажите соотношения

$$h \in N_{S_n}(\langle g\rangle) \ \Leftrightarrow \ h^{-1}gh \in \langle g\rangle \ \Leftrightarrow \ h^{-1}gh = g^k, \ k \in \mathbb{Z}_m^*.$$

52. Докажите, что при $n \geqslant 3$ центр группы S_n тривиален.

53. Пусть f и g — подстановки из $S(\mathbb{Z})$, определяемые следующими условиями: $f = (0, 1)$, $g(a) = a+1$ для $a \in \mathbb{Z}$. Докажите, что в группе $G = \langle f, g\rangle$ лежит множество $H = \{h \in S(\mathbb{Z}) : \, |\operatorname{mob} h| < \infty\}$, и H — подгруппа в G, не имеющая конечной системы образующих.

54. Покажите, что отношение «быть нормальным делителем» на множестве всех подгрупп группы S_4 не транзитивно.

55. Докажите, что если $H < G$, то $N_G(H)$ — наибольшая подгруппа G, в которой H является нормальным делителем, т. е. если $H < K < G$, то выполняется тождество $H \lhd K \ \Leftrightarrow \ K < N_G(H)$.

56. Докажите, что если $H \lhd S_n$ и в H есть транспозиция, то $H = S_n$.

57. Докажите, что для подгруппы H группы G следующие утверждения эквивалентны:

а) $H \lhd G$;

б) H — объединение некоторых классов сопряженных элементов из G;

в) $H = \langle S\rangle$, где S — объединение некоторых классов сопряженных элементов из G.

58. Докажите, что для подгрупп A и B группы $(G, \cdot)$ эквивалентны утверждения:

а) $G = A \dot{\times} B$;

б) $G = AB$, $A \lhd G$, $B \lhd G$, $A \cap B = e$.

59. Докажите следующие соотношения:

а) $(\mathbb{C}^*/\mathbb{R}_{>0}, \cdot) \cong \Gamma$; б) $\mathbb{C}^*/\Gamma \cong \mathbb{R}^*_{>0}$; в) $\Gamma/\Gamma_m \cong \Gamma$;

г) $m\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}_n$; д) $S_n/A_n \cong \mathbb{Z}_2$; е) $S_4/K_4 \cong S_3$;

ж) $\mathbb{Q}/\mathbb{Z} \cong T(\mathbb{C}^*)$.

60. Докажите, что если A, B — подгруппы группы G и $G = A \dot{\times} B$, то $A \lhd G$ и $G/A \cong B$.

61. Покажите, что если G — не абелева группа, то $G/C(G)$ — не циклическая группа.

62. Пусть $H \lhd G$, $|H| = m$, $|G : H| = n$ и $(m, n) = 1$. Докажите, что в G нет других подгрупп порядка m.

63. *Коммутатором* элементов g, h группы $(G, \cdot)$ называется элемент $[g, h] = g^{-1}h^{-1}gh$. *Коммутантом группы* G называется ее подгруппа $[G, G]$, порожденная коммутаторами всех пар элементов из G. Докажите, что $[G, G] \lhd G$, и если $H \lhd G$, то группа G/H абелева тогда и только тогда, когда $[G, G] \subset H$.

64. Докажите, что $[S_n, S_n] = A_n$.

65. Пусть $\varphi\colon G \to K$ — гомоморфизм групп и $H \lhd G$. Докажите, что $\varphi(H) \lhd \varphi(G)$ и $\varphi(G)/\varphi(H) \cong G/H \operatorname{Ker}\varphi$.

66. Пусть $A \lhd B \lhd (G, \cdot)$ и $H \lhd G$. Докажите, что

$$AH \lhd BH \quad \text{и} \quad BH/AH \cong B/A(B \cap H).$$

67. Используя теоремы Силова и теорему Бернсайда, докажите, что все не коммутативные группы порядка $n < 60$ не просты. Докажите это же, не пользуясь теоремой Бернсайда.

68. Вычислите порядок группы $PSL(m, q)$ и докажите, что группы $PSL(2, 2)$ и $PSL(2, 3)$ не являются простыми.

69. Докажите, что любая группа порядка $2p$, где p — простое, не проста.

70. Докажите, что любая группа порядка 15 коммутативна и изоморфна $\mathbb{Z}_{15}$.

71. Пусть A, B — группы и $A_1 < A$, $B_1 < B$. Покажите, что $G = A_1 \otimes B_1$ — подгруппа $A \otimes B$. Докажите, что если A и B — конечные группы, то в $A \otimes B$ все подгруппы G имеют указанный вид тогда и только тогда, когда $(|A|, |B|) = 1$.

72. Пусть A, B — конечные подгруппы абелевой группы $(G, +)$. Докажите, что если $(|A|, |B|) = 1$, то для любой подгруппы $C < G$ выполняется равенство $C \cap (A + B) = (C \cap A) + (C \cap B)$, а если $A \cap B = 0$, но $(|A|, |B|) \neq 1$, то существует подгруппа $C < G$, для которой это равенство неверно.

73. Пусть p — наименьший простой делитель порядка конечной группы G, $H < G$ и $|G : H| = p$. Докажите, что $H \lhd G$.

74. По теореме 34 все циклы длины 3 сопряжены в S_n. Покажите, что при $n > 4$ они сопряжены и в A_n, а при $n \leqslant 4$ могут быть как сопряжены, так и не сопряжены.

75. В группе S_8 опишите все решения уравнения $x^{-1}gx = h$ и найдите их число, если

а) $g = \begin{pmatrix} 1&2&3&4&5&6&7&8 \\ 2&3&1&5&6&4&8&7 \end{pmatrix}$, $h = \begin{pmatrix} 1&2&3&4&5&6&7&8 \\ 7&8&1&2&6&5&3&4 \end{pmatrix}$;

б) $g = \begin{pmatrix} 1&2&3&4&5&6&7&8 \\ 5&4&2&3&1&8&7&6 \end{pmatrix}$, $h = \begin{pmatrix} 1&2&3&4&5&6&7&8 \\ 7&2&1&6&8&4&3&5 \end{pmatrix}$;

в) $g = (1,4)(2,5)(3,6)$, $h = (1,2)(3,4)(7,8)$.

76. Докажите, что множество общих решений уравнений $x^{-1}gx = h$ и $x^{-1}g_1x = h_1$ либо пусто, либо является правым смежным классом группы S_n по подгруппе $N_{S_n}(g) \cap N_{S_n}(g_1)$.

77. В группе S_{15} найдите число решений для каждого из уравнений $x^{-1}gx = h$ и $x^{-1}g_1x = h_1$, где

$$g = h = (1,2,3,4,5)(6,7)(8,9)(10,11),$$
$$g_1 = (1,2,3)(4,5,6)(7,8,9)(10,11,12)(13,14,15),$$
$$h_1 = (1,4,7)(2,10,13)(3,6,14)(5,8,11)(9,12,15).$$

Докажите, что у рассматриваемых уравнений нет общих решений.

78. В группе S_{15} найдите число решений для каждого из уравнений $x^{-1}gx = h$ и $x^{-1}g_1x = h_1$, где

$$g = h = (1,2,3,4,5)(6,7,8,9,10)(11,12,13,14,15),$$
$$g_1 = h_1 = (1,2,3)(4,5,6)(7,8,9)(10,11,12)(13,14,15).$$

Докажите, что у этих уравнений имеется единственное общее решение.

Глава 12

КОНЕЧНЫЕ АБЕЛЕВЫ ГРУППЫ

В предыдущей главе читатель уже заметил, что условие коммутативности группы существенно облегчает изучение многих ее свойств. Это естественно наводит на мысль о целесообразности отдельного систематического изучения коммутативных групп. Кроме того, абелевыми группами настолько «пропитана» вся алгебра, что изучение их строения необходимо не только в теоретико-групповых, но и в общематематических интересах. В настоящее время теория абелевых групп развита весьма глубоко, однако полного описания их строения не существует. В данной главе дается полное описание строения лишь конечных абелевых групп.

§ 1. КАНОНИЧЕСКОЕ РАЗЛОЖЕНИЕ КОНЕЧНОЙ АБЕЛЕВОЙ ГРУППЫ

Согласно теореме 18 главы 11 любая конечная циклическая группа либо примарна, либо есть прямая сумма примарных циклических подгрупп. Этот результат следующим образом обобщается до основной теоремы о строении конечных абелевых групп.

Теорема 1. *Любая конечная абелева группа $(G, +)$ либо является примарной циклической группой, либо раскладывается в прямую сумму примарных циклических подгрупп*:

$$G = \langle \xi_1 \rangle \dotplus \ldots \dotplus \langle \xi_t \rangle, \quad \operatorname{ord} \xi_i = p_i^{k_i}, \quad p_1, \ldots, p_t \text{ — простые числа.} \tag{1}$$

Заметим, что числа $p_1, \ldots, p_t$ в разложении (1), вообще говоря, не являются попарно различными.

□ Рассмотрим сначала случай, когда G — примарная группа. Напомним, что согласно утверждению 4 главы 11 в группе G существует элемент, порядок которого равен ее экспоненте. Для произвольного $d \in \mathbb{N}$ обозначим через $G(d)$ подгруппу группы G вида

$$G(d) = \{g \in G : \ dg = 0\}.$$

Лемма 2. *Пусть G есть p-группа, $\exp G = p^m$, и ξ — элемент порядка p^m из G. Тогда следующие утверждения эквивалентны*:

(а) $G = \langle \xi \rangle$ — *циклическая группа*;

(б) $G(p)$ — *циклическая группа*;

(в) $G(p) \subseteq \langle \xi \rangle$.

□ (а)⇒(б) По теореме 9(в) главы 11 любая подгруппа циклической группы G — циклическая группа.

(б)⇒(в) Так как $\exp G(p) = p$ и $G(p)$ — циклическая группа, то она порождается любым элементом порядка p из группы G. Поскольку $\operatorname{ord} p^{m-1}\xi = p$, то $G(p) = \langle p^{m-1}\xi\rangle \subseteq \langle\xi\rangle$.

(в)⇒(а) Допустим, что $G \neq \langle\xi\rangle$. Выберем в $G \setminus \langle\xi\rangle$ элемент g наименьшего возможного порядка. Тогда $\operatorname{ord} pg < \operatorname{ord} g \leqslant p^m$ и, следовательно, $pg \in \langle\xi\rangle$, т. е. $pg = l\xi$ для некоторого $l \in \mathbb{N}$. Так как $\operatorname{ord} l\xi < p^m = \operatorname{ord}\xi$, то $p \mid l$, скажем $l = pk$, $k \in \mathbb{N}$. Тогда $p(g - k\xi) = 0$ и $g - k\xi \in G(p) \subseteq \langle\xi\rangle$. Отсюда $g \in \langle\xi\rangle$. Противоречие. □

Лемма 3. *В условиях леммы* 2 *существует подгруппа* $H < (G, +)$ *такая, что* $G = \langle\xi\rangle \dotplus H$.

□ Пусть $|G| = p^s$. Докажем лемму индукцией по параметру s. Если $s = 1$, то утверждение очевидно: $G = \langle\xi\rangle$ и $H = 0$. Пусть $r > 1$ и лемма верна для всех групп с условием $s < r$. Докажем лемму для случая, когда $s = r$. Если $G = \langle\xi\rangle$, то лемма верна. Пусть $G \neq \langle\xi\rangle$. Тогда по лемме 2 существует элемент $a \in G(p) \setminus \langle\xi\rangle$. Рассмотрим факторгруппу $\overline{G} = G/\langle a\rangle$ и канонический эпиморфизм $\varphi\colon G \to \overline{G}$. Для любого $g \in G$ положим $\overline{g} = \varphi(g)$. Заметим, что $\operatorname{ord}\overline{\xi} = p^m$. Действительно, в противном случае $p^{m-1}\overline{\xi} = \overline{0}$, т. е. $p^{m-1}\xi \in \langle a\rangle$, и так как $\operatorname{ord} p^{m-1}\xi = p = \operatorname{ord} a$, то $\langle a\rangle = \langle p^{m-1}\xi\rangle \subseteq \langle\xi\rangle$, что невозможно. Отсюда следует, что $\exp\overline{G} = p^m$, поскольку $\operatorname{ord}\overline{\xi} \leqslant \exp\overline{G} \leqslant \exp G = p^m$.

Таким образом, группа $\overline{G}$ и элемент $\overline{\xi}$ удовлетворяют условию леммы 2, и так как $|\overline{G}| = p^{s-1} < p^r$, то по предположению индукции существует подгруппа $\overline{H} \leqslant \overline{G}$ такая, что $\overline{G} = \langle\overline{\xi}\rangle \dotplus \overline{H}$. Пусть $H = \varphi^{-1}(\overline{H})$. Покажем, что $G = \langle\xi\rangle \dotplus H$.

Для любого элемента $g \in G$ имеем: $\overline{g} = l\overline{\xi} + \overline{h}$ при подходящих $l \in \mathbb{N}_0$ и $h \in H$. Тогда $g - l\xi - h = ta$ для некоторого $t \in \mathbb{N}_0$, и так как $ta \in \operatorname{Ker}\varphi \subseteq \varphi^{-1}(\overline{H}) = H$, то $g = l\xi + (h + ta) \in \langle\xi\rangle + H$, т. е. $G = \langle\xi\rangle + H$. Последняя сумма прямая, так как если $h \in \langle\xi\rangle \cap H$, то $\overline{h} \in \langle\overline{\xi}\rangle \cap \overline{H} = \overline{0}$. Следовательно, $h \in \langle a\rangle$ и при условии $h \neq 0$ имеем: $\operatorname{ord} h = p$ и $\langle a\rangle = \langle h\rangle \subseteq \langle\xi\rangle$, что невозможно. □

Отсюда очевидной индукцией по порядку группы выводится

Лемма 4. *Любая конечная абелева* p*-группа либо является циклической, либо раскладывается в прямую сумму циклических подгрупп.*

Теперь доказательство теоремы 1 завершается следующим образом. По следствию теоремы 49 главы 11 конечная абелева группа G есть сумма своих силовских подгрупп, к каждой из которых применима лемма 4. □

Определение 1. Разложение (1), в котором слагаемые упорядочены так, что

$$(p_i \geqslant p_{i+1}) \ \ \& \ \ ((p_i = p_{i+1}) \ \Rightarrow \ (k_i \geqslant k_{i+1})), \quad i \in \overline{1,\, t-1}, \tag{2}$$

назовем *каноническим разложением* конечной абелевой группы G, а вектор $(p_1^{k_1}, \ldots, p_t^{k_t})$ — *типом этого разложения*.

Из примера 18 главы 11 и утверждения 16 главы 11 следует, что существование разложения (1) равносильно тому, что существует изоморфизм

$$G \cong \mathbb{Z}_{p_1^{k_1}} \oplus \ldots \oplus \mathbb{Z}_{p_t^{k_t}}, \tag{3}$$

который мы также будем называть каноническим разложением группы G.

Пример 1. Пусть $G = \mathbb{Z}_{12} \oplus \mathbb{Z}_{18}$. Так как

$$\mathbb{Z}_{12} = 4\mathbb{Z}_{12} + 3\mathbb{Z}_{12} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_4, \quad \mathbb{Z}_{18} = 2\mathbb{Z}_{18} + 9\mathbb{Z}_{18} \cong \mathbb{Z}_9 \oplus \mathbb{Z}_2,$$

то каноническое разложение (3) группы G имеет вид

$$G \cong \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2,$$

а ее каноническое разложение в прямую сумму подгрупп можно выписать следующим образом:

$$G = \langle (0,2) \rangle \dotplus \langle (4,0) \rangle \dotplus \langle (3,0) \rangle \dotplus \langle (0,9) \rangle.$$

Заметим, что группа G имеет несколько различных канонических разложений. Читателю предлагается проверить, что каноническим для G является также, например, разложение

$$G = \langle (4,2) \rangle \dotplus \langle (4,6) \rangle \dotplus \langle (3,9) \rangle \dotplus \langle (0,9) \rangle.$$

§ 2. ТИП КОНЕЧНОЙ АБЕЛЕВОЙ ГРУППЫ

Хотя конечная абелева группа может иметь много различных канонических разложений, все они, тем не менее, имеют одинаковые числовые характеристики.

Теорема 5. *Любые два различных канонических разложения конечной абелевой группы G имеют равные типы.*

□ Суть доказательства состоит в том, что параметры произвольного канонического разложения группы G однозначно выражаются через параметры этой группы, не зависящие от выбора канонического разложения.

1. Рассмотрим сначала случай, когда G является p-группой. Пусть $\exp G = p^k$. Тогда любое каноническое разложение G имеет вид

$$G = \langle \xi_1 \rangle \dotplus \ldots \dotplus \langle \xi_t \rangle, \quad \operatorname{ord} \xi_i = p^{k_i}, \quad k = k_1 \geqslant k_2 \geqslant \ldots \geqslant k_t. \tag{4}$$

Для любого $s \in \mathbb{N}_0$ положим $p^s G = \{p^s g \colon g \in G\}$. Очевидно, $p^s G$ — подгруппа группы G, и параметр $|p^s G|$ не зависит от разложения (4). Пусть $r = r(s)$ — количество показателей k_i в (4) строго больших, чем s:

$$k_1 \geqslant \ldots \geqslant k_r > s \geqslant k_{r+1} \geqslant \ldots \geqslant k_t.$$

Лемма 6. *Если $r = r(s) = 0$ (т. е. $s \geqslant k_1$), то $p^s G = 0$. Если $r > 0$, то группа $p^s G$ имеет каноническое разложение*

$$p^s G = \langle p^s \xi_1 \rangle \dotplus \ldots \dotplus \langle p^s \xi_r \rangle, \quad \operatorname{ord} p^s \xi_i = p^{k_i - s}, \quad i \in \overline{1, r}. \tag{5}$$

□ Произвольный элемент $g \in G$ имеет вид $g = c_1\xi_1 + \ldots + c_t\xi_t$. Отсюда $p^s g = c_1(p^s\xi_1) + \ldots + c_t(p^s\xi_t)$, и так как $p^s\xi_i = 0$ для $i \in \overline{r+1, t}$, то $p^s g = 0$, если $s \geqslant k_1$, а в случае $s < k_1$ элемент $p^s g$ принадлежит подгруппе $H = \langle p^s\xi_1\rangle + \ldots + \langle p^s\xi_r\rangle$, т. е. $p^s G \subseteq H$.

Обратное включение очевидно. Остается заметить, что выписанное разложение для $H = p^s G$ есть прямая сумма ввиду (4). □

Из (5) следует равенство

$$\log_p |p^s G| = k_1 + \ldots + k_{r(s)} - sr(s) \text{ для } s \in \overline{0,\, k_1 - 1}. \tag{6}$$

Пусть $m(s)$ — количество слагаемых порядка p^s в разложении (4). Очевидно, тип разложения (4) однозначно определяется набором чисел $m(1)$, $\ldots$, $m(k)$. Остается показать, что эти числа однозначно определяются порядками $|G|$, $|pG|$, $\ldots$, $|p^{k-1}G|$. Ясно, что $m(s) = r(s-1) - r(s)$ для $s \in \overline{1, k}$. Из (6) имеем

$$\log_p |p^{s-1}G| = k_1 + \ldots + k_{r(s)} + k_{r(s)+1} + \ldots + k_{r(s-1)} - (s-1)r(s-1).$$

Отсюда, ввиду равенств $k_{r(s)+1} = \ldots = k_{r(s-1)} = s$, имеем

$$\begin{aligned}\log_p |p^{s-1}G| &= k_1 + \ldots + k_{r(s)} + s(r(s-1) - r(s)) - (s-1)r(s-1) = \\ &= k_1 + \ldots + k_{r(s)} - sr(s) + r(s-1).\end{aligned}$$

Следовательно,

$$\log_p |p^{s-1}G| - \log_p |p^s G| = r(s-1), \quad s \in \overline{1, k},$$

и окончательно

$$m(s) = \log_p |p^{s-1}G| + \log_p |p^{s+1}G| - 2\log_p |p^s G|, \quad s \in \overline{1, k}.$$

2. Пусть теперь G — произвольная конечная абелева группа, и ее порядок n имеет каноническое разложение $n = q_1^{m_1} \ldots q_r^{m_r}$. Тогда по теореме 49 главы 11 $G(q_i^{m_i}) = G^{(q_i)}$ — единственная силовская q_i-подгруппа группы G, и

$$G = G(q_1^{m_1}) \dotplus \ldots \dotplus G(q_r^{m_r}).$$

Произвольное каноническое разложение (1) группы G можно более детально записать в виде:

$$G = \langle\xi_{11}\rangle \dotplus \ldots \dotplus \langle\xi_{1t_1}\rangle \dotplus \langle\xi_{21}\rangle \dotplus \ldots \dotplus \langle\xi_{rt_r}\rangle, \tag{7}$$

где $\operatorname{ord}\xi_{is} = q_i^{k_{is}}$, $i \in \overline{1, r}$, $s \in \overline{1, t_i}$;

$$t_1 + \ldots + t_r = t; \quad q_1 > \ldots > q_r, \quad k_{i1} \geqslant \ldots \geqslant k_{it_i} \text{ для } i \in \overline{1, r}.$$

Здесь $q_1, \ldots, q_r$ — все различные простые числа из совокупности $p_1, \ldots, p_t$ в (1). Из (7) ясно, что

$$n = \prod_{i=1}^{r} q_i^{k_{i1} + \ldots + k_{it_i}}.$$

Следовательно, $k_{i1} + \ldots + k_{it_i} = m_i$, и, независимо от выбора канонического разложения (7), сумма $\langle \xi_{i1} \rangle \dotplus \ldots \dotplus \langle \xi_{it_i} \rangle$ всех его примарных слагаемых, принадлежащих простому основанию q_i, есть подгруппа порядка $q_i^{m_i}$, т. е. единственная силовская q_i-подгруппа $G(q_i^{m_i})$ группы G. В пункте 1 доказано, что тип канонического разложения

$$G(q_i^{m_i}) = \langle \xi_{i1} \rangle \dotplus \ldots \dotplus \langle \xi_{it_i} \rangle$$

однозначно определяется группой $G(q_i^{m_i})$, т. е. группой G. Отсюда следует, что и тип всего разложения (7) определяется группой G однозначно. □

Определение 2. Тип канонического разложения (1) конечной абелевой группы G будем называть *типом группы* G и обозначать

$$\operatorname{typ} G = (p_1^{k_1}, \ldots, p_t^{k_t}).$$

§ 3. ПЕРЕЧИСЛЕНИЕ КОНЕЧНЫХ АБЕЛЕВЫХ ГРУПП

Совокупность всех абелевых групп разбивается отношением изоморфизма на непересекающиеся классы изоморфных групп. Очевидно, для каждого $n \in \mathbb{N}$ существует лишь конечное число $T(n)$ различных классов изоморфных абелевых групп порядка n. Явной формулы для вычисления $T(n)$ не найдено, однако полученные выше результаты позволяют подсчитать $T(n)$ в каждом конкретном случае.

Теорема 7. *Конечные абелевы группы G и H изоморфны тогда и только тогда, когда* $\operatorname{typ} G = \operatorname{typ} H$.

□ Пусть G имеет каноническое разложение (1) и $\varphi\colon G \to H$ — изоморфизм. Тогда H имеет разложение

$$H = \langle \varphi(\xi_1) \rangle \dotplus \ldots \dotplus \langle \varphi(\xi_t) \rangle,$$

и, так как $\operatorname{ord} \varphi(\xi_i) = \operatorname{ord} \xi_i$, то последнее есть каноническое разложение H, и $\operatorname{typ} H = \operatorname{typ} G$. Наоборот, если $\operatorname{typ} H = \operatorname{typ} G$, то

$$H \cong \mathbb{Z}_{p_1^{k_1}} \oplus \ldots \oplus \mathbb{Z}_{p_t^{k_t}} \cong G. \quad \square$$

Таким образом, $T(n)$ есть число возможных типов абелевых групп порядка n. С использованием описания (1) канонического разложения абелевой группы получаем следующий результат.

Теорема 8. *Если $n = q_1^{m_1} \ldots q_r^{m_r}$ — каноническое разложение числа n, то число $T(n)$ различных классов изоморфных абелевых групп порядка n равно числу различных наборов $\left(q_1^{k_{11}}, \ldots, q_1^{k_{1t_1}}, q_2^{k_{21}}, \ldots, q_r^{k_{rt_r}}\right)$ таких, что*

$$m_i = k_{i1} + \ldots + k_{it_i}, \quad k_{i1} \geqslant \ldots \geqslant k_{it_i} > 0, \quad i \in \overline{1,r}.$$

Определение 3. Представление натурального числа m в виде суммы набора невозрастающих натуральных чисел назовем *разбиением* числа m. Через $R(m)$ обозначим число различных разбиений m.

Следствие 1. *В обозначениях теоремы* 8 *число* $T(n)$ *не зависит от простых делителей* $q_1, \ldots, q_r$ *и удовлетворяет соотношениям*:

$$T(n) = T(q_1^{m_1}) \cdot \ldots \cdot T(q_r^{m_r}) = R(m_1) \cdot \ldots \cdot R(m_r).$$

Пример 2. Пусть $m = 36 = 3^2 \cdot 2^2$. Тогда $T(m) = T(36) = R(2) \cdot R(2)$, и так как $R(2) = 2$ (возможные разбиения: $2 = 2$ и $2 = 1 + 1$), то $T(36) = 4$, т. е. число классов изоморфных абелевых групп порядка 36 равно 4. Любая абелева группа порядка 36 изоморфна единственной из групп:

$$\begin{aligned}
&G_1 = \mathbb{Z}_9 \oplus \mathbb{Z}_4 \cong \mathbb{Z}_{36}, && \operatorname{typ} G = (3^2, 2^2);\\
&G_2 = \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4, && \operatorname{typ} G = (3, 3, 2^2);\\
&G_3 = \mathbb{Z}_9 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, && \operatorname{typ} G = (3^2, 2, 2);\\
&G_4 = \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, && \operatorname{typ} G = (3, 3, 2, 2).
\end{aligned}$$

Как уже отмечалось, явных формул для вычисления числа $R(m)$ не найдено. Методами теории функций комплексного переменного можно получить следующее асимптотическое равенство для $R(m)$:

$$R(m) \sim \frac{1}{4m\sqrt{3}}\, e^{\pi\sqrt{\frac{2m}{3}}} \quad \text{при} \quad m \to \infty,$$

где $f(n) \sim g(n)$ означает, что $\lim\limits_{n\to\infty} \dfrac{f(n)}{g(n)} = 1$.

Полезно заметить, что для любого простого p среди абелевых групп порядка p^n, $n \in \mathbb{N}$, всегда содержится циклическая группа порядка p^n, т. е. группа типа (p^n), и группа экспоненты p, т. е. группа типа $(p, \ldots, p)$, называемая *элементарной p-группой*.

§ 4. ХАРАКТЕРЫ КОНЕЧНЫХ АБЕЛЕВЫХ ГРУПП

Определение 4. *Характером* конечной абелевой группы G называется любой гомоморфизм группы G в мультипликативную группу $\mathbb{C}^*$ поля комплексных чисел.

Любая группа G имеет *тривиальный* характер, отображающий все ее элементы в число $1 \in \mathbb{C}$. Иногда этот характер называют также *главным*.

Для описания всех характеров группы $(G; \cdot)$ мы воспользуемся следующим из теоремы 1 фактом о возможности разложения любой конечной абелевой группы в прямое произведение циклических подгрупп. Пусть

$$G = G_1 \dot{\times} G_2 \dot{\times} \ldots \dot{\times} G_m \tag{8}$$

— одно из таких разложений, $|G_i| = n_i$ и $G_i = \langle g_i \rangle$, $i \in \overline{1, m}$. Если φ — гомоморфизм группы G в $\mathbb{C}^*$, то ограничение $\varphi_i = \varphi\big|_{G_i}$ есть гомоморфизм $\varphi_i \colon G_i \to \mathbb{C}^*$. Наоборот, если задан набор гомоморфизмов $\varphi_i \colon G_i \to \mathbb{C}^*$, $i \in \overline{1, m}$, то по нему естественным образом определяется гомоморфизм φ группы G в $\mathbb{C}^*$ такой, что $\varphi_i = \varphi\big|_{G_i}$: для элемента $g \in G$ вида

$$g = h_1 \cdot h_2 \cdot \ldots \cdot h_m,$$

где $h_i \in G_i$, $i \in \overline{1,m}$, полагаем

$$\varphi(g) = \varphi_1(h_1) \cdot \varphi_2(h_2) \cdot \ldots \cdot \varphi_m(h_m).$$

При этом различным наборам гомоморфизмов групп G_i будут соответствовать, очевидно, различные гомоморфизмы группы G. Таким образом, для описания всех характеров группы G достаточно описать все характеры циклических групп G_i. Если φ_i — гомоморфизм G_i в $\mathbb{C}^*$, то

$$\varphi_i(g_i)^{n_i} = \varphi_i(g_i^{n_i}) = \varphi_i(e) = 1,$$

поскольку $g_i^{n_i} = e$ — единица группы G_i. Следовательно, $\varphi_i(g_i)$ есть корень n_i-й степени из 1 в $\mathbb{C}$. Обратно, если ε — некоторый корень n_i-й степени из 1 в C, то равенства

$$\varphi_i(g_i^k) = \varepsilon^k, \tag{9}$$

$k \in \overline{0,\, n_i - 1}$, задают гомоморфизм группы G_i в $\mathbb{C}^*$. Следовательно, существует ровно n_i различных гомоморфизмов G_i в $\mathbb{C}^*$, и каждый из них определяется выбором корня ε из группы Γ_{n_i} всех корней n_i-й степени из 1 в $\mathbb{C}$. Из (9) видно также, что все характеры группы G_i являются гомоморфизмами в группу Γ_{n_i}. В итоге доказана

Теорема 9. *Пусть G — абелева группа порядка n, и (8) — любое ее разложение в прямое произведение циклических подгрупп. Тогда G имеет ровно n различных характеров, каждый характер χ определяется набором $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m)$, где ε_i — корень n_i-й степени из 1 в $\mathbb{C}$, $i \in \overline{1,m}$, и задается равенствами*

$$\chi(g_1^{k_1} g_2^{k_2} \ldots g_m^{k_m}) = \varepsilon_1^{k_1} \varepsilon_2^{k_2} \ldots \varepsilon_m^{k_m}, \tag{10}$$

$k_i \in \overline{0,\, n_i - 1}$, $i \in \overline{1,m}$.

Множество всех характеров группы G обозначим через $\widehat{G}$.

Выберем теперь в каждой из групп Γ_{n_i} первообразный корень ω_i, $i \in \overline{1,m}$. Тогда каждый из корней ε_i из (10) можно будет записать в виде $\varepsilon_i = \omega_i^{t_i}$, где $t_i \in \overline{0,\, n_i - 1}$. В итоге набор $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m)$ однозначно определяется набором целых чисел $(t_1, t_2, \ldots, t_m)$, где $t_i \in \overline{0, n_i - 1}$, $i \in \overline{1,m}$. Соответствующий этому набору характер обозначим через $\chi_{t_1,t_2,\ldots,t_m}$. Равенство (10) теперь примет вид

$$\chi_{t_1,t_2,\ldots,t_m}\left(\prod_{i=1}^{m} g_i^{k_i}\right) = \prod_{i=1}^{m} \omega_i^{t_i k_i}.$$

Так как каждый элемент группы G однозначно представляется в виде $g_1^{t_1} g_2^{t_2} \ldots g_m^{t_m}$, $t_i \in \overline{0,\, n_i - 1}$, $i \in \overline{1,m}$, то в итоге мы имеем биективное отображение σ группы G на множество $\widehat{G}$ всех ее комплексных характеров:

$$\sigma(g_1^{t_1} g_2^{t_2} \ldots g_m^{t_m}) = \chi_{t_1,t_2,\ldots,t_m}. \tag{11}$$

В связи с этим характеры естественно проиндексировать не наборами целых чисел, а элементами группы G, обозначив

$$\chi_{t_1,t_2,\ldots,t_m} = \chi_g,$$

где $g = g_1^{t_1} g_2^{t_2} \ldots g_m^{t_m}$. Тогда равенство (10) можно записать в следующем виде:

$$\chi_{g_1^{t_1} g_2^{t_2} \dots g_m^{t_m}} \left(\prod_{i=1}^{m} g_i^{k_i} \right) = \prod_{i=1}^{m} \omega_i^{t_i k_i}, \tag{12}$$

а равенство (11) — в виде $\sigma(g) = \chi_g$, $g \in G$.

На множестве $\widehat{G}$ всех характеров группы G можно определить операцию умножения, положив для $\varphi, \psi \in \widehat{G}$ и $g \in G$:

$$(\varphi \cdot \psi)(g) = \varphi(g) \cdot \psi(g).$$

Так как G — абелева группа, то $\varphi \cdot \psi$ также является гомоморфизмом группы G в $\mathbb{C}^*$. В результате мы имеем группоид $(\widehat{G}, \cdot)$. Из равенства (12) сразу следует, что биекция σ является изоморфизмом группы G на группоид $\widehat{G}$, и значит $\widehat{G}$ — тоже группа. В итоге доказана

Теорема 10. *Характеры конечной абелевой группы G образуют группу $\widehat{G}$ относительно операции умножения характеров, и эта группа изоморфна группе G.*

Учитывая, что $\widehat{G}$ — группа, определим порядок характера χ группы G как порядок элемента в группе $\widehat{G}$. Характер χ_e порядка 1, т. е. равный тождественно единице, является единицей группы $\widehat{G}$.

Определение 5. Пусть $\chi \in \widehat{G}$. Отображение $\overline{\chi}\colon G \to \mathbb{C}^*$, определенное по правилу $\overline{\chi}(g) = \overline{\chi(g)}$, где $\overline{\chi(g)}$ — число, сопряженное с $\chi(g)$ в $\mathbb{C}$, называется *характером, сопряженным с χ*.

Нетрудно заметить, что определение сопряженного характера корректно ($\overline{\chi}$ действительно лежит в $\widehat{G}$). Более того, так как значения характеров являются в $\mathbb{C}$ корнями из 1, а число, обратное к корню из единицы, совпадает с сопряженным к исходному, то характер χ^{-1}, обратный к χ в группе $\widehat{G}$, совпадает с $\overline{\chi}$.

Непосредственно из (12) следует

Теорема 11. *При указанной выше нумерации характеров группы G элементами из G имеет место соотношение двойственности для характеров*:

$$\forall\, a, b \in G\colon\ \chi_a(b) = \chi_b(a). \tag{13}$$

Следствие. *Если $a, b \in G$, $a \neq b$, то найдется такой характер $\chi \in \widehat{G}$, что $\chi(a) \neq \chi(b)$.*

Действительно, в противном случае мы бы имели $\chi_c(a) = \chi_c(b)$, или, в силу (13), $\chi_a(c) = \chi_b(c)$ для всех $c \in G$, т. е. $\chi_a = \chi_b$, что противоречит условию $a \neq b$.

Приведем еще ряд менее очевидных свойств характеров.

Теорема 12. *Для любых двух элементов a, b группы G выполняются равенства*

$$\sum_{c \in G} \chi_a(c)\, \overline{\chi}_b(c) = |G| \cdot \delta_{a,b}, \tag{14}$$

$$\sum_{c\in G}\chi_c(a)\,\overline{\chi}_c(b)=|G|\cdot\delta_{a,b},\tag{15}$$

где $\delta_{a,b}=\begin{cases}1, & \text{если } a=b,\\ 0, & \text{если } a\neq b\end{cases}$ *— символ Кронекера.*

Равенства (14) и (15) называются соответственно первым и вторым *соотношениями ортогональности* для характеров группы G.

□ В силу соотношения (13) доказать достаточно лишь одно из равенств (14), (15). Докажем (14). При $a=b$ равенство (14) выполняется, поскольку для любого $c\in G$

$$\chi_a(c)\cdot\overline{\chi}_a(c)=|\chi_a(c)|^2=1.$$

Пусть $a\neq b$, $a=\prod\limits_{i=1}^{m}g_i^{t_i}$, $b=\prod\limits_{i=1}^{m}g_i^{s_i}$, $c=\prod\limits_{i=1}^{m}g_i^{k_i}$, где $t_i,s_i,k_i\in\overline{0,\,n_i-1}$. Тогда, используя равенство (12) и соотношение $\overline{\chi}_a(c)=\chi_a(c)^{-1}$, получим:

$$\sum_{c\in G}\chi_a(c)\overline{\chi}_b(c)=\sum_{k_1,\ldots,k_m}\prod_{i=1}^{m}\omega_i^{t_ik_i}\cdot\prod_{i=1}^{m}\omega_i^{-s_ik_i}=$$

$$=\sum_{k_1,\ldots,k_m}\prod_{i=1}^{m}\omega_i^{r_ik_i}=\prod_{i=1}^{m}\Bigl(\sum_{k_i=0}^{n_i-1}\omega_i^{r_ik_i}\Bigr),$$

где $r_i=t_i-s_i$, $i\in\overline{1,m}$. Так как $a\neq b$, то найдется такое $j\in\overline{1,m}$, что $t_j\neq s_j$. Тогда $r_j\not\equiv 0\,(\mathrm{mod}\,n_j)$, и потому $\omega_j^{r_j}\neq 1$. Значит,

$$\sum_{k_j=0}^{n_j-1}\omega_j^{r_jk_j}=\frac{\omega_j^{r_jn_j}-1}{\omega_j^{r_j}-1}=0,$$

и равенство (14) верно. □

Из (14), (15) при $b=e$ получаем

Следствие. *Для любого $a\in G$ выполняются равенства*

$$\sum_{c\in G}\chi_a(c)=\sum_{c\in G}\chi_c(a)=|G|\cdot\delta_{a,e}.$$

Характеры конечных полей обсуждаются в § 6 главы 22.

ЗАДАЧИ

1. Опишите все конечные абелевы группы, в которых любая собственная подгруппа — циклическая.

2. Пусть G — конечная абелева группа с каноническим разложением (7). Докажите, что минимальная мощность системы образующих группы G есть $\rho(G)=\max\{t_1,\ldots,t_r\}$.

3. Назовем два канонических разложения абелевой группы G (в прямую сумму подгрупп) эквивалентными, если они различаются лишь перестановкой слагаемых. Опишите все классы эквивалентных канонических разложений для групп $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\mathbb{Z}_3 \oplus \mathbb{Z}_3$, $\mathbb{Z}_6 \oplus \mathbb{Z}_2$, $\mathbb{Z}_p \oplus \mathbb{Z}_p$ (p — простое). Докажите, что любые два канонических разложения группы G эквивалентны тогда и только тогда, когда G — циклическая группа.

4. При каких условиях на $n \in \mathbb{N}$ существует ровно k классов изоморфных абелевых групп порядка n, где $k \in \{1, 2, 3, 4\}$?

5. Пусть $N(n, m)$ — число классов изоморфных абелевых групп порядка n с экспонентой m. Докажите, что

а) $N(n, m) > 0$ тогда и только тогда, когда $m \mid n$ и каждый простой делитель p числа n делит m;

б) $N(n, m) = 1$ тогда и только тогда, когда выполняются условия пункта а) и для каждого простого p, делящего n, либо p^2 не делит m, либо p^2 не делит $\dfrac{n}{m}$.

6. Пусть G — абелева группа порядка n,

$$\operatorname{typ} G = (p_1^{n_{11}}, \ldots, p_1^{n_{1t_1}}, p_2^{n_{21}}, \ldots, p_s^{n_{st_s}})$$

и для каждого $i \in \overline{1, s}$ выполняются соотношения

$$n_{i1} = n_{i2} = \ldots = n_{ik_i} > n_{ik_{i+1}} \geqslant \ldots \geqslant n_{it_i}.$$

Докажите, что $\exp G = m = p_1^{n_{11}} p_2^{n_{21}} \ldots p_s^{n_{s1}}$, и число элементов порядка m в группе G равно $n\left(1 - \left(\dfrac{1}{p_1}\right)^{k_1}\right) \cdot \ldots \cdot \left(1 - \left(\dfrac{1}{p_s}\right)^{k_s}\right)$.

7. Составьте таблицу характеров группы $\mathbb{Z}_6$.

Глава 13

ВЕКТОРНЫЕ ПРОСТРАНСТВА

Изучая множества с бинарными операциями, мы часто пользовались также возможностью «умножать» элементы рассматриваемого множества с операцией $*$ на элементы некоторого другого (!) множества по закону, определенным образом согласованному с операцией $*$. Например, в предыдущих главах определялись умножение матриц над кольцом R на элементы этого кольца и умножение элементов произвольной абелевой группы $(G, +)$ на целые числа. Такое умножение естественно назвать «внешней» операцией соответственно на $R_{m,n}$ и G, а бинарную операцию $+$ на $R_{m,n}$ и G — «внутренней».

Настоящая глава посвящена изучению одного из важнейших понятий математики — понятия векторного пространства, в определении которого используются и «внутренняя», и «внешняя» операции.

§ 1. ОПРЕДЕЛЕНИЕ ВЕКТОРНОГО ПРОСТРАНСТВА. БАЗИС ПРОСТРАНСТВА

Определение 1. Говорят, что на множестве L задана *внешняя операция* $\circ$ *умножения справа* на элементы множества K, если задано отображение

$$\circ\colon L \times K \to L.$$

Образ элемента $(l, k) \in L \times K$ при этом отображении называют *произведением* элемента l на элемент k и обозначают через $l \circ k$ (или, для краткости, через lk).

Понятие внешней операции обобщает понятие бинарной операции на L, при определении которой $K = L$.

Определение 2. Множество L с внутренней операцией $+$ сложения и внешней операцией $\circ$ умножения справа на элементы поля P называют *правым векторным пространством над полем* P, а также *правым линейным пространством*, если

1) $(L, +)$ — абелева группа;
2) для любых элементов α, $\beta \in L$ и a, $b \in P$ выполнены соотношения:
   а) $\alpha \circ (ab) = (\alpha \circ a) \circ b$ (закон ассоциативности);
   б) $\alpha \circ (a + b) = \alpha \circ a + \alpha \circ b$;
   в) $(\alpha + \beta) \circ a = \alpha \circ a + \beta \circ a$ (законы дистрибутивности);
   г) $\alpha \circ e = \alpha$, где e — единица поля P (закон унитарности).

Это векторное пространство обозначают через L_P, его элементы называют *векторами*, а элементы из P — *скалярами*.

Заметим, что в соотношениях б) и в) одним знаком $+$ обозначены две разные операции: операция сложения в поле P и операция сложения в группе L. Это не вызывает недоразумения, так как смысл операции $+$ бывает ясен из природы складываемых элементов.

Пример 1. Абелева группа $(P^n, +)$, элементы которой умножаются на элементы поля P по правилу

$$(a_1, \ldots, a_n) \circ a = (a_1 a, \ldots, a_n a),$$

есть правое векторное пространство над полем P (арифметическое пространство P^n, введенное в главе 7). Аналогично, $P^{(n)}$ — векторное пространство над полем P.

Пример 2. Абелева группа $(P_{m,n}, +)$ превращается в векторное пространство над полем P, если в качестве внешней операции взять обычное умножение матриц из $P_{m,n}$ на элементы поля P.

Пример 3. Множество $C[a, b]$ всех действительных функций, непрерывных на отрезке $[a, b]$, является векторным пространством над полем $\mathbb{R}$, если рассматривать обычное сложение функций и определить внешнее умножение как умножение функции на константу.

Аналогично правому векторному пространству можно определить и *левое векторное пространство*. Поскольку далее мы будем изучать только правые векторные пространства, то слово «правое» будем опускать. Часто вместо термина «векторное пространство» мы будем употреблять термин *пространство*, что не вызовет путаницы.

Рассмотрим некоторые простейшие свойства элементов векторного пространства. Через θ_L обозначим нейтральный элемент группы $(L, +)$ и назовем его *нулем векторного пространства* L_P, а через 0 обозначим нуль поля P (часто вместо θ_L будем писать просто θ).

Утверждение 1. *Для любых элементов $\alpha \in L_P$ и $a \in P$ справедливы соотношения*:
(а) $\alpha \circ 0 = \theta \circ a = \theta$;
(б) $(\alpha \circ a = \theta) \Rightarrow (\alpha = \theta$ *или* $a = 0)$;
(в) $(-\alpha) \circ a = \alpha \circ (-a) = -(\alpha \circ a)$;
(г) $(-\alpha) \circ (-a) = \alpha \circ a$.

□ Соотношения (а), (в) и (г) доказываются так же, как аналогичные свойства элементов кольца (теорема 8 главы 3). Докажем (б). Пусть $\alpha \circ a = \theta$. Если $a = 0$, то доказывать нечего. Если же $a \neq 0$, то в поле P существует элемент a^{-1}. Ввиду соотношений г) и а) определения 2 получаем цепочку равенств

$$\alpha = \alpha \circ e = \alpha \circ (aa^{-1}) = (\alpha \circ a) \circ a^{-1} = \theta \circ a^{-1}.$$

Отсюда в силу (а) $\alpha = \theta$. □

Замечание 1. Не всякая абелева группа $(L,+)$ может быть превращена в векторное пространство над данным полем P. Действительно, если $L \neq \theta$ и L_P — векторное пространство, то для любого $l \in L \setminus \{\theta\}$ множество $lP = \{l \circ a :\ a \in P\}$ есть подгруппа группы $(L,+)$, изоморфная группе $(P,+)$ (проверьте). Следовательно, если P — бесконечное поле, то группа L должна быть бесконечной, а если $P = \mathbb{Z}/p$, то порядок любого ненулевого элемента из $(L,+)$ должен быть равен p.

Для конечных (!) систем векторов произвольного пространства L_P точно так же, как и в арифметических пространствах $P^{(n)}$ и P^n, рассмотренных в главе 7, определяются понятия: линейная комбинация векторов, линейное соотношение между векторами, линейная выражаемость вектора через заданную систему векторов, линейно зависимая и линейно независимая система, базис (максимальная линейно независимая подсистема) системы векторов.

Обобщим некоторые из указанных понятий на бесконечные системы векторов.

Определение 3. Говорят, что

1) *вектор $\alpha \in L_P$ линейно выражается через* бесконечную *систему векторов S* пространства L_P, если он линейно выражается через какую-либо конечную подсистему системы S;

2) *система векторов S* пространства L_P *линейно выражается через систему векторов T* этого пространства, если каждый вектор из S линейно выражается через систему T.

Определение 4. Бесконечную систему векторов S пространства L_P называют *линейно зависимой*, если в ней существует хотя бы одна линейно зависимая конечная подсистема. В противном случае систему S называют *линейно независимой*.

Ясно, что любая подсистема линейно независимой системы сама линейно независима.

Пример 4. Кольцо многочленов $P[x]$ над полем P является векторным пространством над полем P относительно обычной операции сложения многочленов и внешней операции умножения, определенной равенством $f(x) \circ a = f(x)a$, где $f(x) \in P[x]$, $a \in P$. Система векторов e, x, x^2, ..., x^n, ... линейно независима, так как для любой ее конечной подсистемы x^{i_1}, ..., x^{i_k} равенство $x^{i_1}a_1 + \ldots + x^{i_k}a_k = 0$, $a_i \in P$, означает, по определению равенства многочленов, что $a_1 = \ldots = a_k = 0$. Ясно, что любой многочлен из $P[x]$ линейно выражается через эту систему.

Сформулируем и наметим доказательства некоторых утверждений, аналоги которых для конечных систем векторов арифметического пространства доказаны в главе 7.

Теорема 2 (критерий линейной зависимости). *Пусть S — произвольная система векторов пространства L_P. Если $|S| = 1$, то система S линейно зависима тогда и только тогда, когда она состоит из нулевого вектора. Если $|S| > 1$, то система S линейно зависима тогда и только тогда, когда в ней существует вектор, линейно выражающийся через систему остальных векторов из S.*

□ Если $|S| = 1$, то теорема верна в силу утверждения 1(б). Пусть $|S| > 1$. Если некоторый вектор $\alpha \in S$ линейно выражается через систему векторов $S \setminus \{\alpha\}$, то по определению 3 он линейно выражается через некоторую конечную систему векторов $\beta_1, \ldots, \beta_k$ из $S \setminus \{\alpha\}$. Тогда конечная (!) подсистема векторов α, β_1, $\ldots$, β_k из S линейно зависима (см. доказательство теоремы 7 главы 7), и по определению 4 система S линейно зависима.

Обратно, пусть система S линейно зависима. По определению 4 существует конечная линейно зависимая ее подсистема $S' = (\alpha_1, \ldots, \alpha_t)$. При $t = 1$ получаем $\alpha_1 = \theta$ (для подсистемы — это случай $|S'| = 1$), а тогда $\alpha_1 = \beta \circ 0$ для любого вектора $\beta \in S \setminus \{\alpha_1\}$. При $t > 1$ рассуждения проводятся дословно так же, как и при доказательстве теоремы 7 главы 7. □

Утверждение 3. *Пусть вектор $\alpha \in L_P$ линейно выражается через линейно независимую систему S векторов пространства L_P в виде*

$$\alpha = \beta_1 c_1 + \ldots + \beta_r c_r + \beta_{r+1} c_{r+1} + \ldots + \beta_t c_t, \quad c_i \in P \tag{1}$$

и

$$\alpha = \beta_1 d_1 + \ldots + \beta_r d_r + \gamma_{r+1} d_{r+1} + \ldots + \gamma_s d_s, \quad d_j \in P, \tag{2}$$

где $\beta_1, \ldots, \beta_t$ и $\gamma_{r+1}, \ldots, \gamma_s$ — непересекающиеся подсистемы попарно различных векторов системы S (возможно $r = 0$, $t = 0$ или $s = 0$). Тогда

$$c_1 = d_1, \ \ldots, \ c_r = d_r \quad \text{и} \quad c_{r+1} = \ldots = c_t = d_{r+1} = \ldots = d_s = 0. \tag{3}$$

□ Вычитая из равенства (1) равенство (2), получим:

$$\theta = \beta_1(c_1 - d_1) + \ldots + \beta_r(c_r - d_r) + \beta_{r+1} c_{r+1} + \ldots$$
$$\ldots + \beta_t c_t + \gamma_{r+1}(-d_{r+1}) + \ldots + \gamma_s(-d_s).$$

Отсюда следуют равенства (3), так как ввиду условия система векторов β_1, $\ldots$, β_t, γ_{r+1}, $\ldots$, γ_s линейно независима. □

Следствие. *Если вектор $\alpha \in L_P$ линейно выражается через линейно независимую систему β_1, $\ldots$, β_r пространства L_P, то он выражается через нее только одним способом.*

Сравните это следствие с утверждением 11 главы 7.

Утверждение 4. *Если S — непустая линейно независимая система векторов пространства L_P и $\alpha \in L_P$, то система векторов $S_1 = (S, \alpha)$ линейно зависима тогда и только тогда, когда вектор α линейно выражается через систему S.*

□ Если вектор α линейно выражается через систему S, то система S_1 линейно зависима по теореме 2, так как $|S_1| > 1$. Обратно, пусть система S_1 линейно зависима. По определению 4 в ней существует конечная линейно зависимая подсистема α_1, $\ldots$, α_k. В этой подсистеме содержится вектор α, так как в противном случае

система S была бы линейно зависимой вопреки условию. Поэтому можем положить $\alpha_k = \alpha$. Дальнейшее доказательство проводится дословно так же, как доказательство утверждения 10 главы 7. □

Определение *базиса* (*максимальной линейно независимой подсистемы*) для произвольной системы векторов S произвольного пространства L_P вводится совершенно так же, как вводилось определение базиса для конечной системы векторов арифметического пространства (определение 9 главы 7).

Определение 5. Подсистему T системы векторов S пространства L_P называют *базисом системы* S, если

1) система T линейно независима;

2) система, получающаяся добавлением к T любого вектора системы S, линейно зависима.

В частности, если $S = L_P$, то базис системы S называют *базисом пространства* L_P.

Пример 5. Как показывает пример 4 базисом пространства $P[x]_P$ является, например, бесконечная система векторов e, x, $\ldots$, x^n, $\ldots$.

Важное свойство базиса для системы векторов, содержащей хотя бы один ненулевой вектор, отмеченное для конечных систем векторов в утверждении 12 главы 7, дает

Утверждение 5. *Если система векторов S пространства L_P содержит хотя бы один ненулевой вектор, то ее подсистема T является базисом тогда и только тогда, когда*

1) *система T линейно независима*;

2′) *любой вектор системы S линейно выражается через систему T.*

□ Условие 1 утверждения совпадает с условием 1 определения 5. Поскольку в системе S есть ненулевой вектор, то из условия 2′ следует, что система T непустая. Аналогично из условия 2 определения 5 также следует, что система T непустая. По утверждению 4 условия 2 и 2′ равносильны. □

Для сокращения записей вида (1) договоримся о следующих обозначениях. Пусть $\gamma_1, \ldots, \gamma_t$ — произвольная система векторов из L_P, $d^{\downarrow} = (d_1, \ldots, d_t)$ — произвольный вектор из $P^{(t)}$ и

$$A = (A_1^{\downarrow}, \ldots, A_s^{\downarrow}) \in P_{t,s}.$$

Положим по определению $\vec{\gamma} = (\gamma_1, \ldots, \gamma_t)$,

$$\vec{\gamma}\, d^{\downarrow} = \gamma_1 d_1 + \ldots + \gamma_t d_t, \quad \vec{\gamma} A = (\vec{\gamma} A_1^{\downarrow}, \ldots, \vec{\gamma} A_s^{\downarrow}). \tag{4}$$

Нетрудно проверить, что тогда для любых матриц $B \in P_{t,s}$, $C \in P_{s,k}$ и любой системы векторов $\vec{\delta} = (\delta_1, \ldots, \delta_t)$, где $\delta_i \in L_P$, $i \in \overline{1,t}$, справедливы равенства

$$\vec{\gamma}(A + B) = \vec{\gamma} A + \vec{\gamma} B, \quad (\vec{\gamma} + \vec{\delta}) A = \vec{\gamma} A + \vec{\delta} A \tag{5}$$

и

$$\vec{\gamma}(AC) = (\vec{\gamma}A)C. \tag{6}$$

Если $\vec{\beta} = (\beta_1, \ldots, \beta_n)$ — базис системы S, то по следствию утверждения 3 для любого вектора $\alpha \in S$ существуют такие однозначно определенные скаляры $c_i \in P$, что $\alpha = \beta_1 c_1 + \ldots + \beta_n c_n$. Воспользовавшись первым из равенств (4), запишем

$$\alpha = \vec{\beta}\,\alpha^{\downarrow}_{\vec{\beta}}, \tag{7}$$

где $\alpha^{\downarrow}_{\vec{\beta}} = (c_1, \ldots, c_n)^T$.

Определение 6. Вектор $\alpha^{\downarrow}_{\vec{\beta}} \in P^{(n)}$ называют *столбцом координат вектора* $\alpha \in S$ *в базисе* $\vec{\beta}$ системы S.

Вопрос о существовании базиса для конечной системы векторов произвольного пространства L_P решает

Теорема 6. *Если S — конечная система векторов пространства L_P, то в S существует базис (возможно пустой). Любую линейно независимую подсистему системы S можно дополнить до базиса системы S.*

□ Доказательство теоремы проводится так же, как доказательство утверждения 13 главы 7. □

Методами, выходящими за рамки нашего курса, может быть доказана

Теорема 7. *Любая система векторов произвольного пространства L_P (в частности, само пространство L_P) имеет базис.*

Мы ограничимся рассмотрением систем векторов, имеющих базис из конечного числа векторов, и обобщим результаты, полученные в следствиях 4 и 6 теоремы 15 главы 7 и утверждении 17 главы 7.

Теорема 8. *Пусть система векторов S пространства L_P имеет базис $\alpha_1, \ldots, \alpha_n$. Тогда*

(а) *любая линейно независимая подсистема системы S состоит не более чем из n векторов*;

(б) *любой базис системы S состоит из n векторов*;

(в) *любая линейно независимая подсистема системы S, состоящая из n векторов, является базисом системы S*;

(г) *любую линейно независимую подсистему системы S можно дополнить до базиса системы S.*

□ (а) Пусть $\beta_1, \ldots, \beta_{n+1}$ — произвольная подсистема системы S. Так как система $\alpha_1, \ldots, \alpha_n$ — базис S, то существует такая матрица $C \in P_{n,n+1}$, что

$$(\beta_1, \ldots, \beta_{n+1}) = (\alpha_1, \ldots, \alpha_n)C.$$

Система линейных уравнений $Cx^{\downarrow} = 0^{\downarrow}$ по теореме 14 главы 8 имеет ненулевое решение $d^{\downarrow}$, так как число неизвестных в ней больше числа уравнений. Тогда, используя (4) и (6), получаем равенства:

$$(\beta_1, \ldots, \beta_{n+1})d^{\downarrow} = (\alpha_1, \ldots, \alpha_n)Cd^{\downarrow} = (\alpha_1, \ldots, \alpha_n)0^{\downarrow} = \theta,$$

которые показывают, что система $\beta_1, \ldots, \beta_{n+1}$ линейно зависима.

(б) В силу (а) число векторов в любом базисе системы S не превосходит n. Если в S имеется базис, состоящий из t векторов, то опять ввиду (а) $n \leqslant t$. Таким образом, $t = n$.

(в) Пусть $\beta_1, \ldots, \beta_n$ — линейно независимая подсистема системы S. Для любого вектора $\alpha \in S$ согласно (а) система векторов $\beta_1, \ldots, \beta_n, \alpha$ линейно зависима. По утверждению 4 вектор α линейно выражается через систему $\beta_1, \ldots, \beta_n$. По утверждению 5 $\beta_1, \ldots, \beta_n$ — базис системы S.

(г) Пусть $\gamma_1, \ldots, \gamma_t$ — линейно независимая подсистема системы S. Если $t = n$, то в силу (в) $\gamma_1, \ldots, \gamma_n$ — базис системы S. Пусть $t < n$. Рассмотрим все линейно независимые подсистемы из S, содержащие векторы $\gamma_1, \ldots, \gamma_t$. Ввиду (а) в любой из них не более n векторов. Пусть $\gamma_1, \ldots, \gamma_t, \gamma_{t+1}, \ldots, \gamma_k$ — такая система с максимально возможным числом векторов. Так как эта система линейно независима и добавление к ней любого вектора из S приводит к линейно зависимой системе, то $\gamma_1, \ldots, \gamma_k$ — базис системы S, и с учетом (а) $k = n$. □

§ 2. ПОДПРОСТРАНСТВА ВЕКТОРНОГО ПРОСТРАНСТВА

Пусть K — подмножество пространства L_P. Будем говорить, что подмножество K *замкнуто относительно умножения на элементы поля* P, если $\alpha \circ a \in K$ для любых $\alpha \in K$ и $a \in P$. В этом случае отображение $L \times P \to L$, определенное правилом $(\beta,\ b) \to \beta \circ b$, индуцирует одновременно отображение $K \times P \to K$, т. е. задает на K внешнюю операцию умножения на элементы поля P.

Определение 7. Непустое подмножество K пространства L_P называют *подпространством*, если

1) K замкнуто относительно операций сложения и умножения на элементы поля P;

2) K является векторным пространством относительно этих операций. Обозначение: $K_P < L_P$ или $K < L_P$.

Критерий того, чтобы подмножество было подпространством дает

Утверждение 9. *Непустое подмножество K пространства L_P является подпространством тогда и только тогда, когда выполнено условие* 1 *определения* 7.

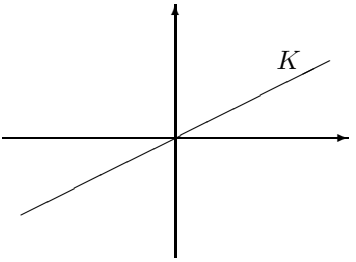
□ Пусть K удовлетворяет условию 1 и $\alpha,\ \beta \in K$. В частности, $\beta(-e) \in K$, где e — единица поля P. Так как $\beta(-e) = -\beta \in K$ по утверждению 1(в), то $\alpha - \beta \in K$ по условию 1. Следовательно, $(K, +)$ — подгруппа группы $(L, +)$.

Соотношения а)–г) определения 2 справедливы для любых $\alpha, \beta \in K$ и $a, b \in P$, так как они справедливы для любых элементов из L и P. Значит, K — векторное пространство над P. □

Таким образом, для $L = P^{(n)}$ определение 7 совпадает с определением 11 главы 7 подпространства в $P^{(n)}$.

В любом пространстве $L_P \neq \theta$ есть, по крайней мере, два подпространства $K_1 = \theta$ и $K_2 = L$. Их называют *несобственными* подпространствами. Все другие подпространства называют *собственными*. Приведем примеры собственных подпространств.

Пример 6. Множество K всех векторов пространства D^2 (или D^3), лежащих на фиксированной прямой (или плоскости), проходящей через начало координат, есть подпространство этого пространства:



Пример 7. $\mathbb{R}_{\mathbb{Q}}$ — подпространство в $\mathbb{C}_{\mathbb{Q}}$.

Утверждение 10. *Пересечение любого семейства подпространств K_α, $\alpha \in A$, пространства L_P является его подпространством.*

Доказательство основывается на применении утверждения 9 и предоставляется читателю.

Определение 8. Пусть S — система векторов пространства L_P. *Подпространством, порожденным системой S*, называют пересечение всех подпространств из L_P, содержащих S. Его обозначают через $(S)_P$.

В силу утверждения 10 $(S)_P$ — действительно подпространство в L_P. В частности, $(\varnothing)_P = \theta$ и $(L)_P = L_P$.

Теорема 11. *Если $S \neq \varnothing$, то подпространство $(S)_P$ состоит из всех конечных линейных комбинаций векторов из S, т. е. из векторов вида*

$$\sum_{i=1}^{k} s_i c_i, \quad \text{где } s_i \in S, \quad c_i \in P, \quad k \in \mathbb{N}. \tag{8}$$

□ Обозначим через T множество векторов из L_P, имеющих вид (8). Так как $(S)_P$ — подпространство пространства L_P, содержащее S, то по определению 7 справедливо включение $T \subset (S)_P$.

Обратно, пусть $t_1 = \sum\limits_{i=1}^{k} s_i c_i$ и $t_2 = \sum\limits_{j=1}^{m} s'_j c'_j$ — элементы из T. Поскольку

$$t_1 + t_2 = \sum_{i=1}^{k} s_i c_i + \sum_{j=1}^{m} s'_j c'_j \in T \tag{9}$$

и для любого $a \in P$

$$t_1 a = \sum_{i=1}^{k} s_i (c_i a) \in T, \tag{10}$$

то по утверждению 9 из (9) и (10) следует, что T — подпространство в L_P. Ввиду включения $T \supset S$ по определению 8 получаем: $T \supset (S)_P$. Значит, $T = (S)_P$. □

Теорема 11 аналогична соответствующим утверждениям для полугрупп и групп. Эта теорема позволяет, в частности, более кратко формулировать различные утверждения, связанные с представлением вектора в виде линейной комбинации других векторов.

Следствие. *Вектор α пространства L_P линейно выражается через систему S векторов этого пространства тогда и только тогда, когда $\alpha \in (S)_P$. Базис системы S является базисом пространства $(S)_P$.*

Доказательство следствия предоставляется читателю.

Утверждение 12. *Пусть $K_1, \ldots, K_t$ — подпространства пространства L_P. Тогда множество*

$$K = K_1 + \ldots + K_t$$

также является подпространством пространства L_P.

□ По следствию теоремы 15 главы 11 $(K, +)$ — подгруппа группы $(L, +)$. Для любых $\alpha_i \in K_i$ и $a \in P$ справедливы включения $\alpha_i a \in K_i$. Поэтому

$$(\alpha_1 + \ldots + \alpha_t)\, a = \alpha_1 a + \ldots + \alpha_t a \in K.$$

По утверждению 9 K — подпространство в L_P. □

Определение 9. Подпространство $K = K_1 + \ldots + K_t$ называют *суммой подпространств* $K_1, \ldots, K_t$.

Если $K = K_1 + \ldots + K_t$, то каждый элемент $\alpha \in K$ представляется в виде $\alpha = \alpha_1 + \ldots + \alpha_t$, где $\alpha_i \in K_i$. Рассмотрим ситуацию, когда такое представление однозначно.

Определение 10. Подпространство $K = K_1 + \ldots + K_t$ называют *прямой суммой подпространств* $K_1, \ldots, K_t$, если каждый элемент $\alpha \in K$ однозначно представим в виде $\alpha = \alpha_1 + \ldots + \alpha_t$, где $\alpha_i \in K_i$. В этом случае пишут: $K = K_1 \dot{+} \ldots \dot{+} K_t$.

Пример 8. Пространство $P^{(2)}$ есть прямая сумма собственных подпространств $K_1 = \left\{ \begin{pmatrix} a \\ 0 \end{pmatrix} \middle| a \in P \right\}$ и $K_2 = \left\{ \begin{pmatrix} 0 \\ b \end{pmatrix} \middle| b \in P \right\}$ (обобщите на случай пространства $P^{(n)}$).

Проверку того, является или нет сумма подпространств прямой, облегчает

Теорема 13. *Если $K_1, \ldots, K_t$, $K = K_1 + \ldots + K_t$ — подпространства пространства L_P, то равносильны свойства*:

(а) $K = K_1 \dot{+} \ldots \dot{+} K_t$;

(б) *если* $\theta = \alpha_1 + \ldots + \alpha_t$, *где* $\alpha_i \in K_i$, *то* $\alpha_i = \ldots = \alpha_t = \theta$;

(в) *для любого* $i \in \overline{1,t}$ *справедливо* $K_i \cap \sum\limits_{j \neq i} K_j = \theta$;

(г) *для любого* $i \in \overline{1,t-1}$ *справедливо* $(K_1 + \ldots + K_i) \cap K_{i+1} = \theta$.

□ Так как каждое из подпространств K_i есть подгруппа группы $(L,+)$, то равносильность свойств (а)–(в) следует из теоремы 17 главы 11. Понятно, что (в)⇒(г). Доказательство, например, импликации (г)⇒(б) предоставляется читателю. □

§ 3. ИЗОМОРФИЗМЫ ВЕКТОРНЫХ ПРОСТРАНСТВ

Определение 11. Отображение $\varphi\colon M_P \to L_P$ называют *изоморфизмом*, если

1) φ — изоморфизм абелевых групп $(M,+)$ и $(L,+)$;

2) для любых элементов $\alpha \in M$ и $a \in P$ справедливо равенство $\varphi(\alpha \circ a) = \varphi(\alpha)a$.

В случае существования такого отображения φ пространства M_P и L_P называют *изоморфными* (обозначение: $M_P \cong L_P$).

Заметим, что $\varphi(\theta_M) = \theta_L$, так как φ — изоморфизм абелевых групп.

Пример 9. Поворот пространства D^2 вокруг начал координат на угол ω против часовой стрелки является изоморфизмом D^2 на D^2 (проверьте).

Утверждение 14. *Если $\varphi\colon M_P \to L_P$ — изоморфизм векторных пространств, то обратное отображение φ^{-1} является изоморфизмом L_P на M_P.*

Утверждение 15. *Если $\varphi\colon M_P \to L_P$ и $\psi\colon L_P \to K_P$ — изоморфизмы векторных пространств, то отображение*

$$\psi \circ \varphi\colon M_P \to K_P$$

— изоморфизм векторных пространств ($\circ$ — композиция отображений).

Доказательство утверждений 14 и 15 осуществляется непосредственной проверкой (определение обратного отображения см. в определении 10 главы 1).

Утверждение 16. *Если $\varphi\colon M_P \to L_P$ — изоморфизм векторных пространств, то для любых векторов $\alpha, \alpha_1, \ldots, \alpha_k \in M_P$ и элементов $a_1, \ldots, a_k \in P$ равенство*

$$\alpha = \alpha_1 a_1 + \ldots + \alpha_k a_k \tag{11}$$

справедливо тогда и только тогда, когда выполняется равенство

$$\varphi(\alpha) = \varphi(\alpha_1)a_1 + \ldots + \varphi(\alpha_k)a_k. \tag{12}$$

□ По определению 11 из равенства (11) следует равенство (12). Так как $\varphi^{-1} \circ \varphi = \varepsilon_M$, то в силу утверждения 14 из равенства (12) следует равенство (11). □

Теорема 17. *Если $\varphi\colon M_P \to L_P$ — изоморфизм и S — система векторов пространства M_P, $S \neq \varnothing$, то*

(а) *система S линейно независима тогда и только тогда, когда линейно независима система $\varphi(S)$;*

(б) $M_P = (S)_P \Leftrightarrow L_P = (\varphi(S))_P$;

(в) *S — базис M_P тогда и только тогда, когда $\varphi(S)$ — базис L_P.*

□ (а) В силу утверждения 16 для любых векторов $\alpha_1, \ldots, \alpha_k \in S$ и элементов $a_1, \ldots, a_k \in P$ линейное соотношение $\sum_{i=1}^{k} \alpha_i a_i = \theta_M$ равносильно линейному соотношению $\sum_{i=1}^{k} \varphi(\alpha_i) a_i = \theta_L$.

(б) По теореме 11 произвольный вектор из M_P имеет вид

$$\alpha = \alpha_1 c_1 + \ldots + \alpha_t c_t,$$

где $\alpha_i \in S$, $c_i \in P$. Поскольку φ — биекция, то произвольный вектор β из L_P имеет вид $\beta = \varphi(\alpha)$. Тогда

$$\beta = \varphi(\alpha_1) c_1 + \ldots + \varphi(\alpha_t) c_t,$$

и по теореме 11 $L_P = (\varphi(S))_P$.

Аналогично, используя изоморфизм φ^{-1}, из равенства $L_P = (\varphi(S))_P$ получаем $M_P = (S)_P$.

(в) Заметим, что базис пространства есть пустая система векторов тогда и только тогда, когда пространство состоит из нулевого вектора. Для пространств, состоящих не только из нулевого вектора, ввиду утверждения 5 свойство (в) следует из (а) и (б). □

Пример 10. Отображение $\varphi\colon P^{(n)} \to P^n$, определенное равенством

$$\varphi\left(\begin{pmatrix} a_1 \\ \ldots \\ a_n \end{pmatrix}\right) = (a_1, \ldots, a_n),$$

является изоморфизмом пространства $P^{(n)}$ на пространство P^n.

§ 4. КОНЕЧНОМЕРНЫЕ ПРОСТРАНСТВА

Перейдем к изучению векторных пространств, для которых существует базис, состоящий из конечного числа векторов.

Определение 12. Пространство L_P называют *конечномерным*, если в нем существует базис, состоящий из конечного числа векторов. Пространства, не являющиеся конечномерными, называют *бесконечномерными* (см. пример 5).

Если L_P — конечномерное пространство и $\alpha_1, \ldots, \alpha_n$ — некоторый его базис, то по теореме 8(б) любой базис L_P состоит также из n векторов. Поэтому корректно

Определение 13. *Размерностью* конечномерного *пространства* L_P называют число векторов в любом его базисе.

Если L_P имеет базис из n векторов, то его называют *пространством размерности* n или n*-мерным* пространством и пишут $\dim L_P = n$.

Пример 11. Пространство $P^{(n)}$ конечномерное и $\dim P^{(n)} = n$, так как $P^{(n)}$ имеет базис $E_1^{\downarrow}$, ..., $E_n^{\downarrow}$. Это, в частности, оправдывает термин «n-мерное арифметическое пространство», введенный в главе 7. Пространство $(P_{n,n})_P$ — конечномерное и $\dim P_{n,n} = n^2$, так как $(P_{n,n})_P$ имеет базис из n^2 матриц $E_{n\times n}^{(i,j)}$ (см. § 1 главы 6).

Как и в $P^{(n)}$, в любом конечномерном пространстве L_P верна

Теорема 18. *Если* $\dim L_P = n$*, то*

(а) *любая линейно независимая система векторов из* L_P *состоит не более чем из* n *векторов*;

(б) *любая линейно независимая система из* n *векторов является базисом* L_P;

(в) *любую линейно независимую систему векторов из* L_P *можно дополнить до базиса* L_P.

□ Теорема 18 является перефразировкой при $S = L_P$ теоремы 8. □

Однако в отличие от пространства $P^{(n)}$, у нас пока нет эффективных способов распознавания линейной зависимости или независимости системы векторов из L_P, состоящей из $k \leqslant n$ векторов. Для получения таких способов мы воспользуемся свойствами изоморфных пространств. Сначала мы покажем, что все пространства над данным полем, имеющие одинаковую размерность, изоморфны.

Утверждение 19. *Если* $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ *— базис пространства* L_P*, то для любых векторов* β, $\gamma \in L_P$ *и любого* $a \in P$ *справедливы равенства*

$$(\beta + \gamma)_{\vec{\alpha}}^{\downarrow} = \beta_{\vec{\alpha}}^{\downarrow} + \gamma_{\vec{\alpha}}^{\downarrow}, \quad (\beta a)_{\vec{\alpha}}^{\downarrow} = \beta_{\vec{\alpha}}^{\downarrow}\, a. \tag{13}$$

□ В силу (6) $\beta = \vec{\alpha}\beta_{\vec{\alpha}}^{\downarrow}$ и $\gamma = \vec{\alpha}\gamma_{\vec{\alpha}}^{\downarrow}$. Тогда, учитывая (5), получаем:

$$\beta + \gamma = \vec{\alpha}\beta_{\vec{\alpha}}^{\downarrow} + \vec{\alpha}\gamma_{\vec{\alpha}}^{\downarrow} = \vec{\alpha}(\beta_{\vec{\alpha}}^{\downarrow} + \gamma_{\vec{\alpha}}^{\downarrow}). \tag{14}$$

Одновременно

$$\beta + \gamma = \vec{\alpha}(\beta + \gamma)_{\vec{\alpha}}^{\downarrow}. \tag{15}$$

Поскольку $\vec{\alpha}$ — базис L_P, то из (14) и (15) в силу следствия утверждения 3 получаем первое из равенств (13). Аналогично доказывается и второе из них. □

Теорема 20. *Если* $\dim L_P = n$*, то* $L_P \cong P^{(n)}$.

□ Пусть $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ — базис пространства L_P. Зададим отображение $\varphi\colon L_P \to P^{(n)}$, положив для вектора $\beta = \vec{\alpha}\beta_{\vec{\alpha}}^{\downarrow}$

$$\varphi(\beta) = \beta_{\vec{\alpha}}^{\downarrow}. \tag{16}$$

Ясно, что отображение φ — биекция. В силу утверждения 19 φ — изоморфизм векторных пространств. □

Теорема 21. *Конечномерные векторные пространства L_P и M_P изоморфны тогда и только тогда, когда* $\dim L_P = \dim M_P$.

□ Если $\dim L_P = \dim M_P = n$, то по теореме 20 существуют изоморфизмы $\varphi\colon L_P \to P^{(n)}$ и $\psi\colon M_P \to P^{(n)}$. По утверждению 14 $\psi^{-1}\colon P^{(n)} \to M_P$ — изоморфизм. Тогда по утверждению 15 $\psi^{-1} \circ \varphi\colon L_P \to M_P$ — изоморфизм.

Обратно, пусть существует изоморфизм $\varphi\colon L_P \to M_P$. Если $\dim L = n$ и $\alpha_1, \ldots, \alpha_n$ — базис L_P, то по теореме 17(в) $\varphi(\alpha_1), \ldots, \varphi(\alpha_n)$ — базис M_P, т. е. $\dim M_P = n$. □

Теоремы 20 и 21 показывают, что n-мерное арифметическое пространство $P^{(n)}$ является, с точностью до изоморфизма, единственным n-мерным пространством над данным полем.

Практический способ определить, линейно зависима или нет система векторов конечномерного пространства, дает

Утверждение 22. *Если* $\dim L_P = n$ *и* $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ *— базис L_P, то система векторов $\beta_1, \ldots, \beta_k$ из L_P линейно независима тогда и только тогда, когда линейно независима система векторов $\beta^{\downarrow}_{1\vec{\alpha}}, \ldots, \beta^{\downarrow}_{k\vec{\alpha}}$.*

□ Отображение $\varphi\colon L_P \to P^{(n)}$, задаваемое формулой (16), есть изоморфизм векторных пространств. По теореме 17(а) получаем требуемое утверждение. □

Из утверждения 22 и критерия линейной независимости системы векторов из $P^{(n)}$ (следствие 3 теоремы 15 главы 7) получаем

Следствие. *Система векторов $\beta_1, \ldots, \beta_n$ является базисом L_P тогда и только тогда, когда матрица $C = (\beta^{\downarrow}_{1\vec{\alpha}}, \ldots, \beta^{\downarrow}_{n\vec{\alpha}})$ невырожденная.*

Определение 14. Пусть $\vec{\beta} = (\beta_1, \ldots, \beta_n)$ и $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ — базисы L_P, где $n = \dim L_P$. Если $\vec{\beta} = \vec{\alpha}C$, то матрицу C называют *матрицей перехода от базиса $\vec{\alpha}$ к базису $\vec{\beta}$*. Таким образом, столбцы матрицы C — это столбцы координат базисных векторов $\beta_1, \ldots, \beta_n$ в базисе $\vec{\alpha}$.

Выясним, как связаны между собой столбцы координат одного и того же вектора в разных базисах. Пусть $\vec{\alpha}$ и $\vec{\beta}$ — базисы пространства L_P и $\gamma \in L_P$. Тогда вектор $\gamma = \vec{\alpha}\gamma^{\downarrow}_{\vec{\alpha}} = \vec{\beta}\gamma^{\downarrow}_{\vec{\beta}}$ и $\vec{\beta} = \vec{\alpha}C$, где $C = P^{*}_{n,n}$. Следовательно, $\vec{\alpha}\gamma^{\downarrow}_{\vec{\alpha}} = \vec{\alpha}C\gamma^{\downarrow}_{\vec{\beta}}$. Отсюда

$$\gamma^{\downarrow}_{\vec{\alpha}} = C\gamma^{\downarrow}_{\vec{\beta}}, \quad \gamma^{\downarrow}_{\vec{\beta}} = C^{-1}\gamma^{\downarrow}_{\vec{\alpha}}. \tag{17}$$

Формулы (17) называют *формулами преобразования координат*.

В заключение отметим, что алгоритмические задачи 1–6, поставленные в § 3 главы 7 для систем векторов из $P^{(n)}$, представляют интерес и в произвольном конечномерном пространстве L_P. Решение любой из этих задач в L_P сводится в силу утверждения 16 и теоремы 20 к решению аналогичной задачи для систем векторов из $P^{(n)}$.

§ 5. ПОДПРОСТРАНСТВА КОНЕЧНОМЕРНОГО ПРОСТРАНСТВА

Всякое подпространство конечномерного пространства само конечномерно, как показывает

Теорема 23. *Пусть* $\dim L_P = n$ *и* $K < L_P$. *Тогда*

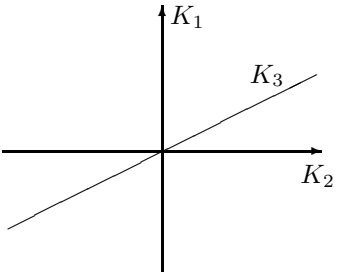
(а) *пространство* K_P *конечномерно и* $\dim K_P \leqslant n$;

(б) *в* L_P *существует такое подпространство* M_P, *что* $L = K \dot{+} M$, *т. е. каждое подпространство в* L_P *выделяется прямым слагаемым.*

□ Утверждение (а) справедливо в силу теорем 18(а) и 8. Покажем справедливость (б). Если $K = \theta$ или $K = L$, то соответственно $M = L$ и $M = \theta$. Пусть $\dim K_P = r$, $0 < r < n$, и $\alpha_1, \ldots, \alpha_r$ — базис K_P. По теореме 18(в) систему $\alpha_1, \ldots, \alpha_r$ можно дополнить до базиса $\alpha_1, \ldots, \alpha_r, \alpha_{r+1}, \ldots, \alpha_n$ пространства L_P. Обозначим $(\alpha_{r+1}, \ldots, \alpha_n)_P = M_P$. Тогда сумма подпространств $K + M$ содержит базис пространства L_P и, значит, $K + M \supset L$. Так как обратное включение очевидно, то $L = K + M$.

Пусть $\beta \in K \cap M$, т. е. $\beta = \sum_{i=1}^{r} \alpha_i c_i = \sum_{j=r+1}^{n} \alpha_j c_j$. Тогда имеем равенство $\theta = \sum_{i=1}^{r} \alpha_i c_i + \sum_{j=i+1}^{n} \alpha_j (-c_j)$. Так как $\alpha_1, \ldots, \alpha_n$ — базис L_P, то $c_i = 0$, $i \in \overline{1,n}$, и $\beta = \theta$. По теореме 13 $L = K \dot{+} M$. □

Пример 12. В пространстве D^2 рассмотрим подпространства K_1, K_2 и K_3:



Ясно, что $D^2 = K_1 \dot{+} K_2 = K_1 \dot{+} K_3$ и $K_2 \neq K_3$. Таким образом, подпространство M_P в теореме 23 определено, вообще говоря, неоднозначно.

В случае конечного поля P мы можем подсчитать число различных подпространств в L_P.

Утверждение 24. *Пусть* $|P| = q$, $\dim L_P = n$ *и* $0 < k < n$. *Тогда в* L_P *имеется ровно*

$$\frac{(q^n-1)(q^n-q)\dots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\dots(q^k-q^{k-1})} \tag{18}$$

различных подпространств размерности k.

□ Доказательство утверждения 18 главы 7 показывает, что

$$(q^n-1)(q^n-q)\dots(q^n-q^{k-1})$$

— это число линейно независимых систем векторов из L_P, содержащих по k векторов. Каждая из таких систем порождает подпространство размерности k. Одновременно с этим каждое подпространство размерности k порождается любой из $(q^k-1)(q^k-q)\dots(q^k-q^{k-1})$ линейно независимых своих подсистем, состоящих из k элементов. Значит, число различных подпространств в L_P, имеющих размерность k, определяется формулой (18). □

Установим связь между размерностями суммы и пересечения двух подпространств.

Теорема 25 (Грассман).[17] *Если* K_1 *и* K_2 *— подпространства конечномерного пространства* L_P, *то*

$$\dim(K_1+K_2) = \dim K_1 + \dim K_2 - \dim(K_1 \cap K_2).$$

□ Пусть $\dim K_1 = m_1$, $\dim K_2 = m_2$ и $\dim(K_1 \cap K_2) = m$. Так как $K_1 \cap K_2 \subset K_1$ и $K_1 \cap K_2 \subset K_2$, то по теореме 18(в) базис $\alpha_1, \dots, \alpha_m$ подпространства $K_1 \cap K_2$ можно дополнить до базиса

$$\alpha_1, \dots, \alpha_m, \beta_{m+1}, \dots, \beta_{m_1} \tag{19}$$

подпространства K_1 и до базиса

$$\alpha_1, \dots, \alpha_m, \gamma_{m+1}, \dots, \gamma_{m_2} \tag{20}$$

подпространства K_2. Это верно и в случае $m = 0$, т. е. когда $K_1 \cap K_2 = \theta$. Покажем, что система векторов

$$\alpha_1, \dots, \alpha_m, \beta_{m+1}, \dots, \beta_{m_1}, \gamma_{m+1}, \dots, \gamma_{m_2} \tag{21}$$

является базисом подпространства $K_1 + K_2$. Этим мы докажем теорему, ибо число векторов в системе (21) равно

$$m_1 + m_2 - m = \dim K_1 + \dim K_2 - \dim(K_1 \cap K_2).$$

Произвольный вектор $\delta \in K_1 + K_2$ имеет вид $\delta = \delta_1 + \delta_2$, где $\delta_1 \in K_1$ и $\delta_2 \in K_2$. Так как векторы δ_1 и δ_2 линейно выражаются соответственно через базисы (19) и (20), то вектор δ линейно выражается через систему (21). Поэтому

$$K_1 + K_2 = (\alpha_1, \dots, \alpha_m, \beta_{m+1}, \dots, \gamma_{m_2})_P.$$

[17] Г. Грассман (1809–1877) — немецкий математик.

Остается показать, что система (21) линейно независима. Если

$$\alpha_1 a_1 + \ldots + \alpha_m a_m + \beta_{m+1} b_{m+1} + \ldots + \beta_{m_1} b_{m_1} + \gamma_{m+1} c_{m+1} + \ldots + \gamma_{m_2} c_{m_2} = \theta,$$

то имеем равенство

$$\begin{aligned} \alpha_1 a_1 + \ldots + \alpha_m a_m + \beta_{m+1} b_{m+1} + \ldots + \beta_{m_1} b_{m_1} = \\ = \gamma_{m+1}(-c_{m+1}) + \ldots + \gamma_{m_2}(-c_{m_2}). \end{aligned} \tag{22}$$

Вектор $\lambda = \gamma_{m+1}(-c_{m+1}) + \ldots + \gamma_{m_2}(-c_{m_2})$ из правой части равенства (22) принадлежит подпространству K_2, а равный ему вектор из левой части равенства (22) принадлежит подпространству K_1. Значит, вектор λ выражается через базис $\alpha_1, \ldots, \alpha_m$ подпространства $K_1 \cap K_2$:

$$\lambda = \alpha_1 a'_1 + \ldots + \alpha_m a'_m = \gamma_{m+1}(-c_{m+1}) + \ldots + \gamma_{m_2}(-c_{m_2}).$$

В силу линейной независимости системы векторов (20) получаем

$$a'_1 = \ldots = a'_m = c_{m+1} = \ldots = c_{m_2} = 0.$$

Но тогда $\lambda = \theta$, и равенство (22) в силу линейной независимости системы векторов (19) дает $a_1 = \ldots = a_m = b_{m+1} = \ldots = b_{m_1} = 0$. Таким образом, система векторов (21) линейно независима. □

Следствие. *Размерность суммы $K_1 + K_2$ подпространств пространства L_P равна сумме их размерностей тогда и только тогда, когда сумма подпространств $K_1 + K_2$ прямая.*

□ Доказательство очевидно в силу теоремы 13. □

Рассмотрим практические способы отыскания базисов суммы и пересечения подпространств K_1 и K_2 пространства L_P.

Пусть $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ — базис пространства L_P, а $\vec{\beta} = (\beta_1, \ldots, \beta_m)$ и $\vec{\gamma} = (\gamma_1, \ldots, \gamma_l)$ — базисы соответственно подпространств K_1 и K_2, векторы которых заданы своими столбцами координат $\beta^{\downarrow}_{i\vec{\alpha}}$ и $\gamma^{\downarrow}_{j\vec{\alpha}}$ в базисе $\vec{\alpha}$.

Тогда $K_1 + K_2 = (\beta_1, \ldots, \beta_m, \gamma_1, \ldots, \gamma_l)_P$, и базисом подпространства $K_1 + K_2$ является базис системы векторов $\beta_1, \ldots, \gamma_l$. Для его нахождения нужно найти базис системы векторов

$$\beta^{\downarrow}_{1\vec{\alpha}}, \ \ldots, \ \beta^{\downarrow}_{m\vec{\alpha}}, \ \gamma^{\downarrow}_{1\vec{\alpha}}, \ \ldots, \ \gamma^{\downarrow}_{l\vec{\alpha}} \tag{23}$$

из $P^{(n)}$, а алгоритм решения этой задачи известен (см. главу 7).

Обозначим $K = K_1 \cap K_2$. Вектор $\delta \in L_P$ принадлежит K тогда и только тогда, когда он линейно выражается через каждую из систем векторов $\vec{\beta}$ и $\vec{\gamma}$, т. е. когда вектор $\delta^{\downarrow}_{\vec{\alpha}}$ линейно выражается через каждую из систем векторов $\beta^{\downarrow}_{i\vec{\alpha}}$ и $\gamma^{\downarrow}_{j\vec{\alpha}}$:

$$\delta^{\downarrow}_{\vec{\alpha}} = (\beta^{\downarrow}_{1\vec{\alpha}}, \ \ldots, \ \beta^{\downarrow}_{m\vec{\alpha}})\, a^{\downarrow} = (\gamma^{\downarrow}_{1\vec{\alpha}}, \ \ldots, \ \gamma^{\downarrow}_{l\vec{\alpha}})\, b^{\downarrow},$$

или в матричной записи

$$\delta^{\downarrow}_{\vec{\alpha}} = Ua^{\downarrow} = Vb^{\downarrow}, \quad \text{где} \quad U = (\beta^{\downarrow}_{1\vec{\alpha}}, \ldots, \beta^{\downarrow}_{m\vec{\alpha}}), \quad V = (\gamma^{\downarrow}_{1\vec{\alpha}}, \ldots, \gamma^{\downarrow}_{l\vec{\alpha}}).$$

Таким образом, подпространство K состоит из всех векторов вида $\vec{\alpha}Ua^{\downarrow}$, где $a^{\downarrow} \in P^{(m)}$ — такой вектор, для которого существует вектор $b^{\downarrow} \in P^{(l)}$, удовлетворяющий условию: вектор $\begin{pmatrix} a^{\downarrow} \\ b^{\downarrow} \end{pmatrix}$ является решением системы линейных уравнений

$$(U, -V)\begin{pmatrix} x^{\downarrow} \\ y^{\downarrow} \end{pmatrix} = 0^{\downarrow}, \tag{24}$$

где $x^{\downarrow} = (x_1, \ldots, x_m)^T$, $y^{\downarrow} = (y_1, \ldots, y_l)^T$.

Покажем, что для любой фундаментальной системы решений

$$\begin{pmatrix} x^{\downarrow}_1 \\ y^{\downarrow}_1 \end{pmatrix}, \ldots, \begin{pmatrix} x^{\downarrow}_t \\ y^{\downarrow}_t \end{pmatrix} \tag{25}$$

системы уравнений (24) справедливо равенство

$$K = (\vec{\alpha}Ux^{\downarrow}_1, \ldots, \vec{\alpha}Ux^{\downarrow}_t)_P. \tag{26}$$

Система $Ux^{\downarrow}_1, \ldots, Ux^{\downarrow}_t$ линейно независима, так как из $\sum\limits_{i=1}^{t} Ux^{\downarrow}_i c_i = 0^{\downarrow}$ следуют равенства

$$\sum_{i=1}^{t} Vy^{\downarrow}_i c_i = 0^{\downarrow}, \quad \sum_{i=1}^{t} x^{\downarrow}_i c_i = 0^{\downarrow}, \quad \sum_{i=1}^{t} y^{\downarrow}_i c_i = 0^{\downarrow}, \quad \sum_{i=1}^{t} \begin{pmatrix} x^{\downarrow}_i \\ y^{\downarrow}_i \end{pmatrix} c_i = 0^{\downarrow},$$

и $c_i = 0$, $i \in \overline{1,t}$.

Кроме того, по следствию 1 теоремы 6 главы 8, $t = m + l - \operatorname{rang}(U, -V)$. Так как $\operatorname{rang}(U, -V) = \operatorname{rang}(U, V)$ и $\operatorname{rang}(U, V)$ по следствию 7 теоремы 15 главы 7 равен числу векторов в базисе системы векторов (23), то по теореме 25 получаем

$$\dim(K_1 \cap K_2) = m + l - \dim(K_1 + K_2) = m + l - \operatorname{rang}(U, -V).$$

Значит, $t = \dim(K_1 \cap K_2) = \dim K$. По теореме 18(б) система векторов $\vec{\alpha}Ux^{\downarrow}_i$, $i \in \overline{1,t}$, — базис подпространства K.

Итак, для отыскания базиса подпространства $K_1 + K_2$ нужно найти базис системы векторов (23). Соответствующие векторы из системы векторов $\beta_1, \ldots, \gamma_l$ образуют базис $K_1 + K_2$.

Для отыскания базиса подпространства $K = K_1 \cap K_2$ нужно:

1) Составить систему линейных уравнений (24).

2) Найти ее произвольную фундаментальную систему решений (25).

3) Выписать базис подпространства K в виде (26).

В конце главы будет приведен еще один способ отыскания базисов суммы и пересечения двух подпространств пространства L_P.

§ 6. ФАКТОРПРОСТРАНСТВА И МНОГООБРАЗИЯ

Пусть L_P — подпространство произвольного пространства M_P. Введем на M_P отношение:

$$(\alpha \equiv \beta\,(L)) \;\Leftrightarrow\; (\alpha - \beta \in L).$$

Так как $(L,+)$ — подгруппа абелевой группы $(M,+)$, то отношение $\equiv (L)$ является конгруэнцией на группе $(M,+)$, и можно рассматривать факторгруппу $(M/L,+)$, где операция определена равенством

$$[\alpha]_L + [\beta]_L = [\alpha+\beta]_L$$

(см. § 11 главы 11).

Введем теперь на $(M/L,+)$ внешнюю операцию умножения, положив

$$[\alpha]_L \circ a = [\alpha a]_L, \quad a \in P. \tag{27}$$

Проверим корректность определения (27).

Пусть $[\alpha]_L = [\beta]_L$, т. е. $\alpha - \beta \in L$. Так как L_P — подпространство в M_P, то $(\alpha-\beta)a = \alpha a - \beta a \in L$. Поэтому $[\alpha a]_L = [\beta a]_L$, и, значит, результат операции не зависит от выбора представителя в классе $[\alpha]_L$.

Теорема 26. $(M/L,+,\circ)$ — *векторное пространство над полем* P.

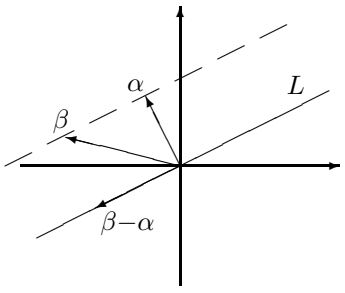
□ Доказательство осуществляется непосредственной проверкой соотношений а)–г) определения 2. Например, цепочка равенств

$$([\alpha]_L + [\beta]_L) \circ a = [\alpha+\beta]_L \circ a = [\alpha a + \beta a]_L = [\alpha a]_L + [\beta a]_L = [\alpha]_L \circ a + [\beta]_L \circ a$$

показывает справедливость соотношения в). Проверка остальных соотношений предоставляется читателю. □

Определение 15. Векторное пространство $(M/L)_P$ называют *факторпространством пространства* M_P *по подпространству* L_P.

Пример 13. В векторном пространстве D^2 зафиксируем подпространство L, состоящее из всех векторов, лежащих на некоторой прямой, проходящей через начало координат:



Векторы β и α находятся в одном классе ($[\beta]_L = [\alpha]_L$) тогда и только тогда, когда $\beta - \alpha \in L$. Поэтому класс $[\alpha]_L$ есть множество всех векторов, концы которых лежат на прямой, проходящей через конец вектора α параллельно прямой L. Значит, факторпространство D^2/L, являющееся совокупностью классов $[\alpha]_L$, можно для наглядности интерпретировать как совокупность прямых, параллельных прямой L.

Если M_P — конечномерное пространство, то легко найти базис факторпространства.

Теорема 27. *Если* $\dim M_P = n$, $L_P < M_P$, $\dim L_P = k$ *и* $\alpha_1, \ldots, \alpha_k$ *— базис* L_P, *то* $\alpha_1, \ldots, \alpha_k, \ldots, \alpha_n$ *— базис* M_P *тогда и только тогда, когда* $[\alpha_{k+1}]_L, \ldots, [\alpha_n]_L$ *— базис пространства* $(M/L)_P$. *В частности,* $\dim(M/L)_P = \dim M_P - \dim L_P$.

□ Пусть

$$\alpha_1, \ldots, \alpha_k,\ \alpha_{k+1}, \ldots, \alpha_n \tag{28}$$

— базис пространства M_P и $\beta = \sum_{i=1}^{n} \alpha_i a_i$ — произвольный вектор из M_P. Тогда вектор $[\beta]_L$ из M/L имеет вид

$$[\beta]_L = \left[\sum_{i=1}^{k} \alpha_i a_i + \sum_{j=k+1}^{n} \alpha_j a_j\right]_L = \sum_{i=1}^{k} [\alpha_i]_L a_i + \sum_{j=k+1}^{n} [\alpha_j]_L a_j.$$

Так как $\alpha_i \in L$ при $i \in \overline{1,k}$, то $[\alpha_i]_L = [\theta]_L$. Значит, всякий вектор из M/L является линейной комбинацией векторов системы

$$[\alpha_{k+1}]_L,\ \ldots,\ [\alpha_n]_L. \tag{29}$$

Пусть $\sum_{j=k+1}^{n} [\alpha_j]_L b_j = [\theta]_L$. Тогда $\left[\sum_{j=k+1}^{n} \alpha_j b_j\right]_L = [\theta]_L$ и, следовательно,

$$\sum_{j=k+1}^{n} \alpha_j b_j = \sum_{i=1}^{k} \alpha_i c_i \in L$$

при некоторых $c_i \in P$. В силу линейной независимости системы векторов (28) получаем $b_j = 0$ при $j \in \overline{k+1,n}$ и $c_i = 0$ при $i \in \overline{1,k}$. Это означает, что система векторов (29) линейно независима. Таким образом, она является базисом факторпространства $(M/L)_P$. В частности, $\dim(M/L)_P = n - k = \dim M_P - \dim L_P$.

Обратно, пусть система (29) — базис пространства $(M/L)_P$. Если $\sum_{i=1}^{n} \alpha_i c_i = \theta$, то $\sum_{i=1}^{n} [\alpha_i]_L c_i = [\theta]_L$ и $\sum_{j=k+1}^{n} [\alpha_j]_L c_j = [\theta]_L$. Тогда $c_j = 0$ при $j \in \overline{k+1,n}$, откуда $\sum_{i=1}^{k} \alpha_i c_i = \theta$, и, в силу линейной независимости системы $\alpha_1, \ldots, \alpha_k$, получаем, что $c_i = 0$ и при $i \in \overline{1,k}$. Так как $\dim M_P = n$, то система (28) — базис пространства M_P. □

Пример 13, помимо прочего, дает геометрическую иллюстрацию следующего понятия, обобщающего понятия прямой и плоскости, а также подпространства векторного пространства.

Определение 16. *Многообразием* пространства M_P, *порожденным вектором* $\alpha \in M_P$ *и подпространством* L_P, называют смежный класс группы $(M,+)$ по подгруппе L:

$$\alpha + L = \{\alpha + \lambda :\ \lambda \in L\},$$

т. е. элемент $[\alpha]_L$ факторпространства $(M/L)_P$.

Утверждение 28. *Многообразия* $\alpha + L_1$ *и* $\beta + L_2$ *пространства* M_P *равны тогда и только тогда, когда* $L_1 = L_2$ *и* $\alpha - \beta \in L_1$.

□ Если $L_2 = L_1$ и $\alpha - \beta \in L_1$, то $[\alpha]_{L_1} = [\beta]_{L_2}$, т. е. $\alpha + L_1 = \beta + L_2$.

Обратно, пусть $\alpha + L_1 = \beta + L_2$. Так как $\theta \in L_2$, то для некоторого $\lambda_1 \in L_1$ получаем $\beta = \alpha + \lambda_1$. Поэтому $\alpha - \beta \in L_1$.

Для любого элемента $\lambda_2 \in L_2$ существует такой элемент $\lambda_1' \in L_1$, что $\alpha + \lambda_1' = \beta + \lambda_2$. Тогда $\lambda_2 = \alpha - \beta + \lambda_1' \in L_1$. Значит, $L_2 \subset L_1$. Аналогично показываем, что $L_1 \subset L_2$, и, значит, $L_1 = L_2$. □

Теперь корректно

Определение 17. Для конечномерного подпространства L_P пространства M_P *размерностью многообразия* $\alpha + L_P$ называют размерность подпространства L_P.

Пример 14. Любая прямая в векторном пространстве D^2 или D^3 является одномерным многообразием. Плоскость в пространстве D^3 является двумерным многообразием.

Пример 15. Если $A_{m\times n}x^{\downarrow} = b^{\downarrow}$ — совместная система уравнений над полем P, то совокупность всех ее решений является многообразием $c' + L$ в пространстве $P^{(n)}$, где c' — частное решение системы, а L — подпространство решений ассоциированной системы однородных уравнений $Ax^{\downarrow} = 0^{\downarrow}$. Если $\operatorname{rang} A = r$, то $\dim L = n - r$, т. е. размерность многообразия $c' + L$ равна $n - r$.

Покажем теперь, что произвольное многообразие можно задать в виде совокупности решений некоторой системы линейных уравнений.

Утверждение 29. *Пусть* $H = a^{\downarrow} + L$ *— многообразие в пространстве* $P^{(n)}$ *и* $a_1^{\downarrow}, \ldots, a_k^{\downarrow}$ *— базис* L_P. *Тогда существуют такие матрица* $A_{r\times n}$ *над* P *и вектор* $b^{\downarrow} \in P^{(r)}$, *что* $\operatorname{rang} A = r = n - k$ *и* H *— совокупность всех решений системы уравнений* $Ax^{\downarrow} = b^{\downarrow}$.

□ Обозначим $B = (a_1^{\downarrow}, \ldots, a_k^{\downarrow})$ и рассмотрим систему линейных уравнений

$$B^T_{k\times n}\, y^{\downarrow} = 0^{\downarrow}. \tag{30}$$

Так как $\operatorname{rang} B^T = \operatorname{rang} B = k$, то система уравнений (30) имеет фундаментальную систему решений $y_1^{\downarrow}, \ldots, y_{n-k}^{\downarrow}$. Обозначим

$$D = (y_1^{\downarrow}, \ldots, y_{n-k}^{\downarrow}), \quad A = D^T, \quad b^{\downarrow} = Aa^{\downarrow}.$$

Система уравнений

$$Ax^{\downarrow} = b^{\downarrow} \tag{31}$$

имеет в качестве частного решения вектор $a^{\downarrow}$. Ассоциированная система $Ax^{\downarrow} = 0^{\downarrow}$ имеет в качестве фундаментальной системы решений систему векторов $a_1^{\downarrow}, \ldots, a_k^{\downarrow}$. Действительно, ввиду (30) выполнено равенство $B^T D = O_{k\times(n-k)}$. Переходя к транспонированным матрицам в последнем равенстве, получаем $D^T B = O_{(n-k)\times k}$, или

$$A\,(a_1^{\downarrow}, \ldots, a_k^{\downarrow}) = O_{(n-k)\times k}.$$

Поскольку $\operatorname{rang} A = \operatorname{rang} D = n - k$, то $a_1^{\downarrow}, \ldots, a_k^{\downarrow}$ — фундаментальная система решений для системы уравнений $Ax^{\downarrow} = 0^{\downarrow}$. А тогда общее решение системы уравнений (31) имеет вид $a^{\downarrow} + a_1^{\downarrow}c_1 + \ldots + a_k^{\downarrow}c_k$, $c_i \in P$, $i \in \overline{1,k}$. Отсюда и следует, что совокупность решений системы $Ax^{\downarrow} = b^{\downarrow}$ есть H. $\square$

Утверждение 29 позволяет описать пересечение многообразий и найти базис пересечения подпространств. Если многообразие $H_i = a_i^{\downarrow} + L_i$, $i \in \overline{1,2}$, есть совокупность решений системы линейных уравнений

$$A_i x^{\downarrow} = b_i^{\downarrow},$$

то $H_1 \cap H_2 \neq \varnothing$ тогда и только тогда, когда совместна система линейных уравнений

$$\begin{pmatrix} A_1 \\ A_2 \end{pmatrix} x^{\downarrow} = \begin{pmatrix} b_1^{\downarrow} \\ b_2^{\downarrow} \end{pmatrix}. \tag{32}$$

В этом случае совокупность решений системы уравнений (32), очевидно, есть $H_1 \cap H_2$.

Для подпространств, т. е. при $a_i^{\downarrow} = 0^{\downarrow}$ и $b_i^{\downarrow} = 0^{\downarrow}$ получаем, что $L_1 \cap L_2$ есть совокупность решений системы однородных уравнений

$$\begin{pmatrix} A_1 \\ A_2 \end{pmatrix} x^{\downarrow} = 0^{\downarrow}. \tag{33}$$

Следовательно, базисом $L_1 \cap L_2$ является фундаментальная система решений системы уравнений (33).

ЗАДАЧИ

1. Покажите на примерах, что соотношения а)–г) определения векторного пространства независимы.

2. Покажите, что если $(L, +)$ — абелева группа и $\exp(L, +) = p$ — простое число, то на $(L, +)$ можно задать (единственным образом) структуру векторного пространства над полем $\mathbb{Z}/p$. При этом любая подгруппа в $(L, +)$ является подпространством.

3. Сколько подгрупп в элементарной абелевой группе порядка p^n?

4. Приведите пример векторного пространства L_P, в котором существует подгруппа $H < (L, +)$, не являющаяся подпространством.

5. Системы векторов S и T пространства L_P называют *эквивалентными*, если каждая из них линейно выражается через другую (пишут $S \sim T$). Покажите, что отношение $\sim$ есть отношение эквивалентности на множестве всех подсистем пространства L_P, и что $S \sim T$ тогда и только тогда, когда $(S)_P = (T)_P$.

6. Опишите конечные системы векторов из L_P, имеющие единственный базис.

7. Покажите, что если некоторый вектор $\alpha \in L_P$ однозначно линейно выражается через систему векторов S пространства L_P, то система S линейно независима.

8. Покажите, что всякое векторное пространство L_P, где $\dim L_P = n$, есть прямая сумма n одномерных подпространств. Сколькими разными способами можно представить L_P в виде такой суммы (с учетом порядка слагаемых), если $|P| = q$?

9. Пусть $K < L_P$, $\dim L_P = n$, $\dim K_P = t$ и $|P| = q$. Сколько существует различных подпространств $M < L_P$ таких, что $L = K \dotplus M$?

10. Пусть K и M — конечномерные подпространства векторного пространства L_P и $K \subset M$. Покажите, что $K = M$ тогда и только тогда, когда $\dim K_P = \dim M_P$.

11. Пусть $\dim L_P = n > 1$ и поле P бесконечно. Покажите, что при $k \in \overline{1, n-1}$ в L_P существует бесконечно много подпространств размерности k.

12. Покажите, что в условиях задачи 11 пространство L_P нельзя представить в виде объединения конечного числа собственных подпространств (используйте индукцию по n).

13. Пусть $H_i = \alpha_i + K_i$ — многообразия в пространстве L_P, $i \in \overline{1, 2}$. Покажите, что справедливы утверждения:

а) $H_1 \cap H_2 \neq \varnothing$ тогда и только тогда, когда $\alpha_1 - \alpha_2 \in K_1 + K_2$;

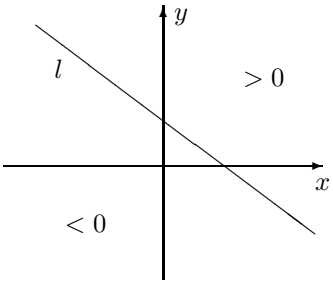
б) для любого $\alpha \in H_1 \cap H_2$ верно равенство $H_1 \cap H_2 = \alpha + (K_1 \cap K_2)$;

в) если $(H_1 \subset H_2)$, то $K_1 \subset K_2$ и $\alpha_1 - \alpha_2 \in K_2$.

Глава 14

СИСТЕМЫ ЛИНЕЙНЫХ НЕРАВЕНСТВ

Всякая прямая l: $ax + by + c = 0$ на плоскости D^2 разбивает эту плоскость на две полуплоскости в соответствии с условиями $ax + by + c \geqslant 0$ и $ax + by + c < 0$:



Точно так же, произвольная плоскость $ax + by + cz + d = 0$ в пространстве D^3 разбивает его на два полупространства $ax+by+cz+d \geqslant 0$ и $ax+by+cz+d < 0$. Поэтому всякий выпуклый многоугольник на плоскости и всякий выпуклый многогранник в пространстве могут быть заданы системами неравенств указанного выше типа.

Это послужило одной из причин, вызвавших потребность в изучении систем линейных неравенств. Первое систематическое изложение теории таких систем осуществил Г. Минковский[18] в книге «Геометрия чисел» (1896).

Рассмотрим задачу, возникающую в производстве. Предприятие выпускает n видов продукции, используя для этого m видов сырья, имеющегося в количестве b_i, $i \in \overline{1, m}$. Для производства единицы продукции j-го вида требуется a_{ij} единиц сырья i-го вида, а доход от ее реализации составляет c_j. Сколько следует произвести продукции каждого вида, чтобы суммарный доход предприятия был наибольшим?

Обозначим через x_i количество произведенной продукции i-го вида. Тогда ясно, что задача сводится к отысканию таких неотрицательных решений системы линейных неравенств

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n \leqslant b_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + \ldots + a_{mn}x_n \leqslant b_m, \end{cases}$$

при которых функция $f(x_1, \ldots, x_n) = \sum\limits_{i=1}^{n} c_i x_i$ принимает максимальное значение.

[18] Г. Минковский (1864–1909) — немецкий математик.

Решение подобных задач привело к созданию нового раздела математики — линейного программирования, основы которого в конце 1930-х годов были разработаны российским математиком Л. В. Канторовичем (1912–1986).

В настоящей главе мы рассмотрим первоначальные сведения по теории систем линейных неравенств над полем действительных чисел.

§ 1. НЕКОТОРЫЕ СВОЙСТВА СИСТЕМ ЛИНЕЙНЫХ УРАВНЕНИЙ

При изучении систем линейных неравенств нам понадобятся некоторые свойства систем линейных уравнений. Вначале докажем следующее утверждение о следствии системы линейных уравнений.

Утверждение 1. *Пусть*

$$Ax^{\downarrow} = b^{\downarrow} \tag{1}$$

— совместная система линейных уравнений над полем P, $A \in P_{m,n}$ и $\vec{c}x^{\downarrow} = d$ — такое уравнение над P, что из $A\alpha^{\downarrow} = b^{\downarrow}$ следует $\vec{c}\alpha^{\downarrow} = d$ для любого $\alpha^{\downarrow} \in P^{(n)}$. Тогда вектор $(\vec{c}, d)$ есть линейная комбинация строк матрицы $(A, b^{\downarrow})$.

□ Рассмотрим систему линейных уравнений:

$$\begin{pmatrix} A \\ \vec{c} \end{pmatrix} x^{\downarrow} = \begin{pmatrix} b^{\downarrow} \\ d \end{pmatrix}. \tag{2}$$

По условию системы уравнений (1) и (2) равносильны. Множество решений каждой из них есть линейное многообразие векторного пространства $P^{(n)}$ (см. пример 15 главы 13). Если $\alpha^{\downarrow} + M$ — множество решений системы уравнений (1), а $\beta^{\downarrow} + L$ — системы уравнений (2), то $\alpha^{\downarrow} + M = \beta^{\downarrow} + L$. По утверждению 28 главы 13 $M = L$.

Так как система уравнений (1) совместна, то $\operatorname{rang} A = r = \operatorname{rang}(A, b^{\downarrow})$. Ранг матрицы $D = \begin{pmatrix} A & b^{\downarrow} \\ \vec{c} & d \end{pmatrix}$ равен r либо $r+1$. Если $\operatorname{rang} D = r+1$, то $\dim L_P = n - (r+1)$. В то же время $\dim M_P = n - r \neq n - (r+1)$. Полученное противоречие показывает, что $\operatorname{rang} D = r$. Но $\operatorname{rang}(A, b^{\downarrow}) = r$, и, следовательно, строка $(\vec{c}, d)$ матрицы D есть линейная комбинация строк матрицы $(A, b^{\downarrow})$. □

Рассмотрим систему линейных уравнений (1) над полем $\mathbb{R}$ действительных чисел, $A \in \mathbb{R}_{m,n}$.

Вектор $d^{\downarrow} \in \mathbb{R}^{(n)}$ называют *неотрицательным*, если все его координаты неотрицательны (пишут: $d^{\downarrow} \geqslant 0^{\downarrow}$). При решении ряда задач возникает вопрос о существовании у системы уравнений (1) неотрицательных решений. Мы укажем один из способов отыскания ответа на этот вопрос.

Пусть система уравнений (1) совместна (для несовместной системы уравнений ответ на вопрос ясен), т. е. $\operatorname{rang} A = \operatorname{rang}(A, b^{\downarrow})$, и какая-либо ранговая подматрица матрицы A находится в ее столбцах $A^{\downarrow}_{i_1}, \ldots, A^{\downarrow}_{i_r}$. Переписывая систему уравнений (1) в виде

$$(A^{\downarrow}_{i_1},\dots,A^{\downarrow}_{i_r})\begin{pmatrix}x_{i_1}\\ \vdots\\ x_{i_r}\end{pmatrix}=b^{\downarrow}-(A^{\downarrow}_{j_1},\dots,A^{\downarrow}_{j_{n-r}})\begin{pmatrix}x_{j_1}\\ \vdots\\ x_{j_{n-r}}\end{pmatrix},$$

где $\{j_1,\dots,j_{n-r}\}=\overline{1,n}\backslash\{i_1,\dots,i_r\}$, и придавая свободным неизвестным $x_{j_1},\dots,x_{j_{n-r}}$ нулевые значения, однозначно определяем соответствующие значения связанных неизвестных: $x_{i_1}=c_{i_1},\ \dots,\ x_{i_r}=c_{i_r}$.

Полученное таким образом решение

$$c^{\downarrow}=(0,\dots,c_{i_1},\dots,c_{i_r},\dots,0)^T$$

системы уравнений (1) называют ее *опорным решением*, соответствующим базису $A^{\downarrow}_{i_1},\dots,A^{\downarrow}_{i_r}$ системы столбцов матрицы A.

Примером опорного решения служит нулевое решение системы однородных линейных уравнений — оно соответствует произвольному базису системы столбцов матрицы этой системы уравнений.

Теорема 2. *Совместная система уравнений* (1) *над полем* $\mathbb{R}$ *имеет неотрицательные решения тогда и только тогда, когда она имеет неотрицательные опорные решения.*

□ Утверждение теоремы в одну сторону очевидно. Докажем ее нетривиальную часть. Пусть система уравнений (1) имеет неотрицательные решения. Среди всех неотрицательных решений этой системы выберем решение $c^{\downarrow}\geqslant 0^{\downarrow}$ с максимально возможным числом нулевых элементов. Если при этом $c^{\downarrow}=0^{\downarrow}$, то $b^{\downarrow}=0^{\downarrow}$, и, как замечено выше, $c^{\downarrow}$ — опорное решение. Поэтому можем считать, что $c^{\downarrow}\neq 0^{\downarrow}$.

Пусть $c_{i_1},\dots,c_{i_k}$ — ненулевые элементы вектора $c^{\downarrow}$. Так как $c^{\downarrow}$ — решение системы уравнений (1), то

$$A^{\downarrow}_{i_1}c_{i_1}+\ldots+A^{\downarrow}_{i_k}c_{i_k}=b^{\downarrow}.$$

Предположим, что система векторов $A^{\downarrow}_{i_1},\dots,A^{\downarrow}_{i_k}$ линейно зависима, т. е. верно $A^{\downarrow}_{i_1}d_1+\ldots+A^{\downarrow}_{i_k}d_k=0^{\downarrow}$ для некоторых $d_i\in\mathbb{R}$ и существует $d_j\neq 0$, $i,j\in\overline{1,k}$. Очевидно, можем считать, что $d_j>0$.

Обозначим через $d_sc^{-1}_{i_s}$ максимальный элемент множества $M=\{d_1c^{-1}_{i_1},\dots,d_kc^{-1}_{i_k}\}$. Так как $d_jc^{-1}_{i_j}\in M$ и $d_j,c_{i_j}>0$, то $d_sc^{-1}_{i_s}>0$ и $d_s>0$. Справедливы равенства:

$$\begin{aligned}b^{\downarrow}&=b^{\downarrow}-0^{\downarrow}=\sum_{t=1}^{k}A^{\downarrow}_{i_t}c_{i_t}-\sum_{t=1}^{k}A_{i_t}d_t=\\&=\sum_{t=1}^{k}A^{\downarrow}_{i_t}c_{i_t}-\Bigl(\sum_{t=1}^{k}A^{\downarrow}_{i_t}d_t\Bigr)c_{i_s}d_s^{-1}=\sum_{t=1}^{k}A^{\downarrow}_{i_t}(c_{i_t}-d_tc_{i_s}d_s^{-1}).\end{aligned}\tag{3}$$

Положим $m_t=c_{i_t}-d_tc_{i_s}d_s^{-1}$. При $t=s$ имеем $m_s=0$. При $t\neq s$ имеем $m_t=(c_{i_t}d_s-d_tc_{i_s})d_s^{-1}$, где $d_s>0$. Поскольку

$$d_sc^{-1}_{i_s}-d_tc^{-1}_{i_t}=c^{-1}_{i_s}c^{-1}_{i_t}\cdot(c_{i_t}d_s-d_tc_{i_s})\geqslant 0$$

и $c_{i_s}c_{i_t} > 0$, то $m_t \geqslant 0$. Из (3) следует, что

$$\sum_{t=1}^{k} A^{\downarrow}_{i_t} m_t = b^{\downarrow}, \quad m_t \geqslant 0, \quad m_s = 0,$$

т. е. вектор $m^{\downarrow} = (0, \ldots, m_1, \ldots, m_k, \ldots, 0)^T$ есть решение системы уравнений (1) с большим, чем у решения $c^{\downarrow}$, числом нулевых координат. Полученное противоречие показывает, что система векторов $A^{\downarrow}_{i_1}, \ldots, A^{\downarrow}_{i_k}$ линейно независима.

Дополнив, если нужно, эту систему до базиса системы столбцов матрицы A векторами $A^{\downarrow}_{i_{k+1}}, \ldots, A^{\downarrow}_{i_r}$, получим равенство

$$A^{\downarrow}_{i_1} c_{i_1} + \ldots + A^{\downarrow}_{i_k} c_{i_k} + A^{\downarrow}_{i_{k+1}} 0 + \ldots + A^{\downarrow}_{i_r} 0 = b^{\downarrow},$$

показывающее, что $c^{\downarrow}$ — опорное решение системы уравнений (1), соответствующее базису $A^{\downarrow}_{i_1}, \ldots, A^{\downarrow}_{i_r}$ системы столбцов матрицы A. □

Поскольку в системе векторов-столбцов матрицы A имеется конечное число базисов, то система уравнений (1) имеет конечное число опорных решений.

§ 2. СИСТЕМЫ ЛИНЕЙНЫХ НЕРАВЕНСТВ И СВЕДЕНИЕ ИХ К СИСТЕМАМ ЛИНЕЙНЫХ УРАВНЕНИЙ

Решая систему линейных уравнений (1), где $A \in \mathbb{R}_{m,n}$, мы по существу (см. § 1 главы 8) рассматриваем отображение $\varphi_A \colon \mathbb{R}^{(n)} \to \mathbb{R}^{(m)}$, определенное условием

$$\forall\, c^{\downarrow} \in \mathbb{R}^{(n)} : \ \varphi_A(c^{\downarrow}) = Ac^{\downarrow},$$

и находим полный прообраз данного вектора $b^{\downarrow} \in \mathbb{R}^{(m)}$ при этом отображении. Если прообраз — пустое множество, то система уравнений (1) несовместна, а если прообраз — непустое множество, то он является подпространством в $\mathbb{R}^{(n)}$ при $b^{\downarrow} = 0^{\downarrow}$ и линейным многообразием при $b^{\downarrow} \neq 0^{\downarrow}$.

Возможна (и нужна) постановка более общих задач: например, выяснить, является ли отображение φ_A сюръективным (т. е. совместна ли система уравнений (1) при любом (!) $b^{\downarrow} \in \mathbb{R}^{(m)}$) или найти полный прообраз при отображении φ_A заданного подмножества из $\mathbb{R}^{(m)}$, состоящего более чем из одного вектора.

Для векторов из $\mathbb{R}^{(m)}$ будем писать $a^{\downarrow} \geqslant b^{\downarrow}$, если $a^{\downarrow} - b^{\downarrow} \geqslant 0^{\downarrow}$. Частным случаем второй из указанных задач является следующая: при заданном векторе $b^{\downarrow} \in \mathbb{R}^{(m)}$ найти полный прообраз множества $\{d^{\downarrow} \in \mathbb{R}^{(m)} : \ d^{\downarrow} \leqslant b^{\downarrow}\}$ при отображении φ_A. В этом случае говорят, что нужно решить *систему линейных неравенств*

$$Ax^{\downarrow} \leqslant b^{\downarrow}. \tag{4}$$

Для систем линейных неравенств точно так же, как и для систем линейных уравнений, вводят понятия *решения* системы, *совместной* (*несовместной*) системы и *равносильных* систем.

Задача отыскания решений системы неравенств (4) может быть сведена к отысканию специальных решений некоторой системы линейных уравнений.

Теорема 3. *Вектор $c^{\downarrow} \in \mathbb{R}^{(n)}$ является решением системы неравенств* (4) *тогда и только тогда, когда существует такой вектор $d^{\downarrow} \in \mathbb{R}^{(m)}$, что $d^{\downarrow} \geqslant 0^{\downarrow}$ и вектор $\begin{pmatrix} c^{\downarrow} \\ d^{\downarrow} \end{pmatrix}$ — решение системы линейных уравнений*

$$(A_{m\times n},\, E_{m\times m})\begin{pmatrix} x^{\downarrow} \\ y^{\downarrow} \end{pmatrix} = b^{\downarrow}. \tag{5}$$

□ Пусть вектор $\begin{pmatrix} c^{\downarrow} \\ d^{\downarrow} \end{pmatrix}$, где $d^{\downarrow} \geqslant 0^{\downarrow}$, есть решение системы уравнений (5). Тогда для $i \in \overline{1,m}$ имеем

$$\sum_{k=1}^{n} a_{i_k} c_k + d_i = b_i.$$

Поскольку $d_i \geqslant 0$, то $\sum_{k=1}^{n} a_{i_k} c_k = b_i - d_i \leqslant b_i$. Следовательно, $c^{\downarrow}$ — решение системы неравенств (4).

Обратно, пусть $c^{\downarrow}$ — решение системы неравенств (4). Положим

$$d_i = b_i - \sum_{k=1}^{n} a_{i_k} c_k, \quad i \in \overline{1,m}.$$

Тогда $d_i \geqslant 0$ и вектор $\begin{pmatrix} c^{\downarrow} \\ d^{\downarrow} \end{pmatrix}$ — решение системы уравнений (5). □

Пример 1. Решить систему неравенств

$$\begin{cases} 2x_1 - x_2 \leqslant 1, \\ -x_1 + x_2 \leqslant 0. \end{cases}$$

Составляем систему уравнений

$$\begin{cases} 2x_1 - x_2 + x_3 = 1, \\ -x_1 + x_2 + x_4 = 0. \end{cases}$$

Ее общее решение имеет вид

$$\begin{pmatrix} 1 - x_3 - x_4 \\ 1 - x_3 - 2x_4 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} -1 \\ -1 \\ 1 \\ 0 \end{pmatrix} x_3 + \begin{pmatrix} -1 \\ -2 \\ 0 \\ 1 \end{pmatrix} x_4.$$

В силу теоремы 3 всякое решение исходной системы неравенств имеет вид

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix} + \begin{pmatrix} -1 \\ -1 \end{pmatrix} x_3 + \begin{pmatrix} -1 \\ -2 \end{pmatrix} x_4; \quad x_3,\, x_4 \geqslant 0.$$

Пример 2. Решить систему неравенств

$$\begin{cases} x_1 + x_2 \leqslant 1, \\ -x_1 - x_2 \leqslant 0. \end{cases}$$

Общее решение системы уравнений

$$\begin{cases} x_1 + x_2 + x_3 = 1, \\ -x_1 - x_2 + x_4 = 0 \end{cases}$$

имеет вид

$$\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \end{pmatrix} x_2 + \begin{pmatrix} 1 \\ 0 \\ -1 \\ 1 \end{pmatrix} x_4.$$

Тогда всякое решение исходной системы неравенств имеет вид

$$\begin{pmatrix} -1 \\ 1 \end{pmatrix} x_2 + \begin{pmatrix} 1 \\ 0 \end{pmatrix} x_4,$$

где $1 - x_4 \geqslant 0$, $x_4 \geqslant 0$, т. е. $1 \geqslant x_4 \geqslant 0$, $x_2 \in \mathbb{R}$.

Пример 3. Решить систему неравенств

$$\begin{cases} x_1 + x_2 \leqslant 1, \\ -x_1 - x_2 \leqslant -2. \end{cases}$$

Общее решение системы уравнений

$$\begin{cases} x_1 + x_2 + x_3 = 1, \\ -x_1 - x_2 + x_4 = -2 \end{cases}$$

имеет вид

$$\begin{pmatrix} 2 \\ 0 \\ -1 \\ 0 \end{pmatrix} + \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \end{pmatrix} x_2 + \begin{pmatrix} 1 \\ 0 \\ -1 \\ 1 \end{pmatrix} x_4,$$

а тогда всякое решение исходной системы неравенств имеет вид

$$\begin{pmatrix} 2 \\ 0 \end{pmatrix} + \begin{pmatrix} -1 \\ 1 \end{pmatrix} x_2 + \begin{pmatrix} 1 \\ 0 \end{pmatrix} x_4,$$

где $-1 - x_4 \geqslant 0$, $x_4 \geqslant 0$, т. е. $x_4 \geqslant 0$ и $x_4 \leqslant -1$. Следовательно, система неравенств несовместна.

Приведенные примеры показывают, что общее решение системы неравенств (4), найденное с помощью теоремы 3, зависит от параметров $x_{n+1} \geqslant 0, \ldots, x_{n+m} \geqslant 0$, область значений которых определяется из системы линейных неравенств, которую, возможно, придется в свою очередь решать.

§ 3. КРИТЕРИЙ СОВМЕСТНОСТИ СИСТЕМЫ ЛИНЕЙНЫХ НЕРАВЕНСТВ

Предварительно рассмотрим некоторые свойства систем линейных неравенств. Если система линейных неравенств $Ax^{\downarrow} \leqslant b^{\downarrow}$, $A \in \mathbb{R}_{m,n}$, и неравенство $\vec{c}x^{\downarrow} \leqslant d$ таковы, что для любого $\alpha^{\downarrow} \in \mathbb{R}^{(n)}$ из $A\alpha^{\downarrow} \leqslant b^{\downarrow}$ следует $\vec{c}\alpha^{\downarrow} \leqslant d$, то неравенство $\vec{c}x^{\downarrow} \leqslant d$ называют *следствием системы неравенств* $Ax^{\downarrow} \leqslant b^{\downarrow}$.

Утверждение 4. *Если неравенство $\vec{c}x^{\downarrow} \leqslant 0$ есть следствие системы неравенств $Ax^{\downarrow} \leqslant 0^{\downarrow}$, то вектор $\vec{c}$ является линейной комбинацией строк матрицы A.*

□ Рассмотрим систему линейных уравнений $A_{m\times n}x^{\downarrow} = 0^{\downarrow}$. Если $\beta^{\downarrow} \in \mathbb{R}^{(n)}$ и $A\beta^{\downarrow} = 0^{\downarrow}$, то и $A(-\beta^{\downarrow}) = 0^{\downarrow}$. По условию тогда $\vec{c}\beta^{\downarrow} \leqslant 0$ и $\vec{c}(-\beta^{\downarrow}) \leqslant 0$. Значит, $\vec{c}\beta^{\downarrow} = 0$. По утверждению 1 вектор $(\vec{c}, 0)$ есть линейная комбинация строк матрицы $(A, 0^{\downarrow})$. □

Лемма 5. *Если неравенство $\vec{c}x^{\downarrow} \leqslant 0$ есть следствие системы неравенств $Ax^{\downarrow} \leqslant 0^{\downarrow}$ и $\vec{c} = \sum_{i=1}^{m} \vec{A}_i\lambda_i$, где $\lambda_1, \ldots, \lambda_{m-1} \geqslant 0$ и $\lambda_m < 0$, то неравенство $\vec{c}x^{\downarrow} \leqslant 0$ является следствием системы неравенств*

$$\begin{pmatrix} \vec{A}_1 \\ \ldots \\ \vec{A}_{m-1} \end{pmatrix} x^{\downarrow} \leqslant 0^{\downarrow}. \tag{6}$$

□ Пусть $\gamma^{\downarrow}$ — произвольное решение системы неравенств (6). При этом либо $\vec{A}_m\gamma^{\downarrow} \leqslant 0$, и тогда $\gamma^{\downarrow}$ — решение системы $Ax^{\downarrow} \leqslant 0^{\downarrow}$ и $\vec{c}\gamma^{\downarrow} \leqslant 0$, либо $\vec{A}_m\gamma^{\downarrow} \geqslant 0$, и снова $\vec{c}\gamma^{\downarrow} = \sum_{i=1}^{m-1} \vec{A}_i\gamma^{\downarrow}\lambda_i + \vec{A}_m\gamma^{\downarrow}\lambda_m \leqslant 0$. □

Уточнением утверждения 4 является следующая

Теорема 6 (Минковский). *Если неравенство $\vec{c}x^{\downarrow} \leqslant 0$ есть следствие системы неравенств $Ax^{\downarrow} \leqslant 0^{\downarrow}$, то вектор $\vec{c}$ является линейной комбинацией системы строк матрицы A с неотрицательными коэффициентами.*

□ Пусть $A = (a_{ij})_{m\times n}$. Если $A = O_{m\times n}$, то $\vec{c} = \vec{0}$, и утверждение теоремы очевидно. Пусть $A \neq O_{m\times n}$. Доказательство теоремы проведем индукцией по числу m неравенств системы.

Пусть $m = 1$, т. е. система неравенств имеет вид

$$\vec{A}_1x^{\downarrow} = a_{11}x_1 + \ldots + a_{1n}x_n \leqslant 0. \tag{7}$$

Перенумеровав, если нужно, неизвестные, будем считать, что $a_{11} \neq 0$. Пусть $a_{11} > 0$. Тогда вектор $(-1, 0, \ldots, 0)$ — решение неравенства (7) и, значит, решение неравенства $\vec{c}x^{\downarrow} \leqslant 0$. Отсюда $c_1 \geqslant 0$. По утверждению 4 $\vec{c} = \vec{A}_1\lambda_1$. Следовательно, $c_1 = a_{11}\lambda_1$ и $\lambda_1 = c_1a_{11}^{-1} \geqslant 0$, что и требовалось. Ясно, как изменить доказательство в случае $a_{11} < 0$.

Пусть утверждение теоремы верно для любой системы неравенств $Bx^{\downarrow} \leqslant 0^{\downarrow}$ и ее следствия $\vec{d}x^{\downarrow} \leqslant 0$, где $B \in \mathbb{R}_{k,n}$, $k \leqslant m - 1$.

Рассмотрим систему неравенств $Ax^{\downarrow} \leqslant 0^{\downarrow}$, где $A \in \mathbb{R}_{m,n}$. По утверждению 4 $\vec{c} = \sum_{i=1}^{m} \vec{A}_i\lambda_i = \vec{\lambda}A$. Среди всех таких векторов $\lambda^{\downarrow}$, что $c^{\downarrow} = A^T\lambda^{\downarrow}$, возьмем вектор $\lambda^{\downarrow}$ с максимальным числом s неотрицательных элементов. Перенумеровав, если нужно, уравнения, можем считать, что $\lambda_1, \ldots, \lambda_s \geqslant 0$. Если $s = m$, то теорема доказана. Пусть $s < m$. Рассмотрим вектор $\vec{f} = \sum_{i=1}^{s} \vec{A}_i\lambda_i + \vec{A}_m\lambda_m$. Тогда $\vec{c} - \vec{f} = \sum_{s<k<m} \vec{A}_k\lambda_k$.

Пусть $A\alpha^{\downarrow} \leqslant 0^{\downarrow}$. Тогда

$$(\vec{c} - \vec{f})\alpha^{\downarrow} = \sum_{s<k<m} \vec{A}_k\lambda_k\alpha^{\downarrow} = \sum_{s<k<m} (\vec{A}_k\alpha^{\downarrow})\lambda_k \geqslant 0,$$

$\vec{c}\alpha^{\downarrow} \leqslant 0$ и $\vec{f}\alpha^{\downarrow} = \vec{c}\alpha^{\downarrow} - (\vec{c} - \vec{f})\alpha^{\downarrow} \leqslant 0$. Так как

$$\vec{f} = \sum_{i=1}^{s} \vec{A}_i\lambda_i + \vec{A}_{s+1}0 + \ldots + \vec{A}_{m-1}0 + \vec{A}_m\lambda_m,$$

то по лемме 5 всякое решение системы неравенств (6) является решением неравенства $\vec{f}x^{\downarrow} \leqslant 0$. По предположению индукции вектор $\vec{f}$ есть линейная комбинация векторов $\vec{A}_1, \ldots, \vec{A}_{m-1}$ с неотрицательными коэффициентами:

$$\vec{f} = \sum_{i=1}^{m-1} \vec{A}_i r_i, \quad r_i \geqslant 0.$$

Тогда

$$\vec{c} = \sum_{s<k<m} \vec{A}_k\lambda_k + \vec{f} = \sum_{s<k<m} \vec{A}_k\lambda_k + \sum_{i=1}^{m-1} \vec{A}_i r_i = \vec{A}_1 r_1 + \ldots + \vec{A}_s r_s + \\ + \vec{A}_{s+1}(r_{s+1} + \lambda_{s+1}) + \ldots + \vec{A}_{m-1}(r_{m-1} + \lambda_{m-1}) + \vec{A}_m 0,$$

т. е. вектор $\vec{c}$ есть линейная комбинация строк матрицы A с большим, чем s, числом неотрицательных элементов. Полученное противоречие показывает, что $s = m$. □

Докажем теперь критерий совместности (несовместности) системы неравенств.

Теорема 7. *Система линейных неравенств* (4):

$$Ax^{\downarrow} \leqslant b^{\downarrow}$$

несовместна тогда и только тогда, когда система линейных уравнений

$$\begin{pmatrix} A^T \\ \vec{b} \end{pmatrix} y^{\downarrow} = \begin{pmatrix} 0^{\downarrow} \\ -1 \end{pmatrix} \tag{8}$$

имеет неотрицательное решение.

□ Пусть система уравнений (8) имеет неотрицательное решение $\beta^{\downarrow}$, и $\alpha^{\downarrow}$ — некоторое решение системы неравенств (4). Тогда $A^T\beta^{\downarrow} = 0^{\downarrow}$, и справедливы соотношения

$A\alpha^{\downarrow} \leqslant b^{\downarrow}$, $\vec{\alpha}A^T \leqslant \vec{b}$ и $\vec{\alpha}A^T\beta^{\downarrow} \leqslant \vec{b}\beta^{\downarrow}$, так как $\beta^{\downarrow} \geqslant 0^{\downarrow}$. Следовательно, $\vec{\alpha} \cdot 0^{\downarrow} \leqslant -1$ и $0 \leqslant -1$. Полученное противоречие показывает, что система неравенств (4) несовместна.

Пусть теперь система неравенств (4) несовместна. Рассмотрим вспомогательную систему неравенств:

$$Dy^{\downarrow} = (A, -b^{\downarrow}) \begin{pmatrix} x^{\downarrow} \\ x_{n+1} \end{pmatrix} \leqslant 0^{\downarrow}. \tag{9}$$

Если $\alpha^{\downarrow} = (\alpha_1, \ldots, \alpha_n, \alpha_{n+1})^T$ — решение системы неравенств (9), то при $\alpha_{n+1} > 0$ получаем, что $(\alpha_1\alpha_{n+1}^{-1}, \ldots, \alpha_n\alpha_{n+1}^{-1})^T$ — решение системы неравенств (4). Следовательно, $\alpha_{n+1} \leqslant 0$. Это означает, что всякое решение системы неравенств (9) является решением неравенства

$$0x_1 + \ldots + 0x_n + x_{n+1} \leqslant 0.$$

По теореме Минковского

$$\vec{c} = (0, 0, \ldots, 0, 1) = \sum_{i=1}^{m} \vec{D}_i\lambda_i, \quad \lambda_i \geqslant 0.$$

Но тогда справедливы равенства

$$\begin{pmatrix} A^T \\ -\vec{b} \end{pmatrix} \lambda^{\downarrow} = D^T\lambda^{\downarrow} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} A^T \\ \vec{b} \end{pmatrix} \lambda^{\downarrow} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -1 \end{pmatrix},$$

т. е. $\lambda^{\downarrow}$ — неотрицательное решение системы уравнений (8). □

§ 4. СИСТЕМЫ ОДНОРОДНЫХ ЛИНЕЙНЫХ НЕРАВЕНСТВ

Систему неравенств

$$Ax^{\downarrow} \leqslant 0^{\downarrow} \tag{10}$$

называют *системой однородных неравенств*.

Утверждение 8. *Если $c_1^{\downarrow}, \ldots, c_s^{\downarrow}$ — решения системы неравенств* (10) *и $\lambda_i \geqslant 0$, $i \in \overline{1, s}$, то вектор $c^{\downarrow} = \sum_{i=1}^{s} c_i^{\downarrow}\lambda_i$ является решением системы неравенств* (10).

□ Так как $Ac^{\downarrow} = A\left(\sum_{i=1}^{s} c_i^{\downarrow}\lambda_i\right) = \sum_{i=1}^{s}(Ac_i^{\downarrow})\lambda_i$, $Ac_i^{\downarrow} \leqslant 0^{\downarrow}$ и $(Ac_i^{\downarrow})\lambda_i \leqslant 0^{\downarrow}$, то $c^{\downarrow}$ — решение системы неравенств (10). □

Утверждение 9. *Если $c^{\downarrow}$ — решение системы неравенств* (4)*, а $d^{\downarrow}$ — решение системы неравенств* (10)*, то вектор $c^{\downarrow} + d^{\downarrow}$ — решение системы неравенств* (4).

□ Справедливость утверждения следует из соотношений

$$A(c^{\downarrow} + d^{\downarrow}) = Ac^{\downarrow} + Ad^{\downarrow} \leqslant b^{\downarrow} + 0^{\downarrow} = b^{\downarrow}. \quad \square$$

Таким образом, для решений систем линейных неравенств частично выполняются те же соотношения, что и для решений системы линейных уравнений и ассоциированной с ней системы однородных уравнений.

ЗАДАЧИ

1. Задайте множество точек плоскости, находящихся внутри и на сторонах треугольника с вершинами $A(-2,0)$, $B(1,3)$ и $C(4,0)$, системой линейных неравенств.

2. Найдите опорные решения системы линейных уравнений:

а) $\begin{cases} x_1 + x_2 - x_3 - x_4 = 1, \\ 2x_1 - x_2 + x_3 - x_4 = 0, \\ x_1 - x_2 + x_3 + 2x_4 = -2, \end{cases}$ б) $\begin{cases} 5x_1 + x_2 - 5x_4 = 2, \\ -7x_1 - x_2 + x_3 + 2x_4 = -5. \end{cases}$

Имеет ли эта система уравнений неотрицательные решения?

3. Решите систему неравенств:

а) $\begin{cases} x - y + 3 \leqslant 0, \\ -x + y - 3 \leqslant 0, \\ x + 2y \geqslant 0, \end{cases}$ б) $\begin{cases} x - y + 2 \geqslant 0, \\ x + y - 4 \leqslant 0, \\ y \geqslant 0. \end{cases}$

Изобразите на плоскости область решений.

4. Покажите, что система неравенств $A_{m\times n}x^{\downarrow} \leqslant 0^{\downarrow}$ при $m \leqslant n$ имеет ненулевое решение.

5. Выясните, совместна или нет система неравенств

$$\begin{cases} 4x_1 - 5x_2 \geqslant 3, \\ -2x_1 - 7x_2 \geqslant 1, \\ -2x_1 + x_2 \geqslant -2. \end{cases}$$

Глава 15

ЛИНЕЙНЫЕ ПРЕОБРАЗОВАНИЯ ВЕКТОРНЫХ ПРОСТРАНСТВ

Предметом исследования многих математических дисциплин является изучение отображений множеств. Так, в математическом анализе изучают, например, действительные функции одного или нескольких переменных, т. е. отображения $\mathbb{R} \to \mathbb{R}$ или $\mathbb{R}^n \to \mathbb{R}$. В аналитической геометрии рассматривают переход от одной системы координат на плоскости или в пространстве к другой, т. е. отображения $D^2 \to D^2$ и $D^3 \to D^3$. В алгебре изучают множества с операциями, а внутренняя бинарная операция на множестве M — это отображение $M \times M \to M$. В предыдущих главах рассматривались отображения как произвольных множеств, так и множеств с заданными на них операциями: подстановки на множестве M, т. е. биекции $M \to M$, гомоморфизмы группоидов, в частности групп, и др.

В этой главе мы рассмотрим важный класс отображений векторных пространств — линейные отображения, или гомоморфизмы. Наиболее подробно будут изучены линейные отображения данного векторного пространства L_P в себя — линейные преобразования пространства L_P.

§ 1. ЛИНЕЙНЫЕ ОТОБРАЖЕНИЯ

Определение 1. Отображение φ пространства L_P в пространство M_P называют *линейным отображением*, или *гомоморфизмом*, если для любых $\alpha, \beta \in L_P$ и $a \in P$ справедливы равенства

$$\varphi(\alpha + \beta) = \varphi(\alpha) + \varphi(\beta), \quad \varphi(\alpha a) = \varphi(\alpha)a.$$

Множество всех линейных отображений пространства L_P в пространство M_P обозначим через $\mathfrak{L}(L_P, M_P)$.

Для любого отображения $\varphi \in \mathfrak{L}(L_P, M_P)$ справедливо равенство $\varphi(\theta_L) = \theta_M$, так как φ — гомоморфизм группы $(L, +)$ в группу $(M, +)$.

Пример 1. Всякий изоморфизм пространства L_P на пространство M_P (см. определение 11 главы 13) является линейным отображением. В частности, поворот плоскости D^2 на угол ω против часовой стрелки вокруг начала координат (пример 9 главы 13) является линейным отображением D^2 в D^2.

Пример 2. Пусть $a \in P$. Зададим отображение $\widehat{a}\colon L_P \to L_P$, положив $\widehat{a}(\alpha) = \alpha a$ для $\alpha \in L_P$. Легко проверить, что $\widehat{a}$ — линейное отображение. Его называют *скалярным отображением*, или *гомотетией*. При $a \neq 0$ гомотетия $\widehat{a}$ является изоморфизмом.

Пример 3. Отображение $\varphi\colon \mathbb{C}_{\mathbb{R}} \to \mathbb{C}_{\mathbb{R}}$, где $\varphi(z) = \overline{z}$, как нетрудно проверить, есть линейное отображение. Отображение $\psi\colon \mathbb{C}_{\mathbb{C}} \to \mathbb{C}_{\mathbb{C}}$, где $\psi(z) = \overline{z}$, не является линейным, так как $\psi(zz_1) = \overline{zz_1} = \overline{z}\,\overline{z}_1 \neq \psi(z)z_1$ при $z_1 \in \mathbb{C} \setminus \mathbb{R}$.

Пример 4. Пусть α — фиксированный ненулевой вектор пространства D^3. Отображение $\varphi\colon D^3 \to D^3$, при котором $\varphi(\beta) = \beta + \alpha$ для любого $\beta \in D^3$ (перенос начала координат), не является линейным отображением, так как $\varphi(\theta) = \alpha \neq \theta$.

Как и в теории групп, введем понятие ядра линейного отображения.

Определение 2. *Ядром линейного отображения* $\varphi \in \mathfrak{L}(L_P, M_P)$ называют множество $\operatorname{Ker}\varphi = \{\alpha \in L_P :\ \varphi(\alpha) = \theta_M\}$.

Непосредственной проверкой устанавливается, что справедливо

Утверждение 1. *Если* $\varphi \in \mathfrak{L}(L_P, M_P)$, *то* $\operatorname{Ker}\varphi$ *и* $\varphi(L_P)$ — *подпространства соответственно пространств* L_P *и* M_P. *Отображение* φ *является изоморфизмом пространств тогда и только тогда, когда* $\operatorname{Ker}\varphi = \theta_L$ *и* $\varphi(L) = M$.

Пример 5. Пусть K_P — произвольное подпространство в L_P. Определим отображение $\varphi_0\colon L_P \to L_P/K_P$, положив

$$\forall\, \alpha \in L_P\ (\varphi_0(\alpha) = [\alpha] = \alpha + K_P). \tag{1}$$

Нетрудно проверить, что отображение φ_0 является линейным отображением пространства L_P на факторпространство L_P/K_P, т. е. является эпиморфизмом пространств.

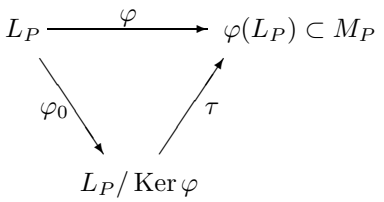
Определение 3. Линейное отображение φ_0, заданное формулой (1), называют *естественным эпиморфизмом* пространства L_P на факторпространство L_P/K_P.

Любое линейное отображение сводится к некоторому естественному эпиморфизму и некоторому изоморфизму, как показывает

Теорема 2 (об эпиморфизме). *Если* $\varphi \in \mathfrak{L}(L_P, M_P)$, *то существует такой изоморфизм пространств*

$$\tau\colon L_P/\operatorname{Ker}\varphi \to \varphi(L_P),$$

что коммутативна диаграмма



где φ_0 — *естественный эпиморфизм.*

□ По утверждению 1 $\operatorname{Ker}\varphi$ — подпространство в L_P. Если рассматривать группы $(L,+)$, $(M,+)$ и $(\operatorname{Ker}\varphi,+)$, то по теореме об эпиморфизме групп существует изоморфизм групп $\tau\colon L/\operatorname{Ker}\varphi \to \varphi(L_P)$, при котором коммутативна указанная диаграмма. Этот изоморфизм задается равенством $\tau([\alpha]) = \varphi(\alpha)$.

Поскольку для любых $[\alpha] \in L_P/\operatorname{Ker}\varphi$ и $a \in P$ справедливы равенства

$$\tau([\alpha]a) = \tau([\alpha a]) = \varphi(\alpha a) = \varphi(\alpha)a = \tau([\alpha])a,$$

то τ — линейное отображение. Значит, τ — изоморфизм векторных пространств. □

Теперь определим на множестве $\mathfrak{L}(L_P, M_P)$ внутреннюю операцию сложения и внешнюю операцию умножения на элементы поля P, положив для $\varphi,\ \psi \in \mathfrak{L}(L_P, M_P)$ и $a \in P$

$$\begin{aligned} &\forall\,\alpha \in L_P\colon\ (\varphi+\psi)(\alpha) = \varphi(\alpha) + \psi(\alpha),\\ &\forall\,\alpha \in L_P,\ a \in P\colon\ (\varphi \odot a)(\alpha) = \varphi(\alpha)a. \end{aligned} \tag{2}$$

Читателю предлагается проверить, что $\varphi+\psi$ и $\varphi\odot a$ — линейные отображения L_P в M_P, т. е. что формулы (2) действительно задают операции на множестве $\mathfrak{L}(L_P, M_P)$.

Теорема 3. *Для произвольных векторных пространств L_P и M_P множество $\mathfrak{L}(L_P, M_P)$ является векторным пространством над полем P относительно операций, заданных формулами* (2).

Доказательство теоремы осуществляется непосредственной проверкой аксиом векторного пространства и предоставляется читателю. Обратим внимание на то, что нулем пространства $\mathfrak{L}(L_P, M_P)_P$ является отображение $\tilde{\theta}\colon L_P \to \theta_M$, а противоположное отображение $-\varphi$ для отображения $\varphi \in \mathfrak{L}(L_P, M_P)$ определяется равенством $(-\varphi)(\alpha) = -\varphi(\alpha)$, $\alpha \in L_P$.

Если пространство L_P конечномерное, то легко описать все его линейные отображения в произвольное пространство M_P.

Утверждение 4. *Пусть* $\dim L_P = n$, $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ *— базис пространства L_P и M_P — произвольное пространство. Тогда*

(а) *всякое отображение $\varphi \in \mathfrak{L}(L_P, M_P)$ однозначно определяется образами $\varphi(\alpha_i)$, $i \in \overline{1,n}$, базисных векторов пространства L_P;*

(б) *для любых векторов $\beta_1, \ldots, \beta_n$ пространства M_P существует единственное отображение $\psi \in \mathfrak{L}(L_P, M_P)$, при котором $\psi(\alpha_i) = \beta_i$, $i \in \overline{1,n}$.*

□ (а) Обозначим $\varphi(\vec{\alpha}) = (\varphi(\alpha_1), \ldots, \varphi(\alpha_n))$. Так как $\varphi \in \mathfrak{L}(L_P, M_P)$, то для произвольного вектора $\gamma = \sum_{i=1}^{n} \alpha_i a_i = \vec{\alpha}\gamma_{\vec{\alpha}}^{\downarrow}$ пространства L_P справедливы равенства

$$\varphi(\gamma) = \varphi\Big(\sum_{i=1}^{n} \alpha_i a_i\Big) = \sum_{i=1}^{n} \varphi(\alpha_i)a_i = \varphi(\vec{\alpha})\gamma_{\vec{\alpha}}^{\downarrow}. \tag{3}$$

Остается заметить, что для любого вектора $\gamma \in L_P$ столбец координат $\gamma_{\vec{\alpha}}^{\downarrow}$ определен однозначно.

(б) Для произвольного вектора $\gamma = \sum_{i=1}^{n} \alpha_i a_i$ пространства L_P положим по определению

$$\psi(\gamma) = \sum_{i=1}^{n} \beta_i a_i.$$

Легко проверить, что $\psi \in \mathfrak{L}(L_P, M_P)$ и $\psi(\alpha_i) = \beta_i$, $i \in \overline{1,n}$, т. е. ψ — требуемое отображение. Его единственность следует из утверждения (а). □

Замечание 1. Утверждение 4(б) устанавливает взаимно однозначное соответствие между множеством $\mathfrak{L}(L_P, M_P)$, где $\dim L_P = n$, и множеством всех систем векторов пространства M_P, состоящих из n векторов.

Уточним теорему об эпиморфизме.

Утверждение 5. *Если в условиях теоремы 2 пространство L_P конечномерное, то* $\dim \varphi(L_P)_P = \dim L_P - \dim \operatorname{Ker} \varphi$.

□ По теореме 2 пространства $L_P/\operatorname{Ker}\varphi$ и $\varphi(L_P)$ изоморфны. Тогда по теореме 21 главы 13 $\dim L_P/\operatorname{Ker}\varphi = \dim \varphi(L_P)$. Остается заметить, что по теореме 27 главы 13 $\dim L_P/\operatorname{Ker}\varphi = \dim L_P - \dim \operatorname{Ker}\varphi$. □

Рассмотрим теперь ситуацию, когда оба пространства L_P и M_P конечномерные.

Утверждение 6. *Пусть $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ и $\vec{\beta} = (\beta_1, \ldots, \beta_m)$ — базисы соответственно пространств L_P и M_P. Тогда*

(а) *для любой матрицы $B \in P_{m,n}$ отображение $\psi\colon L_P \to M_P$, задаваемое формулой*

$$\forall\, \gamma \in L_P:\ \ \psi(\gamma) = \vec{\beta}(B\gamma_{\vec{\alpha}}^{\downarrow}),$$

есть линейное отображение;

(б) *если $\varphi \in \mathfrak{L}(L_P, M_P)$, то существует такая единственная матрица $A \in P_{m,n}$, что для каждого вектора $\gamma \in L_P$ выполняется равенство*

$$\varphi(\gamma) = \vec{\beta}(A\gamma_{\vec{\alpha}}^{\downarrow}). \tag{4}$$

Эта матрица имеет вид

$$A = (\varphi(\alpha_1)_{\vec{\beta}}^{\downarrow}, \ \ldots, \ \varphi(\alpha_n)_{\vec{\beta}}^{\downarrow}). \tag{5}$$

□ (а) Линейность отображения ψ следует из равенств $(\gamma a)_{\vec{\alpha}}^{\downarrow} = \gamma_{\vec{\alpha}}^{\downarrow} a$ и $(\gamma + \delta)_{\vec{\alpha}}^{\downarrow} = \gamma_{\vec{\alpha}}^{\downarrow} + \delta_{\vec{\alpha}}^{\downarrow}$ (см. утверждение 19 главы 13) и формул (5) и (6) главы 13. Например,

$$\psi(\gamma a) = \vec{\beta}(B(\gamma a)_{\vec{\alpha}}^{\downarrow}) = \vec{\beta}(B\gamma_{\vec{\alpha}}^{\downarrow} a) = \vec{\beta}(B\gamma_{\vec{\alpha}}^{\downarrow})a = \varphi(\gamma)a.$$

(б) Так как $\varphi(\alpha_i) = \vec{\beta}\varphi(\alpha_i)_{\vec{\beta}}^{\downarrow}$, $i \in \overline{1,n}$, то ввиду равенства (3) справедливо равенство (4), где матрица A имеет вид (5).

Если же $A \in P_{m,n}$ — произвольная матрица, удовлетворяющая равенству (4), то, как нетрудно видеть, $\varphi(\alpha_i) = \vec{\beta}A_i^{\downarrow}$. Значит, $A_i^{\downarrow} = \varphi(\alpha_i)_{\vec{\beta}}^{\downarrow}$, и, следовательно, матрица A определена однозначно. □

Определение 4. Матрицу $A \in P_{m,n}$, имеющую вид (5), называют *матрицей линейного отображения* $\varphi\colon L_P \to M_P$ *в базисах* $\vec{\alpha}$ *и* $\vec{\beta}$ и обозначают через $A_{\vec{\alpha},\vec{\beta}}(\varphi)$.

Замечание 2. Утверждение 6 при фиксированных базисах $\vec{\alpha}$ и $\vec{\beta}$ устанавливает взаимно однозначное соответствие σ между множествами $\mathfrak{L}(L_P, M_P)$ и $P_{m,n}$:

$$\sigma(\varphi) = A_{\vec{\alpha},\vec{\beta}}(\varphi). \tag{6}$$

Пример 6. Пусть в условиях примера 2 $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ — базис пространства L_P. Тогда $A_{\vec{\alpha},\vec{\alpha}}(\widehat{a}) = aE$.

Уточним утверждение 1.

Утверждение 7. *Если* $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ *и* $\vec{\beta} = (\beta_1, \ldots, \beta_m)$ *— базисы соответственно пространств* L_P *и* M_P*, то для любого отображения* $\varphi \in \mathfrak{L}(L_P, M_P)$ *справедливы равенства*

(а) $\dim \varphi(L_P) = \operatorname{rang} A_{\vec{\alpha},\vec{\beta}}(\varphi)$,

(б) $\dim \operatorname{Ker} \varphi = n - \operatorname{rang} A_{\vec{\alpha},\vec{\beta}}(\varphi)$.

□ (а) Ввиду соотношений (3) $\varphi(L_P) = (\varphi(\alpha_1), \ldots, \varphi(\alpha_n))_P$. Значит, по утверждению 22 главы 13, $\dim \varphi(L_P)$ — это число векторов в базисе системы $\varphi(\alpha_1)^{\downarrow}_{\vec{\beta}}$, $\ldots$, $\varphi(\alpha_n)^{\downarrow}_{\vec{\beta}}$. Из определения 4 и следствия 7 теоремы 15 главы 7 получаем, что $\dim \varphi(L_P) = \operatorname{rang} A_{\vec{\alpha},\vec{\beta}}(\varphi)$.

(б) Следует из (а) и утверждения 5. □

Уточним теорему 3.

Лемма 8. *Пусть* $\varphi,\ \psi \in \mathfrak{L}(L_P, M_P)$, $a \in P$, $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ *и* $\vec{\beta} = (\beta_1, \ldots, \beta_m)$ *— базисы соответственно пространств* L_P *и* M_P*. Тогда справедливы равенства*

$$\begin{aligned} A_{\vec{\alpha},\vec{\beta}}(\varphi + \psi) &= A_{\vec{\alpha},\vec{\beta}}(\varphi) + A_{\vec{\alpha},\vec{\beta}}(\psi), \\ A_{\vec{\alpha},\vec{\beta}}(\varphi \odot a) &= A_{\vec{\alpha},\vec{\beta}}(\varphi)a. \end{aligned} \tag{7}$$

□ Пусть $\gamma \in L_P$. Ввиду определения 4 и равенства (4) имеем:

$$(\varphi + \psi)(\gamma) = \vec{\beta}\,(A_{\vec{\alpha},\vec{\beta}}(\varphi + \psi)\gamma^{\downarrow}_{\vec{\alpha}}). \tag{8}$$

Левую часть равенства (8), пользуясь первым из равенств (2) и формулами (5), (6) главы 13, перепишем в виде

$$\varphi(\gamma) + \psi(\gamma) = \vec{\beta} A_{\vec{\alpha},\vec{\beta}}(\varphi)\gamma^{\downarrow}_{\vec{\alpha}} + \vec{\beta} A_{\vec{\alpha},\vec{\beta}}(\psi)\gamma^{\downarrow}_{\vec{\alpha}} = \vec{\beta}\,(A_{\vec{\alpha},\vec{\beta}}(\varphi) + A_{\vec{\alpha},\vec{\beta}}(\psi))\gamma^{\downarrow}_{\alpha}.$$

Таким образом,

$$\vec{\beta} A_{\vec{\alpha},\vec{\beta}}(\varphi + \psi)\gamma^{\downarrow}_{\vec{\alpha}} = \vec{\beta}\,(A_{\vec{\alpha},\vec{\beta}}(\varphi) + A_{\vec{\alpha},\vec{\beta}}(\psi))\gamma^{\downarrow}_{\vec{\alpha}}. \tag{9}$$

По утверждению 6(б) из (9) следует первое из равенств (7). Аналогично проводится доказательство и второго из этих равенств. □

Теорема 9. *Если* $\dim L_P = n$ *и* $\dim M_P = m$, *то пространство* $\mathfrak{L}(L_P, M_P)_P$ *изоморфно пространству* $(P_{n,m})_P$. *В частности,*

$$\dim \mathfrak{L}(L_P, M_P) = nm.$$

□ В силу замечания 2 и леммы 8 отображение $\sigma\colon \mathfrak{L}(L_P, M_P) \to P_{n,m}$, определенное равенством (6), является изоморфизмом пространства $\mathfrak{L}(L_P, M_P)_P$ на пространство $(P_{m,n})_P$. По теореме 21 главы 13 $\dim(P_{m,n})_P = \dim \mathfrak{L}(L_P, M_P)_P = mn$. □

§ 2. ЛИНЕЙНЫЕ ПРЕОБРАЗОВАНИЯ И ИХ СВОЙСТВА

Определение 5. Линейное отображение $\varphi\colon L_P \to L_P$ называют *линейным преобразованием* пространства L_P. Множество $\mathfrak{L}(L_P, L_P)$ всех линейных преобразований пространства L_P обозначают через $\mathfrak{L}(L_P)$.

Линейные отображения, рассмотренные в примерах 1–3, — это линейные преобразования.

Пример 7. Отображение $\dfrac{d}{dx}\colon P[x]_P \to P[x]_P$, где P — поле, определяемое равенством $\dfrac{d}{dx}(f(x)) = f'(x)$ для $f(x) \in P[x]$, есть линейное преобразование пространства $P[x]_P$.

В § 1 на множестве $\mathfrak{L}(L_P, M_P)$ были введены операции сложения и умножения на элементы поля P. Поскольку элементы из $\mathfrak{L}(L_P)$ — это линейные отображения L_P в L_P, то на $\mathfrak{L}(L_P)$ можно определить также внутреннюю операцию композиции: если $\varphi, \psi \in \mathfrak{L}(L_P)$, то

$$\forall\, \alpha \in L_P:\ (\varphi \circ \psi)(\alpha) = \varphi(\psi(\alpha)). \tag{10}$$

Нетрудно проверить, что $\varphi \circ \psi \in \mathfrak{L}(L_P)$.

Теорема 10. *Для произвольного векторного пространства* L_P *множество* $(\mathfrak{L}(L_P), +, \odot)$ *является векторным пространством над полем* P, *а алгебра* $(\mathfrak{L}(L_P), +, \circ)$ *— кольцом с единицей.*

□ Первое утверждение теоремы следует из теоремы 3. Доказательство второго утверждения осуществляется непосредственной проверкой. Заметим, что единицей кольца $\mathfrak{L}(L_P)$ является тождественное преобразование — гомотетия $\widehat{e} = \varepsilon$, где e — единица поля P, а нулем — гомотетия $\widehat{0}$. □

Определение 6. Кольцо $(\mathfrak{L}(L_P), +, \circ)$ называют *кольцом линейных преобразований* векторного пространства L_P.

Определение 7. Преобразование $\varphi \in \mathfrak{L}(L_P)$ называют *обратимым*, если существует такое преобразование $\psi \in \mathfrak{L}(L_P)$, что $\varphi \circ \psi = \psi \circ \varphi = \varepsilon$, т. е. если $\varphi \in \mathfrak{L}(L_P)^*$.

Теорема 11. *Если* $\varphi \in \mathfrak{L}(L_P)$, *то следующие утверждения эквивалентны*:
(а) $\varphi \in \mathfrak{L}(L_P)^*$;
(б) φ — *изоморфизм* L_P *на* L_P;
(в) φ — *обратимое отображение, т. е.* $\varphi\circ\upsilon = \upsilon\circ\varphi = \varepsilon$ *для некоторого* $\upsilon\colon L \to L$ (*определение* 10 *главы* 1).

□ (а)⇒(в) По условию существует такое $\psi \in \mathfrak{L}(L_P)$, что $\varphi \circ \psi = \psi \circ \varphi = \varepsilon$. Остается положить $\upsilon = \psi$.
(в)⇒(б) По утверждению 4 главы 1 φ — биекция. Значит, по условию и определению 11 главы 13, φ — изоморфизм.
(б)⇒(а) По утверждению 14 главы 13 существует обратное отображение φ^{-1} и $\varphi^{-1} \in \mathfrak{L}(L_P)$. Значит, $\varphi \in \mathfrak{L}(L_P)^*$. □

Рассмотрим теперь случай, когда пространство L_P конечномерное.

Определение 8. Пусть $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ — базис пространства L_P. *Матрицей преобразования* $\varphi \in \mathfrak{L}(L_P)$ *в базисе* $\vec{\alpha}$ называют матрицу

$$A_{\vec{\alpha}}(\varphi) = A_{\vec{\alpha},\vec{\alpha}}(\varphi) = (\varphi(\alpha_1)^{\downarrow}_{\vec{\alpha}}, \ldots, \varphi(\alpha_n)^{\downarrow}_{\vec{\alpha}}).$$

В силу равенств (4) и (5) для любого вектора $\gamma \in L_P$ справедливы равенства

$$\varphi(\gamma) = \vec{\alpha}A_{\vec{\alpha}}(\varphi)\gamma^{\downarrow}_{\vec{\alpha}}, \quad \varphi(\gamma)^{\downarrow}_{\vec{\alpha}} = A_{\vec{\alpha}}(\varphi)\gamma^{\downarrow}_{\vec{\alpha}}. \tag{11}$$

Поэтому

$$\varphi(\vec{\alpha}) = (\varphi(\alpha_1), \ldots, \varphi(\alpha_n)) = (\vec{\alpha}A_{\vec{\alpha}}(\varphi)\alpha^{\downarrow}_{1\vec{\alpha}}, \ldots, \vec{\alpha}A_{\vec{\alpha}}(\varphi)\alpha^{\downarrow}_{n\vec{\alpha}}) = \vec{\alpha}A_{\vec{\alpha}}(\varphi). \tag{12}$$

Лемма 12. *Если* $\varphi, \psi \in \mathfrak{L}(L_P)$ *и* $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ — *базис пространства* L_P, *то справедливо равенство*

$$A_{\vec{\alpha}}(\varphi \circ \psi) = A_{\vec{\alpha}}(\varphi)A_{\vec{\alpha}}(\psi). \tag{13}$$

□ Пользуясь равенствами (10), (11) и (12), для $\gamma \in L_P$ получаем

$$\begin{aligned}(\varphi \circ \psi)(\gamma) = \varphi(\psi(\gamma)) &= \varphi(\vec{\alpha}A_{\vec{\alpha}}(\psi)\gamma^{\downarrow}_{\vec{\alpha}}) = \\ &= \varphi(\vec{\alpha})A_{\vec{\alpha}}(\psi)\gamma^{\downarrow}_{\vec{\alpha}} = \vec{\alpha}A_{\vec{\alpha}}(\varphi)A_{\vec{\alpha}}(\psi)\gamma^{\downarrow}_{\vec{\alpha}}.\end{aligned} \tag{14}$$

В силу первого из равенств (11) имеем

$$(\varphi \circ \psi)(\gamma) = \vec{\alpha}A_{\vec{\alpha}}(\varphi \circ \psi)\gamma^{\downarrow}_{\vec{\alpha}}. \tag{15}$$

Ввиду утверждения 6 из равенств (14) и (15) получаем требуемое равенство (13). □

Теорема 13. *Если* $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ — *базис пространства* L_P, *то пространство* $\mathfrak{L}(L_P)_P$ *изоморфно пространству* $(P_{n,n})_P$ *и, в частности,* $\dim \mathfrak{L}(L_P)_P = n^2$, *а кольцо* $\mathfrak{L}(L_P)$ *изоморфно кольцу* $P_{n,n}$.

□ Первое утверждение теоремы следует непосредственно из теоремы 9. В частности, отображение $\sigma\colon \mathfrak{L}(L_P) \to P_{n,n}$, где $\sigma(\varphi) = A_{\vec{\alpha}}(\varphi)$, есть изоморфизм группы $(\mathfrak{L}(L_P), +)$ на группу $(P_{n,n}, +)$. Из равенства (13) следует, что $\sigma(\varphi \circ \psi) = \sigma(\varphi)\sigma(\psi)$, где $\varphi, \psi \in \mathfrak{L}(L_P)$. Значит, σ — изоморфизм колец. □

Следствие. *В условиях теоремы* 13 *преобразование* $\varphi \in \mathfrak{L}(L_P)$ *обратимо тогда и только тогда, когда обратима матрица* $A_{\vec{\alpha}}(\varphi)$. *При этом*

$$A_{\vec{\alpha}}(\varphi^{-1}) = A_{\vec{\alpha}}(\varphi)^{-1}.$$

Теорема 13, в частности, показывает, что кольцо линейных преобразований $\mathfrak{L}(L_P)$ пространства L_P не является коммутативным. Однако, некоторые преобразования из $\mathfrak{L}(L_P)$ могут быть перестановочными.

Пример 8. Пусть L_P — произвольное пространство, $\varphi \in \mathfrak{L}(L_P)$ и $\widehat{a}$ — гомотетия. Для любого вектора $\gamma \in L_P$ справедливы равенства

$$(\widehat{a} \circ \varphi)(\gamma) = \widehat{a}(\varphi(\gamma)) = \varphi(\gamma)a = \varphi(\gamma a) = \varphi(\widehat{a}(\gamma)) = (\varphi \circ \widehat{a})(\gamma),$$

из которых следует, что $\widehat{a} \circ \varphi = \varphi \circ \widehat{a}$. Ясно, что тогда $\widehat{a} \circ \varphi^k = \varphi^k \circ \widehat{a}$ для любого $k \in \mathbb{N}$.

Теперь для случая конечномерного пространства L_P уточним теорему 11.

Утверждение 14. *Если* $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ *— базис пространства* L_P, *то для преобразования* $\varphi \in \mathfrak{L}(L_P)$ *равносильны утверждения*:

(а) $\varphi \in \mathfrak{L}(L_P)^*$;
(б) φ — *биекция*;
(в) φ — *инъективное преобразование*;
(г) $(\varphi(\alpha_1), \ldots, \varphi(\alpha_n))$ — *базис пространства* L_P;
(д) φ — *сюръективное преобразование*.

Доказательство утверждения 14 предоставляется читателю.

Замечание 3. По утверждению 5 главы 1 для отображения конечного множества в себя совпадают свойства инъективности, сюръективности и биективности. Утверждение 14 показывает, что эти свойства совпадают и для линейного преобразования конечномерного пространства, хотя само пространство может состоять из бесконечного множества элементов.

До сих пор мы рассматривали матрицы различных линейных преобразований конечномерного пространства L_P в фиксированном базисе $\vec{\alpha}$ этого пространства. Рассмотрим теперь вопрос о том, как связаны между собой матрицы одного и того же линейного преобразования в различных базисах этого пространства.

Утверждение 15. *Если* $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ *и* $\vec{\beta} = \vec{\alpha}C$ *— базисы пространства* L_P, *то для любого преобразования* $\varphi \in \mathfrak{L}(L_P)$ *справедливо равенство*

$$A_{\vec{\beta}}(\varphi) = C^{-1} A_{\vec{\alpha}}(\varphi) C. \tag{16}$$

□ Из условия $\vec{\beta} = \vec{\alpha}C$ получаем $\varphi(\vec{\beta}) = \varphi(\vec{\alpha})C$. Ввиду равенств (12) и обратимости матрицы C (следствие утверждения 22 главы 13) имеем:

$$\vec{\beta}A_{\vec{\beta}}(\varphi) = \vec{\alpha}A_{\vec{\alpha}}(\varphi)C = \vec{\beta}C^{-1}A_{\vec{\alpha}}(\varphi)C. \tag{17}$$

В силу линейной независимости системы векторов $\vec{\beta}$ из равенства (17) получаем требуемое равенство (16). □

Определение 9. Говорят, что *матрица $B \in P_{n,n}$ подобна матрице $A \in P_{n,n}$*, если существует такая матрица $C \in P^*_{n,n}$, что $B = C^{-1}AC$. В этом случае пишут $B \approx A$.

Для матрицы $A \in P_{n,n}$ и многочлена $f(x) = \sum\limits_{i=0}^{k} f_i x^i \in P[x]$ положим

$$f(A) = \sum_{i=0}^{k} f_i A^i, \text{ где } A^0 = E_{n\times n}.$$

Ясно, что $f(A) \in P_{n,n}$.

Читателю предлагается самостоятельно доказать

Утверждение 16. *Отношение $\approx$ есть отношение эквивалентности на множестве $P_{n,n}$. Если $A, B \in P_{n,n}$ и $B = C^{-1}AC$, то $\operatorname{rang} B = \operatorname{rang} A$ и для любого многочлена $f(x) \in P[x]$ справедливо равенство $f(B) = C^{-1}f(A)C$.*

Ввиду утверждения 16 из условия $B \approx A$ следует $A \approx B$, т. е. можно говорить, что *матрицы A и B подобны*, вместо того, что матрица B подобна матрице A.

Пример 9. Матрицы, имеющие одинаковый ранг, не обязательно подобны. Действительно, единичная матрица $E_{n\times n}$ подобна только самой себе. Однако, для любой невырожденной матрицы B $\operatorname{rang} E_{n\times n} = n = \operatorname{rang} B$.

С учетом утверждения 15 и определения 9 мы можем сказать, что матрицы одного линейного преобразования в разных базисах подобны. Оказывается, что верно и обратное утверждение.

Утверждение 17. *Матрицы $A, B \in P_{n,n}$ подобны тогда и только тогда, когда они являются матрицами одного линейного преобразования пространства L_P, где $\dim L_P = n$.*

□ Ввиду утверждения 15 требуется лишь доказать, что подобные матрицы являются матрицами одного линейного преобразования. Пусть $B = C^{-1}AC$ и L_P — произвольное пространство, где $\dim L_P = n$. Согласно утверждению 6(а) зададим отображение $\psi \in \mathfrak{L}(L_P)$, положив $\psi(\gamma) = \vec{\alpha}A\gamma^{\downarrow}_{\vec{\alpha}}$, где $\gamma \in L_P$ и $\vec{\alpha}$ — базис пространства L_P. Тогда $A = A_{\vec{\alpha}}(\psi)$.

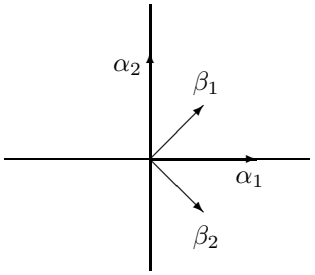
Так как C — невырожденная матрица, то система векторов $\vec{\beta} = \vec{\alpha}C$ является базисом пространства L_P (см. следствие утверждения 22 главы 13). По утверждению 15

$$A_{\vec{\beta}}(\psi) = C^{-1}AC = B,$$

что и требовалось. □

Переход к другому базису пространства L_P позволяет иногда существенно упростить вид матрицы линейного преобразования и этим прояснить «геометрический» смысл преобразования. Пути выбора таких базисов указаны в следующих параграфах.

Пример 10. На плоскости D^2 выберем базисы $\vec{\alpha} = (\alpha_1, \alpha_2)$ и $\vec{\beta} = (\beta_1, \beta_2)$, где $\beta_1 = \frac{1}{2}\alpha_1 + \frac{1}{2}\alpha_2$, $\beta_2 = \frac{1}{2}\alpha_1 - \frac{1}{2}\alpha_2$.



Преобразование φ определим матрицей $A_{\vec{\alpha}}(\varphi) = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$. Нетрудно проверить, что $A_{\vec{\beta}} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Значит, преобразование φ — это ортогональное проектирование на прямую, содержащую вектор β_1.

§ 3. СОБСТВЕННЫЕ ВЕКТОРЫ, СОБСТВЕННЫЕ ЗНАЧЕНИЯ И ХАРАКТЕРИСТИЧЕСКИЙ МНОГОЧЛЕН ЛИНЕЙНОГО ПРЕОБРАЗОВАНИЯ

В дальнейшем, если не оговорено противное, L_P — конечномерное пространство.

Простейшее линейное преобразование пространства L_P — это гомотетия $\widehat{a}$, где $a \in P$. Матрица этого преобразования в любом базисе $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ пространства L_P — скалярная: $A_{\vec{\alpha}}(\widehat{a}) = aE$. Геометрический смысл такого преобразования очевиден: при $a \neq 0$ происходит «растяжение» пространства равномерно вдоль каждой из «осей» $\alpha_1, \ldots, \alpha_n$. Если $\varphi \in \mathfrak{L}(L_P)$ — такое преобразование, что в некотором базисе $\vec{\beta} = (\beta_1, \ldots, \beta_n)$ матрица $A_{\vec{\beta}}(\varphi)$ диагональная, то геометрический смысл преобразования φ также ясен: если $A_{\vec{\beta}}(\varphi) = \operatorname{diag}(r_1, \ldots, r_n)$, то преобразование φ состоит в «растяжении» пространства вдоль каждой «оси» β_i «в r_i раз». Выясним, когда же преобразование φ имеет такой характер.

Определение 10. Ненулевой (!) вектор $\alpha \in L_P$ называют *собственным вектором преобразования $\varphi \in \mathfrak{L}(L_P)$, принадлежащим собственному значению $r \in P$*, если $\varphi(\alpha) = \alpha r$. Элемент $r \in P$ называют *собственным значением преобразования* $\varphi \in \mathfrak{L}(L_P)$, если существует такой ненулевой (!) вектор $\alpha \in L_P$, что $\varphi(\alpha) = \alpha r$.

Пример 11. В примере 10 векторы β_1 и β_2 — собственные векторы преобразования φ, принадлежащие соответственно собственным значениям 1 и 0.

Не всякое линейное преобразование имеет хотя бы один собственный вектор.

Пример 12. При повороте плоскости D^2 на угол $\omega = \pi/2$ вокруг начала координат ни один вектор (кроме нулевого) не переходит в пропорциональный себе вектор. Значит, у этого линейного преобразования нет собственных векторов.

Утверждение 18. *Матрица преобразования $\varphi \in \mathfrak{L}(L_P)$ в базисе $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ диагональная тогда и только тогда, когда базис $\vec{\alpha}$ состоит из собственных векторов преобразования φ.*

□ Если $A_{\vec{\alpha}}(\varphi) = \operatorname{diag}(r_1, \ldots, r_n)$, то по определению 8 $\varphi(\alpha_i) = \alpha_i r_i$, $i \in \overline{1,n}$. Стало быть, базисные векторы являются собственными векторами преобразования φ. Обратно, если $\varphi(\alpha_i) = \alpha_i r_i$, $i \in \overline{1,n}$, то снова по определению 8 $A_{\vec{\alpha}}(\varphi) = \operatorname{diag}(r_1, \ldots, r_n)$. □

Укажем теперь практический способ отыскания собственных векторов и собственных значений линейного преобразования.

Определение 11. *Характеристической матрицей матрицы $A \in P_{n,n}$* называют матрицу $Ex - A \in P[x]_{n,n}$. *Характеристическим многочленом матрицы A* называют многочлен $\chi_A(x) = |Ex - A| \in P[x]$.

В этом определении $E = E_{n\times n}$. Заметим, что $\chi_A(x)$ — унитарный многочлен и $\deg \chi_A(x) = n$.

Пример 13. Если $A = \operatorname{diag}(r_1, \ldots, r_n)$, то $\chi_A(x) = (x - r_1)\ldots(x - r_n)$.

Утверждение 19. *Если $A, B \in P_{n,n}$ и $B \approx A$, то $\chi_B(x) = \chi_A(x)$.*

□ По определению 9 существует невырожденная матрица $C \in P_{n,n}$ такая, что $B = C^{-1}AC$. Тогда при $E = E_{n\times n}$ справедливы равенства

$$\chi_B(x) = |Ex - B| = |Ex - C^{-1}AC| = |C^{-1}(Ex - A)C| = \\ = |C^{-1}| \cdot |Ex - A| \cdot |C| = |Ex - A| = \chi_A(x). \quad \square$$

Утверждение, обратное к утверждению 19, неверно.

Пример 14. Матрицы $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathbb{R}_{2,2}$ имеют равные характеристические многочлены, однако они не подобны (см. пример 8).

Определение 12. Матрицу $A \in P_{n,n}$ называют *полураспавшейся*, если

$$A = \begin{pmatrix} B_{k\times k} & C_{k\times(n-k)} \\ O_{(n-k)\times k} & D_{(n-k)\times(n-k)} \end{pmatrix}, \tag{18}$$

где $1 \leqslant k < n$. Матрица, транспонированная к матрице A, также называется полураспавшейся.

Утверждение 20. *Если A — полураспавшаяся матрица* (18)*, то*

$$\chi_A(x) = \chi_B(x) \times \chi_D(x).$$

□ Справедливость утверждения легко следует из теоремы Лапласа (теорема 10 главы 6). □

Утверждения 15 и 19 делают корректным

ОПРЕДЕЛЕНИЕ 13. *Характеристическим многочленом преобразования* $\varphi \in \mathfrak{L}(L_P)$ конечномерного пространства L_P называют характеристический многочлен матрицы этого преобразования в произвольном базисе пространства L_P. Его обозначают через $\chi_\varphi(x)$.

Теорема 21. *Собственные значения преобразования* $\varphi \in \mathfrak{L}(L_P)$ *суть все корни в поле* P *многочлена* $\chi_\varphi(x)$. *Собственные векторы этого преобразования, принадлежащие собственному значению* $r \in P$, — *это все такие векторы* $\gamma \in L_P \setminus \{\theta\}$, *столбцы координат* $\gamma_{\vec{\alpha}}^{\downarrow}$ *которых в произвольном фиксированном базисе* $\vec{\alpha}$ *пространства* L_P *являются решениями системы линейных уравнений*

$$(Er - A_{\vec{\alpha}}(\varphi))x^{\downarrow} = 0^{\downarrow}, \tag{19}$$

где $\dim L_P = n$ *и* $E = E_{n\times n}$.

□ Для вектора $\gamma \in L_P$ и скаляра $r \in P$ равенство $\varphi(\gamma) = \gamma r$ равносильно равенству $\varphi(\gamma)_{\vec{\alpha}}^{\downarrow} = \gamma_{\vec{\alpha}}^{\downarrow} r$ или ввиду соотношений (11) равенству $A_{\vec{\alpha}}(\varphi)\gamma_{\vec{\alpha}}^{\downarrow} = \gamma_{\vec{\alpha}}^{\downarrow} r$, которое можно переписать в виде

$$(Er - A_{\vec{\alpha}}(\varphi))\gamma_{\vec{\alpha}}^{\downarrow} = 0^{\downarrow}. \tag{20}$$

По определению 10 из равенства (20) получаем, что r — собственное значение преобразования φ тогда и только тогда, когда система линейных уравнений (19) имеет ненулевое решение, т. е. когда $|Er - A_{\vec{\alpha}}(\varphi)| = 0$, или $\chi_\varphi(r) = 0$ (теорема 4 главы 8).

Если же $\chi_\varphi(r) = 0$ и γ — собственный вектор преобразования φ, принадлежащий собственному значению r, то из равенства (20) следует, что $\gamma_{\vec{\alpha}}^{\downarrow}$ — решение системы линейных уравнений (19). □

В заключение параграфа рассмотрим вопрос о линейной независимости систем собственных векторов линейного преобразования.

Утверждение 22. *Пусть* L_P — *произвольное пространство и* $\gamma_{i1}, \ldots, \gamma_{ik_i}$ — *линейно независимая система собственных векторов преобразования* $\varphi \in \mathfrak{L}(L_P)$, *принадлежащих собственному значению* $r_i \in P$, $i \in \overline{1,t}$, *где* $r_s \neq r_l$ *при* $s \neq l$. *Тогда система векторов*

$$\gamma_{11}, \ldots, \gamma_{1k_1}, \ \ldots, \ \gamma_{t1}, \ldots, \gamma_{tk_t} \tag{21}$$

линейно независима.

□ Доказательство утверждения проведем индукцией по числу t. При $t = 1$ система векторов (21) линейно независима по условию.

Предположим, что утверждение верно для любой системы векторов, удовлетворяющей условиям утверждения при $t < m$, и докажем, что тогда оно верно при $t = m$. Пусть

$$\sum_{i=1}^{m}\sum_{j=1}^{k_i} \gamma_{ij}c_{ij} = \theta, \tag{22}$$

где $c_{ij} \in P$. Применив к обеим частям равенства (22) преобразование φ, получим

$$\sum_{i=1}^{m}\sum_{j=1}^{k_i}\gamma_{ij}r_ic_{ij} = \theta. \tag{23}$$

Теперь умножим обе части равенства (22) на r_m и почленно вычтем полученное равенство из равенства (23). Тогда справедливы равенства

$$\sum_{i=1}^{m}\sum_{j=1}^{k_i}\gamma_{ij}(r_i - r_m)c_{ij} = \theta = \sum_{i=1}^{m-1}\sum_{j=1}^{k_i}\gamma_{ij}(r_i - r_m)c_{ij},$$

из которых в силу предположения индукции следует, что $c_{ij} = 0$ при $i \in \overline{1, m-1}$, $j \in \overline{1, k_i}$. Тогда, ввиду условия, из (22) получаем, что $c_{ij} = 0$ и при $i = m$, $j \in \overline{1, k_m}$. □

Утверждение 18 и пример 12 показывают, что не для всякого линейного преобразования φ пространства L_P можно подобрать такой базис $\vec{\alpha}$ пространства, чтобы матрица $A_{\vec{\alpha}}(\varphi)$ была диагональной. Поэтому в следующих параграфах этой главы и в следующей главе будут рассмотрены другие способы получения возможно более простой матрицы $A_{\vec{\alpha}}(\varphi)$.

§ 4. МНОГОЧЛЕНЫ, АННУЛИРУЮЩИЕ ПРЕОБРАЗОВАНИЕ. МИНИМАЛЬНЫЙ МНОГОЧЛЕН

Пусть P — поле, $f(x) = \sum_{i=0}^{k} f_i x^i \in P[x]$, L_P — произвольное пространство над полем P и $\varphi \in \mathfrak{L}(L_P)$. Положим

$$f(\varphi) = \sum_{i=0}^{k} \widehat{f}_i \circ \varphi^i, \quad \text{где} \quad \varphi^0 = \varepsilon.$$

Так как $\mathfrak{L}(L_P)$ — кольцо, то $f(\varphi) \in \mathfrak{L}(L_P)$.

Пример 15. Пусть φ — поворот пространства D^2 на угол $\pi/2$ вокруг начала координат. Если $g(x) = x^2$, то $g(\varphi) = \widehat{-1}$ — поворот на угол π, а если $f(x) = x^2 + 1$, то $f(\varphi) = \widehat{0}$. Для гомотетии $\widehat{a}$ и $t(x) = x - a$ получаем $t(\widehat{a}) = \widehat{0}$.

Утверждение 23. *Пусть L_P — произвольное пространство и $f(x), g(x) \in P[x]$. Тогда*

(а) *если $\varphi \in \mathfrak{L}(L_P)$, $A \in P_{n,n}$, $h(x) = f(x) + g(x)$ и $t(x) = f(x)g(x)$, то справедливы равенства*

$$h(\varphi) = f(\varphi) + g(\varphi), \quad t(\varphi) = f(\varphi) \circ g(\varphi) = g(\varphi) \circ f(\varphi) \tag{24}$$

и

$$h(A) = f(A) + g(A), \quad t(A) = f(A)g(A) = g(A)f(A); \tag{25}$$

(б) *если $(f(x), g(x)) = e$, $\varphi \in L_P$ и $f(\varphi)(\gamma) = g(\varphi)(\gamma) = \theta$, то $\gamma = \theta$.*

□ (а) Справедливость первого из равенств (24) очевидна. Пусть $f(x)=\sum_{i=0}^{l} f_i x^i$ и $g(x)=\sum_{i=0}^{m} g_i x^i$. Тогда

$$t(x)=\sum_{i=0}^{l+m}\Bigl(\sum_{k=0}^{i} f_k g_{i-k}\Bigr)x^i \quad \text{и} \quad t(\varphi)=\sum_{i=0}^{m+l}\Bigl(\sum_{k=0}^{i} \widehat{f}_k\circ\widehat{g}_{i-k}\Bigr)\circ\varphi^i.$$

Одновременно ввиду примера 8 в кольце $\mathfrak{L}(L_P)$ имеем:

$$f(\varphi)\circ g(\varphi)=\Bigl(\sum_{i=0}^{l}\widehat{f}_i\circ\varphi^i\Bigr)\circ\Bigl(\sum_{i=0}^{m}\widehat{g}_i\circ\varphi^i\Bigr)=\sum_{i=0}^{l+m}\Bigl(\sum_{k=0}^{i}\widehat{f}_k\circ\widehat{g}_{i-k}\Bigr)\circ\varphi^i.$$

Значит, $t(\varphi)=f(\varphi)\circ g(\varphi)$. Поскольку $f(x)g(x)=g(x)f(x)$, то $t(\varphi)=g(\varphi)\circ f(\varphi)$.

Аналогично доказываются и равенства (25).

(б) По условию и утверждению 11 главы 9 найдутся такие многочлены $u(x)$, $v(x)\in P[x]$, что $u(x)f(x)+v(x)g(x)=e$. По утверждению (а) получаем

$$u(\varphi)\circ f(\varphi)+v(\varphi)\circ g(\varphi)=\widehat{e}=\varepsilon.$$

Тогда справедливы равенства

$$\gamma=\varepsilon(\gamma)=(u(\varphi)\circ f(\varphi))(\gamma)+(v(\varphi)\circ g(\varphi))(\gamma)=$$
$$=u(\varphi)(f(\varphi)(\gamma))+v(\varphi)(g(\varphi)(\gamma))=u(\varphi)(\theta)+v(\varphi)(\theta)=\theta. \quad \square$$

Утверждение 24. *Если $\vec{\alpha}=(\alpha_1,\ldots,\alpha_n)$ — базис пространства L_P, φ — произвольное преобразование из $\mathfrak{L}(L_P)$ и $f(x)$ — произвольный многочлен из $P[x]$, то*

$$A_{\vec{\alpha}}(f(\varphi))=f(A_{\vec{\alpha}}(\varphi)).$$

□ Доказательство проводится с использованием равенств (7) и (13). Читателю предлагается провести его самостоятельно. □

Определение 14. Говорят, что *многочлен $f(x)\in P[x]$ аннулирует преобразование $\varphi\in\mathfrak{L}(L_P)$* (*матрицу $A\in P_{n,n}$*), если $f(\varphi)=\widehat{0}$ ($f(A)=O_{n\times n}$). В таком случае говорят, что φ (соответственно A) — *корень* многочлена $f(x)$, а $f(x)$ — *аннулирующий многочлен* преобразования φ (матрицы A).

Пример 15 показывает, что для некоторых преобразований существуют аннулирующие многочлены. Следующая теорема является одной из фундаментальных в теории линейных преобразований конечномерных пространств.

Предварительно рассмотрим кольцо матриц $P[x]_{n,n}$, где P — поле (кольцо *полиномиальных матриц*). Пусть $B(x)=(b_{ij}(x))_{n\times n}$, где $b_{ij}(x)=\sum\limits_{k=0}^{s_{ij}} b_k^{(i,j)}x^k$. Обозначим

$$B_k=\bigl(b_k^{(i,j)}\bigr)\in P_{n,n}, \quad \text{где} \quad k\in\overline{0,t} \quad \text{и} \quad t=\max_{i,j}s_{ij}.$$

Так как $P \subset P[x]$ (см. § 1 главы 9), то $B_k \in P[x]_{n,n}$ и $B_k x^k$ — результат умножения матрицы из $P[x]_{n,n}$ на элемент кольца $P[x]$. Поэтому в кольце $P[x]_{n,n}$ матрица $B(x)$ однозначно представима в виде

$$B(x) = B_t x^t + \ldots + B_1 x + B_0.$$

Пусть

$$C(x) = C_l x^l + \ldots + C_1 x + C_0$$

— аналогичное представление матрицы $C(x) \in P[x]_{n,n}$. Ясно, что

$$B(x) + C(x) = \sum_{i=0}^{\max\{t,l\}} (B_i + C_i)\, x^i \tag{26}$$

(если $t > l$, то $C_i = O_{n\times n}$ при $i > l$).

Ввиду дистрибутивности операции умножения матриц над кольцом на элементы этого кольца относительно операции сложения матриц и равенства $Dx^s = x^s D$, где $D \in P_{n,n}$, получаем, что

$$B(x)C(x) = B_t C_l x^{t+l} + \ldots + \left(\sum_{i=0}^{k} B_i C_{k-i}\right) x^k + \ldots + B_0 C_0. \tag{27}$$

Установим теперь связь между кольцом $P[x]_{n,n}$ и кольцом многочленов $P_{n,n}[\overline{x}]$ от одного переменного над кольцом $P_{n,n}$.

Лемма 25. *Если P — поле и $n \in \mathbb{N}$, то отображение $\tau\colon P[x]_{n,n} \to P_{n,n}[\overline{x}]$, определенное равенством*

$$\tau(B_t x^t + \ldots + B_0) = B_t \overline{x}^t + \ldots + B_0,$$

является изоморфизмом кольца $P[x]_{n,n}$ на кольцо $P_{n,n}[\overline{x}]$.

□ Ясно, что τ — сюръективное отображение. Если $\tau(B(x)) = 0(\overline{x})$ — нулевой многочлен, то $B(x) = O_{n\times n}$. Значит, τ инъективно и, таким образом, биективно. Из равенств (26) и (27) следует, что

$$\tau(B(x) + C(x)) = \tau(B(x)) + \tau(C(x)),$$
$$\tau(B(x)C(x)) = \tau(B(x))\,\tau(C(x)).$$

Следовательно, τ — требуемый изоморфизм. □

Теорема 26 (Гамильтон–Кэли).[19] *Если $A \in P_{n,n}$ и $\varphi \in \mathfrak{L}(L_P)$, где $\dim L_P = n$, то справедливы равенства*

$$\chi_A(A) = O_{n\times n}, \qquad \chi_\varphi(\varphi) = \widehat{0}. \tag{28}$$

[19] У. Гамильтон (1805–1865), А. Кэли (1821–1895) — английские математики.

□ Достаточно доказать первое из равенств (28). Действительно, если оно справедливо и $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ — базис пространства L_P, то по утверждению 23 и определению 12 имеем:

$$A_{\vec{\alpha}}(\chi_\varphi(\varphi)) = \chi_\varphi(A_{\vec{\alpha}}(\varphi)) = \chi_{A_{\vec{\alpha}}(\varphi)}(A_{\vec{\alpha}}(\varphi)) = O_{n\times n}$$

и, стало быть, $\chi_\varphi(\varphi) = \widehat{0}$.

Докажем первое из равенств (28). Пусть

$$\chi_A(x) = x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0 \in P[x].$$

В кольце $P_{n,n}[\overline{x}]$ выберем многочлен

$$F(\overline{x}) = E\,\overline{x}^n + c_{n-1}E\,\overline{x}^{n-1} + \ldots + c_0 E, \quad E = E_{n\times n}.$$

Ясно, что $F(A) = \chi_A(A)$. Поэтому достаточно показать, что $F(A) = O_{n\times n}$, или, ввиду теоремы Безу (см. § 3 главы 9), что многочлен $E\overline{x} - A \in P_{n,n}[\overline{x}]$ делит справа многочлен $F(\overline{x})$.

Рассмотрим в кольце $P[x]_{n,n}$ матрицу $Q(x) = (Ex - A)^*$, взаимную к матрице $Ex - A$. Как показано в доказательстве теоремы 11 главы 6, верно равенство

$$(Ex - A)^*\,(Ex - A) = |Ex - A| \cdot E,$$

т. е. равенство

$$Q(x)(Ex - A) = \chi_A(x)E. \tag{29}$$

Применив к обеим частям равенства (29) отображение τ, определенное в лемме 25, получим в кольце $P_{n,n}[\overline{x}]$ равенство

$$\tau(Q(x))\,(E\overline{x} - A) = F(\overline{x}),$$

которое и требовалось получить. □

По теореме Гамильтона–Кэли для любого преобразования $\varphi \in \mathfrak{L}(L_P)$ (любой матрицы $A \in P_{n,n}$) существует унитарный многочлен, аннулирующий преобразование φ (матрицу A). Поэтому существуют такие многочлены минимальной степени. Это делает содержательным

Определение 15. Унитарный многочлен из $P[x]$, аннулирующий преобразование $\varphi \in \mathfrak{L}(L_P)$ (матрицу $A \in P_{n,n}$) и имеющий наименьшую степень среди многочленов с этим свойством, называют *минимальным многочленом преобразования* φ (*матрицы* A).

Теорема 27. *Если* $\varphi \in \mathfrak{L}(L_P)$, *где* $\dim L_P = n$ ($A \in P_{n,n}$), *то*

(а) *в* $P[x]$ *существует единственный минимальный многочлен преобразования* φ (*матрицы* A);

(б) *если* $g(x)$ — *минимальный многочлен преобразования* φ (*матрицы* A), *то для любого многочлена* $f(x) \in P[x]$ *справедливы импликации*

$$f(\varphi) = \widehat{0} \;\Leftrightarrow\; g(x) \mid f(x) \qquad (f(A) = O_{n\times n} \;\Leftrightarrow\; g(x) \mid f(x)).$$

□ (б) Пусть $f(x) = g(x)\,t(x)$, где $t(x) \in P[x]$. По утверждению 23 тогда $f(A) = g(A)\,t(A) = O_{n\times n} \cdot t(A) = O_{n\times n}$.

Обратно, пусть $f(A) = O_{n\times n}$. Разделим многочлен $f(x)$ на $g(x)$ с остатком: $f(x) = q(x)g(x) + r(x)$, где $\deg r(x) < \deg g(x)$. Так как $f(A) = g(A) = O_{n\times n}$ и $f(A) = q(A)g(A) + r(A)$, то $r(A) = O_{n\times n}$.

Если $r(x) = c_s x^s + \ldots + c_0 \neq 0$, то положим $r_1(x) = c_s^{-1} r(x)$. Тогда справедливо равенство матриц $r_1(A) = c_s^{-1} r(A) = O_{n\times n}$. Стало быть, $r_1(x)$ — унитарный многочлен, аннулирующий матрицу A и имеющий степень, меньшую степени многочлена $g(x)$, ибо $\deg r_1(x) = \deg r(x)$. Полученное противоречие показывает, что $r(x) = 0$ и $g(x) \mid f(x)$.

(а) Пусть $g(x)$ и $g_1(x)$ — минимальные многочлены матрицы A. По утверждению (б) $g(x) \mid g_1(x)$ и $g_1(x) \mid g(x)$. Тогда многочлены $g(x)$ и $g_1(x)$ ассоциированы, а поскольку они унитарные, то $g_1(x) = g(x)$.

Аналогично доказывается теорема и для преобразования φ. □

Единственный минимальный многочлен преобразования $\varphi \in \mathfrak{L}(L_P)$ (матрицы $A \in P_{n,n}$) обозначают через $m_\varphi(x)$ ($m_A(x)$).

Следствие 1. *Если $\varphi \in \mathfrak{L}(L_P)$, где $\dim L_P = n$ ($A \in P_{n,n}$), то*

$$m_\varphi(x) \mid \chi_\varphi(x) \quad (m_A(x) \mid \chi_A(x)).$$

□ Это следует из теоремы Гамильтона—Кэли и теоремы 27. □

Следствие 2. *Если $\varphi \in \mathfrak{L}(L_P)$ и $\vec{\alpha}$ — базис пространства L_P, то*

$$m_\varphi(x) = m_{A_{\vec{\alpha}}(\varphi)}(x).$$

□ Пусть $t(x) = m_\varphi(x)$ и $g(x) = m_{A_{\vec{\alpha}}(\varphi)}(x)$. Так как $t(\varphi) = \widehat{0}$, то $A_{\vec{\alpha}}(t(\varphi)) = O_{n\times n}$. Тогда по утверждению 24 справедливы равенства $t(A_{\vec{\alpha}}(\varphi)) = A_{\vec{\alpha}}(t(\varphi)) = O_{n\times n}$. По теореме 27(б) отсюда следует, что $g(x) \mid t(x)$.

Аналогичным образом из равенства $A_{\vec{\alpha}}(g(\varphi)) = g(A_{\vec{\alpha}}(\varphi)) = O_{n\times n}$ получаем $g(\varphi) = \widehat{0}$ и $t(x) \mid g(x)$. Значит, $g(x) = t(x)$, так как $g(x)$ и $t(x)$ — унитарные многочлены. □

Следствие 3. *Если $A, B \in P_{n,n}$ и $B \approx A$, то $m_B(x) = m_A(x)$.*

□ По утверждению 17 матрицы A и B можно считать матрицами одного линейного преобразования φ пространства L_P, где $\dim L_P = n$, в разных его базисах. По следствию 2 $m_A(x) = m_\varphi(x)$ и $m_B(x) = m_\varphi(x)$. □

Другое доказательство следствия 3 можно получить с использованием утверждения 16.

Пример 16. Если $a \in P \setminus \{0\}$, то $m_{\widehat{a}}(x) = x - a$, $m_{\widehat{0}}(x) = 1$.

В некоторых случаях задачу отыскания минимального многочлена матрицы $A \in P_{n,n}$ можно свести к задаче отыскания минимальных многочленов матриц меньших размеров.

Определение 16. Матрицу $A \in P_{n,n}$ называют *распавшейся* или *квазидиагональной*, если

$$A = \begin{pmatrix} B_{k\times k} & O_{k\times(n-k)} \\ O_{(n-k)\times k} & D_{(n-k)\times(n-k)} \end{pmatrix}, \tag{30}$$

где $1 \leqslant k < n$. При условии (30) пишут: $A = \mathrm{Diag}(B, D)$.

Утверждение 28. *Если A есть полураспавшаяся матрица* (18) *или распавшаяся матрица* (30)*, то соответственно*

$$[\,m_B(x),\, m_D(x)\,] \;\big|\; m_A(x) \quad \textit{или} \quad m_A(x) = [\,m_B(x),\, m_D(x)\,].$$

□ Если матрица A имеет вид (18) или (30), а $f(x) \in P[x]$, то

$$f(A) = \begin{pmatrix} f(B) & * \\ O_{(n-k)\times k} & f(D) \end{pmatrix}.$$

Значит, из равенства $m_A(A) = O_{n\times n}$ следуют равенства $m_A(B) = O_{k\times k}$, $m_A(D) = O_{(n-k)\times(n-k)}$. Тогда по теореме 27 справедливы соотношения $m_B(x) \mid m_A(x)$ и $m_D(x) \mid m_A(x)$. Следовательно,

$$[\,m_B(x),\, m_D(x)\,] \;\big|\; m_A(x). \tag{31}$$

Если же матрица A имеет вид (30) и $h(x) = [m_B(x), m_D(x)]$, то

$$h(A) = \mathrm{Diag}(h(B), h(D)) = \mathrm{Diag}(O_{k\times k},\, O_{(n-k)\times(n-k)}) = O_{n\times n}$$

и $m_A(x) \mid h(x)$. Отсюда и из (31) следует, что $m_A(x) = [m_B(x), m_D(x)]$. □

Один из способов вычисления минимального многочлена произвольного преобразования $\varphi \in \mathfrak{L}(L_P)$ будет изложен в следующих параграфах.

§ 5. МИНИМАЛЬНЫЙ МНОГОЧЛЕН ВЕКТОРА ОТНОСИТЕЛЬНО ЛИНЕЙНОГО ПРЕОБРАЗОВАНИЯ

Теорема 27 и ее следствие 1 показывают, что для любого преобразования $\varphi \in \mathfrak{L}(L_P)$, где $\dim L_P = n$, и любого вектора $\gamma \in L_P$ существуют унитарные многочлены $f(x) \in P[x]$ такие, что

$$f(\varphi)(\gamma) = \theta. \tag{32}$$

Например, можно выбрать $f(x) = m_\varphi(x)$ или $f(x) = \chi_\varphi(x)$.

Определение 17. Унитарный многочлен $f(x) \in P[x]$ называют *минимальным многочленом вектора $\gamma \in L_P$ относительно преобразования $\varphi \in \mathfrak{L}(L_P)$*, если для него выполнено свойство (32) и он имеет наименьшую степень среди всех унитарных многочленов из $P[x]$, обладающих этим свойством.

Следующая теорема аналогична теореме 27.

Теорема 29. *Если* $\varphi \in \mathfrak{L}(L_P)$, *где* $\dim L_P = n$, *и* $\gamma \in L_P$, *то*

(а) *в* $P[x]$ *существует единственный минимальный многочлен вектора* γ *относительно преобразования* φ;

(б) *если* $g(x)$ *— минимальный многочлен вектора* γ *относительно преобразования* φ, *то для любого многочлена* $f(x) \in P[x]$ *справедливо соотношение*

$$(f(\varphi)(\gamma) = \theta) \;\Leftrightarrow\; (g(x) \mid f(x)).$$

□ Доказательство проводится совершенно аналогично доказательству теоремы 27 с заменой матрицы A на преобразование φ и рассмотрением не преобразований, а образов вектора γ при этих преобразованиях. □

Единственный минимальный многочлен вектора $\gamma \in L_P$ относительно преобразования $\varphi \in \mathfrak{L}(L_P)$ обозначают через $m_{\gamma,\varphi}(x)$.

Следствие. *Если* $\varphi \in \mathfrak{L}(L_P)$ *и* $\gamma \in L_P$, *то* $m_{\gamma,\varphi}(x) \mid m_\varphi(x)$.

Пример 17. Ясно, что для $\gamma \in L_P$, $\varphi \in \mathfrak{L}(L_P)$ справедливо неравенство $\deg m_{\gamma,\varphi}(x) \geqslant 0$. При этом $m_{\gamma,\varphi}(x) = e$ тогда и только тогда, когда $\gamma = \theta$, а $m_{\gamma,\varphi}(x) = x - r$ тогда и только тогда, когда γ — собственный вектор преобразования φ, принадлежащий собственному значению r.

Таблица, приведенная ниже, показывает аналогию между понятиями, рассмотренными в теории групп, и понятиями, введенными в настоящей главе.

Конечная абелева группа $(G, +)$	Конечномерное пространство L_P
$\lvert G\rvert\colon\ \forall\, g \in G\ (\lvert G\rvert g = 0)$	$\chi_\varphi(x)\colon\ \forall\, \alpha \in L_P\ (\chi_\varphi(\varphi)(\alpha) = \theta)$
$\exp G\colon\ \forall\, g \in G\ (\exp G \cdot g = 0)$	$m_\varphi(x)\colon\ \forall\, \alpha \in L_P\ (m_\varphi(\varphi)(\alpha) = \theta)$
$\operatorname{ord} g,\ g \in G\colon\ kg = 0 \Leftrightarrow \operatorname{ord} g \mid k$	$m_{\alpha,\varphi}(x)\colon\ f(\varphi)(\alpha) = \theta \Leftrightarrow m_{\alpha,\varphi}(x) \mid f(x)$

Как мы сейчас увидим, эта аналогия может быть продолжена. Сравните следующее утверждение с формулой, выражающей порядок степени g^l элемента g группы $(G, \cdot)$ через $\operatorname{ord} g$ и l, и с формулой, выражающей порядок произведения перестановочных элементов, имеющих взаимно простые порядки (теорема 3(в, г) главы 11).

Утверждение 30. *Пусть* $\varphi \in \mathfrak{L}(L_P)$, *где* $\dim L_P = n$, *и* $\alpha \in L_P$. *Тогда справедливы утверждения*:

(а) *если* $f(x) \in P[x]$ *и* $\beta = f(\varphi)(\alpha)$, *то*

$$m_{\beta,\varphi}(x) = \frac{m_{\alpha,\varphi}(x)}{(m_{\alpha,\varphi}(x), f(x))};$$

(б) *если* $\gamma \in L_P$ *и* $(m_{\gamma,\varphi}(x),\, m_{\alpha,\varphi}(x)) = e$, *то*

$$m_{\alpha+\gamma,\varphi}(x) = m_{\alpha,\varphi}(x)\, m_{\gamma,\varphi}(x).$$

□ (а) Пусть $d(x) = (f(x),\, m_{\alpha,\varphi}(x))$, $f(x) = f_1(x)d(x)$ и $m_{\alpha,\varphi}(x) = m_1(x)d(x)$. Нужно доказать равенство

$$m_{\beta,\varphi}(x) = m_1(x). \tag{33}$$

В силу условия и утверждения 23(а) справедлива цепочка равенств:

$$m_1(\varphi)(\beta) = m_1(\varphi)(f(\varphi)(\alpha)) = (m_1(\varphi) \circ f_1(\varphi) \circ d(\varphi))(\alpha) = \\ = f_1(\varphi)(m_{\alpha,\varphi}(\varphi)(\alpha)) = f_1(\varphi)(\theta) = \theta.$$

По теореме 29(б) тогда

$$m_{\beta,\varphi}(x) \mid m_1(x). \tag{34}$$

С другой стороны, из равенств

$$m_{\beta,\varphi}(\varphi)(\beta) = (m_{\beta,\varphi}(\varphi) \circ f(\varphi))(\alpha) = \theta$$

следует, что $m_{\alpha,\varphi}(x) \mid m_{\beta,\varphi}(x)f(x)$. Но тогда $m_1(x) \mid m_{\beta,\varphi}(x)f_1(x)$ и

$$m_1(x) \mid m_{\beta,\varphi}(x), \tag{35}$$

так как $(m_1(x), f_1(x)) = e$. Поскольку $m_1(x)$ и $m_{\beta,\varphi}(x)$ — унитарные многочлены, то из соотношений (34) и (35) получаем равенство (33).

(б) Так как справедливы равенства

$$(m_{\alpha,\varphi}(\varphi) \circ m_{\gamma,\varphi}(\varphi))(\alpha+\gamma) = m_{\gamma,\varphi}(\varphi)(m_{\alpha,\varphi}(\varphi)(\alpha)) + \\ + m_{\alpha,\varphi}(\varphi)(m_{\gamma,\varphi}(\varphi)(\gamma)) = m_{\gamma,\varphi}(\varphi)(\theta) + m_{\alpha,\varphi}(\varphi)(\theta) = \theta,$$

то по теореме 29(б)

$$m_{\alpha+\gamma,\varphi}(x) \mid m_{\alpha,\varphi}(x)\, m_{\gamma,\varphi}(x). \tag{36}$$

С другой стороны, так как $m_{\alpha+\gamma,\varphi}(\varphi)(\alpha+\gamma) = \theta$, то имеет место равенство

$$m_{\alpha+\gamma,\varphi}(\varphi)(\alpha) = -m_{\alpha+\gamma,\varphi}(\varphi)(\gamma). \tag{37}$$

Обозначим через δ равные векторы, стоящие в левой и правой частях равенства (37). Так как $m_{\alpha,\varphi}(\varphi)(\delta) = m_{\gamma,\varphi}(\varphi)(\delta) = \theta$, то по условию и утверждению 23(б) $\delta = \theta$. Это означает, что

$$m_{\alpha,\varphi}(x) \mid m_{\alpha+\gamma,\varphi}(x) \quad \text{и} \quad m_{\gamma,\varphi}(x) \mid m_{\alpha+\gamma,\varphi}(x),$$

а тогда по свойству взаимно простых многочленов

$$m_{\alpha,\varphi}(x)\, m_{\gamma,\varphi}(x) \mid m_{\alpha+\gamma,\varphi}(x). \tag{38}$$

Из соотношений (36) и (38) получаем равенство

$$m_{\alpha+\gamma,\varphi}(x) = m_{\alpha,\varphi}(x)\, m_{\gamma,\varphi}(x). \quad \square$$

Следующие два утверждения дают метод вычисления многочлена $m_\varphi(x)$.

Утверждение 31. *Пусть* $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ *— базис пространства* L_P *и* $\varphi \in \mathfrak{L}(L_P)$. *Тогда*

$$m_\varphi(x) = [\, m_{\alpha_1,\varphi}(x),\ \ldots,\ m_{\alpha_n,\varphi}(x)\,].$$

□ Пусть $t(x) = [m_{\alpha_1,\varphi}(x), \ldots, m_{\alpha_n,\varphi}(x)]$. Из следствия теоремы 29 следует, что $m_{\alpha_i,\varphi}(x) \mid m_\varphi(x)$ при $i \in \overline{1,n}$. Значит,

$$t(x) \mid m_\varphi(x). \tag{39}$$

Поскольку $m_{\alpha_i,\varphi}(x) \mid t(x)$, то по теореме 29(б) $t(\varphi)(\alpha_i) = \theta$, $i \in \overline{1,n}$. Тогда для любого вектора $\gamma = \sum_{i=1}^{n} \alpha_i a_i \in L_P$ имеем $t(\varphi)(\gamma) = \theta$. Значит,

$$m_\varphi(x) \mid t(x). \tag{40}$$

Из соотношений (39), (40) получаем требуемое равенство $t(x) = m_\varphi(x)$. □

Утверждение 32. *Пусть* $\varphi \in \mathfrak{L}(L_P)$, *где* $\dim L_P = n$, *и* $\gamma \in L_P \setminus \{\theta\}$. *Тогда существует такое* $k \in \overline{1,n}$, *что система векторов*

$$\gamma,\ \varphi(\gamma),\ \ldots,\ \varphi^{k-1}(\gamma) \tag{41}$$

линейно независима, а вектор $\varphi^k(\gamma)$ *линейно выражается через эту систему. Если при этом*

$$\varphi^k(\gamma) = \gamma c_0 + \varphi(\gamma)c_1 + \ldots + \varphi^{k-1}(\gamma)c_{k-1}, \tag{42}$$

то

$$m_{\gamma,\varphi}(x) = x^k - c_{k-1}x^{k-1} - \ldots - c_1 x - c_0.$$

□ Рассмотрим последовательность векторов $\gamma, \varphi(\gamma), \ldots, \varphi^i(\gamma), \ldots$. Так как $\dim L_P = n$, то найдется такое $k \in \overline{1,n}$, что система векторов (41) линейно независима, а система векторов $\gamma, \varphi(\gamma), \ldots, \varphi^k(\gamma)$ линейно зависима. По утверждению 4 главы 13 и следствию утверждения 3 главы 13 вектор $\varphi^k(\gamma)$ однозначно линейно выражается через систему векторов (41). Пусть это выражение задано равенством (42).

Обозначим $f(x) = x^k - c_{k-1}x^{k-1} - \ldots - c_0$. Ввиду равенства (42) $f(\varphi)(\gamma) = \theta$. Предположим что многочлен

$$g(x) = x^t - \sum_{i=0}^{t-1} g_i x^i \in P[x]$$

таков, что $t < k$ и

$$g(\varphi)(\gamma) = \varphi^t(\gamma) - \sum_{i=0}^{t-1} \varphi^i(\gamma) g_i = \theta. \tag{43}$$

Равенство (43) означает, что система векторов $\gamma, \varphi(\gamma), \ldots, \varphi^t(\gamma)$ линейно зависима и $t \leqslant k-1$. Это противоречит линейной независимости системы векторов (41). Значит, $f(x)$ — унитарный многочлен наименьшей степени, удовлетворяющий условию $f(\varphi)(\gamma) = \theta$. По определению 17 $f(x) = m_{\gamma,\varphi}(x)$. □

Получим теперь основной результат этого параграфа, позволяющий строить векторы с заданными минимальными многочленами.

Теорема 33. *Если* $\varphi \in \mathfrak{L}(L_P)$, *где* $\dim L_P = n$, *то для каждого унитарного делителя* $g(x)$ *многочлена* $m_\varphi(x)$ *существует такой вектор* $\gamma \in L_P$, *что* $m_{\gamma,\varphi}(x) = g(x)$.

□ Достаточно доказать, что существует такой вектор $\alpha \in L_P$, что $m_{\alpha,\varphi}(x) = m_\varphi(x)$. Действительно, записав $m_\varphi(x) = g(x)d(x)$, возьмем вектор $\gamma = d(\varphi)(\alpha)$. По утверждению 30(а) справедливы равенства

$$m_{\gamma,\varphi}(x) = \frac{m_\varphi(x)}{(m_\varphi(x),\, d(x))} = \frac{m_\varphi(x)}{d(x)} = g(x).$$

Покажем, что нужный вектор α существует. Пусть

$$m_\varphi(x) = g_1(x)^{k_1} \dots g_t(x)^{k_t}$$

— каноническое разложение многочлена $m_\varphi(x)$ над полем P. По утверждению 31 верно равенство

$$m_\varphi(x) = [\, m_{\alpha_1,\varphi}(x),\, \dots,\, m_{\alpha_n,\varphi}(x)\,],$$

где $\vec{\alpha} = (\alpha_1, \dots, \alpha_n)$ — базис пространства L_P. Многочлен $g_j(x)^{k_j}$, $j \in \overline{1,t}$, делит какой-то многочлен $m_{\alpha_{i_j},\varphi}(x)$, так как многочлен $g_j(x)$ неприводим над полем P. Обозначив $\alpha_{i_j} = \beta_j$, запишем $m_{\beta_j,\varphi}(x) = g_j(x)^{k_j} f_j(x)$ (возможно, при $l \neq j$ имеет место равенство $\alpha_{i_j} = \alpha_{i_l}$, т. е. $\beta_j = \beta_l$). По утверждению 30(а) вектор $\gamma_j = f_j(\varphi)(\beta_j)$ имеет минимальный многочлен $g_j(x)^{k_j}$, а по утверждению 30(б) вектор $\alpha = \gamma_1 + \ldots + \gamma_t$ удовлетворяет условию $m_{\alpha,\varphi}(x) = m_\varphi(x)$. □

§ 6. ИНВАРИАНТНЫЕ ПОДПРОСТРАНСТВА. ЦИКЛИЧЕСКИЕ ПОДПРОСТРАНСТВА

Определение 18. Подпространство K_P произвольного пространства L_P называют *инвариантным относительно преобразования* $\varphi \in \mathfrak{L}(L_P)$, если $\varphi(K) \subset K$.

Понятие подпространства, инвариантного относительно линейного преобразования, обобщает понятие собственного вектора этого преобразования.

Пример 18. Пусть $\alpha \in L_P$ и $\varphi \in \mathfrak{L}(L_P)$. Тогда подпространство $K_P = (\alpha)_P$ инвариантно относительно преобразования φ тогда и только тогда, когда α — собственный вектор преобразования φ (проверьте).

Пример 19. Если $\alpha_i \in L_P$, $i \in \overline{1,t}$ — собственные векторы преобразования φ, то подпространство $K_P = (\alpha_1, \dots, \alpha_t)_P$ инвариантно относительно φ (проверьте).

Однако существуют подпространства, инвариантные относительно преобразования φ, не содержащие ни одного собственного вектора этого преобразования.

Пример 20. Пусть ψ — преобразование пространства D^3, осуществляющее его поворот вокруг оси OZ на угол $\pi/2$ против часовой стрелки. Плоскость XOY инвариантна относительно ψ, но не содержит ни одного собственного вектора этого преобразования.

Утверждение 34. *Пусть $\alpha_1, \ldots, \alpha_m \in L_P$, где L_P — произвольное пространство. Подпространство $K_P = (\alpha_1, \ldots, \alpha_m)_P$ инвариантно относительно преобразования $\varphi \in \mathfrak{L}(L_P)$ тогда и только тогда, когда $\varphi(\alpha_i) \in K$ для $i \in \overline{1,m}$.*

Доказательство этого утверждения предоставляется читателю.

Определение 19. Пусть L_P — произвольное пространство, $\varphi \in \mathfrak{L}(L_P)$ и K_P — подпространство в L_P, инвариантное относительно φ. Отображение $\psi\colon K_P \to K_P$, определенное формулой

$$\forall\, \gamma \in K_P:\ \ \psi(\gamma) = \varphi(\gamma),$$

называют *ограничением преобразования φ на подпространстве K_P* (обозначение: $\psi = \varphi\big|_{K_P}$). Очевидно, что $\psi \in \mathfrak{L}(K_P)$.

Существование в конечномерном пространстве L_P, инвариантного относительно преобразования $\varphi \in \mathfrak{L}(L_P)$ собственного подпространства, позволяет упростить матрицу этого преобразования.

Теорема 35. *Пусть $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ — базис пространства L_P и $\varphi \in \mathfrak{L}(L_P)$. Матрица $A_{\vec{\alpha}}(\varphi)$ является полураспавшейся матрицей вида*

$$A_{\vec{\alpha}}(\varphi) = \begin{pmatrix} B_{k\times k} & C_{k\times(n-k)} \\ O_{(n-k)\times k} & D_{(n-k)\times(n-k)} \end{pmatrix} \tag{44}$$

тогда и только тогда, когда подпространство $K_P = (\alpha_1, \ldots, \alpha_k)_P$ инвариантно относительно φ. При выполнении последнего условия матрица B есть матрица преобразования $\psi = \varphi\big|_{K_P}$ в базисе $\vec{\alpha}\,' = (\alpha_1, \ldots, \alpha_k)$, и $\chi_\psi(x) \mid \chi_\varphi(x)$.

□ По определению 8 матрица $A_{\vec{\alpha}}(\varphi)$ имеет вид (44) тогда и только тогда, когда

$$\varphi(\alpha_i) = \alpha_1 b_{1i} + \ldots + \alpha_k b_{ki}, \quad i \in \overline{1,k}, \tag{45}$$

т. е. когда $\varphi(\alpha_i) \in K_P$, $i \in \overline{1,k}$. По утверждению 34 выполнение последних соотношений равносильно тому, что K_P — инвариантное относительно φ подпространство.

По определениям 19 и 8 равенства (45) означают, что $B = A_{\vec{\alpha}'}(\psi)$. По определению 13 $\chi_\varphi(x) = \chi_{A_{\vec{\alpha}}(\varphi)}(x)$ и $\chi_\psi(x) = \chi_B(x)$. Ввиду утверждения 20 имеем $\chi_\varphi(x) = \chi_\psi(x)\chi_D(x)$. □

Теорема 36. *Пусть $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ — базис пространства L_P и $\varphi \in \mathfrak{L}(L_P)$. Матрица $A_{\vec{\alpha}}(\varphi)$ является распавшейся и имеет вид*

$$A_{\vec{\alpha}}(\varphi) = \mathrm{Diag}(B_{k\times k},\, D_{(n-k)\times(n-k)}),$$

где $1 \leqslant k < n$ тогда и только тогда, когда подпространства $K_P = (\alpha_1, \ldots, \alpha_k)_P$ и $M_P = (\alpha_{k+1}, \ldots, \alpha_n)_P$ инвариантны относительно φ.

При этом если $\psi = \varphi\big|_{K_P}$ и $\xi = \varphi\big|_{M_P}$, то выполняются равенства $B = A_{(\alpha_1,\ldots,\alpha_k)}(\psi)$, $D = A_{(\alpha_{k+1},\ldots,\alpha_n)}(\xi)$ и $\chi_\varphi(x) = \chi_\psi(x)\chi_\xi(x)$.

□ Доказательство теоремы аналогично доказательству теоремы 35 и предоставляется читателю. □

Следующие утверждения дают важные примеры инвариантных подпространств.

Утверждение 37. *Если L_P — произвольное пространство, $\varphi \in \mathfrak{L}(L_P)$ и $f(x) \in P[x]$, то подпространства* $\operatorname{Ker} f(\varphi)$ *и $f(\varphi)(L)$ инвариантны относительно преобразования φ.*

□ По утверждению 1 $\operatorname{Ker} f(\varphi)$ и $f(\varphi)(L)$ — подпространства пространства L_P. Пусть $\alpha \in f(\varphi)(L)$, т. е. $\alpha = f(\varphi)(\beta)$, где $\beta \in L_P$. В силу утверждения 23(а) справедливы равенства:

$$\varphi(\alpha) = \varphi(f(\varphi)(\beta)) = f(\varphi)(\varphi(\beta)),$$

показывающие, что $\varphi(\alpha) \in f(\varphi)(L)$. По определению 18 $f(\varphi)(L)$ — подпространство, инвариантное относительно φ.

Пусть $\gamma \in \operatorname{Ker} f(\varphi)$, т. е. $f(\varphi)(\gamma) = \theta$. Тогда

$$f(\varphi)(\varphi(\gamma)) = \varphi(f(\varphi)(\gamma)) = \varphi(\theta) = \theta.$$

Следовательно, $\varphi(\gamma) \in \operatorname{Ker} f(\varphi)$. Значит, подпространство $\operatorname{Ker} f(\varphi)$ инвариантно относительно φ. □

Утверждение 38. *Пусть $\varphi \in \mathfrak{L}(L_P)$, где $\dim L_P = n$, $\alpha \in L_P \setminus \{\theta\}$ и*

$$m_{\alpha,\varphi}(x) = x^k - c_{k-1}x^{k-1} - \ldots - c_0.$$

Тогда

(а) *подпространство $L^\varphi(\alpha) = (\alpha, \varphi(\alpha), \ldots, \varphi^{k-1}(\alpha))_P$ инвариантно относительно φ и $\dim L^\varphi(\alpha)_P = k$;*

(б) *если $\psi = \varphi\big|_{L^\varphi(\alpha)}$, то $\chi_\psi(x) = m_{\alpha,\psi}(x) = m_\psi(x) = m_{\alpha,\varphi}(x)$;*

(в) *подпространство $L^\varphi(\alpha)$ содержится в любом инвариантном относительно φ подпространстве, содержащем вектор α.*

□ (а) По утверждению 32 система векторов $\alpha, \varphi(\alpha), \ldots, \varphi^{k-1}(\alpha)$ линейно независима. Значит, $\dim L^\varphi(\alpha)_P = k$. При $i < k-1$ имеем: $\varphi(\varphi^i(\alpha)) = \varphi^{i+1}(\alpha) \in L^\varphi(\alpha)$. Кроме того, по утверждению 32 $\varphi(\varphi^{k-1}(\alpha)) = \sum_{i=0}^{k-1} \varphi^i(\alpha)c_i \in L^\varphi(\alpha)$. Тогда по утверждению 34 подпространство $L^\varphi(\alpha)$ инвариантно относительно φ.

(б) По определению преобразования ψ верно равенство $m_{\alpha,\psi}(x) = m_{\alpha,\varphi}(x)$. Поэтому $\deg m_{\alpha,\psi}(x) = k$. По следствию теоремы 29 и следствию 1 теоремы 27 $m_{\alpha,\psi}(x) \mid m_\psi(x)$ и $m_\psi(x) \mid \chi_\psi(x)$. По утверждению (а) $\deg \chi_\psi(x) = \dim L^\varphi(\alpha) = k$. Но тогда $\chi_\psi(x) = m_{\alpha,\psi}(x) = m_\psi(x)$.

(в) Пусть M_P — подпространство пространства L_P, инвариантное относительно φ и содержащее вектор α. Тогда $\varphi^i(\alpha) \in M_P$ при любом $i \in \mathbb{N}$. Следовательно, верно включение $L^\varphi(\alpha) \subset M_P$. □

Определение 20. Подпространство $L^{\varphi}(\alpha)$ пространства L_P, построенное в утверждении 38, называют *циклическим относительно φ подпространством, порожденным вектором α*, а его базис α, $\varphi(\alpha)$, $\ldots$, $\varphi^{k-1}(\alpha)$ — *циклическим базисом* этого пространства.

Пространство L_P называют *циклическим относительно преобразования* $\varphi \in \mathfrak{L}(L_P)$, если $L = L^{\varphi}(\alpha)$ для подходящего $\alpha \in L_P$.

Получим критерий цикличности пространства.

Определение 21. Пусть $f(x) = x^n - c_{n-1}x^{n-1} - \ldots - c_1 x - c_0 \in P[x]$. Матрицу

$$S(f(x)) = \begin{pmatrix} 0 & 0 & \ldots & 0 & 0 & c_0 \\ e & 0 & \ldots & 0 & 0 & c_1 \\ 0 & e & \ldots & 0 & 0 & c_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & e & 0 & c_{n-2} \\ 0 & 0 & \ldots & 0 & e & c_{n-1} \end{pmatrix}_{n\times n}$$

называют *сопровождающей матрицей многочлена $f(x)$*.

Пример 21. Пусть пространство L_P циклическое относительно преобразования φ и $L_P = (\alpha, \varphi(\alpha), \ldots, \varphi^{n-1}(\alpha))_P$. По утверждению 32 $\varphi^n(\alpha) = \sum_{i=0}^{n-1} \varphi^i(\alpha) c_i$, где $m_{\alpha,\varphi}(x) = x^n - c_{n-1}x^{n-1} - \ldots - c_0$. Обозначив $\vec{\alpha} = (\alpha, \varphi(\alpha), \ldots, \varphi^{n-1}(\alpha))$, получаем, учитывая утверждение 38(б): $A_{\vec{\alpha}}(\varphi) = S(m_{\alpha,\varphi}(x)) = S(m_{\varphi}(x))$.

Утверждение 39. *Если $\varphi \in \mathfrak{L}(L_P)$, где $\dim L_P = n$, то равносильны утверждения*:

(а) *L_P — циклическое относительно φ пространство*;

(б) *$m_{\varphi}(x) = \chi_{\varphi}(x)$*;

(в) *существует такой базис $\vec{\alpha}$ пространства L_P, что $A_{\vec{\alpha}}(\varphi) = S(f(x))$ для некоторого унитарного многочлена $f(x) \in P[x]$.*

□ (а)⇒(б) Пусть $L_P = L^{\varphi}(\alpha)$ и $\dim L_P = n$. Тогда система векторов $\alpha, \ldots, \varphi^{n-1}(\alpha)$ линейно независима и $\deg m_{\alpha,\varphi}(x) = n$. Поэтому $m_{\alpha,\varphi}(x) = \chi_{\varphi}(x)$. Ввиду соотношений $m_{\alpha,\varphi}(x) \mid m_{\varphi}(x)$ и $m_{\varphi}(x) \mid \chi_{\varphi}(x)$ получаем $m_{\varphi}(x) = \chi_{\varphi}(x)$.

(б)⇒(в) В силу теоремы 33 существует такой вектор $\gamma \in L_P$, что $m_{\gamma,\varphi}(x) = m_{\varphi}(x)$. По условию тогда $m_{\gamma,\varphi}(x) = \chi_{\varphi}(x)$. По утверждению 32 система векторов $\vec{\alpha} = (\gamma, \varphi(\gamma), \ldots, \varphi^{n-1}(\gamma))$ линейно независима и, значит, является циклическим базисом пространства L_P. В силу примера 21

$$A_{\vec{\alpha}}(\varphi) = S(m_{\gamma,\varphi}(x)) = S(\chi_{\varphi}(x)).$$

(в)⇒(а) Пусть $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ — такой базис пространства L_P, что $A_{\vec{\alpha}}(\varphi) = S(f(x))$. Из вида матрицы $S(f(x))$ следует, что тогда $\varphi(\alpha_i) = \alpha_{i+1}$ при $i \in \overline{1, n-1}$. Значит, $\vec{\alpha}$ — циклический базис пространства L_P относительно преобразования φ и $L_P = L^{\varphi}(\alpha_1)$. □

Следствие. *Для матрицы $S(f(x))$ справедливы равенства*

$$\chi_{S(f(x))}(x) = m_{S(f(x))}(x) = f(x).$$

□ Пусть $\deg f(x) = n$ и $\vec{\alpha}$ — базис пространства L_P, $\dim L_P = n$. Зададим $\varphi \in \mathfrak{L}(L_P)$, положив $A_{\vec{\alpha}}(\varphi) = S(f(x))$. По определению 13 и следствию 2 теоремы 27 верны равенства $\chi_\varphi(x) = \chi_{S(f(x))}(x)$ и $m_\varphi(x) = m_{S(f(x))}(x)$. По утверждению 39 получаем $\chi_{S(f(x))}(x) = m_{S(f(x))}(x)$. Непосредственно проверяется, что $\chi_{S(f(x))}(x) = |Ex - S(f(x))| = f(x)$. □

Замечание 4. Утверждение 39 дает критерий того, чтобы подпространство K_P пространства L_P, инвариантное относительно преобразования φ, было циклическим относительно φ подпространством. Действительно, если $\psi = \varphi\big|_{K_P}$, то подпространство K_P циклично относительно φ тогда и только тогда, когда K_P циклично относительно ψ.

Теперь получим критерий того, чтобы конечномерное пространство L_P не имело собственных инвариантных подпространств.

Теорема 40. *Пусть $\varphi \in \mathfrak{L}(L_P)$. Пространство L_P, $\dim L_P = n$, не имеет собственных подпространств, инвариантных относительно φ, тогда и только тогда, когда многочлен $\chi_\varphi(x)$ неприводим над полем P.*

□ Пусть в L_P есть собственное инвариантное относительно φ подпространство K_P. Базис $\alpha_1, \ldots, \alpha_k$, $1 \leqslant k < n$, этого подпространства дополним до базиса $\vec{\alpha} = (\alpha_1, \ldots, \alpha_k, \ldots, \alpha_n)$ пространства L_P. По теореме 35 тогда матрица $A_{\vec{\alpha}}(\varphi)$ — полураспавшаяся и имеет вид (44). По утверждению 20 и определению 13 $\chi_\varphi(x) = \chi_{A_{\vec{\alpha}}(\varphi)}(x) = \chi_B(x)\chi_D(x)$, где $1 \leqslant \deg \chi_B(x) < n$. Значит, многочлен $\chi_\varphi(x)$ приводим над полем P.

Обратно, пусть многочлен $\chi_\varphi(x)$ приводим над полем P. Тогда существует такой унитарный многочлен $g(x) \in P[x]$, что $g(x) \mid m_\varphi(x)$ и $0 < \deg g(x) < n = \deg \chi_\varphi(x)$. Действительно, если $\deg m_\varphi(x) < n$, то можно взять $g(x) = m_\varphi(x)$, а если $\deg m_\varphi(x) = n$, то $m_\varphi(x) = \chi_\varphi(x)$, и унитарный делитель многочлена $\chi_\varphi(x)$ является делителем и многочлена $m_\varphi(x)$.

По теореме 33 существует такой вектор $\gamma \in L_P$, что $m_{\gamma,\varphi}(x) = g(x)$. По утверждению 38 $L^\varphi(\gamma)$ — собственное подпространство в L_P, инвариантное относительно φ. □

Полученный в теореме 40 результат можно применить к решению вопроса о том, можно ли для данного преобразования $\varphi \in \mathfrak{L}(L_P)$ найти такой базис $\vec{\alpha}$ пространства L_P, чтобы матрица $A_{\vec{\alpha}}(\varphi)$ была полураспавшейся.

Определение 22. Матрицу $A \in P_{n,n}$ называют *приводимой*, если она подобна некоторой полураспавшейся матрице, и *неприводимой* в противном случае.

Следствие. *Матрица $A \in P_{n,n}$ неприводима тогда и только тогда, когда многочлен $\chi_A(x)$ неприводим над полем P.*

Следующий результат является в некотором смысле обратным к следствию 1 теоремы 27.

Теорема 41. *Если $A \in P_{n,n}$ и $g(x)$ — неприводимый делитель многочлена $\chi_A(x)$, то $g(x) \mid m_A(x)$.*

□ Проведем доказательство индукцией по числу n. Если $n = 1$, то $\deg \chi_A(x) = 1$, т. е. $\chi_A(x)$ — неприводимый над полем P многочлен. Тогда $m_A(x) = \chi_A(x)$ и $g(x) = m_A(x) = \chi_A(x)$.

Пусть теорема верна для любой матрицы, принадлежащей $P_{m,m}$, при $1 \leqslant m < n$. Докажем, что тогда она верна и для матрицы $A \in P_{n,n}$.

Если многочлен $\chi_A(x)$ неприводим над полем P, то вновь $g(x) = m_A(x) = \chi_A(x)$. Если же многочлен $\chi_A(x)$ приводим над полем P, то по следствию теоремы 40

$$A \approx \begin{pmatrix} B_{k\times k} & C_{k\times(n-k)} \\ O_{(n-k)\times k} & D_{(n-k)\times(n-k)} \end{pmatrix},$$

где $1 \leqslant k < n$. Так как $\chi_A(x) = \chi_B(x)\chi_D(x)$, то $g(x)$ делит либо $\chi_B(x)$, либо $\chi_D(x)$. По предположению индукции $g(x) \mid m_B(x)$ или $g(x) \mid m_D(x)$. Следовательно, $g(x) \mid [m_B(x), m_D(x)]$ и по утверждению 28 $g(x) \mid m_A(x)$. □

Следствие 1. *Если $\varphi \in \mathfrak{L}(L_P)$, где $\dim L_P = n$, и $g(x)$ — неприводимый делитель многочлена $\chi_\varphi(x)$, то $g(x) \mid m_\varphi(x)$.*

Следствие 2. *Если $\varphi \in \mathfrak{L}(L_P)$, где $\dim L_P = n$, то существует такое $k \in \mathbb{N}$, что $\chi_\varphi(x) \mid m_\varphi(x)^k$. При этом $k \leqslant n$.*

Доказательство следствий предоставляется читателю.

Замечание 5. Теорема 41 является аналогом леммы Коши в теории групп (лемма 48 главы 11).

§ 7. РАЗЛОЖЕНИЕ ПРОСТРАНСТВА В ПРЯМУЮ СУММУ ИНВАРИАНТНЫХ ПОДПРОСТРАНСТВ

Основой для дальнейшего является

Теорема 42. *Пусть L_P — произвольное пространство. Если многочлен $f(x) \in P[x]$ аннулирует преобразование $\varphi \in \mathfrak{L}(L_P)$ и*

$$f(x) = f_1(x) \cdot \ldots \cdot f_t(x),$$

где $(f_i(x), f_j(x)) = e$ при $i \neq j$, то пространство L_P раскладывается в прямую сумму инвариантных относительно φ подпространств:

$$L_P = \operatorname{Ker} f_1(\varphi) \dotplus \ldots \dotplus \operatorname{Ker} f_t(\varphi). \tag{46}$$

□ Проведем доказательство индукцией по числу t. При $t = 2$ по условию для многочленов $f_1(x)$ и $f_2(x)$ найдутся многочлены $u_1(x), u_2(x)$ такие, что $f_1(x)u_1(x) + f_2(x)u_2(x) = e$. По утверждению 23(а) отсюда получаем $\varepsilon = \widehat{e} = f_1(\varphi) \circ u_1(\varphi) + f_2(\varphi) \circ u_2(\varphi)$. Поэтому произвольный вектор $\gamma \in L_P$ представим в виде

$$\gamma = \varepsilon(\gamma) = (f_1(\varphi) \circ u_1(\varphi))(\gamma) + (f_2(\varphi) \circ u_2(\varphi))(\gamma).$$

При этом $(f_1(\varphi) \circ u_1(\varphi))(\gamma) \in \operatorname{Ker} f_2(\varphi)$ и $(f_2(\varphi) \circ u_2(\varphi))(\gamma) \in \operatorname{Ker} f_1(\varphi)$, поскольку $f(x) = f_1(x)f_2(x)$ и $f(\varphi) = \widehat{0}$. Следовательно,

$$L_P = \operatorname{Ker} f_1(\varphi) + \operatorname{Ker} f_2(\varphi).$$

Пусть $\beta \in \operatorname{Ker} f_1(\varphi) \cap \operatorname{Ker} f_2(\varphi)$. Тогда $f_1(\varphi)(\beta) = f_2(\varphi)(\beta) = \theta$. Так как $(f_1(x), f_2(x)) = e$, то по утверждению 23(б) $\beta = \theta$. Ввиду теоремы 13 главы 13 получаем:

$$L_P = \operatorname{Ker} f_1(\varphi) \dotplus \operatorname{Ker} f_2(\varphi).$$

Дальнейшее проведение индукции предоставляется читателю. □

Некоторые из подпространств $\operatorname{Ker} f_i(\varphi)$ в разложении (46) могут быть нулевыми.

Пример 22. Пусть $\varphi = \varepsilon$. Для многочлена $f(x) = x(x - e)$ выполнены условия теоремы 42. Тогда

$$L_P = \operatorname{Ker} \varepsilon \dotplus \operatorname{Ker} \widehat{0} = \theta \dotplus L_P.$$

Ниже (теорема 44) будет показано, что при некоторых условиях на многочлен $f(x)$ в разложении (46) нет нулевых слагаемых.

Укажем критерий подобия матрицы $A \in P_{n,n}$ диагональной матрице.

Теорема 43. *Матрица $A \in P_{n,n}$ подобна диагональной матрице тогда и только тогда, когда многочлен $m_A(x)$ раскладывается над полем P на линейные множители и не имеет кратных корней.*

□ Если $A \approx D = \operatorname{diag}(r_1, \ldots, r_n)$, $r_i \in P$, то по следствию 3 теоремы 27 и утверждению 28 $m_A(x) = m_D(x) = [x - r_1, \ldots, x - r_n]$. Стало быть, $m_A(x)$ раскладывается над полем P на линейные множители и не имеет кратных корней.

Обратно, пусть $m_A(x) = (x - r_1) \ldots (x - r_t)$, где $r_i \in P$ и $r_i \neq r_j$ при $i \neq j$. Рассмотрим произвольное пространство M_P, для которого $\dim M_P = n$. Пусть $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ — базис этого пространства. Зададим преобразование $\varphi \in \mathfrak{L}(M_P)$, положив $A_{\vec{\alpha}}(\varphi) = A$. Тогда $m_\varphi(x) = m_A(x)$ по следствию 2 теоремы 27.

По теореме 42 при $f(x) = m_\varphi(x)$ получаем

$$M_P = \operatorname{Ker}(\varphi - \widehat{r}_1) \dotplus \ldots \dotplus \operatorname{Ker}(\varphi - \widehat{r}_t).$$

Каждый ненулевой вектор подпространства $\operatorname{Ker}(\varphi - \widehat{r}_i)$ является собственным вектором преобразования φ, принадлежащим собственному значению r_i. Поэтому базис $\vec{\beta}$ пространства M_P, составленный из базисов подпространств $\operatorname{Ker}(\varphi - \widehat{r}_i)$, $i \in \overline{1,t}$, состоит из собственных векторов преобразования φ. По утверждению 18 $A_{\vec{\beta}}(\varphi)$ — диагональная матрица. Остается заметить, что в силу утверждения 15 матрицы $A_{\vec{\alpha}}(\varphi)$ и $A_{\vec{\beta}}(\varphi)$ подобны. □

Уточним теперь теорему 42 в случае, когда пространство L_P конечномерно и $f(x) = \chi_\varphi(x)$.

Теорема 44. *Если* $\varphi \in \mathfrak{L}(L_P)$, *где* $\dim L_P = n$, *и*

$$\chi_\varphi(x) = f_1(x) \cdot \ldots \cdot f_t(x),$$

где $t > 1$, $(f_i(x), f_j(x)) = e$ *при* $i \neq j$ *и* $\deg f_i(x) > 0$ *при* $i \in \overline{1,t}$, *то пространство* L_P *раскладывается в прямую сумму инвариантных относительно* φ *подпространств*:

$$L_P = \operatorname{Ker} f_1(\varphi) \dotplus \ldots \dotplus \operatorname{Ker} f_t(\varphi). \tag{47}$$

При этом, $\dim \operatorname{Ker} f_i(\varphi) = \deg f_i(x)$ *и* $f_i(x) = \chi_{\varphi_i}(x)$, *где* $\varphi_i = \varphi\big|_{\operatorname{Ker} f_i(\varphi)}$.

□ Равенство (47) получено в теореме 42 ($\chi_\varphi(\varphi) = \widehat{0}$ по теореме Гамильтона–Кэли).

По условию $\deg f_i(x) > 0$. Многочлен $f_i(x)$ или неприводим, или имеет неприводимый унитарный делитель $g_i(x)$ (в первом случае считаем $g_i(x) = f_i(x)$). По следствию 1 теоремы 41 $g_i(x) \mid m_\varphi(x)$. Тогда по теореме 33 существует такой вектор $\alpha_i \in L_P$, что $m_{\alpha_i,\varphi}(x) = g_i(x)$. Отсюда следует, что $\alpha_i \neq \theta$. Кроме того, $f_i(\varphi)(\alpha_i) = \theta$, т. е. $\alpha_i \in \operatorname{Ker} f_i(\varphi)$. Этим показано, что $\operatorname{Ker} f_i(\varphi) \neq \theta$ при $i \in \overline{1,t}$. Отсюда следует, что $\deg \chi_{\varphi_i}(x) > 0$.

По теореме 36 в базисе $\vec{\alpha}$ пространства L_P, составленном из базисов подпространств $\operatorname{Ker} f_i(\varphi)$, матрица $A_{\vec{\alpha}}(\varphi)$ распавшаяся, и $\chi_\varphi(x) = \chi_{\varphi_1}(x) \ldots \chi_{\varphi_t}(x)$. Ввиду условия получаем равенство

$$\chi_\varphi(x) = \chi_{\varphi_1}(x) \ldots \chi_{\varphi_t}(x) = f_1(x) \ldots f_t(x). \tag{48}$$

Пусть $t_i(x)$ — неприводимый над полем P многочлен, делящий многочлен $\chi_{\varphi_i}(x)$. По следствию 1 теоремы 41 $t_i(x) \mid m_{\varphi_i}(x)$. По теореме 33 существует такой вектор $\beta_i \in \operatorname{Ker} f_i(\varphi)$, что $m_{\beta_i,\varphi_i}(x) = t_i(x)$. Поэтому $\beta_i \neq \theta$. Если $t_i(x) \nmid f_i(x)$, то $(t_i(x), f_i(x)) = e$, и по утверждению 23(б) $\beta_i = \theta$. Полученное противоречие показывает, что $t_i(x) \mid f_i(x)$. Поскольку $(f_i(x), f_j(x)) = e$ при $i \neq j$, то отсюда следует, что $(\chi_{\varphi_i}(x), \chi_{\varphi_j}(x)) = e$ при $i \neq j$.

Таким образом, для многочленов $f_i(x)$ и $\chi_{\varphi_j}(x)$ из равенства (48) выполнены соотношения:

1) $\deg f_i(x) > 0$, $\deg \chi_{\varphi_j}(x) > 0$;

2) $(f_i(x), f_j(x)) = (\chi_{\varphi_i}(x), \chi_{\varphi_j}(x)) = e$ при $i \neq j$;

3) любой неприводимый делитель многочлена $\chi_{\varphi_i}(x)$ делит $f_i(x)$, $i \in \overline{1,t}$.

В силу единственности канонического разложения многочлена $\chi_\varphi(x)$ над полем P отсюда следует, что $\chi_{\varphi_i}(x) = f_i(x)$, $i \in \overline{1,t}$. Из последнего равенства и равенства $\dim \operatorname{Ker} f_i(\varphi) = \deg \chi_{\varphi_i}(x)$ получаем, что $\dim \operatorname{Ker} f_i(\varphi) = \deg f_i(x)$. □

Следствие. *Если* $\varphi \in \mathfrak{L}(L_P)$ *и каноническое разложение многочлена* $\chi_\varphi(x)$ *над полем* P *имеет вид*

$$\chi_\varphi(x) = (x - r_1)^{k_1} \ldots (x - r_t)^{k_t},$$

то пространство L_P раскладывается в прямую сумму инвариантных относительно φ подпространств:

$$L_P = \operatorname{Ker}(\varphi - \widehat{r}_1)^{k_1} \dotplus \ldots \dotplus \operatorname{Ker}(\varphi - \widehat{r}_t)^{k_t}, \tag{49}$$

где $\dim \operatorname{Ker}(\varphi - \widehat{r}_i)^{k_i} = k_i$.

Определение 23. Инвариантные относительно преобразования φ подпространства $\operatorname{Ker}(\varphi - \widehat{r}_i)^{k_i}$ из разложения (49) называют *корневыми подпространствами* пространства L_P.

Разложение пространства L_P в прямую сумму циклических подпространств рассматривается в § 3 главы 16.

Замечание 6. Если в теореме 44 в качестве многочленов $f_i(x)$ выбрать примарные сомножители из канонического разложения многочлена $\chi_\varphi(x)$ над полем P, то получим аналог теоремы о разложении конечной абелевой группы в прямую сумму силовских подгрупп. Следующая теорема является аналогом утверждения о единственности каждой такой подгруппы при фиксированном простом p.

Теорема 45. *Если $A \in P_{n,n}$ и $\chi_A(x) = f_1(x)f_2(x)$, где $\deg f_i(x) > 0$, $i \in \overline{1,2}$, и $(f_1(x), f_2(x)) = e$, то матрица A подобна распавшейся матрице*

$$A' = \operatorname{Diag}(A_1, A_2),$$

где $\chi_{A_i}(x) = f_i(x)$, $i \in \overline{1,2}$.

Если матрица A подобна также распавшейся матрице

$$B' = \operatorname{Diag}(B_1, B_2),$$

где $\chi_{B_i}(x) = f_i(x)$, $i \in \overline{1,2}$, то $A_i \approx B_i$.

□ Пусть L_P — произвольное пространство размерности n и $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ — его базис. Зададим преобразование $\varphi \in \mathfrak{L}(L_P)$ условием $A_{\vec{\alpha}}(\varphi) = A$. Тогда $\chi_\varphi(x) = \chi_A(x) = f_1(x)f_2(x)$, и по теореме 44

$$L_P = \operatorname{Ker} f_1(\varphi) \dotplus \operatorname{Ker} f_2(\varphi),$$

где для преобразований $\varphi_i = \varphi\big|_{\operatorname{Ker} f_i(\varphi)}$ верны равенства $\chi_{\varphi_i}(x) = f_i(x)$ и $\dim \operatorname{Ker} f_i(\varphi) = \deg f_i(x)$. Пусть $\deg f_1(x) = k$, $(\beta_1, \ldots, \beta_k)$ — базис подпространства $\operatorname{Ker} f_1(\varphi)$ и $(\beta_{k+1}, \ldots, \beta_n)$ — базис подпространства $\operatorname{Ker} f_2(\varphi)$. Тогда $\vec{\beta} = (\beta_1, \ldots, \beta_k, \beta_{k+1}, \ldots, \beta_n)$ — базис пространства L_P, и по теореме 36

$$A \approx A' = \operatorname{Diag}(A_{(\beta_1,\ldots,\beta_k)}(\varphi_1),\ A_{(\beta_{k+1},\ldots,\beta_n)}(\varphi_2)) = \operatorname{Diag}(A_1, A_2).$$

Поскольку $\chi_{A_i}(x) = \chi_{\varphi_i}(x) = f_i(x)$, то A' — искомая матрица.

Пусть $A \approx B' = \operatorname{Diag}(B_1, B_2)$, где $\chi_{B_i}(x) = f_i(x)$, $i \in \overline{1,2}$. По утверждению 17 существует такой базис $\vec{\gamma} = (\gamma_1, \ldots, \gamma_n)$ пространства L_P, что $B' = A_{\vec{\gamma}}(\varphi)$. Покажем, что $\gamma_1, \ldots, \gamma_k$ — базис подпространства $\operatorname{Ker} f_1(\varphi)$.

Действительно, так как $B_1 \in P_{k,k}$ и $f_1(B_1) = O_{k\times k}$, то из равенств

$$A_{\vec{\gamma}}(f_1(\varphi)) \;=\; f_1(A_{\vec{\gamma}}(\varphi)) \;=\; f_1(B') \;=\; \mathrm{Diag}(f_1(B_1), f_1(B_2)) \;=\; \mathrm{Diag}(O_{k\times k}, f_1(B_2))$$

следует, что преобразование $f_1(\varphi)$ аннулирует векторы $\gamma_1, \ldots, \gamma_k$, т. е. эти векторы принадлежат подпространству $\mathrm{Ker}\, f_1(\varphi)$. Поскольку система векторов $\gamma_1, \ldots, \gamma_k$ линейно независима и $\dim \mathrm{Ker}\, f_1(\varphi) = k$, то $\gamma_1, \ldots, \gamma_k$ — базис подпространства $\mathrm{Ker}\, f_1(\varphi)$.

Но, в таком случае, из равенств

$$A_{\vec{\alpha}}(\varphi) = \mathrm{Diag}(A_1, A_2), \quad A_{\vec{\gamma}}(\varphi) = \mathrm{Diag}(B_1, B_2)$$

следует, что A_1 и B_1 — матрицы одного линейного преобразования φ_1 пространства $\mathrm{Ker}\, f_1(\varphi)$ в разных его базисах $\alpha_1, \ldots, \alpha_k$ и $\gamma_1, \ldots, \gamma_k$. Поэтому $A_1 \approx B_1$ ввиду утверждения 15.

Аналогично показывается, что $A_2 \approx B_2$. $\square$

Следствие. *Если $A \in P_{n,n}$ и каноническое разложение характеристического многочлена $\chi_A(x)$ над полем P имеет вид*

$$\chi_A(x) = g_1(x)^{k_1} \cdot \ldots \cdot g_t(x)^{k_t},$$

то матрица A подобна матрице

$$A' = \mathrm{Diag}(A_1, \ldots, A_t)$$

такой, что

$$\chi_{A_i}(x) = g_i(x)^{k_i}, \quad i \in \overline{1,t}. \tag{50}$$

Условием (50) *матрица A' определена однозначно с точностью до подобия клеток.*

Возможность дальнейшего упрощения матрицы линейного преобразования основана на более глубокой теории, которая будет изложена в следующей главе.

ЗАДАЧИ

1. Докажите, что все линейные преобразования пространства L_P являются скалярными тогда и только тогда, когда $\dim L_P \leqslant 1$.

2. Укажите какой-либо базис пространства $\mathfrak{L}(L_P)_P$, если $\dim L_P = n$.

3. Покажите, что если $\dim L_P = n$ и $\varphi \in \mathfrak{L}(L_P)$, то при справедливости равенства $\dim L_P = \dim \varphi(L_P) + \dim \mathrm{Ker}\, \varphi$ не всегда имеет место равенство $L_P = \varphi(L_P) \dotplus \mathrm{Ker}\, \varphi$.

4. Пусть A, $B \in P_{n,n}$ и $B = C^{-1}AC$. Покажите, что множество всех таких матриц $X \in P_{n,n}$, для которых $X^{-1}AX = B$, есть

$$\{KC\colon\ K \in P^*_{n,n},\ K^{-1}AK = A\}.$$

5. Покажите, что если $\dim L_P = n$, то матрицы преобразования $\varphi \in \mathfrak{L}(L_P)$ в любых базисах равны тогда и только тогда, когда φ — скалярное преобразование.

6. Сколько существует обратимых линейных преобразований пространства L_P, если $\dim L_P = n$ и $|P| = q$?

7. Покажите, что все ненулевые векторы пространства L_P являются собственными векторами преобразования $\varphi \in \mathfrak{L}(L_P)$ тогда и только тогда, когда φ — скалярное преобразование.

8. Пусть $\dim L_{\mathbb{C}} = n$. Покажите, что для любого преобразования $\varphi \in \mathfrak{L}(L_{\mathbb{C}})$ существует собственный вектор.

9. Покажите, что если $\dim L_{\mathbb{R}} = 2k+1$, то для любого преобразования $\varphi \in \mathfrak{L}(L_{\mathbb{R}})$ существует собственный вектор, а если $\dim L_{\mathbb{R}} = 2k$, то существует преобразование $\psi \in \mathfrak{L}(L_{\mathbb{R}})$, не имеющее собственных векторов.

10. Покажите, что если $\dim L_{\mathbb{Q}} = n > 1$, то существует преобразование $\varphi \in \mathfrak{L}(L_{\mathbb{Q}})$, не имеющее собственных векторов.

11. Покажите, что если $\dim L_P = n > 1$ и $|P| = q$, то существует преобразование $\varphi \in \mathfrak{L}(L_P)$, не имеющее собственных векторов.

12. Покажите, что если $\varphi \in \mathfrak{L}(L_P)$, где $\dim L_P = n$, и характеристический многочлен $\chi_\varphi(x)$ раскладывается над полем P на линейные множители, то в любом ненулевом инвариантном относительно φ подпространстве есть собственный вектор преобразования φ.

13. Покажите, что матрицы A, $A' \in P_{n,n}$ подобны, где

$$A = \begin{pmatrix} B_{k\times k} & C_{k\times(n-k)} \\ O_{(n-k)\times k} & D_{(n-k)\times(n-k)} \end{pmatrix}, \quad A' = \begin{pmatrix} D_{(n-k)\times(n-k)} & O_{(n-k)\times k} \\ C_{k\times(n-k)} & B_{k\times k} \end{pmatrix}.$$

14. Покажите, что матрица A подобна диагональной матрице над соответствующим полем, если

а) $A \in \mathbb{R}_{n,n}$, $A^2 = E_{n\times n}$;

б) $A \in \mathbb{C}_{n,n}$, $A^t = E_{n\times n}$, $t \in \mathbb{N}$;

в) $A \in P_{n,n}$, $A^2 = A$.

15. Приведите пример матриц $A, B \in P_{n,n}$ таких, что $\chi_A(x) = \chi_B(x)$ и $m_A(x) = m_B(x)$, но матрицы не подобны.

16. Пусть $\varphi \in \mathfrak{L}(L_P)$, $\dim L_P = n$, $r \in P$ и $\chi_\varphi(x) = (x-r)^k g(x)$, где $(g(x), x-r) = e$. Докажите, что если $\alpha_1, \ldots, \alpha_s$ — линейно независимая система собственных векторов преобразования φ, принадлежащих собственному значению r, то $s \leqslant k$. (*Указание*: дополните систему $\alpha_1, \ldots, \alpha_s$ до базиса $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ пространства L_P, выпишите матрицу $A_{\vec{\alpha}}(\varphi)$ и вычислите $\chi_{A_{\vec{\alpha}}(\varphi)}(x) = \chi_\varphi(x)$.)

Глава 16

ПОДОБИЕ МАТРИЦ НАД ПОЛЕМ

В предыдущей главе, рассматривая матрицы одного и того же линейного преобразования конечномерного векторного пространства в разных базисах, мы обнаружили, что они подобны. Наоборот, две подобные матрицы над полем можно считать матрицами одного и того же линейного преобразования некоторого пространства, заданными в разных его базисах.

В этой главе будет дан критерий подобия матриц над полем, не связанный с соответствующими им преобразованиями, и указан алгоритм решения вопроса о подобии матриц A, $B \in P_{n,n}$ и отыскания решений уравнения $B = X^{-1}AX$ в случае, если матрицы A и B подобны.

Был также поставлен вопрос о том, какая из матриц, подобных данной матрице, имеет наиболее простой вид. В частности, были рассмотрены вопросы о подобии матрицы из $P_{n,n}$ диагональной, полураспавшейся или распавшейся матрице. Здесь будут введены нормальные и жордановы матрицы и показано, что всякая матрица из $P_{n,n}$ подобна матрице, имеющей нормальную форму, а матрица, характеристический многочлен которой раскладывается над полем P на линейные множители, подобна матрице, имеющей жорданову форму.

§ 1. КРИТЕРИЙ ПОДОБИЯ МАТРИЦ НАД ПОЛЕМ

Для решения вопроса о подобии матриц A, $B \in P_{n,n}$ над полем P нам придется рассмотреть кольцо полиномиальных матриц $P[x]_{n,n}$. Так как $P[x]$ — коммутативное кольцо с единицей, то к матрицам из $P[x]_{n,n}$ применимы результаты § 5 главы 6 об элементарных преобразованиях матриц. Если не оговорено противное, то через E будем обозначать матрицу $E_{n\times n} \in P_{n,n}$.

В лемме 25 главы 15 было показано, что существует изоморфизм колец $\tau\colon P[x]_{n,n} \to P_{n,n}[\overline{x}]$. Фраза «разделим матрицу $C(x) \in P[x]_{n,n}$ как многочлен с остатком слева на унитарный многочлен $Ex - D$, $D \in P_{n,n}$», будет означать следующее. Разделим многочлен $C(\overline{x}) = \tau(C(x))$ с остатком на многочлен $\tau(Ex - D) = E\overline{x} - D$:

$$C(\overline{x}) = (E\overline{x} - D)F(\overline{x}) + Q(\overline{x})$$

и, воспользовавшись обратным изоморфизмом τ^{-1}, получим равенство

$$C(x) = (Ex - D)F(x) + Q(x), \tag{1}$$

где $F(x) = \tau^{-1}(F(\overline{x}))$, $Q(x) = \tau^{-1}(Q(\overline{x}))$. Равенство (1) и есть результат деления $C(x)$ с остатком слева на $Ex - D$. Аналогично под «степенью многочлена $C(x) \in P[x]_{n,n}$» понимаем степень многочлена $C(\overline{x}) = \tau(C(x))$.

Ввиду замечания 3 главы 9 будем считать, что $P \subset P[x]$ и потому $P_{n,n} \subset P[x]_{n,n}$.

Теорема 1. *Матрицы A, $B \in P_{n,n}$ подобны над полем P тогда и только тогда, когда в кольце $P[x]_{n,n}$ эквивалентны их характеристические матрицы.*

□ Если $T^{-1}AT = B$ для некоторой матрицы $T \in P^*_{n,n}$, то в кольце $P[x]_{n,n}$ справедливы равенства

$$T^{-1}(Ex - A)T = T^{-1}x\,T - T^{-1}AT = T^{-1}Tx - B = Ex - B.$$

Так как T, $T^{-1} \in P^*_{n,n}$, то по следствию 3 теоремы 4 главы 7 получаем, что $Ex - B \sim Ex - A$.

Обратно, пусть $Ex - B \sim Ex - A$. По утверждению 13 главы 6 при некоторых матрицах $L(x)$, $R(x) \in P[x]^*_{n,n}$ выполнено равенство

$$L(x)(Ex - A)R(x) = Ex - B,$$

которое перепишем в виде

$$L(x)(Ex - A) = (Ex - B)R(x)^{-1}. \tag{2}$$

Разделим матрицы $L(x)$ и $R(x)^{-1}$ как многочлены с остатком на унитарные многочлены $Ex - B$ и $Ex - A$ соответственно слева и справа:

$$L(x) = (Ex - B)U(x) + \overline{L}(x), \tag{3}$$

$$R(x)^{-1} = V(x)(Ex - A) + \overline{R}(x). \tag{4}$$

Поскольку $\deg(E\overline{x} - B) = \deg(E\overline{x} - A) = 1$, то $\deg \overline{L}(x)$, $\deg \overline{R}(x) < 1$ и $\overline{L}(x) = \overline{L}$, $\overline{R}(x) = \overline{R}$ — матрицы над полем P.

Подставив правые части равенств (3) и (4) в равенство (2), получим равенство

$$(Ex - B)U(x)(Ex - A) + \overline{L}(Ex - A) = (Ex - B)V(x)(Ex - A) + (Ex - B)\overline{R},$$

которое после очевидных преобразований запишем в виде

$$(Ex - B)(U(x) - V(x))(Ex - A) = (Ex - B)\overline{R} - \overline{L}(Ex - A). \tag{5}$$

Если $U(x) - V(x) \neq O_{n\times n}$, то в силу унитарности многочленов $Ex - B$ и $Ex - A$ многочлен из левой части равенства (5) имеет степень не ниже второй, а многочлен из правой части — степень не выше первой, что невозможно. Значит, верно равенство $U(x) - V(x) = O_{n\times n}$, и получаем

$$\overline{L}(Ex - A) = (Ex - B)\overline{R}. \tag{6}$$

Тогда по определению равенства многочленов:

$$\overline{L} = \overline{R}, \quad \overline{L}A = B\overline{R}. \tag{7}$$

Остается доказать, что $\overline{R} \in P^*_{n,n}$, поскольку тогда из (7) следует, что $B = \overline{R}A\overline{R}^{-1}$, т. е. $B \approx A$.

Разделим с остатком матрицу $R(x)$ как многочлен на $Ex - B$ справа:

$$R(x) = W(x)(Ex - B) + S, \quad S \in P_{n,n}. \tag{8}$$

Перемножая левые и правые части равенств (4) и (8), приходим к равенствам

$$E = R(x)R(x)^{-1} = R(x)V(x)(Ex - A) + R(x)\overline{R} = \\ = R(x)V(x)(Ex - A) + W(x)(Ex - B)\overline{R} + S\overline{R}.$$

Отсюда и из (6) получаем

$$E = [R(x)V(x) + W(x)\overline{L}\,](Ex - A) + S\overline{R}.$$

В правой части последнего равенства должен быть многочлен нулевой степени. Ввиду унитарности многочлена $Ex - A$:

$$R(x)V(x) + W(x)\overline{L} = O_{n\times n}, \quad E = S\overline{R} \quad \text{и} \quad S = \overline{R}^{-1}. \quad \square$$

Доказательство теоремы 1 дает способ отыскания одного решения уравнения $X^{-1}AX = B$, если существует и известна матрица $R(x)$. Действительно, в этом случае решением будет, например, матрица S, являющаяся остатком от деления матрицы $R(x)$ как многочлена справа на $Ex - B$ (формула (8)). При этом деление с остатком производить не нужно, так как по теореме Безу для $R(x) = R_m x^m + \ldots + R_1 x + R_0$, где $R_i \in P_{n,n}$, $i \in \overline{0,m}$, получаем

$$S = R(B) = R_m B^m + \ldots + R_1 B + R_0. \tag{9}$$

Задача отыскания матрицы S сводится, таким образом, к следующему: выяснить, эквивалентны ли матрицы $Ex - A$ и $Ex - B$ и, если да, указать последовательность элементарных преобразований, переводящих одну в другую. Решение последней задачи для произвольных матриц из $P[x]_{m,n}$ рассматривается в следующем параграфе.

Далее для краткости через O будем иногда обозначать матрицу подходящего размера с нулевыми элементами.

Следствие. *Матрицы*

$$A = \begin{pmatrix} B_{k\times k} & O \\ O & C_{(n-k)\times(n-k)} \end{pmatrix} \quad \textit{и} \quad A' = \begin{pmatrix} C_{(n-k)\times(n-k)} & O \\ O & B_{k\times k} \end{pmatrix},$$

принадлежащие кольцу $P_{n,n}$, подобны над полем P.

$\square$ Ясно, что матрицы A и A' эквивалентны. Тогда эквивалентны матрицы

$$A(x) = \begin{pmatrix} xE_{k\times k} - B & O \\ O & xE_{(n-k)\times(n-k)} - C \end{pmatrix},$$

$$A'(x) = \begin{pmatrix} xE_{(n-k)\times(n-k)} - C & O \\ O & xE_{k\times k} - B \end{pmatrix}.$$

Поскольку $A(x) = xE_{n\times n} - A$ и $A'(x) = xE_{n\times n} - A'$, то по теореме матрицы A и A' подобны. □

Другое доказательство следствия может быть проведено с использованием результатов главы 15 (см. задачу 13 главы 15).

Заметим, что условие подобия двух матриц над полем является более сильным, чем условие их эквивалентности. Подобные матрицы эквивалентны, так как обратимая матрица над полем является произведением элементарных матриц (следствие 3 теоремы 4 главы 7). В то же время любая невырожденная матрица эквивалентна единичной матрице, а единичная матрица подобна только самой себе.

§ 2. КАНОНИЧЕСКАЯ ФОРМА ПОЛИНОМИАЛЬНОЙ МАТРИЦЫ

Задача об эквивалентности матриц из множества $P[x]_{m,n}$ решается путем выделения в каждом классе эквивалентных матриц некоторой однозначно определенной (канонической) матрицы подобно тому, как это сделано в § 6 главы 6 для матриц над кольцом $\mathbb{Z}$ и в § 2 главы 7 для матриц над полем.

Определение 1. Матрицу $K(x) \in P[x]_{m,n}$ называют *канонической*, если
1) $K(x) = \operatorname{diag}(f_1(x), \ldots, f_t(x))_{m\times n}$, где $t = \min\{m, n\}$ и $f_{i-1}(x) \mid f_i(x)$ при $i \in \overline{2,t}$;
2) каждый ненулевой из многочленов $f_i(x)$ — унитарный.

Из определения 1 следует, что если $f_i(x) = 0$ при некотором $i \in \overline{1,t}$, то $f_j(x) = 0$ при $j \in \overline{i,t}$.

Пример 1. Нулевая матрица и всякая матрица вида

$$\begin{pmatrix} E_{k\times k} & O \\ O & O \end{pmatrix}_{m\times n}$$

являются каноническими, что согласуется с определением канонической матрицы над полем.

Покажем, что всякая матрица из $P[x]_{m,n}$ эквивалентна некоторой канонической матрице (сравните с теоремой 17 главы 6).

Лемма 2. *Если $A(x) = (a_{ij}(x)) \in P[x]_{m,n}$, $a_{11}(x) \neq 0$ и существует элемент $a_{ks}(x)$, не делящийся на $a_{11}(x)$, то матрица $A(x)$ эквивалентна матрице $B(x)$, у которой $b_{11}(x) \neq 0$ и $\deg b_{11}(x) < \deg a_{11}(x)$.*

□ Пусть $k = 1$, и при делении с остатком получаем

$$a_{1s}(x) = a_{11}(x)q(x) + r(x), \quad 0 \leqslant \deg r(x) < \deg a_{11}(x).$$

Прибавляя к s-му столбцу матрицы $A(x)$ 1-й столбец, умноженный на $-q(x)$, получим матрицу $A'(x)$, у которой $a'_{1s}(x) = r(x)$. Для получения нужной матрицы $B(x)$ достаточно переставить 1-й и s-й столбцы матрицы $A'(x)$.

Если $k \neq 1$, но $s = 1$, то проделаем аналогичные элементарные преобразования со строками матрицы $A(x)$.

Пусть теперь все элементы первой строки и первого столбца матрицы $A(x)$ делятся на $a_{11}(x)$. Тогда $a_{k1}(x) = a_{11}(x)q_{k1}(x)$, $k \in \overline{2,m}$. Прибавим к k-й строке матрицы $A(x)$ 1-ю строку, умноженную на $-q_{k1}(x)$, а затем k-ю строку полученной матрицы прибавим к ее 1-й строке. Получим матрицу $A'(x) = (a'_{ij}(x))$, у которой $a'_{11}(x) = a_{11}(x)$ и элемент $a'_{1s}(x) = a_{ks}(x) + (e - q_{k1}(x))a_{1s}(x)$ не делится на $a'_{11}(x)$, e — единица поля P. Следовательно, рассматриваемый случай сведен к случаю, когда $k = 1$. □

Теорема 3. *Любая матрица $A(x) \in P[x]_{m,n}$ эквивалентна некоторой канонической матрице.*

□ Если $A(x) = O_{m\times n}$, то $A(x)$ — каноническая матрица. Для матрицы $A(x) \neq O_{m\times n}$ доказательство проведем индукцией по числу $m + n$.

Если $m + n = 2$, то $A(x) = a_{11}(x)$ и $A(x) \sim B(x) = a^*_{11}(x)$, где $a^*_{11}(x)$ — ассоциированный с $a_{11}(x)$ унитарный многочлен. Значит, $B(x)$ — нужная каноническая матрица.

Пусть $f \in \mathbb{N}$ и утверждение теоремы верно для любой матрицы с условием $m+n < f$. Покажем, что тогда оно верно и для любой матрицы с условием $m+n = f$.

Итак, пусть $A(x) \in P[x]_{m,n}$, $m + n = f$, $A(x) \neq O_{m\times n}$. Ясно, что матрица $A(x)$ эквивалентна матрице $B(x) = (b_{ij}(x))$, у которой $b_{11}(x) \neq 0$. Если $b_{11}(x) \nmid b_{ks}(x)$ для некоторых k и s, то по лемме 2 матрица $B(x)$ эквивалентна матрице $C^{(1)}(x) = (c^{(1)}_{ij}(x))$, у которой $c^{(1)}_{11}(x) \neq 0$ и $\deg c^{(1)}_{11}(x) < \deg b_{11}(x)$.

Если $c^{(1)}_{11}(x) \nmid c^{(1)}_{ks}(x)$ для некоторых k и s, то аналогично получаем матрицу $C^{(2)}(x) = (c^{(2)}_{ij}(x))$, у которой $c^{(2)}_{11}(x) \neq 0$ и $\deg c^{(2)}_{11}(x) < \deg c^{(1)}_{11}(x)$, и т. д. Получаем последовательность эквивалентных матриц $A(x) \sim B(x) \sim C^{(1)}(x) \sim \ldots \sim C^{(u)}(x)$ таких, что

$$\deg b_{11}(x) > \deg c^{(1)}_{11}(x) > \ldots > \deg c^{(u)}_{11}(x) \geqslant 0. \tag{10}$$

Эта последовательность матриц не может быть бесконечной ввиду неравенств (10), так как убывающая последовательность целых чисел, ограниченная снизу, является конечной.

Стало быть, существует такая матрица $C^{(l)}(x) = (c^{(l)}_{ij}(x))$, эквивалентная матрице $A(x)$, у которой $c^{(l)}_{11}(x) \neq 0$ и $c^{(l)}_{11}(x) \mid c^{(l)}_{ij}(x)$ при всех i и j. Тогда очевидно, что

$$C^{(l)}(x) \sim \begin{pmatrix} c^{(l)^*}_{11}(x) & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & D(x)_{(m-1)\times(n-1)} & \\ 0 & & & \end{pmatrix} = C(x). \tag{11}$$

При этом по теореме 14 главы 6 все элементы $d_{ij}(x)$ матрицы $D(x)$ делятся на $c^{(l)^*}_{11}(x)$ — ассоциированный с $c^{(l)}_{11}(x)$ унитарный многочлен.

По предположению индукции матрица $D(x)$ эквивалентна некоторой канонической матрице $(m-1+n-1<f)$:

$$F(x)=\operatorname{diag}(f_2(x),\dots,f_t(x))_{(m-1)\times(n-1)},\quad t=\min\{m,n\}.$$

При этом вновь по теореме 14 главы 6 $c_{11}^{(l)^*}(x)\mid f_i(x)$, $i\in\overline{2,t}$.

Произведя со строками и столбцами матрицы $C(x)$ те элементарные преобразования, которые приводят матрицу $D(x)$ к виду $F(x)$, получим каноническую матрицу:

$$K(x)=\operatorname{diag}(c_{11}^{(l)^*}(x),\ f_2(x),\dots,f_t(x))_{m\times n},$$

эквивалентную матрице $A(x)$. $\square$

Замечание 1. Доказательства леммы 2 и теоремы 3 позволяют указать последовательность тех элементарных преобразований, посредством которых матрица $K(x)$ получается из матрицы $A(x)$. Действительно, ввиду доказательства леммы 2 известна последовательность элементарных преобразований, переводящих матрицу $A(x)$ в матрицу $C(x)$ из соотношения (11).

Если $D(x)=O_{(m-1)\times(n-1)}$, то $K(x)=\operatorname{diag}(c_{11}^{(l)^*}(x),0,\dots,0)$. Если же $D(x)\neq O_{(m-1)\times(n-1)}$, то к ней применяем такой же процесс, который применялся к матрице $A(x)$. Последовательностью элементарных преобразований приведем матрицу $A(x)$ к виду

$$C_1(x)=\operatorname{Diag}(c_{11}^{(l)^*}(x),\ d_{11}^{(l_1)^*}(x),\ G(x)),$$

где $c_{11}^{(l)^*}(x)\mid d_{11}^{(l_1)^*}(x)$. Если $G(x)\neq O_{(m-2)\times(n-2)}$, то продолжаем дальше аналогично. Ясно, что для более быстрого получения матрицы $K(x)$ на самом первом шаге следует выбирать матрицу $B(x)$ так, чтобы степень многочлена $b_{11}(x)$ была наименьшей среди степеней всех ненулевых многочленов $a_{ij}(x)$.

Основываясь на этих рассуждениях, можно получить алгоритм приведения матрицы из $P[x]_{n,n}$ к каноническому виду.

Пример 2. Приведем к каноническому виду следующую матрицу:

$$A(x)=\begin{pmatrix}x-2&-1&0\\0&x-2&-1\\0&0&x-2\end{pmatrix}\sim\begin{pmatrix}1&x-2&0\\2-x&0&-1\\0&0&x-2\end{pmatrix}\sim\begin{pmatrix}1&x-2&0\\0&(x-2)^2&-1\\0&0&x-2\end{pmatrix}\sim$$

$$\sim\begin{pmatrix}1&0&0\\0&(x-2)^2&-1\\0&0&x-2\end{pmatrix}\sim\begin{pmatrix}1&0&0\\0&1&(x-2)^2\\0&2-x&0\end{pmatrix}\sim\begin{pmatrix}1&0&0\\0&1&(x-2)^2\\0&0&(x-2)^3\end{pmatrix}\sim$$

$$\sim\begin{pmatrix}1&0&0\\0&1&0\\0&0&(x-2)^3\end{pmatrix}=K(x).$$

Теперь покажем, что каждая матрица $A(x) \in P[x]_{m,n}$ эквивалентна единственной канонической матрице (сравните с теоремами 20 главы 6 и 4 главы 7).

Определение 2. Пусть $A(x) \in P[x]_{m,n}$, $t = \min\{m,n\}$ и $k \in \overline{1,t}$. *Инвариантным делителем k-го порядка* матрицы $A(x)$ называют унитарный наибольший общий делитель всех ее ненулевых миноров k-го порядка, если такие существуют, и нуль, если все миноры k-го порядка матрицы $A(x)$ равны нулю (обозначение: $d^{(k)}_{A(x)}(x)$).

По следствию 1 теоремы Лапласа (§ 3 главы 6) каждый минор k-го порядка матрицы $A(x)$ есть линейная комбинация ее миноров $(k-1)$-го порядка. Поэтому справедливо соотношение:

$$d^{(k-1)}_{A(x)}(x) \mid d^{(k)}_{A(x)}(x).$$

Утверждение 4. *Если $A(x), B(x) \in P[x]_{m,n}$, $A(x) \sim B(x)$ и $t = \min\{m,n\}$, то при $k \in \overline{1,t}$ справедливо равенство $d^{(k)}_{A(x)}(x) = d^{(k)}_{B(x)}(x)$.*

□ В силу теоремы 14 главы 6 всякий общий делитель миноров k-го порядка матрицы $A(x)$ является общим делителем миноров k-го порядка матрицы $B(x)$ и наоборот. Отсюда следует доказываемое утверждение. □

Теорема 5. *Для любой матрицы $A(x) \in P[x]_{m,n}$ существует единственная эквивалентная ей каноническая матрица.*

□ Пусть матрица $A(x)$ эквивалентна канонической матрице

$$K(x) = \operatorname{diag}(\delta_1(x), \ldots, \delta_t(x)),\ t = \min\{m,n\}.$$

Ввиду определения 1 и утверждения 4 при $l \in \overline{1,t}$ справедливы равенства

$$d^{(l)}_{A(x)}(x) = d^{(l)}_{K(x)}(x) = \delta_1(x) \cdot \ldots \cdot \delta_l(x).$$

Следовательно,

$$\delta_1(x) = d^{(1)}_{A(x)}(x), \quad \delta_l(x) \cdot d^{(l-1)}_{A(x)}(x) = d^{(l)}_{A(x)}(x), \quad l \in \overline{2,t}. \tag{12}$$

Таким образом, диагональные элементы канонической матрицы, эквивалентной матрице $A(x)$, определены однозначно через инвариантные делители матрицы $A(x)$. □

Определение 3. Каноническую матрицу

$$K(x) = \operatorname{diag}(\delta_1(x), \ldots, \delta_t(x))_{m\times n}, \quad t = \min\{m,n\},$$

эквивалентную матрице $A(x) \in P[x]_{m,n}$, называют *канонической формой матрицы* $A(x)$ и обозначают $K(A(x))$. При этом многочлен $\delta_i(x)$ называют *i-м инвариантным множителем матрицы* $A(x)$ и обозначают $\delta_i(x) = \delta^{(i)}_{A(x)}(x)$.

Теперь мы можем получить критерий эквивалентности полиномиальных матриц (сравните со следствием 3 теоремы 20 главы 6 и теоремой 5 главы 7).

Теорема 6. *Если* $A(x), B(x) \in P[x]_{m,n}$, *то равносильны утверждения*:
(а) $A(x) \sim B(x)$;
(б) $K(A(x)) = K(B(x))$;
(в) $\delta^{(l)}_{A(x)} = \delta^{(l)}_{B(x)}(x)$, $l \in \overline{1,t}$, $t = \min\{m,n\}$;
(г) $d^{(l)}_{A(x)}(x) = d^{(l)}_{B(x)}(x)$, $l \in \overline{1,t}$, $t = \min\{m,n\}$.

□ Импликации (а)⇒(г)⇒(в)⇒(б)⇒(а) последовательно доказываются применением утверждения 4, формул (12), определения 3, теоремы 3 и свойства транзитивности отношения эквивалентности. □

Ввиду теорем 1 и 6 получаем критерии подобия матриц над полем.

Следствие. *Матрицы* $A, B \in P_{n,n}$ *подобны над полем* P *тогда и только тогда, когда для матриц* $A(x) = Ex - A$ *и* $B(x) = Ex - B$ *выполнено любое из условий* (а)–(г) *теоремы* 6.

Пользуясь замечанием 1 и следствием теоремы 6, опишем алгоритм решения задачи о подобии матриц A, $B \in P_{n,n}$ и нахождения решения уравнения подобия $X^{-1}AX = B$.

1. Каждую из характеристических матриц $Ex - A$ и $Ex - B$ приводим элементарными преобразованиями к каноническому виду:

$$L_1(x)(Ex - A)R_1(x) = K_1(x), \quad L_2(x)(Ex - B)R_2(x) = K_2(x). \tag{13}$$

2. Если канонические матрицы $K_1(x)$ и $K_2(x)$ не равны, то матрицы A и B не подобны над полем P.

3. Если $K_1(x) = K_2(x)$, то $A \approx B$. Из равенств (13) получаем

$$L_2(x)^{-1}L_1(x)(Ex - A)R_1(x)R_2(x)^{-1} = Ex - B.$$

Решение уравнения подобия ищем по формуле (9), где

$$R(x) = R_1(x)R_2(x)^{-1}.$$

В качестве важных примеров вычислим канонические формы для некоторых матриц.

Утверждение 7. *Если*

$$A(x) = \operatorname{diag}(f_1(x), \ldots, f_t(x))_{m\times n},$$

где $t = \min\{m,n\}$ *и* $f_i(x)$, $i \in \overline{1,t}$, — *унитарные попарно взаимно простые многочлены, то*

$$K(A(x)) = \operatorname{diag}(e, \ldots, e, f_1(x)\ldots f_t(x)).$$

□ Ясно, что $d^{(t)}_{A(x)}(x) = f_1(x)\dots f_t(x)$. Так как многочлены $f_i(x)$ попарно взаимно простые, то по утверждению 19 главы 9 многочлены $g_i(x) = \prod_{j\neq i} f_j(x)$ взаимно просты в совокупности. Поэтому

$$d^{(t-1)}_{A(x)}(x) = (g_1(x), \dots, g_t(x)) = e.$$

Тогда $d^{(t-2)}_{A(x)}(x) = \dots = d^{(1)}_{A(x)}(x) = e$, и по формулам (12)

$$\delta^{(1)}_{A(x)}(x) = \dots = \delta^{(t-1)}_{A(x)}(x) = e, \quad \delta^{(t)}_{A(x)}(x) = f_1(x)\dots f_t(x). \quad \square$$

Утверждение 8. *Если* $f(x) \in P[x]$ *— унитарный многочлен над полем* P *и* $\deg f(x) = k$, *то*

$$K(Ex - S(f(x))) = \operatorname{diag}(e, \dots, e, f(x))_{k\times k}.$$

□ Пусть $f(x) = x^k - c_{k-1}x^{k-1} - \dots - c_1x - c_0$. Тогда

$$A(x) = Ex - S(f(x)) = \begin{pmatrix} x & 0 & \dots & 0 & -c_0 \\ -e & x & \dots & 0 & -c_1 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & -e & x - c_{k-1} \end{pmatrix}.$$

Так как $M_{A(x)}\left(\begin{smallmatrix} 2 & \dots & k \\ 1 & \dots & k-1 \end{smallmatrix}\right) = (-1)^{k-1}e$, то $d^{(k-1)}_{A(x)}(x) = e$. Поэтому

$$d^{(k-2)}_{A(x)}(x) = \dots = d^{(1)}_{A(x)}(x) = e.$$

По следствию утверждения 39 гл. 15

$$d^{(k)}_{A(x)}(x) = |Ex - S(f(x))| = \chi_{S(f(x))}(x) = f(x).$$

По формулам (12)

$$K(A(x)) = \operatorname{diag}(e, \dots, e, f(x))_{k\times k}. \quad \square$$

§ 3. НОРМАЛЬНЫЕ ФОРМЫ МАТРИЦ НАД ПОЛЕМ

Теперь укажем некоторые матрицы, которым подобна всякая матрица из $P_{n,n}$.

Определение 4. Матрицу над полем P вида

$$N = \operatorname{Diag}(S(f_1(x)), \dots, S(f_t(x)))_{n\times n}, \tag{14}$$

где $f_i(x)$ — унитарный многочлен и $\deg f_i(x) > 0$, $i \in \overline{1,t}$, называют *матрицей в нормальной форме*.

Утверждение 9. *Матрица $A \in P_{n,n}$ подобна матрице N вида* (14) *тогда и только тогда, когда в кольце $P[x]_{n,n}$*

$$Ex - A \sim \operatorname{diag}(e, \ldots, e, f_1(x), \ldots, f_t(x))_{n\times n}.$$

□ По теореме 1 $A \approx N$ тогда и только тогда, когда $Ex - A \sim Ex - N$. По утверждению 8 при $k_i = \deg f_i(x)$ имеем

$$Ex - N = \operatorname{Diag}(E_{k_1\times k_1}x - S(f_1(x)),\ \ldots,\ E_{k_t\times k_t}x - S(f_t(x)))_{n\times n} \sim$$
$$\sim \operatorname{Diag}(\operatorname{diag}(e, \ldots, e, f_1(x)),\ \ldots,\ \operatorname{diag}(e, \ldots, e, f_t(x)))_{n\times n} = D(x).$$

Переставив строки и столбцы в матрице $D(x)$, получим:

$$D(x) \sim \operatorname{diag}(e, \ldots, e, f_1(x), \ldots, f_t(x)).$$

Теперь утверждение следует из транзитивности отношения эквивалентности матриц. □

Определение 5. Матрицу N вида (14) называют *матрицей в 1-й нормальной форме*, если $f_i(x) \mid f_{i+1}(x)$ для $i \in \overline{1, t-1}$.

Замечание 2. Из доказательства утверждения 9 следует, что если в (14) матрица N является матрицей в 1-й нормальной форме, то $K(Ex - N) = \operatorname{diag}(e, \ldots, e, f_1(x), \ldots$ $\ldots, f_t(x))$.

Теорема 10. *Каждая матрица $A \in P_{n,n}$ подобна единственной матрице N в 1-й нормальной форме.*

□ Пусть

$$Ex - A \sim K(Ex - A) = \operatorname{diag}(e, \ldots, e, f_1(x), \ldots, f_t(t)),$$

где $f_i(x)$ — унитарный многочлен, $\deg f_i(x) > 0$, $i \in \overline{1, t}$ и $f_i(x) \mid f_{i+1}(x)$, $i \in \overline{1, t-1}$. По утверждению 9 матрица A подобна матрице (14) в 1-й нормальной форме.

Пусть N, N' — матрицы в 1-й нормальной форме, $A \approx N$ и $A \approx N'$, где матрица N имеет вид (14), а

$$N' = \operatorname{Diag}(S(g_1(x)), \ldots, S(g_l(x))).$$

Тогда по утверждению 9

$$Ex - A \sim \operatorname{diag}(e, \ldots, e, g_1(x), \ldots, g_l(x)) = F(x).$$

Поскольку матрица $F(x)$ каноническая, то по теореме 5 получаем, что она равна $F(x) = K(Ex - A)$, $l = t$ и $g_i(x) = f_i(x)$ при $i \in \overline{1, t}$. □

Определение 6. Матрицу N_1 в 1-й нормальной форме, подобную матрице A, называют *первой нормальной формой матрицы A* и обозначают через $N_1(A)$.

Теперь мы можем показать, что если L_P — конечномерное пространство и $\varphi \in \mathfrak{L}(L_P)$, то пространство L_P либо является циклическим относительно преобразования φ, либо раскладывается в прямую сумму циклических относительно φ подпространств.

Теорема 11. *Если* $\dim L_P = n$ *и* $\varphi \in \mathfrak{L}(L_P)$*, то существуют такие векторы* $\beta_1, \ldots, \beta_t \in L_P$*,* $t \geqslant 1$*, что*

$$L_P = L^{\varphi}(\beta_1) \dotplus \ldots \dotplus L^{\varphi}(\beta_t).$$

□ Пусть $\vec{\alpha}$ — базис пространства L_P и $A = A_{\vec{\alpha}}(\varphi)$. По теореме 10 $A \approx N_1(A) = T^{-1}AT$, где $T \in P^*_{n,n}$. Тогда $\vec{\gamma} = \vec{\alpha}T$ — также базис пространства L_P и

$$A_{\vec{\gamma}}(\varphi) = N_1(A) = \operatorname{Diag}(S(f_1(x)), \ldots, S(f_t(x)))_{n\times n}, \tag{15}$$

где $\deg f_i(x) = k_i > 0$, $i \in \overline{1,t}$.

Из равенства (15) по теореме 36 главы 15 следует, что пространство L_P раскладывается в прямую сумму подпространств

$$L_P = L_{1P} \dotplus \ldots \dotplus L_{tP},$$

инвариантных относительно φ, где $\dim L_{iP} = \deg f_i(x) = k_i$, $i \in \overline{1,t}$. Поэтому базис $\vec{\gamma}$ можно записать в виде

$$\vec{\gamma} = (\gamma_1^{(1)}, \ldots, \gamma_{k_1}^{(1)}, \gamma_1^{(2)}, \ldots, \gamma_{k_2}^{(2)}, \ldots, \gamma_1^{(t)}, \ldots, \gamma_{k_t}^{(t)}),$$

где $L_{iP} = (\gamma_1^{(i)}, \ldots, \gamma_{k_i}^{(i)})_P$. По той же теореме 36 главы 15

$$A_{(\gamma_1^{(i)}, \ldots, \gamma_{k_i}^{(i)})}(\varphi_i) = S(f_i(x)),$$

где $\varphi_i = \varphi\big|_{L_{iP}}$. Тогда по утверждению 39 главы 15 $L_{iP} = L^{\varphi}(\gamma_1^{(i)})$. Остается положить $\beta_i = \gamma_1^{(i)}$, $i \in \overline{1,t}$. □

В § 5 главы 15 был указан способ вычисления минимального многочлена линейного преобразования через минимальные многочлены базисных векторов пространства относительно этого преобразования. Другой способ дает

Теорема 12 (Фробениус).[20] *Если* $A \in P_{n,n}$*, то*

$$m_A(x) = \delta^{(n)}_{Ex-A}(x).$$

□ По теореме 10 $A \approx N_1(A)$, где матрица $N_1(A)$ имеет вид (14) и $f_i(x) \mid f_{i+1}(x)$ при $i \in \overline{1,t-1}$. Так как минимальные многочлены подобных матриц равны, то $m_A(x) = m_{N_1(A)}(x)$. По утверждению 28 главы 15

$$m_{N_1(A)}(x) = [m_{S(f_1(x))}(x), \ldots, m_{S(f_t(x))}(x)].$$

[20] Ф. Г. Фробениус (1848–1917) — немецкий математик.

Отсюда в силу равенств $\chi_{S(f_i(x))}(x) = f_i(x)$ и утверждения 39 главы 15 получаем

$$m_{N_1(A)}(x) = [f_1(x), \ldots, f_t(x)].$$

Поскольку $f_i(x) \mid f_{i+1}(x)$, $i \in \overline{1, t-1}$, то

$$m_A(x) = m_{N_1(A)}(x) = f_t(x). \tag{16}$$

С другой стороны, ввиду замечания 2,

$$K(Ex - N_1(A)) = \operatorname{diag}(e, \ldots, e, f_1(x), \ldots, f_t(x)).$$

По определению 3

$$\delta^{(n)}_{Ex-N_1(A)}(x) = f_t(x).$$

По следствию теоремы 6 $K(Ex - N_1(A)) = K(Ex - A)$. Значит,

$$\delta^{(n)}_{Ex-A}(x) = f_t(x). \tag{17}$$

Из равенств (16) и (17) получаем требуемое равенство

$$m_A(x) = \delta^{(n)}_{Ex-A}(x). \quad \square$$

Определение 7. Матрицу над полем P вида

$$N_2 = \operatorname{Diag}(S(g_1(x)^{k_1}), \ldots, S(g_r(x)^{k_r}))_{n\times n}, \tag{18}$$

где $g_i(x)$ — унитарный неприводимый над полем P многочлен, $i \in \overline{1, r}$, называют *матрицей во 2-й нормальной форме*.

Теорема 13. *Каждая матрица $A \in P_{n,n}$ подобна некоторой матрице N_2 во 2-й нормальной форме.*

$\square$ Пусть каноническое разложение многочлена $\chi_A(x)$ над полем P имеет вид

$$\chi_A(x) = f_1(x)^{k_1} \ldots f_t(x)^{k_t}.$$

По следствию теоремы 45 главы 15 матрица A подобна матрице

$$A' = \operatorname{Diag}(A_1, \ldots, A_t),$$

где $\chi_{A_i}(x) = f_i(x)^{k_i}$, $i \in \overline{1, t}$. По теореме 10 $A_i \approx N_1(A_i)$ и, стало быть,

$$A' \approx \operatorname{Diag}(N_1(A_1), \ldots, N_1(A_t)).$$

Поскольку характеристические многочлены подобных матриц равны, то

$$\chi_{N_1(A_i)}(x) = \chi_{A_i}(x) = f_i(x)^{k_i}, \ i \in \overline{1, t}.$$

Матрица $N_1(A_i)$ имеет вид

$$N_1(A_i) = \operatorname{Diag}(S(g_1^{(i)}(x)), \ldots, S(g_{r_i}^{(i)}(x))),$$

где $\deg g_j^{(i)}(x) > 0$ и $g_j^{(i)}(x)$ — унитарный многочлен, $j \in \overline{1, r_i}$. Так как

$$\chi_{S(g_j^{(i)}(x))}(x) = g_j^{(i)}(x), \quad \chi_{N_1(A_i)}(x) = \prod_{i=1}^{r_i} \chi_{S(g_j^{(i)}(x))}(x) = f_i(x)^{k_i}$$

и $f_i(x)$ — неприводимый над полем P многочлен, то

$$N_1(A_i) = \operatorname{Diag}(S(f_i(x)^{k_{i1}}), \ldots, S(f_i(x)^{k_{ir_i}})),$$

где $k_{i1} + \ldots + k_{ir_i} = k_i$.

Таким образом, $N_1(A_i)$ — матрица во 2-й нормальной форме при $i \in \overline{1,t}$, и, следовательно, $\operatorname{Diag}(N_1(A_1), \ldots, N_1(A_t))$ — матрица во 2-й нормальной форме, подобная матрице A. □

Теорема 13 позволяет уточнить теорему 11.

Теорема 14. *Если* $\dim L_P = n$ *и* $\varphi \in \mathfrak{L}(L_P)$, *то существуют такие векторы* $\beta_1, \ldots, \beta_t \in L_P$, $t \geqslant 1$, *что*

$$L_P = L^{\varphi}(\beta_1) \dotplus \ldots \dotplus L^{\varphi}(\beta_t)$$

и $\chi_{\varphi_i}(x) = g_i(x)^{k_i}$, *где* $\varphi_i = \varphi\big|_{L^{\varphi}(\beta_i)}$ *и* $g_i(x)$ — *неприводимый над полем* P *многочлен*, $i \in \overline{1,t}$.

□ Доказательство этой теоремы аналогично доказательству теоремы 11. Нужно только вместо матрицы $N_1(A)$ взять любую матрицу во 2-й нормальной форме, подобную матрице A. □

В § 6 главы 15 было показано, что матрица $A \in P_{n,n}$ неприводима над полем P, т. е. не подобна над P никакой полураспавшейся матрице, тогда и только тогда, когда $\chi_A(x)$ — неприводимый над полем P многочлен. Ясно, что при этом $\chi_A(x) = m_A(x)$. Рассмотрим вопрос о подобии матрицы A распавшейся матрице.

Определение 8. Матрицу $A \in P_{n,n}$ называют *неразложимой* над полем P, если она не подобна над P никакой распавшейся матрице.

Теорема 15. *Матрица* $A \in P_{n,n}$ *неразложима над полем* P *тогда и только тогда, когда*

$$\chi_A(x) = m_A(x) = g(x)^k, \tag{19}$$

где $g(x)$ — *неприводимый над полем* P *многочлен.*

□ Пусть матрица A неразложима. По теореме 13 $A \approx N_2$, где N_2 — матрица во 2-й нормальной форме. Ввиду неразложимости матрицы A получаем $N_2 = S(g(x)^k)$, где $g(x)$ — неприводимый над полем P многочлен. По следствию утверждения 39 главы 15 $\chi_{N_2}(x) = m_{N_2}(x) = g(x)^k$. Так как у подобных матриц совпадают соответственно характеристические и минимальные многочлены, то справедливо равенство (19).

Обратно, пусть выполнено равенство (19). Предположим, что матрица A разложима:

$$A \approx \operatorname{Diag}(A_1, A_2) = A',$$

где $A_1 \in P_{k\times k}$, $1 \leqslant k < n$. Тогда по утверждению 28 главы 15

$$m_A(x) = m_{A'}(x) = [m_{A_1}(x),\, m_{A_2}(x)], \tag{20}$$

и по утверждению 19 главы 15

$$\chi_A(x) = \chi_{A_1}(x)\,\chi_{A_2}(x), \tag{21}$$

где $\deg \chi_{A_i}(x) \geqslant 1$. Отсюда и из (19) следует, что $g(x) \mid \chi_{A_i}(x)$, $i \in \overline{1,2}$. По теореме 41 главы 15 каждый неприводимый делитель многочлена $\chi_{A_i}(x)$ делит $m_{A_i}(x)$ и, значит, $g(x) \mid m_{A_i}(x)$. Поэтому из равенства

$$[m_{A_1}(x),\, m_{A_2}(x)] = \frac{m_{A_1}(x)\, m_{A_2}(x)}{(m_{A_1}(x), m_{A_2}(x))}$$

и равенств (20) и (21) получаем

$$\deg m_A(x) < \deg(m_{A_1}(x)\, m_{A_2}(x)) = \deg m_{A_1}(x) + \deg m_{A_2}(x) \leqslant$$
$$\leqslant \deg \chi_{A_1}(x) + \deg \chi_{A_2}(x) = \deg \chi_A(x),$$

вопреки условию (19). Полученное противоречие показывает, что матрица A неразложима. □

Рассмотрим теперь вопрос о том, однозначно ли определена матрица во 2-й нормальной форме, подобная матрице $A \in P_{n,n}$.

Теорема 16. *Матрица N_2 во 2-й нормальной форме, подобная матрице $A \in P_{n,n}$, определена однозначно с точностью до перестановки клеток.*

□ Пусть каноническое разложение многочлена $\chi_A(x)$ над полем P имеет вид

$$\chi_A(x) = g(x)^k g_1(x)^{k_1} \ldots g_s(x)^{k_s}.$$

Если N_2, N_2' — матрицы во 2-й нормальной форме, подобные матрице A, то $\chi_A(x) = \chi_{N_2}(x) = \chi_{N_2'}(x)$. Так как характеристический многочлен распавшейся матрицы равен произведению характеристических многочленов ее клеток и для любого унитарного многочлена $f(x) \in P[x]$ верно равенство $\chi_{S(f(x))}(x) = f(x)$, то в матрицах N_2 и N_2' должны быть клетки вида $S(g(x)^a)$, где $a \in \overline{1,k}$.

Выпишем такие клетки:

$$S(g(x)^{a_1}),\ \ldots,\ S(g(x)^{a_i}),$$

входящие в матрицу N_2, считая, что $a_1 \leqslant a_2 \leqslant \ldots \leqslant a_i$, и все такие клетки

$$S(g(x)^{b_1}),\ \ldots,\ S(g(x)^{b_j}),$$

входящие в матрицу N_2', считая, что $b_1 \leqslant b_2 \leqslant \ldots \leqslant b_j$. Ясно, что сумма $a_1 + \ldots + a_i = b_1 + \ldots + b_j = k$.

По следствию теоремы 1 матрица N_2 (а тогда и матрица A) подобна матрице

$$\operatorname{Diag}(S(g(x)^{a_1}), \ldots, S(g(x)^{a_i}),\, A_2) = \operatorname{Diag}(A_1, A_2),$$

а матрица N_2' (а тогда и матрица A) подобна матрице

$$\operatorname{Diag}(S(g(x)^{b_1}), \ldots, S(g(x)^{b_j}),\ B_2) = \operatorname{Diag}(B_1, B_2),$$

где

$$A_1 = \operatorname{Diag}(S(g(x)^{a_1}), \ldots, S(g(x)^{a_i})),$$
$$B_1 = \operatorname{Diag}(S(g(x)^{b_1}), \ldots, S(g(x)^{b_j})).$$

Значит,

$$\operatorname{Diag}(A_1, A_2) \approx \operatorname{Diag}(B_1, B_2).$$

При этом

$$\chi_{A_1}(x) = \chi_{B_1}(x) = g(x)^k,$$
$$\chi_{A_2}(x) = \chi_{B_2}(x) = g_1(x)^{k_1} \ldots g_s(x)^{k_s} = f(x).$$

Так как $(g(x)^k, f(x)) = e$, то по теореме 45 главы 15 $A_1 \approx B_1$.

Поскольку A_1, B_1 — матрицы в 1-й нормальной форме, то в силу теоремы 10 $A_1 = B_1$. Поэтому $i = j$ и $a_s = b_s$ при $s \in \overline{1, i}$. Аналогично рассуждаем, рассматривая клетки $S(g_j(x)^{k_j})$, $j \in \overline{1, s}$.

Таким образом, набор клеток любой матрицы во 2-й нормальной форме, подобной матрице A, определен однозначно. □

Определение 9. Матрицу во 2-й нормальной форме, подобную данной матрице $A \in P_{n,n}$, называют *2-й нормальной формой матрицы* A и обозначают через $N_2(A)$.

В качестве примера вычислим 2-ю нормальную форму сопровождающей матрицы.

Утверждение 17. *Если каноническое разложение унитарного многочлена* $f(x) \in P[x]$ *имеет вид* $f(x) = g_1(x)^{k_1} \ldots g_s(x)^{k_s}$, *то*

$$N_2(S(f(x))) = \operatorname{Diag}(S(g_1(x)^{k_1}), \ldots, S(g_s(x)^{k_s})).$$

□ Ввиду теоремы 16 достаточно доказать, что матрица во 2-й нормальной форме

$$N_2 = \operatorname{Diag}(S(g_1(x)^{k_1}), \ldots, S(g_s(x)^{k_s}))$$

подобна матрице $S(f(x))$. По теореме 1 для этого достаточно показать эквивалентность матриц $Ex - N_2$ и $Ex - S(f(x))$.

По утверждению 8 матрица

$$Ex - N_2 = \operatorname{Diag}(E^{(1)}x - S(g_1(x)^{k_1}),\ \ldots,\ E^{(s)}x - S(g_s(x)^{k_s})),$$

где E, $E^{(1)}$, $\ldots$, $E^{(s)}$ — единичные матрицы соответствующих размеров, эквивалентна матрице

$$\operatorname{diag}(e, \ldots, e, g_1(x)^{k_1}, \ldots, g_s(x)^{k_s}).$$

В силу утверждения 7 последняя матрица эквивалентна канонической матрице $\operatorname{diag}(e, \ldots, e, f(x))$. Значит,

$$K(Ex - N_2) = \operatorname{diag}(e, \ldots, e, f(x)). \tag{22}$$

Одновременно по утверждению 8

$$K(Ex - S(f(x))) = \operatorname{diag}(e, \ldots, e, f(x)). \tag{23}$$

По теореме 6 из равенств (22) и (23) получаем

$$Ex - N_2 \sim Ex - S(f(x)). \quad \square$$

§ 4. ЖОРДАНОВЫ МАТРИЦЫ

Теперь мы рассмотрим важный класс матриц над полем, у которых характеристические многочлены раскладываются над этим полем на линейные множители.

Определение 10. Пусть P — поле и $r \in P$. *Жордановой клеткой* порядка k с корнем r называют матрицу

$$\Im_k(r) = \begin{pmatrix} r & e & & 0 \\ & \ddots & \ddots & \\ & & \ddots & e \\ 0 & & & r \end{pmatrix}_{k \times k.}$$

Утверждение 18. *Каноническая форма характеристической матрицы для жордановой клетки $\Im_k(r)$ имеет вид*

$$K(Ex - \Im_k(r)) = \operatorname{diag}(e, \ldots, e, (x-r)^k)_{k \times k}. \tag{24}$$

В частности,

$$\chi_{\Im_k(r)}(x) = m_{\Im_k(r)}(x) = (x-r)^k. \tag{25}$$

$\square$ Для матрицы $T(x) = Ex - \Im_k(r)$ нетрудно вычислить инвариантные делители:

$$d^{(k-1)}_{T(x)}(x) = \ldots = d^{(1)}_{T(x)}(x) = e,$$
$$d^{(k)}_{T(x)}(x) = \chi_{\Im_k(r)}(x) = (x-r)^k.$$

Отсюда и из формул (12) получаем равенство (24). Из (24) и теоремы 12 следуют равенства (25). $\square$

Следствие. $\Im_k(r) \approx S((x-r)^k)$.

$\square$ По утверждению 8

$$K(Ex - S((x-r)^k)) = \operatorname{diag}(e, \ldots, e, (x-r)^k)_{k \times k}.$$

Ввиду равенства (24) по следствию теоремы 6 матрицы $S((x-r)^k)$ и $\Im_k(r)$ подобны. $\square$

Вычислим степени жордановой клетки.

Утверждение 19. *Если $m \in \mathbb{N}$, то*

$$\Im_k(r)^m = \begin{pmatrix} r^m & C_m^1 r^{m-1} & C_m^2 r^{m-2} & \dots & \dots \\ & r^m & C_m^1 r^{m-1} & \dots & \dots \\ & & \ddots & \ddots & \\ & & & \ddots & C_m^1 r^{m-1} \\ 0 & & & & r^m \end{pmatrix}. \tag{26}$$

□ Ввиду равенства $\Im_k(r) = rE + \Im_k(0)$ и перестановочности матриц rE и $\Im_k(0)$ для вычисления матрицы $\Im_k(r)^m$ можно применить формулу разложения бинома:

$$\Im_k(r)^m = (rE + \Im_k(0))^m = r^m E + C_m^1 r^{m-1}\Im_k(0) + \ldots + \Im_k(0)^m. \tag{27}$$

Непосредственные вычисления показывают, что верны равенства

$$\Im_k(0)^2 = \begin{pmatrix} 0 & 0 & e & \cdots & 0 \\ & \ddots & \ddots & \ddots & \\ & & \ddots & \ddots & e \\ & & & \ddots & 0 \\ 0 & & & & 0 \end{pmatrix}, \ \dots\ , \Im_k(0)^{k-1} = \begin{pmatrix} 0 & 0 & \dots & 0 & e \\ 0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix}, \tag{28}$$

$$\Im_k(0)^k = O_{k\times k}.$$

Из равенств (27) и (28) следует равенство (26). □

Определение 11. Матрицу $\Im \in P_{n,n}$ называют *матрицей в жордановой форме*, или *жордановой матрицей*, если

$$\Im = \operatorname{Diag}(\Im_{k_1}(r_1), \dots, \Im_{k_s}(r_s))_{n\times n}, \tag{29}$$

где $k_1 + \ldots + k_s = n$ и $r_1, \dots, r_s$ — не обязательно различные элементы из P.

Теорема 20. *Матрица $A \in P_{n,n}$ подобна матрице $\Im$ в жордановой форме тогда и только тогда, когда ее характеристический многочлен $\chi_A(x)$ раскладывается над полем P на линейные множители. При выполнении последнего условия матрица $\Im$, подобная матрице A, определена однозначно с точностью до перестановки клеток.*

□ Если $A \approx \Im$, где матрица $\Im$ имеет вид (29), то

$$\chi_A(x) = \chi_{\Im}(x) = \chi_{\Im_{k_1}(r_1)}(x) \dots \chi_{\Im_{k_s}(r_s)}(x) = (x - r_1)^{k_1} \dots (x - r_s)^{k_s}$$

(см. утверждение 18).

Обратно, пусть каноническое разложение многочлена $\chi_A(x)$ над полем P имеет вид

$$\chi_A(x) = (x - r_1)^{t_1} \dots (x - r_u)^{t_u}, \tag{30}$$

$t_1 + \dots + t_u = n$. По теореме 13 матрица A подобна некоторой матрице во 2-й нормальной форме:

$$N_2(A) = \mathrm{Diag}(S(g_1(x)^{l_1}), \dots, S(g_m(x)^{l_m}))_{n\times n},$$

где $g_i(x)$ — унитарный неприводимый над полем P многочлен, $i \in \overline{1,m}$. Так как

$$\chi_A(x) = \chi_{N_2(A)}(x) = g_1(x)^{l_1} \dots g_m(x)^{l_m},$$

то ввиду равенства (30)

$$N_2(A) = \mathrm{Diag}(S((x - r_1)^{k_{11}}), \dots, S((x - r_2)^{k_{21}}), \dots, S((x - r_u)^{k_{ub_u}})).$$

По следствию утверждения 18 $S((x-r_i)^{k_{ij}}) \approx \Im_{k_{ij}}(r_i)$, а тогда матрица $N_2(A)$ подобна матрице в жордановой форме:

$$\Im = \mathrm{Diag}(\Im_{k_{11}}(r_1), \dots, \Im_{k_{21}}(r_2), \dots, \Im_{k_{ub_u}}(r_u)).$$

Этой же матрице подобна и матрица A в силу транзитивности отношения подобия матриц.

Любая другая, подобная матрице A, матрица $\Im_1$ в жордановой форме может отличаться от матрицы $\Im$ только перестановкой клеток в силу теоремы 16. □

Определение 12. Жорданову матрицу $\Im$, подобную данной матрице $A \in P_{n,n}$, называют *жордановой формой матрицы* A и обозначают через $\Im(A)$.

Опишем алгоритм отыскания жордановой формы матрицы $A \in P_{n,n}$, если известно каноническое разложение (30) ее характеристического многочлена над полем P.

1. В пространстве $P^{(n)}$, где $n = t_1 + \dots + t_u$, выберем базис $\vec{\alpha} = (E_1^{\downarrow}, \dots, E_n^{\downarrow})$ и определим преобразование $\varphi \in \mathfrak{L}(P^{(n)})$, положив $A_{\vec{\alpha}}(\varphi) = A$. По следствию теоремы 44 главы 15

$$P^{(n)} = \mathrm{Ker}(\varphi - \widehat{r}_1)^{t_1} \dotplus \dots \dotplus \mathrm{Ker}(\varphi - \widehat{r}_u)^{t_u},$$

где $\dim \mathrm{Ker}(\varphi - \widehat{r}_i)^{t_i} = t_i$.

Базисом подпространства $\mathrm{Ker}(\varphi - \widehat{r}_i)^{t_i}$ является фундаментальная система решений $\vec{\gamma}_i = (C_{i1}^{\downarrow}, \dots, C_{it_i}^{\downarrow})$ системы линейных уравнений

$$(A - r_i E)^{t_i} x^{\downarrow} = 0^{\downarrow}, \quad i \in \overline{1,u}.$$

В базисе $\vec{\gamma} = (\vec{\gamma}_1, \dots, \vec{\gamma}_u)$ пространства $P^{(n)}$ матрица $A_{\vec{\gamma}}(\varphi)$ имеет вид

$$A_{\vec{\gamma}}(\varphi) = \mathrm{Diag}(A_1, \dots, A_u) = C^{-1}AC,$$

где $\chi_{A_i}(x) = (x - r_i)^{t_i}$ и $C = (C_{11}^{\downarrow}, \dots, C_{ut_u}^{\downarrow})$.

2. Элементарными преобразованиями приводим каждую из матриц $Ex - A_i$ к каноническому виду:

$$K(Ex - A_i) = \operatorname{diag}(e, \ldots, e, (x - r_i)^{k_{i1}}, \ldots, (x - r_i)^{k_{ib_i}})_{t_i \times t_i},$$

где $k_{i1} + \ldots + k_{ib_i} = t_i$ и $k_{i1} \leqslant k_{i2} \leqslant \ldots \leqslant k_{ib_i}$, $i \in \overline{1, u}$.

По утверждению 8

$$K(Ex - \operatorname{Diag}(S((x - r_i)^{k_{i1}}), \ldots, S((x - r_i)^{k_{ib_i}})) = \\ = \operatorname{diag}(e, \ldots, e, (x - r_i)^{k_{i1}}, \ldots, (x - r_i)^{k_{ib_i}}).$$

По следствию теоремы 6

$$A_i \approx \operatorname{Diag}(S((x - r_i)^{k_{i1}}), \ldots, S((x - r_i)^{k_{ib_i}})) = S_i = \operatorname{Diag}(S_{i1}, \ldots, S_{ib_i}).$$

Поэтому

$$A_{\vec{\gamma}}(\varphi) \approx \operatorname{Diag}(S((x - r_i)^{k_{11}}), \ldots, S((x - r_u)^{k_{ub_u}})).$$

В силу следствия утверждения 18 и транзитивности отношения подобия матриц

$$A \approx \Im(A) = \operatorname{Diag}(\Im_{k_{11}}(r_1), \ldots, \Im_{k_{ub_u}}(r_u)).$$

Замечание 3. Параметры k_{ij}, r_i матрицы $\Im(A)$ можно найти и из канонической матрицы

$$K(Ex - A) = \operatorname{diag}(\delta^{(1)}_{Ex-A}(x), \ldots, \delta^{(n)}_{Ex-A}(x))_{n \times n}.$$

Для этого нужно выписать каноническое разложение над полем P каждого из инвариантных множителей $\delta^{(i)}_{Ex-A}(x)$:

$$\delta^{(n)}_{Ex-A}(x) = (x - r_1)^{k_{1b_1}} \ldots (x - r_u)^{k_{ub_u}},$$
$$\delta^{(n-1)}_{Ex-A}(x) = (x - r_1)^{k_{1\,b_1 - 1}} \ldots (x - r_u)^{k_{u\,b_u - 1}}$$

и т. д. до первого неединичного инвариантного множителя. Ввиду равенства $K(Ex - A) = K(Ex - \Im(A))$, эти разложения дают параметры матрицы $\Im(A)$. Однако удобнее иметь дело с матрицами меньшего размера, что и сделано в пунктах 1 и 2.

В ряде задач бывает нужно найти не только жорданову форму матрицы A, но и решение уравнения подобия $X^{-1}AX = \Im(A)$.

3. Пользуясь алгоритмом из § 2, решаем все уравнения подобия $X_i^{-1}A_iX_i = S_i$. Если $D_i^{-1}A_iD_i = S_i$ и $D = \operatorname{Diag}(D_1, \ldots, D_u)$, то

$$D^{-1}A_{\vec{\gamma}}(\varphi)D = \operatorname{Diag}(S_{11}, \ldots, S_{ub_u}) = A_{\vec{\delta}}(\varphi), \tag{31}$$

где $\vec{\delta} = \vec{\gamma}D$.

4. Теперь можно найти такую матрицу F, что

$$F^{-1}A_{\vec{\delta}}(\varphi)F = \Im(A) = A_{\vec{\beta}}(\varphi),$$

где $\vec{\beta} = \vec{\delta}F$.

Действительно, ввиду равенств (31) пространство $P^{(n)}$ распалось в прямую сумму циклических относительно преобразования φ подпространств:

$$P^{(n)} = L^{\varphi}(\delta_1) \dotplus \ldots \dotplus L^{\varphi}(\delta_{b_1+\ldots+b_{u-1}+1}).$$

Для нахождения матрицы F нужно найти решения уравнений вида

$$X^{-1}S((x-r)^k)X = \Im_k(r).$$

Пусть $\vec{\mu} = (\delta_j, \varphi(\delta_j), \ldots)$ — базис одного из подпространств $L^{\varphi}(\delta_j)$ и $m_{\delta_j,\varphi}(x) = (x-r)^k$.

Система векторов

$$\vec{\lambda} = ((\varphi - \widehat{r})^{k-1}(\delta_j),\ (\varphi - \widehat{r})^{k-2}(\delta_j),\ \ldots,\ (\varphi - \widehat{r})(\delta_j),\ \delta_j)$$

линейно независима, так как в противном случае нашелся бы многочлен степени меньше k, аннулирующий вектор δ_j. Поэтому $\vec{\lambda}$ — базис подпространства $L^{\varphi}(\delta_j)$. При этом из равенств $(\varphi - \widehat{r})(\lambda_i) = \lambda_{i-1}$, $i \in \overline{2,k}$, $(\varphi - \widehat{r})(\lambda_1) = \theta$ следуют равенства $\varphi(\lambda_i) = \lambda_i r + \lambda_{i-1}$, которые означают, что $A_{\vec{\lambda}}(\overline{\varphi}) = \Im_k(r)$, где $\overline{\varphi} = \varphi\big|_{L^{\varphi}(\delta_j)}$.

Жорданову форму матрицы A можно использовать для нахождения корней характеристического многочлена степени матрицы A.

Утверждение 21. *Если $A \in P_{n,n}$ и*

$$\chi_A(x) = (x-r_1)^{k_1} \ldots (x-r_t)^{k_t}$$

— каноническое разложение многочлена $\chi_A(x)$ над полем P, то при $l \in \mathbb{N}$ многочлен $\chi_{A^l}(x)$ имеет вид

$$\chi_{A^l}(x) = (x-r_1^l)^{k_1} \ldots (x-r_t^l)^{k_t}. \tag{32}$$

□ По теореме 20 существует такая матрица $C \in P_{n,n}$, что $C^{-1}AC = \Im(A)$. Тогда $C^{-1}A^lC = \Im(A)^l$. Из равенств

$$\chi_A(x) = (x-r_1)^{k_1} \ldots (x-r_t)^{k_t} = \chi_{\Im(A)}(x), \quad \chi_{A^l}(x) = \chi_{\Im(A)^l}(x)$$

и того факта, что диагональные элементы матрицы $\Im(A)$ — это корни многочлена $\chi_A(x)$, ввиду равенства (26) получаем требуемое равенство (32). □

Некоторые приложения жордановых матриц будут указаны также в следующем параграфе.

§ 5. СТОХАСТИЧЕСКИЕ МАТРИЦЫ

Рассмотрим класс матриц, имеющих широкое применение в теории вероятностей.

Определение 13. Матрицу $A = (a_{ij})_{n\times m}$ над полем $\mathbb{R}$ действительных чисел называют *неотрицательной* (*положительной*), если все ее элементы неотрицательны (положительны). Пишут: $A \geqslant 0$ ($A > 0$).

Определение 14. Неотрицательную матрицу $S = (s_{ij})_{n\times n}$ называют *стохастической*, если $\sum_{j=1}^{n} s_{ij} = 1$ для $i \in \overline{1,n}$, и *дважды стохастической*, если стохастическими являются матрицы S и S^T.

Пример 3. $E_{n\times n}$ — дважды стохастическая матрица.

Утверждение 22. *Множество стохастических (дважды стохастических) матриц из $\mathbb{R}_{n,n}$ является полугруппой относительно операции умножения матриц.*

Доказательство осуществляется непосредственной проверкой.

Определение 15. Если $A \in P_{n,n}$, где P — поле, $d^{\downarrow} \in P^{(n)}\backslash\{0^{\downarrow}\}$, $r \in P$ и $Ad^{\downarrow} = d^{\downarrow}r$, то говорят, что $d^{\downarrow}$ — *собственный вектор матрицы A, принадлежащий собственному значению r.*

Утверждение 23. *Пусть S — стохастическая матрица из $\mathbb{R}_{n,n}$. Тогда*

(а) *если $\chi_S(r) = 0$, где $r \in \mathbb{C}$, то $|r| \leqslant 1$;*

(б) *вектор $e^{\downarrow} = (1,\dots,1)^T$ является собственным вектором матрицы S, принадлежащим собственному значению* 1.

□ (а) Если $\chi_S(r) = 0$, то для некоторого ненулевого вектора $d^{\downarrow} \in \mathbb{C}^{(n)}$ имеет место равенство $Sd^{\downarrow} = d^{\downarrow}r$. Расписывая это равенство покоординатно, получим

$$\sum_{j=1}^{n} s_{ij}d_j = d_i r, \quad i \in \overline{1,n}.$$

Пусть d_t — наибольшая по модулю координата вектора $d^{\downarrow}$. Тогда $|d_t| \neq 0$, и можем записать соотношения:

$$|r| = \left|\sum_{j=1}^{n} s_{tj}\,\frac{d_j}{d_t}\right| \leqslant \sum_{j=1}^{n} s_{tj}\left|\frac{d_j}{d_t}\right| \leqslant \sum_{j=1}^{n} s_{tj} = 1.$$

(б) Очевидна справедливость равенства $Se^{\downarrow} = e^{\downarrow}\cdot 1$. □

Критерий стохастичности неотрицательной матрицы из $\mathbb{R}_{n,n}$ дает

Утверждение 24. *Если $A \in \mathbb{R}_{n,n}$ и $A \geqslant 0$, то A — стохастическая матрица тогда и только тогда, когда $e^{\downarrow} = (1,\dots,1)^T$ — ее собственный вектор, принадлежащий собственному значению* 1.

□ В одну сторону утверждение уже доказано (см. утверждение 23). Пусть $A \geqslant 0$ и $Ae^{\downarrow} = e^{\downarrow}\cdot 1$. Тогда $\sum_{j=1}^{n} a_{ij} = 1$ при $i \in \overline{1,n}$. По определению 13 A — стохастическая матрица. □

Для дальнейшего изучения стохастических матриц нам понадобится понятие предела последовательности матриц.

Определение 16. Последовательность матриц

$$A_1, A_2, \ldots, A_t, \ldots, \tag{33}$$

где $A_t = (a_{ij}^{(t)}) \in \mathbb{C}_{n,n}$, называют *сходящейся*, если для любых $i, j \in \overline{1,n}$ существует $\lim\limits_{t\to\infty} a_{ij}^{(t)} = a_{ij}$. В таком случае матрицу $A = (a_{ij})$ называют *пределом* последовательности (33) и пишут $A = \lim\limits_{t\to\infty} A_t$.

Лемма 25. *Если* $A = \lim\limits_{t\to\infty} A_t$ *и* $B \in \mathbb{C}_{n,n}$, *то будут справедливы равенства* $\lim\limits_{t\to\infty}(A_tB) = AB$ *и* $\lim\limits_{t\to\infty}(BA_t) = BA$.

□ Пусть $C_k = A_kB = (c_{ij}^{(k)})$, $C = AB = (c_{ij})$ и $b = \max\limits_{i,j}\{|b_{ij}|\}$. Тогда справедливы соотношения:

$$|c_{ij}^{(k)} - c_{ij}| = \left|\sum_{s=1}^{n} a_{is}^{(k)} b_{sj} - \sum_{s=1}^{n} a_{is}b_{sj}\right| \leqslant n \cdot b \cdot \max_{i,j}\left\{\left|a_{is}^{(k)} - a_{is}\right|\right\}.$$

Так как $a_{ij} = \lim\limits_{k\to\infty} a_{ij}^{(k)}$, то $c_{ij} = \lim\limits_{k\to\infty} c_{ij}^{(k)}$. По определению 16 $C = \lim\limits_{k\to\infty} C_k$. Значит, $AB = \lim\limits_{t\to\infty}(A_tB)$.

Аналогично доказывается и равенство $BA = \lim\limits_{t\to\infty}(BA_t)$. □

Следствие. *Если* $B \in \mathbb{C}_{n\times n}$ *и* $|B| \neq 0$, *то предел последовательности* (33) *существует тогда и только тогда, когда существует предел последовательности* A_1B, A_2B, …, A_tB, … (*или последовательности* BA_1, BA_2, …, BA_t, …).

Теперь нас будут интересовать условия, при которых для стохастической матрицы S существует предел последовательности ее степеней S^t, и свойства этого предела.

Определение 17. Стохастическую матрицу называют *регулярной*, если существует $\lim\limits_{t\to\infty} S^t$.

Утверждение 26. *Если* S — *регулярная стохастическая матрица и* $\lim\limits_{t\to\infty} S^t = T$, *то*

(а) T — *стохастическая матрица*;

(б) $\vec{T}_i S = \vec{T}_i$ *и* $ST_j^{\downarrow} = T_j^{\downarrow}$ *при* $i, j \in \overline{1,n}$.

□ (а) Пусть $S^t = (s_{ij}^{(t)})$ и $T = (t_{ij})$. По утверждению 21 S^t — стохастическая матрица при $t \in \mathbb{N}$. Переходя в равенствах

$$s_{i1}^{(t)} + \ldots + s_{in}^{(t)} = 1, \quad i \in \overline{1,n},$$

к пределу при $t \to \infty$, получаем $t_{i1} + \ldots + t_{in} = 1$. Поскольку $s_{ij}^{(t)} \geqslant 0$ и $t_{ij} = \lim\limits_{t\to\infty} s_{ij}^{(t)}$, то $t_{ij} \geqslant 0$. Значит, T — стохастическая матрица.

(б) По лемме 25 справедливы равенства

$$ST = S \cdot \lim_{t\to\infty} S^t = \lim_{t\to\infty} S^{t+1} = \lim_{t\to\infty} S^t = T.$$

Аналогично показываем, что $TS = T$. Из равенств $ST = T = TS$ и следуют равенства (б). □

Получим критерий регулярности стохастической матрицы.

Теорема 27. *Стохастическая матрица S регулярна тогда и только тогда, когда 1 — простой корень многочлена $m_S(x)$, а остальные его корни в $\mathbb{C}$ по модулю меньше единицы.*

□ Так как многочлен $\chi_S(x)$ над полем $\mathbb{C}$ раскладывается на линейные множители, то по теореме 20 существует такая матрица $C \in \mathbb{C}^*_{n,n}$, что

$$C^{-1}SC = \mathrm{Diag}(\Im_{k_1}(r_1), \ldots, \Im_{k_m}(r_m)) = \Im(S).$$

Поскольку $\Im(S)^t = C^{-1}S^tC$, $t \in \mathbb{N}$, то по лемме 25 и ее следствию предел $\lim\limits_{t\to\infty} S^t$ существует тогда и только тогда, когда существует предел $\lim\limits_{t\to\infty} \Im(S)^t$. Ввиду равенства

$$\Im(S)^t = \mathrm{Diag}(\Im_{k_1}(r_1)^t, \ldots, \Im_{k_m}(r_m)^t),$$

предел $\lim\limits_{t\to\infty} \Im(S)^t$ существует тогда и только тогда, когда существует каждый из пределов $\lim\limits_{t\to\infty} \Im_{k_i}(r_i)^t$, $i \in \overline{1,m}$.

Из равенства (26) заключаем следующее.

Если $|r| < 1$, то $\lim\limits_{t\to\infty} \Im_k(r)^t = O_{k\times k}$, так как при $r \neq 0$ для любого $s < t$ справедливы соотношения

$$|\, C_t^s r^{t-s} \,| = \left| \frac{t(t-1)\ldots(t-s+1)}{s!}\, r^{t-s} \right| \leqslant \left| \frac{t}{r} \right|^s \cdot |\, r \,|^t$$

и $\lim\limits_{t\to\infty} |t/r|^s \cdot |r|^t = 0$, а если $r = 0$, то $\lim\limits_{t\to\infty} \Im_k(0)^t = O_{k\times k}$ (см. равенства (28)).

Если $|r| = 1$, но $r \neq 1$, то предела последовательности $\Im_k(r)^t$ не существует. Действительно, соотношения $|r^t - r^{t-1}| = |r^{t-1}| \cdot |r-1| = |r-1| > 0$ показывают, что в этом случае не существует предела последовательности r^t — диагональных элементов матриц $\Im_k(r)^t$.

Наконец, если $r = 1$, то ввиду равенства (26)

$$\Im_k(1)^t = \begin{pmatrix} 1 & C_t^1 & \ldots & \ldots \\ & \ddots & \ddots & \\ & & \ddots & C_t^1 \\ 0 & & & 1 \end{pmatrix}_{k\times k}$$

и предел последовательности $\Im_k(1)^t$ существует тогда и только тогда, когда $k = 1$, так как $C_t^1 = t$.

Итак, предел $\lim\limits_{t\to\infty} S^t$ существует тогда и только тогда, когда в матрице $\Im(S)$ нет клеток с корнями, по модулю равными единице и отличными от единицы, а клетки с корнем, равным единице, имеют первый порядок.

Набор жордановых клеток в матрице $\Im(S)$ определяется каноническими разложениями над полем $\mathbb{C}$ инвариантных множителей $\delta^{(i)}(x)$ в матрице

$$K(Ex-S)=\operatorname{diag}(\delta^{(1)}(x),\dots,\delta^{(n)}(x))_{n\times n}.$$

Так как $\delta^{(i)}(x)\mid\delta^{(i+1)}(x)$, и по теореме 12 $\delta^{(n)}(x)=m_S(x)$, то указанное выше условие существования предела $\lim\limits_{t\to\infty} S^t$ равносильно тому, что многочлен $m_S(x)$ имеет единицу простым корнем и не имеет других корней, по модулю равных единице. □

Рассмотрим свойства предельной матрицы для последовательности степеней регулярной стохастической матрицы.

Утверждение 28. *Если S — регулярная стохастическая матрица и $T=\lim\limits_{t\to\infty} S^t$, то справедливы свойства*:

(а) *ранг матрицы T равен кратности корня 1 многочлена $\chi_S(x)$*;

(б) *все строки матрицы T равны тогда и только тогда, когда 1 — простой корень многочлена $\chi_S(x)$.*

□ (а) По теореме 27 жорданова форма матрицы S над полем $\mathbb{C}$ имеет вид

$$\Im(S)=\operatorname{Diag}(\underbrace{1,\dots,1}_{k},\Im_{k_1}(r_1),\dots,\Im_{k_m}(r_m)),$$

где k — кратность корня 1 многочлена $\chi_S(x)$ и $|r_i|<1$ при $i\in\overline{1,m}$. Тогда

$$I=\lim_{t\to\infty}\Im(S)^t=\begin{pmatrix} E_{k\times k} & O\\ O & O\end{pmatrix}$$

и $\operatorname{rang} I=k$. Поскольку $S=C\Im(S)C^{-1}$ для некоторой обратимой матрицы C, то по лемме 25 $T=CIC^{-1}$ и, стало быть, $\operatorname{rang} T=\operatorname{rang} I=k$.

(б) Если 1 — простой корень многочлена $\chi_S(x)$, то любой собственный вектор матрицы S, принадлежащий собственному значению 1, пропорционален вектору $e^{\downarrow}=(1,\dots,1)^T$ (см. задачу 16 главы 15). По утверждению 26 все столбцы матрицы T пропорциональны вектору $e^{\downarrow}$. Значит, все строки матрицы T равны.

Обратно, если $\vec{T_i}=\vec{T_j}$ при $i,j\in\overline{1,n}$, то $\operatorname{rang} T=1$, и по свойству (а) 1 — простой корень многочлена $\chi_S(x)$. □

Из утверждений 26 и 28 получаем способ вычисления матрицы T в случае, когда 1 — простой корень многочлена $\chi_S(x)$. Для этого достаточно найти одно ненулевое решение $\vec{q}=(q_1,\dots,q_n)$ системы уравнений $\vec{x}(S-E)=\vec{0}$. Тогда каждая строка матрицы T имеет вид $\dfrac{1}{u}(q_1,\dots,q_n)$, где $u=q_1+\ldots+q_n$ (проверьте).

Докажем регулярность положительной стохастической матрицы.

Теорема 29. *Положительная стохастическая матрица $S\in\mathbb{R}_{n\times n}$ регулярна, и в матрице $T=\lim\limits_{t\to\infty} S^t$ все строки равны.*

□ Пусть $d^{\downarrow} = (d_1, \ldots, d_n)^T$ — собственный вектор матрицы S, принадлежащий собственному значению r, где $|r| = 1$:

$$Sd^{\downarrow} = d^{\downarrow} r. \tag{34}$$

Если $|d_t| = \max\limits_i \{|d_i|\}$, то из равенства (34) ввиду условия $S > 0$ получаем:

$$|d_t| = |d_t r| = \left|\sum_{j=1}^{n} s_{tj} d_j\right| \leqslant \sum_{j=1}^{n} |s_{tj} d_j| = \sum_{j=1}^{n} s_{tj} |d_j| \leqslant \sum_{j=1}^{n} s_{tj} |d_t| = |d_t|. \tag{35}$$

Из соотношений (35) получаем равенства:

$$\left|\sum_{j=1}^{n} s_{tj} d_j\right| = \sum_{j=1}^{n} |s_{tj} d_j|, \qquad \sum_{j=1}^{n} s_{tj} |d_j| = \sum_{j=1}^{n} s_{tj} |d_t|. \tag{36}$$

Первое из равенств (36) означает, что совпадают аргументы комплексных чисел $d_1, \ldots, d_n$ ($s_{tj} > 0$). Второе из равенств (36) означает, что $|d_1| = \ldots = |d_n|$ (достаточно вычесть его левую часть из правой).

Таким образом, $d^{\downarrow} = d\,(1, \ldots, 1)^T$, $d \in \mathbb{C} \setminus \{0\}$. Ввиду равенства (34) имеем цепочку равенств:

$$Sd^{\downarrow} = d^{\downarrow} r = Se^{\downarrow} d = e^{\downarrow} d = e^{\downarrow} dr,$$

откуда получаем $r = 1$. Тогда $x - 1 \mid \chi_S(x)$ и $x - 1 \mid m_S(x)$.

Предположим, что 1 — кратный корень многочлена $m_S(x)$. Тогда $(x-1)^2 \mid m_S(x)$. Зададим преобразование φ пространства $\mathbb{R}^{(n)}$, положив $A_{\vec{\alpha}}(\varphi) = S$, где $\vec{\alpha}$ — некоторый базис $\mathbb{R}^{(n)}$. По теореме 33 главы 15 существует такой вектор $b^{\downarrow} \in \mathbb{R}^{(n)}$, что $m_{b^{\downarrow},\varphi}(x) = (x-1)^2$. Тогда вектор $a^{\downarrow} = (E - S)b^{\downarrow}$ отличен от нулевого вектора, и

$$(E - S)a^{\downarrow} = (E - S)^2 b^{\downarrow} = 0^{\downarrow}.$$

Значит, $a^{\downarrow}$ — собственный вектор матрицы S, принадлежащий собственному значению 1. По доказанному выше $a^{\downarrow} = ae^{\downarrow}$, $a \in \mathbb{C} \setminus \{0\}$. Но $a^{\downarrow} \in \mathbb{R}^{(n)}$. Следовательно, $a \in \mathbb{R} \setminus \{0\}$.

Для вектора $f^{\downarrow} = \dfrac{1}{a}\, b^{\downarrow}$ справедливо соотношение

$$(E - S)f^{\downarrow} = e^{\downarrow}, \tag{37}$$

и $f^{\downarrow} \in \mathbb{R}^{(n)} \setminus \{0^{\downarrow}\}$. Из равенства (37) получаем: $\sum_{j=1}^{n} s_{ij} f_j + 1 = f_i$, $i \in \overline{1, n}$. Обозначим $f_l = \min\limits_i \{f_i\}$. Тогда $\sum_{j=1}^{n} s_{lj} f_j + 1 = f_l$. Вычитая из последнего равенства равенство $\sum_{j=1}^{n} s_{lj} f_l = f_l$, получаем равенство $\sum_{j=1}^{n} s_{lj}(f_j - f_l) = -1$, которое невозможно, так как в левой части все слагаемые неотрицательны.

Итак, 1 — простой корень многочлена $m_S(x)$, а остальные его корни в $\mathbb{C}$ по модулю меньше 1. По теореме 27 S — регулярная матрица, и все строки матрицы T равны по утверждению 28. □

Следствие. *Если стохастическая матрица $S \in \mathbb{R}_{n,n}$ такова, что для некоторого $l \in \mathbb{N}$ матрица S^l положительна, то S — регулярная матрица, и в матрице $Q = \lim\limits_{t\to\infty} S^t$ все строки равны.*

□ Пусть $r_1, \ldots, r_n$ — все корни (с учетом кратностей) многочлена $\chi_S(x)$ в поле $\mathbb{C}$. По утверждению 21 $r_1^l, \ldots, r_n^l$ — все корни многочлена $\chi_{S^l}(x)$ с учетом их кратностей. По теореме среди чисел r_i^l одно равно по модулю единице, а остальные по модулю строго меньше единицы. Но тогда все числа r_i, за исключением одного, по модулю строго меньше единицы, а одно — равно единице, так как $\chi_S(1) = 0$. Следовательно, 1 — простой корень многочлена $\chi_S(x)$, и S — регулярная матрица. □

ЗАДАЧИ

1. Покажите, что матрица $A \in P_{n,n}$ подобна транспонированной матрице A^T.

2. Пусть P — подполе поля F и $A, B \in P_{n,n}$. Покажите, что матрицы A и B подобны над полем P тогда и только тогда, когда они подобны над полем F.

3. Покажите, что матрица $A(x) \in P[x]_{n,n}$ обратима тогда и только тогда, когда она является произведением элементарных матриц.

4. Для матрицы $C(x) = \begin{pmatrix} a(x) & 0 \\ 0 & b(x) \end{pmatrix}$, где $(a(x), b(x)) = e$, укажите последовательность элементарных преобразований, приводящих ее к каноническому виду.

5. Найдите жорданову форму квадрата жордановой клетки $\Im_k(r)$, рассмотрев случаи $r = 0$ и $r \neq 0$.

6. Выясните, является ли стохастическая матрица S регулярной и, если да, найдите предел $\lim\limits_{t\to\infty} S^t$.

а) $S = \frac{1}{6}\begin{pmatrix} 3 & 0 & 3 & 0 \\ 0 & 2 & 2 & 2 \\ 3 & 0 & 0 & 3 \\ 0 & 2 & 2 & 2 \end{pmatrix}$, б) $S = \frac{1}{6}\begin{pmatrix} 0 & 3 & 0 & 3 \\ 2 & 0 & 2 & 2 \\ 0 & 3 & 0 & 3 \\ 2 & 0 & 2 & 2 \end{pmatrix}$, в) $S = \frac{1}{6}\begin{pmatrix} 3 & 3 & 0 \\ 3 & 3 & 0 \\ 2 & 2 & 2 \end{pmatrix}$,

г) $S = \frac{1}{12}\begin{pmatrix} 4 & 4 & 4 & 0 \\ 4 & 4 & 4 & 0 \\ 3 & 3 & 6 & 0 \\ 3 & 3 & 3 & 3 \end{pmatrix}$, д) $S = \frac{1}{4}\begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$.

7. Докажите, что если $S \in \mathbb{R}_{n,n}$ — такая дважды стохастическая матрица, что $S^l > 0$ для некоторого $l \in \mathbb{N}$, то

$$\lim_{t\to\infty} S^t = \frac{1}{n}\begin{pmatrix} 1 & \ldots & 1 \\ \ldots & \ldots & \ldots \\ 1 & \ldots & 1 \end{pmatrix}.$$

Глава 17

ЕВКЛИДОВЫ ПРОСТРАНСТВА

В этой главе для произвольного конечномерного пространства над полем действительных или комплексных чисел вводится ряд геометрических понятий и получаются результаты, обобщающие известные уже читателю из курса аналитической геометрии многочисленные теоремы об углах и расстояниях между векторами, прямыми и плоскостями в декартовом пространстве.

§ 1. ЕВКЛИДОВО ВЕЩЕСТВЕННОЕ ПРОСТРАНСТВО

Определение 1. *Симметричной билинейной функцией* на векторном пространстве L_P над произвольным полем P называется любая функция $\Phi\colon L \times L \to P$ такая, что для всех $c \in P$ и $\alpha, \beta, \gamma \in L$ выполняются соотношения:

1. $\Phi(\alpha c, \beta) = c\Phi(\alpha, \beta)$,
2. $\Phi(\alpha + \beta, \gamma) = \Phi(\alpha, \gamma) + \Phi(\beta, \gamma)$,

} свойства линейности по первому аргументу

3. $\Phi(\alpha, \beta) = \Phi(\beta, \alpha)$ — свойство симметричности.

Очевидно, что ввиду условия 3 из условий 1, 2 следует также свойство линейности функции Φ по второму аргументу:

4. $\Phi(\alpha, \beta c) = c\Phi(\alpha, \beta)$,
5. $\Phi(\gamma, \alpha + \beta) = \Phi(\gamma, \alpha) + \Phi(\gamma, \beta)$.

Из определения симметричной билинейной функции Φ легко выводится также следующее свойство:

$$\forall\, \alpha \in L\colon\ \Phi(\alpha, \theta) = \Phi(\theta, \alpha) = 0.$$

Понятие симметричной билинейной функции на конечномерном пространстве тесно связано со следующим понятием.

Определение 2. Матрица $A \in P_{n,n}$ называется *симметричной*, если $A^T = A$.

Пример 1. Пусть L_P — пространство с базисом $e_1, \ldots, e_n$ и $A \in P_{n,n}$ — симметричная матрица. Тогда функция $\Phi\colon L \times L \to P$, которая на произвольных векторах $\alpha = \sum\limits_{i=1}^{n} e_i a_i$ и $\beta = \sum\limits_{i=1}^{n} e_i b_i$ принимает значение

$$\Phi(\alpha, \beta) = (a_1, \ldots, a_n)\, A \begin{pmatrix} b_1 \\ \cdots \\ b_n \end{pmatrix},$$

есть симметричная билинейная функция на L_P (докажите).

Мы будем изучать симметричные билинейные функции на пространстве $L_{\mathbb{R}}$ над полем действительных чисел $\mathbb{R}$ следующего специального типа.

Определение 3. Симметричная билинейная функция S на пространстве $L_{\mathbb{R}}$ называется *скалярным произведением*, если

$$\forall\, \alpha \in L \setminus \{\theta\}:\ \ S(\alpha, \alpha) > 0.$$

Очевидно, что изучаемые в аналитической геометрии скалярные произведения на декартовой плоскости и в трехмерном пространстве удовлетворяют определению 3. Приведем еще два примера.

Пример 2. Пусть $(e_1, \ldots, e_n)$ — базис $L_{\mathbb{R}}$ и функция $S\colon L \times L \to \mathbb{R}$ такова, что для любых $\alpha = \sum e_i a_i$ и $\beta = \sum e_i b_i$ из L

$$S(\alpha, \beta) = a_1 b_1 + a_2 b_2 + \ldots + a_n b_n.$$

Тогда S — скалярное произведение на $L_{\mathbb{R}}$ (проверьте). Обратите внимание на то, что функция S совпадает с функцией Φ из примера 1 при $P = \mathbb{R}$ и $A = E$.

Пример 3. Пусть $L = C[a, b]$ — пространство всех функций со значениями в $\mathbb{R}$, заданных и непрерывных на отрезке $[a, b]$. Тогда функция S, определенная условием

$$\forall\, \alpha(x), \beta(x) \in C[a, b]:\ \ S(\alpha(x), \beta(x)) = \int\limits_a^b \alpha(x)\beta(x)\, dx,$$

есть скалярное произведение на $L_{\mathbb{R}}$ (докажите).

Определение 4. Векторное пространство $L_{\mathbb{R}}$ с заданным на нем скалярным произведением S называется *евклидовым вещественным пространством* и обозначается через $(L_{\mathbb{R}}, S)$.

Поскольку всюду далее в §§ 1–5 этой главы изучаются лишь вещественные евклидовы пространства, то они для краткости называются просто *евклидовыми пространствами*. При этом обозначение $L_{\mathbb{R}}$ будет постоянно напоминать читателю, что рассматриваются пространства лишь над полем $\mathbb{R}$ вещественных чисел.

Наличие скалярного произведения позволяет ввести в любом (даже бесконечномерном) евклидовом пространстве геометрическую терминологию.

Определение 5. *Нормой* (или *длиной*) вектора α евклидова пространства $(L_{\mathbb{R}}, S)$ называется неотрицательное число $\|\alpha\| = \sqrt{S(\alpha, \alpha)}$.

Введенное понятие обладает основными известными из геометрии свойствами длины вектора, а именно, для любых $\alpha, \beta \in L$ и $c \in P$

$$\|\alpha\| \geqslant 0 \quad \text{и} \quad (\|\alpha\| = 0 \ \Leftrightarrow\ \alpha = \theta), \tag{1}$$

$$\|\alpha c\| = \|\alpha\| \cdot |c|, \tag{2}$$

$$\|\alpha + \beta\| \leqslant \|\alpha\| + \|\beta\|. \tag{3}$$

Последнее соотношение называется *неравенством треугольника*. Свойства (1), (2) очевидны, а доказательство свойства (3) основано на следующей теореме.

Теорема 1 (неравенство Коши–Буняковского).[21] *Для любых векторов α, β евклидова пространства $(L_{\mathbb{R}}, S)$ справедливо неравенство*

$$\|\alpha\| \cdot \|\beta\| \geqslant |S(\alpha, \beta)|.$$

$\square$ Если $\alpha = \theta$, то утверждение очевидно. Пусть $\alpha \neq \theta$. По определению 3 для любого $a \in \mathbb{R}$ справедливо неравенство $S(\alpha a + \beta, \alpha a + \beta) \geqslant 0$, которое в силу свойств 1–5 симметричной билинейной функции S равносильно неравенству

$$S(\alpha, \alpha)a^2 + 2S(\alpha, \beta)a + S(\beta, \beta) \geqslant 0.$$

Полагая здесь $a = -\dfrac{S(\alpha, \beta)}{S(\alpha, \alpha)}$ (отметим, что $S(\alpha, \alpha) \neq 0$), получаем эквивалентное утверждению теоремы неравенство

$$S(\beta, \beta) - \frac{S(\alpha, \beta)^2}{S(\alpha, \alpha)} \geqslant 0. \quad \square$$

Следствие. *Для любых векторов α, β евклидова пространства $(L_{\mathbb{R}}, S)$ верно неравенство* (3).

$$\square\ \|\alpha + \beta\|^2 = \|\alpha\|^2 + \|\beta\|^2 + 2S(\alpha, \beta) \leqslant \|\alpha\|^2 + \|\beta\|^2 + 2\|\alpha\| \cdot \|\beta\| = (\|\alpha\| + \|\beta\|)^2. \ \square$$

Определение 6. *Расстоянием* между векторами α и β евклидова пространства $(L_{\mathbb{R}}, S)$ называется величина $\rho(\alpha, \beta) = \|\alpha - \beta\|$.

Углом между ненулевыми векторами α и β пространства $(L_{\mathbb{R}}, S)$ называется угол $\varphi \in [0, \pi]$, для которого $\cos\varphi = \dfrac{S(\alpha, \beta)}{\|\alpha\| \cdot \|\beta\|}$. Он обозначается символом $(\widehat{\alpha, \beta})$. Векторы α и β называются *ортогональными* (или *S-ортогональными*), если $S(\alpha, \beta) = 0$. В последнем случае пишут также $\alpha \perp \beta$.

Заметим, что корректность определения угла между векторами вытекает из теоремы 1, и при таком его определении, очевидно, справедливы известные из средней школы *теорема косинусов*

$$\|\alpha - \beta\|^2 = \|\alpha\|^2 + \|\beta\|^2 - 2\|\alpha\| \cdot \|\beta\| \cos(\widehat{\alpha, \beta})$$

и *теорема Пифагора*[22]

$$\alpha \perp \beta \ \Leftrightarrow\ \|\alpha - \beta\|^2 = \|\alpha\|^2 + \|\beta\|^2.$$

Замечание 1. Любое подпространство L_1 евклидова пространства $(L_{\mathbb{R}}, S)$ можно рассматривать как евклидово пространство $(L_{1\mathbb{R}}, S_1)$ со скалярным произведением $S_1 \colon L_1 \times L_1 \to \mathbb{R}$, получающимся ограничением функции $S \colon L \times L \to \mathbb{R}$ на подмножество $L_1 \times L_1$. Мы будем писать в этом случае $S_1 = S|_{L_1}$. Таким образом, по определению, $\forall\, \alpha, \beta \in L_1 \colon\ S_1(\alpha, \beta) = S(\alpha, \beta)$. Очевидно, что для любых векторов α, β евклидова пространства $(L_{1\mathbb{R}}, S_1)$ их нормы, расстояние и угол между ними те же, что и в пространстве $(L_{\mathbb{R}}, S)$.

[21] В. Я. Буняковский (1804–1889) — российский математик.

[22] Пифагор (VI век до н. э.) — древнегреческий философ и математик.

§ 2. ОРТОГОНАЛЬНЫЕ СИСТЕМЫ ВЕКТОРОВ, ОРТОГОНАЛИЗАЦИЯ

Определение 7. Система ненулевых векторов $\alpha_1, \ldots, \alpha_k$ евклидова пространства $(L_{\mathbb{R}}, S)$ называется *ортогональной* (или *S-ортогональной*), если $\alpha_i \perp \alpha_j$ для любых $i, j \in \overline{1,k}$ таких, что $i \neq j$.

Преимущества, связанные с использованием ортогональных систем векторов при решении различных задач, показывает

Утверждение 2. *Пусть $\alpha_1, \ldots, \alpha_k$ — ортогональная система ненулевых векторов пространства $(L_{\mathbb{R}}, S)$. Тогда*

(а) *система $\alpha_1, \ldots, \alpha_k$ линейно независима*;

(б) *если $\beta = \alpha_1 a_1 + \ldots + \alpha_k a_k$, то $a_i = \dfrac{S(\beta, \alpha_i)}{S(\alpha_i, \alpha_i)}$ для $i \in \overline{1,k}$.*

□ Утверждение (а) следует из (б) при $\beta = 0$. Утверждение (б) следует из соотношений $S(\beta, \alpha_i) = S(\alpha_i, \alpha_i)a_i$, $S(\alpha_i, \alpha_i) \neq 0$, $i \in \overline{1,k}$. □

Следующий принципиально важный результат дает удобный способ построения ортогонального базиса в любом конечномерном подпространстве евклидова пространства.

Теорема 3. *Для любой линейно независимой системы векторов $\alpha_1, \ldots, \alpha_k$ евклидова пространства $(L_{\mathbb{R}}, S)$ существуют эквивалентные ей ортогональные системы векторов. Одна из таких систем $\beta_1, \ldots, \beta_k$ может быть построена по правилам*:

$$\begin{aligned} &\beta_1 = \alpha_1, \\ &\beta_2 = \alpha_2 - \frac{S(\alpha_2, \beta_1)}{S(\beta_1, \beta_1)}\,\beta_1, \\ &\ldots\ldots\ldots\ldots\ldots \\ &\beta_k = \alpha_k - \frac{S(\alpha_k, \beta_1)}{S(\beta_1, \beta_1)}\,\beta_1 - \ldots - \frac{S(\alpha_k, \beta_{k-1})}{S(\beta_{k-1}, \beta_{k-1})}\,\beta_{k-1}. \end{aligned} \tag{4}$$

□ Индукция по k. При $k = 1$ утверждение очевидно. Пусть $m > 1$ и теорема верна для любой системы, состоящей из $k < m$ векторов. Докажем ее для $k = m$. Так как $k - 1 < m$, то по предположению индукции система векторов $\beta_1, \ldots, \beta_{k-1}$ из (4) есть ортогональная система, эквивалентная системе $\alpha_1, \ldots, \alpha_{k-1}$. Тогда система $\beta_1, \ldots, \beta_{k-1}$ линейно независима и потому не содержит нулевых векторов. Следовательно, $S(\beta_i, \beta_i) \neq 0$ для $i \in \overline{1, k-1}$, и вектор β_k определен равенствами (4) корректно. Так как для такого вектора β_k при любом $t \in \overline{1, k-1}$ верны равенства $S(\beta_k, \beta_t) = S(\alpha_k, \beta_t) - \dfrac{S(\alpha_k, \beta_t)}{S(\beta_t, \beta_t)}\,S(\beta_t, \beta_t) = 0$, то система $\beta_1, \ldots, \beta_k$ ортогональна. Ее эквивалентность системе $\alpha_1, \ldots, \alpha_k$ следует из (4). □

Определение 8. Процесс построения по формулам (4) ортогональной системы векторов $\beta_1, \ldots, \beta_k$, эквивалентной линейно независимой системе $\alpha_1, \ldots, \alpha_k$, называется *процессом ортогонализации* последней.

Пример 4. В условиях примера 3 построим ортогональную систему многочленов в пространстве $C[-1,1]$, эквивалентную системе $\alpha_1 = 1$, $\alpha_2 = x$, $\alpha_3 = x^2$. По формулам (4) получаем $\beta_1 = 1$. Тогда

$$S(\beta_1,\beta_1) = \int\limits_{-1}^{1} dx = 2, \quad S(\alpha_2,\beta_1) = \int\limits_{-1}^{1} x\,dx = 0 \ \text{ и } \ \beta_2 = \alpha_2 - \frac{0}{2}\,\beta_1 = x.$$

Отсюда

$$S(\beta_2,\beta_2) = \frac{2}{3}, \quad S(\alpha_3,\beta_1) = \frac{2}{3}, \quad S(\alpha_3,\beta_2) = 0$$

и

$$\beta_3 = \alpha_3 - \frac{2}{3\cdot 2}\,\beta_1 - \frac{0\cdot 3}{2}\,\beta_2 = x^2 - \frac{1}{3}\,.$$

Таким образом, искомая система: $\beta_1 = 1$, $\beta_2 = x$, $\beta_3 = x^2 - \frac{1}{3}$.

Замечание 2. В условиях теоремы 3 для любого $l \in \overline{1,k}$ система $\beta_1,\dots,\beta_l$ есть ортогональная система, эквивалентная системе $\alpha_1,\dots,\alpha_l$. При этом, если система $\alpha_1,\dots,\alpha_l$ сама ортогональна, то $\beta_i = \alpha_i$ для $i \in \overline{1,l}$ (проверьте).

Определение 9. В евклидовом пространстве вектор α со свойством $\|\alpha\| = 1$ называется *нормированным* вектором, а ортогональная система нормированных векторов называется *ортонормированной* системой векторов.

Теорема 4. *В конечномерном евклидовом пространстве существует ортонормированный базис. Любую линейно независимую ортогональную* (*ортонормированную*) *систему векторов* $\alpha_1,\dots,\alpha_l$ *этого пространства можно дополнить до его ортогонального* (*ортонормированного*) *базиса.*

□ Если систему $\alpha_1,\dots,\alpha_l$ дополнить до базиса $\alpha_1,\dots,\alpha_l,\dots,\alpha_n$ всего пространства и провести процесс ортогонализации, то по теореме 3 получится ортогональная система $\beta_1,\dots,\beta_n$, эквивалентная базису пространства и потому являющаяся его базисом. При этом, согласно замечанию 2, $\beta_i = \alpha_i$ для $i \in \overline{1,l}$. Ортонормированный базис пространства получается из построенного по формулам

$$e_1 = \frac{1}{\|\beta_1\|}\,\beta_1, \quad \dots, \quad e_n = \frac{1}{\|\beta_n\|}\,\beta_n. \quad \square$$

Из утверждения 2(б) следует, что если $e_1,\dots,e_n$ — ортонормированный базис пространства $(L_{\mathbb{R}},S)$, то координаты в этом базисе произвольного вектора $\alpha = \sum_{i=1}^{n} e_i a_i \in L_{\mathbb{R}}$ могут быть получены по формулам $a_i = S(\alpha,e_i)$, $i \in \overline{1,n}$.

Замечание 3. Пример 2 показывает, что на конечномерном пространстве $L_{\mathbb{R}}$ всегда можно так задать скалярное произведение, что данный его базис $e_1,\dots,e_n$ будет ортонормированным.

§ 3. ОРТОГОНАЛЬНЫЕ ПОДПРОСТРАНСТВА. ОРТОГОНАЛЬНОЕ ДОПОЛНЕНИЕ. РАССТОЯНИЕ МЕЖДУ МНОГООБРАЗИЯМИ

Известные из геометрии определения перпендикулярности прямых и перпендикулярности прямой и плоскости распространяются на многообразия произвольного евклидова пространства следующим образом.

Определение 10. *Подпространства* L_1 и L_2 евклидова пространства $(L_{\mathbb{R}}, S)$ называются *ортогональными*, если для любых $\alpha_1 \in L_1$ и $\alpha_2 \in L_2$ выполняется соотношение $S(\alpha_1, \alpha_2) = 0$. *Многообразия* $\gamma_1 + L_1$ и $\gamma_2 + L_2$ называются *ортогональными*, если ортогональны порождающие их подпространства L_1 и L_2.

Справедливо следующее обобщение известных из курса элементарной геометрии теорем о возможности проведения через данную точку единственного перпендикуляра к данной прямой (на плоскости) или к данной плоскости (в трехмерном пространстве).

Определение 11. *Ортогональным дополнением* к подпространству K евклидова пространства $(L_{\mathbb{R}}, S)$ называется множество

$$K^{\perp} = \{\beta \in L \colon \forall\, \alpha \in K \;\; S(\alpha, \beta) = 0\}.$$

Читателю предлагается самостоятельно убедиться в том, что $K^{\perp}$ — подпространство в $L_{\mathbb{R}}$. Очевидно, что это самое большое из подпространств, ортогональных подпространству K.

Теорема 5. *Конечномерное евклидово пространство $(L_{\mathbb{R}}, S)$ есть прямая сумма любого своего подпространства K и его ортогонального дополнения $K^{\perp}$, т. е.* $L_{\mathbb{R}} = K \dotplus K^{\perp}$.

□ Если $K = \{\theta\}$ или $K = L$, то, соответственно, $K^{\perp} = L$ или $K^{\perp} = \{\theta\}$, и утверждение очевидно. Пусть $\dim L_{\mathbb{R}} = n$ и $\dim K_{\mathbb{R}} = t$, $t \in \overline{1, n-1}$. В силу теорем 3 и 4 в $K_{\mathbb{R}}$ существует ортонормированный базис $e_1, \ldots, e_t$, который можно дополнить до ортонормированного базиса $e_1, \ldots, e_t, \ldots, e_n$ пространства $(L_{\mathbb{R}}, S)$. Пусть $M = (e_{t+1}, \ldots, e_n)_{\mathbb{R}}$. Очевидно, достаточно доказать, что $K^{\perp} = M$.

Нетрудно видеть, что вектор $\alpha \in L_{\mathbb{R}}$ ортогонален любому вектору из подпространства $K = (e_1, \ldots, e_t)_{\mathbb{R}}$ тогда и только тогда, когда

$$S(\alpha, e_i) = 0 \text{ для } i \in \overline{1, t}. \tag{5}$$

Если $\alpha = \sum_{i=1}^{n} e_i a_i$, то $S(\alpha, e_i) = a_i$ для $i \in \overline{1, n}$, поэтому условие (5) равносильно условию $a_1 = \ldots = a_t = 0$, т. е. условию $\alpha \in M$. □

Следствие. *Для любого t-мерного подпространства K евклидова пространства $(L_{\mathbb{R}}, S)$ размерности n существует единственное ортогональное K подпространство M размерности $n - t$: $M = K^{\perp}$.*

□ Очевидно, $M \subset K^\perp$, и так как $\dim M_{\mathbb{R}} = \dim K^\perp_{\mathbb{R}}$, то $M = K^\perp$. □

Например, если K — плоскость в трехмерном евклидовом пространстве, проходящая через точку θ, то $K^\perp$ — единственная перпендикулярная этой плоскости прямая, проходящая через точку θ.

Из теоремы 5 следует, что, каково бы ни было подпространство K евклидова пространства $(L_{\mathbb{R}}, S)$, любой вектор $\alpha \in L$ может быть однозначно представлен в виде

$$\alpha = \beta + \gamma, \quad \beta \in K, \quad \gamma \in K^\perp. \tag{6}$$

Определение 12. Векторы β и γ в равенстве (6) называются соответственно *ортогональной проекцией* α на K и *ортогональной составляющей* α относительно K и обозначаются

$$\beta = \operatorname{пр}_K \alpha, \quad \gamma = \operatorname{пр}_{K^\perp} \alpha.$$

Отметим, что введенные понятия хорошо согласуются с определением угла между векторами, поскольку для любых $\alpha_1, \alpha_2 \in L \setminus \{\theta\}$, если $K = (\alpha_1)_{\mathbb{R}}$, то

$$|\cos(\widehat{\alpha_1, \alpha_2})| = \frac{\|\operatorname{пр}_K(\alpha_2)\|}{\|\alpha_2\|}$$

(проверьте это равенство самостоятельно).

В курсе аналитической геометрии много внимания уделялось вычислению расстояний между основными геометрическими объектами: точками, прямыми и плоскостями. Как уже отмечалось в главе 13, обобщением последних понятий является понятие многообразия в n-мерном пространстве.

Определение 13. *Расстоянием между многообразиями* H_1 и H_2 евклидова пространства $(L_{\mathbb{R}}, S)$ называется величина

$$\rho(H_1, H_2) = \inf\{\|\alpha_1 - \alpha_2\| : \alpha_1 \in H_1, \alpha_2 \in H_2\}.$$

Понятие ортогональной проекции позволяет с единых позиций обобщить многочисленные результаты из аналитической геометрии.

Теорема 6. *Пусть для* $i \in \overline{1,2}$ *многообразие* $H_i = u_i + K_i$ *задается вектором* u_i *и подпространством* K_i *конечномерного евклидова пространства* $(L_{\mathbb{R}}, S)$. *Тогда*

$$\rho(H_1, H_2) = \|\operatorname{пр}_{(K_1+K_2)^\perp}(u_1 - u_2)\|.$$

□ Произвольно выбранные векторы $\alpha_1 \in H_1$, $\alpha_2 \in H_2$ представим в виде $\alpha_i = u_i + \beta_i$, где $\beta_i \in K_i$, $i \in \overline{1,2}$. Верны равенства

$$\begin{aligned}\alpha_1 - \alpha_2 &= u_1 - u_2 + (\beta_1 - \beta_2) = \\ &= \operatorname{пр}_{(K_1+K_2)^\perp}(u_1 - u_2) + \operatorname{пр}_{K_1+K_2}(u_1 - u_2) + \beta_1 - \beta_2.\end{aligned}$$

Рассмотрим векторы

$$v = \operatorname{пр}_{(K_1+K_2)^\perp}(u_1 - u_2), \qquad w = \operatorname{пр}_{K_1+K_2}(u_1 - u_2) + \beta_1 - \beta_2.$$

Заметим, что $v \in (K_1 + K_2)^{\perp}$, $w \in K_1 + K_2$ и $\alpha_1 - \alpha_2 = v + w$. Поэтому

$$\|\alpha_1 - \alpha_2\|^2 = \|v\|^2 + \|w\|^2 \geqslant \|v\|^2.$$

Вектор v не меняется при изменении векторов $\alpha_1 \in H_1$, $\alpha_2 \in H_2$, поскольку векторы u_1, u_2 в доказательстве фиксированы. Остается заметить, что α_1 и α_2 можно выбрать так, что $\|\alpha_1 - \alpha_2\| = \|v\|$. Для этого достаточно подобрать соответствующие векторам α_1 и α_2 векторы $\beta_1 \in K_1$ и $\beta_2 \in K_2$ так, чтобы выполнялось равенство $w = \theta$, т. е. равенство $\beta_2 - \beta_1 = \text{пр}_{K_1+K_2}(u_1 + u_2)$. Последнее можно сделать ввиду условия $\text{пр}_{K_1+K_2}(u_1 + u_2) \in K_1 + K_2$. Теперь очевидно, что

$$\|v\| = \min\{\|\alpha_1 - \alpha_2\| :\ \alpha_1 \in H_1,\ \alpha_2 \in H_2\}. \quad \square$$

§ 4. МАТРИЦА ГРАМА СИСТЕМЫ ВЕКТОРОВ. ОПИСАНИЕ ВСЕХ СКАЛЯРНЫХ ПРОИЗВЕДЕНИЙ

1. Рассмотрим сначала ситуацию, когда L_P — векторное пространство над произвольным полем P и Φ — симметричная билинейная функция на L_P.

Определение 14. *Матрицей Грама*[23] системы векторов $\alpha_1, \ldots, \alpha_k$ пространства L_P относительно функции Φ называется матрица

$$\Gamma_\Phi(\vec{\alpha}) = \Gamma_\Phi(\alpha_1, \ldots, \alpha_k) = \begin{pmatrix} \Phi(\alpha_1, \alpha_1) & \ldots & \Phi(\alpha_1, \alpha_k) \\ \ldots & \ldots & \ldots \\ \Phi(\alpha_k, \alpha_1) & \ldots & \Phi(\alpha_k, \alpha_k) \end{pmatrix}.$$

Очевидно, что матрица $\Gamma_\Phi(\vec{\alpha})$ симметрична ввиду симметричности функции Φ.

Удобства, связанные с использованием матриц Грама при изучении симметричных билинейных функций, основаны на следующих ее свойствах.

Лемма 7. *Для любых* $\alpha_1, \ldots, \alpha_k \in L_P$ *и* $a_1, \ldots, a_k, b_1, \ldots, b_k \in P$ *справедливы равенства*:

$$\Gamma_\Phi(\alpha_1, \ldots, \alpha_k) \cdot \begin{pmatrix} b_1 \\ \cdots \\ b_k \end{pmatrix} = \begin{pmatrix} \Phi\left(\alpha_1, \sum_{i=1}^k \alpha_i b_i\right) \\ \cdots\cdots \\ \Phi\left(\alpha_k, \sum_{i=1}^k \alpha_i b_i\right) \end{pmatrix},$$

$$(a_1, \ldots, a_k) \cdot \Gamma_\Phi(\alpha_1, \ldots, \alpha_k) \cdot \begin{pmatrix} b_1 \\ \cdots \\ b_k \end{pmatrix} = \Phi\Big(\sum_{i=1}^k \alpha_i a_i,\ \sum_{i=1}^k \alpha_i b_i\Big).$$

$\square$ Доказательство легко осуществляется непосредственным перемножением матриц в левых частях выписанных равенств с использованием свойств линейности функции Φ. $\square$

В частности, из леммы следует, что если $\vec{e} = (e_1, \ldots, e_n)$ — базис пространства L_P, то функция Φ однозначно определяется матрицей $\Gamma_\Phi(e_1, \ldots, e_n)$. Действительно,

[23] И. Грам (1850–1916) — датский математик.

если для $\alpha \in L_P$ через $\vec{\alpha}_{\vec{e}}$ обозначить строку координат вектора α в базисе $\vec{e}$, т. е. $\vec{\alpha}_{\vec{e}} = (\alpha_{\vec{e}}^{\downarrow})^T$, то в силу леммы 7 для любых $\alpha, \beta \in L_P$ справедливо равенство

$$\Phi(\alpha, \beta) = \vec{\alpha}_{\vec{e}} \cdot \Gamma_\Phi(e_1, \ldots, e_n) \cdot \beta_{\vec{e}}^{\downarrow}. \tag{7}$$

Наоборот, как уже указывалось в примере 1, для любой симметричной матрицы $A \in P_{n,n}$ функция Φ, определяемая равенством

$$\Phi(\alpha, \beta) = \vec{\alpha}_{\vec{e}} A \beta_{\vec{e}}^{\downarrow},$$

есть симметричная билинейная функция, и при этом $A = \Gamma_\Phi(e_1, \ldots, e_n)$ (докажите). Таким образом, при фиксированном базисе $\vec{e}$ пространства L_P соответствие $\Phi \to \Gamma_\Phi(e_1, \ldots, e_n)$ есть биекция множества всех симметричных билинейных функций на L_P на множество всех симметричных матриц из $P_{n,n}$.

Лемма 8. *Если система векторов $u_1, \ldots, u_k$ выражается через базис $e_1, \ldots, e_n$ пространства L_P по формуле $(u_1, \ldots, u_k) = (e_1, \ldots, e_n)C$, где $C = C_{n \times k}$, то справедливо равенство*

$$\Gamma_\Phi(u_1, \ldots, u_k) = C^T \Gamma_\Phi(e_1, \ldots, e_n) C.$$

□ Заметим, что j-й столбец матрицы C есть $u_{j\vec{e}}^{\downarrow}$, а i-я строка матрицы C^T есть $\vec{u}_{i\vec{e}}$. Теперь из формулы (7) следует, что (i, j)-й элемент матрицы в правой части доказываемого равенства есть $\Phi(u_i, u_j)$. □

2. Теперь изучим специфические свойства матриц Грама систем векторов евклидова пространства $(L_{\mathbb{R}}, S)$ относительно функции S. Прежде всего, очевидно, что система векторов $\alpha_1, \ldots, \alpha_k$ этого пространства ортогональна тогда и только тогда, когда $\Gamma_S(\alpha_1, \ldots, \alpha_k)$ — диагональная матрица, а ортонормированность системы эквивалентна равенству $\Gamma_S(\alpha_1, \ldots, \alpha_k) = E_{k \times k}$. На основании этого замечания можно предложить следующий способ описания всех ортонормированных базисов пространства $(L_{\mathbb{R}}, S)$ по одному базису.

Определение 15. Матрица $C \in \mathbb{R}_{n,n}$ называется *ортогональной*, если она обратима и $C^{-1} = C^T$.

Утверждение 9. *Если $e_1, \ldots, e_n$ — ортонормированный базис евклидова пространства $(L_{\mathbb{R}}, S)$, то система векторов $(u_1, \ldots, u_n) = (e_1, \ldots, e_n)C$ является ортонормированным базисом этого пространства тогда и только тогда, когда C — ортогональная матрица.*

□ По лемме 8 справедливы равенства

$$\Gamma_\Phi(u_1, \ldots, u_n) = C^T \Gamma_\Phi(e_1, \ldots, e_n) C = C^T C.$$

Поэтому условие $\Gamma_\Phi(u_1, \ldots, u_n) = E$ равносильно равенству $C^T = C^{-1}$. □

Утверждение 10. *Система векторов $u_1, \ldots, u_k$ евклидова пространства $(L_{\mathbb{R}}, S)$ линейно зависима тогда и только тогда, когда матрица $\Gamma_S(u_1, \ldots, u_k)$ вырождена. Если система $u_1, \ldots, u_k$ линейно независима, то*

$$|\Gamma_S(u_1, \ldots, u_k)| > 0.$$

□ Если $\sum_{i=1}^{k} u_i b_i = \theta$, то по лемме 7 $\Gamma_S(u_1, \dots, u_k) b^{\downarrow} = 0^{\downarrow}$, где $b^{\downarrow} = (b_1, \dots, b_k)^T$, и при условии $b^{\downarrow} \neq 0^{\downarrow}$ матрица $\Gamma_S(u_1, \dots, u_k)$ вырожденная. Наоборот, если $\Gamma_S(u_1, \dots, u_k)$ — вырожденная матрица, то существует вектор $b^{\downarrow} \in \mathbb{R}^{(k)} \setminus 0^{\downarrow}$ такой, что $\Gamma_S(u_1, \dots, u_k) b^{\downarrow} = 0^{\downarrow}$. Тогда по лемме 7

$$(b_1, \dots, b_k)\, \Gamma_S(u_1, \dots, u_k)\, b^{\downarrow} = S\big(\sum u_i b_i,\, \sum u_i b_i\big) = 0,$$

и так как S — скалярное произведение, то $\sum u_i b_i = \theta$.

Если система $u_1, \dots, u_k$ линейно независима, то по теоремам 3 и 4 в $L_{\mathbb{R}}$ существует эквивалентная ей ортонормированная система векторов $e_1, \dots, e_k$. Пусть $(u_1, \dots, u_k) = (e_1, \dots, e_k)C$. Тогда по лемме 8

$$|\Gamma_S(u_1, \dots, u_k)| = |C^T| \cdot |\Gamma_S(e_1, \dots, e_k)| \cdot |C| = |C|^2 > 0. \quad \square$$

Следствие. *Если $u_1, \dots, u_n$ — произвольный базис евклидова пространства $(L_{\mathbb{R}}, S)$, то столбец координат любого вектора $\alpha \in L_{\mathbb{R}}$ в базисе $\vec{u}$ есть единственное решение системы линейных уравнений*

$$\Gamma_S(u_1, \dots, u_n) x^{\downarrow} = \begin{pmatrix} S(u_1, \alpha) \\ \dots\dots\dots \\ S(u_n, \alpha) \end{pmatrix}.$$

□ По лемме 7 вектор $a^{\downarrow}_{\vec{u}}$ является решением указанной системы, а по утверждению 10 она разрешима однозначно. □

3. Полученные результаты позволяют дать описание всех способов задания скалярного произведения на конечномерном пространстве $L_{\mathbb{R}}$.

Определение 16. *Главным угловым минором порядка $k \in \overline{1,n}$* матрицы $A \in \mathbb{R}_{n,n}$ называется минор $M_A\begin{pmatrix} 1 & \dots & k \\ 1 & \dots & k \end{pmatrix}$.

Теорема 11 (Сильвестр).[24] *Пусть $u_1, \dots, u_n$ — базис пространства $L_{\mathbb{R}}$ и A — симметричная матрица из $\mathbb{R}_{n,n}$. Тогда симметричная билинейная функция S на $L_{\mathbb{R}}$, определяемая условием*

$$\forall\, \alpha, \beta \in L_{\mathbb{R}}: \;\; S(\alpha, \beta) = \vec{\alpha}_{\vec{u}}\, A\, \beta^{\downarrow}_{\vec{u}}, \tag{8}$$

задает на $L_{\mathbb{R}}$ скалярное произведение в том и только в том случае, если все главные угловые миноры матрицы A положительны.

□ Пусть $A = (a_{ij})_{n \times n}$. Тогда для любого $k \in \overline{1,n}$ верно равенство

$$\Gamma_S(u_1, \dots, u_k) = \begin{pmatrix} a_{11} & \dots & a_{1k} \\ \dots & \dots & \dots \\ a_{k1} & \dots & a_{kk} \end{pmatrix}. \tag{9}$$

[24] Д. Д. Сильвестр (1814–1897) — английский математик.

Поэтому если S — скалярное произведение, то по утверждению 10 все главные угловые миноры матрицы A положительны.

Наоборот, пусть все главные угловые миноры матрицы A положительны. Докажем индукцией по n, что в таком случае S — скалярное произведение. При $n = 1$ имеем $A = (a_{11})$, $a_{11} > 0$, и утверждение очевидно.

Пусть $m > 1$ и утверждение верно при всех $n < m$. Докажем его при $n = m$. Рассмотрим подпространство $L' = (u_1, \ldots, u_{n-1})_{\mathbb{R}}$ и на нем — симметричную билинейную функцию $S' = S\big|_{L'}$. Очевидно, что

$$\Gamma_{S'}(u_1, \ldots, u_{n-1}) = \Gamma_S(u_1, \ldots, u_{n-1}),$$

и так как в силу (9) в этой матрице все главные угловые миноры положительны, то по предположению индукции S' — скалярное произведение на $L'_{\mathbb{R}}$. По теореме 4 в евклидовом пространстве $(L'_{\mathbb{R}}, S')$ существует ортонормированный базис $e_1, \ldots, e_{n-1}$. Тогда, так как $S' = S\big|_{L'}$, то

$$\Gamma_S(e_1, \ldots, e_{n-1}) = E_{(n-1)\times(n-1)}. \tag{10}$$

Рассмотрим вектор

$$e_n = u_n - \sum_{i=1}^{n-1} e_i S(u_n, e_i). \tag{11}$$

Легко видеть, что система $e_1, \ldots, e_n$ эквивалентна системе $u_1, \ldots, u_n$, и потому она — базис $L_{\mathbb{R}}$. Из соотношений (10) и (11) нетрудно видеть, что $S(e_n, e_i) = 0$ для $i \in \overline{1, n-1}$, и потому

$$\Gamma_S(e_1, \ldots, e_n) = \operatorname{diag}(1, \ldots, 1, S(e_n, e_n)). \tag{12}$$

Пусть $\vec{e} = \vec{u}C_{n\times n}$. Тогда по лемме 8 $\Gamma_S(\vec{e}) = C^T \Gamma_S(\vec{u}) C$. Так как по условию $|\Gamma_S(\vec{u})| = |A| > 0$, то $|\Gamma_S(\vec{e})| = |C|^2 \cdot |\Gamma_S(\vec{u})| > 0$. Отсюда, ввиду (12), следует неравенство $S(e_n, e_n) > 0$, и для любого вектора $\alpha = \sum_{i=1}^{n} e_i a_i$ из $L_{\mathbb{R}} \setminus \{\theta\}$ верны соотношения

$$S(\alpha, \alpha) = \sum_{i=1}^{n-1} a_i^2 + a_n^2 S(e_n, e_n) > 0. \quad \square$$

§ 5. ИЗОМЕТРИЧНОСТЬ ЕВКЛИДОВЫХ ПРОСТРАНСТВ

Из теоремы 11 видно, что существует бесконечно много различных скалярных произведений на ненулевом конечномерном пространстве $L_{\mathbb{R}}$. Однако, как показывает следующий результат, с алгебраической точки зрения все они «одинаковы».

Теорема 12. *Пусть $(L_{\mathbb{R}}, S)$ и $(M_{\mathbb{R}}, F)$ — евклидовы пространства одной размерности n. Тогда существует изоморфизм $\sigma\colon L_{\mathbb{R}} \to M_{\mathbb{R}}$ со свойством*

$$\forall\, \alpha, \beta \in L_{\mathbb{R}}:\ \ F(\sigma(\alpha), \sigma(\beta)) = S(\alpha, \beta). \tag{13}$$

□ Выберем в пространствах $(L_{\mathbb{R}}, S)$ и $(M_{\mathbb{R}}, F)$ ортонормированные базисы, соответственно, $e_1, \ldots, e_n$ и $u_1, \ldots, u_n$. Зададим отображение σ, положив для вектора $\alpha = \sum_{i=1}^{n} e_i a_i$:

$$\sigma(\alpha) = \sum_{i=1}^{n} u_i a_i.$$

По утверждению 3 главы 15 σ — линейное отображение $L_{\mathbb{R}}$ на $M_{\mathbb{R}}$ и изоморфизм, так как $u_1, \ldots, u_n$ — базис. При этом для любого вектора $\beta = \sum_{i=1}^{n} e_i b_i \in L_{\mathbb{R}}$, как нетрудно увидеть,

$$S(\alpha, \beta) = \sum_{i=1}^{n} a_i b_i = F(\sigma(\alpha), \sigma(\beta)). \quad \square$$

Определение 17. В условиях теоремы 12 изоморфизм σ со свойством (13) называется *изометрией* евклидовых пространств $(L_{\mathbb{R}}, S)$ и $(M_{\mathbb{R}}, F)$.

Таким образом, любые два евклидовых пространства одинаковой размерности *изометричны*. Заметим, что, так как изометрия «сохраняет» скалярное произведение, то она «сохраняет» длину каждого вектора и углы между любыми векторами.

§ 6. ЕВКЛИДОВО КОМПЛЕКСНОЕ (УНИТАРНОЕ) ПРОСТРАНСТВО

На векторном пространстве $L_{\mathbb{C}}$ над полем $\mathbb{C}$ комплексных чисел можно также определить скалярное произведение, с помощью которого можно ввести на $L_{\mathbb{C}}$ и эффективно использовать всю геометрическую терминологию, за исключением понятия угла между векторами. Для этого надо лишь немного изменить определения 1 и 2. Чтобы лучше пояснить смысл вносимых изменений, напомним о разнице в выражениях модуля действительного и комплексного числа через это число:

$$\text{если } z \in \mathbb{R}, \text{ то } |z| = \sqrt{z^2},$$
$$\text{если } z \in \mathbb{C}, \text{ то } |z| = \sqrt{z\overline{z}},$$

где $\overline{z}$ — число, сопряженное к z.

Определение 18. *Эрмитовой*[25] *билинейной функцией* на пространстве $L_{\mathbb{C}}$ называется любая функция $\Phi\colon L \times L \to \mathbb{C}$ такая, что для всех $z \in \mathbb{C}$ и $\alpha, \beta, \gamma \in L$ выполняются соотношения:

1. $\Phi(\alpha z, \beta) = z\Phi(\alpha, \beta)$,
2. $\Phi(\alpha + \beta, \gamma) = \Phi(\alpha, \gamma) + \Phi(\beta, \gamma)$,
3. $\Phi(\alpha, \beta) = \overline{\Phi(\beta, \alpha)}$.

Очевидно, что ввиду 3 из 1 и 2 следуют также свойства:

4. $\Phi(\alpha, \beta z) = \overline{z}\Phi(\alpha, \beta)$,
5. $\Phi(\gamma, \alpha + \beta) = \Phi(\gamma, \alpha) + \Phi(\gamma, \beta)$.

Кроме того, функция Φ обладает, очевидно, свойством

6. $\forall\, \alpha \in L\colon\ \Phi(\alpha, \alpha) \in \mathbb{R}$.

[25] Ш. Эрмит (1822–1901) — французский математик.

Для построения примеров эрмитовых билинейных функций введем

Определение 19. Матрица $A = (a_{ij}) \in \mathbb{C}_{n,n}$ называется *эрмитовой*, если $A^T = \overline{A}$, т. е. $a_{ij} = \overline{a}_{ji}$ для $i, j \in \overline{1,n}$.

Заметим, что любая симметричная матрица над $\mathbb{R}$ является эрмитовой.

Пример 5. Пусть $e_1, \ldots, e_n$ — базис $L_{\mathbb{C}}$ и $A \in \mathbb{C}_{n,n}$ — эрмитова матрица. Тогда функция $\Phi\colon L \times L \to \mathbb{C}$, которая на произвольных векторах $\alpha = \sum e_i a_i$ и $\beta = \sum e_i b_i$ из L принимает значение

$$\Phi(\alpha, \beta) = (a_1, \ldots, a_n) \cdot A \cdot \begin{pmatrix} \overline{b}_1 \\ \cdots \\ \overline{b}_n \end{pmatrix},$$

есть эрмитова билинейная функция на $L_{\mathbb{C}}$ (докажите).

Определение 20. Эрмитова билинейная функция S на пространстве $L_{\mathbb{C}}$ называется *скалярным произведением*, если

$$\forall\, \alpha \in L \setminus \{\theta\}\colon \ S(\alpha, \alpha) > 0$$

(условие $S(\alpha, \alpha) \in \mathbb{R}$ выполнено ввиду свойства 6 эрмитовой билинейной функции).

Пример 6. Пусть $e_1, \ldots, e_n$ — базис $L_{\mathbb{C}}$, и функция $S\colon L \times L \to \mathbb{C}$ такова, что для любых $\alpha = \sum_{i=1}^{n} e_i a_i$, $\beta = \sum_{i=1}^{n} e_i b_i$ из L

$$S(\alpha, \beta) = a_1 \overline{b}_1 + \ldots + a_n \overline{b}_n.$$

Тогда S — скалярное произведение на $L_{\mathbb{C}}$ (докажите это и сравните с примером 2, учитывая замечания перед определением 18).

Определение 21. Векторное пространство $L_{\mathbb{C}}$ с заданным на нем скалярным произведением S называется *евклидовым комплексным* или *унитарным пространством* и обозначается через $(L_{\mathbb{C}}, S)$.

Замечание 4. Дословно так же, как и в евклидовом пространстве, в унитарном пространстве вводятся понятия нормы вектора (определение 5); расстояния между векторами (определение 6); ортогональной и ортонормированной систем векторов (определения 7, 9); ортогональных подпространств; ортогонального дополнения к подпространству и ортогональной проекции вектора на подпространство (определения 10–12); расстояния между многообразиями (определение 13). При этом оказываются справедливыми теоремы 1–6 и утверждение 2, причем их доказательства остаются неизменными за исключением следующих моментов.

1. При доказательстве неравенства Коши—Буняковского (теорема 1) из неравенства $S(\alpha a + \beta, \alpha a + \beta) \geqslant 0$ в рассматриваемой ситуации следует неравенство

$$S(\alpha, \alpha)|a|^2 + S(\alpha, \beta)a + \overline{S(\alpha, \beta)}\,\overline{a} + S(\beta, \beta) \geqslant 0.$$

Поэтому здесь нужно выбирать $a = -\dfrac{\overline{S(\alpha,\beta)}}{S(\alpha,\alpha)}$. Тогда из последнего неравенства следует:

$$S(\beta,\beta) - \frac{|S(\alpha,\beta)|^2}{S(\alpha,\alpha)} \geqslant 0.$$

2. При доказательстве неравенства треугольника (следствие теоремы 1) сначала выводится равенство

$$\|\alpha+\beta\|^2 = \|\alpha\|^2 + \|\beta\|^2 + S(\alpha,\beta) + \overline{S(\alpha,\beta)},$$

а затем используется неравенство $S(\alpha,\beta) + \overline{S(\alpha,\beta)} \leqslant 2|S(\alpha,\beta)|$.

Соответствующие выкладки читателю предлагается провести самостоятельно.

Замечание 5. Понятие угла между векторами α и β в унитарном пространстве не определяется. Определение 6 в этом случае теряет смысл, поскольку $S(\alpha,\beta)$ — число комплексное.

Замечание 6. Матрица Грама произвольной системы векторов $\alpha_1,\dots,\alpha_k$ унитарного пространства $(L_{\mathbb{C}}, S)$ определяется так же, как и в евклидовом вещественном пространстве, равенством

$$\Gamma_S(\alpha_1,\dots,\alpha_k) = (S(\alpha_i,\alpha_j))_{k\times k}.$$

Эта матрица является эрмитовой. Если $e_1,\dots,e_n$ — базис $L_{\mathbb{C}}$, то для любых $\alpha,\beta \in L$ верно равенство

$$S(\alpha,\beta) = \vec{\alpha}_{\vec{e}}\,\Gamma_S(e_1,\dots,e_n)\,\overline{\beta}^{\downarrow}_{\vec{e}},$$

где $\overline{\beta}^{\downarrow}$ — вектор, сопряженный к $\beta^{\downarrow}$.

Определение 22. Матрица $C \in \mathbb{C}_n$ называется *унитарной*, если она обратима и $C^{-1} = \overline{C}^{\,T}$.

В частности, любая ортогональная матрица над $\mathbb{R}$ является унитарной. Аналогом утверждения 9 для унитарного пространства $(L_{\mathbb{C}}, S)$ является

Утверждение 13. *Если $e_1,\dots,e_n$ — ортонормированный базис $(L_{\mathbb{C}}, S)$, то система векторов $(u_1,\dots,u_n) = (e_1,\dots,e_n)C$ является ортонормированным базисом $(L_{\mathbb{C}}, S)$ тогда и только тогда, когда C — унитарная матрица.*

Доказательство аналогично доказательству утверждения 9.

Аналоги утверждения 10 и теоремы 11 (для эрмитовых билинейных форм) читателю предлагается сформулировать и доказать самостоятельно. Теорема 12 и определение 17 переносятся на унитарное пространство дословно.

Замечание 7. Нетрудно видеть, что скалярное произведение S на пространстве $L_{\mathbb{R}}$ формально удовлетворяет всем условиям определений 18 и 20, поскольку $S(\alpha,\beta) \in \mathbb{R}$ для любых $\alpha,\beta \in L_{\mathbb{R}}$, и потому $S(\beta,\alpha) = \overline{S(\beta,\alpha)}$. В связи с этим определения скалярного произведения на $L_{\mathbb{R}}$ и $L_{\mathbb{C}}$ можно сформулировать одновременно следующим образом.

Определение 23. Пусть $\mathbb{P} \in \{\mathbb{R}, \mathbb{C}\}$. Тогда *скалярным произведением* на пространстве $L_{\mathbb{P}}$ называют функцию $S\colon L \times L \to \mathbb{P}$ такую, что для любых $c \in \mathbb{P}$ и $\alpha, \beta, \gamma \in L$ выполняются условия:

1. $S(\alpha c, \beta) = cS(\alpha, \beta)$,
2. $S(\alpha + \beta, \gamma) = S(\alpha, \gamma) + S(\beta, \gamma)$,
3. $S(\alpha, \beta) = \overline{S(\beta, \alpha)}$ (и как следствие $S(\alpha, \alpha) \in \mathbb{R}$),
4. если $\alpha \neq \theta$, то $S(\alpha, \alpha) > 0$.

Конечномерное пространство $L_{\mathbb{P}}$ с заданным на нем скалярным произведением S называют *евклидовым пространством* и обозначают $(L_{\mathbb{P}}, S)$.

Таким образом, мы расширили содержание термина евклидово пространство, включив в него не только евклидовы вещественные пространства (как делали это в §§ 1–5), но и евклидовы комплексные пространства. Введенная терминология оказывается весьма удобной и, как следует из результатов этого параграфа, не противоречит первоначальному узкому толкованию термина «евклидово пространство» в §§ 1–5. Эта терминология будет широко использована в следующей главе.

ЗАДАЧИ

1. Докажите, что

а) для любых чисел $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{R}$ справедливо *неравенство Коши*:

$$\left(\sum_{i=1}^{n} a_i^2\right)\left(\sum_{i=1}^{n} b_i^2\right) \geqslant \left(\sum_{i=1}^{n} a_i b_i\right)^2;$$

б) для любых непрерывных на отрезке $[a, b]$ функций $f(x)$ и $g(x)$ справедливо *неравенство Буняковского*:

$$\int_a^b f(x)^2\,dx \cdot \int_a^b g(x)^2\,dx \geqslant \left(\int_a^b f(x)g(x)\,dx\right)^2.$$

2. Докажите, что для любых векторов α, β евклидова пространства $(L_{\mathbb{R}}, S)$ справедливы следующие утверждения:

а) $\forall\, a \in \mathbb{R}\colon\ \|\alpha a\| = |a| \cdot \|\alpha\|$;

б) $\|\alpha\| - \|\beta\| \leqslant \|\alpha - \beta\| \leqslant \|\alpha\| + \|\beta\|$;

в) $\|\alpha\| \cdot \|\beta\| = |S(\alpha, \beta)| \ \Leftrightarrow\ \dim(\alpha, \beta)_{\mathbb{R}} \leqslant 1$;

г) $\|\alpha + \beta\| = \|\alpha\| + \|\beta\| \ \Leftrightarrow\ \exists\, a \in \mathbb{R}\colon\ (\alpha = \beta a,\ a \geqslant 0)$;

д) $\|\alpha - \beta\| = \|\alpha\| + \|\beta\| \ \Leftrightarrow\ \exists\, a \in \mathbb{R}\colon\ (\alpha = \beta a,\ a \leqslant 0)$;

е) $\|\alpha - \beta\| = \|\alpha\| - \|\beta\| \ \Leftrightarrow\ \exists\, a \in \mathbb{R}\colon\ (\alpha = \beta a,\ a \geqslant 1)$.

3. Докажите, что если $e_1, \ldots, e_n$ — ортонормированный базис евклидова пространства $(L_{\mathbb{P}}, S)$, то для любого вектора $\alpha = \sum_{i=1}^{n} e_i a_i \in L$ верны

а) *равенство Парсеваля*[26]: $\|\alpha\| = \sum_{i=1}^{n} |a_i|^2$,

б) *неравенство Бесселя*[27]: $\forall\, k \in \overline{1, n}\colon\ \|\alpha\| \geqslant \sum_{i=1}^{k} |a_i|^2$.

[26] М. А. Парсеваль (1755–1836) — французский математик.

[27] Ф. В. Бессель (1784–1846) — немецкий математик.

4. Докажите, что в трехмерном декартовом пространстве с обычным скалярным произведением S площадь параллелограмма, стороны которого задаются векторами α_1 и α_2, равна $\sqrt{|\Gamma_S(\alpha_1,\alpha_2)|}$, а объем параллелепипеда со сторонами $\alpha_1,\alpha_2,\alpha_3$ равен $\sqrt{|\Gamma_S(\alpha_1,\alpha_2,\alpha_3)|}$.

5. В условиях предыдущей задачи покажите, что если к системе векторов $\alpha_1,\alpha_2,\alpha_3$ применить процесс ортогонализации, то получившаяся система векторов β_1,β_2,β_3 образует прямоугольный параллелепипед, равновеликий исходному.

6. Пусть $(L_{\mathbb{P}},S)$ — евклидово пространство, K — его подпространство с базисом $u_1,\ldots,u_m$ и α — произвольный вектор из L. Докажите, что если в результате ортогонализации системы векторов $u_1,\ldots,u_m,\alpha$ получается система $\beta_1,\ldots,\beta_m,\beta_{m+1}$, то $\beta_1,\ldots,\beta_m$ — ортогональный базис K, а $\beta_{m+1}=\operatorname{пр}_{K^\perp}\alpha$ — ортогональная составляющая вектора α относительно K.

7. В условиях предыдущей задачи докажите, что ортогональная проекция вектора α на подпространство K имеет вид

$$\operatorname{пр}_K\alpha = u_1c_1+\ldots+u_mc_m,$$

где $(c_1,\ldots,c_m)^T$ — единственное решение системы линейных уравнений

$$\Gamma_S(u_1,\ldots,u_m)\,x^{\downarrow}=\begin{pmatrix} S(\alpha,u_1)\\ \cdots\cdots\\ S(\alpha,u_m)\end{pmatrix}.$$

8. Пусть $\alpha_1,\ldots,\alpha_t$ и $\beta_1,\ldots,\beta_t$ — системы векторов n-мерных евклидовых пространств соответственно $(L_{\mathbb{P}},S)$ и $(K_{\mathbb{P}},F)$. Докажите, что существует изометрия $\varphi\colon L_{\mathbb{P}}\to K_{\mathbb{P}}$ со свойством $\varphi(\alpha_i)=\beta_i$ для $i\in\overline{1,t}$ тогда и только тогда, когда

$$\Gamma_S(\alpha_1,\ldots,\alpha_t)=\Gamma_F(\beta_1,\ldots,\beta_t).$$

9. Докажите, что для произвольного базиса $u_1,\ldots,u_n$ евклидова пространства $(L_{\mathbb{P}},S)$ существует единственная система векторов $v_1,\ldots,v_n$ такая, что

$$S(u_i,v_j)=\begin{cases}1, & \text{если } i=j,\\ 0, & \text{если } i\neq j.\end{cases}$$

При этом $v_1,\ldots,v_n$ — базис $L_{\mathbb{P}}$ (называемый базисом, *сопряженным* к $\vec{u}$). Ясно, что $\vec{u}=\vec{v}$ тогда и только тогда, когда $\vec{u}$ — ортонормированный базис.

10. Пусть K,M — произвольные подпространства конечномерного евклидова пространства $(L_{\mathbb{P}},S)$. Докажите соотношения:

а) $K\subset M \;\Leftrightarrow\; K^\perp\supset M^\perp$,

б) $(K^\perp)^\perp=K$,

в) $(K+M)^\perp=K^\perp\cap M^\perp$,

г) $(K\cap M)^\perp=K^\perp+M^\perp$.

Какие из этих соотношений верны и в бесконечномерном пространстве?

Глава 18

ЛИНЕЙНЫЕ ПРЕОБРАЗОВАНИЯ КОНЕЧНОМЕРНЫХ ЕВКЛИДОВЫХ ПРОСТРАНСТВ

Всюду далее в этой главе $\mathbb{P}$ — поле комплексных или действительных чисел, т. е. $\mathbb{P} \in \{\mathbb{C}, \mathbb{R}\}$, и $(L_{\mathbb{P}}, S)$ — (конечномерное) евклидово пространство со скалярным произведением S, т. е. $(L_{\mathbb{P}}, S)$ — либо евклидово вещественное пространство (при $\mathbb{P} = \mathbb{R}$), либо евклидово комплексное (унитарное) пространство (при $\mathbb{P} = \mathbb{C}$).

Цель этой главы — изучение линейных преобразований пространства $(L_{\mathbb{P}}, S)$, свойства которых определенным образом связаны со свойствами заданного на $L_{\mathbb{P}}$ скалярного произведения S. Получающиеся при этом результаты оказываются не только интересными с теоретической точки зрения, но и весьма полезными в прикладном аспекте. Так, например, будет показано, что любая симметричная матрица над $\mathbb{R}$ подобна диагональной матрице над $\mathbb{R}$, и будут описаны все изометрические отображения пространства $(L_{\mathbb{P}}, S)$ на себя.

§ 1. ПРЕОБРАЗОВАНИЕ, СОПРЯЖЕННОЕ К ДАННОМУ. САМОСОПРЯЖЕННЫЕ И ИЗОМЕТРИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ

Определение 1. Линейное преобразование ψ евклидова пространства $(L_{\mathbb{P}}, S)$ называется *сопряженным к линейному преобразованию* φ этого пространства, если

$$\forall\, \alpha, \beta \in L_{\mathbb{P}}: \;\; S(\varphi(\alpha), \beta) = S(\alpha, \psi(\beta)). \tag{1}$$

Заметим, что отношение сопряженности преобразований симметрично, поскольку при условии (1) верны равенства

$$S(\psi(\alpha), \beta) = \overline{S(\beta, \psi(\alpha))} = \overline{S(\varphi(\beta), \alpha)} = S(\alpha, \varphi(\beta)),$$

т. е. φ — преобразование, сопряженное к ψ.

Пример 1. Пусть K — подпространство в $(L_{\mathbb{P}}, S)$ и φ — ортогональное проектирование L на K:

$$\forall\, \alpha \in L: \;\; \varphi(\alpha) = \mathrm{пр}_K \alpha.$$

Тогда $\varphi \in \mathfrak{L}(L_{\mathbb{P}})$ и сопряженным к φ будет само φ, поскольку для любых $\alpha, \beta \in L$ верны равенства

$$S(\varphi(\alpha), \beta) = S(\mathrm{пр}_K(\alpha),\, \beta) = S(\mathrm{пр}_K(\alpha),\; \mathrm{пр}_K(\beta)) = S(\alpha,\, \mathrm{пр}_K(\beta)) = S(\alpha, \varphi(\beta)).$$

Приведенный пример делает содержательным

Определение 2. Линейное преобразование φ евклидова пространства $(L_{\mathbb{P}}, S)$ называется *самосопряженным*, если оно сопряжено к самому себе.

Укажем еще один важный класс преобразований, для которых легко описываются сопряженные.

Определение 3. Линейное преобразование φ евклидова пространства $(L_{\mathbb{P}}, S)$ называется *изометрическим* или *изометрией*, если

$$\forall\, \alpha, \beta \in L:\ \ S(\varphi(\alpha),\, \varphi(\beta)) = S(\alpha, \beta).$$

Утверждение 1. *Линейное преобразование φ евклидова пространства $(L_{\mathbb{P}}, S)$ является изометрическим тогда и только тогда, когда оно обратимо и сопряжено к преобразованию φ^{-1}.*

□ Если φ — изометрия, то для любого $\alpha \in L \setminus \theta$: $\|\varphi(\alpha)\| = \|\alpha\| > 0$, т. е. $\varphi(\alpha) \neq \theta$ и φ обратимо (проверьте). Тогда для любых $\alpha, \beta \in L$ верны равенства

$$S(\varphi(\alpha), \beta) = S(\varphi(\alpha), \varphi(\varphi^{-1}(\beta))) = S(\alpha, \varphi^{-1}(\beta)),$$

и потому φ^{-1} сопряжено к φ.

Наоборот, если $\varphi \in \mathfrak{L}(L_{\mathbb{P}})^*$ и φ^{-1} сопряжено к φ, то

$$\forall\, \alpha, \beta \in L:\ \ S(\varphi(\alpha), \varphi(\beta)) = S(\alpha, \varphi^{-1}(\varphi(\beta))) = S(\alpha, \beta),$$

т. е. φ — изометрия. □

Пример 2. Пусть $\mathbb{P} = \mathbb{R}$, $L = D^2$ — пространство векторов декартовой плоскости с обычным скалярным произведением и φ — преобразование, осуществляющее поворот любого вектора вокруг начала координат на фиксированный угол ω против часовой стрелки. Тогда, очевидно, φ — изометрия. Сопряженным к φ преобразованием будет поворот на угол $-\omega$.

Приведенные примеры являются наиболее важными с точки зрения теории, которая будет изложена в данной главе.

Прежде всего ответим на вопросы о том, сколько сопряженных преобразований можно построить для данного линейного преобразования и всегда ли они существуют? Соответствующая теорема существования и единственности опирается на следующее полезное в ряде случаев утверждение.

Лемма 2. *Если $e_1, \ldots, e_n$ — произвольный базис евклидова пространства $(L_{\mathbb{P}}, S)$, то преобразования $\varphi, \psi \in \mathfrak{L}(L_{\mathbb{P}})$ сопряжены тогда и только тогда, когда*

$$S(\varphi(e_i), e_j) = S(e_i, \psi(e_j)) \quad \textit{для} \quad i, j \in \overline{1, n}. \tag{2}$$

□ Необходимость равенств (2) для сопряженности преобразований φ и ψ следует из определения 1. Допустим теперь, что они выполнены. Тогда для произвольных векторов $\alpha = \sum_{i=1}^{n} e_i a_i$ и $\beta = \sum_{i=1}^{n} e_i b_i$ из $L_{\mathbb{P}}$ справедливы соотношения

$$S(\varphi(\alpha), \beta) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_i \overline{b}_j S(\varphi(e_i), e_j) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_i \overline{b}_j S(e_i, \psi(e_j)) = S(\alpha, \psi(\beta)).$$

Следовательно, ψ — преобразование, сопряженное к φ. □

Теорема 3. *Если $(e_1, \ldots, e_n) = \vec{e}$ — ортонормированный базис евклидова пространства $(L_{\mathbb{P}}, S)$, то линейные преобразования φ и ψ этого пространства сопряжены тогда и только тогда, когда*

$$A_{\vec{e}}(\psi) = \overline{A_{\vec{e}}(\varphi)}^{\,T}. \tag{3}$$

□ Пусть $A_{\vec{e}}(\varphi) = (a_{ij})_{n\times n}$, $A_{\vec{e}}(\psi) = (b_{ij})_{n\times n}$. Тогда для любых базисных векторов e_i и e_j справедливы равенства

$$\varphi(e_i) = \sum_{t=1}^{n} e_t a_{ti}, \quad \psi(e_j) = \sum_{s=1}^{n} e_s b_{sj}.$$

Отсюда, пользуясь тем, что $\vec{e}$ — ортонормированный базис, получаем равенства

$$S(\psi(e_j), e_i) = \sum_{s=1}^{n} b_{sj} S(e_s, e_i) = b_{ij},$$

$$S(e_j, \varphi(e_i)) = \sum_{t=1}^{n} \overline{a}_{ti} S(e_j, e_t) = \overline{a}_{ji}.$$

В силу леммы 2 сопряженность преобразований φ и ψ эквивалентна системе равенств $b_{ij} = \overline{a}_{ji}$ для $i, j \in \overline{1, n}$, т. е. эквивалентна равенству (3). □

Следствие 1. *Для любого линейного преобразования φ евклидова пространства $(L_{\mathbb{P}}, S)$ существует единственное сопряженное к нему преобразование $\psi \in \mathfrak{L}(L_{\mathbb{P}})$.*

□ Это преобразование однозначно определяется из (3). □

Всюду далее линейное преобразование, сопряженное к данному преобразованию $\varphi \in \mathfrak{L}(L_{\mathbb{P}})$ пространства $(L_{\mathbb{P}}, S)$, обозначается через φ^* (согласно следствию 1 теоремы 3 такое обозначение корректно). Теперь равенство (3) можно переписать следующим образом:

$$A_{\vec{e}}(\varphi^*) = \overline{A_{\vec{e}}(\varphi)}^{\,T}. \tag{4}$$

Замечание 1. Важно помнить, что равенство (4) справедливо лишь в случае, когда $\vec{e}$ — ортонормированный базис пространства $(L_{\mathbb{P}}, S)$. Если $\vec{u}$ — произвольный базис этого пространства, то матрицы $A_{\vec{u}}(\varphi^*)$ и $A_{\vec{u}}(\varphi)$ связаны более сложным соотношением:

$$A_{\vec{u}}(\varphi^*) = \overline{\Gamma_S(\vec{u})^{-1} A_{\vec{u}}(\varphi)^T \Gamma_S(\vec{u})},$$

где $\Gamma_S(\vec{u})$ — матрица Грама базиса $\vec{u}$ (см. § 4 главы 14). Докажите это равенство самостоятельно.

Теорема 3 позволяет следующим образом охарактеризовать самосопряженные и изометрические преобразования.

Напомним, что матрица $A \in \mathbb{P}_{n,n}$ называется *эрмитовой*, если $A = \overline{A}^T$. Очевидно, множество эрмитовых матриц над полем действительных чисел совпадает с множеством симметричных матриц. Матрица $A \in \mathbb{P}_{n,n}$ называется *унитарной*, если $\overline{A}^T = A^{-1}$, и *ортогональной*, если $A^T = A^{-1}$. В случае $\mathbb{P} = \mathbb{R}$ последние два понятия совпадают.

Следствие 2. *Пусть $(L_{\mathbb{P}}, S)$ — евклидово пространство с ортонормированным базисом $(e_1, \ldots, e_n) = \vec{e}$ и $\varphi \in \mathfrak{L}(L_{\mathbb{P}})$. Тогда*

(а) *φ — самосопряженное преобразование в том и только в том случае, если $A_{\vec{e}}(\varphi)$ — эрмитова матрица*;

(б) *φ — изометрическое преобразование в том и только в том случае, если $A_{\vec{e}}(\varphi)$ — унитарная матрица.*

□ Достаточно воспользоваться равенством (4), заметив, что условие самосопряженности преобразования φ записывается равенством $\varphi^* = \varphi$, а условие его изометричности — равенством $\varphi^* = \varphi^{-1}$ (см. утверждение 1). □

В связи с результатами последнего утверждения при изучении изометрических преобразований употребляется следующая терминология.

Определение 4. Изометрическое преобразование евклидова вещественного пространства называется *ортогональным*, а изометрическое преобразование унитарного пространства называется *унитарным*.

Мы, однако, будем чаще пользоваться общим термином — *изометрическое преобразование*.

В заключение этого параграфа отметим следующие свойства сопряженных преобразований.

Утверждение 4. *Для произвольных линейных преобразований φ и ψ евклидова пространства $(L_{\mathbb{P}}, S)$ и для произвольного многочлена $f(x) = c_0 + c_1 x + \ldots + c_m x^m \in \mathbb{P}[x]$ справедливы соотношения*:

(а) $(\varphi^*)^* = \varphi$;

(б) $(\varphi + \psi)^* = \varphi^* + \psi^*$;

(в) $(\varphi\psi)^* = \psi^*\varphi^*$;

(г) $f(\varphi)^* = \overline{f}(\varphi^*)$, *где* $\overline{f}(x) = \overline{c}_0 + \overline{c}_1 x + \ldots + \overline{c}_m x^m$;

(д) $(\varphi^{-1})^* = (\varphi^*)^{-1}$, *если φ — обратимое преобразование.*

Утверждение 5. *Если K — подпространство пространства $(L_{\mathbb{P}}, S)$, инвариантное относительно преобразования $\varphi \in \mathfrak{L}(L_{\mathbb{P}})$, то его ортогональное дополнение $K^{\perp}$ инвариантно относительно φ^*.*

Доказательства этих утверждений легко получаются с использованием теоремы 3 и равенства (4). Проведите их самостоятельно.

§ 2. НОРМАЛЬНЫЕ ПРЕОБРАЗОВАНИЯ

Самосопряженные и изометрические преобразования евклидовых пространств обладают общим свойством, которое позволяет с единых позиций описывать их геометрическое строение.

Определение 5. Линейное преобразование φ евклидова пространства $(L_{\mathbb{P}}, S)$ называется *нормальным*, если $\varphi^*\varphi = \varphi\varphi^*$.

Очевидно, самосопряженные ($\varphi^* = \varphi$) и изометрические ($\varphi^* = \varphi^{-1}$) преобразования являются нормальными. Основное свойство нормальных преобразований состоит в следующем.

Теорема 6. *Если K — подпространство евклидова пространства $(L_{\mathbb{P}}, S)$, инвариантное относительно его нормального преобразования φ, то подпространства K и $K^{\perp}$ инвариантны относительно преобразований φ и φ^*. При этом преобразование $\varphi_1 = \varphi\big|_K$ есть нормальное преобразование евклидова пространства K со скалярным произведением $S_1 = S\big|_K$ и справедливо равенство $\varphi_1^* = \varphi^*\big|_K$.*

□ Пусть $(e_1, \ldots, e_m)$ — ортонормированный базис $K_{\mathbb{P}}$. Дополним его до ортонормированного базиса $\vec{e} = (e_1, \ldots, e_m, \ldots, e_n)$ пространства $L_{\mathbb{P}}$. Заметим, что в этом случае $K_{\mathbb{P}}^{\perp} = (e_{m+1}, \ldots, e_n)_{\mathbb{P}}$ (см. доказательство теоремы 5 главы 17). Так как по условию $\varphi(K) \subset K$, то по теореме 35 главы 15 матрица преобразования φ в базисе $\vec{e}$ имеет вид

$$A_{\vec{e}}(\varphi) = \begin{pmatrix} B_{m\times m} & C_{m\times(n-m)} \\ O & D_{(n-m)\times(n-m)} \end{pmatrix}, \tag{5}$$

а по теореме 3 справедливо равенство

$$A_{\vec{e}}(\varphi^*) = \overline{A_{\vec{e}}(\varphi)}^{\,T} = \begin{pmatrix} \overline{B}^{\,T} & O \\ \overline{C}^{\,T} & \overline{D}^{\,T} \end{pmatrix}. \tag{6}$$

Для доказательства первой части теоремы, очевидно, достаточно показать, что в (5) $C = O_{m\times(n-m)}$.

Так как φ — нормальное преобразование, то матрицы (5) и (6) перестановочны, и поскольку

$$A_{\vec{e}}(\varphi)\, A_{\vec{e}}(\varphi^*) = \begin{pmatrix} B\overline{B}^{\,T} + C\overline{C}^{\,T} & * \\ * & * \end{pmatrix}, \quad A_{\vec{e}}(\varphi^*)\, A_{\vec{e}}(\varphi) = \begin{pmatrix} \overline{B}^{\,T}B & * \\ * & * \end{pmatrix},$$

то справедливо равенство

$$C\overline{C}^{\,T} = \overline{B}^{\,T}B - B\overline{B}^{\,T}. \tag{7}$$

Нетрудно проверить, что *след* (сумма диагональных элементов) *матрицы* $\overline{B}^T B - B\overline{B}^T$ равен нулю. С другой стороны, если $C = (c_{ij})_{m\times(n-m)}$, то след матрицы $C\overline{C}^T$ равен

$$\sum_{i=1}^{m}\sum_{j=1}^{n-m} c_{ij}\overline{c}_{ij} = \sum_{i=1}^{m}\sum_{j=1}^{n-m} |c_{ij}|^2.$$

Поэтому из (7) следует, что $c_{ij} = 0$ для $i \in \overline{1,m}$, $j \in \overline{1,n-m}$, т. е. $C = O_{m\times(n-m)}$.

Для доказательства последнего утверждения теоремы достаточно заметить, что преобразование $\psi = \varphi^*\big|_K$ является сопряженным к φ_1 относительно скалярного произведения S_1, и так как $\varphi^*\varphi = \varphi\varphi^*$, то $\psi\varphi_1 = \varphi_1\psi$. □

Следствие. *Если φ — нормальное преобразование евклидова пространства $(L_{\mathbb{P}}, S)$ и α — его собственный вектор, принадлежащий значению $r \in \mathbb{P}$, то α — собственный вектор преобразования φ^*, принадлежащий значению $\overline{r}$.*

□ Так как подпространство $K = (\alpha)_{\mathbb{P}}$ инвариантно относительно φ, то по теореме оно инвариантно и относительно φ^*, т. е. α — собственный вектор преобразования φ^*.

Пусть $\varphi^*(\alpha) = \alpha r_1$. Тогда справедливы равенства:

$$S(\varphi^*(\alpha), \alpha) = r_1 S(\alpha, \alpha),$$
$$S(\varphi^*(\alpha), \alpha) = S(\alpha, \varphi(\alpha)) = \overline{r} S(\alpha, \alpha),$$

и так как $S(\alpha, \alpha) \neq 0$, то $r_1 = \overline{r}$. □

Полученный результат позволяет следующим образом упростить задачу описания нормальных преобразований.

Теорема 7. *Если φ — нормальное преобразование евклидова пространства $(L_{\mathbb{P}}, S)$, то либо многочлен $\chi_\varphi(x)$ неприводим над $\mathbb{P}$, либо пространство L раскладывается в прямую сумму инвариантных относительно φ попарно ортогональных подпространств*:

$$L_{\mathbb{P}} = L_{1\mathbb{P}} \dotplus \ldots \dotplus L_{t\mathbb{P}} \tag{8}$$

таких, что характеристический многочлен каждого из преобразований $\varphi_i = \varphi\big|_{L_i}$, $i \in \overline{1,t}$, неприводим над $\mathbb{P}$.

□ Докажем теорему индукцией по числу t сомножителей в разложении многочлена $\chi_\varphi(x)$ на неприводимые множители над полем $\mathbb{P}$.

Если $t = 1$, то доказывать нечего. Пусть $t = k > 1$, и при $t < k$ теорема верна. Выберем неприводимый делитель $g(x)$ многочлена $\chi_\varphi(x)$. Тогда по теореме 41 главы 15 $g(x) \mid m_\varphi(x)$, и по теореме 33 главы 15 существует вектор $\alpha_1 \in L_{\mathbb{P}}$ такой, что $m_{\alpha_1,\varphi}(x) = g(x)$. Пусть $L_1 = L^\varphi(\alpha_1)$ — циклическое относительно φ подпространство, порожденное вектором α_1. Тогда L_1 инвариантно относительно φ, и по утверждению 38(б) главы 15 характеристический многочлен преобразования $\varphi_1 = \varphi\big|_L$ совпадает с $g(x)$, и потому неприводим над $\mathbb{P}$.

Рассмотрим подпространство $L' = L_1^{\perp}$ пространства $L_{\mathbb{P}}$. По теореме 6 оно инвариантно относительно преобразования φ, причем $\varphi' = \varphi\big|_{L'}$ — нормальное преобразование евклидова пространства $(L'_{\mathbb{P}}, S')$, где $S' = S\big|_{L'}$. Так как $L = L_1 \dotplus L'$, то $\chi_{\varphi}(x) = \chi_{\varphi_1}(x)\,\chi_{\varphi'}(x)$, и многочлен $\chi_{\varphi'}(x)$ раскладывается над полем $\mathbb{P}$ в произведение $t-1<k$ неприводимых сомножителей.

Если $t = 2$, то нужное разложение пространства $L_{\mathbb{P}}$ уже получено. Если же $t-1>1$, то по предположению индукции пространство $L'_{\mathbb{P}}$ раскладывается в прямую сумму инвариантных относительно φ' попарно S'-ортогональных подпространств: $L' = L_2 \dotplus \ldots \dotplus L_t$ таких, что для каждого из преобразований $\varphi_i = \varphi'\big|_{L_i}$, $i \in \overline{2,t}$, многочлен $\chi_{\varphi_i}(x)$ неприводим над $\mathbb{P}$. Остается заметить, что в таком случае справедливо равенство (8), и подпространства L_i, $i \in \overline{1,t}$, удовлетворяют всем утверждениям теоремы 7 (проверка этого предоставляется читателю). □

Теперь описание общих свойств нормальных преобразований завершается следующим образом.

Теорема 8. *Пусть φ — нормальное преобразование евклидова пространства $(L_{\mathbb{P}}, S)$ размерности n, и многочлен $\chi_{\varphi}(x)$ неприводим над полем $\mathbb{P}$. Тогда либо $n = 1$ и $\varphi = \widehat{r}$ для некоторого $r \in \mathbb{P}$, либо $\mathbb{P} = \mathbb{R}$, $n = 2$, и в любом ортонормированном базисе $\vec{e} = (e_1, e_2)$ пространства $(L_{\mathbb{R}}, S)$ матрица преобразования φ имеет вид*

$$A_{\vec{e}}(\varphi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \tag{9}$$

где $b \neq 0$ и $a+bi$, $a-bi$ — корни многочлена $\chi_{\varphi}(x)$ в поле $\mathbb{C}$.

□ Если $n = 1$, то утверждение очевидно. Если $\deg \chi_{\varphi}(x) = n > 1$, то многочлен $\chi_{\varphi}(x)$ неприводим над $\mathbb{P}$ лишь в случае, когда $\mathbb{P} = \mathbb{R}$ и $n = 2$ (см. § 7 главы 9). В этой ситуации пусть $\vec{e} = (e_1, e_2)$ — ортонормированный базис $(L_{\mathbb{R}}, S)$ и

$$A_{\vec{e}}(\varphi) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{10}$$

Тогда $A_{\vec{e}}(\varphi^*) = A_{\vec{e}}(\varphi)^T$, и из условия нормальности φ следует равенство

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

которое влечет за собой равенства

$$a^2 + b^2 = a^2 + c^2, \tag{11}$$

$$ac + bd = ab + cd. \tag{12}$$

Из (11) следует, что $b^2 = c^2$, т. е. $c \in \{b, -b\}$. При условии $c = b$ из (10) следует, что $\chi_{\varphi}(x) = x^2 - (a+d)x + ad - b^2$, и $\chi_{\varphi}(x)$ имеет положительный дискриминант, что противоречит его неприводимости над $\mathbb{R}$. Следовательно, $c = -b$, и так как $b \neq 0$ ввиду неприводимости $\chi_{\varphi}(x)$, то из (12) следует, что $a - d = d - a$, т. е. $a = d$, и справедливо равенство (9). Тогда многочлен $\chi_{\varphi}(x)$ имеет вид $\chi_{\varphi}(x) = x^2 - 2ax + a^2 + b^2$, и его корни в $\mathbb{C}$ суть $a+bi$ и $a-bi$. □

Теорема 9. *Пусть φ — линейное преобразование евклидова пространства $(L_{\mathbb{P}}, S)$. Тогда справедливы утверждения*:

(а) *если многочлен $\chi_\varphi(x)$ раскладывается над полем $\mathbb{P}$ на линейные множители (в частности, если $\mathbb{P} = \mathbb{C}$), то преобразование φ нормально тогда и только тогда, когда в $L_{\mathbb{P}}$ существует ортонормированный базис, состоящий из собственных векторов преобразования φ*;

(б) *если $\mathbb{P} = \mathbb{R}$, то преобразование φ нормально тогда и только тогда, когда существует ортонормированный базис $\vec{e}$ пространства $L_{\mathbb{R}}$ такой, что*

$$A_{\vec{e}}(\varphi) = \operatorname{Diag}\left(r_1, \ldots, r_k, \begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix}, \ldots, \begin{pmatrix} a_s & b_s \\ -b_s & a_s \end{pmatrix}\right), \quad b_i \neq 0, \ \ i \in \overline{1,s}, \qquad (13)$$

при этом в (13) *допускается отсутствие клеток первого порядка, т. е. равенство $k = 0$, или отсутствие клеток второго порядка, т. е. равенство $s = 0$.*

□ Если в некотором ортонормированном базисе $\vec{e}$ пространства $L_{\mathbb{P}}$ матрица $A_{\vec{e}}(\varphi)$ диагональна (т. е. выполнены условия пункта (а)) или при условии $\mathbb{P} = \mathbb{R}$ имеет вид (13) (т. е. выполнены условия пункта (б)), то, как легко проверить, матрица $A_{\vec{e}}(\varphi)$ перестановочна с матрицей $\overline{A_{\vec{e}}(\varphi)}^{\,T} = A_{\vec{e}}(\varphi^*)$, и потому $\varphi\varphi^* = \varphi^*\varphi$, т. е. φ — нормальное преобразование.

Наоборот, пусть φ — нормальное преобразование пространства $(L_{\mathbb{P}}, S)$. Тогда по теореме 7 существует разложение

$$L_{\mathbb{P}} = L_{1\mathbb{P}} \dotplus \ldots \dotplus L_{t\mathbb{P}}, \quad t \geqslant 1, \qquad (14)$$

в котором каждое подпространство L_i инвариантно относительно φ, для $\varphi_i = \varphi\big|_{L_i}$ многочлен $\chi_{\varphi_i}(x)$ неприводим над $\mathbb{P}$, и если $t > 1$, то подпространства L_i и L_j при $i \neq j$ ортогональны. При этом в силу теоремы 6 φ_i — нормальное преобразование евклидова пространства $(L_{i\mathbb{P}}, S_i)$, где $S_i = S\big|_{L_i}$ для $i \in \overline{1,t}$.

Выберем в каждом из подпространств $L_{i\mathbb{P}}$ ортонормированный базис и обозначим через A_i матрицу преобразования φ_i в этом базисе. Пусть $\vec{e} = (e_1, \ldots, e_n)$ — система векторов L, составленная из выбранных базисов слагаемых L_i в разложении (14). Тогда, очевидно, $\vec{e}$ — ортонормированный базис $(L_{\mathbb{P}}, S)$, и по теореме 36 главы 15

$$A_{\vec{e}}(\varphi) = \operatorname{Diag}(A_1, \ldots, A_t). \qquad (15)$$

Остается заметить, что поскольку каждый из многочленов $\chi_{A_i}(x)$ есть неприводимый над $\mathbb{P}$ делитель $\chi_\varphi(x)$, то справедливы следующие утверждения:

(а) если многочлен $\chi_\varphi(x)$ распадается над $\mathbb{P}$ на линейные множители, то все матрицы A_i в (15) имеют размеры 1×1, т. е. $t = n$, и $\vec{e}$ — базис из собственных векторов преобразования φ;

(б) если $\mathbb{P} = \mathbb{R}$, то по теореме 8 каждая матрица A_i имеет размеры 1×1 или 2×2, причем в последнем случае она имеет вид (9).

Поэтому если дополнительно предположить, что слагаемые в (14) удовлетворяют условию $\dim L_{1\mathbb{P}} \leqslant \dim L_{2\mathbb{P}} \leqslant \ldots \leqslant \dim L_{t\mathbb{P}}$, то можно утверждать, что матрица (15) имеет вид (13). □

Определение 6. Если φ — нормальное преобразование евклидова пространства $(L_{\mathbb{P}}, S)$ и $\vec{e}$ — такой ортонормированный базис $L_{\mathbb{P}}$, что матрица $A_{\vec{e}}(\varphi)$ диагональна или в случае $\mathbb{P} = \mathbb{R}$ имеет вид (13), то будем говорить, что $\vec{e}$ — *геометрически нормальный базис преобразования* φ, а $A_{\vec{e}}(\varphi)$ — *матрица в геометрически нормальной форме*.

Замечание 2. Геометрически нормальная форма матрицы нормального преобразования тесно связана с ее второй нормальной формой: если $A_{\vec{e}}(\varphi)$ — диагональная матрица, то это матрица во второй нормальной форме; если же $\mathbb{P} = \mathbb{R}$ и $A_{\vec{e}}(\varphi)$ имеет вид (13), то вторая нормальная форма матрицы $A_{\vec{e}}(\varphi)$ имеет вид

$$N_2(A_{\vec{e}}(\varphi)) = \operatorname{Diag}\left(r_1, \ldots, r_k, \begin{pmatrix} 0 & -a_1^2 - b_1^2 \\ 1 & 2a_1 \end{pmatrix}, \ldots, \begin{pmatrix} 0 & -a_s^2 - b_s^2 \\ 1 & 2a_s \end{pmatrix}\right),$$

и $N_2(A_{\vec{e}}(\varphi)) = A_{\vec{u}}(\varphi)$, где

$$\vec{u} = (e_1, \ldots, e_k, e_{k+1}, \varphi(e_{k+1}), e_{k+3}, \varphi(e_{k+3}), \ldots, e_{k+2s-1}, \varphi(e_{k+2s-1})).$$

Доказательства этих утверждений предоставляются читателю.

На практике, если характеристический многочлен нормального преобразования φ евклидова пространства $(L_{\mathbb{P}}, S)$ распадается над полем $\mathbb{P}$ на линейные множители, то построение геометрически нормального базиса для φ основывается на следующих рассуждениях.

Пусть $r_1, \ldots, r_t \in \mathbb{P}$ — все различные собственные значения преобразования φ. Тогда $\chi_\varphi(x) = (x - r_1)^{n_1} \ldots (x - r_t)^{n_t}$, по теореме 44 главы 15

$$L_{\mathbb{P}} = \operatorname{Ker}(\varphi - \widehat{r}_1)^{n_1} \dotplus \ldots \dotplus \operatorname{Ker}(\varphi - \widehat{r}_t)^{n_t},$$

и в силу теоремы 9(а)

$$L_{\mathbb{P}} = \operatorname{Ker}(\varphi - \widehat{r}_1) \dotplus \ldots \dotplus \operatorname{Ker}(\varphi - \widehat{r}_t)$$

(покажите). Пусть для $j \in \overline{1,t}$

$$u_1^{(j)}, \ldots, u_{n_j}^{(j)}$$

— произвольный базис пространства $\operatorname{Ker}(\varphi - \widehat{r}_j)$. Если к этому базису применить процесс ортогонализации и пронормировать получившуюся систему векторов, то получится ортонормированный базис $e_1^{(j)}, \ldots, e_{n_j}^{(j)}$ пространства $\operatorname{Ker}(\varphi - \widehat{r}_j)$. В таком случае система

$$e_1^{(1)}, \ldots, e_{n_1}^{(1)}, e_1^{(2)}, \ldots, e_1^{(t)}, \ldots, e_{n_t}^{(t)}$$

есть базис $L_{\mathbb{P}}$, состоящий из собственных векторов φ, причем это — ортонормированный базис, поскольку верна

Теорема 10. *Собственные векторы нормального преобразования φ евклидова пространства $(L_{\mathbb{P}}, S)$, принадлежащие различным собственным значениям, ортогональны.*

□ Пусть $\alpha_1, \alpha_2 \in L_{\mathbb{P}} \setminus \theta$ и $\varphi(\alpha_i) = \alpha_i r_i$ для $i \in \overline{1,2}$, где $r_1, r_2 \in \mathbb{P}$ и $r_1 \neq r_2$. Тогда по следствию теоремы 6 $\varphi^*(\alpha_2) = \alpha_2 \overline{r}_2$ и верны равенства

$$S(\varphi(\alpha_1), \alpha_2) = r_1 S(\alpha_1, \alpha_2),$$
$$S(\varphi(\alpha_1), \alpha_2) = S(\alpha_1, \varphi^*(\alpha_2)) = S(\alpha_1, \alpha_2 \overline{r}_2) = r_2 S(\alpha_1, \alpha_2).$$

Отсюда $(r_1 - r_2) S(\alpha_1, \alpha_2) = 0$ и $S(\alpha_1, \alpha_2) = 0$. □

§ 3. СВОЙСТВА САМОСОПРЯЖЕННЫХ ПРЕОБРАЗОВАНИЙ

Полное описание и простую геометрическую интерпретацию самосопряженных преобразований дает

Теорема 11. *Линейное преобразование φ евклидова пространства $(L_{\mathbb{P}}, S)$ является самосопряженным тогда и только тогда, когда*

(а) *в пространстве $L_{\mathbb{P}}$ существует ортонормированный базис $\vec{e}$, состоящий из собственных векторов преобразования φ;*

(б) *все собственные значения преобразования φ — действительные числа.*

□ Пусть верны утверждения (а) и (б). Тогда $A_{\vec{e}}(\varphi) = \operatorname{diag}(r_1, \ldots, r_n)$, где $r_1, \ldots, r_n \in \mathbb{R}$, и потому $\overline{A_{\vec{e}}(\varphi)}^T = \operatorname{diag}(\overline{r}_1, \ldots, \overline{r}_n) = A_{\vec{e}}(\varphi)$, т. е. $A_{\vec{e}}(\varphi)$ — эрмитова матрица. По следствию 2 теоремы 3 φ — самосопряженное преобразование.

Наоборот, пусть $\varphi = \varphi^*$. Тогда φ — нормальное преобразование пространства $(L_{\mathbb{P}}, S)$, и по теореме 9 в пространстве L для преобразования φ существует геометрически нормальный базис $\vec{e}$. Матрица $A_{\vec{e}}(\varphi)$ либо диагональна, либо имеет вид (13). Но последнее невозможно, так как по следствию 2 теоремы 3 $\overline{A_{\vec{e}}(\varphi)}^T = A_{\vec{e}}(\varphi)$, а матрица вида (13) при $s \neq 0$ такому равенству не удовлетворяет. Следовательно, $A_{\vec{e}}(\varphi) = \operatorname{diag}(r_1, \ldots, r_n)$, и для $i \in \overline{1,n}$ выполняется условие $\overline{r}_i = r_i$, т. е. $r_i \in \mathbb{R}$. Таким образом, φ обладает свойствами (а) и (б). □

Доказанная теорема дает следующую характеризацию самосопряженных преобразований в классе нормальных преобразований.

Следствие 1. *Линейное преобразование φ евклидова пространства $(L_{\mathbb{P}}, S)$ является самосопряженным тогда и только тогда, когда оно нормально и все корни многочлена $\chi_\varphi(x)$ в поле $\mathbb{C}$ являются действительными числами.*

□ Достаточно сравнить формулировки теорем 11 и 9(а). □

Следствие 2. *Любая эрмитова матрица $A \in \mathbb{P}_{n,n}$ (в частности, любая симметричная матрица $A \in \mathbb{R}_{n,n}$) подобна диагональной матрице D с действительными элементами, причем матрица $T \in \mathbb{P}^*_{n,n}$, удовлетворяющая равенству $T^{-1}AT = D$, может быть выбрана унитарной, если $\mathbb{P} = \mathbb{C}$, и ортогональной, если $\mathbb{P} = \mathbb{R}$ (т. е. если A — симметричная матрица над $\mathbb{R}$).*

□ Рассмотрим евклидово пространство $(L_{\mathbb{P}}, S)$ с ортонормированным базисом $(u_1, \ldots, u_n) = \vec{u}$ и зададим его линейное преобразование φ равенством $A_{\vec{u}}(\varphi) = A$. Тогда по следствию 2 теоремы 3 φ — самосопряженное преобразование, и по доказанной теореме в пространстве L существует ортонормированный базис $\vec{e}$, состоящий из собственных векторов преобразования φ, причем $A_{\vec{e}}(\varphi) = D$ — диагональная матрица из $\mathbb{R}_{n,n}$. Остается заметить, что если T — матрица перехода от базиса $\vec{u}$ к базису $\vec{e}$, то $T^{-1}AT = D$, и при $\mathbb{P} = \mathbb{R}$ матрица T ортогональна (см. утверждение 9 главы 17), а при $\mathbb{P} = \mathbb{C}$ она унитарна (см. утверждение 13 главы 17). □

Отметим, что способ построения матрицы T в доказанном следствии по сути дела указан в конце § 2.

§ 4. СВОЙСТВА ИЗОМЕТРИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

В утверждении 1 уже показано, что изометрические преобразования евклидова пространства $(L_{\mathbb{P}}, S)$ могут быть охарактеризованы как линейные преобразования со свойством $\varphi^* = \varphi^{-1}$. Приведем еще две важных характеризации таких преобразований.

Теорема 12. *Для линейного преобразования φ евклидова пространства $(L_{\mathbb{P}}, S)$ следующие утверждения эквивалентны*:

(а) *φ — изометрия*;

(б) *существует базис $e_1, \ldots, e_n$ пространства $L_{\mathbb{P}}$ такой, что*

$$S(\varphi(e_i), \varphi(e_j)) = S(e_i, e_j) \quad \textit{для всех} \quad i, j \in \overline{1,n};$$

(в) $\forall\, \alpha \in L: \ \|\varphi(\alpha)\| = \|\alpha\|$.

Множество $I(L_{\mathbb{P}}, S)$ всех изометрических преобразований пространства $(L_{\mathbb{P}}, S)$ есть подгруппа группы $\mathfrak{L}(L_{\mathbb{P}})^*$ всех его обратимых линейных преобразований.

□ Импликация (а)⇒(б) следует непосредственно из определения 3.

Если выполнено (б), то для любого вектора $\alpha = \sum_{i=1}^{n} e_i a_i$ верны равенства

$$\|\varphi(\alpha)\|^2 = S(\varphi(\alpha), \varphi(\alpha)) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_i \overline{a}_j S(\varphi(e_i), \varphi(e_j)) =$$

$$= \sum_{i=1}^{n}\sum_{j=1}^{n} a_i \overline{a}_j S(e_i, e_j) = S(\alpha, \alpha) = \|\alpha\|^2.$$

Следовательно, верна импликация (б)⇒(в).

Докажем (в)⇒(а). Рассмотрим преобразование $\psi = \varphi^* \circ \varphi$. Нам достаточно доказать, что $\psi = \widehat{1}$ — тождественное преобразование. Заметим, что ψ — самосопряженное преобразование, так как по утверждению 4 $\psi^* = (\varphi^* \circ \varphi)^* = \varphi^* \circ \varphi^{**} = \varphi^* \circ \varphi = \psi$. По теореме 11(а) в пространстве $L_{\mathbb{P}}$ существует базис $\vec{e}$, состоящий из собственных векторов преобразования ψ. Пусть $\psi(e_i) = e_i r_i$, $r_i \in \mathbb{P}$ для $i \in \overline{1,n}$. Тогда ввиду утверждения (в) для $i \in \overline{1,n}$ имеем:

$$S(e_i, e_i) = S(\varphi(e_i), \varphi(e_i)) = S((\varphi^* \circ \varphi)(e_i),\, e_i) = S(\psi(e_i), e_i) = r_i S(e_i, e_i).$$

Следовательно, $r_1 = \ldots = r_n = 1$ и $A_{\vec{e}}(\psi) = E$, т. е. $\psi = \widehat{1}$.

Докажем последнее утверждение теоремы. Пусть $\varphi, \psi \in I(L_{\mathbb{P}}, S)$. Тогда по доказанному выше для любого вектора $\beta \in L$ верно равенство $\|\varphi^{-1}(\beta)\| = \|\beta\|$, и потому для любого $\alpha \in L$ верны равенства

$$\|(\varphi^{-1} \circ \psi)(\alpha)\| = \|\psi(\alpha)\| = \|\alpha\|.$$

Следовательно, $\varphi^{-1} \circ \psi \in I(L_{\mathbb{P}}, S)$ и $I(L_{\mathbb{P}}, S)$ — подгруппа в $\mathfrak{L}(L_{\mathbb{P}})^*$. □

Полное описание и геометрическую интерпретацию изометрических преобразований дает

Теорема 13. *Линейное преобразование φ евклидова пространства $(L_{\mathbb{P}}, S)$ является изометрическим тогда и только тогда, когда либо*

(а) *в пространстве $L_{\mathbb{P}}$ существует ортонормированный базис $\vec{e}$ такой, что*

$$A_{\vec{e}}(\varphi) = \operatorname{diag}(r_1, \ldots, r_n) \tag{16}$$

и выполняются условия

$$r_1, \ldots, r_n \in \mathbb{P}, \quad |r_i| = 1 \ \text{ для } \ i \in \overline{1,n}; \tag{17}$$

либо

(б) $\mathbb{P} = \mathbb{R}$ *и в пространстве $L_{\mathbb{R}}$ существует ортонормированный базис $\vec{e}$ такой, что*

$$A_{\vec{e}}(\varphi) = \operatorname{Diag}\left(r_1, \ldots, r_k, \begin{pmatrix} \cos\omega_1 & \sin\omega_1 \\ -\sin\omega_1 & \cos\omega_1 \end{pmatrix}, \ldots, \begin{pmatrix} \cos\omega_s & \sin\omega_s \\ -\sin\omega_s & \cos\omega_s \end{pmatrix}\right) \tag{18}$$

и выполняются условия

$$r_1, \ldots, r_k \in \{1, -1\}, \quad \omega_1, \ldots, \omega_s \in (0, 2\pi) \setminus \{\pi\} \tag{19}$$

(*при этом, как и в теореме* 9(б), *возможны случаи $k = 0$ или $s = 0$*).

□ Если для φ верно утверждение (а) или утверждение (б), то для соответствующего базиса $\vec{e}$ матрица $A_{\vec{e}}(\varphi^*) = \overline{A_{\vec{e}}(\varphi)}^T$, очевидно, является обратной к матрице $A_{\vec{e}}(\varphi)$, и потому $\varphi^* = \varphi^{-1}$, т. е. φ — изометрия.

Наоборот, пусть φ — изометрическое преобразование пространства $(L_{\mathbb{P}}, S)$. Тогда φ — нормальное преобразование, и по теореме 9 для φ в пространстве $L_{\mathbb{P}}$ существует геометрически нормальный базис $\vec{e}$. Так как $\vec{e}$ — ортонормированный базис, то условие изометричности φ может быть записано равенством

$$\overline{A_{\vec{e}}(\varphi)}^T = A_{\vec{e}}(\varphi)^{-1}. \tag{20}$$

При этом по определению 6 возможна одна из следующих ситуаций.

(а) Матрица $A_{\vec{e}}(\varphi)$ имеет вид (16). В этом случае условие (20), очевидно, эквивалентно условию (17).

(б) $\mathbb{P} = \mathbb{R}$ и матрица $A_{\vec{e}}(\varphi)$ имеет вид (13). В этом случае условие (20) эквивалентно тому, что в (13) $r_1, \ldots, r_k \in \{1, -1\}$, а каждая клетка $\begin{pmatrix} a_j & b_j \\ -b_j & a_j \end{pmatrix}$ удовлетворяет условию

$$a_j^2 + b_j^2 = 1. \tag{21}$$

Последнее равносильно тому, что $a_j = \cos\omega_j$, $b_j = \sin\omega_j$ для подходящего $\omega_j \in (0, 2\pi)$, при этом условие $b_j \neq 0$ из (13) эквивалентно условию $\omega_j \neq \pi$ из (19). □

Следствие. *Линейное преобразование φ евклидова пространства $(L_{\mathbb{P}}, S)$ является изометрическим тогда и только тогда, когда оно нормально и все корни многочлена $\chi_\varphi(x)$ в поле $\mathbb{C}$ равны по модулю единице.*

□ Достаточно сравнить формулировки теорем 9 и 13 и заметить, что корни характеристического многочлена матрицы $\begin{pmatrix} a_j & b_j \\ -b_j & a_j \end{pmatrix}$ над $\mathbb{R}$ равны по модулю единице тогда и только тогда, когда выполняется условие (21). □

Из теоремы 13 видно, что в евклидовом вещественном пространстве размерности 2 нетождественная изометрия при подходящем выборе декартовых координат сводится к симметрии относительно одной из координатных осей или к повороту векторов вокруг начала координат (см. пример 2). В пространствах бóльших размерностей изометрические преобразования «составляются» из указанных выше простейших преобразований при подходящем выборе осей (и плоскостей).

ЗАДАЧИ

1. Докажите, что если φ — нормальное преобразование евклидова пространства $(L_{\mathbb{P}}, S)$, то для любого многочлена $f(x) \in \mathbb{P}[x]$ преобразование $f(\varphi)$ также нормально.

2. Докажите, что минимальный многочлен нормального преобразования не имеет кратных множителей в каноническом разложении.

3. Матрица $A \in \mathbb{P}_{n,n}$ называется *нормальной*, если $\overline{A}^T A = A\overline{A}^T$. Докажите, что две нормальные матрицы подобны тогда и только тогда, когда равны их характеристические многочлены. (Покажите, что многочлен $m_A(x)$ не имеет кратных множителей в каноническом разложении, и воспользуйтесь этим.)

4. Пусть характеристический многочлен нормального преобразования φ имеет вид $\chi_\varphi(x) = f_1(x)f_2(x)$, где $(f_1(x), f_2(x)) = e$. Докажите, что подпространства $\operatorname{Ker} f_1(\varphi)$ и $\operatorname{Ker} f_2(\varphi)$ ортогональны. (Обратите внимание, что это утверждение есть обобщение теоремы 10.)

5. Пусть минимальный многочлен нормального преобразования φ евклидова пространства $(L_{\mathbb{P}}, S)$ имеет над $\mathbb{P}$ каноническое разложение $m_\varphi(x) = g_1(x) \ldots g_t(x)$. Докажите, что $L = \operatorname{Ker} g_1(\varphi) \dotplus \ldots \dotplus \operatorname{Ker} g_t(\varphi)$ и слагаемые в этом разложении попарно ортогональны.

6. Пусть φ — линейное преобразование евклидова пространства $(L_{\mathbb{P}}, S)$ такое, что многочлен $\chi_\varphi(x)$ распадается над $\mathbb{P}$ на линейные множители. Докажите, что если любое подпространство M пространства $L_{\mathbb{P}}$, инвариантное относительно φ, инвариантно и относительно φ^*, то φ — нормальное преобразование. Обратите внимание на то, что это — утверждение, обратное к теореме 6. (Индукцией по $n = \dim L_{\mathbb{P}}$ докажите, что в $L_{\mathbb{P}}$ существует ортонормированный базис, состоящий из собственных векторов преобразования φ.)

7. Приведите пример, показывающий, что в условиях предыдущей задачи нельзя отказаться от того, что $\mathbb{P}$ — поле разложения для $\chi_\varphi(x)$. (Постройте линейное преобразование евклидова вещественного пространства размерности 2 с неприводимым характеристическим многочленом, у которого матрица в ортонормированном базисе не является нормальной.)

8. Докажите, что произвольное (не обязательно линейное) преобразование φ евклидова пространства $(L_{\mathbb{P}}, S)$ со свойством

$$\forall\, \alpha, \beta \in L:\ \ S(\varphi(\alpha),\, \varphi(\beta)) = S(\alpha, \beta)$$

является изометрией (т. е. линейным преобразованием). (Покажите, что для любых $\alpha, \beta \in L$ и $a \in \mathbb{P}$ верны равенства $\|\varphi(\alpha a) - \varphi(\alpha)a\| = 0$ и $\|\varphi(\alpha+\beta) - \varphi(\alpha) - \varphi(\beta)\| = 0$.)

9. Докажите, что линейное преобразование φ евклидова пространства является нормальным тогда и только тогда, когда оно имеет вид $\varphi = \sigma\psi$, где σ — изометрическое преобразование, а ψ — перестановочное с σ самосопряженное преобразование.

10. Докажите, что две симметричные матрицы $A, B \in \mathbb{R}_{n,n}$ подобны тогда и только тогда, когда они ортогонально подобны (т. е. существует ортогональная матрица $T \in \mathbb{R}_{n,n}$ такая, что $T^{-1}AT = B$).

11. Докажите, что ортогональная матрица $A \in \mathbb{R}_{n,n}$ подобна диагональной матрице над $\mathbb{R}$ тогда и только тогда, когда A симметрична.

12. Пусть $\alpha_1, \ldots, \alpha_m$ и $\beta_1, \ldots, \beta_m$ — две системы векторов евклидова пространства $(L_{\mathbb{P}}, S)$. Докажите, что для существования изометрического преобразования φ этого пространства со свойством $\varphi(\alpha_i) = \beta_i$, $i \in \overline{1, m}$, необходимо и достаточно, чтобы были равны матрицы Грама $\Gamma_S(\alpha_1, \ldots, \alpha_m)$ и $\Gamma_S(\beta_1, \ldots, \beta_m)$. (Рассмотрите сначала случаи, когда указанные системы а) являются базисами $L_{\mathbb{P}}$, б) линейно независимы.)

13. Пусть $\alpha_1, \ldots, \alpha_{n-1}$ и $\beta_1, \ldots, \beta_{n-1}$ — ортонормированные системы векторов евклидова пространства $(L_{\mathbb{P}}, S)$ размерности n. Докажите, что существуют ровно два изометрических преобразования φ со свойством $\varphi(\alpha_i) = \beta_i$, $i \in \overline{1, n-1}$ и бесконечно много других линейных преобразований с этим свойством.

Глава 19

КВАДРАТИЧНЫЕ ФОРМЫ

Здесь читатель познакомится с важным классом многочленов от n переменных и различными способами их преобразований. В частности, будут показаны приложения теории, развитой в двух предыдущих главах. Излагаемые ниже результаты обобщают и усиливают изложенные в курсе аналитической геометрии результаты о поверхностях и кривых второго порядка в декартовом пространстве.

В этой главе изучаются квадратичные формы лишь над такими полями, в которых единица e удовлетворяет условию

$$e + e \neq 0. \tag{1}$$

Таким образом, из рассмотрения исключается, например поле $P = \mathbb{Z}_2$, но рассматриваются все поля вида $P = \mathbb{Z}_p$, где p — нечетное простое, а также поля $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Далее условие (1) используется без дополнительных оговорок.

§ 1. ОБЩИЕ СВОЙСТВА КВАДРАТИЧНЫХ ФОРМ. КАНОНИЧЕСКИЙ ВИД

Понятие формы и, в частности, квадратичной формы от n переменных над полем P уже известно читателю из главы 9 (определение 25). Мы дадим здесь несколько иное, более удобное для дальнейшего исследования, определение такой формы.

Определение 1. *Квадратичной формой* от n переменных $x_1, \ldots, x_n$ над полем P называется любой многочлен $f(\vec{x}) \in P[x_1, \ldots, x_n]$ вида

$$f(\vec{x}) = a_{11}x_1^2 + a_{12}x_1x_2 + \ldots + a_{1n}x_1x_n + a_{22}x_2^2 + a_{21}x_2x_1 + \ldots + a_{nn}x_n^2,$$

где $a_{ij} \in P$ для $i, j \in \overline{1, n}$.

Коротко квадратичную форму $f(\vec{x})$ записывают равенством

$$f(\vec{x}) = \sum_{i,j=1}^{n} a_{ij}x_ix_j. \tag{2}$$

Замечание 1. Выражение (2) не является, вообще говоря, канонической записью многочлена $f(\vec{x})$ в смысле определения 24 главы 9. Последняя при условии (2) имеет вид

$$f(\vec{x}) = \sum_{i=1}^{n} a_{ii}x_i^2 + \sum_{1\leqslant i<j\leqslant n} (a_{ij} + a_{ji})\, x_i x_j.$$

Кроме того, согласно приведенному определению, нулевой многочлен является квадратичной формой. Только в этом и состоит отличие определения 1 от определения 26 главы 9.

С квадратичными формами от двух и трех переменных читатель встречался в курсе аналитической геометрии, где было доказано, что уравнение любой кривой (поверхности) второго порядка на плоскости (в пространстве) в случае, если она имеет хотя бы один центр, может быть после параллельного переноса координатных осей записано в виде $f(x_1, x_2) = c$ (соответственно $f(x_1, x_2, x_3) = c$), где f — квадратичная форма над $\mathbb{R}$.

Определение 2. *Матрицей квадратичной формы* (2) называется матрица $B_f = (b_{ij})_{n\times n}$ над полем P, элементы которой определяются равенствами

$$b_{ij} = (2e)^{-1}(a_{ij} + a_{ji}), \quad i, j \in \overline{1, n} \tag{3}$$

(определение корректно ввиду условия (1)).

Нетрудно заметить, что B_f — симметричная матрица над P, и наряду с (2) справедливо равенство

$$f(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} b_{ij}x_i x_j, \tag{4}$$

которое можно записать в векторной форме

$$f(\vec{x}) = \vec{x}\, B_f\, x^{\downarrow}, \quad \text{где} \quad \vec{x} = (x_1, \ldots, x_n), \quad x^{\downarrow} = \vec{x}^{\,T}. \tag{5}$$

Отметим, что согласно замечанию 1 при условиях (3), (4) каноническая запись квадратичной формы $f(\vec{x})$ имеет вид

$$f(\vec{x}) = \sum_{i=1}^{n} b_{ii}x_i^2 + \sum_{1\leqslant i<j\leqslant n} 2b_{ij}x_i x_j. \tag{6}$$

Из введенных определений и равенства (6) легко следует

Утверждение 1. *Квадратичные формы $f(x_1, \ldots, x_n)$ и $g(x_1, \ldots, x_n)$ над P равны тогда и только тогда, когда равны их матрицы. Для любой симметричной матрицы $B \in P_{n,n}$ многочлен $f(x_1, \ldots, x_n) = \vec{x}Bx^{\downarrow}$ есть квадратичная форма, причем $B_f = B$.*

□ Доказательство сводится к сравнению канонических записей многочленов $f(\vec{x})$ и $g(\vec{x})$, выраженных через коэффициенты соответствующих матриц. Выкладки предоставляются читателю. □

Таким образом, существует взаимно однозначное соответствие $f \to B_f$ между множеством всех квадратичных форм f из $P[x_1, \ldots, x_n]$ и множеством всех симметричных матриц $B \in P_{n,n}$.

Определение 3. Будем говорить, что квадратичная форма $g(\vec{y}) = g(y_1, \ldots, y_n)$ получается из квадратичной формы $f(\vec{x})$ *невырожденным* (*линейным*) *преобразованием переменных*, если существует невырожденная матрица $C \in P_{n,n}$ такая, что после замены в форме $f(\vec{x})$ переменных $x_1, \ldots, x_n$ по формуле

$$x^{\downarrow} = Cy^{\downarrow} \tag{7}$$

выполняется равенство

$$f(x_1(y_1, \ldots, y_n), \ \ldots, \ x_n(y_1, \ldots, y_n)) = g(y_1, \ldots, y_n). \tag{8}$$

В этом случае говорят также, что форма $g(\vec{y})$ получается из $f(\vec{x})$ *невырожденной заменой переменных* (7).

Утверждение 2. *При условии* (7) *равенство* (8) *выполняется тогда и только тогда, когда*

$$B_g = C^T B_f C. \tag{9}$$

□ Пользуясь векторной записью формы $g(\vec{y})$ и равенством (7), получаем:

$$f(x_1(\vec{y}), \ldots, x_n(\vec{y})) = (\vec{y}\,C^T)B_f(Cy^{\downarrow}) = \vec{y}\,(C^T B_f C)y^{\downarrow},$$

причем матрица $C^T B_f C$ симметрична. Отсюда и из утверждения 1 следует, что при условии (8) выполняется (9). Обратное утверждение теперь очевидно. □

Определение 4. Говорят, что квадратичная форма $f(x_1, \ldots, x_n)$ *эквивалентна* квадратичной форме $g(y_1, \ldots, y_n)$, и пишут $f(\vec{x}) \sim g(\vec{y})$, если $f(\vec{x})$ переводится в $g(\vec{y})$ некоторым невырожденным линейным преобразованием переменных.

Утверждение 3. *Отношение эквивалентности квадратичных форм рефлексивно, симметрично и транзитивно.*

□ Равенство (9) ввиду обратимости матрицы C влечет за собой равенство $B_f = (C^{-1})^T B_g C^{-1}$, и потому в силу утверждения 2 из $f \sim g$ следует $g \sim f$. Следовательно, отношение $\sim$ симметрично. Доказательство остальных свойств предоставляется читателю. □

Определение 5. *Рангом квадратичной формы* $f(\vec{x})$ называется ранг ее матрицы B_f. Его обозначают символом $\operatorname{rang} f$.

Утверждение 4. *Если квадратичные формы $f(\vec{x})$ и $g(\vec{y})$ над полем P эквивалентны, то их ранги равны.*

□ Достаточно воспользоваться равенством (9) и условием $|C| \neq 0$. □

Далее читатель увидит, что обращение утверждения 4 верно не всегда, например, оно верно, если $P = \mathbb{C}$, и не верно, если $P = \mathbb{R}$.

Замечание 2. Квадратичная форма $f(x_1,\dots,x_n)$ может не зависеть (зависеть лишь формально) от некоторого переменного x_s из $x_1,\dots,x_n$, т. е. ее каноническая запись (6) в виде многочлена может удовлетворять условиям

$$b_{ss}=0,\quad 2b_{is}=2b_{sj}=0 \ \text{ для } \ i\in\overline{1,s-1},\ j\in\overline{s+1,n}.$$

Это, ввиду равенств $b_{is}=b_{si}$, $i\in\overline{1,n}$ и условия (1), эквивалентно равенствам $b_{si}=b_{is}=0$, $i\in\overline{1,n}$, т. е. эквивалентно тому, что в матрице B_f s-я строка и s-й столбец нулевые. Наоборот, если $m>n$, то квадратичную форму $f(x_1,\dots,x_n)$ можно считать (формально) формой от m переменных $x_1,\dots,x_n,\dots,x_m$, рассматривая вместо нее форму $f(x_1,\dots,x_n,\dots,x_m)=f(x_1,\dots,x_n)+0x_{n+1}^2+\dots+0x_m^2$, т. е. приписывая к матрице B_f $(m-n)$ нулевых строк и столбцов. Используя этот подход, мы будем в дальнейшем говорить об эквивалентности квадратичных форм $f(x_1,\dots,x_n)$ и $g(y_1,\dots,y_m)$ и в случае, когда $n<m$, имея в виду эквивалентность формы $g(y_1,\dots,y_m)$ и указанной выше формы $f(x_1,\dots,x_n,\dots,x_m)$.

Пример 1. Форма $g(y_1,y_2)=y_1^2+2y_1y_2+y_2^2$ над $\mathbb{R}$ эквивалентна форме $f(x_1)=x_1^2$, поскольку невырожденная замена переменных $\binom{y_1}{y_2}=\begin{pmatrix}1&-1\\0&1\end{pmatrix}\binom{x_1}{x_2}$ приводит к равенствам

$$g(y_1,y_2)=(x_1-x_2)^2+2(x_1-x_2)x_2+x_2^2=f(x_1).$$

Наоборот, чтобы получить из формы $f(x_1)$ форму $g(y_1,y_2)$, надо записать $f(x_1)$ в виде $f(x_1)=x_1^2+0x_2^2$ (уравнять число переменных) и произвести обратную невырожденную (!) замену $\binom{x_1}{x_2}=\begin{pmatrix}1&1\\0&1\end{pmatrix}\binom{y_1}{y_2}$.

Определение 6. Квадратичная форма $f(x_1,\dots,x_n)$ над полем P называется *канонической*, если она имеет вид

$$f(x_1,\dots,x_n)=b_{11}x_1^2+\dots+b_{nn}x_n^2,$$

т. е. если B_f — диагональная матрица.

Таким образом, каноническая форма $f(\vec{x})$ — это такая квадратичная форма, для которой стандартная запись в виде (4) совпадает с ее канонической записью (6) как многочлена над P.

Следующий фундаментальный результат обобщает известные из курса аналитической геометрии утверждения о возможности приведения центральной кривой или поверхности второго порядка к «главным осям».

Теорема 5. *Любая квадратичная форма $f(x_1,\dots,x_n)$ над полем P (в котором $2e\neq 0$) эквивалентна некоторой канонической квадратичной форме.*

□ Индукция по n. При $n=1$ сама форма f является канонической. Пусть $m\geqslant 2$ и теорема верна для всех квадратичных форм от $n<m$ переменных. Рассмотрим случай, когда $n=m$.

Если $f(x_1,\dots,x_n)$ — нулевой многочлен, т. е. в (4) все коэффициенты b_{ij} равны нулю (см. замечание 1), то $f = 0x_1^2 + \dots + 0x_n^2$ — каноническая форма. Допустим теперь, что $f(x_1,\dots,x_n) \neq 0$. Тогда возможны две ситуации.

1. В равенстве (4) $b_{ii} \neq 0$ для некоторого $i \in \overline{1,n}$. Предположим, что $b_{11} \neq 0$ (случай, когда $b_{11} = 0$ и $b_{ii} \neq 0$ для $i > 1$ рассматривается аналогично). Выделим в форме f все слагаемые, содержащие переменное x_1: очевидно, что, пользуясь равенствами $b_{1i} = b_{i1}$ для $i \in \overline{1,n}$, ее можно записать в виде

$$f(x_1,\dots,x_n) = b_{11}x_1^2 + 2b_{12}x_1x_2 + \dots + 2b_{1n}x_1x_n + f_1(x_2,\dots,x_n),$$

где $f_1(x_2,\dots,x_n)$ — квадратичная форма от переменных $x_2,\dots,x_n$. Теперь нетрудно увидеть, что верно равенство

$$f(x_1,\dots,x_n) = \frac{1}{b_{11}}(b_{11}x_1 + b_{12}x_2 + \dots + b_{1n}x_n)^2 + f_2(x_2,\dots,x_n), \tag{10}$$

где

$$f_2(x_2,\dots,x_n) = f_1(x_2,\dots,x_n) - \frac{1}{b_{11}}(b_{12}x_2 + \dots + b_{1n}x_n)^2$$

— квадратичная форма от $x_2,\dots,x_n$. Рассмотрим квадратичную форму

$$g(y_1,\dots,y_n) = \frac{1}{b_{11}}\,y_1^2 + f_2(y_2,\dots,y_n). \tag{11}$$

Ввиду равенства (10) форма g эквивалентна форме f, так как переводится в нее невырожденной заменой переменных

$$y^{\downarrow} = Cx^{\downarrow}, \quad C = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ 0 & e & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & e \end{pmatrix}, \quad |C| = b_{11} \neq 0. \tag{12}$$

Так как $f_2(y_2,\dots,y_n)$ — форма от $n-1 < m$ переменных, то по предположению индукции существует невырожденная замена переменных

$$\begin{pmatrix} y_2 \\ \dots \\ y_n \end{pmatrix} = C_1 \begin{pmatrix} z_2 \\ \dots \\ z_n \end{pmatrix},$$

переводящая форму f_2 в некоторую каноническую форму

$$d_2z_2^2 + \dots + d_nz_n^2.$$

Отсюда и из равенства (11) следует, что форма g переводится невырожденной заменой переменных

$$\begin{pmatrix} y_1 \\ y_2 \\ \dots \\ y_n \end{pmatrix} = \begin{pmatrix} e & 0 & \dots & 0 \\ 0 & & & \\ \dots & & C_1 & \\ 0 & & & \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \\ \dots \\ z_n \end{pmatrix}$$

в каноническую форму

$$\frac{1}{b_{11}}\,z_1^2 + d_2 z_2^2 + \ldots + d_n z_n^2. \tag{13}$$

Остается заметить, что так как форма g переводится в форму f заменой (12), то f переводится в g заменой $x^{\downarrow} = C^{-1}y^{\downarrow}$ и переводится в каноническую форму (13) невырожденной линейной заменой переменных

$$x^{\downarrow} = C^{-1}\begin{pmatrix} e & 0 & \ldots & 0 \\ 0 & & & \\ \ldots & & C_1 & \\ 0 & & & \end{pmatrix} z^{\downarrow}.$$

2. В равенстве (4) $b_{ii} = 0$ для всех $i \in \overline{1,n}$. Тогда форму f можно записать в виде

$$f(x_1, \ldots, x_n) = \sum_{1 \leqslant i < j \leqslant n} 2b_{ij}x_i x_j,$$

и поскольку $f \neq 0$, в этом представлении хотя бы один из коэффициентов b_{ij} $(i < j)$ отличен от нуля. Для упрощения выкладок допустим, что $b_{12} \neq 0$ (остальные случаи рассматриваются аналогично). Тогда, как нетрудно видеть, невырожденная замена переменных

$$x_1 = y_1 + y_2, \quad x_2 = y_1 - y_2, \quad x_i = y_i, \quad i \in \overline{3,n},$$

переводит форму f в форму

$$g(\vec{y}) = 2b_{12}y_1^2 - 2b_{12}y_2^2 + \sum_{1 \leqslant i < j \leqslant n} 2b'_{ij}y_i y_j.$$

Ввиду условия $b_{12} \neq 0$ форма g удовлетворяет условиям пункта 1 и, как там показано, эквивалентна некоторой канонической форме. Следовательно, той же форме эквивалентна и исходная форма f. $\square$

Замечание 3. Для квадратичных форм над полем P, в котором $2e = 0$, понятие эквивалентности вводится аналогично с помощью определений 3 и 4. Однако для таких форм уже нельзя ввести запись вида (5) с симметричной матрицей B_f, и для них не верна теорема 5. Например, форма $f(x_1, x_2) = x_1x_2$ над полем $P = \mathbb{Z}_2$ не эквивалентна никакой канонической форме в смысле определения 6 (покажите). Более того, любая такая каноническая квадратичная форма $f(\vec{x}) = b_1x_1^2 + \ldots + b_nx_n^2$ над $\mathbb{Z}_2$ эквивалентна форме y_1^2, поскольку $f(\vec{x}) = (b_1x_1 + \ldots + b_nx_n)^2$.

В связи с этим для квадратичных форм над указанными полями понятие канонической формы вводится иначе, более сложно. При этом имеет место

Теорема (Диксон). *Любая квадратичная форма $f(x_1, \ldots, x_n)$ над полем $\mathbb{Z}_2$, отличная от нуля (как многочлен), эквивалентна одной и только одной из следующих форм*:

$$\begin{aligned}
&y_1^2,\\
&y_1y_2 + y_3y_4 + \ldots + y_{2k-1}y_{2k}, && 2k \leqslant n,\\
&y_1y_2 + y_3y_4 + \ldots + y_{2k-1}y_{2k} + y_{2k+1}^2, && 2k+1 \leqslant n,\\
&y_1y_2 + y_3y_4 + \ldots + y_{2k-1}y_{2k} + y_1^2 + y_2^2, && 2k \leqslant n.
\end{aligned}$$

Доказательство этой теоремы выходит за рамки нашего курса.

§ 2. КВАДРАТИЧНЫЕ ФОРМЫ НАД ПОЛЯМИ ДЕЙСТВИТЕЛЬНЫХ И КОМПЛЕКСНЫХ ЧИСЕЛ

1. Над полями $\mathbb{R}$ и $\mathbb{C}$ любая квадратичная форма эквивалентна форме, еще более простой, чем каноническая.

Теорема 6. (а) *Любая ненулевая квадратичная форма $f(x_1, \ldots, x_n)$ над полем $\mathbb{C}$ эквивалентна форме вида*

$$h(z_1, \ldots, z_n) = z_1^2 + \ldots + z_r^2. \tag{14}$$

При этом $r = \operatorname{rang} f$.

(б) *Любая ненулевая квадратичная форма $f(x_1, \ldots, x_n)$ над полем $\mathbb{R}$ эквивалентна форме вида*

$$h(z_1, \ldots, z_n) = z_1^2 + \ldots + z_p^2 - z_{p+1}^2 - \ldots - z_{p+q}^2. \tag{15}$$

При этом $p+q = \operatorname{rang} f$ и в (15) *могут отсутствовать слагаемые со знаком плюс $(p = 0)$ или минус $(q = 0)$.*

□ В силу теоремы 5 форма $f(\vec{x})$ эквивалентна канонической форме

$$g(y_1, \ldots, y_n) = d_1y_1^2 + \ldots + d_ny_n^2, \tag{16}$$

где коэффициенты d_i лежат соответственно в $\mathbb{C}$ или в $\mathbb{R}$.

Если $\operatorname{rang} f = r$, то по утверждению 4 $\operatorname{rang} g = r$ и в (16) имеется ровно r коэффициентов d_i, отличных от нуля. Перенумеровывая, если надо, переменные $y_1, \ldots, y_n$ (что является невырожденной линейной заменой переменных), можно добиться выполнения соотношений

$$d_1 \neq 0, \ \ldots, \ d_r \neq 0, \quad d_{r+1} = \ldots = d_n = 0.$$

В случае (а) в поле $\mathbb{C}$ существуют элементы $c_1, \ldots, c_r$ такие, что $c_i^2 = d_i$, $i \in \overline{1,t}$. Тогда невырожденная замена переменных

$$y_1 = \frac{1}{c_1}\, z_1, \ \ldots, \ y_r = \frac{1}{c_r}\, z_r, \quad y_{r+1} = z_{r+1}, \ \ldots, \ y_n = z_n \tag{17}$$

переводит форму (16) в форму (14).

В случае (б), перенумеровывая, если надо, переменные $y_1, \ldots, y_n$, можно добиться того, что в (16)

$$d_1 > 0, \ \ldots, \ d_p > 0, \quad d_{p+1} < 0, \ \ldots, \ d_{p+q} < 0, \quad d_{p+q+1} = \ldots = d_n = 0,$$

где $p, q \in \mathbb{N}_0$, $p+q = r$. В поле $\mathbb{R}$ можно выбрать элементы $c_1, \ldots, c_r$, удовлетворяющие условиям

$$c_1^2 = d_1, \ \ldots, \ c_p^2 = d_p, \quad c_{p+1}^2 = -d_{p+1}, \ \ldots, \ c_{p+q}^2 = -d_{p+q}.$$

Тогда замена переменных по формуле (17) переводит форму (16) в форму (15). □

Следствие. *Квадратичные формы над полем $\mathbb{C}$ эквивалентны тогда и только тогда, когда их ранги равны.*

Определение 7. Квадратичные формы (14) и (15) называются *нормальными квадратичными формами* соответственно над полями комплексных и действительных чисел.

2. Из теоремы 6(а) следует, что любая квадратичная форма над $\mathbb{C}$ эквивалентна единственной (с точностью до обозначения переменных) нормальной квадратичной форме (определяемой параметром $\operatorname{rang} f$). Аналогичное утверждение верно и для квадратичных форм над $\mathbb{R}$.

Теорема 7 (закон инерции Сильвестра). *Если квадратичная форма над $\mathbb{R}$ $f(\vec{x}) \in \mathbb{R}[x_1, \ldots, x_n]$ эквивалентна двум нормальным формам*:

$$g(y_1, \ldots, y_n) = y_1^2 + \ldots + y_s^2 - y_{s+1}^2 - \ldots - y_{s+t}^2$$

и

$$h(z_1, \ldots, z_n) = z_1^2 + \ldots + z_p^2 - z_{p+1}^2 - \ldots - z_{p+q}^2,$$

то справедливы равенства $p = s$, $q = t$.

□ Поскольку по теореме 6(б) $s + t = \operatorname{rang} f = p + q$, то достаточно доказать, что $s = p$. Предположим, что $s \neq p$, и для определенности $s > p$.

Согласно утверждению 3 формы g и h эквивалентны.

Пусть форма g переводится в форму h невырожденной линейной заменой переменных $y^{\downarrow} = Cz^{\downarrow}$. Тогда по утверждению 2

$$B_h = C^T B_g C. \tag{18}$$

Рассмотрим векторное пространство $L_{\mathbb{R}}$ с базисом $(e_1, \ldots, e_n) = \vec{e}$ и зададим на нем симметричную билинейную функцию Φ, определив ее матрицу Грама равенством

$$\Gamma_\Phi(\vec{e}) = B_g = \operatorname{Diag}(E_s, -E_t, O), \tag{19}$$

где E_k — единичная матрица размеров $k \times k$. Заметим, что система векторов $\vec{u} = (u_1, \ldots, u_n) = \vec{e}C$ также есть базис $L_{\mathbb{R}}$, и в силу леммы 8 главы 17 и равенств (18) и (19) ее матрица Грама относительно функции Φ имеет вид

$$\Gamma_\Phi(\vec{u}) = C^T \Gamma_\Phi(\vec{e}) C = C^T B_g C = B_h = \operatorname{Diag}(E_p, -E_q, O). \tag{20}$$

Рассмотрим в $L_{\mathbb{R}}$ подпространства $K = (e_1, \ldots, e_s)_{\mathbb{R}}$ и $M = (u_{p+1}, \ldots, u_n)_{\mathbb{R}}$. Так как $s > p$, то верны соотношения

$$\dim(K \cap M) = \dim K + \dim M - \dim(K + M) \geqslant s + (n - p) - n = s - p > 0.$$

Следовательно, в пространстве $K \cap M$ содержится ненулевой вектор α.

Но тогда, с одной стороны, так как $\alpha \in K$, то координаты α в базисе $\vec{e}$ имеют вид $\vec{\alpha}_{\vec{e}} = (a_1, \ldots, a_s, 0, \ldots, 0) \neq \vec{0}$, и в силу (19)

$$\Phi(\alpha, \alpha) = \vec{\alpha}_{\vec{e}}\, \Gamma_\Phi(\vec{e})\, \alpha_{\vec{e}}^{\downarrow} = a_1^2 + \ldots + a_s^2 > 0. \tag{21}$$

С другой стороны, так как $\alpha \in M$, то $\vec{\alpha}_{\vec{u}} = (0, \ldots, 0, b_{p+1}, \ldots, b_n)$, и в силу (20)

$$\Phi(\alpha, \alpha) = \vec{\alpha}_{\vec{u}}\, \Gamma_\Phi(\vec{u})\, \alpha_{\vec{u}}^{\downarrow} = -b_{p+1}^2 - \ldots - b_{p+q}^2 \leqslant 0. \tag{22}$$

Противоречивость неравенств (21) и (22) доказывает невозможность условия $s \neq p$. $\square$

Теперь корректно

Определение 8. *Положительным* и *отрицательным индексами инерции* квадратичной формы f над полем $\mathbb{R}$ называются соответственно число p слагаемых с коэффициентом $+1$ и число q слагаемых с коэффициентом -1 в нормальной квадратичной форме (15), эквивалентной f.

Следствие. *Квадратичные формы над полем $\mathbb{R}$ эквивалентны тогда и только тогда, когда совпадают их положительные и отрицательные индексы инерции.*

3. Как видно из доказательства теоремы 7, свойства квадратичных форм тесно связаны со свойствами симметричных билинейных функций.

Определение 9. Говорят, что квадратичная форма $f(x_1, \ldots, x_n)$ над полем P и симметричная билинейная функция Φ на векторном пространстве L_P размерности n *ассоциированы*, если для некоторого базиса $(e_1, \ldots, e_n) = \vec{e}$ пространства L_P выполняется равенство $\Gamma_\Phi(\vec{e}) = B_f$; говорят также, что f и Φ ассоциированы в базисе $\vec{e}$ пространства L_P.

Определение 10. Квадратичная форма $f(x_1, \ldots, x_n)$ над полем действительных чисел $\mathbb{R}$ называется *положительно определенной*, если для любого ненулевого вектора $\vec{a} = (a_1, \ldots, a_n)$ над $\mathbb{R}$ значение формы f на векторе $\vec{a}$, определяемое равенством $f(\vec{a}) = \vec{a}\, B_f\, a^{\downarrow}$, положительно.

Утверждение 8. *Для квадратичной формы $f(x_1, \ldots, x_n)$ над полем $\mathbb{R}$ следующие утверждения равносильны*:

(а) *форма f положительно определена*;

(б) *ассоциированная с f (в произвольном базисе) симметричная билинейная функция Φ на пространстве $L_{\mathbb{R}}$ размерности n есть скалярное произведение*;

(в) *положительный индекс инерции формы f равен n.*

□ Эквивалентность утверждений (а) и (б) доказывается следующим образом. Пусть f и Φ ассоциированы в базисе $\vec{e} = (e_1, \ldots, e_n)$ пространства $L_{\mathbb{R}}$. Тогда для любого вектора $\alpha \in L_{\mathbb{R}}$ верны равенства

$$\Phi(\alpha, \alpha) = \vec{\alpha}_{\vec{e}}\, \Gamma_{\Phi}(\vec{e})\, \alpha_{\vec{e}}^{\downarrow} = \vec{\alpha}_{\vec{e}}\, B_f\, \alpha_{\vec{e}}^{\downarrow} = f(\vec{\alpha}_{\vec{e}}),$$

и поскольку $\{\vec{\alpha}_{\vec{e}}\colon\ \alpha \in L\} = \mathbb{R}^n$, то положительная определенность формы f эквивалентна условию

$$\forall\, \alpha \in L \setminus \theta\colon\ \Phi(\alpha, \alpha) > 0.$$

Доказательство эквивалентности утверждений (а) и (в) основано на том, что условие (а) равносильно положительной определенности нормальной квадратичной формы (15), эквивалентной форме f. Дальнейшая его детализация предоставляется читателю. □

Теорема 9 (Сильвестр). *Квадратичная форма $f(x_1, \ldots, x_n)$ над полем $\mathbb{R}$ положительно определена тогда и только тогда, когда все главные угловые миноры ее матрицы B_f положительны.*

□ Достаточно воспользоваться эквивалентностью пунктов (а) и (б) утверждения 8 и теоремой 11 главы 17. □

4. Как уже было отмечено, теорема 5 переносит результаты, полученные в курсе аналитической геометрии для квадратичных форм от 2-х и 3-х переменных над полем $\mathbb{R}$, на квадратичные формы от n переменных над произвольным полем со свойством (1). Однако в аналитической геометрии были получены результаты более сильные, чем в теореме 5. А именно, там было доказано, что квадратичная форма от 2-х или 3-х переменных может быть переведена в каноническую не просто некоторой невырожденной линейной заменой переменных, а такой заменой, которая соответствует повороту плоскости или пространства (т. е. ортогональному преобразованию). Следующая теорема дает аналогичное усиление результатов теоремы 5 для квадратичных форм от произвольного числа n переменных над $\mathbb{R}$.

Определение 11. Назовем квадратичные формы $f(x_1, \ldots, x_n)$ и $g(y_1, \ldots, y_n)$ над $\mathbb{R}$ *ортогонально эквивалентными*, если существует ортогональная матрица $C \in \mathbb{R}_{n,n}$ такая, что замена переменных $x^{\downarrow} = Cy^{\downarrow}$ переводит форму f в форму g.

Теорема 10. *Любая квадратичная форма $f(x_1, \ldots, x_n)$ над $\mathbb{R}$ ортогонально эквивалентна некоторой канонической квадратичной форме.*

□ Так как B_f — симметричная матрица над $\mathbb{R}$, то по следствию 2 теоремы 11 главы 18 существует ортогональная матрица $C \in \mathbb{R}_{n,n}$ такая, что

$$C^{-1} B_f C = \operatorname{diag}(r_1, \ldots, r_n).$$

Так как $C^{-1} = C^T$, то отсюда ввиду утверждения 2 следует, что замена переменных $x^{\downarrow} = Cy^{\downarrow}$ переводит форму f в каноническую форму $g(y_1, \ldots, y_n) = r_1 y_1^2 + \ldots + r_n y_n^2$. □

Этот результат позволяет доказать следующее важное при решении некоторых прикладных задач утверждение.

Теорема 11 (о паре форм). *Если $f(x_1,\ldots,x_n)$ и $g(x_1,\ldots,x_n)$ — квадратичные формы над $\mathbb{R}$, причем f положительно определена, то существует невырожденная линейная замена переменных, переводящая одновременно f в нормальную, а g — в каноническую форму.*

□ По теореме 6(б) существует невырожденная замена переменных

$$x^{\downarrow} = Uy^{\downarrow}, \tag{23}$$

переводящая f в нормальную форму $f_1(\vec{y})$, которая по утверждению 8 имеет вид $f_1(\vec{y}) = y_1^2 + \ldots + y_n^2$. Та же замена (23) переводит форму $g(\vec{x})$ в некоторую квадратичную форму $g_1(\vec{y})$. По теореме 10 существует ортогональная матрица $C \in \mathbb{R}_{n,n}$ такая, что замена

$$y^{\downarrow} = Cz^{\downarrow} \tag{24}$$

переводит $g_1(\vec{y})$ в каноническую форму. Но замена (24) переводит форму $f_1(\vec{y})$ также в нормальную форму $f_2(\vec{z}) = z_1^2 + \ldots + z_n^2$, так как в силу ортогональности матрицы C

$$B_{f_2} = C^T B_{f_1} C = C^T E C = C^T C = E.$$

Таким образом, замена $x^{\downarrow} = UCz^{\downarrow}$ переводит f в нормальную форму, а g — в каноническую форму. □

ЗАДАЧИ

1. Докажите, что квадратичные формы $f(x_1,\ldots,x_n)$ и $g(y_1,\ldots,y_n)$ над полем P эквивалентны тогда и только тогда, когда на векторном пространстве L_P размерности n существует симметричная билинейная функция Φ, ассоциированная с $f(\vec{x})$ и с $g(\vec{y})$.

2. Покажите, что для квадратичной формы $f(x_1,\ldots,x_n)$ над P и симметричной билинейной функции Φ на пространстве L_P с базисом $\vec{e} = (e_1,\ldots,e_n)$ следующие утверждения эквивалентны:

а) $f(\vec{x})$ и Φ ассоциированы в базисе $\vec{e}$;

б) $\forall\, \alpha, \beta \in L_P:\ \Phi(\alpha,\beta) = \dfrac{1}{2e}\big(f(\vec{\alpha}_{\vec{e}} + \vec{\beta}_{\vec{e}}) - f(\vec{\alpha}_{\vec{e}}) - f(\vec{\beta}_{\vec{e}})\big)$;

в) $\forall\, \alpha \in L_P:\ \Phi(\alpha,\alpha) = f(\vec{\alpha}_{\vec{e}})$.

3. Подсчитайте число классов эквивалентных квадратичных форм от n переменных над полями $\mathbb{C}$ и $\mathbb{R}$ (сначала подсчитайте число классов форм данного ранга $r \in \overline{0,n}$).

4. Квадратичная форма $f(x_1,\ldots,x_n)$ над $\mathbb{R}$ называется *отрицательно определенной*, если для любого $\vec{a} \in \mathbb{R}^n \setminus \vec{0}$ справедливо неравенство $f(\vec{a}) < 0$. Докажите, что для $f(x_1,\ldots,x_n)$ следующие утверждения эквивалентны:

а) f отрицательно определена;

б) отрицательный индекс инерции f равен n;

в) в матрице B_f все главные угловые миноры нечетного порядка отрицательны, а четного порядка — положительны.

5. Докажите, что квадратичные формы $f(x_1, \ldots, x_n)$ и $g(y_1, \ldots, y_n)$ над полем $\mathbb{R}$ ортогонально эквивалентны тогда и только тогда, когда $\chi_{B_f}(x) = \chi_{B_g}(x)$.

6. Докажите, что ортогонально эквивалентная квадратичной форме $f(x_1, \ldots, x_n)$ над $\mathbb{R}$ каноническая квадратичная форма $r_1 y_1^2 + \ldots + r_n y_n^2$ определена однозначно, с точностью до перестановки коэффициентов $r_1, \ldots, r_n$.

7. Пусть P — конечное поле из q элементов, q нечетно, и ω — циклический образующий группы P^*. Докажите, что любая квадратичная форма $f(x_1, \ldots, x_n)$ над P эквивалентна канонической форме вида

$$g(\vec{y}) = y_1^2 + \ldots + y_s^2 + \omega y_{s+1}^2 + \ldots + \omega y_{s+t}^2, \quad s, t \in \overline{0, n}, \quad s + t \leqslant n.$$

Выведите отсюда верхнюю оценку числа классов эквивалентных квадратичных форм в $P[x_1, \ldots, x_n]$.

8. Докажите, что над полем $\mathbb{Z}_3$ форма $f(\vec{x}) = x_1^2 + x_2^2$ эквивалентна форме $2y_1^2 + 2y_2^2$ (этот пример доказывает, что в условиях предыдущей задачи параметры s и t в форме $g(\vec{y})$, эквивалентной $f(\vec{x})$, определены неоднозначно).

9. В условиях задачи 7 докажите, что форма $f(\vec{x}) = x_1^2 + x_2^2$ не эквивалентна форме $g(\vec{y}) = y_1^2 + \omega y_2^2$. (Предположив, что $f(\vec{x})$ переводится в $g(\vec{y})$ невырожденной заменой $x^{\downarrow} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} y^{\downarrow}$, покажите, что выполняется одно из противоречивых соотношений: $\omega a^2 = d^2$, где $a \neq 0$, или $\omega = b^2$.)

10. Квадратичная форма $f(x_1, \ldots, x_n)$ над полем P называется *распадающейся*, если она представима в виде произведения двух линейных форм:

$$f(\vec{x}) = (a_1 x_1 + \ldots + a_n x_n) \cdot (b_1 x_1 + \ldots + b_n x_n).$$

Докажите, что

а) если форма f распадается, то $\operatorname{rang} f \leqslant 2$;

б) форма f над полем $\mathbb{C}$ распадается тогда и только тогда, когда $\operatorname{rang} f \leqslant 2$;

в) форма f над полем $\mathbb{R}$ распадается тогда и только тогда, когда либо $\operatorname{rang} f \leqslant 1$, либо $\operatorname{rang} f = 2$ и положительный индекс инерции f равен отрицательному индексу инерции (т. е. $f \sim y_1^2 - y_2^2$).

Глава 20

ЭЛЕМЕНТЫ ТЕОРИИ КОЛЕЦ

В предыдущих главах достаточно подробно были изучены кольцо целых чисел, кольца вычетов, кольца матриц и кольца многочленов. В этой главе будут изложены основы общей теории колец.

§ 1. ПОДКОЛЬЦА И ОПЕРАЦИИ НАД НИМИ

Аналогом понятия подгруппы в группе является понятие подкольца в кольце. Напомним (см. определение 19 главы 3), что непустое подмножество S кольца R называют *подкольцом*, если оно замкнуто относительно операций сложения и умножения, заданных на R, и само является кольцом относительно этих операций (обозначение: $S < (R, +, \cdot)$ или $S < R$).

С примерами подколец читатель уже неоднократно встречался. Заметим, что во всяком кольце R, отличном от нуля, имеется, по крайней мере, два подкольца — нулевое и само кольцо R. Эти подкольца называют *несобственными*, а все остальные подкольца кольца R называют *собственными*.

Для того чтобы, пользуясь определением, узнать, является ли данное подмножество S кольца R подкольцом, нужно проверить для S условие замкнутости относительно операций сложения и умножения и все аксиомы кольца. В действительности, проверка того, что S является подкольцом, более проста.

Утверждение 1. *Непустое подмножество S кольца R является подкольцом тогда и только тогда, когда выполнены условия*:

$$\begin{aligned} &\forall\, s_1, s_2 \in S\ (s_1 - s_2 \in S), \\ &\forall\, s_1, s_2 \in S\ (s_1 s_2 \in S), \end{aligned} \tag{1}$$

т. е. когда S — подгруппа группы $(R, +)$ и подполугруппа полугруппы $(R, \cdot)$.

□ Если S — подкольцо кольца R, то по определению кольца выполнены условия (1).

Обратно, пусть выполнены условия (1). В силу первого из них S — подгруппа группы $(R, +)$ (см. утверждение 6 главы 11) и, в частности, множество S замкнуто относительно операции сложения. Второе из условий (1) означает замкнутость S относительно операции умножения. В силу определения 1 главы 10 S — подполугруппа полугруппы $(R, \cdot)$.

Так как в кольце R справедливы законы дистрибутивности умножения относительно сложения, то эти законы выполнены и в S. Значит, $(S,+,\cdot)$ — кольцо. □

Пример 1. Опишем все подкольца кольца $\mathbb{Z}$. Ввиду результатов § 3 главы 11 все подгруппы группы $(\mathbb{Z},+)$ исчерпываются множествами $m\mathbb{Z}$, $m\in\mathbb{N}_0$. Так как каждое из этих множеств удовлетворяет условиям (1), то это — все подкольца кольца $\mathbb{Z}$.

Если R — конечное кольцо, то проверку того, является ли его подмножество подкольцом, можно еще упростить.

Утверждение 2. *Непустое подмножество S конечного кольца R является подкольцом тогда и только тогда, когда S замкнуто относительно операций сложения и умножения, заданных на R.*

□ Условие

$$\forall\, s_1, s_2 \in S\ (s_1+s_2\in S)$$

в силу конечности группы $(R,+)$ равносильно тому, что S — ее подгруппа (см. следствие 1 утверждения 6 главы 11). Остается применить утверждение 1. □

Для подколец, так же как и для подгрупп, имеет место следующее утверждение (докажите его в качестве упражнения).

Утверждение 3. *Если S — подкольцо кольца R, а T — подкольцо кольца S, то T — подкольцо кольца R, т. е. отношение «быть подкольцом» транзитивно на любом множестве колец.*

Если S — подкольцо кольца R, то нулевые элементы 0_S и 0_R этих колец совпадают (как нейтральные элементы группы $(R,+)$ и ее подгруппы $(S,+)$). Вопрос же о единице подкольца S кольца R с единицей e_R решается не однозначно. А именно, S может не иметь единицы, может иметь единицу $e_S=e_R$ и может иметь единицу $e_S\neq e_R$.

Пример 2. Указанные выше три ситуации осуществляются, например, для кольца матриц $\mathbb{R}_{2,2}$ и его подколец

$$S_1=\left\{\begin{pmatrix} a & b\\ 0 & 0\end{pmatrix}\Big|\ a,b\in\mathbb{R}\right\},\quad S_2=\left\{\begin{pmatrix} a & 0\\ 0 & b\end{pmatrix}\Big|\ a,b\in\mathbb{R}\right\},\quad S_3=\left\{\begin{pmatrix} a & 0\\ 0 & 0\end{pmatrix}\Big|\ a\in\mathbb{R}\right\}.$$

Рассмотрим случай, когда R — кольцо без делителей нуля.

Утверждение 4. *Если R — кольцо без делителей нуля с единицей e_R и S — его ненулевое подкольцо с единицей e_S, то $e_S=e_R$.*

□ Так как e_R — единица кольца R и $e_S\in R$, то $e_Se_R=e_S$. Поскольку e_S — единица кольца S, то $e_Se_S=e_S$. Тогда $e_Se_R=e_Se_S$ и $e_S(e_R-e_S)=0$. Так как $e_S\neq 0$ и в R нет делителей нуля, то $e_S=e_R$. □

Кольцо, не имеющее делителей нуля, может не содержать единицу. Например, таковым является кольцо $2\mathbb{Z}$. Если же R — конечное кольцо, то наличие хотя бы одного ненулевого элемента, не являющегося делителем нуля, обеспечивает существование в R единицы.

Утверждение 5. *Пусть R — конечное кольцо, содержащее элемент $a \neq 0$, не являющийся делителем нуля. Тогда R — кольцо с единицей, и любой элемент из $R \setminus \{0\}$, не являющийся делителем нуля, обратим.*

□ Если $c, b \in R$ и $ca = ba$, то $(c - b)a = 0$ и $c = b$, так как элемент a не является делителем нуля. Значит, все элементы из $Ra = \{ra\colon r \in R\}$ различны. Тогда $|Ra| = |R|$, и ввиду конечности множества R имеем $Ra = R$. Аналогично показываем, что $aR = R$.

Из равенства $Ra = R$ следует, что существует такой элемент $e_1 \in R$, что $e_1 a = a$. Пусть b — произвольный элемент кольца R. Обозначим $c = be_1$. Тогда верны равенства $ca = be_1 a = ba$ и, следовательно, $c = b$. Таким образом, $be_1 = b$ для любого элемента $b \in R$. Аналогично, из равенства $aR = R$ выводим существование такого элемента $e_2 \in R$, что $e_2 b = b$ для любого $b \in R$. Тогда $e_1 = e_2 e_1 = e_2$, и R — кольцо с единицей $e = e_1 = e_2$.

Для любого элемента $d \in R \setminus \{0\}$, не являющегося делителем нуля, как и выше, показываем, что $dR = Rd = R$. По утверждению 10 главы 3 тогда $d \in R^*$. □

Следствие. *Конечное ненулевое коммутативное кольцо R является полем тогда и только тогда, когда в R нет делителей нуля.*

Рассмотрим некоторые операции над подкольцами данного кольца. Так как подкольца A и B кольца R являются, в частности, подгруппами абелевой группы $(R, +)$, то их сумма $A + B = \{a + b\colon a \in A, b \in B\}$ есть подгруппа группы $(R, +)$. Однако, эта сумма может не быть подкольцом.

Пример 3. В кольце матриц $P_{2,2}$ над полем P рассмотрим подкольца

$$A = \left\{ \begin{pmatrix} 0 & 0 \\ a & 0 \end{pmatrix} \,\middle|\, a \in P \right\} \quad \text{и} \quad B = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \,\middle|\, b \in P \right\}.$$

Множество $A + B = \left\{ \begin{pmatrix} 0 & b \\ a & 0 \end{pmatrix} \right\}$ не замкнуто относительно умножения: при условии $ab \neq 0$ верно соотношение $\begin{pmatrix} 0 & 0 \\ a & 0 \end{pmatrix} \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & ab \end{pmatrix} \notin A + B$. Значит, $A + B$ — не подкольцо кольца $P_{2,2}$.

В § 3 будут указаны условия, при которых сумма подколец является подкольцом.

Рассмотрим теперь пересечение подколец данного кольца.

Утверждение 6. *Если $\{S_\alpha\colon \alpha \in A\}$ — произвольное семейство подколец кольца R, то $T = \bigcap\limits_{\alpha \in A} S_\alpha$ — подкольцо кольца R.*

□ Доказательство проводится с использованием утверждения 1 и предоставляется читателю. □

Утверждение 6 показывает, что корректно

Определение 1. Пусть S — подмножество кольца R. *Подкольцом* кольца R, *порожденным подмножеством* S, называют пересечение всех подколец кольца R, содержащих S (обозначение: $[S]_R$).

По аналогии с соответствующими утверждениями для подполугрупп и подгрупп (см., например, теорему 8 главы 11) докажем

Утверждение 7. *Если S — непустое подмножество кольца R, то $[S]_R$ есть множество всех элементов кольца R, имеющих вид*

$$r = \sum_{i=1}^{n} a_i s_{1i} \dots s_{k_i i}, \quad \text{где} \quad n \in \mathbb{N},\ a_i \in \mathbb{Z},\ k_i \in \mathbb{N},\ s_{ti} \in S. \tag{2}$$

□ Обозначим через T множество всех элементов кольца R, имеющих вид (2). Так как $[S]_R$ — подкольцо кольца R, содержащее S, то $[S]_R \supset T$.

Поскольку разность и произведение любых двух элементов из T являются элементами из T, то по утверждению 1 T — подкольцо кольца R. Ясно, что $T \supset S$. Тогда по определению 1 $T \supset [S]_R$ и, стало быть, $T = [S]_R$. □

Пример 4. Если $a \in R$, то $[a]_R$ — множество всех элементов вида

$$c_1 a + \dots + c_n a^n, \quad n \in \mathbb{N}, \quad c_i \in \mathbb{Z}.$$

§ 2. ХАРАКТЕРИСТИКА КОЛЬЦА

Введем для колец понятие, тесно связанное с понятием экспоненты группы.

Определение 2. *Характеристикой кольца R* называют такое наименьшее $t \in \mathbb{N}$, что

$$\forall\, r \in R\ (tr = 0),$$

если такие числа t существуют. В противном случае говорят, что кольцо R имеет *нулевую характеристику*. Пишут: $\operatorname{Char} R = t$, $\operatorname{Char} R = 0$.

Ясно, что если $\exp(R, +) < \infty$, то характеристика кольца совпадает с экспонентой группы $(R, +)$ (см. определение 5 главы 11).

Пример 5. $\operatorname{Char} \mathbb{Z} = 0$; $\operatorname{Char} \mathbb{Z}/n = n$.

Если $r \in R$, то через $\operatorname{ord} r$ будем обозначать порядок r как элемента группы $(R, +)$ (*аддитивный порядок* элемента r).

Утверждение 8. *Пусть R — кольцо с единицей e. Тогда*

$$\operatorname{Char} R = \begin{cases} \operatorname{ord} e, & \text{если} \quad \operatorname{ord} e < \infty, \\ 0, & \text{если} \quad \operatorname{ord} e = \infty. \end{cases}$$

Если, кроме того, R — кольцо без делителей нуля, то либо $\operatorname{Char} R = 0$, либо $\operatorname{Char} R$ — простое число.

□ Для любых $t \in \mathbb{N}$ и $r \in R$ имеем $tr = t(er) = (te)r$. Поэтому если $\operatorname{ord} e = t \in \mathbb{N}$, то $tr = 0$ для любого $r \in R$ и, следовательно, $\operatorname{Char} R \leqslant t$. Кроме того, $\operatorname{ord} e \leqslant \operatorname{Char} R$. Значит, $\operatorname{Char} R = t$. Если же $\operatorname{ord} e = \infty$, то ясно, что $\operatorname{Char} R = 0$.

Пусть теперь в R нет делителей нуля. Если $\operatorname{Char} R = 0$, то доказывать нечего. Пусть $\operatorname{Char} R = n \in \mathbb{N}$. Если $n = n_1 n_2$, где $n_i \in \mathbb{N}$, $1 < n_i < n$, то справедливы равенства $ne = (n_1 n_2)e = (n_1 e)(n_2 e)$. Так как $\operatorname{Char} R = \operatorname{ord} e = n$, то $n_1 e \neq 0$, $n_2 e \neq 0$, и условие $ne = 0$ противоречит тому, что в R нет делителей нуля. Значит, $\operatorname{Char} R$ — простое число. □

Следствие. *Если R — кольцо с единицей и без делителей нуля, а S — его подкольцо с единицей, то* $\operatorname{Char} R = \operatorname{Char} S$.

□ По утверждению 4 $e_S = e_R$. Остается применить утверждение 8. □

Формула разложения бинома $(a + b)^n$ верна для элементов любого коммутативного кольца. Для колец простой характеристики при некоторых показателях n она приобретает особенно простой вид.

Утверждение 9. *Если R — коммутативное кольцо и* $\operatorname{Char} R = p$ *— простое число, то для любых элементов $a, b \in R$ и любого $t \in \mathbb{N}$ справедливо равенство*

$$(a + b)^{p^t} = a^{p^t} + b^{p^t}.$$

□ По аналогии с доказательством теоремы 3 главы 2 можно доказать формулу разложения бинома:

$$(a + b)^p = \sum_{i=0}^{p} C_p^i a^{p-i} b^i.$$

Коэффициент $C_p^i = \dfrac{p(p-1)\dots(p-i+1)}{i!}$ является целым числом. При $1 < i < p$ имеем $(p, i) = 1$. Тогда по свойству взаимно простых чисел $(p, i!) = 1$ и из равенства $i!\, C_p^i = p(p-1)\dots(p-i+1)$ получаем $p \mid C_p^i$, т. е. $C_p^i = pu_i$ для некоторого $u_i \in \mathbb{N}$.

Так как $\operatorname{Char} R = p$, то при $1 < i < p$ имеем $C_p^i a^{p-i} b^i = pu_i a^{p-i} b^i = 0$. Стало быть, $(a + b)^p = a^p + b^p$.

При $t > 1$ утверждение доказывается $(t-1)$-кратным возведением последнего равенства в степень p. □

§ 3. ИДЕАЛЫ И ОПЕРАЦИИ НАД НИМИ

Среди подколец кольца особую роль играют подкольца, называемые идеалами.

Определение 3. *Идеалом* кольца R называют любое его подкольцо I, удовлетворяющее условию

$$\forall\, i \in I,\ \forall\, r \in R\ (ir \in I,\ ri \in I), \tag{3}$$

т. е. выдерживающее умножение на элементы кольца R (обозначение: $I \lhd (R, +, \cdot)$ или $I \lhd R$).

Ясно, что в определении 3 можно вместо подкольца I кольца R рассматривать подгруппу $(I,+)$ группы $(R,+)$, удовлетворяющую условию (3).

Понятие идеала кольца есть аналог понятия нормального делителя группы.

В любом ненулевом кольце R есть, по крайней мере, два идеала — нулевой и само кольцо R. Эти идеалы называют *несобственными*. Все остальные идеалы кольца R называют *собственными* идеалами.

Пример 6. Если R — коммутативное кольцо и $a \in R$, то $aR \lhd R$ (проверьте). В частности, в силу примера 1 все подкольца кольца $\mathbb{Z}$ являются его идеалами.

Имеются кольца, в которых нет собственных идеалов.

Пример 7. Пусть P — поле и $I \lhd P$, $I \neq 0$. Для элемента $i \in I \setminus \{0\}$ в P существует обратный элемент i^{-1}. По условию (3) $e = ii^{-1} \in I$. Тогда для любого элемента $r \in P$ (опять по условию (3)) $r = re \in I$. Стало быть, $P \subset I$ и $P = I$. Таким образом, в поле нет собственных идеалов.

Наиболее типичной является ситуация, когда в кольце R некоторые собственные подкольца являются идеалами, а некоторые — нет.

Пример 8. В кольце многочленов $P[x]$ над полем P подкольца вида $f(x)P[x]$ являются идеалами (см. пример 6), а все ненулевые подкольца, содержащиеся в P, и, в частности само поле P, не являются идеалами.

Заметим, что отношение «быть идеалом» (как и отношение «быть нормальным делителем») не всегда транзитивно на множестве подколец данного кольца (подгрупп данной группы).

Пример 9. В кольце $\mathbb{Z}_4[x]$ подкольцо $2\mathbb{Z}_4[x]$ многочленов, имеющих коэффициенты 0 или 2, является идеалом. Подкольцо $2\mathbb{Z}_4$ является идеалом кольца $2\mathbb{Z}_4[x]$. Однако подкольцо $2\mathbb{Z}_4$ кольца $\mathbb{Z}_4[x]$ не является в нем идеалом (проверьте).

Рассмотрим операции над идеалами и подкольцами.

Утверждение 10. *Если I — идеал, а L — подкольцо кольца R, то*

(а) *$I + L$ — подкольцо кольца R,*

(б) *$I \cap L$ — идеал кольца L.*

□ (а) Ясно, что $I + L$ — подгруппа группы $(R,+)$. Пусть $i_1 + l_1$, $i_2 + l_2 \in I + L$. Так как справедливы равенства

$$(i_1 + l_1)(i_2 + l_2) = i_1 i_2 + i_1 l_2 + l_1 i_2 + l_1 l_2 = i_3 + l_3,$$

где $i_3 = i_1 i_2 + l_1 i_2 + i_1 l_2 \in I$ и $l_3 = l_1 l_2 \in L$, то по утверждению 1 $I + L$ — подкольцо кольца R.

(б) По утверждению 6 $I \cap L$ — подкольцо кольца R. Так как $I \cap L \subset L$, то $I \cap L$ — подкольцо кольца L. Если $l \in L$ и $i \in I \cap L$, то $il \in L$ и $il \in I$. Значит, $il \in I \cap L$. Аналогично проверяем, что $li \in I \cap L$. Следовательно, $I \cap L$ — идеал кольца L. □

Утверждение 11. *Если I, J — идеалы кольца R, то $I + J$ — идеал кольца R.*

□ По утверждению 10(а) $I + J$ — подкольцо кольца R. Если $i + j \in I + J$ и $r \in R$, то справедливы соотношения $(i + j)r = ir + jr \in I + J$. Аналогично, $r(i + j) \in I + J$. Значит, $I + J$ — идеал кольца R. □

Утверждение 12. *Если $\{I_\alpha : \alpha \in A\}$ — произвольное семейство идеалов кольца R, то $T = \bigcap\limits_{\alpha \in A} I_\alpha$ — идеал кольца R.*

Доказательство осуществляется непосредственной проверкой с учетом утверждения 6 и предоставляется читателю.

Из утверждения 12 следует, что корректно

Определение 4. *Идеалом, порожденным подмножеством S* кольца R, называют пересечение всех идеалов кольца R, содержащих S (обозначение: $(S)_R$).

Так как идеал кольца R является его подкольцом, то из определений 4 и 1 следует включение $[S]_R \subset (S)_R$, которое может быть как строгим, так и нестрогим.

Пример 10. Если $a \in \mathbb{Z}$, то $[a]_{\mathbb{Z}} = (a)_{\mathbb{Z}} = a\mathbb{Z}$. В поле $\mathbb{Q}$, очевидно, $[\mathbb{N}]_{\mathbb{Q}} = \mathbb{Z}$ и $(\mathbb{N})_{\mathbb{Q}} = \mathbb{Q}$, а тогда $[\mathbb{N}]_{\mathbb{Q}} \lneqq (\mathbb{N})_{\mathbb{Q}}$.

Утверждение 13. *Если R — коммутативное кольцо с единицей e и S — непустое подмножество из R, то $(S)_R$ есть множество всех элементов вида*

$$r = \sum_{i=1}^{k} s_i r_i, \quad \textit{где} \quad k \in \mathbb{N},\ s_i \in S,\ r_i \in R. \tag{4}$$

□ Обозначим через T множество всех элементов вида (4). Так как идеал $(S)_R$ содержит S, то по определению 3 $(S)_R \supset T$.

Покажем обратное включение. Пусть $r \in R$, $t_1 = \sum_{i=1}^{k} s_i r_i \in T$ и элемент $t_2 = \sum_{j=1}^{l} s'_j r'_j \in T$. Тогда

$$t_1 - t_2 = s_1 r_1 + \ldots + s_k r_k + s'_1(-r'_1) + \ldots + s'_l(-r'_l) \in T.$$

В силу коммутативности кольца R имеем:

$$rt_1 = t_1 r = \sum_{i=1}^{k} s_i (r_i r) \in T.$$

Таким образом, T — идеал кольца R. Поскольку в R есть единица e, и $se = s$ для $s \in S$, то $S \subset T$. Тогда по определению 4 справедливо включение $(S)_R \subset T$. Поэтому, $(S)_R = T$. □

Замечание 1. Обратите внимание на отличие вида (4) элементов идеала $(S)_R$ от вида элементов подгруппы $\langle F\rangle$ группы $(G,+)$, порожденной подмножеством F (теорема 8 главы 11):

$$g=\sum_{i=1}^{k} f_i c_i, \quad \text{где} \quad k\in\mathbb{N}, \quad f_i\in F \quad \text{и} \quad c_i\in\mathbb{Z}\ (!).$$

Определение 5. Идеал I кольца R называют *главным*, если существует такой элемент $s\in R$, что $I=(s)_R$ (говорят, что элемент s порождает идеал I). Коммутативное кольцо R с единицей называют *кольцом главных идеалов*, если все его идеалы главные.

Теорема 14. *Кольцо $\mathbb{Z}$, произвольное поле P и кольцо многочленов $P[x]$ являются кольцами главных идеалов.*

□ По утверждению 13 главный идеал коммутативного кольца R с единицей имеет вид

$$(s)_R=sR. \tag{5}$$

Как показано в примере 6, идеалы кольца $\mathbb{Z}$ имеют вид $m\mathbb{Z}$, $m\in\mathbb{N}_0$, т. е. $\mathbb{Z}$ — кольцо главных идеалов.

Ввиду примера 7 идеалы поля P — это $0=0P$ и $P=eP$, где e — единица поля P. Значит, P — кольцо главных идеалов.

Пусть I — идеал кольца $P[x]$. Если $I=0$, то $I=0P[x]$ — главный идеал. Если $I\neq 0$, то среди его ненулевых элементов возьмем многочлен $i(x)$ наименьшей степени. Покажем, что $I=i(x)P[x]$.

Произвольный многочлен $j(x)\in I$ разделим на $i(x)$ с остатком:

$$j(x)=i(x)q(x)+r(x),\ \deg r(x)<\deg i(x).$$

Так как $r(x)=j(x)-i(x)q(x)$, то $r(x)\in I$. Если $r(x)\neq 0$, то получаем противоречие с выбором элемента $i(x)$. Значит, $r(x)=0$ и $j(x)\in i(x)P[x]$. Стало быть, $I\subset i(x)P[x]$.

Поскольку $i(x)\subset I$, то $i(x)P[x]\subset I$. Итак, $I=i(x)P[x]$, и $P[x]$ — кольцо главных идеалов. □

Из равенства (5) следует, что для многочленов $f(x),g(x)\in P[x]$ включение $f(x)P[x]\subset g(x)P[x]$ справедливо тогда и только тогда, когда $g(x)\mid f(x)$. Поэтому $(f(x))_{P[x]}=(g(x))_{P[x]}$ тогда и только тогда, когда многочлены $f(x)$ и $g(x)$ ассоциированы.

Отсюда получаем

Следствие. *Если $I\lhd P[x]$ и $I\neq 0$, то существует единственный унитарный многочлен, порождающий идеал I.*

□ Если $I=(f(x))_{P[x]}$ и $f^*(x)$ — ассоциированный с $f(x)$ унитарный многочлен, то $I=(f^*(x))_{P[x]}$. Остается заметить, что ассоциированные унитарные многочлены равны. □

Заметим, что не всякое коммутативное кольцо с единицей является кольцом главных идеалов.

Пример 11. В кольце $\mathbb{Z}_4[x]$ идеал, порожденный множеством $S=\{2,x\}$, не является главным (покажите).

§ 4. ПРОСТЫЕ КОЛЬЦА

По аналогии с определением простой группы введем определение простого кольца.

Определение 6. Кольцо R называют *простым*, если оно ненулевое и в нем нет собственных идеалов.

Согласно примеру 7, произвольное поле является простым кольцом.

Пример 12. Если R — кольцо простого порядка, то оно простое кольцо, так как в группе $(R,+)$ нет даже собственных подгрупп.

Задача описания всех простых колец (как и простых групп) является весьма сложной. Однако она легко решается в классе коммутативных колец.

Теорема 15. *Коммутативное кольцо $R \neq 0$ является простым тогда и только тогда, когда одно поле или кольцо простого порядка с нулевым умножением.*

□ Примеры 7 и 12 показывают, что поля и кольца простого порядка являются простыми кольцами. Пусть R — простое кольцо. Если R — кольцо с нулевым умножением (см. определение 12 главы 3), то группа $(R,+)$ — простая, так как любая ее подгруппа является идеалом кольца R (проверьте). По теореме 44 главы 11 $|R|$ — простое число.

Пусть теперь R — кольцо с ненулевым умножением. Если $r \in R$, то в силу примера 6 $rR \lhd R$. Так как R — простое кольцо, то $rR = 0$ или $rR = R$.

Если $rR = 0$ для любого элемента $r \in R$, то R — кольцо с нулевым умножением, что противоречит условию. Значит, существует такой элемент $r \in R$, что

$$rR = R. \tag{6}$$

Легко проверить, что множество $I = \{g \in R\colon\ rg = 0\}$ — идеал кольца R. Стало быть, $I = R$ или $I = 0$. В первом случае получаем $rR = 0$ вопреки равенству (6). Поэтому $I = 0$, и, следовательно, элемент r не является делителем нуля.

Из равенства (6) следует, что $rx = r$ для некоторого элемента $x \in R$. Пусть $b \in R$ и $xb = c$. Из равенств $rxb = rb = rc$ получаем $r(b - c) = 0$, и, следовательно, $b = c$. Значит, $xb = b$ для любого элемента $b \in R$. Поскольку R — коммутативное кольцо, то $x = e$ — единица кольца R.

Тогда для любого элемента $r \in R\backslash\{0\}$ получаем $rR \neq 0$ и, значит, $rR = R$. Отсюда следует, что существует такой элемент $r' \in R$, что $rr' = e$. Это и означает, что R — поле. □

Следствие 1. *Коммутативное кольцо $R \neq 0$ является полем тогда и только тогда, когда R — простое кольцо с ненулевым умножением.*

Следствие 2. *Коммутативное кольцо R с единицей является полем тогда и только тогда, когда R — простое кольцо.*

Примеры некоммутативных простых колец дает

Утверждение 16. *Если P — поле и $n \in \mathbb{N}$, то кольцо матриц $P_{n,n}$ — простое кольцо.*

□ Пусть I — ненулевой идеал кольца $P_{n,n}$, $A = (a_{i,j})_{n\times n} \in I \setminus \{O_{n\times n}\}$ и $a_{kl} \neq 0$. Тогда для любого $i \in \overline{1,n}$ справедливы соотношения (проверьте):

$$a_{kl}^{-1}E^{(i,i)}(E^{(i,k)}AE^{(l,i)}) = a_{kl}^{-1}E^{(i,i)} \cdot a_{kl}E^{(i,i)} = E^{(i,i)} \in I.$$

Поэтому $E_{n\times n} = E^{(1,1)} + \ldots + E^{(n,n)} \in I$, и, следовательно, $I = P_{n,n}$. □

В классе конечных колец простые кольца описываются утверждением, которое мы приведем без доказательства: *конечное ненулевое кольцо R является простым тогда и только тогда, когда R — либо конечное поле, либо кольцо матриц над конечным полем, либо кольцо простого порядка с нулевым умножением.*

§ 5. КОНГРУЭНЦИИ И ИДЕАЛЫ КОЛЕЦ. ФАКТОРКОЛЬЦА

Напомним, что бинарное отношение ρ на полугруппе $(M, *)$ называют конгруэнцией, если ρ — отношение эквивалентности, согласованное с операцией $*$, т. е. удовлетворяющее условию

$$\forall\, m_1, m_2, m_1', m_2' \in M\ (m_1\,\rho\, m_2,\ m_1'\,\rho\, m_2'\ \Rightarrow\ (m_1 * m_1')\,\rho\,(m_2 * m_2'))$$

(определение 5 главы 10). В главе 11 были рассмотрены конгруэнции на группе и установлена их тесная связь с нормальными делителями этой группы. Рассмотрим аналогичные вопросы для колец.

Определение 7. Бинарное отношение ρ на кольце $(R, +, \cdot)$ называют *конгруэнцией*, если ρ — отношение эквивалентности, согласованное с операциями $+$ и $\cdot$.

Если ρ — конгруэнция на кольце R, то на факторможестве

$$R/\rho = \{[r]_\rho :\ r \in R\},$$

где $[r]_\rho = \{a \in R :\ a\,\rho\, r\}$, определены индуцированные операции (определение 6 главы 10):

$$[a]_\rho + [b]_\rho = [a+b]_\rho, \quad [a_\rho] \cdot [b]_\rho = [ab]_\rho.$$

При этом по следствию утверждения 6 главы 10 $(R/\rho, +)$ — абелева группа и $(R/\rho, \cdot)$ — полугруппа.

Утверждение 17. *Если ρ — конгруэнция на кольце $(R, +, \cdot)$, то алгебра $(R/\rho, +, \cdot)$ является кольцом.*

□ В силу сказанного выше остается проверить справедливость законов дистрибутивности. Цепочка равенств

$$([a]_\rho + [b]_\rho) \cdot [c_\rho] = [a+b]_\rho \cdot [c]_\rho = [(a+b)c]_\rho = [ac+bc]_\rho =$$
$$= [ac]_\rho + [bc]_\rho = [a]_\rho \cdot [c]_\rho + [b]_\rho \cdot [c]_\rho$$

доказывает справедливость одного из них. Аналогично проверяется и другой закон дистрибутивности. □

Определение 8. Если ρ — конгруэнция на кольце R, то кольцо R/ρ называют *факторкольцом* кольца R *по конгруэнции* ρ.

Таким образом, по конгруэнциям на кольце R можно строить, исходя из кольца R, новые кольца. Поэтому естественно возникает задача об описании всех конгруэнций на кольце R.

Пример 13. Если $m \in \mathbb{N}$, то по теореме 2 главы 5 отношение $\equiv (m)$ (сравнимости по модулю m) на кольце $\mathbb{Z}$, заданное условием

$$(a \equiv b\,(m)) \;\Leftrightarrow\; (m \mid a-b), \tag{7}$$

является конгруэнцией. Факторкольцо $\mathbb{Z}/\equiv(m)$ — это кольцо вычетов $\mathbb{Z}/m$ кольца $\mathbb{Z}$ по модулю m. Ясно, что условие (7) можно записать в виде

$$(a \equiv b\,(m)) \;\Leftrightarrow\; (a-b \in m\mathbb{Z}).$$

Обратим внимание на то, что $m\mathbb{Z}$ — идеал кольца $\mathbb{Z}$. Как мы сейчас увидим, возникновение в примере 13 идеала $m\mathbb{Z}$, связанного с конгруэнцией $\equiv (m)$, было не случайным.

Определение 9. Пусть I — идеал кольца R. Говорят, что *элементы* $a, b \in R$ *сравнимы по идеалу* I, если $a-b \in I$. При этом пишут $a \equiv b\,(I)$, или $a\,\rho_I\,b$.

Теорема 18. (а) *Если I — идеал кольца R, то отношение сравнимости ρ_I по идеалу I является конгруэнцией на кольце R;*

(б) *Если ρ — конгруэнция на кольце R, то класс $[0]_\rho$ является идеалом кольца R и ρ есть отношение сравнимости по идеалу $I = [0]_\rho$.*

□ (а) Легко проверить, что ρ_I — отношение эквивалентности. Пусть $a \equiv a_1(I)$ и $b \equiv b_1(I)$, т. е. $a-a_1 \in I$ и $b-b_1 \in I$. Соотношения

$$(a-a_1)+(b-b_1) = (a+b)-(a_1+b_1) \in I,$$
$$ab - a_1b_1 = ab - a_1b + a_1b - a_1b_1 = (a-a_1)b + a_1(b-b_1) \in I$$

показывают, что $(a+b) \equiv (a_1+b_1)(I)$ и $ab \equiv a_1b_1(I)$, т. е. ρ_I — конгруэнция.

(б) Пусть $i, j \in [0]_\rho$, т. е. $i\,\rho\,0$ и $j\,\rho\,0$. Так как $(-j)\,\rho\,(-j)$, то $(-j)\,\rho\,0$, $(i-j)\,\rho\,0$ и $i-j \in [0]_\rho$. Значит, $[0]_\rho$ — подгруппа группы $(R,+)$. Если $r \in R$, то справедливы соотношения $r\,\rho\,r$, $(ri)\,\rho\,0$ и $(ir)\,\rho\,0$. Следовательно, $ir, ri \in [0]_\rho$ и $I = [0]_\rho$ — идеал кольца R.

Ясно, что

$$(a\,\rho\,b) \;\Leftrightarrow\; (a-b \in [0]_\rho) \;\Leftrightarrow\; (a \equiv b\,(I)). \quad \square$$

Определение 10. Если I — идеал кольца R, то *факторкольцом кольца по R идеалу I* называют факторкольцо кольца R по конгруэнции $\equiv I$ (или ρ_I). Его обозначают через R/I.

Учитывая результаты главы 11, легко увидеть, что кольцо $(R/I, +, \cdot)$ — это факторгруппа $(R/I, +)$, элементами которой являются смежные классы $a+I$ и на которой операция умножения задана равенством

$$(a + I)(b + I) = ab + I. \tag{8}$$

Утверждение 19. *Если R — коммутативное кольцо (кольцо с единицей e), то для любого идеала I кольца R факторкольцо R/I коммутативно (содержит единицу $e + I$).*

□ Доказательство очевидно в силу равенства (8). □

Замечание 2. Обозначим через $\mathcal{K}(R)$ множество всех конгруэнций на кольце R и через $\mathcal{L}(R)$ — множество всех идеалов кольца R. Зададим следующие отображения $\varphi\colon \mathcal{K}(R) \to \mathcal{L}(R)$ и $\psi\colon \mathcal{L}(R) \to \mathcal{K}(R)$, положив (в обозначениях теоремы 18)

$$\varphi(\rho) = [0]_\rho, \quad \psi(I) = \rho_I,$$

где $\rho \in \mathcal{K}(R)$, $I \in \mathcal{L}(R)$. Тогда по теореме 18

$$(\varphi \circ \psi)(I) = \varphi(\psi(I)) = \varphi(\rho_I) = I, \quad (\psi \circ \varphi)(\rho) = \psi(\varphi(\rho)) = \psi(I) = \rho.$$

Значит, $\varphi \circ \psi = \varepsilon_{\mathcal{L}(R)}$ и $\psi \circ \varphi = \varepsilon_{\mathcal{K}(R)}$. По утверждению 4 главы 1 φ и ψ — биекции. Таким образом, существует взаимно однозначное соответствие между множествами $\mathcal{K}(R)$ и $\mathcal{L}(R)$.

Теорема 18, в частности, позволяет описать все конгруэнции на кольцах $\mathbb{Z}$ и $P[x]$, где P — поле.

Пример 14. По теореме 14 все идеалы колец $\mathbb{Z}$ и $P[x]$ имеют вид, соответственно, $m\mathbb{Z} = (m)_{\mathbb{Z}}$, где $m \in \mathbb{N}_0$, и $f(x)P[x] = (f(x))_{P[x]}$, где $f(x) \in P[x]$. По определению 10 факторкольца колец $\mathbb{Z}$ и $P[x]$ имеют вид $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/(m)_{\mathbb{Z}} = \mathbb{Z}/m$ и $P[x]/f(x)P[x] = P[x]/(f(x))_{P[x]}$.

Кольцо вычетов $\mathbb{Z}/m$ было подробно изучено в главе 5. Кольцо $P[x]/f(x)P[x]$ также принято называть *кольцом вычетов* кольца $P[x]$ по модулю $f(x)$ и обозначать через $P[x]/f(x)$. Рассмотрим подробнее это кольцо.

По определению 10 элементами кольца $P[x]/f(x)$ являются классы $[a(x)]_{f(x)} = a(x) + f(x)P[x]$.

Если $f(x) = 0$, то $P[x]/0 \cong P[x]$, поскольку $a(x) - b(x) \in 0 \cdot P[x]$ тогда и только тогда, когда $a(x) = b(x)$.

Пусть $f(x) = f \in P \setminus \{0\}$. Тогда $f \cdot P[x] = P[x]$, и для любых многочленов $a(x)$ и $b(x)$ справедливо соотношение $a(x) - b(x) \in f \cdot P[x]$. Значит, $P[x]/f = [0]_f$ — кольцо из одного элемента.

Пусть теперь $\deg f(x) = n > 0$. Произвольный многочлен $b(x) \in P[x]$ разделим на $f(x)$ с остатком: $b(x) = f(x)q(x) + r(x)$, $\deg r(x) < n$. Тогда

$$b(x) - r(x) = f(x)q(x) \in f(x)P[x].$$

Это означает, что в любом классе $[b(x)]_{f(x)} \in P[x]/f(x)$ содержится многочлен, имеющий степень строго меньшую, чем $n = \deg f(x)$. Более того, в классе $[b(x)]_{f(x)}$ такой многочлен только один, поскольку разность двух различных (!) многочленов, имеющих степени, меньшие n, не делится на $f(x)$. Таким образом, при условии $\deg f(x) = n > 0$ множество $P[x]/f(x)$ описывается следующим образом:

$$P[x]/f(x) = \left\{[a_0 + a_1x + \ldots + a_{n-1}x^{n-1}]_{f(x)} :\ a_i \in P,\ i \in \overline{0, n-1}\right\}. \tag{9}$$

В частности, если $|P| < \infty$, то $|P[x]/f(x)| = |P|^n$.

Изложенная выше конструкция построения новых колец как факторколец данного кольца позволяет указать и способы построения полей. Напомним, что в главе 5 было построено поле $\mathbb{Z}/p$, где p — простое число.

Утверждение 20. *Если P — поле, $f(x) \in P[x]$ и $\deg f(x) > 0$, то равносильны утверждения*:

(а) *многочлен $f(x)$ неприводим над P*;

(б) *$P[x]/f(x)$ — поле.*

□ (а)⇒(б) Пусть $[a(x)]_{f(x)} \in P[x]/f(x)$ и $[a(x)]_{f(x)} \neq [0]_{f(x)}$. В силу (9) можно считать, что $\deg a(x) < \deg f(x)$. Поэтому $f(x) \nmid a(x)$. Тогда по свойству неприводимых многочленов $(f(x), a(x)) = e$. Значит, для некоторых многочленов $u(x), v(x) \in P[x]$ справедливо равенство $u(x)f(x) + v(x)a(x) = e$. Поэтому в кольце $P[x]/f(x)$ справедливы равенства:

$$[u(x)f(x) + v(x)a(x)]_{f(x)} = [u(x)]_{f(x)}[f(x)]_{f(x)} + [v(x)]_{f(x)}[a(x)]_{f(x)} = [e]_{f(x)}.$$

Поскольку $[f(x)]_{f(x)} = [0]_{f(x)}$, то $[v(x)]_{f(x)}[a(x)]_{f(x)} = [e]_{f(x)}$, и, следовательно, $[v(x)]_{f(x)} = [a(x)]^{-1}_{f(x)}$. Стало быть, $P[x]/f(x)$ — поле.

(б)⇒(а) Предположим, что $f(x) = g(x)h(x)$, где $g(x), h(x) \in P[x]$ и $0 < \deg g(x)$, $\deg h(x) < \deg f(x)$. Тогда в кольце $P[x]/f(x)$ справедливы соотношения

$$[0]_{f(x)} = [f(x)]_{f(x)} = [g(x)]_{f(x)}[h(x)]_{f(x)},$$

$[g(x)]_{f(x)} \neq [0]_{f(x)}$, $[h(x)]_{f(x)} \neq [0]_{f(x)}$, противоречащие условию (б). Значит, многочлен $f(x)$ неприводим над полем P. □

Утверждение 20 позволяет получать поля с числом элементов p^t, где p — простое число и $t \in \mathbb{N}$. Действительно, если $P = \mathbb{Z}/p$ и $f(x)$ — неприводимый над P многочлен степени t, то в силу равенства (9) число элементов в поле $P[x]/f(x)$ равно p^t.

Пример 15. Многочлен $f(x) = x^2 + x + e \in \mathbb{Z}/2[x]$ неприводим над полем $\mathbb{Z}/2$. Поэтому поле $\mathbb{Z}/2[x]/f(x)$ состоит из четырех элементов. В силу равенства (9)

$$\mathbb{Z}/2[x]/f(x) = \left\{[0]_{f(x)},\ [e]_{f(x)},\ [x]_{f(x)},\ [x+e]_{f(x)}\right\}.$$

Выпишите таблицы сложения и умножения в этом поле.

§ 6. ГОМОМОРФИЗМЫ КОЛЕЦ

Согласно определению 4 главы 10 *гомоморфизм* φ кольца $(R,+,\cdot)$ в кольцо $(L,+,\cdot)$ — это такое отображение $\varphi\colon R\to L$, при котором для любой операции $*\in\{+,\cdot\}$ выполнено условие

$$\forall\, a,b\in R\colon\ \varphi(a*b)=\varphi(a)*\varphi(b).$$

В главах 10 и 11 было показано, что всякий эпиморфизм полугрупп и групп сводится к некоторому естественному эпиморфизму и некоторому изоморфизму. Рассмотрим соответствующую ситуацию для колец.

Из утверждения 6 главы 10 и следствия утверждения 5 главы 10 получаем

Утверждение 21. *Если ρ — конгруэнция на кольце R, то отображение*

$$\varphi_0\colon R\to R/\rho,$$

определенное равенством $\varphi_0(r)=[r]_\rho$, $r\in R$, является эпиморфизмом колец.

Определение 11. Эпиморфизм φ_0, определенный в утверждении 21, называют *естественным эпиморфизмом* кольца R на факторкольцо R/ρ.

Если I — идеал кольца R, то по определению 10 $R/I=R/\rho_I$. Поэтому отображение $\psi\colon R\to R/I$, при котором $\psi(r)=r+I=[r]_{\rho_I}$, является естественным эпиморфизмом.

Для произвольного гомоморфизма колец $\varphi\colon R\to L$ обозначим

$$\operatorname{Ker}\varphi=\{r\in R\colon\ \varphi(r)=0_L\}$$

и назовем $\operatorname{Ker}\varphi$ *ядром гомоморфизма* φ.

Утверждение 22. *Если $\varphi\colon R\to L$ — гомоморфизм колец, то $\operatorname{Ker}\varphi$ — идеал кольца R. При этом φ — мономорфизм тогда и только тогда, когда $\operatorname{Ker}\varphi=0_R$.*

□ Ясно, что $\operatorname{Ker}\varphi$ совпадает с ядром гомоморфизма групп

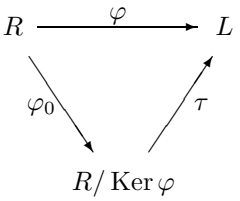
$$\varphi\colon (R,+)\to(L,+).$$

По теореме 38 главы 11 $\operatorname{Ker}\varphi$ — подгруппа группы $(R,+)$. Пусть $a\in\operatorname{Ker}\varphi$ и $r\in R$. Тогда $\varphi(ar)=\varphi(a)\varphi(r)=0_L\varphi(r)=0_L$. Значит, $ar\in\operatorname{Ker}\varphi$. Аналогично показываем, что $ra\in\operatorname{Ker}\varphi$. Следовательно, $\operatorname{Ker}\varphi$ — идеал кольца R.

Второе утверждение теоремы справедливо ввиду следствия теоремы 38 главы 11. □

Теорема 23 (об эпиморфизме колец). *Если $\varphi\colon R\to L$ — эпиморфизм колец, то $R/\operatorname{Ker}\varphi\cong L$ и существует изоморфизм колец $\tau\colon R/\operatorname{Ker}\varphi\to L$, при котором*

коммутативна диаграмма



где φ_0 — естественный эпиморфизм.

□ Доказательство теоремы 23 получается непосредственно из доказательств теорем об эпиморфизме полугрупп и групп (см. теоремы 7 главы 10 и 39 главы 11). Достаточно лишь учесть, что отношение сравнимости по ядру $\operatorname{Ker}\varphi$ на кольце R совпадает с используемой в полугруппах и группах сравнимостью по конгруэнции ρ, и заметить, что построенный в теореме 39 главы 11 изоморфизм групп $\tau\colon R/\operatorname{Ker}\varphi \to L$ является в рассматриваемом случае изоморфизмом колец. □

Следующие теоремы аналогичны соответствующим теоремам для групп.

Теорема 24 (об образах и полных прообразах). *Пусть $\varphi\colon R \to L$ — гомоморфизм колец. Тогда справедливы утверждения*:

(а) *если A — подкольцо кольца R, то $\varphi(A)$ — подкольцо кольца L и $\varphi^{-1}(\varphi(A)) = A + \operatorname{Ker}\varphi$;*

(б) *если B — подкольцо кольца L, то $\varphi^{-1}(B)$ — подкольцо кольца R, $\varphi^{-1}(B) \supset \operatorname{Ker}\varphi$ и $\varphi(\varphi^{-1}(B)) = B \cap \varphi(R)$;*

(в) *если J — идеал кольца L, то $\varphi^{-1}(J)$ — идеал кольца R;*

(г) *если I — идеал кольца R, то $\varphi(I)$ — идеал кольца $\varphi(R)$.*

При условии теоремы 24 обозначим через $\Pi_\varphi(R)$ множество всех подколец кольца R, содержащих $\operatorname{Ker}\varphi$, и через $\Pi(L)$ — множество всех подколец кольца L. В силу утверждений (а) и (б) теоремы 24 можно задать отображения $\alpha\colon \Pi_\varphi(R) \to \Pi(L)$ и $\beta\colon \Pi(L) \to \Pi_\varphi(R)$, положив

$$\alpha(A) = \varphi(A), \quad \beta(B) = \varphi^{-1}(B) \tag{10}$$

для $A \in \Pi_\varphi(R)$ и $B \in \Pi(L)$.

Теорема 25 (о соответствии). *Если $\varphi\colon R \to L$ — эпиморфизм колец, то отображения α и β, определенные равенствами* (10)*, суть взаимно обратные биекции. Кроме того, при отображениях α и β сохраняется отношение «быть идеалом» и отношение включения (из $A_1 < A$ следует $\alpha(A_1) < \alpha(A)$, а из $B_1 < B$ следует $\beta(B_1) < \beta(B)$).*

Теорема 26 (первая теорема об изоморфизме). *Если $\varphi\colon R \to L$ — гомоморфизм колец, то для любого подкольца A кольца R справедливо соотношение*

$$A/A \cap \operatorname{Ker}\varphi \cong \varphi(A).$$

Следствие. *Если I — идеал кольца R и A — подкольцо кольца R, то имеет место изоморфизм колец*

$$A + I/I \cong A/A \cap I.$$

Теорема 27 (вторая теорема об изоморфизме). *Если $\varphi\colon R \to L$ — эпиморфизм колец, I — идеал кольца R, то имеет место изоморфизм колец*

$$R/I + \operatorname{Ker}\varphi \cong L/\varphi(I).$$

Следствие. *Если I и J — идеалы кольца R и $I \subset J$, то имеет место изоморфизм колец*

$$R/J \cong (R/I)/(J/I).$$

Доказательство теорем 24–27 и следствий теорем 26 и 27 аналогичны доказательствам соответствующих утверждений для групп (§§ 11, 12 главы 11) и предоставляются читателю.

Рассмотрим пример применения теоремы о соответствии.

Пример 16. Опишем идеалы кольца $\mathbb{Z}/m$. Рассмотрим естественный эпиморфизм $\varphi\colon \mathbb{Z} \to \mathbb{Z}/m$. Ясно, что $\operatorname{Ker}\varphi = m\mathbb{Z}$. Тогда по теореме 25 каждому идеалу кольца $\mathbb{Z}/m$ ставится в соответствие единственный идеал кольца $\mathbb{Z}$, содержащий $m\mathbb{Z}$. А так как включение $m\mathbb{Z} \subset n\mathbb{Z}$ равносильно делимости $n \mid m$, то все идеалы кольца $\mathbb{Z}/m$ исчерпываются его подмножествами вида $n \cdot \mathbb{Z}/m$, где $n \in \mathbb{N}$ и $n \mid m$. В частности, отсюда, учитывая следствие 2 теоремы 15, можно получить известное утверждение: $\mathbb{Z}/m$ — поле тогда и только тогда, когда m — простое число.

В качестве примера применения теоремы об эпиморфизме колец получим результат, который будет использован в следующей главе.

Замечание 3. Если P и F — поля с различными единицами e_P и e_F, то для колец многочленов от одного переменного над P и F следует использовать различные обозначения (например, $P[x]$ и $F[\overline{x}]$, где $x = (0, e_P, 0, \ldots)$ и $\overline{x} = (0, e_F, 0, \ldots)$). Однако чтобы не загромождать формулировки и доказательства лишними символами, мы будем использовать в следующем утверждении обозначения $P[x]$ и $F[x]$. Такие же обозначения будем применять в теоремах 16, 22 главы 21 и теореме 2 главы 22.

Утверждение 28. *Пусть $\sigma\colon P \to F$ — изоморфизм полей, и отображение $\sigma'\colon P[x] \to F[x]$ для любого многочлена $a(x) = \sum_{i=0}^{n} a_i x^i \in P[x]$ определяется равенством*

$$\sigma'(a(x)) = \sum_{i=0}^{n} \sigma(a_i) x^i.$$

Тогда

(а) *σ' — изоморфизм колец*;

(б) *если многочлены $f(x), g(x) \in P[x]$, то $f(x) \mid g(x)$ тогда и только тогда, когда $\sigma'(f(x)) \mid \sigma'(g(x))$; многочлен $g(x)$ неприводим над P тогда и только тогда, когда многочлен $\sigma'(g(x))$ неприводим над F*;

(в) *для любого $f(x) \in P[x]$ имеет место изоморфизм колец*

$$P[x]/f(x) \cong F[x]/\sigma'(f(x)). \tag{11}$$

□ (а) Пусть $f(x) = f_0 + \ldots + f_m x^m$ и $g(x) = g_0 + \ldots + g_l x^l$ — произвольные многочлены из $P[x]$. Очевидно, что $\sigma'(f(x) + g(x)) = \sigma'(f(x)) + \sigma'(g(x))$, т. е. σ' — гомоморфизм относительно операции сложения. Поскольку справедлива цепочка равенств

$$\sigma'(f(x)g(x)) = \sigma'\Bigg(\sum_{i=0}^{m+l}\Bigg(\sum_{j=0}^{i} f_i g_{i-j}\Bigg)x^i\Bigg) =$$
$$= \sum_{i=0}^{m+l}\Bigg(\sum_{j=0}^{i} \sigma(f_i)\,\sigma(g_{i-j})\Bigg)x^i = \sigma'(f(x))\,\sigma'(g(x)),$$

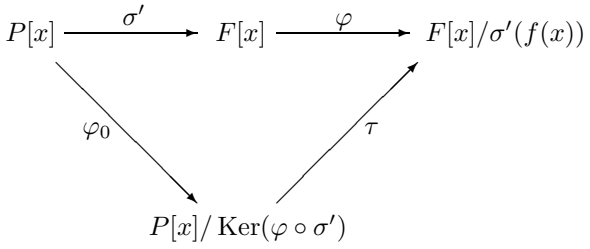
то σ' — гомоморфизм колец. Ясно, что σ' — эпиморфизм и $\operatorname{Ker}\sigma' = 0_P$. Значит, σ' — изоморфизм колец.

(б) Так как σ' — изоморфизм колец, то обратное отображение $(\sigma')^{-1}\colon F[x] \to P[x]$ — также изоморфизм колец. Поэтому справедлива импликация

$$(g(x) = f(x)h(x)) \;\Leftrightarrow\; (\sigma'(g(x)) = \sigma'(f(x))\,\sigma'(h(x))),$$

из которой и следуют утверждения (б).

(в) Пусть $\varphi\colon F[x] \to F[x]/\sigma'(f(x))$ — естественный эпиморфизм. По теореме об эпиморфизме колец, примененной к эпиморфизму $\varphi \circ \sigma'$, имеем коммутативную диаграмму:



где τ — изоморфизм. Так как справедливы равенства

$$(\varphi \circ \sigma')(t(x)) = \varphi\left(\sum \sigma(t_i)x^i\right) = \left[\sum \sigma(t_i)x^i\right]_{\sigma'(f(x))},$$

то $\operatorname{Ker}(\varphi \circ \sigma') = \{t(x) \in P[x]\colon\ \sigma'(f(x)) \mid \sigma'(t(x))\}$. Тогда по утверждению (б)

$$\operatorname{Ker}(\varphi \circ \sigma') = \{t(x) \in P[x]\colon\ f(x) \mid t(x)\} = (f(x))_{P[x]}.$$

Таким образом, τ и есть требуемый изоморфизм (11). □

§ 7. РАЗЛОЖЕНИЕ КОЛЬЦА В ПРЯМУЮ СУММУ

В некоторых случаях изучение кольца можно свести к изучению его собственных идеалов.

Определение 12. Кольцо R называют *разложимым*, если существуют такие его собственные идеалы $I_1, \ldots, I_t$, $t \geqslant 2$, что $R = I_1 + \ldots + I_t$ и сумма $I_1 + \ldots + I_t$ является прямой суммой абелевых групп $(I_s, +)$. В этом случае пишут $R = I_1 \dot{+} \ldots \dot{+} I_t$ и говорят, что кольцо R есть *прямая сумма идеалов* I_s, $s \in \overline{1,t}$. Если же таких идеалов не существует, то кольцо R называют *неразложимым*.

Пример 17. Пусть $R = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle|\ a, b \in P \right\}$, где P — поле. Легко проверить, что $A = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \right\}$ и $B = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & b \end{pmatrix} \right\}$ — идеалы кольца R и $R = A \dot{+} B$.

Пример 18. Всякое простое кольцо неразложимо, так как не имеет собственных идеалов.

Пример 19. Кольцо $\mathbb{Z}$ неразложимо. Оно хотя и имеет собственные идеалы, но любые два таких идеала $m\mathbb{Z}$ и $n\mathbb{Z}$, $m, n \notin \{0, \pm 1\}$, имеют, очевидно, ненулевое пересечение: $m\mathbb{Z} \cap n\mathbb{Z} \supset mn\mathbb{Z} \neq 0$.

Примеры разложимых конечных колец дает

Утверждение 29. *Если R — конечное кольцо и число $|R|$ имеет каноническое разложение $|R| = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, где $k > 1$, то в кольце R существует единственный идеал I_s порядка $|I_s| = p_s^{\alpha_s}$, $s \in \overline{1,k}$, и кольцо R разложимо*:

$$R = I_1 \dot{+} \ldots \dot{+} I_k. \tag{12}$$

□ В абелевой группе $(R, +)$ по теореме 49 главы 11 существует единственная силовская p_s-подгруппа I_s порядка $p_s^{\alpha_s}$. Она имеет вид

$$I_s = \{r \in R \colon\ p_s^{\alpha_s} r = 0\}.$$

Нетрудно увидеть, что $I_s \lhd R$. Остается заметить, что согласно следствию теоремы 49 главы 11 справедливо равенство (12). □

Пусть R — разложимое кольцо и

$$R = I_1 \dot{+} \ldots \dot{+} I_t \tag{13}$$

— его разложение. По определению 15 главы 11 и замечанию 5 главы 11 каждый элемент r кольца R однозначно представим в виде

$$r = i_1 + \ldots + i_t, \tag{14}$$

где $i_s \in I_s$, $s \in \overline{1,t}$. Элементы $i_s \in I_s$ из равенства (14) называют *компонентами элемента* r. Если $r' = i'_1 + \ldots + i'_t$, $i'_s \in I_s$, то $r + r' = (i_1 + i'_1) + \ldots + (i_t + i'_t)$. Кроме того, справедливо также равенство

$$rr' = i_1 i'_1 + i_2 i'_2 + \ldots + i_t i'_t, \tag{15}$$

показывающее, что умножение элементов кольца R производится покомпонентно. Действительно, $rr' = \sum\limits_{s,l=1}^{t} i_s i'_l$. Так как I_s, I_l — идеалы кольца R, то $i_s i'_l \in I_s \cap I_l$. Поскольку сумма $I_1 + \ldots + I_t$ — прямая, то $I_s \cap I_l = 0$ при $s \neq l$. Следовательно, $i_s i'_l = 0$ при $s \neq l$, и справедливо равенство (15).

Таким образом, если R — разложимое кольцо и (13) — его разложение, то изучение кольца R сводится к изучению его собственных идеалов I_s, $s \in \overline{1,t}$, поскольку свойства операций в кольце R определяются свойствами операций в идеалах I_s, $s \in \overline{1,t}$.

Замечание 4. В условиях утверждения 29 компоненты i_s произвольного элемента $r \in R$ могут быть найдены следующим образом. Обозначим $m_s = \dfrac{|R|}{p_s^{\alpha_s}}$, $s \in \overline{1,k}$. Так как $(p_i, p_j) = 1$ при $i \neq j$, то $(m_1, \ldots, m_k) = 1$ (аналогичный факт для многочленов доказан в утверждении 19 главы 9). Поэтому существуют такие $u_1, \ldots, u_k \in \mathbb{Z}$, что $\sum_{i=1}^{k} u_i m_i = 1$. Тогда $i_s = u_s m_s r$ (докажите).

Простейшие свойства разложимого кольца описывает

Теорема 30. *Пусть R — разложимое кольцо и* (13) *— его разложение. Тогда*

(а) *в кольце R есть делители нуля*;

(б) *кольцо R коммутативно тогда и только тогда, когда коммутативно каждое подкольцо I_s, $s \in \overline{1,t}$*;

(в) *R — кольцо с единицей тогда и только тогда, когда каждое кольцо I_s содержит единицу*; *при этом если e — единица кольца R и e_s — единица кольца I_s, $s \in \overline{1,t}$, то $e = e_1 + \ldots + e_t$ и $I_s = e_s R$*;

(г) *если R — кольцо с единицей, то элемент $r = i_1 + \ldots + i_t \in R$, $i_s \in I_s$, обратим в R тогда и только тогда, когда $i_s \in I_s^*$, $s \in \overline{1,t}$.*

□ (а) Если $r_s \in I_s \setminus \{0\}$, $r_l \in I_l \setminus \{0\}$ и $s \neq l$, то $r_s r_l = 0$.

(б) Свойство (б) следует из равенства (15).

(в) Пусть e — единица кольца R. Тогда существуют такие однозначно определенные элементы $a_s \in I_s$, $s \in \overline{1,t}$, что $e = a_1 + \ldots + a_t$. Для любого элемента $b_s \in I_s$ верны равенства $b_s e = b_s a_s = b_s$ и $e b_s = a_s b_s = b_s$, показывающие, что a_s — единица кольца I_s.

Наоборот, если e_s — единица кольца I_s, $s \in \overline{1,t}$, то из равенства (15) следует, что $e_1 + \ldots + e_t$ — единица кольца R. Очевидно, что $e_s R \subset I_s$ и $I_s = e_s I_s \subset e_s R$. Следовательно, $I_s = e_s R$.

(г) Свойство очевидно в силу равенства (15) и свойства (в). □

Замечание 5. Согласно теореме 30 и утверждению 29 всякое конечное коммутативное кольцо R с единицей однозначно разложимо в прямую сумму (12), где I_s — коммутативное кольцо с единицей, имеющее примарный порядок $|I_s| = p_s^{\alpha_s}$, p_s — простое число. К настоящему времени полного описания коммутативных колец примарного порядка (в отличие от примарных абелевых групп) нет.

Приведем теперь конструкцию, аналогичную конструкции внешней прямой суммы абелевых групп.

Пусть $R_1, \ldots, R_k$ — кольца, $k > 1$. На декартовом произведении $R = R_1 \times \ldots \times R_k$ определим операции $+$ и $\cdot$, положив

$$\begin{aligned}(a_1, \ldots, a_k) + (b_1, \ldots, b_k) &= (a_1 + b_1, \ldots, a_k + b_k),\\ (a_1, \ldots, a_k) \cdot (b_1, \ldots, b_k) &= (a_1 b_1, \ldots, a_k b_k).\end{aligned} \tag{16}$$

Теорема 31. *Множество R является кольцом относительно операций, определенных равенствами* (16). *Для каждого $s \in \overline{1,k}$ кольцо R содержит подкольцо $\overline{R}_s$, изоморфное кольцу R_s, и $R = \overline{R}_1 \dotplus \ldots \dotplus \overline{R}_k$.*

□ Тот факт, что алгебра $(R, +, \cdot)$ является кольцом, доказывается непосредственной проверкой.

Обозначим $\overline{R}_s = \{(0, \ldots, 0, b_s, 0, \ldots, 0) : b_s \in R_s\}$, $s \in \overline{1,k}$. Легко проверить, что $\overline{R}_s$ — подкольцо кольца R, изоморфное кольцу R_s при соответствии $b_s \to (0, \ldots, 0, b_s, 0, \ldots, 0)$. Кроме того, $\overline{R}_s \lhd R$ и $R = \overline{R}_1 \dotplus \ldots \dotplus \overline{R}_k$ (проверьте). □

Определение 13. Кольцо R, построенное в теореме 31, называют *внешней прямой суммой колец R_s, $s \in \overline{1,k}$*, и обозначают

$$R = R_1 \oplus \ldots \oplus R_k.$$

Простейшие свойства кольца R в силу разложения $R = \overline{R}_1 \dotplus \ldots \dotplus \overline{R}_k$ и изоморфизма $R_s \cong \overline{R}_s$, $s \in \overline{1,k}$, получаются из теоремы 30.

В качестве важного примера рассмотрим кольца вычетов.

Теорема 32. *Если $n \in \mathbb{N}$, $n = n_1 n_2$, $n_1 > 1$, $n_2 > 1$ и $(n_1, n_2) = 1$, то имеет место изоморфизм колец*

$$\mathbb{Z}/n \cong \mathbb{Z}/n_1 \oplus \mathbb{Z}/n_2.$$

□ Зададим отображение $\varphi\colon \mathbb{Z}/n \to \mathbb{Z}/n_1 \oplus \mathbb{Z}/n_2$, положив $\varphi([a]_n) = ([a]_{n_1}, [a]_{n_2})$. Пусть $* \in \{+, \cdot\}$. Равенства

$$\varphi([a]_n * [b]_n) = \varphi([a * b]_n) = ([a * b]_{n_1}, [a * b]_{n_2}) = ([a]_{n_1} * [b]_{n_1}, [a]_{n_2} * [b]_{n_2}) =$$

$$= ([a]_{n_1}, [a]_{n_2}) * ([b]_{n_1}, [b]_{n_2}) = \varphi([a]_n) * \varphi([b]_n)$$

показывают, что отображение φ является гомоморфизмом колец. Если $([a]_{n_1}, [a]_{n_2}) = ([0]_{n_1}, [0]_{n_2})$, то $a \equiv 0\,(n_1)$, $a \equiv 0\,(n_2)$, и так как $(n_1, n_2) = 1$, то $[a]_n = [0]_n$. Значит, φ инъективно. Поскольку $|\mathbb{Z}/n| = |\mathbb{Z}/n_1 \oplus \mathbb{Z}/n_2|$, то φ — искомый изоморфизм колец. □

Следствие. *Если* $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ *— каноническое разложение числа* $n \in \mathbb{N}$, *то имеет место изоморфизм колец*

$$\mathbb{Z}/n \cong \mathbb{Z}/p_1^{\alpha_1} \oplus \dots \oplus \mathbb{Z}/p_k^{\alpha_k}.$$

В заключение параграфа докажем кольцевой аналог того факта, что конечные циклические группы одинакового порядка изоморфны.

Утверждение 33. *Если* R_1 *и* R_2 *— такие кольца с единицами, что* $|R_1| = |R_2|$ *и* $(R_i, +)$ *— циклические группы, то кольца* R_1 *и* R_2 *изоморфны (в частности, если* $|R_i| = m$, *то* $R_i \cong \mathbb{Z}/m$).

□ По условию $(R_1, +) = \langle a \rangle$ и $(R_2, +) = \langle b \rangle$. Пусть $\operatorname{ord} a = \operatorname{ord} b = t$ и e_i — единица кольца R_i, $i = 1, 2$. Тогда $e_1 = sa$ и $a^2 = ua$ для некоторых $s, u \in \overline{0, t-1}$. Кроме того, из равенств $a = e_1 a = sa \cdot a = sua$ следует, что $su \equiv 1\,(t)$, и поэтому $(s, t) = 1$. Значит, элемент $e_1 = sa$ также порождает группу $(R_1, +)$: $(R_1, +) = \langle e_1 \rangle$, так как $\operatorname{ord} e_1 = |R_1|$ (см. теорему 3 главы 11). Аналогично получаем, что $(R_2, +) = \langle e_2 \rangle$. Следовательно, каждый элемент кольца R_i однозначно представим в виде ke_i, где $k \in \overline{0, t-1}$, $i \in \overline{1, 2}$.

Теперь ясно, что отображение $\varphi\colon R_1 \to R_2$, определенное равенством $\varphi(ke_1) = ke_2$, есть биекция. Для любой операции $* \in \{+, \cdot\}$ при любых $k, l \in \overline{0, t-1}$ выполняется равенство

$$(ke_i) * (le_i) = r_t(k * l)\, e_i,$$

где $r_t(m)$ — остаток от деления m на t. Поэтому нетрудно проверить, что φ — изоморфизм колец. □

§ 8. ЗАМЕНА ПОДКОЛЬЦА ИЗОМОРФНЫМ ЕМУ КОЛЬЦОМ

В предыдущих главах неоднократно встречалась следующая ситуация: имеются кольца A и B, кольцо B содержит подкольцо $\overline{A}$, изоморфное кольцу A, но не содержит самого кольца A, т. е. $A \not\subset B$, но существует мономорфизм $\varphi\colon A \to B$ такой, что $\varphi(A) = \overline{A} < B$. В такой ситуации мы говорили, что будем рассматривать кольцо A как подкольцо кольца B, «отождествляя» элемент $a \in A$ с соответствующим ему элементом $\varphi(a) \in \overline{A}$.

Так было сделано в главе 4, когда каждый элемент a поля $\mathbb{R}$ действительных чисел отождествлялся с элементом $(a, 0)$ поля $\mathbb{C}$ комплексных чисел. При этом было замечено, что отображение $\varphi\colon \mathbb{R} \to \overline{\mathbb{R}} = \{(a, 0)\colon a \in \mathbb{R}\}$, заданное правилом $\varphi(a) = (a, 0)$, является изоморфизмом. Аналогичный прием был использован при построении кольца многочленов $R[x]$ над кольцом R с единицей. Каждый элемент a кольца R отождествлялся с многочленом ax^0 (см. замечание 3 главы 9).

Нестрогость подобных рассуждений очевидна: заменяя часть элементов кольца B элементами кольца A, мы получаем новое множество $C = (B \setminus \varphi(A)) \cup A$, на котором не определены кольцевые операции.

Приведем способ определения операций на множестве C, при котором C превращается в кольцо, изоморфное кольцу B и содержащее A в качестве подкольца.

Утверждение 34. *Пусть* $\varphi\colon A \to B$ *— мономорфизм колец и* $A \cap B = \varnothing$. *Тогда существует такое кольцо* C, *что*

(а) $A < C$;

(б) *существует изоморфизм колец* $\psi\colon C \to B$ *такой, что* $\psi(a) = \varphi(a)$ *для любого* $a \in A$.

□ Пусть $C = (B \setminus \varphi(A)) \cup A$. Зададим отображение $\psi\colon C \to B$ по правилу

$$\psi(c) = \begin{cases} \varphi(c), & \text{если } c \in A, \\ c, & \text{если } c \in C \setminus A. \end{cases}$$

Очевидно, что ψ — биекция. Пусть $*$ — операция сложения или умножения на кольце B. Зададим на C операцию $\overline{*}$, положив

$$\forall\, c_1, c_2 \in C\colon\ c_1 \mathbin{\overline{*}} c_2 = \psi^{-1}(\psi(c_1) * \psi(c_2)). \tag{17}$$

Из равенства (17) следует, что для любых элементов $c_1, c_2 \in C$

$$\psi(c_1 \mathbin{\overline{*}} c_2) = \psi(c_1) * \psi(c_2).$$

Значит, ψ — изоморфизм алгебры $(C, \overline{+}, \overline{\cdot}\,)$ на кольцо $(B, +, \cdot)$. Следовательно, $(C, \overline{+}, \overline{\cdot}\,)$ — кольцо (см. теорему 16 главы 3).

Справедливость утверждений (а) и (б) очевидна. □

Теперь ясно, что при построении поля $\mathbb{C}$ комплексных чисел и кольца многочленов $R[x]$ над кольцом R на самом деле была использована конструкция, указанная в утверждении 34.

ЗАДАЧИ

1. Пусть R — кольцо. Его подмножество

$$C(R) = \{r \in R\colon\ \forall\, a \in R\ (ra = ar)\}$$

называют *центром кольца* R. Покажите, что $C(R)$ — коммутативное подкольцо кольца R.

2. Опишите все подкольца кольца $\mathbb{Z}/m$.

3. Для ненулевого кольца R, содержащего элемент, не являющийся делителем нуля, найдите $C(R_{n,n})$, $n \in \mathbb{N}$.

4. Пусть R — подкольцо коммутативного кольца R', R' — кольцо с единицей e, R — кольцо с единицей $e_R = e$ и $a_1, \ldots, a_n \in R$. Покажите, что

$$[R, a_1, \ldots, a_n] = R[a_1, \ldots, a_n] = \{r' \in R'\colon\ r' = f(a_1, \ldots, a_n),\ f(\vec{x}) \in R[\vec{x}]\}$$

(кольцо $R[a_1, \ldots, a_n]$ введено в § 8 главы 9).

5. Опишите вид элементов идеала $(S)_R$, если R — коммутативное кольцо без единицы и $S \subset R$.

6. Опишите вид элементов идеала $(S)_R$, если R — некоммутативное кольцо с единицей и $S \subset R$.

7. Покажите, что совокупность всех многочленов из кольца $P[x]$, где P — поле, имеющих корнем данный элемент $a \in P$, является идеалом в $P[x]$. Каким элементом из $P[x]$ порождается этот идеал?

8. Покажите, что если R — простое кольцо с единицей, то кольцо матриц $R_{n,n}$ — также простое кольцо. (Покажите, что всякий идеал кольца $R_{n,n}$ имеет вид $V_{n,n}$, где V — некоторый идеал кольца R.)

9. Идеал M кольца R называют *максимальным*, если $M \neq R$ и для любого идеала I кольца R из соотношений $M \subset I \subset R$ следует $I = M$ или $I = R$. Покажите, что если $J \lhd R$ и $J \neq R$, то J — максимальный идеал тогда и только тогда, когда R/J — простое кольцо (используйте теоремы 24 и 25). Если R — коммутативное кольцо с единицей, то J — максимальный идеал тогда и только тогда, когда R/J — поле.

10. Докажите, что факторкольцо кольца главных идеалов является кольцом главных идеалов.

11. Идеал I кольца R называют *простым*, если $I \neq R$ и для любых $a, b \in R$ из $ab \in I$ следует $a \in I$ или $b \in I$. Покажите, что если $J \lhd R$ и $J \neq R$, то J — простой идеал тогда и только тогда, когда R/J — кольцо без делителей нуля.

12. Покажите, что если R — конечное коммутативное кольцо с единицей, то его идеал является максимальным тогда и только тогда, когда он простой. Покажите, что это верно и в случае, когда R — *область целостности*, т. е. кольцо без делителей нуля, являющаяся кольцом главных идеалов.

13. Докажите, что кольцо $\mathbb{Z}/m$ неразложимо тогда и только тогда, когда $m = p^k$, где p — простое число.

14. Пусть I и J — идеалы кольца R. Покажите, что если $I + J = R$, то

$$R/I \cap J \cong R/J \oplus R/I.$$

15. Пусть каноническое разложение многочлена $f(x)$ над полем P имеет вид $f(x) = g_1(x)^{k_1} \dots g_t(x)^{k_t}$. Покажите, что

$$P[x]/f(x) \cong P[x]/g_1(x)^{k_1} \oplus \dots \oplus P[x]/g_t(x)^{k_t}.$$

Укажите разложение кольца $P[x]/f(x)$ в прямую сумму идеалов. Докажите, что $P[x]/f(x)$ — неразложимое кольцо тогда и только тогда, когда $t = 1$.

16. В условиях предыдущей задачи пусть $|P| = q$, $\deg f(x) = m$ и $\deg g_i(x) = m_i$, $i \in \overline{1,t}$. Покажите, что

$$|(P[x]/f(x))^*| = q^m \left(1 - \frac{1}{q^{m_1}}\right) \dots \left(1 - \frac{1}{q^{m_t}}\right)$$

(обратите внимание на то, что $|(P[x]/f(x))^*|$ — это количество таких многочленов $h(x) \in P[x]$, что $(f(x), h(x)) = e$ и $\deg h(x) < \deg f(x)$, т. е. получен аналог формулы для функции Эйлера).

17. Приведите пример разложимого кольца примарного порядка с единицей.

18. Докажите, что идеал I кольца $\mathbb{Z}[x]$ максимален тогда и только тогда, когда $I = (f(x), p)$, где p — простое число, а $f(x) = \sum_{i=0}^{n} a_i x^i$ — такой многочлен, что $\sum_{i=0}^{n} r_p(a_i)x^i$ — неприводимый многочлен в $\mathbb{Z}/p[x]$.

19. Докажите, что идеал I кольца $\mathbb{Z}[x]$ простой тогда и только тогда, когда он либо максимален, либо порождается простым числом, либо порождается примитивным (определение 20 главы 9) неприводимым многочленом из $\mathbb{Z}[x]$.

20. Элемент f кольца R называют *идемпотентом*, если $f^2 = f$. Докажите, что кольцо R с единицей e разложимо тогда и только тогда, когда оно содержит идемпотент f, $f \notin \{0, e\}$ и $f \in C(R)$ (см. задачу 1).

Глава 21

ОСНОВЫ ТЕОРИИ ПОЛЕЙ

Читателю уже известны примеры полей. Это числовые поля $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\{a + b\sqrt{p}\colon\ a, b \in \mathbb{Q}\}$, p — простое число, и нечисловые поля — поля вычетов $\mathbb{Z}/p$ и $P[x]/f(x)$, где p — простое число и $f(x)$ — неприводимый над полем P многочлен. В настоящей главе будут рассмотрены общие свойства полей, классификация полей и строение некоторых из них.

§ 1. ПОДПОЛЯ И РАСШИРЕНИЯ ПОЛЕЙ

Напомним (определение 19 главы 3), что подмножество L поля P называют *подполем*, если L замкнуто относительно операций, заданных на P, и само является полем относительно этих операций.

Пример 1. В любом поле P есть хотя бы одно подполе — само поле P. В поле $\mathbb{C}$ бесконечно много подполей — все числовые поля. В поле $\mathbb{Z}/p$ нет других подполей, кроме него самого, так как в группе $(\mathbb{Z}/p, +)$ нет собственных подгрупп.

Получим критерий того, чтобы подмножество поля было его подполем.

Утверждение 1. *Подмножество L поля P, содержащее хотя бы один ненулевой элемент, является подполем тогда и только тогда, когда выполнены условия*:
(а) $\forall\, l_1, l_2 \in L\colon\ (l_1 - l_2 \in L,\ l_1 l_2 \in L)$;
(б) $\forall\, l \in L \setminus \{0\}\colon\ (l^{-1} \in L)$,
где l^{-1} — элемент, обратный к элементу l в поле P.

□ По утверждению 1 главы 20 условие (а) равносильно тому, что L — подкольцо поля P. Ввиду коммутативности поля P кольцо L коммутативное. Поэтому выполнение дополнительно условия (б) равносильно тому, что L — поле, т. е. тому, что L — подполе поля P (обратные элементы в P и в L к элементу $l \in L$ совпадают по утверждению 5 главы 11, так как $(L \setminus \{0\}, \cdot) < (P \setminus \{0\}, \cdot)$). □

Следствие 1. *Отношение «быть подполем» транзитивно на любом множестве полей.*

Следствие 2. *Пересечение любого семейства подполей поля P является его подполем.*

Доказательство следствий очевидно и предоставляется читателю.

Для конечного подмножества L поля P указанный в утверждении 1 критерий можно существенно упростить.

Утверждение 2. *Конечное подмножество L поля P, содержащее хотя бы один ненулевой элемент, является подполем тогда и только тогда, когда выполнено условие*

$$\forall\, l_1, l_2 \in L:\ \ (l_1 + l_2 \in L,\ l_1 l_2 \in L).$$

□ Справедливость утверждения вытекает из утверждения 1 и следствия 1 утверждения 6 главы 11. □

Определение 1. Поле P называют *простым*, если в нем нет подполей, кроме самого поля P.

Пример 2. В силу примера 1 поле $\mathbb{Z}/p$ простое. Поле $\mathbb{Q}$ также простое. Действительно, пусть T — подполе поля $\mathbb{Q}$. Тогда, по утверждению 4 главы 20, $T \ni 1$, и, следовательно, T содержит любой элемент $m \in \mathbb{Z}$. Если $n \in \mathbb{Z} \setminus \{0\}$, то $T \ni n^{-1} = \dfrac{1}{n}$. Поэтому $T \ni \dfrac{m}{n}$ и $T = \mathbb{Q}$.

Теорема 3. *В любом поле P содержится единственное простое подполе.*

□ Пусть P_0 — пересечение всех подполей поля P. По следствию 2 утверждения 1 P_0 — подполе поля P. В силу следствия 1 утверждения 1 P_0 — простое поле. Если P_0' — какое-либо простое подполе поля P, то $P_0 \subset P_0'$, и, так как P_0' — простое поле, $P_0' = P_0$. □

Определение 2. Если P — подполе поля P', то говорят, что P' — *расширение поля P*.

В частности, по теореме 3 всякое поле является расширением своего простого подполя.

Следствие 2 утверждения 1 показывает, что корректно

Определение 3. Пусть P' — расширение поля P и M — подмножество поля P'. Пересечение всех подполей поля P', содержащих P и M, называют *расширением поля P, порожденным подмножеством M*. Его обозначают через $P(M)$.

Пример 3. В поле $\mathbb{C}$ расширение поля $\mathbb{R}$, порожденное элементом $i \in \mathbb{C}$, совпадает с полем $\mathbb{C}$. Действительно, $\mathbb{R}(i)$ — подполе поля $\mathbb{C}$, содержащее $\mathbb{R}$ и i. Поэтому $\mathbb{R}(i)$ содержит все элементы вида $a + bi$, где $a, b \in \mathbb{R}$. Значит, $\mathbb{R}(i) = \mathbb{C}$.

Рассмотрим некоторые свойства расширений полей.

Утверждение 4. *Если P' — расширение поля P, а L, M, T — подмножества поля P' и $L \supset T$, то*

(а) $P(L) \supset P(T)$;

(б) $P(L \cup M) = P(L)(M)$.

□ (а) По определению 3 $P(L)$ — подполе поля P', содержащее P и L. Тогда по условию $P(L)$ содержит P и T. Поэтому $P(L)$ содержит пересечение $P(T)$ всех подполей поля P', содержащих P и T.

(б) По определению 3 $P(L\cup M)$ — пересечение всех подполей поля P', содержащих P, L и M, а $P(L)(M)$ — некоторое подполе поля P', содержащее P, L и M. Значит,

$$P(L)(M) \supset P(L \cup M). \tag{1}$$

По определению 3 $P(L)(M)$ — пересечение всех подполей поля P', содержащих $P(L)$ и M. По утверждению (а) $P(L \cup M) \supset P(L)$. Ясно, что $P(L \cup M) \supset M$. Следовательно, $P(L \cup M)$ — некоторое подполе поля P', содержащее $P(L)$ и M. Поэтому

$$P(L)(M) \subset P(L \cup M). \tag{2}$$

Из включений (1) и (2) получаем требуемое равенство. □

В параграфе 3 мы опишем все простые поля. Предварительно введем одну конструкцию построения полей.

§ 2. ПОЛЯ ЧАСТНЫХ

Определение 4. Поле P называют *полем частных кольца* R, если

1) существует изоморфное вложение $\varphi\colon R \to P$;

2) каждый элемент поля P имеет вид $\varphi(a)\,\varphi(b)^{-1}$, где $a \in R$ и $b \in R \setminus \{0\}$.

Пример 4. По определению 4 поле $\mathbb{Q}$ является полем частных кольца $\mathbb{Z}$. В качестве φ можно взять тождественное вложение.

Из условия 1 определения 4 следует, что если ненулевое кольцо R имеет поле частных, то R — коммутативное кольцо без делителей нуля. Оказывается, этого уже достаточно для существования поля частных.

Теорема 5. *Если R — ненулевое коммутативное кольцо без делителей нуля, то для него существует поле частных.*

□ На множестве $M = R \times (R \setminus \{0\})$ определим отношение:

$$((r, s) \sim (r_1, s_1)) \;\Leftrightarrow\; (rs_1 = r_1 s).$$

Ясно, что это отношение рефлексивно и симметрично. Покажем, что оно транзитивно. Пусть $(r, s) \sim (r_1, s_1)$ и $(r_1, s_1) \sim (r_2, s_2)$. Тогда справедливы равенства

$$rs_1 = r_1 s, \quad r_1 s_2 = r_2 s_1. \tag{3}$$

Умножив первое из равенств (3) на s_2, а второе — на s, получим равенства $rs_1 s_2 = r_1 s s_2$ и $r_1 s_2 s = r_2 s_1 s$. Так как R — коммутативное кольцо, то $rs_2 s_1 = r_2 s s_1$ и $(rs_2 - r_2 s)s_1 = 0$. Поскольку $s_1 \neq 0$ и R — кольцо без делителей нуля, то $rs_2 = r_2 s$ и $(r, s) \sim (r_2, s_2)$. Значит, отношение $\sim$ является отношением эквивалентности, и множество M разбивается на классы $[(r, s)]_\sim$ эквивалентных элементов.

Обозначим $\widehat{R} = M/\sim$. В дальнейшем, для кратности, класс $[(r,s)]_\sim$ будем обозначать через $\frac{r}{s}$. На множестве $\widehat{R}$ определим операции, положив

$$\frac{a}{s} + \frac{b}{s_1} = \frac{as_1 + bs}{ss_1}, \qquad \frac{a}{s} \cdot \frac{b}{s_1} = \frac{ab}{ss_1}.$$

Покажем, что операции определены корректно. Так как $s, s_1 \in R \setminus \{0\}$ и в R нет делителей нуля, то $ss_1 \in R \setminus \{0\}$.

Пусть $\frac{a}{s} = \frac{a'}{s'}$ и $\frac{b}{s_1} = \frac{b'}{s'_1}$, т. е.

$$as' = a's, \quad bs'_1 = b's_1. \tag{4}$$

По определению $\frac{a'}{s'} + \frac{b'}{s'_1} = \frac{a's'_1 + b's'}{s's'_1}$. Для доказательства корректности задания операции сложения нужно показать, что $\frac{as_1 + bs}{ss_1} = \frac{a's'_1 + b's'}{s's'_1}$, т. е. что выполнено равенство

$$(as_1 + bs)s's'_1 = (a's'_1 + b's')ss_1. \tag{5}$$

Ввиду (4) справедливы равенства $as's_1s'_1 = a'ss_1s'_1$ и $bs'_1ss' = b's_1ss'$, складывая которые, получаем равенство (5). Аналогично доказывается корректность задания операции умножения.

Теперь покажем, что $(\widehat{R}, +, \cdot)$ — поле. Ясно, что операции сложения и умножения коммутативны. Для любых элементов $s_1, s_2 \in R \setminus \{0\}$ справедливы равенства $\frac{0}{s_1} = \frac{0}{s_2}$ и $\frac{s_1}{s_1} = \frac{s_2}{s_2}$. Равенства

$$\frac{a}{s} + \frac{0}{s} = \frac{as}{ss} = \frac{a}{s} \quad \text{и} \quad \frac{a}{s} \cdot \frac{s}{s} = \frac{as}{ss} = \frac{a}{s}$$

показывают, что $\frac{0}{s}$ — нейтральный элемент по сложению, а $\frac{s}{s}$ — по умножению.

Равенства $\frac{a}{s} + \frac{-a}{s} = \frac{0}{ss} = \frac{0}{s}$ показывают, что $-\frac{a}{s} = \frac{-a}{s}$. Ассоциативность операции сложения следует из равенств

$$\left(\frac{a}{s} + \frac{b}{s_1}\right) + \frac{c}{s_2} = \frac{as_1 + bs}{ss_1} + \frac{c}{s_2} = \frac{(as_1 + bs)s_2 + c(ss_1)}{ss_1s_2}$$

и

$$\frac{a}{s} + \left(\frac{b}{s_1} + \frac{c}{s_2}\right) = \frac{a}{s} + \frac{bs_2 + cs_1}{s_1s_2} = \frac{a(s_1s_2) + (bs_2 + cs_1)s}{ss_1s_2}$$

и свойств операций в кольце R. Значит, $(\widehat{R}, +)$ — абелева группа.

Читателю предлагается проверить, что операция умножения ассоциативна и дистрибутивна относительно сложения. Значит, $(\widehat{R}, +, \cdot)$ — коммутативное кольцо с единицей.

Если $\frac{a}{s} \neq \frac{0}{s}$, то $a \in R \setminus \{0\}$, и справедливы равенства $\frac{a}{s} \cdot \frac{s}{a} = \frac{as}{as} = \frac{s}{s}$, показывающие, что

$$\frac{s}{a} = \left(\frac{a}{s}\right)^{-1}.$$

Таким образом, $(\widehat{R}, +, \cdot)$ — поле.

Определим отображение $\varphi\colon R \to \widehat{R}$, положив при фиксированном $s \in R \setminus \{0\}$ для любого $r \in R$

$$\varphi(r) = \frac{rs}{s}.$$

Легко проверить, что φ — гомоморфизм колец и $\operatorname{Ker}\varphi = 0$. Следовательно, φ — изоморфное вложение.

Поскольку

$$\frac{r_1}{s_1} = \frac{r_1}{s} \cdot \frac{s}{s_1} = \varphi(r_1)\,\varphi(s_1)^{-1},$$

то по определению 4 $\widehat{R}$ — поле частных кольца R. □

Пример 5. Пусть P — поле и R — его ненулевое подкольцо. Рассмотрим множество $T = \{ab^{-1}\colon a \in R,\ b \in R \setminus \{0\}\}$. Пользуясь утверждением 1, легко показать, что T — подполе поля P, содержащее кольцо R. По определению 4 T — поле частных кольца R. Нетрудно проверить, что T — пересечение всех подполей поля P, содержащих R.

Пример 6. Кольцо многочленов $P[x]$ над полем P является ненулевым коммутативным кольцом без делителей нуля. По теореме 5 для него существует поле частных:

$$\widehat{P[x]} = \left\{ \frac{f(x)}{g(x)} :\ f(x) \in P[x],\quad g(x) \in P[x] \setminus \{0\} \right\}.$$

Замечание 1. Если $\widehat{R}$ — поле частных кольца R, то в $\widehat{R}$ содержится подкольцо, изоморфное кольцу R. Применив конструкцию, изложенную в § 8 главы 20, получим поле $\overline{R}$, изоморфное полю $\widehat{R}$ и содержащее кольцо R. Элементы поля $\overline{R}$ имеют вид ab^{-1}, где $a \in R$, $b \in R \setminus \{0\}$. Поле $\overline{R}$ также является полем частных кольца R.

Определение 5. Поле $\overline{P[x]}$ обозначают через $P(x)$ и называют *полем рациональных функций от переменного* x. Поле $\overline{P[x_1, \ldots, x_n]}$ обозначают через $P(x_1, \ldots, x_n)$ и называют *полем рациональных функций от переменных* $x_1, \ldots, x_n$.

Рассмотрим вопрос о единственности поля частных данного кольца.

Теорема 6. *Пусть $\psi\colon R_1 \to R_2$ — изоморфизм ненулевых коммутативных колец без делителей нуля, R_i' — поле частных кольца R_i, $\varphi_i\colon R_i \to R_i'$ — изоморфное вложение, удовлетворяющее определению 4, $i = 1, 2$. Тогда существует такой изоморфизм $\mu\colon R_1' \to R_2'$, что $\mu(\varphi_1(a)) = \varphi_2(\psi(a))$ для любого элемента $a \in R_1$, т. е. коммутативна диаграмма*

$$\begin{array}{ccc} R_1 & \xrightarrow{\ \psi\ } & R_2 \\ {\scriptstyle\varphi_1}\downarrow & & \downarrow{\scriptstyle\varphi_2} \\ R_1' & \xrightarrow{\ \mu\ } & R_2' \end{array}$$

□ Зададим отображение $\mu\colon R_1' \to R_2'$, положив

$$\mu(\varphi_1(a)\,\varphi_1(b)^{-1}) = \varphi_2(\psi(a))\,\varphi_2(\psi(b))^{-1}$$

для $a \in R_1$, $b \in R_1 \setminus \{0\}$. Элементы $\varphi_1(b)^{-1}$ и $\varphi_2(\psi(b))^{-1}$ определены, так как ψ — изоморфизм, а φ_1, φ_2 — изоморфные вложения.

Покажем корректность определения отображения μ. Предположим, что $\varphi_1(a)\,\varphi_1(b)^{-1} = \varphi_1(a_1)\,\varphi_1(b_1)^{-1}$. Тогда $\varphi_1(a)\,\varphi_1(b_1) = \varphi_1(a_1)\,\varphi_1(b)$, $\varphi_1(ab_1 - a_1b) = 0$ и $ab_1 = a_1b$. Поэтому

$$\psi(a)\,\psi(b_1) = \psi(a_1)\,\psi(b), \quad \varphi_2(\psi(a))\,\varphi_2(\psi(b_1)) = \varphi_2(\psi(a_1))\,\varphi_2(\psi(b))$$

и $\varphi_2(\psi(a))\,\varphi_2(\psi(b))^{-1} = \varphi_2(\psi(a_1))\,\varphi_2(\psi(b_1))^{-1}$. Значит,

$$\mu(\varphi_1(a)\,\varphi_1(b)^{-1}) = \mu(\varphi_1(a_1)\,\varphi_1(b_1)^{-1}).$$

Непосредственной проверкой устанавливается, что μ — изоморфизм полей. При этом $\varphi_1(a) = \varphi_1(ab)\,\varphi_1(b)^{-1}$ и, следовательно,

$$\mu(\varphi_1(a)) = \varphi_2(\psi(ab))\,\varphi_2(\psi(b))^{-1} = \varphi_2(\psi(a)). \quad \square$$

Следствие 1. *Если R' и R'' — произвольные поля частных ненулевого коммутативного кольца R без делителей нуля, а φ_1, φ_2 — изоморфные вложения R в R' и R'' соответственно, удовлетворяющие определению* 4*, то существует такой изоморфизм $\mu\colon R' \to R''$, что для любого $a \in R$ справедливо равенство $\mu(\varphi_1(a)) = \varphi_2(a)$.*

Если P, P_1 и P_2 — поля, $P \subset P_1 \cap P_2$ и существует изоморфизм $\mu\colon P_1 \to P_2$, при котором $\mu(a) = a$ для $a \in P$, то говорят, что поля P_1 и P_2 *изоморфны над* P.

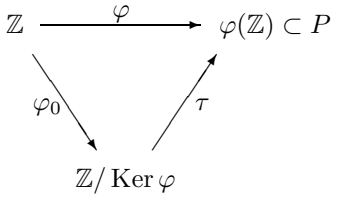
Следствие 2. *Если в условиях следствия* 1 *φ_1 и φ_2 — тождественные вложения, то μ — изоморфизм полей R' и R'' над R.*

§ 3. ПРОСТЫЕ ПОЛЯ

Опишем простые поля.

Теорема 7. *Поле P простое тогда и только тогда, когда оно изоморфно полю $\mathbb{Z}/p$ при некотором простом p или полю $\mathbb{Q}$.*

□ В примере 2 показано, что поля $\mathbb{Z}/p$ и $\mathbb{Q}$ — простые. Пусть P — простое поле с единицей e и нулем 0. Зададим отображение $\varphi\colon \mathbb{Z} \to P$, положив $\varphi(n) = ne$. Легко проверить, что φ — гомоморфизм колец. По теореме об эпиморфизме колец имеем коммутативную диаграмму



где τ — изоморфизм.

По утверждению 8 главы 20 возможны два случая: $\mathrm{Char}\, P = 0$ или $\mathrm{Char}\, P = p$, где p — простое число. Так как $\mathrm{Ker}\,\varphi = \{n \in \mathbb{Z}\colon\ ne = 0\}$, то в первом случае $\mathrm{Ker}\,\varphi = 0$, а во втором — $\mathrm{Ker}\,\varphi = p\mathbb{Z}$.

Если $\mathrm{Ker}\,\varphi = 0$, то $\mathbb{Z} \cong \varphi(\mathbb{Z}) \subset P$. Поскольку P — простое поле, то ввиду примера 5 оно — поле частных кольца $\varphi(\mathbb{Z})$. Так как $\mathbb{Q}$ — поле частных кольца $\mathbb{Z}$, то по теореме 6 $P \cong \mathbb{Q}$.

Пусть $\mathrm{Ker}\,\varphi = p\mathbb{Z}$. Тогда $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/p$ — поле и, следовательно, $\varphi(\mathbb{Z})$ — поле. Ввиду простоты поля P получаем $\varphi(\mathbb{Z}) = P$. В таком случае, $P \cong \mathbb{Z}/p$. □

Итак, все простые поля описаны.

§ 4. КЛАССИФИКАЦИЯ РАСШИРЕНИЙ ПОЛЯ

Определение 6. Пусть P — подполе и M — подмножество поля P'. *Расширение* $P(M)$ *поля* P, порожденное M, называют *конечным*, если M — конечное множество, и *простым*, если $|M| = 1$.

Пример 7. Пусть $P(x) = \{f(x)g(x)^{-1}\colon\ f(x) \in P[x],\ g(x) \in P[x] \setminus \{0\}\}$ — поле частных кольца многочленов $P[x]$ над полем P (определение 5). Рассмотрим в поле $P(x)$ подполе P и подмножество $M = \{x\}$. Простое расширение поля P, порожденное подмножеством $\{x\}$, совпадает, как легко видеть, со всем полем $P(x)$. Таким образом, введенное в определении 5 обозначение $P(x)$ согласуется с обозначением, введенным в определении 3.

Ввиду утверждения 4(б) конечное расширение $P(m_1, \ldots, m_n)$ поля P можно считать полученным в виде последовательности простых расширений: $P(m_1, \ldots, m_n) = P(m_1)(m_2)\ldots(m_n)$.

Возможны различные способы классификации расширений полей. Первый способ — классифицировать расширения по минимальному числу элементов, порождающих эти расширения. Второй способ основывается на том, что в ситуации $P \subset P'$ поле P' можно рассматривать как векторное пространство над полем P (например правое), взяв в качестве внешней операции умножения внутреннюю операцию умножения в поле P'.

Определение 7. Если P'_P — конечномерное пространство, то его размерность называют *степенью расширения* P' *над* P и обозначают $[P' : P]$, а поле P' называют *расширением конечной степени* поля P. Если P'_P — бесконечномерное пространство, то говорят о *расширении бесконечной степени* и пишут $[P' : P] = \infty$.

Расширения можно классифицировать по их степеням.

Пример 8. В силу примера 3 $\mathbb{C} = \mathbb{R}(i)$. Так как 1, i — базис пространства $\mathbb{C}_{\mathbb{R}}$, то $[\mathbb{C} : \mathbb{R}] = 2$.

Утверждение 8. *Если* P' *— расширение конечной степени поля* P*, то* P' *— конечное расширение поля* P.

□ Пусть $[P' : P] = n$. Тогда в пространстве P'_P существует базис $\alpha_1, \ldots, \alpha_n$. Поле $P(\alpha_1, \ldots, \alpha_n)$ содержит все элементы поля P', и, следовательно, $P' = P(\alpha_1, \ldots, \alpha_n)$. □

Позже (пример 13) будет показано, что конечное расширение может не быть расширением конечной степени.

Рассмотрим последовательность расширений полей («башню полей»).

Теорема 9 (о башне полей). *Если $P_1 \subset P_2 \subset \ldots \subset P_n$ — последовательность полей, то степень расширения $[P_n : P_1]$ конечна тогда и только тогда, когда конечны все степени $[P_i : P_{i-1}]$, $i \in \overline{2,n}$. При выполнении последнего условия справедливо равенство*

$$[P_n : P_1] = \prod_{i=2}^{n} [P_i : P_{i-1}].$$

□ Пусть $[P_n : P_1] < \infty$. Если при некотором $i \in \overline{2,n}$ степень расширения $[P_i : P_{i-1}]$ бесконечна, то в поле P_i, а значит, и в поле P_n существует бесконечная линейно независимая над P_{i-1} система элементов. Поскольку эта система элементов линейно независима и над полем P_1, то приходим к противоречию с условием. Поэтому $[P_i : P_{i-1}] < \infty$ для $i \in \overline{2,n}$.

Обратно, пусть $[P_i : P_{i-1}] = k_i < \infty$ для $i \in \overline{2,n}$. Проведем доказательство конечности степени расширения $[P_n : P_1]$ индукцией по числу n полей башни. При $n = 2$ утверждение очевидно. Пусть оно верно при $n \leqslant l - 1$. Покажем, что тогда оно верно при $n = l$.

По предположению индукции $[P_{l-1} : P_1] = \prod_{i=2}^{l-1} k_i = m < \infty$. Значит, существует базис $\vec{\alpha} = (\alpha_1, \ldots, \alpha_m)$ пространства $(P_{l-1})_{P_1}$. По условию существует базис $\vec{\beta} = (\beta_1, \ldots, \beta_{k_l})$ пространства $(P_l)_{P_{l-1}}$. Покажем, что система элементов $\alpha_i\beta_j$, $i \in \overline{1,m}$, $j \in \overline{1,k_l}$, является базисом пространства $(P_l)_{P_1}$. Тогда теорема будет доказана, так как будет показано, что $[P_l : P_1] = m \cdot k_l = \prod_{i=2}^{l} k_i$.

Элементы поля P_l представляются в виде $\sum_{i=1}^{k_l} \beta_i b_i$, где $b_i \in P_{l-1}$, а элементы поля P_{l-1} — в виде $b_i = \sum_{j=1}^{m} \alpha_j a_{ij}$, где $a_{ij} \in P_1$. Получаем выражение элементов поля P_l через элементы $\alpha_j\beta_i$:

$$\sum_{i=1}^{k_l} \beta_i b_i = \sum_{i=1}^{k_l} \beta_i \left(\sum_{j=1}^{m} \alpha_j a_{ij} \right) = \sum_{i,j} (\beta_i \alpha_j) a_{ij}, \quad i \in \overline{1,k_l},\ j \in \overline{1,m}.$$

Остается показать, что система элементов $\beta_i\alpha_j$ линейно независима над полем P_1. Пусть

$$\sum_{i,j} (\beta_i \alpha_j) a_{ij} = 0, \quad a_{ij} \in P_1,\ i \in \overline{1,k_l},\ j \in \overline{1,m}. \tag{6}$$

Так как $\sum_{j=1}^{m} \alpha_j a_{ij} \in P_{l-1}$ при любом $i \in \overline{1,k_l}$ и $\vec{\beta}$ — базис пространства $(P_l)_{P_{l-1}}$, то из равенства (6) следуют равенства

$$\sum_{j=1}^{m} \alpha_i a_{ij} = 0, \quad i \in \overline{1,k_l}.$$

Поскольку $a_{ij} \in P_1$ и $\vec{\alpha}$ — базис пространства $(P_{l-1})_{P_1}$, то $a_{ij} = 0$ при $j \in \overline{1,m}$, $i \in \overline{1,k_l}$. □

Рассмотрим еще один способ классификации расширений полей.

Определение 8. Пусть P', P — поля и $P' \supset P$. Элемент $\alpha \in P'$ называют *алгебраическим над полем* P, если система элементов $\alpha^0 = e$, α, α^2, …, α^n, … линейно зависима над P. В противном случае элемент α называют *трансцендентным над полем* P.

Пример 9. Пусть $P' \supset P$ и $\alpha \in P$. Соотношение $e\alpha + \alpha(-e) = 0$ показывает, что все элементы поля P алгебраичны над P.

Пример 10. Если $P' \supset P$ и некоторый элемент $\alpha \in P'$ трансцендентен над полем P, то $P(\alpha)$ — бесконечномерное пространство над P.

Пример 11. Элемент $i \in \mathbb{C}$ алгебраичен над $\mathbb{R}$, так как справедливо соотношение $i^0 \cdot 1 + i \cdot 0 + i^2 \cdot 1 = 0$.

Критерий алгебраичности элемента дает

Утверждение 10. *Пусть P' — расширение поля P. Элемент $\alpha \in P'$ алгебраичен над P тогда и только тогда, когда α — корень некоторого ненулевого многочлена из $P[x]$.*

□ Элемент $\alpha \in P'$ является алгебраическим над полем P тогда и только тогда, когда существуют различные числа $i_1, \ldots, i_n \in \mathbb{N}_0$ и элементы $a_1, \ldots, a_n$ поля P, не все равные нулю, такие, что

$$\sum_{j=1}^{n} \alpha^{i_j} a_j = 0. \tag{7}$$

Ясно, что равенство (7) справедливо тогда и только тогда, когда α — корень многочлена

$$f(x) = \sum_{j=1}^{n} a_j x^{i_j} \in P[x],$$

который отличен от нулевого многочлена. □

Следствие 1. *Пусть $P \subset P'$. Если элемент $\alpha \in P'$ алгебраичен над полем P, то он алгебраичен над любым полем P_1, удовлетворяющим условию $P \subset P_1 \subset P'$.*

Следствие 2. *Если $P \subset P'$ и $\alpha \in P'$ — алгебраический над P элемент, то в $P[x]$ существует единственный унитарный неприводимый над P многочлен $m(x)$, корнем которого является α. При этом для любого многочлена $t(x) \in P[x]$*

$$(t(\alpha) = 0) \;\Leftrightarrow\; (m(x) \mid t(x)).$$

□ По утверждению 10 множество

$$T = \{f(x) \in P[x] : \ f(\alpha) = 0\}$$

содержит элемент, отличный от нуля. Легко проверить, что T — идеал кольца $P[x]$. По следствию теоремы 14 главы 20 существует единственный унитарный многочлен $m(x)$ такой, что $T = (m(x))_{P[x]}$. При этом для $t(x) \in P[x]$ справедливо включение $t(x) \in T$ тогда и только тогда, когда $m(x) \mid t(x)$.

Если $m(x) = u(x)v(x)$, где $u(x), v(x) \in P[x]$, $\deg u(x) < \deg m(x)$ и $\deg v(x) < \deg m(x)$, то $u(a) \neq 0$ и $v(a) \neq 0$, что вместе с условием $m(a) = 0$ противоречит отсутствию делителей нуля в поле P'. Значит, $m(x)$ — неприводимый над полем P многочлен. □

Следствие 2 показывает, что корректно

Определение 9. Если P', P — поля, $P \subset P'$ и $\alpha \in P'$ — алгебраический над P элемент, то единственный унитарный неприводимый над полем P многочлен, корнем которого является α, называют *минимальным многочленом элемента α над полем P* и обозначают через $m_{\alpha,P}(x)$.

Следствие 3. *Если $P \subset P'$, то элемент $\alpha \in P'$ трансцендентен над полем P тогда и только тогда, когда $f(\alpha) \neq 0$ для любого многочлена $f(x) \in P[x] \setminus \{0\}$.*

Пример 12. Множество $\mathbb{Q}[x]$ счетно. Так как ненулевой многочлен из $\mathbb{Q}[x]$ может иметь в поле $\mathbb{R}$ только конечное число корней, то в $\mathbb{R}$ имеется не более чем счетное множество элементов, алгебраических над $\mathbb{Q}$. Поскольку множество $\mathbb{R}$ несчетно, то в $\mathbb{R}$ существуют трансцендентные над $\mathbb{Q}$ элементы. Методами математического анализа можно показать, что такими являются, например, число π и основание натуральных логарифмов e. Элементы из $\mathbb{R}$, трансцендентные над $\mathbb{Q}$, обычно называют *трансцендентными числами*.

Пример 13. Элемент x поля рациональных функций $P(x)$ трансцендентен над P. Действительно, если $f(y) = \sum_{i=0}^{n} a_i y^i \in P[y]$ — такой многочлен над P, что x — его корень, то многочлен $f(x) = \sum_{i=0}^{n} a_i x^i$ равен нулю. Но тогда $a_i = 0$ при $i \in \overline{0,n}$ и $f(y)$ — нулевой многочлен. По следствию 3 утверждения 10 элемент x трансцендентен над P. Этот пример показывает, что простое расширение поля может быть расширением бесконечной степени (см. пример 10).

Определение 10. Расширение P' поля P называют *алгебраическим*, если все элементы поля P' — алгебраические над полем P, и *трансцендентным*, если в P' существует хотя бы один трансцендентный над P элемент.

Пример 14. В силу примера 13 поле $P(x)$ — трансцендентное расширение поля P. Поле $\mathbb{C}$ является алгебраическим расширением поля $\mathbb{R}$, так как произвольный элемент $a + bi \in \mathbb{C}$ есть корень ненулевого многочлена $(x - a)^2 + b^2 \in \mathbb{R}[x]$.

Важные примеры алгебраических расширений дает

Утверждение 11. *Если P' — расширение конечной степени поля P, то P' — алгебраическое расширение P.*

□ В векторном пространстве P'_P по условию нет линейно независимых систем, состоящих более чем из $[P' : P]$ элементов. Тогда по определению 8 все элементы поля P' алгебраичны над полем P. По определению 10 P' — алгебраическое расширение поля P. □

Позже будет показано, что обратное утверждение неверно (см. пример 17).

§ 5. ПРОСТЫЕ РАСШИРЕНИЯ ПОЛЕЙ

Строение простых расширений полей описывает

Теорема 12. *Пусть P', P — поля, $P \subset P'$ и $\alpha \in P'$. Тогда справедливы утверждения*:

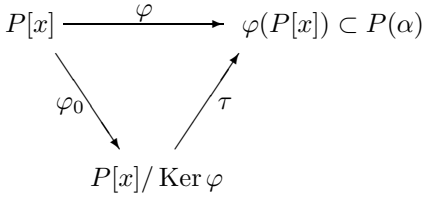
(а) *если элемент α трансцендентен над P, то*

$$P(\alpha) \cong P(x);$$

(б) *если элемент α алгебраичен над P, то*

$$P(\alpha) \cong P[x]/m_{\alpha,P}(x).$$

□ Определим отображение $\varphi\colon P[x] \to P(\alpha)$, положив $\varphi(t(x)) = t(\alpha)$ для $t(x) \in P[x]$. Очевидно, что φ — гомоморфизм колец. По теореме об эпиморфизме колец имеем коммутативную диаграмму



где τ — изоморфизм, определяемый соотношением $\tau([f(x)]) = \varphi(f(x))$. По теореме 36 главы 9 $\varphi(P[x]) = P[\alpha]$. По теореме об образах и полных прообразах при гомоморфизме колец $P[\alpha]$ — подкольцо поля $P(\alpha)$. Так как $\varphi(a) = a$ для любого $a \in P$ и $\varphi(x) = \alpha$, то $P[\alpha]$ содержит P и α. Ясно, что

$$\operatorname{Ker}\varphi = \{t(x) \in P[x] :\ t(\alpha) = 0\}.$$

(а) Пусть элемент α трансцендентен над P. Тогда по следствию 3 утверждения 10 $\operatorname{Ker}\varphi = 0$. Стало быть, $P[x] \cong P[\alpha] \subset P(\alpha)$.

В силу примера 5 поле частных T кольца $P[\alpha]$ — это пересечение всех подполей поля $P(\alpha)$, содержащих $P[\alpha]$, т. е. содержащих P и α (любое подполе из $P(\alpha)$, содержащее P и α, содержит $P[\alpha]$). По определению 3 $T = P(\alpha)$.

В силу определения 5 $P(x)$ — поле частных кольца $P[x]$. По теореме 6 изоморфизм $P[x] \cong P[\alpha]$ влечет изоморфизм $P(x) \cong P(\alpha)$.

(б) Пусть элемент α алгебраичен над P. Тогда $\operatorname{Ker}\varphi = (m_{\alpha,P}(x))_{P[x]}$. Так как по определению 9 $m_{\alpha,P}(x)$ — неприводимый над P многочлен, то по утверждению 20 главы 20 $P[x]/m_{\alpha,P}(x)$ — поле. Значит, и $P[\alpha]$ — поле. Поскольку $P[\alpha]$ содержит P и α, то $P[\alpha] = P(\alpha)$. Окончательно получаем, что

$$P(\alpha) \cong P[x]/m_{\alpha,P}(x). \quad \square$$

Теорема 12 позволяет описать вид элементов поля $P(\alpha)$.

Утверждение 13. *Пусть $P \subset P'$ и $\alpha \in P'$. Тогда справедливы утверждения*:

(а) *если элемент α трансцендентен над P, то элементы поля $P(\alpha)$ имеют вид $g(\alpha)h(\alpha)^{-1}$, где $g(x) \in P[x]$, $h(x) \in P[x] \setminus \{0\}$;*

(б) *если элемент α алгебраичен над P, то каждый элемент β поля $P(\alpha)$ однозначно записывается в виде $\beta = r(\alpha)$, где $r(x) \in P[x]$ и $\deg r(x) < \deg m_{\alpha,P}(x)$.*

$\square$ (а) При доказательстве утверждения (а) теоремы 12 показано, что $P(\alpha)$ — поле частных своего подкольца $P[\alpha]$, элементы которого имеют вид $t(\alpha)$, где $t(x) \in P[x]$. По замечанию 1 элементы поля $P(\alpha)$ имеют указанный вид.

(б) При доказательстве утверждения (б) теоремы 12 показано, что $P(\alpha) = P[\alpha]$. Значит, если $\beta \in P(\alpha)$, то $\beta = t(\alpha)$, где $t(x) \in P[x]$. Разделим $t(x)$ с остатком на $m_{\alpha,P}(x)$:

$$t(x) = g(x)\, m_{\alpha,P}(x) + r(x), \quad \deg r(x) < \deg m_{\alpha,P}(x).$$

Так как $m_{\alpha,P}(\alpha) = 0$, то $t(\alpha) = r(\alpha)$. Следовательно, элементы поля $P(\alpha)$ имеют указанный вид.

Если $t_1(x) \in P[x]$, $\deg t_1(x) < \deg m_{\alpha,P}(x)$ и $t_1(\alpha) = r(\alpha)$, то многочлен $u(x) = r(x) - t_1(x)$ имеет корень α. По следствию 2 утверждения 10 и определению 9 $m_{\alpha,P}(x) \mid u(x)$. Однако $\deg u(x) < \deg m_{\alpha,P}(x)$. Поэтому $u(x) = 0$ и $t_1(x) = r(x)$. $\square$

Теперь мы можем вычислить степень простого расширения поля, порожденного алгебраическим элементом.

Утверждение 14. *Пусть $P \subset P'$ и $\alpha \in P'$ — алгебраический над P элемент. Тогда*

$$[P(\alpha) : P] = \deg m_{\alpha,P}(x),$$

и, в частности, $P(\alpha)$ — алгебраическое расширение поля P.

$\square$ Пусть $\deg m_{\alpha,P}(x) = n$. По утверждению 13(б) элементы поля $P(\alpha)$ линейно выражаются над P через систему элементов $\alpha^0 = e, \alpha, \ldots, \alpha^{n-1}$. Ввиду утверждения 13(б) система элементов $e, \alpha, \ldots, \alpha^{n-1}$ линейно независима над P и $\dim P(\alpha)_P = [P(\alpha) : P] = \deg m_{\alpha,P}(x)$.

По утверждению 11 $P(\alpha)$ — алгебраическое расширение поля P. $\square$

Покажем, что в некоторых случаях простые расширения данного поля изоморфны.

Теорема 15. *Пусть $P' = P(\alpha)$ и $P'' = P(\beta)$, где элементы α и β трансцендентны над P. Тогда поля $P(\alpha)$ и $P(\beta)$ изоморфны, и существует такой изоморфизм $\mu\colon P(\alpha) \to P(\beta)$, что $\mu(a) = a$ для любого $a \in P$ и $\mu(\alpha) = \beta$ (т. е. поля $P(\alpha)$ и $P(\beta)$ изоморфны над P).*

□ Определим отображения $\tau_1\colon P[x] \to P(\alpha)$ и $\tau_2\colon P[x] \to P(\beta)$, положив $\tau_1(t(x)) = t(\alpha)$ и $\tau_2(t(x)) = t(\beta)$ для $t(x) \in P[x]$.

Как и в доказательстве теоремы 12(а), пользуясь трансцендентностью элементов α и β над полем P, получаем

$$P[x] \cong \tau_1(P[x]) = P[\alpha], \quad P[x] \cong \tau_2(P[x]) = P[\beta].$$

Обозначим $\psi = \tau_2 \circ \tau_1^{-1}$. Тогда $\psi\colon P[\alpha] \to P[\beta]$ — изоморфизм колец, при котором $\psi(a) = a$ для $a \in P$ и $\psi(\alpha) = \beta$.

Поскольку $P(\alpha)$ и $P(\beta)$ — поля частных, соответственно, колец $P[\alpha]$ и $P[\beta]$ и существуют тождественные вложения $\varepsilon_1\colon P[\alpha] \to P(\alpha)$ и $\varepsilon_2\colon P[\beta] \to P(\beta)$, то по теореме 5 существует такой изоморфизм $\mu\colon P(\alpha) \to P(\beta)$, что коммутативна диаграмма

$$\begin{array}{ccc} P[\alpha] & \xrightarrow{\psi} & P[\beta] \\ {\scriptstyle\varepsilon_1}\downarrow & & \downarrow{\scriptstyle\varepsilon_2} \\ P(\alpha) & \xrightarrow{\mu} & P(\beta) \end{array}$$

Тогда $\mu(a) = a$ при $a \in P$ и $\mu(\alpha) = \beta$. □

Теорема 16. *Пусть для* $i \in \overline{1,2}$ $P_i' = P_i(\alpha_i)$ *— расширение поля* P_i*, порожденное корнем* α_i *унитарного неприводимого над* P_i *многочлена* $g_i(x) \in P_i[x]$*. Если существует такой изоморфизм* $\sigma\colon P_1 \to P_2$*, что* $\sigma'(g_1(x)) = g_2(x)$*, то существует такой изоморфизм* $\tau\colon P_1' \to P_2'$*, что* $\tau\big|_{P_1} = \sigma$ *и* $\tau(\alpha_1) = \alpha_2$ (определение отображения σ' см. в утверждении 28 главы 20).

□ Ясно, что многочлены $g_1(x)$ и $g_2(x)$ являются минимальными многочленами соответственно элементов α_1 и α_2 над полями P_1 и P_2 (см. замечание 3 главы 20). По теореме 15(б) имеют место изоморфизмы:

$$\tau_1\colon P_1[x]/g_1(x) \to P_1(\alpha_1), \quad \tau_2\colon P_2[x]/g_2(x) \to P_2(\alpha_2),$$

при которых $\tau_i([x]_{g_i(x)}) = \alpha_i$ и $\tau_i([a_i]_{g_i(x)}) = a_i$ для $a_i \in P_i$.

Поскольку $g_2(x) = \sigma'(g_1(x))$, то по утверждению 28 главы 20 существует изоморфизм

$$\nu\colon P_1[x]/g_1(x) \to P_2[x]/g_2(x),$$

при котором $\nu([t(x)]_{g_1(x)}) = [\sigma'(t(x))]_{g_2(x)}$.

Положив $\tau = \tau_2 \circ \nu \circ \tau_1^{-1}$, получаем изоморфизм

$$\tau\colon P_1(\alpha_1) \to P_2(\alpha_2).$$

При этом для $a \in P_1$ справедливы равенства

$$\tau(a) = \tau_2(\nu(\tau_1^{-1}(a))) = \tau_2(\nu([a]_{g_1(x)})) = \tau_2([\sigma'(a)]_{g_2(x)}) = \sigma'(a).$$

Поскольку $\sigma'\big|_{P_1} = \sigma$, то $\tau(a) = \sigma(a)$ и $\tau\big|_{P_1} = \sigma$.

Кроме того, так как $\sigma'(x) = x$, то

$$\tau(\alpha_1) = \tau_2(\nu(\tau_1^{-1}(\alpha_1))) = \tau_2(\nu([x]_{g_1(x)})) = \tau_2([\sigma'(x)_{g_2(x)}]) = \alpha_2. \quad \square$$

Следствие. *Пусть P' — расширение поля P. Если элементы α и β из P' алгебраичны над P и $m_{\alpha,P}(x) = m_{\beta,P}(x)$, то существует такой изоморфизм $\mu\colon P(\alpha) \to P(\beta)$, что $\mu(a) = a$ для $a \in P$ и $\mu(\alpha) = \beta$ (т. е. поля $P(\alpha)$ и $P(\beta)$ изоморфны над P).*

Пример 15. Поля $P(\alpha)$ и $P(\beta)$ могут быть изоморфными и в случае, когда $m_{\alpha,P}(x) \neq m_{\beta,P}(x)$. Например, $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(2\sqrt{2})$, хотя $m_{\sqrt{2},\mathbb{Q}}(x) = x^2 - 2$, а $m_{2\sqrt{2},\mathbb{Q}}(x) = x^2 - 8$.

Рассмотрим еще некоторые свойства конечных расширений полей.

Утверждение 17. *Пусть P', P — поля, $P \subset P'$ и элементы $\alpha_1, \ldots, \alpha_k \in P'$ таковы, что α_i алгебраичен над полем $P(\alpha_1, \ldots, \alpha_{i-1})$, $i \in \overline{2,k}$, а α_1 — над P. Тогда степень расширения $[P(\alpha_1, \ldots, \alpha_k) : P]$ конечна. В частности, $P(\alpha_1, \ldots, \alpha_k)$ — алгебраическое расширение поля P.*

□ Рассмотрим башню полей

$$P \subset P(\alpha_1) \subset \ldots \subset P(\alpha_1, \ldots, \alpha_{k-1}) \subset P(\alpha_1, \ldots, \alpha_k).$$

По утверждению 4 верны равенства $P(\alpha_1, \ldots, \alpha_i) = P(\alpha_1, \ldots, \alpha_{i-1})(\alpha_i)$, $i \in \overline{2,k}$. По условию и утверждению 14

$$[P(\alpha_1, \ldots, \alpha_i) : P(\alpha_1, \ldots, \alpha_{i-1})] < \infty, \quad i \in \overline{2,k}; \quad [P(\alpha_1) : P] < \infty.$$

Тогда по теореме о башне полей $[P(\alpha_1, \ldots, \alpha_k) : P] < \infty$, и по утверждению 11 $P(\alpha_1, \ldots, \alpha_k)$ — алгебраическое расширение поля P. □

Следствие. *Степень расширения $[P' : P]$ конечна тогда и только тогда, когда P' — конечное алгебраическое расширение поля P.*

□ Доказательство следует из утверждений 11 и 17. □

Опишем вид элементов конечного расширения поля.

Утверждение 18. *Пусть $P \subset P'$ и $M = \{m_1, \ldots, m_n\}$ — подмножество из P'. Тогда $P(m_1, \ldots, m_n)$ — множество всех элементов из P', имеющих вид $f(m_1, \ldots, m_n)\, g(m_1, \ldots, m_n)^{-1}$, где*

$$f(\vec{x}),\, g(\vec{x}) \in P[x_1, \ldots, x_n], \quad g(m_1, \ldots, m_n) \neq 0. \tag{8}$$

□ Ясно, что множество T всех различных элементов вида (8) содержится в $P(m_1, \ldots, m_n)$. Непосредственной проверкой с применением утверждения 1 устанавливаем, что T — подполе поля $P(m_1, \ldots, m_n)$, а тогда и поля P'. Поскольку $T \supset M$ и $T \supset P$, то по определению 3 $T = P(m_1, \ldots, m_n)$. □

§ 6. ПОЛЯ РАЗЛОЖЕНИЯ МНОГОЧЛЕНА

Докажем одну из важнейших теорем теории полей.

Теорема 19. *Для любого поля P и любого неприводимого над P многочлена $f(x) \in P[x]$ существует такое поле T, что $T = P(\alpha)$, где $\alpha \in T$ — корень многочлена $f(x)$.*

□ Рассмотрим естественный гомоморфизм

$$\varphi_0 \colon P[x] \to P[x]/f(x) = T_1,$$

$\varphi_0(g(x)) = [g(x)]_{f(x)}$. Так как многочлен $f(x)$ неприводим над полем P, то T_1 — поле.

Покажем, что в T_1 содержится подполе, изоморфное полю P. Если $a, b \in P$ и $a \neq b$, то $\varphi_0(a) \neq \varphi_0(b)$, так как в противном случае выполнялось бы равенство $[a]_{f(x)} = [b]_{f(x)}$, означающее, что многочлен нулевой степени $a - b$ делится на многочлен $f(x)$, имеющий степень не меньше первой. Теперь ясно, что $\{[a]_{f(x)} \colon a \in P\}$ — подполе поля T_1, изоморфное полю P.

Так как

$$T_1 = \{[g(x)]_{f(x)} \colon g(x) \in P[x], \quad \deg g(x) < \deg f(x)\},$$

то

$$T_1 = \left\{ \sum_{i=0}^{\deg f(x)-1} [a_i]_{f(x)} [x]^i_{f(x)} \colon a_i \in P \right\}.$$

Применив к полю T_1 конструкцию, изложенную в § 8 главы 20, получаем поле T, изоморфное полю T_1 и содержащее поле P:

$$T = \left\{ \sum_{i=0}^{\deg f(x)-1} a_i \, [x]^i_{f(x)} \colon a_i \in P \right\} \overset{\psi}{\cong} T_1.$$

Последнее равенство означает, что $T = P([x]_{f(x)})$.

Пусть $f(x) = \sum_{i=0}^{n} f_i x^i$. Тогда $f([x]_{f(x)}) = \sum_{i=0}^{n} f_i [x]^i_{f(x)}$. По определению операций в поле T сначала вычисляем $\psi(f([x]_{f(x)})) \in T_1$:

$$\sum_{i=0}^{n} [f_i]_{f(x)} [x]^i_{f(x)} = \sum_{i=0}^{n} [f_i x^i]_{f(x)} = [f(x)]_{f(x)} = [0]_{f(x)} = \psi(f([x]_{f(x)})),$$

а затем берем соответствующее значение в поле T. Так как при изоморфизме полей только нулевой элемент переходит в нулевой, то $f([x]_{f(x)}) = 0$, и, значит, $[x]_{f(x)}$ — корень многочлена $f(x)$ в поле T. □

Следствие. *Для любого поля P и любого многочлена $f(x) \in P[x]$, $\deg f(x) \geqslant 1$, существует поле, содержащее поле P и корень α многочлена $f(x)$.*

□ Пусть

$$f(x) = f_n\, g_1(x)^{k_1} \dots\, g_s(x)^{k_s} \tag{9}$$

— каноническое разложение $f(x)$ над полем P. По теореме существует поле $T = P(\alpha)$, содержащее поле P и корень α многочлена $g_1(x)$. Ясно, что $f(\alpha) = 0$. □

Определение 11. Поле P' называют *полем разложения многочлена* $f(x) \in P[x]$ *над полем* P, если $P' \supset P$ и над полем P' многочлен $f(x)$ раскладывается на линейные множители.

Это определение обобщает определение 18 главы 9, где рассматривается случай, когда само поле P является полем разложения многочлена $f(x) \in P[x]$.

Теорема 20. *Для любого поля P и любого многочлена $f(x) \in P[x]$, $\deg f(x) \geqslant 1$, существует поле разложения $f(x)$ над P.*

□ Пусть многочлен $f(x)$ имеет над полем P каноническое разложение (9). Обозначим $\deg g_i(x) = l_i$ и

$$d_P(f) = \sum_{l_i \neq 1,\ i \in \overline{1,s}} l_i.$$

Доказательство теоремы проведем индукцией по числу $d_P(f)$.

Если $d_P(f) = 0$, то многочлен $f(x)$ раскладывается над полем P на линейные множители. Поле P по определению 11 и является полем разложения $f(x)$ над P.

Предположим, что теорема верна для любого поля P_1 и любого такого многочлена $g(x) \in P_1[x]$, что $d_{P_1}(g) \leqslant k - 1$, и покажем, что тогда она верна для любого поля P и любого многочлена $f(x) \in P[x]$ с условием $d_P(x) = k$.

Пусть в разложении (9) $\deg g_1(x) = l_1 > 1$. По следствию теоремы 19 существует расширение $P(\alpha)$ поля P, где α — корень многочлена $g_1(x)$. Разложим многочлен $f(x)$ над полем $P(\alpha)$ на неприводимые множители. Тогда $d_{P(\alpha)}(f) < k$, так как над полем $P(\alpha)$ у многочлена $f(x)$ появляется, по крайней мере, k_1 новых линейных множителей. По предположению индукции существует такое поле $P' \supset P(\alpha)$, над которым многочлен $f(x)$ раскладывается на линейные множители. Поскольку $P' \supset P(\alpha) \supset P$, то P' — поле разложения многочлена $f(x)$ над P. □

Покажем, что среди полей разложения многочлена $f(x)$ над полем P существует «наименьшее».

Определение 12. Поле разложения P' многочлена $f(x) \in P[x]$ над полем P называют *минимальным*, если P' порождается над P корнями многочлена $f(x)$.

Теорема 21. *Для любого поля P и любого многочлена $f(x) \in P[x]$, $\deg f(x) \geqslant 1$, существует минимальное поле разложения $f(x)$ над P. В любом поле разложения $f(x)$ над P содержится некоторое его минимальное поле разложения над P.*

□ По теореме 20 для многочлена $f(x)$ существует поле разложения P' над P. Возьмем в P' все корни $\alpha_1, \dots, \alpha_n$ многочлена $f(x)$. Тогда поле $P(\alpha_1, \dots, \alpha_n)$ по определению 12 является минимальным полем разложения $f(x)$ над P. □

Покажем теперь, что любые два минимальных поля разложения многочлена $f(x) \in P[x]$ над полем P изоморфны. Этот факт мы получим из более общей теоремы.

Теорема 22. *Пусть* $\sigma\colon P_1 \to P_2$ *— изоморфизм полей,*

$$f(x) = \sum_{i=0}^{n} f_i x^i \in P_1[x], \qquad \sigma'(f(x)) = \sum_{i=0}^{n} \sigma(f_i) x^i \in P_2[x],$$

$\overline{P}_1$ *— некоторое минимальное поле разложения многочлена* $f(x)$ *над* P_1 *и* $\overline{P}_2$ *— некоторое минимальное поле разложения многочлена* $\sigma'(f(x))$ *над* P_2*. Тогда существует изоморфизм полей* $\varphi\colon \overline{P}_1 \to \overline{P}_2$*, при котором* $\varphi(a) = \sigma(a)$ *для* $a \in P_1$ *(см. замечание* 3 *главы* 20*).*

□ Проведем доказательство индукцией по числу $d_{P_1}(f)$, определенному в доказательстве теоремы 20. Если $d_{P_1}(f) = 0$, то P_1 — единственное минимальное поле разложения $f(x)$ над P_1. В этом случае $f(x) = f_n \cdot \prod_{i=1}^{n}(x - \alpha_i)$, $\alpha_i \in P_1$, и по утверждению 28 главы 20

$$\sigma'(f(x)) = \sigma(f_n) \prod_{i=1}^{n} (x - \sigma(\alpha_i)).$$

Значит, P_2 — единственное минимальное поле разложения многочлена $\sigma'(f(x))$ над P_2. В качестве требуемого изоморфизма φ можно взять σ.

Предположим, что теорема верна для любых изоморфных полей P_1 и P_2 и любого многочлена $f(x) \in P_1[x]$, для которого $d_{P_1}(f) \leqslant k - 1$, где $k > 1$.

Пусть $d_{P_1}(f) = k$, а разложение (9) — каноническое разложение многочлена $f(x)$ над полем P_1, где $\deg g_1(x) = l_1 > 1$. По утверждению 28 главы 20

$$\sigma'(f(x)) = \sigma(f_n) \prod_{i=1}^{s} \sigma'(g_i(x))^{k_i}$$

— каноническое разложение многочлена $\sigma'(f(x))$ над полем P_2.

В поле $\overline{P}_1$ рассмотрим подполе $P_1(\alpha_1)$, где $g_1(\alpha_1) = 0$. Ясно, что $d_{P_1(\alpha_1)}(f) < k$. В поле $\overline{P}_2$ выберем произвольный корень β_1 многочлена $\sigma'(g_1(x))$ и рассмотрим подполе $P_2(\beta_1)$. По теореме 16 существует изоморфизм

$$\tau\colon P_1(\alpha_1) \to P_2(\beta_1),$$

причем $\tau(a) = \sigma(a)$ для $a \in P_1$.

Поле $\overline{P}_1$ является минимальным полем разложения многочлена $f(x)$ над полем $P_1(\alpha_1)$, поскольку $\overline{P}_1 = P_1(\alpha_1, \ldots, \alpha_n) = P(\alpha_1)(\alpha_2, \ldots, \alpha_n)$. Аналогично $\overline{P}_2$ — минимальное поле разложения многочлена $\sigma'(f(x))$ над полем $P_2(\beta_1)$.

Так как $d_{P_1(\alpha_1)}(f) < k$ и $\sigma'(f(x)) = \tau'(f(x))$, то по предположению индукции существует изоморфизм $\varphi\colon \overline{P}_1 \to \overline{P}_2$, при котором $\varphi(\gamma) = \tau(\gamma)$ для $\gamma \in P_1(\alpha_1)$. Тогда $\varphi(a) = \tau(a) = \sigma(a)$ для $a \in P_1$. □

Следствие. *Пусть P' и P'' — произвольные минимальные поля разложения многочлена $f(x) \in P[x]$ над P. Тогда поля P' и P'' изоморфны над P.*

Для произвольного поля P и произвольного многочлена $f(x) \in P[x]$, $\deg f(x) \geqslant 1$, мы доказали существование поля, содержащего P и все корни $f(x)$. Представляют интерес поля, в которых содержатся все корни всех многочленов над ними.

По определению 19 главы 9 поле P называют *алгебраически замкнутым*, если в нем содержатся все корни любого многочлена $f(x) \in P[x]$ степени $\deg f(x) \geqslant 1$.

Пример 16. Поле $\mathbb{C}$ алгебраически замкнуто в силу теоремы Гаусса (см. теорему 25 главы 9).

Определение 13. Алгебраическое расширение поля P, являющееся алгебраически замкнутым полем, называется *алгебраическим замыканием* поля P.

Приведем без доказательства теорему о существовании алгебраического замыкания поля.

Теорема (Штейниц). *Для любого поля P существует его алгебраическое замыкание $\overline{P}$. Любые два алгебраических замыкания поля P изоморфны над P.*

Опираясь на теорему Штейница, можно привести пример алгебраического расширения поля, имеющего бесконечную степень.

Пример 17. Алгебраическое замыкание $\overline{\mathbb{Q}}$ поля $\mathbb{Q}$ является расширением бесконечной степени, так как над полем $\mathbb{Q}$ существуют неприводимые многочлены любой степени (см. следствие теоремы 31 главы 9).

ЗАДАЧИ

1. Постройте поле частных для кольца $2\mathbb{Z}$.

2. Покажите, что для любого поля P его аддитивная группа $(P, +)$ не изоморфна мультипликативной группе $(P^*, \cdot)$.

3. Покажите, что подполе $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ поля $\mathbb{R}$ есть множество чисел следующего вида $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$, где $a, b, c, d \in \mathbb{Q}$.

4. Покажите, что $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

5. Покажите, что $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.

6. Докажите, что если $[P' : P] = p$, где p — простое число, то в поле P' нет подполей, содержащих P и отличных от P' и P, и P' — простое расширение P.

7. Найдите минимальный многочлен элемента $1 + i \in \mathbb{C}$ над полем $\mathbb{Q}$.

8. В поле $P(x)$ рассмотрите расширение $P(x^2)$ поля P, порожденное элементом x^2. Покажите, что $[P(x) : P(x^2)] = 2$, а элемент x^2 трансцендентен над P.

9. Докажите, что любой многочлен $f(x) \in P[x]$, где $\deg f(x) = n > 0$, трансцендентен над полем P, а $[P(x) : P(f(x))] \leqslant n$.

10. Докажите, что всякая рациональная функция $f(x)g(x)^{-1} \in P(x)$, где $(f(x), g(x)) = e$ и $\deg g(x) > 0$ или $\deg f(x) > 0$, трансцендентна над полем P.

11. Пусть $P \subset P'$ и $A(P)$ — совокупность всех элементов из P', алгебраических над P. Покажите, что $A(P)$ — подполе поля P', содержащее P.

12. Проверьте, что многочлен $f(x) = x^3 + x + e$ неприводим над полем $P = GF(2)$, и постройте поле $P(\alpha)$, порожденное корнем этого многочлена.

13. Пусть α и β — соответственно корни в поле $\mathbb{C}$ неприводимых над $\mathbb{Q}$ многочленов $x^2 + 1$ и $x^2 + 2$. Покажите, что $\mathbb{Q}(\alpha) \ncong \mathbb{Q}(\beta)$.

14. Пусть P' — алгебраическое расширение поля P, а P'' — алгебраическое расширение поля P'. Покажите, что P'' — алгебраическое расширение поля P.

15. Для многочлена $x^3 - 2 \in \mathbb{Q}[x]$ постройте минимальное поле разложения T в $\mathbb{C}$. Найдите степень $[T : \mathbb{Q}]$.

16. Пусть P' — расширение поля P, $\alpha_1, \ldots, \alpha_n$ — элементы из P'. Докажите, что $P(\alpha_1, \ldots, \alpha_n) = P[\alpha_1, \ldots, \alpha_n]$ тогда и только тогда, когда элементы $\alpha_1, \ldots, \alpha_n$ алгебраичны над полем P.

Глава 22

КОНЕЧНЫЕ ПОЛЯ И МНОГОЧЛЕНЫ НАД НИМИ

Теория конечных полей (*полей Галуа*) представляет собой хорошую иллюстрацию общей теории полей, так как для конечных полей решение многих задач из этой общей теории, не имеющих удовлетворительного решения в целом, может быть доведено до конца. Примерами конечных полей служат поля вычетов $\mathbb{Z}/p$, где p — простое число, и $\mathbb{Z}/p[x]/f(x)$, где многочлен $f(x)$ неприводим над $\mathbb{Z}/p$.

§ 1. ОСНОВНЫЕ СВОЙСТВА КОНЕЧНЫХ ПОЛЕЙ

Рассмотрим вопрос о возможном числе элементов конечного поля.

Теорема 1. *Если P — конечное поле, то $|P| = p^t$, где p — простое число и $t \in \mathbb{N}$. При этом*

(а) $p = \operatorname{Char} P$;

(б) $t = [P : P_0]$, *где P_0 — простое подполе поля P*;

(в) *поле P является минимальным полем разложения над P_0 многочлена $x^{p^t} - x \in P_0[x]$ и совпадает с множеством всех его корней.*

□ Так как P — конечное поле, то конечно его простое подполе P_0 и конечна степень расширения $[P : P_0]$. По теореме 7 главы 21 $P_0 \cong \mathbb{Z}/p$ для некоторого простого $p \in \mathbb{N}$. Отсюда следует, что $\operatorname{Char} P = \operatorname{Char} P_0 = p$ и $|P| = p^t$, где $t = [P : P_0]$.

Остается доказать утверждение (в). Поскольку порядок группы P^* равен $p^t - 1$, то $a^{p^t-1} = e$ для всех $a \in P^*$. Теперь ясно, что совокупность элементов поля P является множеством корней многочлена $F(x) = x(x^{p^t-1} - e) = x^{p^t} - x$. □

Следствие. *Если P — поле из p^t элементов и $a \in P$, то для любого $s \in \mathbb{N}$ справедливо равенство $a^{p^{ts}} = a$.*

□ Доказательство проводится индукцией по s и предоставляется читателю. □

Теорема 2. *Для любого простого числа p и любого $t \in \mathbb{N}$ существует единственное с точностью до изоморфизма поле, состоящее из p^t элементов.*

□ Для простого числа p и произвольного $t \in \mathbb{N}$ рассмотрим многочлен $F(x) = x^{p^t} - x \in \mathbb{Z}/p[x]$. По теореме 21 главы 21 существует минимальное поле разложения P' многочлена $F(x)$ над $\mathbb{Z}/p$. Так как $F'(x) = p^t x^{p^t-1} - e = -e$,

то $(F(x), F'(x)) = e$. Значит, многочлен $F(x)$ не имеет в поле P' кратных корней. Пусть $M = \{\alpha_1, \alpha_2, \ldots, \alpha_{p^t}\}$ — множество всех его различных корней в P'. Тогда справедливы равенства

$$\alpha_i^{p^t} = \alpha_i, \quad i \in \overline{1, p^t}, \tag{1}$$

из которых следует, что

$$(\alpha_i \alpha_j)^{p^t} = \alpha_i^{p^t} \alpha_j^{p^t} = \alpha_i \alpha_j, \quad i, j \in \overline{1, p^t}. \tag{2}$$

Ввиду утверждения 9 главы 20 и равенств (1) получаем:

$$(\alpha_i + \alpha_j)^{p^t} = \alpha_i^{p^t} + \alpha_j^{p^t} = \alpha_i + \alpha_j. \tag{3}$$

Равенства (2) и (3) показывают, что множество M замкнуто относительно операций сложения и умножения. Поскольку множество M конечно, то по утверждению 2 главы 21 M — поле. Оно состоит из p^t элементов.

Пусть теперь P_1 и P_2 — произвольные поля с единицами соответственно e_1 и e_2, состоящие из p^t элементов. По теореме 1(в) поле P_i является минимальным полем разложения многочлена $F_i(x) = e_i x^{p^t} - e_i x \in P_{0i}[x]$ над простым подполем P_{0i} поля P_i, $i \in \overline{1, 2}$ (см. замечание 3 главы 20).

Так как $\operatorname{Char} P_{01} = \operatorname{Char} P_{02} = p$, то по теореме 7 главы 21 каждое из полей P_{01} и P_{02} изоморфно полю $\mathbb{Z}/p$. Значит, существует изоморфизм полей $\sigma\colon P_{01} \to P_{02}$ и изоморфизм колец $\sigma'\colon P_{01}[x] \to P_{02}[x]$, при котором $\sigma'\left(\sum_{i=0}^m a_i x^i\right) = \sum_{i=0}^m \sigma(a_i) x^i$. Ясно, что $\sigma'(F_1(x)) = F_2(x)$. Поэтому по теореме 22 главы 21 поля P_1 и P_2 изоморфны. □

Теорема 2 позволяет при рассмотрении многих вопросов, связанных с конечными полями, фиксировать произвольное поле из p^t элементов, которое обозначается в таком случае через $GF(p^t)$.

В дальнейшем мы будем использовать следующие признаки делимости многочленов и целых чисел.

Лемма 3. (а) *Для любых $r, s, a \in \mathbb{N}$ число $a^r - 1$ делит число $a^{rs} - 1$.*

(б) *Для любых $r, s \in \mathbb{N}$ и любого поля P многочлен $g(x) = x^r - e \in P[x]$ делит многочлен $f(x) = x^{rs} - e \in P[x]$.*

□ Непосредственно проверяются равенства

$$a^{rs} - 1 = (a^r - 1)(a^{r(s-1)} + \ldots + a^r + 1),$$
$$x^{rs} - e = (x^r - e)(x^{r(s-1)} + \ldots + x^r + e). \quad \square$$

Опишем подполя данного конечного поля.

Теорема 4. *Пусть P_1, P_2 — конечные поля. Поле P_1 содержит подполе, изоморфное полю P_2, тогда и только тогда, когда $|P_1| = |P_2|^t$ для некоторого $t \in \mathbb{N}$. При выполнении последнего условия в поле P_1 содержится единственное подполе, изоморфное полю P_2.*

□ Пусть T — подполе поля P_1 и $T \cong P_2$. Тогда $|T| = |P_2|$. Так как P_1 — пространство над T, то для $t = [P_1 : T]$ имеем $|P_1| = |P_2|^t$.

Обратно, пусть $|P_1| = |P_2|^t$. Поскольку $|P_1| = p_1^k$, а $|P_2| = p_2^l$, где p_1, p_2 — простые числа и $k, l \in \mathbb{N}$, то $p_1^k = p_2^{lt}$. По основной теореме арифметики $p_1 = p_2 = p$ и $k = lt$.

По лемме 3(а) $p^l - 1 \mid p^k - 1$. Тогда по лемме 3(б) $x^{p^l-1} - e \mid x^{p^k-1} - e$, и, значит, для многочленов $G(x) = x^{p^l} - x$ и $F(x) = x^{p^k} - x$ выполнено соотношение $G(x) \mid F(x)$. По теореме 1 поле P_1 — минимальное поле разложения многочлена $F(x)$ над простым подполем P_0. Так как $G(x) \mid F(x)$, то многочлен $G(x)$ раскладывается над полем P_1 на линейные множители. Как и в доказательстве теоремы 2, получаем, что корни многочлена $G(x)$ образуют в поле P_1 подполе T, состоящее из $p^l = |P_2|$ элементов. По теореме 2 $T \cong P_2$.

Предположим, что в P_1 содержится подполе T_1, также состоящее из p^l элементов. Если $T_1 \neq T$, то многочлен $G(x) = x^{p^l} - x$ имеет в поле P_1 больше, чем p^l корней, что невозможно. Значит, T — единственное подполе поля P_1, содержащее p^l элементов. □

Следствие. *В поле $P = GF(p^t)$ для любого $d \in \mathbb{N}$ такого, что $d \mid t$, существует единственное подполе из p^d элементов. Этими полями исчерпываются все подполя поля P.*

Рассмотрим мультипликативную группу поля P. Через $\operatorname{Ord} a$ будем обозначать порядок элемента $a \in (P^*, \cdot)$ — *мультипликативный порядок* a.

Определение 1. Элемент a поля $P = GF(p^t)$ называют *примитивным*, если все ненулевые элементы поля P суть степени элемента a, т. е. если $(P^*, \cdot) = \langle a \rangle$.

Теорема 5 (о примитивном элементе). *В поле $P = GF(p^t)$ существует примитивный элемент.*

□ Группа $(P^*, \cdot)$ абелева и конечная. По утверждению 4 главы 11 в ней существует такой элемент a, что $\operatorname{Ord} a = \exp P^*$. Значит, любой элемент $b \in P^*$ удовлетворяет соотношению $b^{\operatorname{Ord} a} = e$. Если $\operatorname{Ord} a < |P^*| = p^t - 1$, то многочлен $x^{\operatorname{Ord} a} - e$ имеет в поле P больше корней, чем его степень, что невозможно. Поэтому $\operatorname{Ord} a = p^t - 1$, и $(P^*, \cdot) = \langle a \rangle$. Ясно, что a — примитивный элемент поля P. □

Следствие. *Поле $P = GF(p^t)$ является простым алгебраическим расширением любого своего подполя.*

□ Например, поле P, как расширение любого своего подполя, порождается каждым своим примитивным элементом. □

§ 2. НЕПРИВОДИМЫЕ МНОГОЧЛЕНЫ НАД КОНЕЧНЫМИ ПОЛЯМИ

Покажем, что над любым конечным полем существуют неприводимые многочлены любой степени $n \geqslant 1$.

Теорема 6. *Если $P = GF(p^t)$, то для любого $n \in \mathbb{N}$ существует многочлен $f(x) \in P[x]$ степени n, неприводимый над P.*

□ Пусть $P' = GF(p^{tn})$ — минимальное поле разложения многочлена $F(x) = x^{p^{tn}} - x \in P[x]$ над P (см. доказательство теоремы 2). По следствию теоремы 5 $P' = P(a)$, где a — примитивный элемент поля P'.

Так как элемент a алгебраичен над полем P, то он — корень некоторого неприводимого над P многочлена $f(x) \in P[x]$. По утверждению 14 главы 21 $[P' : P] = \deg f(x)$. А поскольку $[P' : P] = n$, то $\deg f(x) = n$. □

Из теоремы 6 вытекает следующий способ построения поля из p^t элементов, который обычно используется на практике. Выбирается простое поле $\mathbb{Z}_p$ и неприводимый многочлен $f(x) \in \mathbb{Z}_p[x]$ степени t, существующий по теореме 6. Факторкольцо $\mathbb{Z}_p[x]/f(x)$ есть искомое поле.

Опишем корни неприводимого многочлена над конечным полем.

Теорема 7. *Пусть $f(x)$ — неприводимый многочлен степени n над полем $P = GF(q)$, $q = p^t$, и $S = P(\alpha)$ — расширение поля P, порожденное корнем α многочлена $f(x)$. Тогда справедливы следующие утверждения*:

(а) *S — минимальное поле разложения многочлена $f(x)$ над P,*[28] *причем $f(x)$ имеет в S ровно n различных корней*

$$\alpha,\ \alpha^q,\ \ldots,\ \alpha^{q^{n-1}}; \tag{4}$$

(б) $f(x) \mid x^{q^n} - x$.

□ (а) Пусть $f(x) = \sum_{i=0}^{n} f_i x^i$. Так как $f_i \in P$, то по следствию теоремы 1 $f_i^q = f_i$ при $i \in \overline{0,n}$. Поэтому для любого $s \in \mathbb{N}_0$ справедливы равенства

$$f(\alpha^{q^s}) = \sum_{i=0}^{n} f_i (\alpha^{q^s})^i = \sum_{i=0}^{n} (f_i \alpha^i)^{q^s} = f(\alpha)^{q^s} = 0.$$

Значит, все элементы вида (4) являются корнями многочлена $f(x)$.

Докажем, что они различны. Допустим, что $\alpha^{q^s} = \alpha^{q^t}$, где $0 \leqslant s < t \leqslant n-1$. Тогда при $r = t - s$ получаем $\alpha^{q^{s+r}} - \alpha^{q^s} = \left(\alpha^{q^r} - \alpha\right)^{q^s} = 0$ и, стало быть,

$$\alpha^{q^r} = \alpha, \quad 0 < r < n. \tag{5}$$

Элементы поля S имеют вид $\beta = \sum_{i=0}^{n-1} c_i \alpha^i$, где $c_i \in P$. Поскольку $c_i^{q^r} = c_i$ при $i \in \overline{0, n-1}$, то ввиду (5) $\beta^{q^r} = \beta$. Следовательно, все q^n элементов поля S являются

[28] Полезно заметить, что если P — произвольное поле, то это утверждение неверно (покажите).

корнями многочлена $x^{q^r}-x$, что невозможно в силу условия $r<n$. Поэтому элементы системы (4) различны.

(б) Так как $[S:P]=\deg f(x)=n$, то $|S|=q^n$, и по теореме 1(в) все элементы поля S — корни многочлена $G(x)=x^{q^n}-x\in P[x]$. Поэтому $G(x)$ и $f(x)$ не взаимно просты над полем S, а тогда и над полем P. Ввиду неприводимости многочлена $f(x)$ получаем $f(x)\mid G(x)$. □

Следствие 1. *Если $f(x)$ — неприводимый многочлен степени n над полем $P=GF(q)$, $f(x)\neq x$, и α, β — его корни в некотором поле разложения над P, то*

(а) $\operatorname{Ord}\alpha=\operatorname{Ord}\beta$;

(б) $\operatorname{Ord}\alpha\mid q^n-1$;

(в) $\operatorname{Ord}\alpha\nmid q^r-1$, *если* $0<r<n$.

В частности, $(\operatorname{Ord}\alpha,p)=1$.

□ (а) Пусть $\operatorname{Ord}\alpha=d$. Тогда α — корень многочлена $x^d-e\in P[x]$. Следовательно, $(f(x),x^d-e)\neq e$, и поэтому $f(x)\mid x^d-e$. Поскольку $f(\beta)=0$, то $\operatorname{Ord}\beta\leqslant d=\operatorname{Ord}\alpha$.

Аналогично показывается, что $\operatorname{Ord}\alpha\leqslant\operatorname{Ord}\beta$.

(б) По теореме 7(б) $f(x)\mid(x^{q^n-1}-e)x$. Ввиду неприводимости многочлена $f(x)$ и условия $f(x)\neq x$, получаем $f(x)\mid x^{q^n-1}-e$. Стало быть, $\operatorname{Ord}\alpha\mid q^n-1$.

(в) Утверждение (в), по сути дела, доказано при доказательстве пункта (а) теоремы 7. □

Следствие 2. *Неприводимый многочлен над конечным полем взаимно прост со своей производной.*

□ Утверждение справедливо ввиду теоремы 7(а) и следствия 2 теоремы 23 главы 9. □

Минимальное поле разложения неприводимого над конечным полем многочлена является полем разложения одновременно для целого класса многочленов.

Утверждение 8. *В условиях теоремы 7 поле $P(\alpha)$ является полем разложения любого неприводимого над P многочлена $g(x)\in P[x]$, для которого* $\deg g(x)\mid n$, *и не содержит ни одного корня неприводимого над P многочлена $h(x)\in P[x]$, для которого* $\deg h(x)\nmid n$.

□ Если $g(x)\in P[x]$ — неприводимый над P многочлен степени m, то ввиду теоремы 7(б) $g(x)\mid x^{q^m}-x$. Пусть $m\mid n$. Тогда по лемме 3(а) $q^m-1\mid q^n-1$ и по лемме 3(б) $x^{q^m-1}-e\mid x^{q^n-1}-e$. Следовательно, $x^{q^m}-x\mid x^{q^n}-x$. Таким образом, $g(x)\mid x^{q^n}-x$, и по теореме 1(в) $P(\alpha)$ — поле разложения многочлена $g(x)$.

Если неприводимый над P многочлен $g(x)$ степени m имеет корень $\gamma\in P(\alpha)$, то $[P(\gamma):P]=m$. Тогда по теореме о башне полей, примененной к башне $P(\alpha)\supset P(\gamma)\supset P$, получаем $m\mid n$. □

§ 3. КРИТЕРИЙ НЕПРИВОДИМОСТИ МНОГОЧЛЕНА НАД КОНЕЧНЫМ ПОЛЕМ

Всюду далее в этом параграфе $P = GF(q)$, $q = p^t$, p — простое число. Для проверки неприводимости над P заданного унитарного многочлена $f(x) \in P[x]$ степени n существует простейший алгоритм: перебор всех унитарных многочленов $g(x) \in P[x]$ степени $m \leqslant n/2$ и проверка (делением с остатком) условия $g(x) \mid f(x)$. Однако, это — слишком трудоемкий алгоритм.

Ниже предлагается гораздо более простой алгоритм, основанный на следующем критерии.

Теорема 9 (Батлер, 1954).[29] *Многочлен $f(x) \in P[x]$ степени $n > 0$ неприводим над полем $P = GF(p^t)$ тогда и только тогда, когда выполнены условия*:

(а) $(f(x), f'(x)) = e$;

(б) *уравнение*

$$z^q - z = 0 \tag{6}$$

имеет в кольце $R = P[x]/f(x)$ ровно q решений.

□ Уравнение (6) имеет в кольце R по крайней мере q решений: это элементы множества

$$\overline{P} = \{[a]_f : \ a \in P\}.$$

Действительно, $[a]_f^{p^t} = [a^{p^t}]_f = [a]_f$. При этом $[a_1]_f \neq [a_2]_f$, если $a_1, a_2 \in P$ и $a_1 \neq a_2$, поскольку $f(x) \nmid a_2 - a_1$.

Пусть многочлен $f(x)$ неприводим над P. Тогда по следствию 2 теоремы 7 выполнено условие (а). Кроме того, в этом случае R — поле, и поэтому уравнение (6) не может иметь в R более q решений. Значит, выполнено условие (б).

Обратно, пусть выполнены условия (а) и (б). Тогда уравнение (6) не имеет в R других решений, кроме элементов множества $\overline{P}$. Предположим, что многочлен $f(x)$ приводим над полем P. Тогда $n > 1$ и существуют такие многочлены $f_1(x)$, $f_2(x) \in P[x]$, что

$$f(x) = f_1(x)f_2(x), \quad 1 \leqslant \deg f_i(x) < n, \quad i \in \overline{1,2}.$$

Покажем, что уравнение (6) имеет решение в $R \setminus \overline{P}$, и тем самым придем к противоречию, доказывающему неприводимость $f(x)$. Из условия (а) следует, что $(f_1(x), f_2(x)) = e$. Поэтому существуют такие многочлены $u(x), v(x) \in P[x]$, что

$$u(x)f_1(x) + v(x)f_2(x) = e. \tag{7}$$

При этом можно считать, что $\deg u(x) < \deg f_2(x)$ (иначе, разделим $u(x)$ на $f_2(x)$ с остатком: $u(x) = q(x)f_2(x) + r(x)$, и получим $r(x)f_1(x) + (q(x)f_1(x) + v(x))f_2(x) = e$). Ясно также, что $u(x) \neq 0$. Таким образом, $0 < \deg u(x)f_1(x) < \deg f(x)$, и элемент $\varepsilon = [u(x)f_1(x)]_f \in R$ удовлетворяет условию $\varepsilon \in R \setminus \overline{P}$.

[29] М. Батлер — современный американский математик.

Умножая обе части равенства (7) на $u(x)f_1(x)$, получаем

$$(u(x)f_1(x))^2 + u(x)v(x)f(x) = u(x)f_1(x).$$

Отсюда следует равенство $\varepsilon^2 = \varepsilon$, а значит и равенство $\varepsilon^q = \varepsilon$. Таким образом, ε — $(q+1)$-е решение уравнения (6) в кольце R, что противоречит условию (б). Теорема доказана.[30] $\square$

Используя теорему 9, получим практический способ распознавания приводимости или неприводимости многочлена $f(x) \in P[x]$ над P. Можно считать, что $\deg f(x) = n > 1$.

1. Если $(f(x), f'(x)) \neq e$, то по теореме 9 многочлен $f(x)$ приводим над P.

2. Пусть $(f(x), f'(x)) = e$. Подсчитаем число решений уравнения (6) в кольце R.

Произвольный элемент кольца R можно записать в виде $[c(x)]_f = [c_0 + c_1x + \ldots$ $\ldots + c_{n-1}x^{n-1}]_f$, где $c_i \in P$. Элемент $[c(x)]_f$ является решением уравнения (6) тогда и только тогда, когда справедливо равенство

$$[c(x)^q]_f = [c(x)]_f,$$

которое можно записать в виде

$$[c_0^{p^t} + c_1^{p^t}x^{p^t} + \ldots + c_{n-1}^{p^t}x^{(n-1)p^t}]_f = [c_0 + \ldots + c_{n-1}x^{n-1}]_f,$$

или в виде

$$[c_0 \cdot 0 + c_1(x^{p^t} - x) + \ldots + c_{n-1}(x^{(n-1)p^t} - x^{n-1})]_f = [0]_f, \tag{8}$$

если учесть, что $c_i^{p^t} = c_i$, $i \in \overline{0, n-1}$.

Для каждого $i \in \overline{1, n-1}$ существует такой однозначно определенный многочлен

$$\alpha_i(x) = \alpha_{0,i} + \alpha_{1,i}x + \ldots + \alpha_{n-1,i}x^{n-1} \in P[x],$$

что

$$[x^{iq} - x^i]_f = [\alpha_i(x)]_f.$$

Поэтому равенство (8) можно переписать в виде

$$[c_0 \cdot 0 + c_1\alpha_1(x) + \ldots + c_{n-1}\alpha_{n-1}(x)]_f = [0]_f. \tag{9}$$

Так как $\deg f(x) = n$, а $\deg \alpha_i(x) < n$ при $i \in \overline{1, n-1}$, то равенство (9) в кольце R эквивалентно равенству в кольце $P[x]$:

$$c_0 \cdot 0 + c_1\alpha_1(x) + \ldots + c_{n-1}\alpha_{n-1}(x) = 0. \tag{10}$$

Приравнивая коэффициенты при одинаковых степенях x в правой и левой частях равенства (10), получим систему линейных уравнений

$$\begin{cases} 0c_0 + \alpha_{0,1}c_1 + \ldots + \alpha_{0,n-1}c_{n-1} = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ 0c_0 + \alpha_{n-1,1}c_1 + \ldots + \alpha_{n-1,n-1}c_{n-1} = 0, \end{cases}$$

[30] Приведенное доказательство теоремы Батлера предложено А. В. Куприяновым.

которую запишем в матричной форме:

$$AC^{\downarrow} = 0^{\downarrow}, \tag{11}$$

где

$$A = \begin{pmatrix} 0 & \alpha_{0,1} & \dots & \alpha_{0,n-1} \\ \dots & \dots & \dots & \dots \\ 0 & \alpha_{n-1,1} & \dots & \alpha_{n-1,n-1} \end{pmatrix}.$$

Таким образом, число решений уравнения (6) в кольце R равно числу решений системы линейных уравнений (11), т. е. равно $q^{n-\operatorname{rang} A}$. По теореме 9 многочлен $f(x)$ неприводим над P тогда и только тогда, когда $n - \operatorname{rang} A = 1$, т. е. $\operatorname{rang} A = n - 1$.

Изложенный алгоритм позволяет не только ответить на вопрос: приводим или неприводим многочлен $f(x)$ над полем $P = GF(p^t)$. Используя его, можно разложить многочлен $f(x)$ в случае приводимости в произведение многочленов меньших степеней. Рассмотрим два случая.

Случай 1. $d(x) = (f(x), f'(x)) \neq e$. Если при этом $f'(x) \neq 0$, то $0 \leqslant \deg f'(x) < n$. Значит, $0 < \deg d(x) < n$ и $f(x) = d(x)f_1(x)$, где $0 < \deg f_1(x) < n$.

Пусть $f'(x) = 0$. Из равенств

$$f(x) = \sum_{i=0}^{n} f_i x^i, \quad f'(x) = \sum_{i=1}^{n} i f_i x^{i-1} = 0$$

получаем, что $if_i = 0$ при $i \in \overline{1,n}$. Следовательно, если $j \in \overline{1,n}$ и $f_j \neq 0$, то $p \mid j$, так как $\operatorname{Char} P = p$. Поэтому многочлен $f(x)$ имеет вид

$$f(x) = f_n x^{p\cdot(n/p)} + \ldots + f_j x^{p\cdot(j/p)} + \ldots + f_0 \quad (f_j \neq 0).$$

Ввиду равенств $\left(f_j^{p^{t-1}}\right)^p = f_j$ можем записать:

$$f(x) = h_n^p\, x^{p\cdot(n/p)} + \ldots + h_j^p\, x^{p\cdot(j/p)} + \ldots + h_0^p = h(x)^p,$$

где $h(x) = h_n x^{n/p} + \ldots + h_j x^{j/p} + \ldots + h_0$ и $h_j = f_j^{p^{t-1}}$, $f_j \neq 0$.

Случай 2. $(f(x), f'(x)) = e$. Пусть многочлен $f(x)$ приводим над полем P. В этом случае $\operatorname{rang} A < n-1$, и существует ненулевое решение $c^{\downarrow} = (c_0, \ldots, c_{n-1})^T$ системы уравнений (11), где $c_i \neq 0$ при некотором $i \in \overline{1, n-1}$. Тогда $[c(x)]_f$ — решение уравнения (6), где $c(x) = c_0 + c_1 x + \ldots + c_{n-1}x^{n-1}$, $0 < \deg c(x) < n$.

Теорема 10 (Берлекэмп, 1967).[31] *Если $P = GF(p^t)$, $f(x) \in P[x]$ — унитарный многочлен степени n и $[c(x)]_f$ — такое решение уравнения* (6)*, что $0 < \deg c(x) < n$, то*

$$f(x) = \prod_{\alpha \in P} (f(x),\, c(x) - \alpha), \tag{12}$$

и существует такой элемент $\beta \in P$, что $0 < \deg(f(x),\, c(x) - \beta) < n$.

[31] Е. Р. Берлекэмп — современный американский математик.

Сначала докажем вспомогательное утверждение.

Лемма 11. *Пусть P — произвольное поле, $a_i(x) \in P[x]$, $i \in \overline{1,k}$, и $(a_i(x), a_j(x)) = e$ при $i \neq j$. Если $f(x)$ — такой унитарный многочлен из $P[x]$, что $f(x) \mid \prod_{i=1}^{k} a_i(x)$, то*

$$f(x) = \prod_{i=1}^{k} (f(x),\, a_i(x)).$$

□ Пусть $k = 2$. Обозначим $f_i(x) = (f(x),\, a_i(x))$ для $i = 1, 2$. Из условия $(a_1(x), a_2(x)) = e$ получаем условие $(f_1(x), f_2(x)) = e$. Отсюда и из соотношений

$$f_1(x) \mid f(x), \quad f_2(x) \mid f(x)$$

по свойству взаимно простых многочленов следует соотношение

$$f_1(x) f_2(x) \mid f(x). \tag{13}$$

Для подходящих многочленов $u_i(x), v_i(x) \in P[x]$ справедливы равенства

$$\begin{aligned} f_1(x) &= f(x)u_1(x) + a_1(x)v_1(x), \\ f_2(x) &= f(x)u_2(x) + a_2(x)v_2(x). \end{aligned} \tag{14}$$

Перемножив левые и правые части равенств (14), ввиду условия $f(x) \mid a_1(x)a_2(x)$ получим:

$$f(x) \mid f_1(x) f_2(x). \tag{15}$$

Из соотношений (13) и (15) получаем требуемое равенство

$$f(x) = (f(x), a_1(x)) \cdot (f(x), a_2(x)),$$

так как $f(x)$, $(f(x),\, a_1(x))$ и $(f(x),\, a_2(x))$ — унитарные многочлены. Дальнейшее доказательство проводится индукцией. □

Перейдем к доказательству теоремы.

□ По теореме 1 справедливо равенство

$$x^q - x = \prod_{\alpha \in P} (x - \alpha).$$

Рассмотрим многочлен $F(y) = y^q - y = \prod_{\alpha \in P}(y - \alpha) \in P[y]$. Так как $P[x] \supset P$, то для значения многочлена $F(y)$ в точке $c(x) \in P[x]$ получаем равенство

$$c(x)^{p^t} - c(x) = \prod_{\alpha \in P} (c(x) - \alpha). \tag{16}$$

Если $\alpha, \beta \in P$ и $\alpha \neq \beta$, то

$$(c(x) - \alpha,\, c(x) - \beta) = e, \tag{17}$$

так как $c(x) - \alpha = (c(x) - \beta) + (\beta - \alpha)$. По условию $[c(x)]_f^q = [c(x)]_f$. Значит, $f(x) \mid c(x)^{p^t} - c(x)$. Учитывая равенство (16), получаем

$$f(x) \Big| \prod_{\alpha \in P} (c(x) - \alpha). \tag{18}$$

В силу леммы 11 из равенства (17) и соотношения (18) следует требуемое равенство (12), а ввиду условий $0 < \deg c(x) < n$ существует нужный элемент β. $\square$

Условие унитарности многочлена $f(x)$ в теореме 10 не ограничивает общности, так как произвольный многочлен $f(x)$ можно записать в виде $f(x) = f_n \cdot f^*(x)$, где f_n — старший коэффициент многочлена $f(x)$, а $f^*(x)$ — унитарный ассоциированный с $f(x)$ многочлен.

Пример 1. Выяснить, приводим или нет многочлен $f(x) = x^4 - 2 \in GF(3)[x]$ над полем $GF(3)$, и в случае приводимости разложить его на множители.

Так как $(f(x), f'(x)) = (x^4 - 2, x^3) = e$, то имеет место случай 2. Вычислим многочлены $\alpha_i(x)$, $i \in \overline{1,3}$.

$i = 1$: $x^3 - x \equiv x^3 + 2x \pmod{f(x)}$, отсюда $\alpha_1(x) = 0 + 2x + 0x^2 + 1x^3$.

$i = 2$: так как $x^4 \equiv 2 \pmod{f(x)}$, то $x^6 \equiv 2x^2 \pmod{f(x)}$ и $x^6 - x^2 \equiv 2x^2 + 2x^2 \equiv$ $\equiv x^2 \pmod{f(x)}$. Поэтому $\alpha_2(x) = 0 + 0x + 1x^2 + 0x^3$.

$i = 3$: так как $x^5 \equiv 2x \pmod{f(x)}$, то $x^9 \equiv 4x \pmod{f(x)}$ и $x^9 \equiv x \pmod{f(x)}$. Значит, $x^9 - x^3 \equiv x + 2x^3 \pmod{f(x)}$ и $\alpha_3(x) = 0 + 1x + 0x^2 + 2x^3$.

Система уравнений (11) имеет вид:

$$AC^{\downarrow} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}. \tag{19}$$

Легко проверить, что $\operatorname{rang} A = 2 < n-1 = 3$. Следовательно, многочлен $f(x)$ приводим над $GF(3)$.

Общее решение системы (19) имеет вид $c^{\downarrow} = (c_0, c_1, 0, c_1)^T$. Поэтому можно выбрать решение уравнения (6) $c(x) = x^3 + x$. По теореме 10

$$f(x) = x^4 - 2 = (x^4 - 2,\, x^3 + x)(x^4 - 2,\, x^3 + x - 1)(x^4 - 2,\, x^3 + x - 2).$$

Нетрудно проверить, что

$$f(x) = (x^2 + 2x + 2)(x^2 + x + 2).$$

§ 4. ЧИСЛО НЕПРИВОДИМЫХ МНОГОЧЛЕНОВ ДАННОЙ СТЕПЕНИ

Для определения числа неприводимых многочленов данной степени над конечным полем рассмотрим сначала некоторые числовые функции.

Определение 2. *Функция Мёбиуса*[32] $\mu(n)$ от натурального аргумента n определяется следующим образом: если n имеет каноническое разложение $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, то

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1, \\ (-1)^k, & \text{если } \alpha_1 = \ldots = \alpha_k = 1, \\ 0, & \text{если существует } \alpha_i > 1. \end{cases}$$

Утверждение 12. *При любом $n \in \mathbb{N}$ справедливы равенства*:

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \textit{если } n = 1, \\ 0, & \textit{если } n \neq 1. \end{cases}$$

□ При $n = 1$ по определению 2 $\mu(1) = 1$. Пусть $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. При подсчете суммы $\sum_{d|n} \mu(d)$ следует рассматривать только делители d числа n, имеющие вид $d = 1$ и $d = p_{i_1} \dots p_{i_s}$, где $i_j \in \overline{1,k}$, $i_l \neq i_m$ при $l \neq m$. Тогда

$$\sum_{d|n} \mu(d) = \mu(1) + \sum_{i=1}^{k} \mu(p_i) + \sum_{i<j} \mu(p_i p_j) + \ldots + \mu(p_1 \dots p_k) =$$
$$= 1 - C_k^1 + C_k^2 + \ldots + (-1)^s C_k^s + \ldots + (-1)^k = (1-1)^k = 0. \quad \square$$

Утверждение 13 (формула обращения Мёбиуса). *Если $F(n)$ и $f(n)$ — функции натурального аргумента, связанные при любом $n \in \mathbb{N}$ соотношением*

$$\sum_{d|n} f(d) = F(n), \tag{20}$$

то при любом $n \in \mathbb{N}$ имеет место равенство

$$\sum_{d|n} F(n/d)\mu(d) = f(n). \tag{21}$$

□ Пользуясь равенством (20), запишем левую часть доказываемого равенства (21) в виде

$$\sum_{d|n} \left(\sum_{d_1 | \frac{n}{d}} f(d_1) \right) \mu(d) \tag{22}$$

[32] А. Ф. Мёбиус (1790–1868) — немецкий математик.

и соберем коэффициенты при $f(d_1)$ для каждого фиксированного d_1. Значение $\mu(d)$ является одним из коэффициентов при $f(d_1)$ тогда и только тогда, когда $d \mid n$ и $d_1 \mid \frac{n}{d}$, т. е. когда $d \mid \frac{n}{d_1}$. По утверждению 12

$$\sum_{d \mid \frac{n}{d_1}} \mu(d) = \begin{cases} 1, & \text{если } \frac{n}{d_1} = 1, \text{ т. е. при } d_1 = n, \\ 0, & \text{если } \frac{n}{d_1} \neq 1, \text{ т. е. при } d_1 \neq n. \end{cases}$$

Таким образом, в сумме (22) остается лишь одно ненулевое слагаемое — $1 \cdot f(n)$. Этим и доказывается равенство (21). □

Обозначим через $\Phi_P(d)$ число унитарных неприводимых над полем P многочленов степени d.

Утверждение 14. *Если $P = GF(q)$, то при $n \in \mathbb{N}$ справедливо равенство*

$$q^n = \sum_{d \mid n} d\Phi_P(d).$$

□ Пусть $f(x) \in P[x]$ — неприводимый над полем P многочлен степени n. По теореме 19 главы 21 существует расширение S поля P такое, что $S = P(\alpha)$, где $f(\alpha) = 0$. По теореме 7 поле S является минимальным полем разложения для $f(x)$ над P и содержит n его различных корней.

По утверждению 8 для любого неприводимого над P многочлена $g(x) \in P[x]$ степени d, где $d \mid n$, поле S является полем разложения. По теореме 7 оно содержит d различных корней многочлена $g(x)$.

Различные унитарные неприводимые над P многочлены не имеют общих корней в поле S, так как в противном случае они были бы не взаимно просты над P и совпадали. Значит, в поле S содержится, по крайней мере, $\sum_{d \mid n} d\Phi_P(d)$ различных элементов:

$$|S| = q^n \geqslant \sum_{d \mid n} d\Phi_P(d).$$

С другой стороны, каждый элемент поля S является корнем многочлена $F(x) = x^{q^n} - x$ и, следовательно, — корнем некоторого унитарного неприводимого над P многочлена $r(x) \in P[x]$. По утверждению 8 $\deg r(x) \mid n$. Отсюда $|S| \leqslant \sum_{d \mid n} d\Phi_P(d)$, и требуемое равенство доказано. □

Теорема 15. *Если $P = GF(q)$, то при $n \in \mathbb{N}$ справедливо равенство*

$$\Phi_P(n) = \frac{1}{n} \sum_{d \mid n} \mu(d) q^{n/d}. \tag{23}$$

□ Положим $F(n) = q^n$ и $f(d) = d\Phi_P(d)$. По утверждению 14 справедливо равенство $F(n) = \sum_{d \mid n} f(d)$. Тогда по утверждению 13

$$n\Phi_P(n) = \sum_{d \mid n} (p^t)^{n/d} \mu(d),$$

откуда и следует формула (23). □

§ 5. НЕКОТОРЫЕ МЕТОДЫ ПОСТРОЕНИЯ НЕПРИВОДИМЫХ МНОГОЧЛЕНОВ НАД КОНЕЧНЫМ ПОЛЕМ

Как уже отмечалось в § 3, один из способов построения неприводимого многочлена данной степени n над полем $P = GF(q)$, где $q = p^t$, состоит в случайном переборе многочленов вида

$$f(x) = x^n + f_{n-1}x^{n-1} + \ldots + f_0, \quad f_i \in P, \tag{24}$$

где $f_0 \neq 0$, и проверке их неприводимости на ЭВМ с помощью алгоритма, указанного в § 3. Теперь можно оценить эффективность этого способа.

Число многочленов вида (24) равно $(q-1)q^{n-1}$, а число неприводимых из них по формуле (23) есть

$$\Phi(n) = \frac{1}{n}\sum_{d|n}\mu(d)\,q^{\frac{n}{d}} = \frac{1}{n}\,(q^n - q^{\frac{n}{p_1}} - q^{\frac{n}{p_2}} - \ldots + q^{\frac{n}{p_1 p_2}} + \ldots),$$

где p_i — простые делители числа n. Значит, вероятность успеха, т. е. вероятность неприводимости случайно выбранного многочлена (24), равна

$$\frac{\Phi(n)}{(q-1)q^{n-1}}.$$

Последнее число при достаточно больших n приблизительно равно $\frac{q}{n(q-1)}$. Поэтому, проделав $\frac{n(q-1)}{q}$ испытаний, можно ожидать, что найдется хотя бы один неприводимый многочлен. Число операций, нужных при проверке на неприводимость одного многочлена, имеет порядок qn^3. Следовательно, для построения указанным способом одного неприводимого многочлена степени n требуется в среднем порядка $(q-1)n^4$ операций.

Изложим также один из алгебраических методов построения неприводимых многочленов большой степени из неприводимых многочленов относительно малой степени.

Обозначим $P = GF(q)$ и рассмотрим два отображения $\sigma\colon P[x] \to P[x]$ и $\tau\colon P[x] \to P[x]$, определенные формулами

$$\sigma\Big(\sum_{i=0}^{n} a_i x^i\Big) = \sum_{i=0}^{n} a_i x^{q^i-1}, \qquad \tau\Big(\sum_{i=0}^{n} a_i x^i\Big) = \sum_{i=0}^{n} a_i x^{q^i}. \tag{25}$$

Ясно, что

$$\tau(a(x)) = x\,\sigma(a(x)). \tag{26}$$

Пример 2. Если $P = GF(2)$ и $a(x) = e + x + x^2$, то

$$\sigma(a(x)) = e + x + x^3, \quad \tau(a(x)) = x + x^2 + x^4.$$

Утверждение 16. *Для любых $g(x), h(x) \in P[x]$ и любых $a, b \in P$, $i \in \mathbb{N}$ справедливы равенства*:

(а) $\sigma(ag(x) + bh(x)) = a\sigma(g(x)) + b\sigma(h(x))$;
(б) $\tau(ag(x) + bh(x)) = a\tau(g(x)) + b\tau(h(x))$;
(в) $\tau(x^i h(x)) = \tau(h(x))^{q^i}$.

□ Равенства (а) и (б) легко следуют из формул (25).

Докажем (в). Пусть $h(x) = \sum_{j=0}^{n} h_j x^j$. Так как $h_j^q = h_j$, то $h_j^{q^i} = h_j$, и справедливы равенства

$$\tau(x^i h(x)) = \tau\left(\sum_{j=0}^{n} h_j x^{j+i}\right) = \sum_{j=0}^{n} h_j x^{q^{j+i}} = \sum_{j=0}^{n} h_j^{q^i} (x^{q^j})^{q^i} =$$

$$= \left(\sum_{j=0}^{n} h_j x^{q^j}\right)^{q^i} = \tau(h(x))^{q^i}. \quad \square$$

Утверждение 17. *Если $g(x)$ и $h(x)$ — такие многочлены из $P[x]$, что $g(x) \mid h(x)$, то*

(а) $\tau(g(x)) \mid \tau(h(x))$;
(б) $\sigma(g(x)) \mid \sigma(h(x))$.

□ (а) Пусть $h(x) = g(x)\, v(x)$, где $v(x) = \sum_{i=0}^{n} v_i x^i$. Тогда в силу утверждения 16 справедливы равенства

$$\tau(h(x)) = \tau\left(\sum_{i=0}^{n} v_i x^i g(x)\right) = \sum_{i=0}^{n} v_i \tau(x^i g(x)) = \sum_{i=0}^{n} v_i \tau(g(x))^{q^i} =$$

$$= \tau(g(x)) \sum_{i=0}^{n} v_i \tau(g(x))^{q^i - 1},$$

показывающие выполнение соотношения (а).

(б) Из соотношения (а) и равенства (26) следует соотношение (б). □

Следствие. *Если многочлен $\sigma(h(x))$ неприводим над P, то и многочлен $h(x)$ неприводим над P.*

Утверждение 18. *Пусть многочлен $f(x) \in P[x]$ неприводим над P и $g(x) \in P[x]$ — такой многочлен, что*

$$(\sigma(f(x)),\, \sigma(g(x))) \neq e. \tag{27}$$

Тогда $f(x) \mid g(x)$.

□ Если $f(x) \nmid g(x)$, то $(f(x), g(x)) = e$ и существуют такие многочлены $u(x), v(x) \in P[x]$, что $u(x)f(x) + v(x)g(x) = e$. Тогда по утверждению 16(а) выполняется равенство

$$\sigma(u(x)f(x)) + \sigma(v(x)g(x)) = \sigma(e) = e. \tag{28}$$

Из соотношений $f(x) \mid u(x)f(x)$ и $g(x) \mid v(x)g(x)$ по утверждению 17(б) получаем соотношения

$$\sigma(f(x)) \mid \sigma(u(x)f(x)), \quad \sigma(g(x)) \mid \sigma(v(x)g(x)). \tag{29}$$

Из соотношений (28) и (29) для подходящих $u_1(x), v_1(x) \in P[x]$ следует равенство

$$\sigma(f(x))u_1(x) + \sigma(g(x))v_1(x) = e. \tag{30}$$

Полученное противоречие с условием (27) доказывает, что $f(x) \mid g(x)$. □

Определение 3. Пусть $f(x)$ — произвольный многочлен над полем P и $\{\alpha_1, \ldots, \alpha_s\}$ — множество всех его ненулевых корней в поле разложения над P. Через $O(f)$ обозначим НОК мультипликативных порядков элементов α_i:

$$O(f) = [\operatorname{Ord}\alpha_1, \ldots, \operatorname{Ord}\alpha_s].$$

Если $f(x) = x^l$, то положим $O(f) = 1$.

Читателю предлагается самостоятельно доказать, что параметр $O(f)$ не зависит от выбора поля разложения многочлена $f(x)$.

Пример 3. Если $f(x)$ — унитарный неприводимый над $GF(q)$ многочлен и $f(x) \neq x$, то по следствию 1 теоремы 7 $O(f) = \operatorname{Ord}\alpha$, где α — произвольный корень $f(x)$ в поле разложения над $GF(q)$. Ясно, что при этом $O(f) \mid q^n - 1$, где $n = \deg f(x)$.

Теорема 19 (Цирлер, 1967).[33] *Если унитарный многочлен $f(x) \in P[x]$ неприводим над $P = GF(q)$ и $f(x) \neq x$, то все неприводимые над P делители многочлена $\sigma(f(x))$ имеют степень $O(f)$.*

□ Пусть $O(f) = m$, $f_1(x)$ — неприводимый над P делитель многочлена $\sigma(f(x))$ и $\deg f_1(x) = k$.

По определению 3 все корни многочлена $f(x)$ являются корнями многочлена $x^m - e \in P[x]$. Поскольку $f(x)$ не имеет кратных корней, то $f(x) \mid x^m - e$. По утверждению 17(б) $\sigma(f(x)) \mid \sigma(x^m - e)$. Так как $\sigma(x^m - e) = x^{q^m - 1} - e$, то $f_1(x) \mid x^{q^m-1} - e$ и $f_1(x) \mid x^{q^m} - x$.

По теореме 1 поле $GF(q^m)$ является полем разложения многочлена $x^{q^m} - x$, а тогда — полем разложения и многочлена $f_1(x)$. Значит, поле $GF(q^m)$ содержит минимальное поле разложения многочлена $f_1(x)$ — поле $GF(q^k)$. Отсюда по теореме 4 следует, что $k \mid m$.

По условию $f(x) \neq x$, и поэтому $(f(x), x) = e$. Тогда $(\sigma(f(x)), x) = e$ и из соотношений $f_1(x) \mid x^{q^k} - x$ и $f_1(x) \mid \sigma(f(x))$ следует, что $f_1(x) \mid x^{q^k-1} - e$. Поскольку $x^{q^k-1} - e = \sigma(x^k - e)$, то $(\sigma(f(x)), \sigma(x^k - e)) \neq e$ и по утверждению 18 $f(x) \mid x^k - e$. Таким образом, если $f(\alpha) = 0$, то $\alpha^k = e$ и $O(f) \mid k$, или $m \mid k$. Итак, $k = m$. □

Определение 4. Неприводимый над полем $P = GF(q)$ унитарный многочлен $f(x) \in P[x] \setminus \{x\}$ степени n со свойством $O(f) = q^n - 1$ называется *примитивным*.

[33] Н. Цирлер — современный американский математик.

Следствие (Орэ).[34]

Если многочлен $f(x) \in P[x]$ неприводим над $P = GF(q)$, $\deg f(x) = n$ и $f(x) \neq x$, то многочлен $\sigma(f(x))$ неприводим над P тогда и только тогда, когда $f(x)$ — примитивный многочлен.

□ Если многочлен $\sigma(f(x))$ неприводим над P, то по следствию утверждения 17 многочлен $f(x)$ неприводим над P. Тогда по теореме 19 $\deg \sigma(f(x)) = O(f) = q^n - 1$.

Обратно, пусть $O(f) = q^n - 1$. По теореме 19 степень каждого неприводимого над P делителя многочлена $\sigma(f(x))$ равна $q^n - 1$. Поскольку $\deg \sigma(f(x)) = q^n - 1$, то $\sigma(f(x))$ — неприводимый над P многочлен. □

Пример 4. Существуют простые числа вида $2^n - 1$, например: $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$, $2^7 - 1 = 127$ (их называют *числами Мерсенна*). Если $f(x) \in GF(2)[x]$ — унитарный многочлен, неприводимый над $GF(2)$, $\deg f(x) = n > 1$, и $2^n - 1$ — простое число, то из $O(f) \mid 2^n - 1$ следует $O(f) = 2^n - 1$. Тогда по следствию теоремы 19 многочлен $\sigma(f(x))$ неприводим над $GF(2)$. Воспользуемся этим и последовательно построим неприводимые над $GF(2)$ многочлены:

$$\begin{aligned} f(x) &= x^2 + x + e, \\ \sigma(f(x)) &= x^3 + x + e, \\ \sigma^2(f(x)) &= \sigma(\sigma(f(x))) = x^7 + x + e, \\ \sigma^3(f(x)) &= x^{127} + x + e. \end{aligned}$$

§ 6. ХАРАКТЕРЫ КОНЕЧНЫХ ПОЛЕЙ И СУММЫ ГАУССА

Напомним, что характеры конечных абелевых групп рассматривались в § 4 главы 12.

Определение 5. Пусть $P = GF(q)$ — конечное поле из q элементов. Характеры его мультипликативной группы P^* и аддитивной группы $(P, +)$ называются соответственно *мультипликативными* и *аддитивными характерами* поля P.

Соответствующие группы характеров поля P обозначим через $\widehat{P^*}$ и $\widehat{P}$. Условимся обозначать мультипликативные и аддитивные характеры поля P соответственно буквами χ и ψ с индексами.

Так как группа P^* — циклическая порядка $q - 1$, то в силу теоремы 10 главы 12 $\widehat{P^*}$ — также циклическая группа порядка $q - 1$. Поэтому порядки мультипликативных характеров поля P суть делители числа $q - 1$, и для каждого делителя d числа $q - 1$ существует $\varphi(d)$ характеров порядка d. Группа $(P, +)$ является элементарной абелевой p-группой, где p — простое число и $q = p^m$, и значит все нетривиальные аддитивные характеры поля P имеют порядок p.

Установим связи между мультипликативными и аддитивными характерами поля P. Для этого нам понадобятся тригонометрические суммы Гаусса.

[34] О. Орэ (1899–1968) — норвежский математик.

Определение 6. *Суммой Гаусса* для мультипликативного характера χ и аддитивного характера ψ поля P называется комплексное число

$$G(\chi,\psi)=\sum_{x\in P^*}\chi(x)\cdot\psi(x).$$

Аддитивные характеры поля P можно занумеровать элементами из P. Если $q=p^m$, то имеет место изоморфизм

$$\delta\colon (P,+)\to(\mathbb{Z}_p)^m,$$

и каждому элементу $a\in(P,+)$ однозначно ставится в соответствие вектор $\delta(a)=(a_1,a_2,\ldots,a_m)$, где $a_i\in\overline{0,p-1}$. Выберем в $\mathbb{C}^*$ первообразный корень степени p из единицы $\omega=e^{2\pi i/p}$. Обозначим через ψ_a характер, определенный равенством

$$\psi_a(x)=\omega^{a_1x_1+\ldots+a_mx_m},$$

где $(x_1,\ldots,x_m)=\delta(x)$. В частности, для простого поля $P=GF(p)$ имеем $\psi_a(x)=\omega^{ax}$. В этом случае сумма Гаусса $G(\chi,\psi)$ обозначается также символом $G(\chi,a)$ и определяется равенством

$$G(\chi,a)=\sum_{x\in P^*}\chi(x)\cdot\omega^{ax}.$$

Кроме того, в этом случае $G(\chi,e)$ обозначают через $G(\chi)$.

Теперь можно сформулировать теорему о соотношениях между характерами из $\widehat{P^*}$ и $\widehat{P}$.

Теорема 20. *Пусть χ и ψ — соответственно мультипликативный и аддитивный характеры поля $P=GF(q)$. Тогда для любого $a\in P^*$ выполняются соотношения*

$$\chi(a)=\frac{1}{q}\sum_{b\in P}G(\chi,\overline{\psi}_b)\cdot\psi_b(a), \tag{31}$$

$$\psi(a)=\frac{1}{q-1}\sum_{b\in P^*}G(\overline{\chi}_b,\psi)\cdot\chi_b(a). \tag{32}$$

□ Формулы (31), (32) доказываются непосредственным вычислением их правых частей с использованием определения 6 и второго соотношения ортогональности (теорема 12 главы 12) для аддитивных и мультипликативных характеров поля P. □

В связи с теоремой 20, а также в связи с другими приложениями сумм Гаусса, представляет интерес задача вычисления их значений. Частичное решение этой задачи содержит следующая теорема о свойствах сумм Гаусса.

Теорема 21. *Для любых $\chi\in\widehat{P^*}$ и $\psi\in\widehat{P}$ выполняются соотношения*:

(a) $G(\chi,\psi)=\begin{cases}q-1, & \text{если } \chi=\chi_e,\ \psi=\psi_0,\\ -1, & \text{если } \chi=\chi_e,\ \psi\neq\psi_0,\\ 0, & \text{если } \chi\neq\chi_e,\ \psi=\psi_0;\end{cases}$

если $\chi \neq \chi_e$, $\psi \neq \psi_0$, *то*

(б) $G(\chi,\psi)\cdot\overline{G(\chi,\psi)} = q$;

(в) $|G(\chi,\psi)| = \sqrt{q}$.

□ Равенства утверждения (а) следуют непосредственно из определений и следствия теоремы 12 главы 12. Равенство (в) следует из (б). Проверим равенство (б):

$$G(\chi,\psi)\cdot\overline{G(\chi,\psi)} = \left(\sum_{a\in P^*}\chi(a)\,\psi(a)\right)\cdot\left(\sum_{b\in P^*}\overline{\chi}(b)\,\overline{\psi}(b)\right) =$$

$$= \sum_{a,b\in P^*}\chi(a)\,\overline{\chi}(b)\cdot\psi(a)\,\overline{\psi}(b) = \sum_{a,b\in P^*}\chi(ab^{-1})\cdot\psi(a-b).$$

Сгруппируем слагаемые по параметру $d = ab^{-1}$. Получим (прибавляя и вычитая $\psi(0)$):

$$G(\chi,\psi)\cdot\overline{G(\chi,\psi)} = \sum_{d\in P^*}\chi(d)\cdot\left(\sum_{b\in P}\psi(b(d-e)) - \psi(0)\right).$$

Заметим, что при $d \neq e$ элемент $b(d-e)$ пробегает вместе с b все поле P, и в этом случае согласно следствию теоремы 12 главы 12

$$\sum_{b\in P}\psi(b(d-e)) = 0.$$

Если же $d = e$, то $\sum_{b\in P}\psi(b(d-e)) = q$. Отсюда

$$G(\chi,\psi)\cdot\overline{G(\chi,\psi)} = \sum_{d\in P^*\setminus\{e\}}\chi(d)\cdot(-1) + (q-1).$$

Учитывая следствие теоремы 12 главы 12 для характера χ, получаем требуемое равенство (б). □

ЗАДАЧИ

1. Опишите структуру подполей поля $GF(2^{36})$.

2. Найдите все примитивные элементы полей $GF(5)$, $GF(2^2)$, $GF(7)$, $GF(11)$.

3. Сколько существует примитивных элементов в поле $GF(p^t)$?

4. Докажите, что мультипликативная группа P^* бесконечного поля P не является циклической.

5. Пользуясь критерием Батлера, определите, приводимы или нет над полем $GF(2)$ многочлены x^2+e и x^3+x+e.

6. Пользуясь критерием Батлера, определите, приводим или нет над полем $GF(3)$ многочлен x^3+x^2+e.

7. Покажите, что если $n_1, n_2 \in \mathbb{N}$ и $(n_1,n_2)=1$, то $\mu(n_1n_2) = \mu(n_1)\mu(n_2)$.

8. Покажите, что для $n \in \mathbb{N}$ справедливо равенство $n = \sum_{d|n} \varphi(d)$, где φ — функция Эйлера.

9. Покажите, что для $n \in \mathbb{N}$ справедливо равенство

$$\varphi(n) = \sum_{d|n} \frac{n}{d}\, \mu(d).$$

10. Постройте поля из 8, 9, 25, 49 элементов и найдите их примитивные элементы.

11. Найдите выражение $\Phi_P(n)$ при простом n, $P = GF(q)$, $q = p^t$.

12. Найдите $O(f)$, где $f(x) = x^3 + 2x + 2 \in GF(3)[x]$.

13. Покажите, что число унитарных многочленов $f(x) \in GF(q)[x]$ степени n таких, что $O(f) = q^n - 1$ (примитивных многочленов) равно $\dfrac{1}{n}\,\varphi(q^n - 1)$.

14. Постройте неприводимый над $GF(2)$ многочлен степени 31.

15. Докажите, что если $f(x) = \sum_{i=0}^{n} f_i x^i$ — примитивный многочлен степени n над полем $P = GF(q)$ (т. е. $O(f) = q^n - 1$), то многочлен

$$\sum_{i=0}^{n} f_i x^{\frac{q^i - 1}{q-1}}$$

неприводим над P.

16. Постройте неприводимые многочлены степени m над полем $GF(q)$ в следующих ситуациях:

q	3		4		5		
m	4	8	5	15	6	12	24

17. Проверьте, приводим или нет над полем $GF(3)$ многочлен $x^4 + x^3 + x + 2$. В случае приводимости разложите его на неприводимые множители.

18. Для многочленов f_1, f_2 постройте в явном виде изоморфизм полей $P_1 = \mathbb{Z}_2[x]/f_1(x)$ и $P_2 = \mathbb{Z}_2[x]/f_2(x)$, где $f_1(x) = x^3 + x + 1$, $f_2(x) = x^3 + x^2 + 1$.

19. Пусть $P = GF(q)$ — поле с примитивным элементом a и число $m \in \{2, 3\}$ делит $q - 1$. Докажите, что многочлен $x^m - a$ неприводим над P.

20. Пусть $P = GF(q)$, $f(x) \in P[x]$ — неприводимый многочлен степени n и T — расширение поля P степени m. Пусть Q — расширение поля T такое, что $Q = T(\alpha)$, где $f(\alpha) = 0$. Докажите, что

(а) Q — минимальное поле разложения $f(x)$ над T и $[Q : P] = [m, n]$.

(б) Многочлен $f(x)$ неприводим над T тогда и только тогда, когда $(m, n) = 1$.

(в) Если $d = (m, n)$, то многочлен $f(x)$ есть произведение d неприводимых над T многочленов степеней $k = n/d$.

Глава 23

ЗАДАНИЕ ГРУПП ОБРАЗУЮЩИМИ ЭЛЕМЕНТАМИ И ОПРЕДЕЛЯЮЩИМИ СООТНОШЕНИЯМИ

Один из широко распространенных методов задания различных алгебр основан на использовании их систем образующих элементов и некоторых соотношений между образующими элементами. В данной главе мы познакомимся с этим методом в применении к группам.

Любую конечную группу, как и всякий конечный группоид, можно задать таблицей Кэли, т. е. списками всех его элементов $g_1, \ldots, g_n$ и всех соотношений вида $g_i g_j = g_{k(i,j)}$, $i, j \in \overline{1,n}$. В принципе то же самое можно сказать и о задании бесконечной группы, только в этом случае все элементы группы и всю ее таблицу Кэли нельзя выписать в явном виде. Практически всю таблицу Кэли невозможно выписать и для конечной группы, если ее порядок достаточно велик. В связи с этим естественно возникает вопрос: нельзя ли задать группу, указав лишь некоторую (по возможности небольшую) часть ее элементов и некоторую систему соотношений между этими элементами?

Прежде чем рассматривать этот вопрос в общем виде, разберем два простых примера.

Пример 1. Пусть C_m — циклическая группа порядка m и g — любой из порождающих ее элементов. Тогда в C_m выполняется соотношение $g^m = e$, и все ее элементы исчерпываются степенями $g^0, \ldots, g^{m-1}$ элемента g. В этом смысле группа C_m вполне определяется одним элементом g и одним соотношением $g^m = e$.

Пример 2. Рассмотрим группу движений правильного n-угольника, или *группу диэдра* степени n (см. § 7 главы 11). Ее подстановочное представление D_n является подгруппой симметрической группы S_n и порождается двумя подстановками:

$$g_1 = \begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ 2 & 3 & \ldots & n & 1 \end{pmatrix}, \quad g_2 = \begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ n & n-1 & \ldots & 2 & 1 \end{pmatrix}.$$

Легко видеть, что в группе D_n выполняются соотношения

$$g_1^n = e, \quad g_2^2 = e, \quad g_2 g_1 = g_1^{-1} g_2, \quad g_2 g_1^{-1} = g_1 g_2. \tag{1}$$

Пользуясь этими соотношениями, любое произведение элементов g_1, g_1^{-1}, g_2, g_2^{-1} можно преобразовать к виду

$$g_1^k g_2^l, \quad k \in \overline{0, n-1}, \quad l \in \overline{0,1}. \tag{2}$$

Докажите это индукцией по числу сомножителей в исходном произведении. А так как по следствию 2 теоремы 25 главы 11 порядок D_n равен $2n$, то все произведения вида (2) попарно различны. Следовательно, каждый элемент группы D_n однозначно представляется в виде (2). Пользуясь соотношениями (1), легко найти и правило умножения элементов из D_n, записанных в виде (2):

$$g_1^k g_2^l \cdot g_1^s g_2^t = \begin{cases} g_1^{r_n(k+s)} g_2^t, & \text{если } l = 0, \\ g_1^{r_n(k-s)} g_2^{t+1}, & \text{если } l = 1, \end{cases} \tag{3}$$

где $r_n(x)$ — остаток от деления x на n. Таким образом, группа D_n полностью определяется системой образующих элементов $\{g_1, g_2\}$ и системой соотношений (1). В связи с этим систему (1) называют *системой определяющих соотношений* группы D_n в системе образующих $\{g_1, g_2\}$.

В общем случае понятие системы определяющих соотношений группы в заданной системе образующих будет определено ниже. Здесь же отметим еще, что в принципе группу D_n можно отождествить с группой G_n всех выражений вида (2), перемножаемых по правилу (3). Такое представление группы D_n группой G_n иногда бывает полезным в силу того, что при больших n правило (3) значительно проще правила умножения элементов из D_n как движений правильного n-угольника, или как подстановок степени n. В качестве примера воспользуйтесь этим для решения уравнения $xg_1g_2x = g_2g_1$ в группе D_n.

§ 1. ОБЩАЯ КОНСТРУКЦИЯ ГРУППЫ, ЗАДАННОЙ ОБРАЗУЮЩИМИ ЭЛЕМЕНТАМИ И ОПРЕДЕЛЯЮЩИМИ СООТНОШЕНИЯМИ

Зафиксируем множество букв с индексами $A = \{a_i : i \in I\}$. Каждой букве a_i сопоставим символ a_i^{-1} и образуем множество

$$\overline{A} = \{a_i^{\varepsilon} : i \in I, \ \varepsilon \in \{1, -1\}\},$$

где $a_i^1 = a_i$, которое назовем *алфавитом*.

Определение 1. Любую последовательность вида

$$a_{i_1}^{\varepsilon_1} \dots a_{i_k}^{\varepsilon_k}, \tag{4}$$

составленную из элементов множества $\overline{A}$, назовем *словом длины k в алфавите $\overline{A}$*. В целях общности последовательность, не содержащую ни одного члена, будем называть *словом длины нуль*, или *пустым словом*.

Условимся обозначать слова буквами P, Q, R, L без индексов и с индексами, пустое слово — буквой e, длину слова P — через $l(P)$, равенство слов P, Q — в виде $P = Q$, множество всех слов в алфавите $\overline{A}$ — через $W(\overline{A})$.

Определение 2. *Произведением слов P, Q* назовем слово, обозначаемое через PQ и получающееся путем приписывания к слову P справа слова Q.

Легко видеть, что множество $W(\overline{A})$ с операцией произведения слов является полугруппой с нейтральным (единичным) элементом e. Ее называют *полугруппой слов* в алфавите $\overline{A}$.

Определение 3. *Обратным к слову* (4) назовем слово $a_{i_k}^{-\varepsilon_k} \dots a_{i_1}^{-\varepsilon_1}$. Обратным к пустому слову назовем само это слово. Слово, обратное к P, обозначим через P^{-1}.

Заметим, что при $P \neq e$ слово P^{-1} не является обратным элементом к P в полугруппе $(W(\overline{A}); \cdot)$.

Определение 4. Говорят, что слово P *входит в слово* Q, или является *подсловом* слова Q, если $Q \equiv LPR$ при некоторых (возможно пустых) словах L, R.

Если слово P входит в Q много раз, то говорят о нескольких *вхождениях* слова P в Q. В частности, считается, что пустое слово e имеет $k+1$ вхождений в слово (4):

$$a_{i_1}^{\varepsilon_1} \dots a_{i_k}^{\varepsilon_k} \equiv e a_{i_1}^{\varepsilon_1} e \dots e a_{i_k}^{\varepsilon_k} e.$$

Слово вида $\underbrace{P^{\varepsilon} \dots P^{\varepsilon}}_{k}$, где $\varepsilon \in \{1, -1\}$, будем обозначать ради краткости через P^k при $\varepsilon = 1$ и через P^{-k} при $\varepsilon = -1$.

Определение 5. Любую пару (P, Q) слов P, Q из $W(\overline{A})$ назовем *соотношением в алфавите* $\overline{A}$. При этом P и Q будем называть соответственно *левой и правой частями соотношения* (P, Q). Соотношения вида $(a_i^{\varepsilon} a_i^{-\varepsilon}, e)$ и $(e, a_i^{\varepsilon} a_i^{-\varepsilon})$, где $\varepsilon \in \{1, -1\}$, будем называть *тривиальными*.

Зафиксируем произвольное (возможно пустое) множество S соотношений в алфавите $\overline{A}$ и определим по нему отношение эквивалентности на множестве $W(\overline{A})$.

Определение 6. *Элементарным преобразованием слова* P по соотношению (P_1, Q_1) назовем замену в P любого одного вхождения слова P_1 или Q_1 соответственно словом Q_1 или P_1. Если $P, Q \in W(\overline{A})$ и Q получено из P одним элементарным преобразованием по соотношению (P_1, Q_1), то будем писать $P \underset{(P_1, Q_1)}{\longrightarrow} Q$. В этом случае будем писать также $P \underset{S}{\to} Q$, если S — некоторая система соотношений и $(P_1, Q_1) \in S$ или (P_1, Q_1) — тривиальное соотношение.

Из определения видно, что если $P \underset{S}{\to} Q$, то и $Q \underset{S}{\to} P$. Следовательно, корректно

Определение 7. Слова $P, Q \in W(\overline{A})$ называют *S-эквивалентными* (и пишут $P \underset{S}{\sim} Q$), а соотношение (P, Q) — *следствием системы* S, если

$$\exists\, k \in \mathbb{N}_0,\ \exists\, R_0, R_1, \dots, R_k \in W(\overline{A}):\ P \equiv R_0 \underset{S}{\to} R_1 \underset{S}{\to} \dots \underset{S}{\to} R_k \equiv Q.$$

Пример 3. Для любого слова $P \in W(\overline{A})$ и любой системы соотношений S имеем:

$$PP^{-1} \underset{S}{\sim} e, \quad P^{-1}P \underset{S}{\sim} e. \tag{5}$$

Пусть P есть слово (4). Тогда $PP^{-1} \equiv a_{i_1}^{\varepsilon_1} \dots a_{i_k}^{\varepsilon_k} a_{i_k}^{-\varepsilon_k} \dots a_{i_1}^{-\varepsilon_1}$, и, производя последовательно замены подслов $a_{i_k}^{\varepsilon_k} a_{i_k}^{-\varepsilon_k}$, $\dots$, $a_{i_1}^{\varepsilon_1} a_{i_1}^{-\varepsilon_1}$ пустым словом e, мы получим в итоге e. А так как при этом производились элементарные преобразования по тривиальным соотношениям вида $(a_i^{\varepsilon} a_i^{-\varepsilon}, e)$, то согласно определению 7 имеем $PP^{-1} \underset{S}{\sim} e$ при любой системе S (и даже при $S = \varnothing$). Аналогично доказывается, что $P^{-1}P \underset{S}{\sim} e$.

Теорема 1. *Отношение $\underset{S}{\sim}$ является конгруэнцией на полугруппе $(W(\overline{A}); \cdot)$, а соответствующая факторполугруппа является группой.*

□ Непосредственно из определения 7 видно, что отношение $\underset{S}{\sim}$ рефлексивно, симметрично, транзитивно и обладает свойством

$$\forall\, P, Q, L, R \in W(\overline{A}):\ (P \underset{S}{\sim} Q,\ L \underset{S}{\sim} R)\ \Rightarrow\ (PL \underset{S}{\sim} QR).$$

Значит, $\underset{S}{\sim}$ — конгруэнция на полугруппе слов $(W(\overline{A}); \cdot)$. Обозначим класс S-эквивалентных слов, содержащий слово P, через $[P]_S$, а множество всех классов через $W(\overline{A})/S$. Из следствия утверждения 6 главы 10 получаем: множество $W(\overline{A})/S$ с операцией, определенной формулой

$$\forall\, [P]_S, [Q]_S \in W(\overline{A})/S:\ [P]_S \cdot [Q]_S = [PQ]_S,$$

есть полугруппа. Легко видеть, что ее нейтральным элементом является класс $[e]_S$, и, как следует из (5), обратным к классу $[P]_S$ является класс $[P^{-1}]_S$. Следовательно, $W(\overline{A})/S$ — группа. □

Определение 8. Группу $(W(\overline{A})/S; \cdot)$ из теоремы 1 называют *абстрактной группой*, заданной системой образующих A и системой определяющих соотношений S, и обозначают в виде $\langle A;\, S \rangle$.

Заметим, что здесь термин «система образующих группы» использован в несколько ином смысле, чем в главе 11, поскольку элементы a_i из A не являются даже элементами группы $\langle A;\, S \rangle$. В действительности эта группа порождается системой ее элементов $[a_i]_S$, $i \in I$, а использование указанного термина оправдывается лишь тем, что иногда, допуская вольность речи, элементами группы $\langle A;\, S \rangle$ называют не только классы слов, но и сами слова.

Из определений 7 и 8 следует

Утверждение 2. *Пусть S_1, S_2 — системы соотношений в алфавите $\overline{A}$. Все соотношения системы S_2 являются следствиями системы S_1 в том и только в том случае, когда $\langle A;\, S_1 \rangle = \langle A;\, S_1 \cup S_2 \rangle$.*

□ Если все соотношения из S_2 являются следствиями системы S_1, то легко видеть, что для любых слов P, $Q \in W(\overline{A})$ верна импликация

$$P \underset{S_1 \cup S_2}{\sim} Q \;\Rightarrow\; P \underset{S_1}{\sim} Q.$$

Следовательно, $[P]_{S_1 \cup S_2} = [P]_{S_1}$, и потому $\langle A;\, S_1 \cup S_2\rangle = \langle A;\, S_1\rangle$.

Обратно, пусть выполнено последнее равенство и $(P, Q) \in S_2$. Тогда верно $P \in [Q]_{S_2} \subset [Q]_{S_1 \cup S_2} = [Q]_{S_1}$, т. е. (P, Q) есть следствие системы S_1. □

Определение 9. Две системы соотношений S_1, S_2 называют *эквивалентными* и пишут $S_1 \approx S_2$, если каждое соотношение любой одной из них является следствием другой системы. Если системы S_1, S_2 содержат по одному соотношению, то вместо эквивалентности систем говорят об *эквивалентности соотношений*, сохраняя то же обозначение $\approx$.

Утверждение 3. *Отношение $\approx$ на множестве M всех систем соотношений в алфавите $\overline{A}$ является отношением эквивалентности, причем*

$$\forall\, S_1, S_2 \in M:\;\; S_1 \approx S_2 \;\Leftrightarrow\; \langle A;\, S_1\rangle = \langle A;\, S_2\rangle. \tag{6}$$

□ Утверждение (6) является следствием утверждения 2, а тот факт, что $\approx$ есть отношение эквивалентности, легко доказывается с использованием утверждения (6). □

Утверждение 4. *Для любых слов L, P, Q, $R \in W(\overline{A})$ и любых ε, $\delta \in \{1, -1\}$ имеют место эквивалентности*:

(а) $(P, Q) \approx (Q, P)$;
(б) $(P, Q) \approx (L^{\varepsilon} L^{-\varepsilon} P R^{\delta} R^{-\delta},\, Q)$;
(в) $(P, Q) \approx (LPR,\, LQR)$;
(г) $(P, Q) \approx (PQ^{-1},\, e)$;
(д) $(P, Q) \approx (P^{-1},\, Q^{-1})$;
(е) $(PQ,\, QP) \approx (P^{\varepsilon} Q^{\delta},\, Q^{\delta} P^{\varepsilon})$.

□ Эквивалентность (а) очевидна, (б) следует из (5) при $S = \varnothing$, (в) доказывается соотношениями

$$LPR \underset{(P,Q)}{\longrightarrow} LQR, \quad P \underset{\varnothing}{\sim} L^{-1}LPRR^{-1} \underset{(LPR,\, LQR)}{\longrightarrow} L^{-1}LQRR^{-1} \underset{\varnothing}{\sim} Q.$$

Пользуясь соотношениями (а), (б), (в), доказываем свойства (г), (д):

$$(P, Q) \approx (PQ^{-1},\, QQ^{-1}) \approx (PQ^{-1},\, e);$$
$$(P, Q) \approx (P^{-1}PQ^{-1},\, P^{-1}QQ^{-1}) \approx (Q^{-1},\, P^{-1}) \approx (P^{-1},\, Q^{-1});$$

и свойство (е):

$$(PQ,\, QP) \approx ((PQ)^{-1},\, (QP)^{-1}) \approx (Q^{-1}P^{-1},\, P^{-1}Q^{-1}) \approx (P^{-1}Q^{-1},\, Q^{-1}P^{-1});$$
$$(PQ,\, QP) \approx (P^{-1}PQP^{-1},\, P^{-1}QPP^{-1}) \approx (QP^{-1},\, P^{-1}Q) \approx (P^{-1}Q,\, QP^{-1});$$
$$(PQ,\, QP) \approx (Q^{-1}PQQ^{-1},\, Q^{-1}QPQ^{-1}) \approx (Q^{-1}P,\, PQ^{-1}) \approx (PQ^{-1},\, Q^{-1}P). \quad \square$$

Определение 10. Любое соотношение вида (P, e) назовем *приведенным*.

Из утверждения 4(г) получаем

Следствие. *Для любой системы соотношений S в алфавите $\overline{A}$ существует эквивалентная ей система приведенных соотношений в алфавите $\overline{A}$.*

Приведем одно утверждение о взаимосвязи между группами $\langle A;\, S_1\rangle$ и $\langle A;\, S_2\rangle$, доказанное в 1883 г. американским математиком У. Диком.

Теорема 5. *Если $G_1 = \langle A;\, S_1\rangle$, $G_2 = \langle A;\, S_2\rangle$ и $S_1 \subset S_2$, то отображение $\varphi\colon G_1 \to G_2$, определенное формулой*

$$\forall\, [P]_{S_1} \in G_1 :\ \varphi([P]_{S_1}) = [P]_{S_2}, \tag{7}$$

является эпиморфизмом. Если при этом S_2 состоит из приведенных соотношений $(P_j,\, e)$, $j \in J$, то ядро эпиморфизма φ совпадает с пересечением H всех нормальных делителей группы G_1, содержащих множество $\{[P_j]_{S_1} : j \in J\}$.

□ Определение отображения φ корректно, поскольку из включения $S_1 \subset S_2$ очевидным образом следует импликация

$$([P]_{S_1} = [Q]_{S_1}) \ \Rightarrow\ ([P]_{S_2} = [Q]_{S_2}).$$

Сюръективность отображения φ очевидна, а тот факт, что φ — гомоморфизм, проверяется непосредственно:

$$\varphi([P]_{S_1} \cdot [Q]_{S_1}) = \varphi([PQ]_{S_1}) = [PQ]_{S_2} = [P]_{S_2} \cdot [Q]_{S_2} = \varphi([P]_{S_1})\,\varphi([Q]_{S_1}).$$

Пусть теперь $S_2 = \{(P_j,\, e) :\ j \in J\}$. Докажем, что $\operatorname{Ker}\varphi = H$. Так как $\operatorname{Ker}\varphi \lhd G_1$ и $[R]_{S_1} \in \operatorname{Ker}\varphi \Leftrightarrow R \underset{S_2}{\sim} e$, то $\operatorname{Ker}\varphi \ni [P_j]_{S_1}$, и потому $\operatorname{Ker}\varphi \supset H$. Докажем обратное включение. Для этого достаточно показать, что если $R \equiv R_0 \underset{S_2}{\to} R_1 \underset{S_2}{\to} \ldots \underset{S_2}{\to} R_k \equiv e$, то $[R]_{S_1} \in H$. Докажем этот факт индукцией по k. Если $k = 0$, то $R_0 \equiv e$, и утверждение очевидно. Допустим, что оно верно при $k = n$, и пусть $k = n + 1$. По предположению индукции $[R_1]_{S_1} \in H$, и остается рассмотреть переход $R_0 \underset{S_2}{\to} R_1$. Согласно условию он осуществлен по соотношению вида $(P,\, e)$, где $P \equiv P_j$ или $P \equiv a_i^{\varepsilon}\, a_i^{-\varepsilon}$, $j \in J$, $i \in I$, $\varepsilon \in \{1, -1\}$. Возможны два случая:

1. $R_0 \equiv R'PR''$, $R_1 \equiv R'R''$,
2. $R_0 \equiv R'R''$, $R_1 \equiv R'PR''$.

В случае 1 $R'PR'' \underset{S_1}{\sim} R'PR'^{-1}R'R''$, причем $[R'PR'^{-1}]_{S_1} \in H$, так как $[P]_{S_1} \in H$ и $H \lhd \langle A;\, S_1\rangle$. Отсюда $[R_0]_{S_1} = [R'PR'^{-1}]_{S_1} \cdot [R_1]_{S_1} \in H$. Аналогично, в случае 2 получим

$$[R_0]_{S_1} = [R'PR'^{-1}]_{S_1}^{-1} \cdot [R_1]_{S_1} \in H. \quad \square$$

Рассмотрим прямое произведение двух групп, заданных системами образующих элементов и определяющих соотношений.

Теорема 6. *Если* $G_1 = \langle A;\, S_1\rangle$, $G_2 = \langle B;\, S_2\rangle$, $A = \{a_i :\, i \in I\}$, $B = \{b_j :\, j \in J\}$ *и* $\overline{A} \cap \overline{B} = \varnothing$, *то*

$$G_1 \otimes G_2 \cong \langle A \cup B;\, S_1 \cup S_2 \cup K\rangle,$$

где $K = \{(a_i b_j,\, b_j a_i) :\, i \in I,\, j \in J\}$.

$\square$ Докажем, что искомым изоморфизмом является отображение

$$\varphi\colon G_1 \otimes G_2 \to \langle A \cup B;\ S_1 \cup S_2 \cup K\rangle,$$

определенное формулой

$$\forall\, ([P]_{S_1},\, [Q]_{S_2}) \in G_1 \otimes G_2 :\ \varphi(([P]_{S_1},\, [Q]_{S_2})) = [PQ]_{S_1 \cup S_2 \cup K}.$$

Очевидно, отображение φ определено корректно. По утверждению 4(e) система $S_1 \cup S_2 \cup K$ эквивалентна системе $U = S_1 \cup S_2 \cup K'$, где

$$K' = \left\{(a_i^{\varepsilon} b_j^{\delta},\, b_j^{\delta} a_i^{\varepsilon}) :\, i \in I,\ j \in J,\ \varepsilon, \delta \in \{1, -1\}\right\}.$$

Пусть теперь R — любое слово из $W(\overline{A \cup B})$. Обозначим через R_A, R_B слова, полученные из R удалением соответственно всех символов из $\overline{B}$, $\overline{A}$. Очевидно, что $R_A \in W(\overline{A})$, $R_B \in W(\overline{B})$ и $R \underset{K}{\sim} R_A R_B$. Отсюда следует, что $\varphi(([R_A]_{S_1},\, [R_B]_{S_2})) = [R]_U$, т. е. φ сюръективно. Для доказательства инъективности достаточно доказать утверждение

$$\forall\, R, L \in W(\overline{A \cup B}) :\ (R \underset{U}{\to} L) \ \Rightarrow\ (R_A \underset{S_1}{\sim} L_A,\ R_B \underset{S_2}{\sim} L_B).$$

Пусть элементарное преобразование $R \underset{U}{\to} L$ заключалось в замене подслова P из R словом Q, т. е. $R \equiv R'PR''$, $L \equiv R'QR''$.

Возможны три случая:

1. $(P, Q) \in K'$. Тогда $R_A \equiv L_A$, $R_B \equiv L_B$, и утверждение верно.

2. $P,\, Q \in W(\overline{A})$. Тогда $R_A \equiv R'_A P R''_A$, $R_B \equiv R'_B R''_B$, $L_A \equiv L'_A Q L''_A$, $L_B \equiv R'_B R''_B$. Отсюда видно, что $R_A \underset{S_1}{\sim} L_A$, $R_B \equiv L_B$, и утверждение снова верно.

3. $P,\, Q \in W(\overline{B})$. Этот случай симметричен случаю 2.

Таким образом, отображение φ инъективно, и остается проверить, что φ — гомоморфизм. Проделайте эту проверку самостоятельно. $\square$

§ 2. ЗАДАНИЕ ПРОИЗВОЛЬНОЙ ГРУППЫ СИСТЕМАМИ ОБРАЗУЮЩИХ ЭЛЕМЕНТОВ И ОПРЕДЕЛЯЮЩИХ СООТНОШЕНИЙ

Пусть G — любая группа и $G_1 = \{g_i : i \in I\} \subset G$.

Определение 11. Всякое верное в группе G равенство вида

$$g_{i_1}^{\varepsilon_1} \dots g_{i_k}^{\varepsilon_k} = g_{j_1}^{\delta_1} \dots g_{j_l}^{\delta_l} \tag{8}$$

или

$$g_{i_1}^{\varepsilon_1} \dots g_{i_k}^{\varepsilon_k} = e_G, \tag{9}$$

где $i_1, \dots, i_k, j_1, \dots, j_l \in I$, $\varepsilon_1, \dots, \varepsilon_k, \delta_1, \dots, \delta_l \in \{1, -1\}$, e_G — единичный элемент группы G, называют *соотношением между элементами* множества G_1 в группе G, или просто *соотношением* в G.

Пусть G_1 порождает G и S_1 — произвольная система соотношений между элементами из G_1 в группе G. Систему S_1 естественно было бы назвать системой определяющих соотношений, если любое соотношение в G является следствием системы S_1. Однако так поступить мы не можем, поскольку не определено понятие «следствия системы соотношений в группе G». Для преодоления указанной трудности перейдем от группы G к подходящей абстрактной группе $\widetilde{G} = \langle A; S \rangle$. Выберем в качестве A множество букв $\{a_i : i \in I\}$ с тем же множеством индексов I, что и для элементов из G_1, а в качестве S — систему, полученную заменой в S_1 каждого соотношения вида (8) или (9) соответственно соотношением

$$(a_{i_1}^{\varepsilon_1} \dots a_{i_k}^{\varepsilon_k},\ a_{j_1}^{\delta_1} \dots a_{j_l}^{\delta_l}) \quad \text{или} \quad (a_{j_1}^{\varepsilon_1} \dots a_{j_k}^{\varepsilon_k},\ e).$$

Сопоставим любому слову $P \equiv a_{r_1}^{\gamma_1} \dots a_{r_t}^{\gamma_t}$ элемент $\widehat{P} = g_{r_1}^{\gamma_1} \dots g_{r_t}^{\gamma_t}$ группы G, считая $\widehat{e} = e_G$, и определим отображение $\psi \colon \widetilde{G} \to G$ равенствами

$$\forall\, [P]_S \in \widetilde{G} : \ \psi([P]_S) = \widehat{P}. \tag{10}$$

Из построения системы S легко усмотреть, что соотношение $P \underset{S}{\to} Q$, а потому и $P \underset{S}{\sim} Q$, влечет равенство $\widehat{P} = \widehat{Q}$ в G. Значит, отображение ψ определено корректно.

Утверждение 7. *Отображение ψ, определенное формулой* (10)*, является эпиморфизмом групп.*

□ Так как G_1 порождает G, то любой элемент g из G представим в виде $g_{i_1}^{\varepsilon_1} \dots g_{i_k}^{\varepsilon_k}$. Следовательно, $\psi([a_{i_1}^{\varepsilon_1} \dots a_{i_k}^{\varepsilon_k}]_S) = g$, и отображение ψ сюръективно. Тот факт, что ψ — гомоморфизм, следует из очевидного равенства $\widehat{PQ} = \widehat{P}\widehat{Q}$ для любых слов $P, Q \in W(\overline{A})$. □

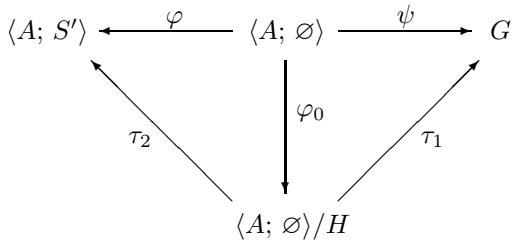
Определение 12. Множество соотношений S_1 между элементами системы образующих $G_1 = \{g_i : i \in I\}$ группы G называют *системой определяющих соотношений группы G в системе образующих G_1*, если определенное формулой (10) отображение ψ группы $\widetilde{G} = \langle A; S\rangle$ в G является изоморфизмом групп. При этом пару $(A; S)$ называют заданием группы G относительно системы образующих G_1, или просто *заданием группы G*. Говорят также, что группа G задается системой образующих элементов G_1 и системой определяющих соотношений S_1.

Из определения 12 следует, в частности, что пара $(A; S)$ является заданием группы $\langle A; S\rangle$ относительно системы образующих $\{[a_i]_S : a_i \in A\}$.

Теперь можно ответить на вопрос, поставленный в начале главы.

Теорема 8. *Для любой группы G и любой ее системы образующих $G_1 = \{g_i : i \in I\}$ существует задание группы G относительно системы образующих G_1.*

□ Выбрав в качестве S_1 пустую систему соотношений в группе G, мы, как и выше, построим по G_1 и S_1 группу $\widetilde{G} = \langle A; \varnothing\rangle$ и рассмотрим определенный формулой (10) при $S = \varnothing$ эпиморфизм $\psi : \widetilde{G} \to G$. Пусть $\operatorname{Ker}\psi = H = \{[P_j]_\varnothing : j \in J\}$, $S' = \{(P_j, e) : j \in J\}$ и φ — отображение группы $\langle A; \varnothing\rangle$ в группу $\langle A; S'\rangle$, определенное формулой (7) при $S_1 = \varnothing$, $S_2 = S'$. По теореме 5 φ есть эпиморфизм и $\operatorname{Ker}\varphi$ есть пересечение всех нормальных делителей группы $\langle A; \varnothing\rangle$, содержащих H. А так как $H \lhd \langle A; \varnothing\rangle$, то $\operatorname{Ker}\varphi = H$. Теперь, применив дважды теорему об эпиморфизме групп, получим коммутативную диаграмму:



в которой φ_0 — естественный эпиморфизм, а τ_1, τ_2 — изоморфизмы, причем $\tau_2^{-1}\tau_1([P]_{S'}) = \widehat{P}$ для любого слова $P \in W(\overline{A})$. Отсюда и из определения 12 следует, что $\langle A; S'\rangle$ есть искомое задание группы G относительно системы образующих G_1. □

Заметим, что указанная в доказательстве теоремы 8 система определяющих соотношений S' группы G, как правило, избыточна. Легко видеть, что при построении системы S' вместо H можно было бы взять любое множество, порождающее нормальный делитель H.

Напомним (см. определение 8 главы 11), что группа G называется *конечно порожденной*, если она имеет конечную систему образующих.

Определение 13. Группа G называется *конечно определенной*, если она может быть задана конечными системами образующих элементов и определяющих соотношений.

Пример 4. Группа $G = (\mathbb{Z}; +)$ относительно системы образующих $\{1\}$ имеет задание $(a_1; \varnothing)$. Действительно, пересечением всех нормальных делителей группы $H = \langle a_1; \varnothing\rangle$, содержащих множество $\varnothing$, является единичная подгруппа, и потому указанный в теореме 8 эпиморфизм ψ является изоморфизмом.

Для нахождения систем определяющих соотношений конечной группы может оказаться полезным

Утверждение 9. *Пусть $G = \{g_1, \ldots, g_n\}$ — система образующих конечной группы G, $A = \{a_1, \ldots, a_n\}$ — множество букв, и S — система соотношений в алфавите $\overline{A}$. Если для каждого соотношения (P, Q) из S в группе G выполняется равенство $\widehat{P} = \widehat{Q}$ и $|\langle A; S\rangle| \leqslant |G|$, то $(A; S)$ есть задание группы G относительно системы образующих G_1.*

□ Для доказательства утверждения достаточно заметить, что в силу неравенства $|\langle A; S\rangle| \leqslant |G|$ определенный формулой (10) эпиморфизм $\psi\colon \langle A; S\rangle \to G$ является изоморфизмом. □

Пример 5. Из утверждения 9 легко следует, что рассмотренные в примерах 1, 2 циклическая группа C_m порядка m и группа диэдра D_n порядка $2n$ имеют, соответственно, задания

$$(a_1;\ (a_1^m,\, e)), \quad (a_1, a_2;\ (a_1^n, e),\, (a_2^2, e),\, (a_2 a_1,\, a_1^{-1} a_2)).$$

Применим утверждение 9 к нахождению задания симметрической группы S_n в системе образующих $G_n = \{g_i :\ i \in \overline{1,\, n-1}\}$, где $g_i = (i,\, i+1)$ — транспозиция из S_n. Нетрудно проверить, что для элементов из G_n в S_n выполняются соотношения:

(а) $g_i^2 = \varepsilon$ для $i \in \overline{1,\, n-1}$, где ε — единичный элемент в S_n;

(б) $g_i g_j = g_j g_i$ для $i, j \in \overline{1,\, n-1}$, $|i-j| > 1$ (если $n > 3$);

(в) $g_i g_{i+1} g_i = g_{i+1} g_i g_{i+1}$ для $i \in \overline{1,\, n-2}$ (если $n > 2$).

Оказывается, справедлива

Теорема 10. *Система* (а)–(в) *является системой определяющих соотношений группы S_n относительно ее системы образующих G_n.*

□ Рассмотрим абстрактную группу $H_n = \langle B_n; T_n\rangle$, в которой $B_n = \{b_1, \ldots, b_{n-1}\}$, а T_n состоит из трех систем соотношений:

(а′) $(b_i^2,\, e)$, $i \in \overline{1,\, n-1}$;

(б′) $(b_i b_j,\, b_j b_i)$, $i, j \in \overline{1,\, n-1}$, $|i-j| > 1$ (если $n > 3$);

(в′) $(b_i b_{i+1} b_i,\, b_{i+1} b_i b_{i+1})$, $i \in \overline{1, n-2}$ (если $n > 2$).

Согласно утверждению 9 для доказательства теоремы 10 достаточно доказать неравенство

$$|H_n| \leqslant n!\,. \tag{11}$$

Докажем сначала вспомогательное утверждение.

Лемма. *Любое слово P в алфавите B_n T_n-эквивалентно слову вида $P_1 Q_1$, где P_1 не содержит буквы b_{n-1}, а $Q_1 \rightleftharpoons b_{n-1} b_{n-2} \ldots b_{n-k}$, $k \in \overline{1,\, n-1}$, или $Q_1 \rightleftharpoons e$.*

□ Из соотношений (а′) легко следует, что $b_i^{-1} \underset{T_n}{\sim} b_i$. Поэтому можно считать, что в исходное слово P не входят символы b_i^{-1}, $i \in \overline{1,\, n-1}$. Если в P не входит b_{n-1}, то утверждение леммы верно. Пусть

$$P \equiv P_1 b_{n-1} P_2,$$

где P_1 не содержит буквы b_{n-1}. В этом случае утверждение леммы докажем индукцией по длине $l(P_2)$ слова P_2. При $l(P_2) = 0$ оно очевидно. Допустим, что оно верно при всех P_2 с условием $l(P_2) \leqslant r$, и докажем его при $l(P_2) = r+1$. Если $P_2 \equiv b_{n-1} \dots b_{n-t}$, то утверждение леммы верно. Поэтому будем считать, что

$$P \equiv P_1 b_{n-1} \dots b_{n-t} b_s P_2',$$

где $s \neq n-t-1$, $1 \leqslant t \leqslant n-1$. Будем применять к слову P различные элементарные преобразования в зависимости от параметра s.

1. При $s = n-t$ заменим в P подслово $b_{n-t}b_s$ пустым словом (по соотношению из (а′));

2. При $s < n-t-1$ переставим в P букву b_s последовательно со всеми буквами $b_{n-t}, \dots, b_{n-1}$ (по соотношениям из (б′));

3. При $s > n-t-1$ переставим b_s с буквами b_{n-t}, …, b_{s-2}; в полученном слове

$$P_1 b_{n-1} \dots b_{s+1} \underline{b_s b_{s-1} b_s} b_{s-2} \dots b_{n-t} P_2'$$

заменим подчеркнутое подслово $b_s b_{s-1} b_s$ словом $b_{s-1} b_s b_{s-1}$ (по соотношению из (в′)), а затем переставим b_{s-1} с буквами b_{s+1}, …, b_{n-1}. Во всех случаях мы получим T_n-эквивалентное слову P слово P', которое или не содержит b_{n-1}, или имеет вид $P_1' b_{n-1} P_2'$, где P_1' не содержит b_{n-1}, а $l(P_2') \leqslant r$. По предположению индукции слово P' T_n-эквивалентно слову нужного вида. □

Теперь индукцией по n легко доказать, что любое слово P из $W(\overline{B}_n)$ эквивалентно слову вида

$$b_{k_1} b_{k_1-1} \dots b_{k_1-t_1} b_{k_2} b_{k_2-1} \dots b_{k_2-t_2} \dots b_{k_s} b_{k_s-1} \dots b_{k_s-t_s}, \tag{12}$$

где $1 \leqslant k_1 < k_2 < \dots < k_s \leqslant n-1$, $0 \leqslant t_i < k_i$, $i \in \overline{1,s}$, и что число различных слов вида (12) из $W(\overline{B}_n)$ не превосходит $n!$. Следовательно, $|H_n| \leqslant n!$, т. е. неравенство (11) верно и теорема доказана. □

Определение 14. Группа G называется *свободной группой*, а ее система образующих G_1 — *свободной системой образующих*, если для группы G существует задание вида $(A;\, \varnothing)$ относительно системы образующих G_1.

Так как пара $(A;\, \varnothing)$ является заданием группы $\langle A;\, \varnothing\rangle$ относительно системы образующих $\widetilde{A} = \{[a_i]_\varnothing : a_i \in A\}$, то $\langle A;\, \varnothing\rangle$ является свободной группой со свободной системой образующих $\widetilde{A}$. Из примера 4 видно, что $(\mathbb{Z};+)$ является свободной группой со свободной системой образующих $\{1\}$.

Заметим, что свободная система образующих свободной группы находится неоднозначно. Так, свободной системой образующих группы $(\mathbb{Z}; +)$ является не только система $\{1\}$, но и $\{-1\}$. Докажите это в качестве упражнения.

Отметим без доказательства известный из теории групп факт о равномощности любых двух свободных систем образующих свободной группы.

О большой роли свободных групп в теории групп свидетельствует

Утверждение 11. *Любая группа является гомоморфным образом подходящей свободной группы и потому изоморфна факторгруппе свободной группы.*

□ Для любой группы G существует система образующих (например, все множество G). Если $G = \langle G_1 \rangle$, то по теореме 8 существует задание $(A; S)$ группы G относительно системы образующих G_1. По определению 12 $G \cong \langle A; S \rangle$, а по теореме 5 группа $\langle A; S \rangle$ является гомоморфным образом группы $\langle A; \varnothing \rangle$. Следовательно, G есть гомоморфный образ группы $\langle A; \varnothing \rangle$, и по теореме об эпиморфизме групп $G \cong \langle A; \varnothing \rangle / H$, где H — ядро эпиморфизма группы $\langle A; \varnothing \rangle$ на G. □

§ 3. ПЕРЕХОД ОТ ОДНОГО ЗАДАНИЯ ГРУППЫ К ДРУГОМУ ЗАДАНИЮ. ТЕОРЕМА ТИЦЕ

Легко видеть, что для одной и той же группы можно указать много различных заданий с помощью образующих элементов и определяющих соотношений. Система простейших преобразований, позволяющая переходить от любого одного задания группы к любому другому ее заданию, была указана в 1908 г. немецким математиком Х. Тице.

Определение 15. *Преобразованиями Тице* задания $(A; S)$[35] группы называются:

I) добавление к S любого следствия системы S;

II) удаление из S любого следствия остальных соотношений;

III) добавление к A новой (не содержащейся в $\overline{A}$) буквы a с одновременным добавлением к S соотношения (R, a), где R — любое фиксированное слово из $W(\overline{A})$;

IV) удаление из A буквы a и из S соотношения (R, a) при условии, что a и a^{-1} не входят в R и в другие соотношения из S.

Иногда при определении преобразований Тице вместо IV берут более общее преобразование:

V) удаление из A буквы a и из S соотношения (R, a), где $R \in W(\overline{A \setminus \{a\}})$, с одновременной заменой во всех остальных соотношениях из S каждого символа a^{ε}, $\varepsilon \in \{1, -1\}$, на R^{ε}.

Можно показать, что, взяв IV вместо V, мы не потеряли в общности.

Утверждение 12. *Любое преобразование типа* V *задания* $(A; S)$ *можно осуществить с помощью преобразований типа* I–IV.

[35] Здесь и ниже под заданием $(A; S)$ всегда можно понимать задание группы $\langle A; S \rangle$.

□ Пусть $a \in A$, $(R, a) \in S$, $P \in W(\overline{A})$. Обозначим через $\widetilde{P}$ слово, полученное из P заменой каждого символа a^ε, $\varepsilon \in \{1, -1\}$, словом R^ε. Легко видеть, что

$$\{(P, Q),\ (R, a)\} \approx \{(\widetilde{P}, \widetilde{Q}),\ (R, a)\}.$$

Поэтому можно с помощью преобразований I добавить к S все соотношения $(\widetilde{P}, \widetilde{Q})$, где $(P, Q) \in S \setminus \{(R, a)\}$, а затем с помощью преобразований II из полученной системы удалить все соотношения системы $S \setminus \{(R, a)\}$. Теперь для осуществления преобразования V осталось с помощью преобразования IV удалить a и соотношение (R, a). □

В дальнейшем нам понадобится также

Утверждение 13. *С помощью преобразований Тице можно перейти от задания $(A; S)$ к заданию $(A'; S')$, где A' получено из A заменой любой одной буквы a некоторой буквой $b \notin \overline{A}$, а S' получено из S заменой каждого символа a^ε, $\varepsilon \in \{1, -1\}$, на b^ε.*

□ Для осуществления указанного перехода достаточно с помощью преобразования III добавить к A букву b, а к S — соотношение (a, b), а затем с помощью преобразования V удалить букву a с необходимой заменой соотношений. □

О значении преобразований Тице свидетельствует

Теорема 14 (Тице). *Пусть $G = \langle A; S\rangle$, $H = \langle B; T\rangle$ — абстрактные группы, заданные конечными системами образующих элементов и определяющих соотношений. Группы G, H изоморфны тогда и только тогда, когда задание $(A; S)$ можно перевести в $(B; T)$ конечной последовательностью преобразований Тице.*

□ Пусть $(B; T)$ получено из $(A; S)$ конечной цепочкой преобразований Тице. Докажем, что $G \cong H$. Ясно, что достаточно рассмотреть случай, когда $(B; T)$ получено из $(A; S)$ лишь одним преобразованием. Если им было преобразование типа I или II, то $G = H$ по утверждению 2. Пусть использовалось преобразование типа III, и $B = A \cup \{a\}$, $T = S \cup \{(R, a)\}$, где $a \notin \overline{A}$, $R \in W(\overline{A})$. Определим отображение $\varphi\colon H \to G$, положив

$$\forall\, [P]_T \in H:\ \ \varphi([P])_T = [\widetilde{P}]_S. \tag{13}$$

Для доказательства корректности этого определения достаточно показать, что

$$\forall\, P, Q \in W(\overline{B}):\ \ (P \underset{T}{\to} Q)\ \Rightarrow\ (\widetilde{P} \underset{S}{\to} \widetilde{Q}).$$

Пусть преобразование $P \underset{T}{\to} Q$ осуществлено по соотношению (P_1, Q_1) и $P = P' P_1 P''$, $Q = P' Q_1 P''$. Возможны случаи:

1. $(P_1, Q_1) \in S$,
2. $(P_1, Q_1) = (a_i^\varepsilon a_i^{-\varepsilon}, e)$, $a_i \in A$,
3. $(P_1, Q_1) = (a^\varepsilon a^{-\varepsilon}, e)$,
4. $(P_1, Q_1) = (R, a)$.

В случаях 1, 2 $\widetilde{P} \equiv \widetilde{P}'P_1\widetilde{P}''$, $\widetilde{Q} \equiv \widetilde{P}'Q_1\widetilde{P}''$, и очевидно $\widetilde{P} \underset{S}{\to} \widetilde{Q}$. В случае 3 $\widetilde{P} \equiv \widetilde{P}'R^{\varepsilon}R^{-\varepsilon}\widetilde{P}''$, $\widetilde{Q} \equiv \widetilde{P}'\widetilde{P}''$, и $\widetilde{P} \underset{S}{\sim} \widetilde{Q}$ в силу условия $R^{\varepsilon}R^{-\varepsilon} \underset{S}{\sim} e$ (см. (5)). В случае 4 $\widetilde{P} \equiv \widetilde{Q}$, и потому $\widetilde{P} \underset{S}{\sim} \widetilde{Q}$. Таким образом, φ определено корректно. Так как для $P \in W(\overline{A})$ имеет место равенство $\widetilde{P} \equiv P$, то $\varphi([P]_T) = [P]_S$, и потому φ сюръективно. Отображение φ инъективно, поскольку из соотношений $S \subset T$, $\widetilde{P} \underset{T}{\sim} P$, $\widetilde{Q} \underset{T}{\sim} Q$ получаем соответственно:

$$\widetilde{P} \underset{S}{\sim} \widetilde{Q} \;\Rightarrow\; \widetilde{P} \underset{T}{\sim} \widetilde{Q}, \quad \widetilde{P} \underset{T}{\sim} \widetilde{Q} \;\Rightarrow\; P \underset{T}{\sim} Q.$$

Кроме того, из очевидного равенства $\widetilde{PQ} \equiv \widetilde{P}\widetilde{Q}$ легко следует, что φ — гомоморфизм. Следовательно, φ — изоморфизм, и $G \cong H$.

Пусть, наконец, $(B; T)$ получено из $(A; S)$ преобразованием типа IV. Тогда $(A; S)$ можно получить из $(B; T)$ преобразованием типа III, и изоморфизм $G \cong H$ доказан выше. В итоге теорема Тице в одну сторону доказана.

Обратно, пусть имеется изоморфизм $\varphi\colon H \to G$. Докажем, что от $(A; S)$ к $(B; T)$ можно перейти конечной последовательностью преобразований Тице. При этом, учитывая утверждение 12 и доказанную часть теоремы Тице, можно считать, что $\overline{A} \cap \overline{B} = \varnothing$. Обозначим

$$A = \{a_1, \ldots, a_n\}, \quad B = \{b_1, \ldots, b_m\} \quad \text{и} \quad \varphi([b_i]_T) = [R_i]_S,$$

где $R_i \in W(\overline{A})$, $i \in \overline{1,m}$. Преобразованиями типа III перейдем сначала от задания $(A; S)$ к заданию $(A \cup B;\ S \cup S')$, где $S' = \{(b_i, R_i)\colon i \in \overline{1,m}\}$, что возможно в силу условия $\overline{A} \cap \overline{B} = \varnothing$. Теперь докажем, что любое соотношение (P, Q) из T есть следствие системы $S \cup S'$, т. е. $P \underset{S\cup S'}{\sim} Q$. Пусть $P \equiv b_{i_1}^{\varepsilon_1} \ldots b_{i_k}^{\varepsilon_k}$, $Q \equiv b_{j_1}^{\delta_1} \ldots b_{j_l}^{\delta_l}$. Так как $\varphi([b_i]_T) = [R_i]_S$ и φ — изоморфизм группы H на G, то имеем:

$$\varphi([P]_T) = [R_{i_1}^{\varepsilon_1} \ldots R_{i_k}^{\varepsilon_k}]_S, \quad \varphi([Q]_T) = [R_{j_1}^{\delta_1} \ldots R_{j_l}^{\delta_l}]_S. \tag{14}$$

Из условия $(P, Q) \in T$ следует, что $P \underset{T}{\sim} Q$, и в H выполняется равенство $[P]_T = [Q]_T$. Отсюда и из (14) получаем равенство в группе G: $[R_{i_1}^{\varepsilon_1} \ldots R_{i_k}^{\varepsilon_k}]_S = [R_{j_1}^{\delta_1} \ldots R_{j_l}^{\delta_l}]_S$, т. е. эквивалентность

$$R_{i_1}^{\varepsilon_1} \ldots R_{i_k}^{\varepsilon_k} \underset{S}{\sim} R_{j_1}^{\delta_1} \ldots R_{j_l}^{\delta_l}.$$

Заменив в ней по соотношениям из S' каждое из слов R_t буквой b_t, $t \in \overline{1,m}$, мы получим искомое соотношение $P \underset{S\cup S'}{\sim} Q$.

Теперь с помощью преобразований Тице типа I мы можем от задания $(A \cup B;\ S \cup S')$ перейти к заданию $(A \cup B; S \cup S' \cup T)$. Пусть $\varphi([L_j]_T) = [a_j]_S$, $j \in \overline{1,n}$, где $L_j \in W(\overline{B})$. Так как φ — изоморфизм и $\varphi([b_i]_T) = [R_i]_S$, то для $L_j \equiv b_{t_1}^{\gamma_1} \ldots b_{t_k}^{\gamma_k}$ получим $\varphi([L_j]_T) = [R_{t_1}^{\gamma_1} \ldots R_{t_k}^{\gamma_k}]_S$. Следовательно, $a_j \underset{S}{\sim} R_{t_1}^{\gamma_1} \ldots R_{t_k}^{\gamma_k}$, и потому $a_j \underset{S\cup S'}{\sim} L_j$. Таким образом, следствиями системы $S \cup S'$ являются все соотношения системы $T' = \{(a_j, L_j)\colon j \in \overline{1,n}\}$, и с помощью преобразований Тице типа I мы

можем от задания $(A\cup B;\ S\cup S'\cup T)$ перейти к заданию $(A\cup B;\ S\cup T\cup S'\cup T')$. В силу симметрии к этому заданию можно перейти преобразованиями Тице и от задания $(B;\ T)$. А так как для каждого преобразования Тице есть обратное преобразование Тице, то преобразованиями Тице можно перевести задание $(A;\ S)$ в $(B;\ T)$. Осталось заметить, что последовательность необходимых при этом преобразований конечна. □

Рассмотрим практически важное приложение теоремы Тице к построению задания группы относительно одной системы образующих по ее заданию относительно другой системы образующих. При решении этой задачи нам будет удобно произведения элементов из множества $x_1,\ \ldots,\ x_k,\ x_1^{-1},\ \ldots,\ x_k^{-1}$ в группе G обозначать в виде $P_i(x_1,\ldots,x_k)$, $Q_i(x_1,\ldots,x_k)$. Тогда произведение в группе G или слово в некотором алфавите, полученное заменой в $P(x_1,\ldots,x_k)$ каждого элемента $x_i,\ i\in\overline{1,k}$, соответственно произведением в G или словом Q_i, запишется в виде $P(Q_1,\ldots,Q_k)$. При этом следует иметь в виду, что если x_i заменяется произведением или словом $c_{i_1}^{\varepsilon_1}\ldots c_{i_r}^{\varepsilon_r}$, то одновременно x_i^{-1} заменяется на $c_{i_r}^{-\varepsilon_r}\ldots c_{i_1}^{-\varepsilon_1}$.

Теорема 15. *Пусть $G_1=\{g_1,\ldots,g_n\}$, $H_1=\{h_1,\ldots,h_m\}$ — системы образующих группы G, S_1 — система определяющих соотношений группы G в системе образующих G_1, и в G выполняются соотношения*:

$$g_i=P_i(h_1,\ldots,h_m),\ i\in\overline{1,n};\quad h_j=Q_j(g_1,\ldots,g_n),\ j\in\overline{1,m}.$$

Тогда система соотношений T_1 в G, полученная заменой во всех соотношениях из S_1 и во всех соотношениях системы

$$S_2=\{h_j=Q_j(g_1,\ldots,g_n):\ j\in\overline{1,m}\}$$

элемента g_i произведением $P_i(h_1,\ldots,h_m)$, $i\in\overline{1,n}$, является системой определяющих соотношений группы G относительно системы образующих H_1.

□ Пусть $A=\{a_1,\ldots,a_n\}$ и $(A;\ S)$ есть задание группы G относительно системы образующих G_1. Тогда согласно определению 12 отображение $\psi\colon\langle A;\ S\rangle\to G$, заданное в (10), является изоморфизмом групп. Следовательно, справедливы соотношения

$$a_i\underset{S}{\sim}P_i(Q_1(a_1,\ldots,a_n),\ldots,Q_m(a_1,\ldots,a_n)),\quad i\in\overline{1,m}. \tag{15}$$

Выберем множество букв $B=\{b_1,\ldots,b_m\}$, не содержащихся в $\overline{A}$, и преобразованиями Тице типа III перейдем от задания $(A;\ S)$ к заданию $(A\cup B;\ S\cup S')$, где

$$S'=\{(b_j,\ Q_j(a_1,\ldots,a_n)):\ j\in\overline{1,m}\}.$$

Из (15) следует, что $a_i\underset{S\cup S'}{\sim}P_i(b_1,\ldots,b_m)$, $i\in\overline{1,n}$, и потому с помощью преобразований Тице типа I можно от задания $(A\cup B;\ S\cup S')$ перейти к заданию $(A\cup B;\ S\cup S'\cup T')$, где $T'=\{(a_i,P_i(b_1,\ldots,b_m)):\ i\in\overline{1,n}\}$. Теперь, преобразованиями типа V удалим из задания $(A\cup B;\ S\cup S'\cup T')$ все буквы $a_i\in A$ и все соотношения системы T', заменив во всех остальных соотношениях каждый символ a_i^{ε} словом $P_i^{\varepsilon}(b_1,\ldots,b_m)$, $i\in\overline{1,n}$, $\varepsilon\in\{1,-1\}$. В итоге получим задание $(B;\ T)$ группы G. Покажем, что это есть задание относительно системы образующих H_1. Из построения изоморфизма φ группы

$\langle A, a;\, S, (R, a)\rangle$ в группу $\langle A;\, S\rangle$, осуществленного при доказательстве теоремы Тице (см. (13)), следует, что изоморфизмом группы $\langle A \cup B;\, S \cup S' \cup T'\rangle$, или, что то же самое, группы $\langle A \cup B;\, S \cup S'\rangle$, на группу $\langle A;\, S\rangle$ может служить отображение φ_1, определенное для любого элемента $[P(a_1, \ldots, a_n, b_1, \ldots, b_m)]_{S\cup S'}$ равенством

$$\varphi_1([P(a_1, \ldots, a_n, b_1, \ldots, b_m)]_{S\cup S'}) = [P(a_1, \ldots, a_n, Q_1, \ldots, Q_m)]_S.$$

Из соображений симметрии следует, что изоморфизмом группы $\langle A\cup B;\, S\cup S'\cup T'\rangle$ на группу $\langle B;\, T\rangle$ является отображение φ_2, определенное при любом $P \in W(\overline{A \cup B})$ равенством

$$\varphi_2([P(a_1, \ldots, a_n, b_1, \ldots, b_m)]_{S\cup S'\cup T'}) = [P(P_1, \ldots, P_n, b_1, \ldots, b_n)]_T.$$

Следовательно, отображение $\psi_1 = \varphi_2^{-1}\varphi_1\psi$ является изоморфизмом группы $\langle B;\, T\rangle$ на группу G, причем легко проверить, что $\psi_1([b_i]_T) = h_i$ для всех $i \in \overline{1, m}$. Отсюда следует, что $\psi_1([b_{i_1}^{\varepsilon_1} \ldots b_{i_k}^{\varepsilon_k}]_T) = h_{i_1}^{\varepsilon_1} \ldots h_{i_k}^{\varepsilon_k}$ для любого элемента $[b_{i_1}^{\varepsilon_1} \ldots b_{i_k}^{\varepsilon_k}]_T \in \langle B;\, T\rangle$, и согласно определению 12 $(B;\, T)$ есть задание группы G относительно H_1. Остается заметить, что соотношение $P(h_1, \ldots, h_m) = Q(h_1, \ldots, h_m)$ лежит в T_1 в том и только том случае, когда $(P(b_1, \ldots, b_m),\, Q(b_1, \ldots, b_m)) \in T$. $\square$

Пример 6. Найти систему определяющих соотношений и задание группы S_n относительно системы образующих

$$H_n = \{h_1, h_2\}, \text{ где } h_1 = (1, 2),\ h_2 = (1, 2, \ldots, n).$$

Воспользуемся заданием группы S_n относительно системы образующих $G_n = \{g_1, \ldots, g_{n-1}\}$ из теоремы 10. Легко видеть, что в S_n выполняются соотношения

$$g_i = h_2^{-(i-1)} h_1 h_2^{i-1}, \quad i \in \overline{1, n-1}, \quad h_1 = g_1, \quad h_2 = g_{n-1} g_{n-2} \ldots g_1.$$

Тогда по теореме 15 имеем систему определяющих соотношений группы S_n в системе образующих H_n:

(а″) $h_2^{-(i-1)} h_1 h_2^{i-1} h_2^{-(i-1)} h_1 h_2^{i-1} = e$, $i \in \overline{1, n-1}$;

(б″) $h_2^{-(i-1)} h_1 h_2^{i-1} h_2^{-(j-1)} h_1 h_2^{j-1} = h_2^{-(j-1)} h_1 h_2^{j-1} h_2^{-(i-1)} h_1 h_2^{i-1}$,
$i, j \in \overline{1, n-1}$, $|i - j| > 1$ (если $n > 3$);

(в″) $h_2^{-(i-1)} h_1 h_2^{i-1} h_2^{-i} h_1 h_2^{i} h_2^{-(i-1)} h_1 h_2^{i-1} = h_2^{-i} h_1 h_2^{i} h_2^{-(i-1)} h_1 h_2^{i-1} h_2^{-i} h_1 h_2^{i}$,
$i \in \overline{1, n-2}$ (если $n > 2$);

(г″) $h_2 = h_2^{-(n-2)} h_1 h_2^{n-2} h_2^{-(n-3)} h_1 h_2^{n-3} \ldots h_2^{-1} h_1 h_2 h_1$.

Отсюда и из утверждения 4 легко следует, что вместо (а″)–(г″) можно взять и более простую систему соотношений:

(а‴) $h_1^2 = e$;

(б‴) $h_2^k h_1 h_2^{-k} h_1 = h_1 h_2^k h_1 h_2^{-k}$, $k \in \overline{2, n-1}$ (если $n > 3$);

(в‴) $h_2 h_1 h_2^{-1} h_1 h_2 h_1 = h_1 h_2 h_1 h_2^{-1} h_1 h_2$ (если $n > 2$);

(г‴) $h_2^n = (h_2 h_1)^{n-1}$.

§ 4. ОПИСАНИЕ КОНЕЧНО ОПРЕДЕЛЕННЫХ АБЕЛЕВЫХ ГРУПП

В этом параграфе задания групп образующими элементами и определяющими соотношениями применяются к описанию строения конечно определенных и, в частности, конечных абелевых групп.

Для описания конечно определенных абелевых групп с точностью до изоморфизма достаточно рассмотреть абелевы абстрактные группы, заданные конечными системами образующих элементов и определяющих соотношений. При изучении таких групп будем пользоваться аддитивной терминологией. Тогда для алфавита $A = \{a_1, \ldots, a_n\}$ множество $\overline{A}$ будет состоять из символов $+a_1, \ldots, +a_n, -a_1, \ldots, -a_n$, и любое непустое слово в алфавите $\overline{A}$ запишется в виде $\varepsilon_1 a_{i_1} \ldots \varepsilon_k a_{i_k}$, где $\varepsilon_i \in \{+, -\}$, $i \in \overline{1,k}$. Условимся обозначать пустое слово буквой θ, а слово вида $\underbrace{\varepsilon a_i \ldots \varepsilon a_i}_{k}$ — через ca_i, где $c = \varepsilon k$ — числовой коэффициент. В частности, $0a_i$ — пустое слово. Вместо $+1a_i$, $-1a_i$ будем писать соответственно $+a_i$, $-a_i$.

Легко видеть, что при любой системе соотношений S в алфавите $\overline{A}$ группа $\langle A;\, S\rangle$ коммутативна в том и только том случае, когда все соотношения системы $K = \{(a_i + a_j;\, a_j + a_i) :\ i, j \in \overline{1,n}\}$ являются следствиями системы S. В связи с этим можно условиться систему K всегда включать в систему определяющих соотношений абелевой группы, выделяя ее в отдельную подсистему. Тогда задание абелевой группы запишется в виде $(A;\, S \cup K)$, где S — любая (возможно пустая) система соотношений.

Утверждение 16. *С помощью соотношений из K и тривиальных соотношений любое слово P в алфавите $\overline{A}$ можно преобразовать к единственному каноническому слову вида*

$$c_1 a_1 \ldots c_n a_n, \tag{16}$$

где $c_1, \ldots, c_n \in \mathbb{Z}$. При этом c_i есть сумма всех коэффициентов перед буквой a_i в слове P.

□ Возможность преобразования слова P к слову вида (16) очевидна. Единственность следует из того, что при указанных преобразованиях слова остается неизменной сумма всех коэффициентов любой буквы a_i. □

Из утверждения 16 получаем

Утверждение 17. *Любая конечно определенная абелева группа имеет задание вида $(A;\, S \cup K)$, где $A = \{a_1, \ldots, a_n\}$, а система S или пуста, или имеет вид*

$$\begin{gathered}(c_{11}a_1 \ldots c_{1n}a_n,\, \theta),\\ \ldots\ldots\ldots\ldots\ldots\\ (c_{m1}a_1 \ldots c_{mn}a_n,\, \theta).\end{gathered} \tag{17}$$

Определение 16. Целочисленную матрицу $(c_{ij})_{m\times n}$, составленную из коэффициентов системы (17), назовем *матрицей задания* $(A;\, S \cup K)$ *группы* G и обозначим через $C_{A,S}$. В случае $S = \varnothing$ будем считать, что $C_{A,S} = O_{1\times n}$.

Заметим, что матрица $C_{A,S}$ не зависит от обозначения элементов из A. Поэтому по матрице $C_{A,S}$ задание $(A;\, S)$ восстанавливается лишь с точностью до обозначения образующих элементов.

Выясним, какие преобразования матрицы $C_{A,S}$ отвечают преобразованиям Тице задания $(A;\, S \cup K)$. Предварительно докажем

Утверждение 18. *Соотношение*

$$(c_1 a_1 \dots c_n a_n,\, \theta) \tag{18}$$

является следствием системы $S \cup K$ тогда и только тогда, когда вектор-строка $\gamma = (c_1, \dots, c_n)$ является целочисленной линейной комбинацией строк матрицы $C_{A,S}$.

□ Пусть соотношение (18) есть следствие системы $U = S \cup K$, где S есть система (17). Тогда существует цепочка преобразований:

$$c_1 a_1 \dots c_n a_n = R_0 \underset{U}{\to} R_1 \underset{U}{\to} \dots \underset{U}{\to} R_t = \theta. \tag{19}$$

Используя соотношения из K и тривиальные соотношения, приведем каждое слово R_i к каноническому слову R_i', $i \in \overline{0,t}$, и выясним, как связаны между собой слова R_i' и R_{i+1}'. Если преобразование $R_i \to R_{i+1}$ осуществлялось по соотношению из K или по тривиальному соотношению, то $R_i' = R_{i+1}'$ по утверждению 16. Если же использовалось соотношение $(c_{j1} a_1 \dots c_{jn} a_n,\, \theta)$, то в силу утверждения 16 имеем: строка коэффициентов $\vec{\gamma}_{i+1}$ слова R_{i+1}' получается из строки коэффициентов $\vec{\gamma}_i$ слова R_i' прибавлением или вычитанием j-й строки $(c_{j1}, \dots, c_{jn}) = \vec{C}_j$ матрицы $C_{A,S}$. Итак, в любом случае $\vec{\gamma}_{i+1} = \vec{\gamma}_i + \varepsilon \vec{C}_j$, где $\varepsilon \in \{0, 1, -1\}$. Отсюда и из (19) имеем:

$$\vec{\gamma} + \varepsilon_1 \vec{C}_{j_1} + \dots + \varepsilon_t \vec{C}_{j_t} = (0, \dots, 0), \quad \text{где} \quad \varepsilon_1, \dots, \varepsilon_t \in \{0, 1, -1\}.$$

Следовательно, $\vec{\gamma} = -\varepsilon_1 \vec{C}_{j_1} - \dots - \varepsilon_t \vec{C}_{j_t}$ — линейная комбинация строк матрицы $C_{A,S}$. Обратное утверждение очевидно. □

Утверждение 19. *Пусть $(A;\, S \cup K)$, $(B;\, T \cup K)$ — конечные задания абелевых групп. Задание $(B;\, T \cup K)$ получено из $(A;\, S \cup K)$ одним преобразованием Тице типа* I–IV *в том и только том случае, когда матрица $C_{B,T}$ получена из $C_{A,S}$ соответственно*:

I′) *добавлением строки, являющейся целочисленной линейной комбинацией строк матрицы $C_{A,S}$*;

II′) *удалением строки, являющейся целочисленной линейной комбинацией остальных строк*;

III′) *добавлением столбца и строки с 1 на их пересечении и с нулевыми остальными элементами добавляемого столбца*;

IV′) *удалением столбца и строки с 1 на их пересечении при условии, что остальные элементы удаляемого столбца нулевые и $C_{A,S} \neq (0, \dots, 0, 1, 0 \dots 0)$ (в последнем случае удаляется лишь столбец с 1).*

□ Доказательство осуществляется непосредственной проверкой с использованием определения 15 и утверждения 18. Проделайте ее в качестве упражнения. □

В дальнейшем для краткости будем называть преобразования III′, IV′ соответственно *расширением* и *сужением матрицы*.

Утверждение 20. *Любое элементарное преобразование матрицы $C_{m\times n}$ над кольцом $\mathbb{Z}$ можно осуществить с помощью преобразований типа* I′–IV′.

□ 1. Для умножения строки $\vec{C}_i$ матрицы C на обратимый элемент $\delta = \pm 1$ кольца $\mathbb{Z}$ достаточно добавить к C (между строками $\vec{C}_i$ и $\vec{C}_{i+1}$) строку $\delta\vec{C}_i$, а затем удалить $\vec{C}_i$.

2. Для прибавления строки $\vec{C}_i$, умноженной на $r \in \mathbb{Z}$, к строке $\vec{C}_j$ достаточно добавить к C (между строками $\vec{C}_j$ и $\vec{C}_{j+1}$) строку $\vec{C}_j + r\vec{C}_i$, а затем удалить $\vec{C}_j$ (как линейную комбинацию строк $\vec{C}_i$ и $\vec{C}_j + r\vec{C}_i$).

3. Для умножения столбца $\vec{C}_j$ на -1 достаточно расширить матрицу C до матрицы

$$C' = \begin{pmatrix} C_1^{\downarrow} & \dots & C_{j-1}^{\downarrow} & C_j^{\downarrow} & O^{\downarrow} & C_{j+1}^{\downarrow} & \dots & C_n^{\downarrow} \\ 0 & \dots & 0 & 1 & 1 & 0 & \dots & 0 \end{pmatrix},$$

в матрице C' к i-й строке, $i \in \overline{1,m}$, прибавить $(m+1)$-ю строку, умноженную на $-c_{ij}$, и полученную матрицу сузить путем удаления j-го столбца и $(m+1)$-й строки.

4. Для прибавления к столбцу $C_i^{\downarrow}$ столбца $C_j^{\downarrow}$, умноженного на $r \in \mathbb{Z}$, $i \neq j$, достаточно расширить C до матрицы

$$C'' = \begin{pmatrix} C_1^{\downarrow} & \dots & C_{i-1}^{\downarrow} & C_i^{\downarrow} & C_{i+1}^{\downarrow} & \dots & C_{j-1}^{\downarrow} & C_j^{\downarrow} & O^{\downarrow} & C_{j+1}^{\downarrow} & \dots & C_n^{\downarrow} \\ 0 & \dots & 0 & r & 0 & \dots & 0 & -1 & 1 & 0 & \dots & 0 \end{pmatrix},$$

в C'' к l-й строке, $l \in \overline{1,m}$, прибавить $(m+1)$-ю строку, умноженную на c_{lj}, после чего $(m+1)$-ю строку умножить на -1, и полученную матрицу сузить путем удаления j-го столбца и $(m+1)$-й строки. □

Определение 17. Пусть C — матрица над $\mathbb{Z}$, и ее каноническая форма $\mathcal{K}(C)$ имеет вид

$$\operatorname{diag}(\underbrace{1,\dots,1}_{r}, d_1, \dots, d_s, \underbrace{0,\dots,0}_{t})_{m\times m}, \quad \text{где } r, s, t \in \mathbb{N}_0,$$

$d_1, \dots, d_s \in \mathbb{N} \setminus \{1\}$. Упорядоченный набор чисел $(n-(r+s), d_1, \dots, d_s)$ назовем *системой инвариантов матрицы* C и обозначим через $I(C)$.

Утверждение 21. *Если матрица C' получена из матрицы C с помощью преобразований* I′–IV′*, то $I(C') = I(C)$.*

□ Достаточно рассмотреть случаи, когда C' получена из $C_{m\times n}$ одним преобразованием вида I′ или III′. Рассмотрим эти случаи.

1. C' получена из C добавлением строки $\vec{D} = \vec{C}_1 r_1 + \dots + \vec{C}_m r_m$. При нахождении матрицы $\mathcal{K}(C')$ можно начать с прибавления к строке $\vec{D}$ строк $\vec{C}_1, \dots, \vec{C}_m$, умноженных соответственно на $-r_1, \dots, -r_m$. В итоге строка $\vec{D}$ заменится нулевой строкой.

Отсюда видно, что $\mathcal{K}(C')$ отличается от $\mathcal{K}(C)$ одной лишней нулевой строкой. Отсюда и из определения 17 видно, что $I(C') = I(C)$.

2. Если C' получена из C преобразованием типа III′, то с помощью перестановок строк и столбцов в матрице C' ее можно привести к виду

$$\begin{pmatrix} 1 & d_1 & d_2 & \dots & d_n \\ 0 & & & & \\ \vdots & & C & & \\ 0 & & & & \end{pmatrix}.$$

Отсюда видно, что главная диагональ матрицы C' будет отличаться от диагонали матрицы C только одной лишней единицей. Следовательно, $I(C') = I(C)$. □

Теорема 22. *Пусть $G = \langle A;\, S \cup K\rangle$ и $H = \langle B;\, T \cup K\rangle$ — абелевы группы, заданные конечными системами образующих элементов и определяющих соотношений. Тогда*

$$G \cong H \;\Leftrightarrow\; I(C_{A,S}) = I(C_{B,T}).$$

□ Если $G \cong H$, то по теореме Тице от задания $\langle A;\, S \cup K\rangle$ к заданию $\langle B;\, T \cup K\rangle$ можно перейти с помощью преобразований Тице, а тогда по утверждению 19 от матрицы $C_{A,S}$ к $C_{B,T}$ можно перейти с помощью преобразований типа I′–IV′. Следовательно, по утверждению 21, $I(C_{A,S}) = I(C_{B,T})$.

Обратно, пусть $I(C_{A,S}) = I(C_{B,T})$. Тогда в силу определения 17 матрицы $\mathcal{K}(C_{A,S})$, $\mathcal{K}(C_{B,T})$ имеют одно и то же число нулевых столбцов, и их главные диагонали могут отличаться лишь числом единиц и нулей. Отсюда видно, что любую из матриц $\mathcal{K}(C_{A,S})$, $\mathcal{K}(C_{B,T})$ можно перевести в другую преобразованиями I′–IV′. А так как в силу утверждения 20 то же верно для матриц C и $\mathcal{K}(C)$ при любой матрице C над $\mathbb{Z}$, то от матрицы $C_{A,S}$ к $C_{B,T}$ можно перейти преобразованиями I′–IV′. Отсюда и из утверждения 19 следует, что от задания $\langle A;\, S \cup K\rangle$ к заданию $\langle B;\, T \cup K\rangle$ можно перейти с помощью преобразований Тице, и $G \cong H$ по теореме 15. □

Из теоремы 22 следует, что корректно

Определение 18. Систему инвариантов матрицы любого конечного задания абелевой группы G назовем *системой инвариантов группы G* и обозначим через $I(G)$.

Теперь докажем основную теорему о строении конечно определенных абелевых групп.

Теорема 23. *Любая конечно определенная абелева группа G либо является примарной циклической, либо бесконечной циклической, либо разлагается в прямую сумму конечного числа примарных циклических и бесконечных циклических групп, и такое разложение единственно с точностью до изоморфизма слагаемых и порядка их расположения в сумме.*

□ Пусть $I(G) = (m, d_1, \ldots, d_r)$. Из определения 18 и теоремы 22 следует, что группа G имеет задание $(A;\, S \cup K)$, где $A = \{a_1, \ldots, a_{r+m}\}$, $S = \{(d_i a_i, \theta) :\ i \in \overline{1,r}\}$. Отсюда и из теоремы 6 (с учетом примеров 4, 5) получим:

$$G = G_1 \oplus \ldots \oplus G_r \oplus H_1 \oplus \ldots \oplus H_m, \tag{20}$$

где $G_i = \langle a_i;\, (d_i a_i, \theta)\rangle$ — циклическая группа порядка d_i, $i \in \overline{1,r}$, и $H_j = \langle a_j;\, \varnothing\rangle$ — бесконечная циклическая группа, $j \in \overline{1,m}$. Разложив в (20) каждую из непримарных групп G_i в прямую сумму примарных циклических подгрупп (это можно сделать в силу теоремы 18 главы 11), мы и получим искомое разложение группы G.

Для доказательства единственности рассмотрим произвольное разложение группы G в прямую сумму примарных циклических и бесконечных циклических групп. С точностью до изоморфизма слагаемых и порядка их расположения такое разложение можно записать в виде

$$G \cong \mathbb{Z}/p_1^{k_{11}} \oplus \ldots \oplus \mathbb{Z}/p_1^{k_{1n_1}} \oplus \ldots \oplus \mathbb{Z}/p_v^{k_{v1}} \oplus \ldots \oplus \mathbb{Z}/p_v^{k_{vn_v}} \oplus \underbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{m'}, \tag{21}$$

где $p_1, \ldots, p_v$ — простые числа, $p_1 < \ldots < p_v$, $k_{ij} \in \mathbb{N}$,

$$1 \leqslant k_{i1} \leqslant \ldots \leqslant k_{in_i}, \quad i \in \overline{1,v}, \quad j \in \overline{1,n_i}, \quad m' \in \mathbb{N}_0.$$

По разложению (21) построим последовательность групп $\widetilde{G}_1, \widetilde{G}_2, \ldots, \widetilde{G}_{r_1}$, где $\widetilde{G}_1$ — прямая сумма примарных слагаемых из (21), взятых по одному слагаемому максимального порядка для каждого из чисел p_i, $i \in \overline{1,v}$, $\widetilde{G}_2$ строится аналогичным образом по прямой сумме остальных примарных слагаемых из (21), и т. д. до исчерпания всех примарных слагаемых из разложения (21). Так как $\widetilde{G}_i$ — прямая сумма циклических групп попарно взаимно простых порядков, то $\widetilde{G}_i$ — циклическая группа, и мы наряду с (20) имеем еще одно разложение группы G в прямую сумму циклических групп:

$$G \cong \widetilde{G}_1 \oplus \ldots \oplus \widetilde{G}_{r_1} \oplus \underbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{m'}.$$

Если $|\widetilde{G}_i| = \widetilde{d}_i$ для $i = 1, \ldots, r_1$, то по теореме 6 группа $\widetilde{G}$ имеет задание $\langle B;\, T \cup K\rangle$, где $B = \{b_1, \ldots, b_{r_1+m'}\}$, $T = \{(\widetilde{d}_i b_i,\, \theta) :\ i \in \overline{1,r_1}\}$.

Так как из построения групп $\widetilde{G}_i$ видно, что $\widetilde{d}_i \mid \widetilde{d}_{i-1}$, $i \in \overline{2,r_1}$, то имеем $I(G) = (m', \widetilde{d}_{r_1}, \ldots, \widetilde{d}_1)$. Заметим, что если бы в разложении группы G отсутствовали примарные слагаемые, то мы бы имели $I(G) = (m')$. Таким образом, во всех случаях число бесконечных слагаемых в интересующих нас разложениях группы G равно первому числу в наборе $I(G)$, а набор порядков всех примарных слагаемых однозначно определяется каноническими разложениями остальных чисел набора $I(G)$. □

Определение 19. Разложение вида (21) абелевой группы G называется ее *каноническим разложением*, а соответствующий ему набор чисел $(m', p_1^{k_{11}}, \ldots, p_1^{k_{1n_1}}, \ldots$ $\ldots, p_v^{k_{1v}}, \ldots, p_v^{k_{vn_v}})$ — *типом группы* G.

Из теоремы 23 следует, что конечно определенная абелева группа определяется с точностью до изоморфизма своим типом.

Замечание 1. В частном случае, когда группа G конечна, из теоремы 23 получаются теоремы 1 и 5 главы 12 о строении конечных абелевых групп.

Теорема 23 помогает решать самые разные вопросы о свойствах абелевых групп. В частности, из нее вытекает следующий результат, являющийся обращением теоремы Лагранжа для конечных абелевых групп (см. следствие 1 теоремы 11 главы 11).

Утверждение 24. *Для любого делителя d порядка конечной абелевой группы G в G существует подгруппа порядка d.*

Среди конечно определенных абелевых групп особый интерес представляют группы, у которых в каноническом разложении отсутствуют бесконечные или примарные слагаемые. В первом случае это суть конечные абелевы группы, во втором — так называемые свободные абелевы группы.

Определение 20. Группа G называется *свободной абелевой группой*, если она имеет задание $(A;\, K)$, где, как и выше, $K = \{(a_i + a_j, a_j + a_i) \colon a_i, a_j \in A\}$. При этом, если $(A;\, K)$ есть задание группы G относительно ее системы образующих G_1, то G_1 называется *свободной системой образующих абелевой группы G*.

В частности, группа $\langle A;\, K\rangle$ является свободной абелевой группой со свободной системой образующих $\{[a_i]_K \colon a_i \in A\}$.

Непосредственно из теоремы 22 следует

Утверждение 25. *Любые две конечные свободные системы образующих абелевой группы G равномощны.*

Следовательно, корректно

Определение 21. Число элементов в любой свободной системе образующих конечно порожденной свободной абелевой группы G называют *рангом группы G*.

Из доказательства теоремы 23 легко получить полное описание всех свободных абелевых групп конечных рангов.

Утверждение 26. *Группа G является свободной абелевой группой ранга n тогда и только тогда, когда она является прямой суммой n бесконечных циклических групп, и, в частности, когда* $G \cong \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{n}$.

Замечание 2. Не следует путать понятие свободной абелевой группы с определенным ранее (см. определение 3) понятием свободной группы. Свободная группа $F_n = \langle a_1, \ldots, a_n;\, \varnothing\rangle$ является абелевой только при $n = 1$. Действительно, как следует из утверждения 11 и его доказательства, гомоморфным образом группы F_2 является любая группа с двумя образующими, среди которых есть и неабелевы (например, группа диэдра D_n при $n > 2$).

Для абелевых групп имеет место аналог утверждения 11: любая абелева группа изоморфна факторгруппе подходящей свободной абелевой группы. Точнее, справедлива

Теорема 27. *Если $G = \langle A; S \cup K\rangle$ — абелева группа, где $A = \{a_1, \ldots, a_n\}$, $S = \{(P_j, \theta) : j \in \overline{1,m}\}$, то G изоморфна факторгруппе группы $\langle A; K\rangle$ по ее подгруппе H, порожденной системой элементов $\{[P_j]_K : j \in \overline{1,m}\}$. При этом изоморфизмом может служить отображение φ, определенное равенствами*

$$\forall\, P \in W(\overline{A}) :\ \varphi([P]_K + H) = [P]_{S\cup K}.$$

□ Доказывается теорема точно так же, как теорема 5 при $S_1 = K$, $S_2 = S \cup K$. Следует лишь учесть, что в абелевой группе любая подгруппа является нормальным делителем. □

Заметим, что свободная абелева группа может быть задана и несвободной системой образующих. Так, например, свободная абелева группа $\mathbb{Z}$ ранга 1 порождается числами 1, 2 и имеет относительно системы образующих $\{1, 2\}$ задание $\langle a_1, a_2; (2a_1,\, a_2)\rangle$. В связи с этим представляет интерес

Теорема 28. *Для любой системы образующих $G_1 = \{g_1, \ldots, g_n\}$ абелевой группы G эквивалентны утверждения*:

(а) *G_1 — свободная система образующих абелевой группы G*;

(б) *соотношение*

$$c_1 g_1 + \ldots + c_n g_n = 0, \tag{22}$$

где $c_1, \ldots, c_n \in \mathbb{Z}$, выполняется в G лишь при $c_1 = \ldots = c_n = 0$.

□ Пусть выполняется условие (а). Тогда из определений 20 и 12 имеем: существует изоморфизм φ группы $F = \langle a_1, \ldots, a_n; K\rangle$ на G, при котором $\varphi([a_i]_K) = g_i$, $i \in \overline{1,n}$. Следовательно, если в G выполнено равенство (22), то в F верно равенство $c_1[a_1]_K + \ldots + c_n[a_n]_K = [\theta]_K$, т. е. соотношение $s = (c_1 a_1 \ldots c_n a_n,\, \theta)$ является следствием системы K, и $F = \langle a_1, \ldots, a_n; K \cup \{s\}\rangle$ (в силу утверждения 2). Тогда по теореме 22 для $A = \{a_1, \ldots, a_n\}$:

$$I(C_{A,\varnothing}) = I(C_{A,\{s\}}). \tag{23}$$

А так как $C_{A,\varnothing} = O$, то равенство (23) возможно лишь в одном случае, когда $c_1 = \ldots = c_n = 0$, и утверждение (б) доказано.

Пусть теперь выполнено условие (б). Так как G_1 порождает G, то в силу теоремы 8 и определения 12 существуют абстрактная группа $F = \langle a_1, \ldots, a_n; S\rangle$ и изоморфизм $\varphi\colon F \to G$, при котором $\varphi([a_i]_S) = g_i$, $i \in \overline{1,n}$. Так как группа G абелева, то F тоже абелева. Следовательно, $F = \langle a_1, \ldots, a_n; S \cup K\rangle$, и, не теряя общности, можно считать, что система S или пуста, или состоит из соотношений вида $(\varepsilon_1 a_1 \ldots \varepsilon_n a_n, \theta)$ при $(\varepsilon_1, \ldots, \varepsilon_n) \neq (0, \ldots, 0)$. Отсюда и из условия (б) следует, что $S = \varnothing$, и потому G_1 — свободная система образующих абелевой группы G (см. определение 20). □

§ 5. О ШИРИНЕ И ДЛИНЕ КОНЕЧНОЙ ГРУППЫ ОТНОСИТЕЛЬНО ЗАДАННОЙ СИСТЕМЫ ОБРАЗУЮЩИХ

Рассмотрим несколько понятий, связанных с порождением конечной группы G некоторой ее системой образующих $G_1 = \{g_1, \dots, g_n\}$.

Определение 22. *Слоем группы G в системе образующих G_1* назовем любое из ее подмножеств вида G_1^k, $k \in \mathbb{N}_0$.

Так как группа G конечна, то $g_i^{-1} = g_i^{\operatorname{ord} g_i - 1}$, и потому каждый элемент группы G представим в виде произведения элементов из G_1. В связи с этим корректно

Определение 23. *Длиной группы G* относительно системы образующих G_1 называется минимальное натуральное число l, при котором выполняется равенство

$$G = \bigcup_{k=1}^{l} G_1^k.$$

Определение 24. *Шириной группы G* относительно системы образующих G_1 называется минимальное число слоев в системе образующих G_1, которыми может быть исчерпана группа G.

Длину и ширину группы G относительно системы образующих G_1 обозначим соответственно через $l(G; G_1)$, $d(G; G_1)$.

Параметр $d(G; G_1)$ легко определить по системе определяющих соотношений группы G в системе образующих G_1. Так как G конечна, то любую ее систему определяющих соотношений S_1 можно преобразовать в систему определяющих соотношений вида:

$$S = \{g_{i1} \dots g_{it_i} = e : \ i \in \overline{1, m}, \ t_i \in \mathbb{N}, \ g_{ij} \in G_1\}. \tag{24}$$

Для этого достаточно заменить каждое соотношение из S_1 приведенным соотношением, добавить к полученной системе все соотношения $g_i^{\operatorname{ord} g_i} = e$, $i \in \overline{1, n}$, и заменить в остальных соотношениях элементы g_i^{-1} на $g_i^{\operatorname{ord} g_i - 1}$.

Определение 25. Систему определяющих соотношений вида (24) группы G назовем *приведенной системой определяющих соотношений в алфавите G_1*, а левые части всех соотношений из (24) — *определяющими словами* этой системы.

Теорема 29. *Ширина конечной группы G относительно системы образующих G_1 равна наибольшему общему делителю длин определяющих слов любой приведенной системы S определяющих соотношений группы G в алфавите G_1.*

□ Пусть $G_1 = \{g_1, \dots g_n\}$ и S есть система (24). Обозначим $d_1 = d(G; G_1)$, $d_2 = (t_1, \dots, t_m)$, и докажем, что $d_1 = d_2$. Если в группе G между элементами из G_1 выполняется соотношение

$$g_{j_1} g_{j_2} \dots g_{j_k} = g_{r_1} g_{r_2} \dots g_{r_l},$$

то от его левой части к правой можно перейти, используя лишь соотношения из S и тривиальные соотношения вида $g_i^{\varepsilon} g_i^{-\varepsilon} = e$, $\varepsilon \in \{1, -1\}$. Отсюда следует, что $k \equiv l \,(\mathrm{mod}\, d_2)$, и если $k \not\equiv l \,(\mathrm{mod}\, d_2)$, то $G_1^k \cap G_1^l = \varnothing$. Значит, среди слоев, покрывающих группу G, должны обязательно присутствовать слои $G_1^{r_1}, \ldots, G_1^{r_{d_2}}$, где $r_1, \ldots, r_{d_2}$ образуют полную систему вычетов по модулю d_2. Следовательно, $d_1 \geqslant d_2$.

Докажем неравенство $d_1 \leqslant d_2$. Так как $|G| < \infty$ и $|G_1^k| \leqslant |G_1^{k+1}|$ при любом $k \in \mathbb{N}_0$, то найдется такое $k_0 \in \mathbb{N}$, что $|G_1^{k_0}| = |G_1^{k_0+1}|$. А так как

$$G_1^{k_0+1} = \bigcup_{i=1}^{n} G_1^{k_0} g_i = \bigcup_{i=1}^{n} g_i G_i^{k_0},$$

то имеем:

$$G_1^{k_0+1} = g_i G_1^{k_0} = G_1^{k_0} g_i, \quad i \in \overline{1,n}. \tag{25}$$

Теперь индукцией по l нетрудно доказать, что для любых $k \geqslant k_0$, $l \in \mathbb{N}_0$, $g \in G_1^l$ выполняются равенства

$$G_1^{k+l} = G_1^k g = g G_1^k. \tag{26}$$

При $l = 0$ они очевидны. Допустим, что они верны для $l = l_0$, и докажем их для $l = l_0 + 1$. Используя равенства (25) и равенства (26) при $l = l_0$, $k = k_0 + r$, мы для любого элемента $g = g_{j_1} \ldots g_{j_{l_0+1}} \in G_1^{l_0+1}$ получим:

$$\begin{aligned} G_1^{k+l_0+1} &= G_1^{k_0+1} \cdot G_1^{r+l_0} = g_{j_1} G_1^{k_0} \cdot G_1^{r+l_0} = \\ &= g_{j_1} G_1^{k+l_0} = g_{j_1} (g_{j_2} \ldots g_{j_{l_0+1}}) G_1^k = g G_1^k. \end{aligned}$$

Аналогично доказывается равенство $G_1^{k+l_0+1} = G_1^k g$.

Так как соотношения из S выполняются в G, то $e \in G_1^{t_i}$, $i \in \overline{1,m}$. Поэтому из (26) при $g = e$ получаем: $G_1^{k+t_i} = G_1^k$ при любых $k \geqslant k_0$, $i \in \overline{1,n}$. Это означает, что последовательность

$$G_1^0,\ G_1^1,\ G_1^2,\ \ldots \tag{27}$$

является периодической, и любое из чисел $t_1, \ldots, t_m$ является ее периодом. Следовательно, наименьший период τ последовательности (27) делит каждое из чисел $t_1, \ldots, t_m$, а потому и их НОД d_2. Однако легко видеть, что период τ совпадает с шириной группы G, и мы имеем $d_1 \mid d_2$, а значит, и $d_1 \leqslant d_2$. В итоге имеем: $d_1 = d_2$. $\square$

Из доказательства теоремы 29 легко получить

Следствие. *Ширина конечной группы G относительно системы образующих G_1 совпадает с индексом минимального нормального делителя группы G, по которому G_1 содержится в одном смежном классе.*

$\square$ Выберем число $s \geqslant k_0$ такое, что $e \in G_1^s$. Тогда из (26) имеем $G_1^s \cdot G_1^s = G_1^{s+s} = G_1^s$, а также $G_1^s g = g G_1^s$ для любого $g \in G$ и $G_1^{s+1} = G_1^s \cdot G_1 = G_1^s g_i$ для любого $g_i \in G_1$. Отсюда видно, что $G_1^s \lhd G$, и G_1 содержится в смежном классе $G^s g_i$. Допустим, что существует нормальный делитель H группы G такой, что $H \subset G_1^s$ и $G_1 \subset H g_i$, $i \in \overline{1,n}$. Тогда $G_1^s \subset (H g_i)^s = H g_i^s$. Отсюда и из условия $e \in G_1^s$ следует, что $H g_i^s = H$, и потому $G_1^s \leqslant H$. В итоге $H = G_1^s$, т. е. G_1^s есть минимальный нормальный делитель со свойством $G_1 \subset G_1^s g_i$, $i \in \overline{1,n}$. $\square$

Пример 7. Найти ширину группы диэдра D_n относительно системы образующих $G_1 = \{g_1, g_2\}$, указанной в примере 1.

Из примера 5 видно, что D_n задается следующей приведенной системой определяющих соотношений в алфавите G_1:

$$g_1^n = e, \quad g_2^2 = e, \quad g_1 g_2 g_1 g_2 = e.$$

Следовательно,

$$d(D_n;\, G_1) = (n, 2, 4) = \begin{cases} 1, & \text{если } n \text{ нечетно,} \\ 2, & \text{если } n \text{ четно.} \end{cases}$$

Пример 8. Найти ширину группы S_n относительно системы образующих $G_1 = \{(1, i) :\ i \in \overline{2, n}\}$.

Для решения этой задачи воспользуемся следствием из теоремы 29. При $n \neq 4$ неединичными нормальными делителями группы S_n являются лишь сама группа S_n и знакопеременная группа A_n. А так как все постановки из G_1 нечетны, то они лежат в одном смежном классе по подгруппе A_n. Следовательно, в этом случае $d(S_n;\, G_1) = |S_n : A_n| = 2$. В группе S_4, кроме S_4 и A_4, есть еще неединичный нормальный делитель K_4 — группа Клейна. Однако нетрудно проверить, что G_1 не лежит в одном смежном классе группы S_4 по K_4. Поэтому и в этом случае ширина группы равна 2.

Заметим, что задача нахождения длины группы относительно заданной системы образующих решается, как правило, сложнее, чем задача нахождения ширины группы. Однако и при нахождении длины группы в некоторых случаях помогает знание системы определяющих соотношений.

Пример 9. Найти длину группы S_n относительно системы образующих $G_n = \{g_1, \ldots, g_{n-1}\}$, $g_i = (i,\, i+1)$, $i \in \overline{1, n-1}$.

Воспользуемся заданием $\langle B_n;\, T_n\rangle$ группы S_n относительно системы образующих G_n, указанным в теореме 10. В ходе доказательства теоремы 10 было, в частности, установлено, что любое слово в алфавите B_n можно с помощью соотношений из T_n преобразовать к слову вида (12). При этом указанная при доказательстве этого факта последовательность элементарных преобразований состоит из преобразований, не увеличивающих длину слова. Следовательно, число вида (12) является самым коротким словом среди всех T_n-эквивалентных ему слов в алфавите B_n. Теперь заметим, что самое длинное слово вида (12)

$$b_1 b_2 b_1 b_3 b_2 b_1 \ldots b_{n-1} \ldots b_2 b_1$$

имеет длину $n(n-1)/2$. Следовательно, длина группы $H_n = \langle B_n;\, T_n\rangle$ относительно системы образующих $\widetilde{B}_n = \{[b_i]_{T_n} :\ i \in \overline{1,\, n-1}\}$ равна $n(n-1)/2$. А так как $H_n \cong S_n$, и существует изоморфизм $\varphi\colon H_n \to S_n$, отображающий $[b_i]_{T_n}$ в g_i, $i \in \overline{1,\, n-1}$, то

$$l(S_n;\, G_n) = \frac{n(n-1)}{2}.$$

ЗАДАЧИ

1. Докажите, что для любых слов P, Q, $R \in W(\overline{A})$ и для любой системы соотношений S в алфавите $\overline{A}$:

$$PQ \underset{S}{\sim} PR \;\Leftrightarrow\; Q \underset{S}{\sim} R.$$

2. Пусть $G = \langle A; S\rangle$, где $A = \{a, b, c\}$, $S = \{(ab, ba), (ac, ca), (bc, c^{-1}b)\}$.

а) Докажите, что каждое слово в алфавите $\overline{A}$ S-эквивалентно слову вида $a^k b^l c^m$, где $k, l, m \in \mathbb{Z}$.

б) Является ли группа G коммутативной?

в) Является ли группа G конечной?

г) Разложима ли группа G в прямое произведение подгрупп?

д) Какую подгруппу порождает в ней каждый из элементов $[a]_S, [b]_S$?

3. Отображение $\rho\colon W(\overline{A}) \to W(\overline{A})$, где $A = \{a_1, \ldots, a_n\}$, определяется индуктивно: $\rho(e) = e$,

$$\rho(Pa_i^{\varepsilon}) = \begin{cases} \rho(P)\, a_i^{\varepsilon}, & \text{если } \rho(P) = a_{i_1}^{\varepsilon_1} \ldots a_{i_k}^{\varepsilon_k},\ a_{i_k}^{\varepsilon_k} \neq a_i^{-\varepsilon}, \\ \rho(a_{i_1}^{\varepsilon_1} \ldots a_{i_{k-1}}^{\varepsilon_{k-1}}), & \text{если } \rho(P) = a_{i_1}^{\varepsilon_1} \ldots a_{i_k}^{\varepsilon_k},\ a_{i_k}^{\varepsilon_k} = a_i^{-\varepsilon}. \end{cases}$$

Докажите, что для любых слов P, $Q \in W(\overline{A})$:

а) $\rho(P)$ несократимо (т. е. не содержит подслов вида $a_i^{\varepsilon} a_i^{-\varepsilon}$);

б) $\rho(P) \underset{\varnothing}{\sim} P$;

в) если P несократимо, то $\rho(P) = P$;

г) $\rho(PQ) = \rho(\rho(P)Q)$;

д) $\rho(Pa_i^{\varepsilon} a_i^{-\varepsilon}) = \rho(P)$;

е) $\rho(Pa_i^{\varepsilon} a_i^{-\varepsilon} Q) = \rho(PQ)$.

4. Докажите, что любое слово $P \in W(\overline{A})$ $\varnothing$-эквивалентно единственному несократимому слову. (*Указание*: воспользоваться результатами задачи 3.)

5. Говорят, что в группе $\langle A; S\rangle$ разрешима *проблема равенства слов*, если существует алгоритм, позволяющий для любых слов P, $Q \in W(\overline{A})$ узнавать, являются они S-эквивалентными или нет. Докажите, что в свободной группе $G = \langle a_1, \ldots, a_n; \varnothing\rangle$ разрешима проблема равенства слов.

6. Докажите, что в конечно порожденной группе G любая система образующих содержит конечную подсистему, порождающую группу G.

7. Докажите, что в свободной группе $G = \langle a_1, a_2; \varnothing\rangle$ подгруппа H, порожденная множеством $G_1 = \{[a^i b^i]_{\varnothing} : i \in \mathbb{N}\}$, не является конечно порожденной.

8. Докажите, что для $r, s, t \in \mathbb{N}$ и $d = (r, t^s - 1)$ выполняется равенство

$$\langle a, b;\ (a^r, e),\ (b^s, e),\ (ab, ba^t)\rangle = \langle a, b;\ (a^d, e),\ (b^s, e),\ (ab, ba^t)\rangle.$$

9. Найдите задание группы $G = \mathbb{Z}/m \oplus \mathbb{Z}/n$.

10. Найдите задания группы A_4 в следующих системах образующих:
а) $A = \{a_1, a_2\}$, где $a_1 = (1,2)(3,4),\ a_2 = (1,2,3)$;
б) $B = \{b_1, b_2\}$, где $b_1 = (1,2,3),\ b_2 = (1,2,4)$.

11. Опишите с точностью до изоморфизма все группы порядка 8 и найдите их задания образующими элементами и определяющими соотношениями.

12. Пусть p — простое число, θ — примитивный элемент поля $\mathbb{Z}_p$. Докажите, что *группа биективных аффинных преобразований* (т. е. преобразований вида $\binom{x}{ax+b}$, $a \neq 0$) поля $\mathbb{Z}_p$ имеет задание

$$\langle g, h;\ (g^p, e),\ (h^{p-1}, e),\ (gh, hg^\theta)\rangle$$

относительно системы образующих $\binom{x}{x+1}$, $\binom{x}{\theta x}$.

13. Докажите, что группа

$$G = \langle a_1, a_2, a_3, \ldots;\ (a_1, a_2^2),\ (a_2, a_3^2),\ \ldots\rangle$$

изоморфна аддитивной группе рациональных чисел вида $\frac{a}{2^k}$, где $a \in \mathbb{Z}$, $k \in \mathbb{N}_0$.

14. Пользуясь преобразованиями Тице, переведите задание $\langle A; (P, Q)\rangle$ в задания: $\langle A; (PQ^{-1}, e)\rangle$, $\langle A; (P^{-1}, Q^{-1})\rangle$.

15. Докажите, что $\langle a, b, c;\ (b^2, e),\ ((bc)^2, e)\rangle \cong \langle x, y, z;\ (y^2, e),\ (z^2, e)\rangle$.

16. Зная задание группы S_4 в системе образующих $A = \{(1,2),\ (2,3),\ (3,4)\}$ (см. теорему 10), найдите ее задания в системах образующих

$$B = \{(1,2),\ (1,2,3,4)\}, \quad C = \{(1,2),\ (1,3),\ (1,4)\}.$$

17. Найдите длину группы диэдра D_n относительно системы образующих $G_1 = \{g_1, g_2\}$ из примера 2.

18. Найдите длину и ширину группы S_n относительно системы всех транспозиций из S_n.

19. Найдите ширину и оцените сверху длину группы S_n относительно системы образующих $g_1 = (1,2),\ g_2 = (1,2,\ldots,n)$ (см. пример 6).

20. Докажите, что группа

$$G = \langle a_1, a_2, a_3;\ (a_1^r, e),\ (a_2^s, e),\ (a_3, a_2^{-1}a_1^{-1}a_2a_1),\ (a_1a_3, a_3a_1),\ (a_2a_3, a_3a_2)\rangle$$

конечна, и оцените ее длину относительно системы образующих $A = \{[a_1],\ [a_2],\ [a_3]\}$.

21. Найдите ширину и длину абелевой группы

$$G = \langle a_1, \ldots, a_n;\ (d_1a_1, \theta),\ \ldots,\ (d_na_n, \theta),\ (a_ia_j, a_ja_i),\ i, j \in \overline{1, n}\,\rangle$$

относительно системы образующих $\{[a_1],\ \ldots,\ [a_n]\}$.

22. Докажите, что любая конечно порожденная абелева группа является конечно определенной.

Глава 24

ГРУППЫ ПОДСТАНОВОК (ДОПОЛНЕНИЕ)

§ 1. ПОДСТАНОВОЧНЫЕ ПРЕДСТАВЛЕНИЯ КОНЕЧНЫХ ГРУПП

Прежде, чем продолжить начатое в главе 11 изучение групп подстановок, укажем на некоторые возможности использования групп подстановок для задания и изучения произвольных групп. Эти возможности основаны на переходе от заданной группы к ее изоморфному или гомоморфному образу в симметрической группе $S(\Omega)$ подстановок некоторого множества Ω.

Определение 1. *Подстановочным представлением* произвольной группы G называют всякий гомоморфизм φ группы G в симметрическую группу подстановок $S(\Omega)$ любого конечного множества Ω. При этом число $|\Omega|$ называют *степенью представления* и обозначают через $\deg\varphi$. Представление φ называют *точным*, если φ — мономорфизм, и *транзитивным*, если группа $\varphi(G)$ транзитивна на Ω.

Заметим, что иногда и гомоморфный образ $\varphi(G)$ группы G при гомоморфизме $\varphi\colon G \to S(\Omega)$ называют подстановочным представлением группы G. Такое двоякое использование одного термина не ведет к путанице, поскольку из контекста обычно бывает видно, о чем идет речь.

Из доказательства теоремы Кэли (см. теорему 22 главы 11) следует, что для любой группы G отображение $\rho\colon G \to S(G)$, сопоставляющее каждому элементу $g \in G$ подстановку $\widehat{g}$ из $S(G)$, определенную формулой

$$\forall\, x \in G:\ \ \widehat{g}(x) = xg, \tag{1}$$

является точным подстановочным представлением группы G. Если подстановку $\widehat{g}$ из (1) условиться обозначать в виде $\binom{x}{xg}$, предполагая, что x пробегает множество G, то можно будет записать

$$\forall\, g \in G:\ \ \rho(g) = \begin{pmatrix} x \\ xg \end{pmatrix}. \tag{2}$$

Нетрудно проверить, что точным подстановочным представлением группы G является также отображение $\rho'\colon G \to S(G)$, определенное формулой

$$\forall\, g \in G:\ \ \rho'(g) = \begin{pmatrix} x \\ g^{-1}x \end{pmatrix} \tag{3}$$

(проделайте проверку в качестве упражнения).

Определение 2. Подстановочные представления ρ и ρ', определенные формулами (2) и (3), называются соответственно *правым* и *левым регулярными представлениями* группы G.

Заметим, что для неабелевой группы G отображение $\rho'' \colon G \to S(G)$, определенное формулой

$$\forall\, g \in G\colon\ \rho''(g) = \begin{pmatrix} x \\ gx \end{pmatrix},$$

не является гомоморфизмом, поскольку

$$\forall\, g_1, g_2 \in G\colon\ \rho''(g_1 g_2) = \rho''(g_2) \cdot \rho''(g_1).$$

Установим связь между группами $\rho(G)$ и $\rho'(G)$.

Определение 3. *Централизатором подмножества* (в частности, подгруппы) H в группе G называют множество $Z_G(H)$ всех элементов группы G, перестановочных с каждым элементом из H. Очевидно, что $Z_G(H)$ есть подгруппа группы G, содержащая центр группы $\langle H \rangle$.

Оказывается, имеет место

Теорема 1. *Централизатор правого регулярного представления группы G в группе $S(G)$ совпадает с левым регулярным представлением группы G.*

□ Пусть $H = Z_{S(G)}(\rho(G))$ и $h \in H$. Тогда при любом $g \in G$ выполняется равенство

$$h \cdot \begin{pmatrix} x \\ xg \end{pmatrix} = \begin{pmatrix} x \\ xg \end{pmatrix} \cdot h. \tag{4}$$

Следовательно, $\forall\, x, g \in G\colon\ h(x) \cdot g = h(xg)$. Отсюда при $x = e$ получаем, что $\forall\, g \in G\colon\ h(g) = h(e) \cdot g$. Значит, $h = \begin{pmatrix} x \\ g_0 x \end{pmatrix}$, где $g_0 = h(e)$, и включение $H \subset \rho'(G)$ доказано. Обратное включение очевидно, поскольку при любых $g_1, g \in G$ подстановка $h = \begin{pmatrix} x \\ g_1 x \end{pmatrix}$ удовлетворяет равенству (4). □

Следствие. *Если G — абелева группа, то $Z_{S(G)}(\rho(G)) = \rho(G)$.*

Так как $\deg \rho = \deg \rho' = |G|$, то практическое использование представлений ρ, ρ' для групп G больших порядков затруднительно. Возникает вопрос о существовании для группы более «экономных» представлений, чем ρ и ρ'. О том, что группа G может иметь точные подстановочные представления степени, меньшей $|G|$, свидетельствует

Пример 1. Полная линейная группа $GL(n, q)$ над полем $P = GF(q)$, наряду с представлениями ρ, ρ' степени $N = |GL(n, q)| = \prod_{i=0}^{n-1}(q^n - q^i)$, имеет точное представление степени q^n — отображение φ, сопоставляющее каждому линейному преобразованию $g \in GL(n, q)$ подстановку

$$\varphi(g) = \begin{pmatrix} x^{\downarrow} \\ g(x^{\downarrow}) \end{pmatrix}$$

пространства $P^{(n)}$.

В общем случае вопрос о нахождении для группы G точных подстановочных представлений наименьшей степени является сложной и нерешенной проблемой.

В теории групп и ее приложениях часто используют подстановочные представления группы G на смежных классах по различным ее подгруппам или на подгруппах сопряженных с заданной подгруппой. Для определения этих представлений сформулируем три вспомогательных утверждения (докажите их самостоятельно).

Утверждение 2. *Если* $\Omega_H = \{Hg_i : i \in I\}$ *есть множество всех правых смежных классов группы* G *по подгруппе* H, *то*

$$\forall\, g \in G:\ \{Hg_ig : i \in I\} = \Omega_H.$$

Утверждение 3. *Если* $\Delta_H = \{g_j^{-1}Hg_j : j \in J\}$ *есть множество всех подгрупп группы* G, *сопряженных с подгруппой* H, *то*

$$\forall\, g \in G:\ \{g^{-1}g_j^{-1}Hg_jg : j \in J\} = \Delta_H.$$

Утверждение 4. *Отображения* φ_H, ψ_H *группы* G *соответственно в группы* $S(\Omega_H)$, $S(\Delta_H)$, *определенные формулами*

$$\forall\, g \in G:\quad \varphi_H(g) = \begin{pmatrix} Hg_i \\ Hg_i \cdot g \end{pmatrix},\quad \psi_H(g) = \begin{pmatrix} g_i^{-1}Hg_i \\ g^{-1}g_i^{-1}Hg_ig \end{pmatrix}, \tag{5}$$

являются гомоморфизмами (*т. е. подстановочными представлениями группы* G).

Определение 4. Отображения φ_H и ψ_H, определенные формулами (5), называются *подстановочными представлениями* группы G соответственно *на правых смежных классах по подгруппе* H и *на подгруппах, сопряженных с подгруппой* H.

Укажем простейшие свойства представлений φ_H и ψ_H.

Утверждение 5. *Пусть* G *— конечная группа и* $\Omega_H = \{Hg_i : i \in I\}$ *— множество всех ее правых смежных классов по подгруппе* H. *Тогда*

(а) $\deg \varphi_H = |G : H|$;

(б) φ_H *транзитивно на* Ω_H;

(в) $\operatorname{Ker} \varphi_H = \bigcap\limits_{x \in G} x^{-1}Hx$;

(г) φ_H *точно* $\Leftrightarrow \bigcap\limits_{x \in G} x^{-1}Hx = \{e\}$;

(д) *если* $H \lhd G$, *то* $\operatorname{Ker} \varphi_H = H$ *и* $\varphi_H(G) \cong G/H$.

□ Утверждения (а) и (б) очевидны, (г) и (д) следуют из (в), и остается доказать утверждение (в). Из определения отображения φ_H имеем:

$$g \in \operatorname{Ker} \varphi_H \ \Leftrightarrow\ \forall\, i \in I:\ Hg_ig = Hg_i \ \Leftrightarrow\ \forall\, i \in I:\ g \in g_i^{-1}Hg_i.$$

Отсюда следует, что $\operatorname{Ker} \varphi_H = \bigcap_{i \in I} g_i^{-1}Hg_i$.

Так как произвольный элемент x из G представляется в виде hg_i где $h \in H$, $i \in I$, то $x^{-1}Hx = g_i^{-1}h^{-1}Hhg_i = g_i^{-1}Hg_i$. Следовательно,

$$\bigcap_{i\in I} g_i^{-1}Hg_i = \bigcap_{x\in G} x^{-1}Hx, \tag{6}$$

и утверждение (в) верно. □

Утверждение 6. *Пусть G — конечная группа и $\Delta_H = \{g_i^{-1}Hg_i : i \in J\}$ — множество всех подгрупп из G, сопряженных с подгруппой H. Тогда*

(а) $\deg \psi_H = |G : N_G(H)|$;

(б) *ψ_H транзитивно на Δ_H*;

(в) $\operatorname{Ker}\psi_H = \bigcap\limits_{x\in G} N_G(x^{-1}Hx)$;

(г) *ψ_H точно* $\Leftrightarrow \bigcap\limits_{x\in G} N_G(x^{-1}Hx) = \{e\}$.

□ Для любых элементов $x, y \in G$ имеем:

$$x^{-1}Hx = y^{-1}Hy \;\Leftrightarrow\; Hxy^{-1} = xy^{-1}H \;\Leftrightarrow\; xy^{-1} \in N_G(H).$$

Значит, число различных подгрупп в G, сопряженных с H, равно числу смежных классов группы G по подгруппе $N_G(H)$, и утверждение (а) доказано. Утверждение (б) следует из разрешимости в G уравнения $g_i x = g_j$. Докажем (в). По определению отображения ψ_H

$$g\in\operatorname{Ker}\psi_H \;\Leftrightarrow\; \forall\, i\in J:\; g^{-1}g_i^{-1}Hg_ig = g_i^{-1}Hg_i \;\Leftrightarrow\; \forall\, i\in J:\; N_G(g_i^{-1}Hg_i)\ni g.$$

Отсюда следует, что $\operatorname{Ker}\psi_H = \bigcap_{i\in J} N_G(g_i^{-1}Hg_i)$. Теперь, используя те же соображения, что и при доказательстве равенства (6), получим утверждение (в). Наконец, заметим, что (г) следует из (в). □

Пример 2. Пусть G — группа подстановок множества $\Omega = \overline{1,n}$, $\Delta = \{i_1, \ldots, i_k\}$ — орбита группы G и $H = G_{i_1}$ — стабилизатор точки i_1. По лемме Бернсайда (см. теорему 25 главы 11) $|G : G_{i_1}| = |\Delta| = k$, т. е. $\deg \varphi_H = k$. Для нахождения ядра представления φ_H заметим, что $x^{-1}G_{i_1}x = G_{x(i_1)}$. Отсюда и из утверждения 5(в) получаем:

$$\operatorname{Ker}\varphi_H = \bigcap_{x\in G} G_{x(i_1)} = G_\Delta,$$

где G_Δ — группа всех подстановок из G, оставляющих на месте каждую точку из Δ. В частности, если $G_\Delta = \{e\}$, то представление φ_H точное.

Определение 5. Группы подстановок G_1, G_2 соответственно множеств Ω_1, Ω_2 называются *подстановочно изоморфными*, если существуют биекции $\psi\colon \Omega_1 \to \Omega_2$, $\varphi\colon G_1 \to G_2$, удовлетворяющие условию

$$\forall\, a \in \Omega_1,\ \forall\, g \in G_1:\ \varphi(g)(\psi(a)) = \psi(g(a)). \tag{7}$$

Используя операцию умножения отображений, условие (7) можно записать в следующем виде:

$$\forall\, g \in G_1 :\ \ \psi \cdot \varphi(g) = g \cdot \psi,$$

или

$$\forall\, g \in G_1 :\ \ \varphi(g) = \psi^{-1} g \psi.$$

Из последней записи условия (7) хорошо видно, что φ — изоморфизм групп: $\varphi(g_1 g_2) = \psi^{-1} g_1 g_2 \psi = \psi^{-1} g_1 \psi \psi^{-1} g_2 \psi = \varphi(g_1)\varphi(g_2)$, что и оправдывает вторую часть термина «подстановочный изоморфизм».

Подстановочно изоморфными группами являются симметрические группы $S(M_1)$, $S(M_2)$ при $|M_1| = |M_2|$ (см. утверждение 15 главы 3). Нетрудно привести также и примеры изоморфных, но не подстановочно изоморфных групп подстановок. В частности, любая группа подстановок G степени n при условии $|G| > n$ не является подстановочно изоморфной своему правому регулярному представлению.

Заметим еще, что условие (7) в более наглядной форме означает:

$$\text{если}\ \ g = \begin{pmatrix} a_1 & \dots & a_n \\ a_{i_1} & \dots & a_{i_n} \end{pmatrix},\ \ \text{то}\ \ \varphi(g) = \begin{pmatrix} \psi(a_1) & \dots & \psi(a_n) \\ \psi(a_{i_1}) & \dots & \psi(a_{i_n}) \end{pmatrix}.$$

Отсюда видно, что подстановочно изоморфные группы по существу отличаются лишь обозначениями подстановок и элементов, на которых действуют подстановки. В связи с этим ясно, что подстановочные представления группы достаточно описывать лишь с точностью до подстановочного изоморфизма образов.

Определение 6. Подстановочные представления φ_1, φ_2 группы G называют *подстановочно эквивалентными*, если группы $\varphi_1(G)$, $\varphi_2(G)$ подстановочно изоморфны. Обозначение: $\varphi_1 \sim \varphi_2$.

Следующая теорема описывает с помощью подгрупп группы G все транзитивные подстановочные представления группы G.

Теорема 7. *Любое транзитивное подстановочное представление конечной группы G подстановочно эквивалентно представлению φ_H группы G на смежных классах по подходящей подгруппе H.*

□ Пусть α — транзитивное представление группы G подстановками множества $\Omega = \overline{1,n}$, и $\alpha(G) = \Gamma < S_n$. Так как Γ транзитивна, то ее разложение в смежные классы по стабилизатору Γ_1 точки 1 можно записать в виде

$$\Gamma = \Gamma_1\gamma_1 \cup \ldots \cup \Gamma_1\gamma_n, \quad \gamma_i(1) = i, \quad i \in \overline{1,n}.$$

Положим $H = \alpha^{-1}(\Gamma_1)$ и выберем в G элементы $g_1, \ldots, g_n$ так, что $\alpha(g_i) = \gamma_i$, $i \in \overline{1,n}$. Следующая цепочка импликаций показывает, что Hg_1, …, Hg_n — разные смежные классы из G:

$$g_i^{-1} g_j \in H \ \Rightarrow\ \alpha(g_i^{-1} g_j) \in \alpha(H) \ \Rightarrow\ \gamma_i^{-1}\gamma_j \in \Gamma_1 \ \Rightarrow\ i = j.$$

Так как $\operatorname{Ker}\alpha = N \subset H$, то по теореме об эпиморфизме групп $\Gamma \cong G/N$, $\Gamma_1 \cong H/N$, и потому $|G:H| = |\Gamma:\Gamma_1|$. В итоге имеем разложение группы G в смежные классы по H: $G = Hg_1 \cup \ldots \cup Hg_n$. Докажем, что $\alpha \sim \varphi_H$. Для этого построим отображения

$$\psi\colon \Omega \to \Omega_H, \quad \varphi\colon \Gamma \to \widehat{G} = \varphi_H(G),$$

положив

$$\forall\, i \in \Omega\colon\ \psi(i) = Hg_i, \qquad \forall\, \gamma \in \Gamma\colon\ \varphi(\gamma) = \begin{pmatrix} Hg_i \\ Hg_i \cdot \alpha^{-1}(\gamma) \end{pmatrix}.$$

Так как $\alpha^{-1}(\gamma) = Ng$ для некоторого $g \in G$, $N \lhd G$ и $N \subset H$, то определение отображения φ корректно, и остается проверить условие (7). По определению отображений φ, ψ имеем:

$$\varphi(\gamma)(\psi(a)) = \varphi(\gamma)(Hg_a) = Hg_a \cdot \alpha^{-1}(\gamma), \quad \psi(\gamma)(a) = Hg_{\gamma(a)}.$$

Покажем, что смежные классы $Hg_a\alpha^{-1}(\gamma)$ и $Hg_{\gamma(a)}$ совпадают, т. е. $g_a\alpha^{-1}(\gamma)g_{\gamma(a)}^{-1} \in H$. Достаточно доказать, что $\alpha(g_a\alpha^{-1}(\gamma)g_{\gamma(a)}^{-1}) \in \alpha(H)$, т. е. $\gamma_a\gamma\gamma_{\gamma(a)}^{-1}(1) = 1$. Последнее равенство проверяется непосредственно:

$$\gamma_a\gamma\gamma_{\gamma(a)}^{-1}(1) = (\gamma\gamma_{\gamma(a)}^{-1})(a) = \gamma_{\gamma(a)}^{-1}(\gamma(a)) = 1. \quad \square$$

§ 2. РЕГУЛЯРНЫЕ ГРУППЫ ПОДСТАНОВОК

Определение 7. Группа подстановок $G < S(\Omega)$ называется *регулярной*, если для любых $a, b \in \Omega$ в G существует единственная подстановка g, удовлетворяющая условию $g(a) = b$.

Следующее утверждение указывает некоторые другие определяющие свойства регулярных групп.

Утверждение 8. *Для любой группы $G < S(\Omega)$ эквивалентны условия*:
(а) *G регулярна*;
(б) *G транзитивна и* $\forall\, a \in \Omega\colon\ |G_a| = 1$;
(в) *G транзитивна и* $|G| = |\Omega|$.

$\square$ Для доказательства утверждения достаточно убедиться в справедливости импликаций (а)⇒(б), (б)⇒(в), (в)⇒(а). Первая из них очевидна, вторая следует непосредственно из леммы Бернсайда, третья легко доказывается методом от противного. $\square$

С алгебраической точки зрения класс регулярных групп содержит все конечные группы, поскольку справедливо

Утверждение 9. *Любая конечная группа G изоморфна регулярной группе подстановок множества G.*

□ Для доказательства этого утверждения достаточно заметить, что правое регулярное представление $\rho(G)$ группы G является регулярной группой подстановок множества G. Действительно, $\rho(G)$ транзитивна в силу разрешимости в G уравнения $g_1 x = g_2$ при любых $g_1, g_2 \in G$, и $|\rho(G)| = |G|$ в силу изоморфизма групп $\rho(G)$ и G. □

Пример 3. Пусть $\Omega = \mathbb{Z}_n = \overline{0, n-1}$, и $+$ — операция сложения в кольце $\mathbb{Z}_n$. Правое регулярное представление G_n группы $(\mathbb{Z}_n; +)$ состоит из подстановок $g_a = \begin{pmatrix} x \\ x+a \end{pmatrix}$, $a \in \Omega$. Группа G_n, как и $(\mathbb{Z}_n; +)$, является циклической группой, она порождается подстановкой

$$(0, 1, \ldots, n-1) = \begin{pmatrix} x \\ x+1 \end{pmatrix}.$$

Пример 4. Пусть $\Omega = \{(a_1, \ldots, a_n) : a_i \in GF(2)\}$ — n-мерное векторное пространство строк над полем $GF(2)$, и $\oplus$ — операция сложения векторов (т. е. покомпонентного сложения по модулю 2). Тогда правое регулярное представление Σ_{2^n} группы $(\Omega; \oplus)$ состоит из подстановок $\sigma_a = \begin{pmatrix} x \\ x \oplus a \end{pmatrix}$, $a \in \Omega$, и является, как и Σ_{2^n}, элементарной абелевой 2-группой. Группа Σ_{2^n} называется также *группой сдвигов* группы $(\Omega; \oplus)$.

Следующее утверждение свидетельствует о том, что правыми регулярными представлениями конечных групп исчерпываются все регулярные группы подстановок.

Утверждение 10. *Любая регулярная группа подстановок $G < S(\Omega)$ совпадает с правым регулярным представлением подходящей группы $(\Omega; *)$.*

□ В G элементы можно занумеровать элементами из Ω, сопоставив элементу $g \in G$ номер $a = g(1)$. Таким образом,

$$\forall\, a \in \Omega :\ \ g_a(1) = a. \tag{8}$$

Определим на множестве Ω операцию $*$, положив для $a, b \in \Omega$:

$$a * b = g_b(a), \tag{9}$$

и покажем, что формула $\forall\, a \in \Omega :\ \ \varphi(g_a) = a$ задает изоморфизм φ группы G на группоид $(\Omega; *)$. Очевидно, что φ биективно. Кроме того, из (8) и (9), имеем: $(g_a g_b)(1) = g_b(g_a(1)) = g_b(a) = a * b$. Следовательно, $g_a g_b = g_{a*b}$, и потому $\varphi(g_a g_b) = a * b = \varphi(g_a) * \varphi(g_b)$. Так как φ — изоморфизм, то по следствию теоремы 13 главы 3 $(\Omega; *)$ — группа, и в силу (9) G — ее правое регулярное представление. □

Замечание 1. Равенство (9) сводит действие подстановки регулярной группы $G < S(\Omega)$ к соответствующей операции $*$ на Ω.

Непосредственно из теоремы 1 получаем

Утверждение 11. *Централизатор любой регулярной группы подстановок $G < S(\Omega)$ в группе $S(\Omega)$ изоморфен G и совпадает с G, если группа G абелева.*

Отметим одно свойство цикловых структур подстановок из регулярных групп.

Утверждение 12. *Пусть G — правое регулярное представление группы $(\Omega;\cdot)$. Тогда подстановка $g = \begin{pmatrix} x \\ xa \end{pmatrix}$ из G разлагается в произведение $|\Omega|/l$ независимых циклов длины l, где $l = \operatorname{ord} a$.*

□ Из алгоритма разложения подстановки g в произведение независимых циклов (см. § 8 главы 11) следует, что длина цикла, содержащего элемент x_0, есть наименьшее натуральное число l, удовлетворяющее условию $g^l(x_0) = x_0$, или, в нашем случае, $x_0 \cdot a^l = x_0$, что равносильно условию $l = \operatorname{ord} a$. □

§ 3. КРАТНО ТРАНЗИТИВНЫЕ ГРУППЫ ПОДСТАНОВОК

Определение 8. Группа подстановок $G < S(\Omega)$, где $|\Omega| \geqslant k$, называется *k-транзитивной* (*точно k-транзитивной*), если для любых двух наборов $\alpha = (a_1, \ldots, a_k)$, $\beta = (b_1, \ldots, b_k)$ по k различных букв из множества Ω в G существует подстановка (единственная подстановка) g, переводящая α в β, т. е. удовлетворяющая условию $g(a_i) = b_i$, $i \in \overline{1,k}$, или, короче, $g(\alpha) = \beta$.

Из определения 8 видно, что классы 1-транзитивных и точно 1-транзитивных групп совпадают соответственно с классами транзитивных и регулярных групп подстановок. Группы, k-транзитивные при $k > 1$, называют *кратно транзитивными*. Простейшими примерами кратно транзитивных групп являются симметрическая группа подстановок S_n при $n > 1$ и знакопеременная группа A_n при $n > 2$. Очевидно, что группа S_n точно n-транзитивна. Группа A_n при $n > 2$ точно $(n-2)$-транзитивна. Действительно, для наборов $\alpha = (a_1, \ldots, a_{n-2})$, $\beta = (b_1, \ldots, b_{n-2})$ в S_n существуют ровно две подстановки, переводящие α в β, и эти подстановки имеют разную четность. Следовательно, ровно одна из них содержится в группе A_n.

Перед тем, как рассмотреть другие примеры, приведем критерии k-транзитивности и точной k-транзитивности.

Теорема 13. *Группа подстановок $G < S(\Omega)$ (точно) k-транзитивна тогда и только тогда, когда* 1) *G транзитивна,* 2) *стабилизатор G_a группы G хотя бы для одной точки $a \in \Omega$ (точно) $(k-1)$-транзитивен как группа подстановок на множестве $\Omega \setminus \{a\}$.*

□ Если группа G (точно) k-транзитивна, то условия 1)–2) проверяются очевидным образом. Обратно, пусть для группы G выполнены условия 1)–2) и $\alpha = (a_1, \ldots, a_k)$, $\beta = (b_1, \ldots, b_k)$ — любые наборы по k различных букв из Ω. По условию 1) в группе G найдутся подстановки g_1, g_2 такие, что $g_1(a_1) = a$, $g_2(b_1) = a$. Пусть при этом $g_1(\alpha) = (a, a'_2, \ldots, a'_k)$, $g_2(\beta) = (a, b'_2, \ldots, b'_k)$. По условию 2) в G_a найдется подстановка g_3 такая, что $g_3(a'_2, \ldots, a'_k) = (b'_2, \ldots, b'_k)$. Легко видеть, что подстановка $g_1 g_3 g_2$ переводит α в β, и потому G является k-транзитивной.

Докажем теперь, что G точно k-транзитивна, если группа G_a точно $(k-1)$-транзитивна. Допустим, что G не является точно k-транзитивной. Используя введенные обозначения, можно считать, что в G существуют две разные подстановки g_4, g_5, переводящие набор α в β. Тогда $g_1^{-1}g_4g_2$, $g_1^{-1}g_5g_2$ являются различными подстановками группы G_a, переводящими набор $(a'_2, \ldots, a'_k)$ в $(b'_2, \ldots, b'_k)$, что противоречит точной $(k-1)$-транзитивности группы G_a. □

Утверждение 14. *Пусть G — k-транзитивная группа подстановок степени n. Тогда*

(а) *порядок группы G кратен числу $n(n-1)\ldots(n-k+1)$;*

(б) $|G| = n(n-1)\ldots(n-k+1) \Leftrightarrow$ *G точно k-транзитивна.*

□ Утверждение (а) следует из равенства

$$|G| = n(n-1)\ldots(n-k+1)\,|G_{a_1,\ldots,a_k}|, \tag{10}$$

которое получается последовательным применением леммы Бернсайда к группам G, G_{a_1}, …, $G_{a_1,\ldots,a_{k-1}}$. Утверждение (б) легко доказывается индукцией по k с использованием утверждения 8, леммы Бернсайда и теоремы 13. □

Из утверждения 14(б) и равенства (10) получаем

Следствие. *Группа подстановок $G < S(\Omega)$ точно k-транзитивна тогда и только тогда, когда она k-транзитивна и $|G_{a_1,\ldots,a_k}| = 1$ для любых различных $a_1, \ldots, a_k \in \Omega$.*

Рассмотрим теперь ряд практически интересных примеров кратно транзитивных групп.

Пример 5. Пусть $G = AGL(n,q)$ — *полная аффинная группа* преобразований пространства P^n над полем $P = GF(q)$. Напомним, что она состоит из всех подстановок

$$A_{\psi,\alpha} = \begin{pmatrix} x \\ \psi(x) + \alpha \end{pmatrix},$$

где ψ — любое невырожденное линейное преобразование пространства P^n, а α — любой вектор из P^n.

Группа G транзитивна, так как любой вектор γ в любой вектор δ можно перевести подстановкой $A_{\psi,\alpha}$ при $\psi = \varepsilon$, $\alpha = \delta - \gamma$. Стабилизатором нулевого вектора θ в группе G является, очевидно, полная линейная группа $GL(n,q)$. Она, как группа подстановок на множестве $P^n \setminus \{\theta\}$, транзитивна. Действительно, если α_1, β_1 — любые ненулевые векторы, то по теореме 8 главы 13 их можно дополнить до базисов $(\alpha_1, \alpha_2, \ldots, \alpha_n)$, $(\beta_1, \beta_2, \ldots, \beta_n)$ пространства P^n. Теперь осталось заметить, что любой один базис пространства P^n в любой другой базис можно перевести с помощью обратимого линейного преобразования пространства P^n. Итак, группы G и G_θ транзитивны. Тогда по теореме 13 группа $G = AGL(n,q)$ 2-транзитивна и точно 2-транзитивна при $n = 1$.

Если $P = GF(2)$ и $n > 1$, то любая система из двух различных ненулевых векторов α_1, α_2 линейно независима. Следовательно, в этом случае точно

так же можно доказать, что группа $GL(n,2)$, как группа подстановок множества $P^n\setminus\{\theta\}$, 2-транзитивна, а потому группа $AGL(n,2)$ 3-транзитивна. Покажите, что при $P\neq GF(2)$ и $n>1$ аналогичные утверждения неверны.

Пример 6. Полная аффинная группа $AGL(1,\mathbb{Z}_m)$, состоящая из подстановок вида

$$F_{a,b}=\begin{pmatrix} x \\ ax+b \end{pmatrix},\quad a,b\in\mathbb{Z}_m,\quad (a,m)=1,$$

транзитивна на множестве $\mathbb{Z}_m$, поскольку для любых $c,d\in\mathbb{Z}_m$ элемент c переводится в d подстановкой $F_{1,d-c}$. Так как $|AGL(1,\mathbb{Z}_m)|=m\varphi(m)$, где φ — функция Эйлера, то из утверждения 14 следует, что группа $AGL(1,\mathbb{Z}_m)$ не может быть 2-транзитивной, если $\varphi(m)\neq m-1$, т. е. если m — не простое число. Если же m — простое число, то группа $AGL(1,\mathbb{Z}_m)$ точно 2-транзитивна, поскольку в ней стабилизатор нуля H_m состоит из подстановок вида $\left(\begin{smallmatrix} x \\ ax \end{smallmatrix}\right)$, $a\in\mathbb{Z}_m^*$, и может рассматриваться как регулярная группа подстановок множества $\mathbb{Z}_m^*$.

Заметим еще, что множество G_m всех преобразований вида $\left(\begin{smallmatrix} x \\ x+b \end{smallmatrix}\right)$, $b\in\mathbb{Z}_m$, образует подгруппу (и даже нормальный делитель) группы $AGL(1,\mathbb{Z}_m)$, и $AGL(1,\mathbb{Z}_m)=G_mH_m$.

Пример 7. Пусть $\Omega=P\cup\{\infty\}$, где P — любое поле, и $\infty\notin P$. Каждой невырожденной матрице $A=\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ поставим в соответствие преобразование $g_A\colon\Omega\to\Omega$, определяемое по правилу:

$$g_A(\alpha)=\begin{cases} \dfrac{a\alpha+b}{c\alpha+d}, & \text{если } \alpha\in P,\quad c\alpha+d\neq 0,\\ \infty, & \text{если } \alpha\in P,\quad c\alpha+d=0,\ \text{или}\\ & \qquad \alpha=\infty,\ c=0,\\ \dfrac{a}{c}, & \text{если } \alpha=\infty,\ c\neq 0. \end{cases} \tag{11}$$

Преобразование g_A будем обозначать в виде

$$g_A=\begin{pmatrix} x \\ \frac{ax+b}{cx+d} \end{pmatrix}.$$

Легко проверить, что g_A — подстановка множества Ω, и множество

$$G=\{g_A:\ A\in P_{2,2}^*\}$$

является группой. Она называется *группой дробно-линейных преобразований* поля P.

Из (11) видно, что $g_A(\alpha)$ при любом фиксированном $\alpha\in\Omega$ и подходящих $a,b,c,d\in P$ может принимать любое значение из Ω. Следовательно, G транзитивна. Стабилизатор G_∞ точки ∞ в группе G состоит из всех подстановок вида $\left(\begin{smallmatrix} x \\ ax+b \end{smallmatrix}\right)$,

$a \in P^*$, $b \in P$, и является точно 2-транзитивным (см. пример 5 при $n = 1$). Отсюда на основании теоремы 13 имеем: группа G точно 3-транзитивна. По утверждению 14 ее порядок при $P = GF(q)$ равен

$$(q+1)q(q-1) = q(q^2-1).$$

Заметим, что рассмотренные в примере 7 группы входят в серию так называемых *проективных линейных групп*. В общем случае проективная линейная группа $PGL(n,q)$ степени n над полем $P = GF(q)$ определяется как группа подстановок множества $\Omega_n(q)$ одномерных подпространств пространства P^n, индуцируемых линейными преобразованиями пространства P^n. При $n = 2$ группа $PGL(n,q)$ подстановочно изоморфна группе дробно-линейных преобразований поля P из примера 7. При этом биекции ψ и φ из определения подстановочно изоморфных групп (см. определение 5) можно задать следующим образом: ψ переводит любой элемент a из P в пространство $((a,1))_P$ и ∞ — в $((1,0))_P$; φ сопоставляет преобразованию g_A множества $P \cup \{\infty\}$ подстановку множества $\Omega_n(q)$, индуцируемую линейным преобразованием с матрицей A в стандартном базисе $e_1 = (1,0)$, $e_2 = (0,1)$ пространства P^2.

Докажите последнее утверждение в качестве упражнения.

В заключение данного параграфа отметим, что вопрос о построении k-транзитивных групп подстановок, отличных от симметрических и знакопеременных групп, при больших значениях k является в целом нерешенным. К настоящему времени известны лишь две 4-транзитивные группы (степеней 11 и 23) и две 5-транзитивные группы (степеней 12 и 24). Они были найдены французским математиком Э. Л. Матье (1835–1890) и носят его имя. Примеров k-транзитивных групп, отличных от A_n и S_n, при $k \geqslant 6$ не найдено. В 1873 г. К. Жорданом доказано, что при $k \geqslant 6$ точно k-транзитивных групп, отличных от A_n и S_n, не существует, а при $k = 4, 5$ единственными такими группами являются указанные выше группы Матье степеней 11, 12.

§ 4. ПРИМИТИВНЫЕ И ИМПРИМИТИВНЫЕ ГРУППЫ ПОДСТАНОВОК

Определение 9. Подмножество $\Omega_1 \subset \Omega$ называется *блоком* группы $G < S(\Omega)$, если $\Omega_1 \neq \varnothing$ и

$$\forall\, g \in G\colon \quad (g(\Omega_1) = \Omega_1 \quad \text{или} \quad g(\Omega_1) \cap \Omega_1 = \varnothing).$$

Примерами блоков любой группы $G < S(\Omega)$ являются само множество Ω и все его одноэлементные подмножества. Эти блоки называются *тривиальными*. Легко видеть, что в интранзитивной группе G любая орбита является блоком.

Заметим еще, что если Ω_1 — блок группы G и $g \in G$, то $g(\Omega_1)$ — тоже блок группы G.

В зависимости от наличия или отсутствия нетривиальных блоков все транзитивные группы делятся на два класса.

Определение 10. Транзитивная группа подстановок G называется *примитивной*, если она не имеет нетривиальных блоков и *импримитивной* в противном случае.

Пример 8. Пусть G — подгруппа из S_6, порожденная подстановкой $g = (1,2,3,4,5,6)$. Легко проверить, что она имеет следующие нетривиальные блоки:

$$\Omega_1 = \{1,3,5\}, \quad \Omega_2 = \{2,4,6\}, \quad \Omega_3 = \{1,4\}, \quad \Omega_4 = \{2,5\}, \quad \Omega_5 = \{3,6\}.$$

Так как G транзитивна, то по определению 10 она импримитивна.

В примере 8 длины всех блоков группы G являются делителем числа 6, т. е. степени подстановок. Оказывается, этот факт не случаен. Однако прежде, чем доказать его в общем случае, дадим

Определение 11. Система блоков $\Omega_1, \ldots, \Omega_k$ импримитивной группы $G < S(\Omega)$ называется *полной системой блоков, сопряженных с блоком* Ω_1, если $\Omega_1 \cup \ldots \cup \Omega_k$ есть разбиение множества Ω, и для любого $i \in \overline{1,k}$ в G существует подстановка g_i такая, что $\Omega_i = g_i(\Omega_1)$.

Утверждение 15. *Для произвольного блока Ω_1 любой импримитивной группы G существует полная система блоков, сопряженных с Ω_1.*

□ Пусть $G = \{g_1, \ldots, g_N\}$. По сделанному ранее замечанию множества $g_i(\Omega_1)$ являются блоками группы G при всех $i \in \overline{1,N}$. Так как G транзитивна, то $\bigcup_{i=1}^{N} g_i(\Omega_1) = \Omega$. Кроме того, любые два блока $g_i(\Omega_1)$, $g_j(\Omega_1)$ или совпадают, или не пересекаются. Следовательно, выбрав каждый из встречающихся в системе $g_1(\Omega_1), \ldots, g_N(\Omega_1)$ блоков ровно по одному разу, мы получим искомую полную систему блоков группы G. □

В группе G, рассмотренной в примере 8, полными системами блоков являются $\{\Omega_1, \Omega_2\}$ и $\{\Omega_3, \Omega_4, \Omega_5\}$.

Следствие. *Порядок любого блока импримитивной группы $G < S(\Omega)$ делит число $|\Omega|$.*

□ По утверждению 15 для любого блока Ω_1 группы G существует полная система блоков, сопряженных с Ω_1. Так как все блоки системы равномощны, то $|\Omega| = |\Omega_1| \cdot k$, где k — число блоков в рассматриваемой полной системе. Следовательно, $|\Omega_1|$ делит $|\Omega|$. □

Наличие у импримитивной группы подстановок $G < S(\Omega)$ полных систем нетривиальных блоков позволяет строить для группы G подстановочные представления степеней меньших чем $|\Omega|$.

Утверждение 16. *Пусть $\overline{\Omega} = \{\Omega_1, \ldots, \Omega_k\}$ — полная система блоков импримитивной группы G. Тогда отображение $\varphi\colon G \to S(\overline{\Omega})$, определенное формулой*

$$\forall\, g \in G\colon \quad \varphi(g) = \begin{pmatrix} \Omega_1 & \ldots & \Omega_k \\ g(\Omega_1) & \ldots & g(\Omega_k) \end{pmatrix},$$

является гомоморфизмом.

Доказательство осуществляется непосредственной проверкой.

Пользуясь утверждением 15, нетрудно описать все блоки любой регулярной группы.

Утверждение 17. *Если группа $G < S(\Omega)$ является правым регулярным представлением группы $(\Omega; *)$, то подмножество $\Omega_1 \subset \Omega$ является блоком группы G тогда и только тогда, когда Ω_1 является правым смежным классом группы $(\Omega; *)$ по некоторой ее подгруппе.*

□ Пусть Ω_1 — правый смежный класс группы $(\Omega; *)$ по некоторой подгруппе H. Тогда для любой подстановки $g_a = \begin{pmatrix} x \\ xa \end{pmatrix}$ из G множество $g_a(\Omega_1) = \Omega_1 a$ будет также правым смежным классом группы $(\Omega; *)$ по подгруппе H. Следовательно, $g_a(\Omega_1) \cap \Omega_1 \in \{\varnothing, \Omega_1\}$, т. е. Ω_1 — блок группы G. Обратно, пусть Ω_1 — блок группы G и $\Omega_1, \ldots, \Omega_k$ — ее полная система блоков, сопряженных с Ω_1, т. е. $\Omega_i = g_{a_i}(\Omega_1) = \Omega_1 a_i$ для некоторых $a_1, \ldots, a_k \in \Omega$. Выберем блок Ω_s, содержащий единицу e группы $(\Omega; *)$. Если $a \in \Omega_s$, то $g_a(\Omega_s) = \Omega_s a$, и $(\Omega_s a \cap \Omega_s) \ni a$. А так как Ω_s — блок, то имеем $\Omega_s a = \Omega_s$ для любого $a \in \Omega_s$. Следовательно, Ω_s — подгруппа в G, а $\Omega_1, \ldots, \Omega_k$ суть все правые смежные классы $(\Omega; *)$ по Ω_s. □

Следствие. *Регулярная группа подстановок $G < S(\Omega)$ примитивна, если $|\Omega|$ — простое число, и импримитивна, если $|\Omega|$ — составное число.*

□ Первое утверждение очевидно, а второе следует из утверждения 21 и теоремы 47 главы 11. □

Следующее утверждение показывает, что класс примитивных групп является промежуточным между классами транзитивных и 2-транзитивных групп.

Утверждение 18. *Любая 2-транзитивная группа примитивна.*

□ Допустим, что 2-транзитивная группа $G < S(\Omega)$ имеет нетривиальный блок Ω_1. Тогда существуют $a, b \in \Omega_1$, $a \neq b$, $c \in \Omega \setminus \Omega_1$ и подстановка $g \in G$ такие, что $g(a) = b$, $g(b) = c$. Отсюда имеем $g(\Omega_1) \neq \Omega_1$ и $g(\Omega_1) \cap \Omega_1 \ni b$, — противоречие с тем, что Ω_1 — блок группы G. □

Определение 12. Примитивные, но не 2-транзитивные группы подстановок называют *унипримитивными*.

Примерами унипримитивных групп являются регулярные группы подстановок простой степени. Они примитивны по следствию утверждения 15 и не 2-транзитивны по утверждению 14(а).

Докажем критерий примитивности.

Теорема 19. *Транзитивная группа подстановок $G < S(\Omega)$ примитивна тогда и только тогда, когда стабилизатор G_a любой точки $a \in \Omega$ является максимальной подгруппой в G, т. е. в G нет подгрупп H, удовлетворяющих условию*

$$G_a \lneqq H \lneqq G. \tag{12}$$

□ Пусть для некоторого $a \in \Omega$ в группе G существует подгруппа, удовлетворяющая условию (12). Докажем, что орбита $H(a)$ группы H является блоком группы G. Действительно, если $H(a) \cap g(H(a)) \ni b$ для некоторых $g \in G$, $b \in \Omega$, то существуют $h_1, h_2 \in H$ такие, что $b = h_1(a) = g(h_2(a))$. Тогда $h_2 g h_1^{-1}(a) = a$, т. е. $h_2 g h_1^{-1} \in G_a$. Отсюда следует, что $g \in h_2^{-1} G_a h_1 \subset H$, и потому $g(H(a)) = H(a)$. Итак, $\Omega_1 = H(a)$ — блок G. Покажем, что он нетривиальный. Так как $H \neq G_a$, то в H найдется такая подстановка h, что $h(a) = c \neq a$. Следовательно, $\Omega_1 \ni a, c$ и $|\Omega_1| > 1$. Кроме того, $\Omega_1 \neq \Omega$, так как в противном случае $\Omega_1 = G(a)$ и, используя лемму Бернсайда и очевидное равенство $H_a = G_a$, получим $|H| = |H(a)| \cdot |H_a| = |G(a)| \cdot |G_a| = |G|$, — противоречие с условием (12). Таким образом, $H(a)$ — нетривиальный блок группы G, т. е. группа G не примитивна.

Обратно, пусть G не примитивна и a — любой элемент из Ω. По утверждению 15 найдется нетривиальный блок Ω_1 группы G, содержащий a. Рассмотрим множество подстановок

$$H = \{g \in G : \ g(\Omega_1) = \Omega_1\}.$$

Очевидно, что H — подгруппа в G, содержащая G_a. Так как G транзитивна и $\Omega_1 \neq \Omega$, то $H \neq G$. А так как $|\Omega_1| > 1$, то Ω_1, кроме a, содержит некоторый элемент b, и тогда подстановка из G, переводящая a в b, содержится в $H \setminus G_a$. Таким образом, в G нашлась подгруппа H, удовлетворяющая условию (12). □

Условие примитивности играет важную роль при описании групп подстановок, заданных системами образующих. Об этом, в частности, свидетельствует

Теорема 20 (К. Жордан, 1871). *Если группа $G < S(\Omega)$ примитивна и содержит транспозицию, то $G = S(\Omega)$.*

□ Пусть (a, b_1) — транспозиция из G, $M = \{(a, b_1), (a, b_2), \ldots, (a, b_k)\}$ — множество всех транспозиций из G, не оставляющих на месте a, и $H = \langle M \rangle$. Так как $(a, b_1) \in H$, то по теореме 19 $G = \langle G_a, H \rangle$. А так как для любых $g \in G_a$ и $i \in \overline{1, k}$ верно равенство $g^{-1}(a, b_i)g = (a, g(b_i))$, то $H \lhd G$, и потому $G = G_a \cdot H$. Следовательно, каждый элемент из G представим в виде

$$g(a, b_{i_1})(a, b_{i_2}) \ldots (a, b_{i_s}),$$

где $g \in G_a$. Ясно, что такими подстановками букву a можно перевести лишь в буквы $a, b_1, \ldots, b_k$, и в силу транзитивности группы G имеем $\{a, b_1, \ldots, b_k\} = \Omega$. Отсюда и из теоремы 32 главы 11 следует, что $H = S(\Omega)$, а тогда и подавно $G = S(\Omega)$. □

В заключение данного параграфа укажем еще одно приложение теоремы 19. А именно, из теоремы 19, используя следствие 2 утверждения 6 главы 11, легко получить

Утверждение 21. *Подстановочное представление $\varphi_H(G)$ группы G на ее правых смежных классах по подгруппе H является примитивной группой тогда и только тогда, когда H — максимальная подгруппа группы G.*

ЗАДАЧИ

1. Опишите всевозможные степени транзитивных подстановочных представлений конечной абелевой группы заданного порядка.

2. При каких условиях являются регулярными группами подстановочные представления группы G на смежных классах по подгруппе H и на подгруппах, сопряженных с H?

3. Докажите, что если индекс подгруппы H группы G равен наименьшему простому делителю порядка группы G, то $H \lhd G$.

4. Докажите, что нормализатор регулярной группы подстановок Σ_{2^n} (см. пример 4) совпадает с группой $AGL(n, 2)$.

5. Докажите, что группа подстановок $G < S(\Omega)$ k-транзитивна тогда и только тогда, когда подстановками из G можно какой-либо один набор k различных букв из Ω перевести во все наборы k различных букв из Ω.

6. Докажите, что для конечного коммутативного кольца R с единицей и $n \in \mathbb{N}$ выполняются следующие утверждения:

а) группа $AGL(n, R)$ транзитивна;

б) $AGL(n, R)$ примитивна $\Leftrightarrow R$ — поле;

в) $AGL(n, R)$ 2-транзитивна $\Leftrightarrow R$ — поле;

г) $AGL(n, R)$ 3-транзитивна $\Leftrightarrow R = GF(2)$ или $R = GF(3)$, $n = 1$;

д) $AGL(n, R)$ 4-транзитивна $\Leftrightarrow R = GF(2)$, $n = 2$;

е) $AGL(2, 2) \cong S_4$;

ж) $GL(2, 2) \cong S_3$.

7. При каких значениях n группа $AGL(n, 2)$ точно 3-транзитивна?

8. Докажите, что проективная линейная группа $PGL(n, q)$ изоморфна факторгруппе полной линейной группы $GL(n, q)$ по ее центру.

9. Пусть транзитивная группа подстановок G степени n содержит подстановку g, представимую в виде произведения двух независимых циклов длин n_1, n_2, где $n_1 + n_2 = n$ и $(n_1, n_2) = 1$. Докажите, что G примитивна.

10. Выясните, как изменится класс примитивных групп, если в определении примитивной группы опустить условие транзитивности.

11. Опишите все полные системы блоков циклической группы $G < S_n$, порожденной подстановкой $g = (1, 2, \ldots, n)$.

12. Выясните, при каком условии группа $G = \langle a, g \rangle$, где $a = (i, j)$, $g = (1, 2, \ldots, n)$, будет примитивной.

13. Докажите, что любой неединичный нормальный делитель примитивной группы подстановок транзитивен.

14. Установите биективное соответствие между блоками транзитивной группы G, содержащими точку a, и всеми подгруппами группы G, содержащими стабилизатор G_a. (*Указание*: воспользуйтесь основной идеей доказательства теоремы 19.)

15. Пусть $G < S(\Omega)$, Δ — орбита группы G, и φ — отображение G в группу $S(\Delta)$, определенное формулой $\forall g \in G\colon\ \varphi(g) = g\big|_\Delta$, где $g\big|_\Delta$ — ограничение g на Δ. Покажите, что φ — представление группы G, подстановочно эквивалентное представлению φ_H группы G на ее смежных классах по стабилизатору $H = G_\Delta$ всех точек из Δ.

16. Для подстановочного представления φ импримитивной группы G на полной системе блоков (см. утверждение 16) найдите такую подгруппу $H < G$, что $\varphi = \varphi_H$.

Глава 25

ЛИНЕЙНЫЕ РЕКУРРЕНТНЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ

Линейные рекуррентные последовательности — древнейшие объекты изучения в алгебре и теории чисел. Исторически первыми из них изучались арифметические и геометрические прогрессии. Хорошо известна также последовательность Фибоначчи (см. ниже пример 4), первоначально введенная в 1202 г. в знаменитой «Книге об абаке» итальянским математиком Леонардо Пизанским (Фибоначчи) (около 1180–1240). Свойства этой последовательности до сих пор широко используются в различных областях математики. В частности, они были существенно использованы нашим современником, ленинградским математиком Ю. В. Матиясевичем при решении 10-й проблемы Гильберта[36] об отсутствии алгоритма для распознавания разрешимости алгебраических уравнений над $\mathbb{Z}$ (диофантовых уравнений, названных так в честь древнегреческого математика Диофанта (III век до н. э.)).

Основы теории линейных рекуррентных, или «возвратных», последовательностей были заложены в трудах английского математика Абрахама де Муавра и одного из членов Петербургской академии наук, швейцарского математика Даниила Бернулли (1700–1782). Развернутую теорию изложил крупнейший математик XVIII в., петербургский академик швейцарец Леонард Эйлер. Из более поздних работ следует выделить труды российских академиков П. Л. Чебышева, А. А. Маркова (1856–1922) и французского математика Е. Люка́ (1842–1891).

В наше время теория линейных рекуррентных последовательностей переживает второй этап интенсивного развития, связанный с различными приложениями дискретной математики. В частности, ее используют при построении помехоустойчивых кодов для передачи информации и при моделировании на ЭВМ псевдослучайных последовательностей для проведения вычислений методом Монте-Карло.

§ 1. СЕМЕЙСТВО ЛРП С ДАННЫМ ХАРАКТЕРИСТИЧЕСКИМ МНОГОЧЛЕНОМ И ЕГО БАЗИСЫ

1. Всюду далее R — коммутативное кольцо с единицей e.

Определение 1. *Последовательностью над* R назовем любую функцию $u\colon \mathbb{N}_0 \to R$, при этом для каждого $i \in \mathbb{N}_0$ элемент $u(i)$ назовем i-м членом последовательности u. Множество всех последовательностей над R обозначим через R^∞.

[36] Д. Гильберт (1862–1943) — немецкий математик.

Для наглядности, последовательность $u \in R^\infty$ можно записывать в виде бесконечного вектора

$$u = (u(0),\, u(1),\, \ldots,\, u(i),\, \ldots).$$

Последовательность $(0, 0, \ldots, 0, \ldots)$ будем называть *нулевой* и обозначать через (0).

Определение 2. Последовательность $u \in R^\infty$ называют *линейной рекуррентной последовательностью* (сокращенно ЛРП) *порядка* $m > 0$ *над* R, если существуют константы $f_0, f_1, \ldots, f_{m-1} \in R$ такие, что

$$\forall\, i \in \mathbb{N}_0 :\ u(i+m) = f_{m-1}u(i+m-1) + \ldots + f_1 u(i+1) + f_0 u(i). \qquad (1)$$

В этом случае соотношение (1) называют *законом рекурсии* ЛРП u, многочлен $F(x) = x^m - f_{m-1}x^{m-1} - \ldots - f_1 x - f_0$ — *характеристическим многочленом* ЛРП u, а вектор $u\overline{[0, m-1]} = (u(0), \ldots, u(m-1))$ — ее *начальным вектором*. Последовательность (0) считается по определению единственной линейной рекуррентной последовательностью порядка 0 с характеристическим многочленом $F(x) = e$.

Пример 1 (*геометрическая прогрессия*). Для любых $a, q \in R$ последовательность $u = (a,\, aq,\, \ldots,\, aq^i,\, \ldots)$ есть ЛРП первого порядка с характеристическим многочленом $x - q$ и начальным вектором $u(0) = a$.

Пример 2 (*арифметическая прогрессия*). Для любых $a, d \in R$ последовательность $v \in R^\infty$ с общим членом $v(i) = a + di$, $i \in \mathbb{N}_0$, есть ЛРП порядка 2 с характеристическим многочленом $F(x) = x^2 - 2x + e = (x - e)^2$ и начальным вектором $(a, a + d)$.

Пример 3 (*конгруэнтная последовательность*). При фиксированных $a, q, d \in R$ последовательность $w \in R^\infty$, задающаяся соотношениями

$$w(0) = a, \quad w(i+1) = qw(i) + d, \quad i \in \mathbb{N}_0,$$

есть ЛРП с характеристическим многочленом $F(x) = (x - e)(x - q)$ и начальным вектором $w[ov0, 1] = (a, aq + d)$. Арифметическая прогрессия (пример 2) есть частный случай конгруэнтной последовательности при $q = e$. Такие последовательности над кольцом $R \in \{\mathbb{Z}_{10^n}, \mathbb{Z}_{2^n}\}$ часто используются при моделировании датчиков псевдослучайных чисел на ЭВМ.

Пример 4 (*последовательность Фибоначчи*). Эта последовательность была придумана для решения задачи, называемой «задачей о размножении кроликов». Допустим, что у каждой пары зрелых кроликов через месяц рождается новая пара кроликов, которая еще через месяц достигает зрелости. Сколько всего пар зрелых кроликов можно получить от одной зрелой пары за i месяцев? Если обозначить искомую величину через $u(i)$, то нетрудно увидеть что

$$u(0) = 1, \quad u(1) = 1, \quad u(i+2) = u(i+1) + u(i), \quad i \in \mathbb{N}.$$

Таким образом, u — ЛРП над $\mathbb{Z}$ с характеристическим многочленом $F(x) = x^2 - x - 1$ и начальным вектором $u\overline{[0, 1]} = (1, 1)$.

Пример 5. Последовательность Δ, где $\Delta(i)$ — значение «ленточного» определителя порядка $i+1$ над кольцом R:

$$\Delta(i) = \begin{vmatrix} b & c & 0 & 0 & \dots & \dots & 0 \\ a & b & c & 0 & \dots & \dots & 0 \\ 0 & a & b & c & \dots & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & \dots & 0 & a & b & c \\ 0 & \dots & \dots & 0 & 0 & a & b \end{vmatrix}_{(i+1)\times(i+1)}$$

есть ЛРП с характеристическим многочленом $x^2 - bx + ac$ и начальным вектором $\Delta[\overline{0,1}] = (b,\, b^2 - ac)$. Этот факт устанавливается путем разложения определителя $\Delta(i)$ по 1-й строке.

Зафиксируем унитарный многочлен $F(x) = x^m - f_{m-1}x^{m-1} - \ldots - f_0 \in R[x]$ степени $m \geqslant 0$ и обозначим через $L_R(F)$ *семейство всех ЛРП над R с характеристическим многочленом $F(x)$*. Тогда непосредственно из определения 2 вытекает

Утверждение 1. *Любая ЛРП $u \in L_R(F)$ однозначно задается своим начальным вектором $u[\overline{0, m-1}]$. Если $|R| < \infty$, то $|L_R(F)| = |R|^m$.*

2. При исследовании свойств ЛРП весьма плодотворным оказывается алгебраический подход, связанный с введением на R^∞ различных операций.

Определение 3. *Суммой последовательностей $u, v \in R^\infty$* и *произведением последовательности u на константу $r \in R$* называют, соответственно, последовательности $w = u + v$ и $z = ru$, определяемые соотношениями

$$w(i) = u(i) + v(i), \quad z(i) = ru(i), \quad i \in \mathbb{N}_0.$$

Очевидно, что группоид $(R^\infty, +)$ есть абелева группа с нулем (0), и для любых $a, b \in R$, $u, v \in R^\infty$ справедливы соотношения

$$(ab)u = a(bu), \quad (a+b)u = au + bu,$$
$$a(u+v) = au + av, \quad eu = u.$$

В частности, если P — поле, то определенные выше операции задают на P^∞ структуру левого векторного пространства ${}_P P^\infty$, имеющего, очевидно, бесконечную размерность.

Из определений 2, 3 легко следует

Утверждение 2. *Для любого унитарного многочлена $F(x) \in R[x]$ подмножество $L_R(F) \subset R^\infty$ есть подгруппа группы $(R^\infty, +)$, выдерживающая умножение на элементы из R. Если P — поле и $F(x) \in P[x]$ — унитарный многочлен, то $L_P(F)$ — подпространство пространства P^∞.*

Таким образом, в случае, когда P — поле, можно говорить о базисе пространства $L_P(F)$. Мы, однако, не будем рассматривать эту простейшую ситуацию отдельно, а введем и изучим аналог понятия базиса пространства для произвольного семейства $L_R(F)$.

Определение 4. Для унитарного многочлена $F(x) \in R[x]$ степени $m > 0$ систему последовательностей $u_1, \ldots, u_m \in L_R(F)$ назовем *базисом семейства* $L_R(F)$, если для любой последовательности $u \in L_R(F)$ существует единственный набор констант $c_1, \ldots, c_m \in R$ такой, что

$$u = c_1 u_1 + \ldots + c_m u_m. \tag{2}$$

Доказательство существования и описание базисов семейства $L_R(F)$ дает

Утверждение 3. *В обозначениях определения* 4 *система последовательностей* $u_1, \ldots, u_m \in L_R(F)$ *есть базис* $L_R(F)$ *тогда и только тогда, когда составленная из начальных векторов этих последовательностей матрица*

$$U = \begin{pmatrix} u_1[\overline{0\,,m-1}] \\ \cdots\cdots\cdots\cdots \\ u_m[\overline{0\,,m-1}] \end{pmatrix}$$

обратима над кольцом R.

□ Если U — обратимая матрица, то для любой последовательности $u \in L_R(F)$ существует единственный набор $(c_1, \ldots, c_m) \in R^m$ такой, что

$$u[\overline{0, m-1}] = (c_1, \ldots, c_m) \cdot U. \tag{3}$$

Рассмотрим последовательность $v = c_1 u_1 + \ldots + c_m u_m$. По утверждению 2 $v \in L_R(F)$. Кроме того, очевидно, что $v[\overline{0, m-1}] = (c_1 \ldots c_m)U = u[\overline{0, m-1}]$. Поэтому в силу утверждения 1 $v = u$, т. е. справедливо (2). Единственность представления последовательности u в виде (2) следует из того, что (2) влечет (3). Таким образом, $u_1, \ldots, u_m$ — базис $L_R(F)$.

Наоборот, пусть $u_1, \ldots, u_m$ — базис $L_R(F)$. Определим для каждого $k \in \overline{1, m}$ последовательность e_k^F как ЛРП $e_k^F \in L_R(F)$ с начальным вектором $e_k^F[\overline{0, m-1}] = \vec{E}_k$, где $\vec{E}_k$ — k-я строка единичной матрицы $E_{m\times m}$. По предположению каждая из последовательностей e_k^F представляется в виде

$$e_k^F = c_{k1} u_1 + \ldots + c_{km} u_m\,.$$

Но тогда для матрицы $C = (c_{kl})_{m\times m}$ справедливы равенства

$$C \cdot U = \begin{pmatrix} e_1^F[\overline{0, m-1}] \\ \cdots\cdots\cdots\cdots \\ e_m^F[\overline{0, m-1}] \end{pmatrix} = E_{m\times m}.$$

Следовательно, U — обратимая матрица. □

Пример 6. Определенная выше система ЛРП $e_1^F, \dots, e_m^F \in L_R(F)$ есть базис семейства $L_R(F)$.

Следствие. *Если $F(x)$ — произвольный унитарный многочлен над полем P, то* $\dim L_P(F) = \deg F(x)$.

§ 2. УМНОЖЕНИЕ ПОСЛЕДОВАТЕЛЬНОСТИ НА МНОГОЧЛЕН. ГЕНЕРАТОР ЛРП

1. Утверждение 3 позволяет описать все семейство $L_R(F)$ как множество линейных комбинаций лишь $m = \deg F(x)$ последовательностей из $L_R(F)$. Оказывается, семейство $L_R(F)$ можно описать еще более «экономно» — через одну последовательность специального вида.

Определим на R^∞ внешнюю операцию умножения слева на многочлены из $R[x]$. Для любых $k \in \mathbb{N}_0$ и $u \in R^\infty$ положим

$$x^k \cdot u = v, \quad \text{где} \quad v(i) = u(i+k) \quad \text{для} \quad i \in \mathbb{N}_0.$$

Другими словами, умножение на x^k есть *сдвиг последовательности* u на k шагов влево, или вычеркивание из u первых k членов:

$$x^k \cdot (u(0), u(1), \dots) = (u(k), u(k+1), \dots).$$

Определение 5. *Произведением многочлена $A(x) = \sum_{k=0}^m a_k x^k$ на последовательность $u \in R^\infty$* называется последовательность $A(x)u$ из R^∞ вида

$$A(x)u = \sum_{k=0}^{m} a_k (x^k \cdot u). \tag{4}$$

Из (4) легко видеть, что

$$A(x)u = w, \quad \text{где} \quad w(i) = \sum_{k=0}^{m} a_k u(i+k) \quad \text{для} \quad i \in \mathbb{N}_0.$$

Утверждение 4. *Для любого унитарного многочлена $F(x) \in R[x]$ верно равенство*

$$L_R(F) = \{u \in R^\infty : \ F(x)u = (0)\}. \tag{5}$$

□ Если $F(x) = e$, то по определению 2 $L_R(F) = \{(0)\}$, и равенство (5) очевидно. Если $\deg F(x) = m > 0$, то при обозначениях определения 2 достаточно заметить, что если $u \in R^\infty$, то $F(x)u = v$, где

$$v(i) = u(i+m) - f_{m-1}u(i+m-1) - \dots - f_0 u(i), \quad i \in \mathbb{N}_0.$$

Поэтому условие (1) равносильно условию $F(x)u = (0)$. □

Основные свойства операции умножения последовательности на многочлен описывает

Теорема 5. *Для любых* $A(x), B(x) \in R[x]$ *и* $u, v \in R^\infty$ *справедливы равенства*:

$$A(x)(u+v) = A(x)u + A(x)v, \tag{6}$$

$$(A(x)+B(x))u = A(x)u + B(x)u, \tag{7}$$

$$(A(x)B(x))u = A(x)(B(x)u). \tag{8}$$

□ Равенства (6) и (7) легко выводятся из определения 5. Для доказательства (8) заметим, что для любых $a, b \in R$ и $k, l \in \mathbb{N}_0$ из определений легко следует равенство $ax^k \cdot (bx^l \cdot u) = abx^{k+l} \cdot u$. Поэтому если $A(x) = \sum_{k\geqslant 0} a_k x^k$, $B(x) = \sum_{l\geqslant 0} b_l x^l$, то из (7) и (6) следуют равенства

$$(A(x)B(x)) \cdot u = \left(\sum_{k,l\geqslant 0} a_k b_l x^{k+l}\right) \cdot u = \sum_{k,l\geqslant 0} a_k x^k (b_l x^l \cdot u) =$$

$$= \sum_{k\geqslant 0} a_k x^k (B(x) \cdot u) = A(x) \cdot (B(x) \cdot u)). \quad \square$$

Следствие 1. *Для любого унитарного многочлена* $F(x) \in R[x]$ *семейство* $L_R(F)$ *выдерживает умножение на многочлены из* $R[x]$.

□ Если $u \in L_R(F)$, $A(x) \in R[x]$, то $F(x)(A(x)u) = (F(x)A(x))u = A(x)(F(x)u) = A(x)(0) = (0)$. Следовательно, $A(x)u \in L_R(F)$. □

Следствие 2. *Любая ЛРП* u *над кольцом* R *имеет бесконечно много характеристических многочленов.*

□ Если $u \in L_R(F)$, то любой унитарный многочлен $H(x) \in R[x] \cdot F(x)$ является характеристическим для ЛРП u. □

Замечание 1. Если P — поле, то отображение $\sigma\colon P^\infty \to P^\infty$ по правилу

$$\forall\, u \in P^\infty\colon\ \sigma(u) = x \cdot u \tag{9}$$

есть линейное преобразование пространства ${}_P P^\infty$ со свойством

$$\forall\, A(x) \in P[x],\ \forall\, u \in P^\infty\colon\ A(\sigma)(u) = A(x)u.$$

Поэтому теорема 5 в случае, когда $R = P$ — поле, есть следствие теоремы 10 главы 15. Следствие 1 в этом случае означает, что $L_P(F)$ — подпространство пространства ${}_P P^\infty$, инвариантное относительно линейного преобразования σ.

2. Для унитарного многочлена $F(x) \in R[x]$ степени $m > 0$ через e^F обозначим линейную рекурренту из $L_R(F)$ с начальным вектором $e^F[\overline{0, m-1}] = (0, \ldots, 0, e)$ (т. е. последовательность e^F_m из примера 6). Будем называть e^F *импульсной последовательностью* с характеристическим многочленом $F(x)$.

Теорема 6. *Пусть* $F(x) = x^m - f_{m-1}x^{m-1} - \ldots - f_0 \in R[x]$, $m > 0$. *Тогда для любой ЛРП* $u \in L_R(F)$ *существует единственный многочлен* $\Phi(x) \in R[x]$ *такой, что*

$$u = \Phi(x) \cdot e^F, \quad \deg \Phi(x) < m, \tag{10}$$

и этот многочлен имеет вид

$$\Phi(x) = u(0)x^{m-1} + \sum_{k=1}^{m-1} \big(u(k) - f_{m-1}u(k-1) - \ldots \\ \ldots - f_{m-k}u(0)\big)\, x^{m-1-k}. \tag{11}$$

□ По утверждению 3 система ЛРП e^F, xe^F, $\ldots$, $x^{m-1}e^F \in L_R(F)$ есть базис семейства $L_R(F)$, так как матрица начальных векторов этой системы

$$U = \begin{pmatrix} e^F[\overline{0, m-1}] \\ xe^F[\overline{0, m-1}] \\ \ldots\ldots\ldots\ldots\ldots \\ x^{m-1}e^F[\overline{0, m-1}] \end{pmatrix} = \begin{pmatrix} e^F[\overline{0, m-1}] \\ e^F[\overline{1, m}] \\ \ldots\ldots\ldots\ldots\ldots \\ e^F[\overline{m-1,\, 2m-2}] \end{pmatrix} = \\ = \begin{pmatrix} 0 & \ldots & \ldots & 0 & e \\ 0 & \ldots & \ldots & e & e^F(m) \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ e & e^F(m) & \ldots & \ldots & e^F(2m-2) \end{pmatrix} \tag{12}$$

обратима над R. Следовательно, существует единственный набор коэффициентов $\varphi_0, \ldots, \varphi_{m-1} \in R$ такой, что

$$u = \varphi_0 \cdot e^F + \varphi_1 \cdot xe^F + \ldots + \varphi_{m-1} \cdot x^{m-1}e^F.$$

Теперь очевидно, что $\Phi(x) = \varphi_0 + \varphi_1 x + \ldots + \varphi_{m-1}x^{m-1}$ — искомый единственный многочлен, удовлетворяющий условиям (10).

Для вывода формулы (11) заметим, что коэффициенты многочлена $\Phi(x)$ удовлетворяют равенству

$$u[\overline{0, m-1}] = (\varphi_0, \ldots, \varphi_{m-1}) \cdot U. \tag{13}$$

Покажем, что обратной для U является матрица

$$V = \begin{pmatrix} -f_1 & -f_2 & -f_3 & \ldots & -f_{m-1} & e \\ -f_2 & -f_3 & -f_4 & \ldots & e & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ -f_{m-1} & e & 0 & \ldots & 0 & 0 \\ e & 0 & 0 & \ldots & 0 & 0 \end{pmatrix}. \tag{14}$$

Рассмотрим произведение строки $\vec{V}_s$ матрицы V на столбец $U_t^{\downarrow}$ матрицы U. Из (12) и (14) сразу видно, что $\vec{V}_s U_t^{\downarrow} = 0$, если $s > t$, и $\vec{V}_s U_s^{\downarrow} = e$ для $s \in \overline{1, m}$. Остается показать, что если $s < t$, то $\vec{V}_s U_t^{\downarrow} = 0$. Заметим, что

$$\vec{V}_s = (-f_s, -f_{s+1}, \ldots, -f_{m-1}, e, 0, \ldots, 0),$$

$$U_t^{\downarrow} = (\underbrace{e^F(t-1), e^F(t), \ldots, e^F(t+m-s-1)}_{m-(s-1)}, \ldots, e^F(t+m-2))^T.$$

Поэтому

$$\vec{V}_s U_t^{\downarrow} = -f_s e^F(t-1) - f_{s+1} e^F(t) - \ldots - f_{m-1} e^F(t+m-s-2) + e^F(t+m-s-1).$$

Отсюда, полагая $j = t-s-1$, получаем, что $j \geqslant 0$ и

$$\vec{V}_s U_t^{\downarrow} = e^F(j+m) - f_{m-1} e^F(j+m-1) - \ldots - f_s e^F(j+s).$$

Пользуясь тем, что $j+s = t-1 < m$ и, следовательно, $e^F(i) = 0$ для $i < j+s$, приходим к соотношениям

$$\vec{V}_s U_t^{\downarrow} = e^F(j+m) - f_{m-1} e^F(j+m-1) - \ldots - f_s e^F(j+s) - \ldots - f_0 e^F(j) = 0.$$

Следовательно, $V = U^{-1}$, и вектор коэффициентов многочлена $\Phi(x)$ находится из (13) по формуле

$$(\varphi_0, \ldots, \varphi_{m-1}) = (u(0), \ldots, u(m-1)) \cdot V.$$

Отсюда и из (14) следует (11). $\square$

Замечание 2. В случае, когда $R = P$ — поле, теорема 6 по сути дела утверждает, что $L_P(F)$ — подпространство пространства P^∞, не только инвариантное относительно преобразования σ, определяемого условием (9), но и циклическое относительно σ, причем e^F — вектор, порождающий подпространство $L_P(F)$, т. е. в обозначениях определения 19 главы 15 $L_P(F) = L^\sigma(e^F)$.

Определение 6. Многочлен $\Phi(x)$, удовлетворяющий условиям (10), называется *генератором ЛРП u относительно ее характеристического многочлена $F(x)$*.

§ 3. МИНИМАЛЬНЫЙ МНОГОЧЛЕН И АННУЛЯТОР ЛРП

1. Как уже отмечалось, любая ЛРП над R имеет характеристические многочлены сколь угодно большой степени (следствие 2 теоремы 5). Естественное желание задать ЛРП наиболее компактным способом приводит к необходимости введения и изучения следующих понятий.

Определение 7. Характеристический многочлен ЛРП u, имеющий наименьшую возможную степень, называется ее *минимальным многочленом*, а его степень называется *рангом* ЛРП u и обозначается через $\operatorname{rang} u$.

Очевидно, что ранг ЛРП определяется однозначно. В то же время, минимальных многочленов у одной ЛРП может быть несколько и даже бесконечно много.

Пример 7. Геометрическая прогрессия $u = (a, aq, aq^2, \ldots)$ из примера 1 при условии $a \neq 0$ есть ЛРП ранга 1 с минимальным многочленом $F(x) = x - q$. Если при этом элемент $a \in R$ является делителем нуля и $ab = 0$ для $b \in R \setminus 0$, то минимальным многочленом для u будет также многочлен $F(x) + b$.

Однако для любой ЛРП u над полем P существует единственный минимальный многочлен. Это можно доказать воспользовавшись замечанием 1 и показав, что если $u \in L_P(F)$, то минимальный многочлен ЛРП u есть минимальный многочлен вектора u пространства $L_P(F)$ относительно линейного преобразования $\overline{\sigma} = \sigma\big|_{L_P(F)}$. Нам будет удобнее доказать этот факт, используя

Определение 8. *Аннулятором последовательности* $u \in R^\infty$ называется множество

$$\operatorname{Ann}(u) = \{H(x) \in R[x] : \ H(x)u = (0)\}.$$

Очевидно, что $\operatorname{Ann}(u)$ — идеал кольца $R[x]$, а последовательность $u \in R^\infty$ есть ЛРП над R тогда и только тогда, когда в этом идеале есть унитарные многочлены, и минимальный многочлен ЛРП u есть любой унитарный многочлен наименьшей степени из $\operatorname{Ann}(u)$.

Теорема 7. *Любая ЛРП u над полем P имеет единственный минимальный многочлен $G(x) \in P[x]$, и он удовлетворяет равенству*

$$\operatorname{Ann}(u) = P[x]G(x). \tag{15}$$

□ Так как $P[x]$ — кольцо главных идеалов (теорема 14 главы 20), то существует единственный унитарный многочлен $G(x) \in P[x]$ такой, что выполняется равенство (15). Из (15) следует, что $G(x)$ — характеристический многочлен ЛРП u, на который делится любой другой ее характеристический многочлен. Следовательно, $G(x)$ — единственный минимальный многочлен ЛРП u. □

В дальнейшем минимальный многочлен ЛРП u над полем обозначается через $M_u(x)$. В общем случае справедлива

Теорема 8. *Для любого унитарного многочлена $G(x) \in R[x]$ и любой последовательности $u \in R^\infty$ следующие утверждения эквивалентны*:

(а) *u — ЛРП с единственным минимальным многочленом $G(x)$*;

(б) $\operatorname{Ann}(u) = R[x]G(x)$.

□ (а)⇒(б) Так как $G(x)u = (0)$, то $R[x]G(x) \subset \operatorname{Ann}(u)$. Наоборот, пусть $H(x) \in \operatorname{Ann}(u)$. Разделим $H(x)$ с остатком на $G(x)$:

$$H(x) = Q(x)G(x) + A(x), \quad \deg A(x) < \deg G(x).$$

Тогда $A(x) \in \operatorname{Ann}(u)$, так как $H(x)u = G(x)u = (0)$. Следовательно, многочлен $G_1(x) = G(x) + A(x)$ — унитарный из $\operatorname{Ann}(u)$ той же степени, что и $G(x)$, т. е. $G_1(x)$ — минимальный многочлен ЛРП u. Но тогда ввиду условия (а) $G_1(x) = G(x)$, т. е. $A(x) = 0$ и $H(x) \in R[x]G[x]$.

Импликация (б)⇒(а) доказывается так же, как и в теореме 7. □

2. Укажем некоторые способы построения ЛРП с заданным минимальным многочленом.

Утверждение 9. *Пусть $F(x) \in R[x]$ — унитарный многочлен степени $m > 0$, $u \in L_R(F)$ и $u\overline{[0, m-1]} = (0, \ldots, 0, a)$, где $a \in R$ — элемент, не являющийся делителем нуля. Тогда $F(x)$ — единственный минимальный многочлен ЛРП u.*

□ Достаточно доказать, что $\mathrm{Ann}(u) = R[x]F(x)$. Так как включение $R[x]F(x) \subset \mathrm{Ann}(u)$ очевидно, то для этого достаточно доказать, что любой многочлен $H(x) \in \mathrm{Ann}(u)$ степени меньшей, чем m, равен нулю. Пусть $H(x) = h_0 + h_1 x + \ldots + h_k x^k$, $h_k \neq 0$, $k < m$. Тогда последовательность $v = H(x)u$, ввиду условия на $u\overline{[0, m-1]}$, имеет ненулевой член: $v(m-k-1) = h_k u(m-1) = h_k a \neq 0$. Это противоречит условию $H(x)u = (0)$. □

Следствие. *Для любого унитарного многочлена $F(x) \in R[x]$ справедливо равенство* $\mathrm{Ann}(e^F) = R[x]F(x)$.

Определение 9. Для элемента $\alpha \in R$ и любого $l \in \mathbb{N}_0$ последовательность $\alpha^{[l]} \in R^\infty$, определяемая равенствами

$$\alpha^{[l]}(i) = 0 \ \text{ для } \ i < l, \quad \alpha^{[l]}(l) = e, \quad \alpha^{[l]}(i) = \binom{i}{l} \cdot \alpha^{i-l} \ \text{ для } \ i > l,$$

где $\binom{i}{l} = C_i^l = \dfrac{i\,!}{l\,!\,(i-l)!}$ — биномиальный коэффициент, называется *биномиальной последовательностью* порядка $l+1$ с корнем α.

Утверждение 10. *Для любого $\alpha \in R$ последовательность $\alpha^{[l]}$ есть ЛРП с единственным минимальным многочленом $G(x) = (x-\alpha)^{l+1}$. Более того, $\alpha^{[l]} = e^G$.*

□ Докажем индукцией по l включение $\alpha^{[l]} \in L_R((x-\alpha)^{l+1})$. При $l = 0$ оно очевидно. Пусть $l > 0$ и $\alpha^{[l-1]} \in L_R((x-\alpha)^l)$. Тогда, используя известное равенство $\binom{i+1}{l} - \binom{i}{l} = \binom{i}{l-1}$, получаем $(x-\alpha)\alpha^{[l]} = v$, где $v(i) = 0$, если $i < l-1$, а если $i \geqslant l-1$, то

$$v(i) = \left(\binom{i+1}{l} - \binom{i}{l}\right)\alpha^{i-l+1} = \binom{i}{l-1}\alpha^{i-(l-1)} = \alpha^{[l-1]}(i),$$

т. е. $(x-\alpha)\,\alpha^{[l]} = \alpha^{[l-1]}$. Отсюда, пользуясь предположением индукции, имеем: $(x-\alpha)^{l+1}\alpha^{[l]} = (x-\alpha)^l \alpha^{[l-1]} = (0)$.

Остается заметить, что $\alpha^{[l]}\overline{[0, l]} = (0, \ldots, 0, e) = e^G\overline{[0, l]}$. □

Простой способ вычисления минимального многочлена ЛРП над полем дает

Теорема 11. *Пусть u — ЛРП над полем P с характеристическим многочленом $F(x)$ и генератором $\Phi(x)$. Тогда*

(а) $M_u(x) = \dfrac{F(x)}{(F(x),\, \Phi(x))}$;

(б) *если $v = H(x)u$ для некоторого $H(x) \in P[x]$, то*

$$M_v(x) = \frac{M_u(x)}{(H(x),\, M_u(x))}.$$

□ (а) По определению генератора $u = \Phi(x)e^F$, и так как по следствию утверждения 9 $M_{e^F}(x) = F(x)$, то (а) следует из (б).

(б) Достаточно заметить, что по теореме 6 для любого $A(x) \in P[x]$ справедливы соотношения:

$$A(x)v = (0) \;\Leftrightarrow\; A(x)H(x)u = (0) \;\Leftrightarrow$$
$$\Leftrightarrow\; M_u(x) \mid A(x)H(x) \;\Leftrightarrow\; \frac{M_u(x)}{(H(x),\, M_u(x))} \;\Big|\; A(x). \quad \square$$

Следствие. *Минимальный многочлен ЛРП $u \in L_P(F)$ равен $F(x)$ тогда и только тогда, когда генератор u относительно $F(x)$ взаимно прост с $F(x)$. В частности, $F(x)$ является минимальным многочленом для любой ненулевой ЛРП из $L_P(F)$ тогда и только тогда, когда $F(x)$ неприводим над P.*

Для линейных рекуррент над кольцом теорема 11(а) может быть обобщена следующим образом.

Утверждение 12. *Если u — ЛРП над кольцом R с характеристическим многочленом $F(x)$ и генератором $\Phi(x)$, то*

$$\mathrm{Ann}(u) = \big\{A(x) \in R[x] :\; F(x) \mid A(x)\Phi(x)\big\}.$$

□ Так как $u = \Phi(x)e^F$, то по следствию утверждения 9

$$A(x)u = (0) \;\Leftrightarrow\; A(x)\Phi(x)e^F = (0) \;\Leftrightarrow\; F(x) \mid A(x)\Phi(x). \quad \square$$

§ 4. СООТНОШЕНИЯ МЕЖДУ СЕМЕЙСТВАМИ ЛРП С РАЗЛИЧНЫМИ ХАРАКТЕРИСТИЧЕСКИМИ МНОГОЧЛЕНАМИ

Утверждение 13. *Для любых унитарных многочленов $F(x)$, $G(x)$ из $R[x]$ справедливы импликации*

$$(L_R(G) \subset L_R(F)) \;\Leftrightarrow\; (G(x) \mid F(x)).$$

□ Пусть $G(x) \mid F(x)$. Тогда

$$u \in L_R(G) \;\Rightarrow\; G(x)u = (0) \;\Rightarrow\; F(x)u = (0) \;\Rightarrow\; u \in L_R(F).$$

Пусть $L_R(G) \subset L_R(F)$. Тогда $e^G \in L_R(F)$, $F(x)e^G = (0)$, и по следствию утверждения 9 $G(x) \mid F(x)$. □

Определение 10. Многочлены $F(x)$, $G(x) \in R[x]$ называют *взаимно простыми*, если $R[x]F(x) + R[x]G(x) = R[x]$, т. е.

$$A(x)F(x) + B(x)G(x) = e$$

для некоторых $A(x)$, $B(x) \in R[x]$. В этом случае пишут $(F(x), G(x)) = e$.

С использованием этого определения дословно так же, как и для многочленов над полем (теорема 12 главы 9), доказывается

Утверждение 14. *Для любых многочленов* $F(x), G(x), H(x) \in R[x]$ *справедливы утверждения*:
(а) $((F(x),G(x))=e,\ \ (F(x),H(x))=e)\ \Rightarrow\ (F(x),\ G(x)H(x))=e$;
(б) $((F(x),G(x))=e,\ \ F(x)\mid G(x)H(x))\ \Rightarrow\ F(x)\mid H(x)$;
(в) $((F(x),G(x))=e,\ \ F(x)\mid H(x),\ \ G(x)\mid H(x))\ \Rightarrow\ F(x)G(x)\mid H(x)$.

Теорема 15. *Пусть* $F_0(x), F_1(x) \in R[x]$ *— унитарные взаимно простые многочлены и* $F(x)=F_0(x)F_1(x)$. *Тогда*

$$L_R(F) = L_R(F_0) \dotplus L_R(F_1). \tag{16}$$

Если R *— поле и последовательность* $u \in L_R(F)$ *представлена в виде* $u=u_0+u_1$, $u_s \in L_R(F_s)$, $s \in \overline{0,1}$, *то*

$$(M_{u_0}(x),\ M_{u_1}(x))=e, \quad M_u(x)=M_{u_0}(x)\,M_{u_1}(x). \tag{17}$$

□ По утверждению 13 $L_R(F_s) \subset L_R(F)$ для $s \in \overline{0,1}$ и по утверждению 2

$$L_R(F) \supset L_R(F_0) + L_R(F_1). \tag{18}$$

Так как по условию $A_0(x)F_0(x)+A_1(x)F_1(x)=e$ для подходящих $A_0(x)$, $A_1(x) \in R[x]$, то любая последовательность $u \in L_R(F)$ представляется в виде

$$u=u_0+u_1, \ \ \text{где}\ \ u_s=A_{1-s}(x)F_{1-s}(x)u \ \ \text{для}\ \ s \in \overline{0,1}. \tag{19}$$

Очевидно, что $F_s(x)u_s=A_{1-s}(x)F(x)u=(0)$, т. е. $u_s \in L_R(F_s)$ для $s \in \overline{0,1}$. Отсюда и из (18) следует равенство $L_R(F)=L_R(F_0)+L_R(F_1)$. Если $u \in L_R(F_0) \cap L_R(F_1)$, то $F_s(x)u=0$ для $s \in \overline{0,1}$, и потому в (19) $u_0=u_1=(0)$, т. е. $u=(0)$. Равенство (16) доказано.

Если R — поле и $u=u_0+u_1$, $u_s \in L_R(F_s)$, $s \in \overline{0,1}$, то по теореме 7 $M_{u_s}(x) \mid F_s(x)$, и потому $(M_{u_0}(x), M_{u_1}(x))=e$.

Теперь для доказательства второго равенства в (17) остается заметить, что $M_{u_s}(x)$ есть минимальный многочлен вектора $u_s \in L_R(F)$ относительно линейного преобразования $\sigma=\sigma\big|_{L_R(F)}$ (см. замечание 2), и воспользоваться утверждением 30(б) главы 15. □

Для ЛРП над полем первое утверждение теоремы 15 может быть существенно усиленно.

Теорема 16. *Для любых унитарных многочленов* $F(x)$ *и* $G(x)$ *над полем* P *справедливы равенства*:

$$L_P(F) \cap L_P(G) = L_P(D), \ \ \textit{где}\ D(x)=(F(x),G(x)); \tag{20}$$

$$L_P(F) + L_P(G) = L_P(H), \ \ \textit{где}\ H(x)=[F(x),G(x)]. \tag{21}$$

□ По утверждению 13 $L_P(D) \subset L_P(F) \cap L_P(G)$. С другой стороны, так как $D(x) = A(x)F(x) + B(x)G(x)$ для подходящих $A(x), B(x) \in P[x]$, то для любой ЛРП $u \in L_P(F) \cap L_P(G)$ справедливы равенства

$$D(x)u = A(x)F(x)u + B(x)G(x)u = (0) + (0) = (0),$$

т. е. $u \in L_P(D)$. Равенство (20) доказано.

Из утверждения 13 следует также включение $L_P(F) + L_P(G) \subset L_P(H)$. Остается заметить, что по следствию утверждения 3 и в силу (20)

$$\dim(L_P(F) + L_P(G)) = \dim L_P(F) + \dim L_P(G) - \dim(L_P(F) \cap L_P(G)) =$$
$$= \deg F(x) + \deg G(x) - \deg D(x) = \deg H(x) = \dim L_P(H). \quad \square$$

§ 5. БИНОМИАЛЬНЫЙ БАЗИС ПРОСТРАНСТВА ЛРП НАД ПОЛЕМ

Все рассмотренные выше базисы пространства $L_P(F)$ не давали способов представления общего члена $u(i)$ произвольной ЛРП $u \in L_P(F)$ в виде просто вычисляемой и записываемой явной функции от параметра i. Опишем важный частный случай, когда такой способ существует.

Теорема 17. *Пусть многочлен $F(x) \in P[x]$ раскладывается над полем P на линейные множители и имеет каноническое разложение*

$$F(x) = (x - \alpha_1)^{k_1+1} \dots (x - \alpha_r)^{k_r+1}, \quad k_s \geqslant 0 \text{ для } s \in \overline{1, r}. \tag{22}$$

Тогда базисом пространства $L_P(F)$ является система биномиальных последовательностей

$$\begin{array}{l} \alpha_1^{[0]},\ \alpha_1^{[1]},\ \dots,\ \alpha_1^{[k_1]}, \\ \alpha_2^{[0]},\ \alpha_2^{[1]},\ \dots,\ \alpha_2^{[k_2]}, \\ \dots\dots\dots\dots\dots\dots \\ \alpha_r^{[0]},\ \alpha_r^{[1]},\ \dots,\ \alpha_r^{[k_r]} \end{array} \tag{23}$$

(*см. определение* 9).

□ По теореме 15 пространство $L_P(F)$ есть прямая сумма подпространств:

$$L_P(F) = L_P((x - \alpha_1)^{k_1+1}) \dotplus \dots \dotplus L_P((x - \alpha_r)^{k_r+1}).$$

Остается доказать, что система последовательностей $\alpha_s^{[0]}, \dots, \alpha_s^{[k_s]}$ есть базис пространства $L_P((x - \alpha_s)^{k_s+1})$. Включения $\alpha_s^{[l]} \in L_P((x - \alpha_s)^{k_s+1})$ для $l \in \overline{0, k_s}$ следуют из утверждения 10. Теперь достаточно заметить, что система из k_s+1 векторов длины $k_s + 1$:

$$\begin{array}{l} \alpha_s^{[0]}\,\overline{[0, k_s]} = (e, *, *, \dots, *), \\ \alpha_s^{[1]}\,\overline{[0, k_s]} = (0, e, *, \dots, *), \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ \alpha_s^{[k_s]}\overline{[0, k_s]} = (0, 0, \dots, 0, e) \end{array}$$

линейно независима над P, и воспользоваться утверждением 3. □

Следствие 1. *При условии* (22) *если* $\alpha_1, \ldots, \alpha_r \in P \setminus 0$, *то базисом пространства* $L_P(F)$ *является также система сбалансированных биномиальных последовательностей*:

$$\alpha_s^{\langle l\rangle} = \alpha_s^l \cdot \alpha_s^{[l]}, \quad s \in \overline{1,r}, \quad l \in \overline{0,k_s}, \tag{24}$$

и для каждой ЛРП $u \in L_P(F)$ *существует единственный набор коэффициентов*

$$a_{10},\, a_{11},\, \ldots,\, a_{1k_1},\ a_{20},\, \ldots,\, a_{2k_2},\ \ldots,\, a_{rk_r} \in P$$

такой, что для каждого $i \in \mathbb{N}_0$ *выполняется равенство*

$$\begin{aligned} u(i) = a_{10}\alpha_1^i + a_{11}\binom{i}{1}\alpha_1^i + \ldots + a_{1k_1}\binom{i}{k_1}\alpha_1^i + a_{20}\alpha_2^i + \ldots \\ \ldots + a_{2k_2}\binom{i}{k_2}\alpha_2^i + \ldots + a_{r0}\alpha_r^i + \ldots + a_{rk_r}\binom{i}{k_r}\alpha_r^i. \end{aligned} \tag{25}$$

□ Ввиду условия $\alpha_s^l \in P^*$ любое нетривиальное линейное соотношение между последовательностями (24) дает нетривиальное линейное соотношение между последовательностями (23), и потому невозможно. Нужные коэффициенты $a_{s,l}$ суть коэффициенты в разложении вектора $u \in L_P(F)$ по базису (24):

$$u = \sum_{s=1}^{r}\sum_{l=0}^{k_r} a_{sl}\alpha_s^{\langle l\rangle},$$

поскольку по определению $\alpha_s^{\langle l\rangle}(i) = \binom{i}{l}\alpha_s^i$ для всех $i \in \mathbb{N}_0$. □

По разложению (25) последовательности u можно легко построить ее минимальный многочлен и найти $\operatorname{rang} u$. Мы рассмотрим здесь наиболее простой и важный частный случай (описание $M_u(x)$ в общем случае дано в задаче 26).

Следствие 2. *Если* $\alpha_1, \ldots, \alpha_r$ — *попарно различные элементы множества* $P \setminus 0$, *то для любых* $a_1, \ldots, a_r \in P$ *последовательность* $u \in P^\infty$ *элементов вида*

$$u(i) = a_1\alpha_1^i + \ldots + a_r\alpha_r^i$$

есть ЛРП с характеристическим многочленом

$$F(x) = (x-\alpha_1)\ldots(x-\alpha_r).$$

При этом ранг последовательности u *равен числу ненулевых коэффициентов среди* $a_1, \ldots, a_r$, u

$$M_u(x) = (x-\alpha_1)^{\varepsilon_1}\ldots(x-\alpha_r)^{\varepsilon_r},$$

где $\varepsilon_s = \begin{cases} 1, & \text{если } a_s \neq 0, \\ 0, & \text{если } a_s = 0 \end{cases}$ *для* $s \in \overline{1,r}$.

□ Включение $u \in L_P(F)$ очевидно. Тогда $M_u(x) \mid F(x)$, т. е. $M_u(x)$ — произведение некоторых одночленов из $(x-\alpha_1), \ldots, (x-\alpha_r)$. Упрощая обозначения, допустим, что

$$M_u(x) = (x-\alpha_1)\ldots(x-\alpha_t), \quad 1 \leqslant t \leqslant r. \tag{26}$$

Тогда по следствию 1 существуют $c_1, \ldots, c_t \in P$ такие, что

$$\forall\, i \in \mathbb{N}_0 : \ u(i) = c_1\alpha_1^i + \ldots + c_t\alpha_t^i.$$

Отсюда, пользуясь единственностью представления (25), получаем равенства $a_1 = c_1, \ldots, a_t = c_t$, $a_{t+1} = \ldots = a_r = 0$. Остается заметить, что все коэффициенты $c_1, \ldots, c_t$ отличны от нуля. Действительно, если, например, $c_t = 0$, то $u \in L_P((x-\alpha_1)\ldots(x-\alpha_{t-1}))$, что противоречит условию (26). □

Замечание 3. Пусть в обозначениях теоремы 17 $m = \deg F(x) = (k_1+1) + \ldots$ $\ldots + (k_r+1)$. Тогда каждая ЛРП $u \in L_P(F)$ однозначно определяется своим начальным вектором $u[\overline{0, m-1}]$, и, как следует из доказательства следствия 1 теоремы 17, для нахождения коэффициентов $a_{s,l}$ в разложении (25) достаточно решить систему m линейных уравнений с m неизвестными $\{x_{sl} : \ s \in \overline{1,r}, \ l \in \overline{0,k_s}\}$, которая в векторной форме имеет вид

$$u[\overline{0,m-1}] = \sum_{s=1}^{r}\sum_{l=0}^{k_s} x_{sl}\,\alpha_s^{\langle l\rangle}[\overline{0,m-1}]. \tag{27}$$

Однозначная разрешимость этой системы следует из линейной независимости системы векторов $\{\alpha_s^{\langle l\rangle}[\overline{0,m-1}] : \ s \in \overline{1,r}, \ l \in \overline{0,k_s}\}$ (см. теорему 17 и утверждение 3).

Пример 8. Пусть u — ЛРП над полем $P = \mathbb{Z}_5$ с характеристическим многочленом $F(x) = x^6 - 2x^3 + x^2 + 3x + 2$ и начальным вектором $u[\overline{0,5}] = (0,\ e,\ e,\ 0,\ 3e,\ e)$. Требуется найти $u(1986)$.

Перебором элементов поля P убеждаемся, что многочлен $F(x)$ имеет в P корни $\alpha_1 = e$, $\alpha_2 = 2e$, $\alpha_3 = 3e$, и его каноническое разложение над P имеет вид

$$F(x) = (x-e)^3(x-2e)^2(x-3e).$$

Следовательно, $F(x)$ удовлетворяет условиям следствия 1 теоремы 17, и последовательность u однозначно представляется в виде

$$u = a_{10}\alpha_1^{\langle 0\rangle} + a_{11}\alpha_1^{\langle 1\rangle} + a_{12}\alpha_1^{\langle 2\rangle} + a_{20}\alpha_2^{\langle 0\rangle} + a_{21}\alpha_2^{\langle 1\rangle} + a_{30}\alpha_3^{\langle 0\rangle}.$$

Выражение (25) для i-го члена этой последовательности имеет в рассматриваемом случае вид

$$u(i) = a_{10}e^i + a_{11}ie^i + a_{12}\binom{i}{2}e^i + a_{20}(2e)^i + a_{21}i(2e)^i + a_{30}(3e)^i =$$
$$= \left(a_{10} + a_{11}i + a_{12}\binom{i}{2}\right)e + (a_{20} + a_{21}i)(2e)^i + a_{30}(3e)^i,$$

а система линейных уравнений (27) для определения коэффициентов в этом представлении выглядит следующим образом:

$$\begin{pmatrix} e^0 & 0e^0 & 0\cdot e^0 & (2e)^0 & 0\cdot(2e)^0 & (3e)^0 \\ e^1 & e^1 & 0\cdot e^1 & (2e)^1 & 1\cdot(2e)^1 & (3e)^1 \\ e^2 & 2e^2 & 1\cdot e^2 & (2e)^2 & 2\cdot(2e)^2 & (3e)^2 \\ e^3 & 3e^3 & 3\cdot e^3 & (2e)^3 & 3\cdot(2e)^3 & (3e)^3 \\ e^4 & 4e^4 & 6\cdot e^4 & (2e)^4 & 4\cdot(2e)^4 & (3e)^4 \\ e^5 & 5e^5 & 10\cdot e^5 & (2e)^5 & 5\cdot(2e)^5 & (3e)^5 \end{pmatrix} \begin{pmatrix} x_{10} \\ x_{11} \\ x_{12} \\ x_{20} \\ x_{21} \\ x_{30} \end{pmatrix} = \begin{pmatrix} 0 \\ e \\ e \\ 0 \\ 3e \\ e \end{pmatrix}.$$

После преобразований в арифметике поля $\mathbb{Z}_5$ эта система принимает вид

$$\begin{pmatrix} e & 0 & 0 & e & 0 & e \\ e & e & 0 & 2e & 2e & 3e \\ e & 2e & e & 4e & 3e & 4e \\ e & 3e & 3e & 3e & 4e & 2e \\ e & 4e & e & e & 4e & e \\ e & 0 & 0 & 2e & 0 & 3e \end{pmatrix} \begin{pmatrix} x_{10} \\ x_{11} \\ x_{12} \\ x_{20} \\ x_{21} \\ x_{30} \end{pmatrix} = \begin{pmatrix} 0 \\ e \\ e \\ 0 \\ 3e \\ e \end{pmatrix}.$$

Решая ее, получаем $(a_{10}, a_{11}, a_{12}, a_{20}, a_{21}, a_{30}) = (e, e, e, 2e, 2e, 2e)$, т. е. для всех $i \in \mathbb{N}$ справедливо равенство

$$u(i) = \left(1 + i + \binom{i}{2}\right) e + (2 + 2i)(2e)^i + 2(3e)^i.$$

Отсюда, при $i = 1986$ находим:

$$\begin{aligned} u(1986) &= 2e + 4\cdot(2e)^{4\cdot 496+2} + 2\cdot(3e)^{4\cdot 496+2} = \\ &= 2e + 4\cdot(2e)^2 + 2\cdot(3e)^2 = 2e + e + 3e = e. \end{aligned}$$

Замечание 4. Теорема 17 может быть использована для описания общего члена ЛРП $u \in L_P(F)$ и в случае, когда многочлен $F(x)$ не раскладывается над полем P на линейные множители. В этой ситуации рассматривается поле разложения Q многочлена $F(x)$ над полем P и каноническое разложение (22) $F(x)$ над Q. Так как $u \in L_Q(F)$, то можно утверждать, что общий член $u(i)$ последовательности u имеет вид (25), где a_{sl} — некоторые коэффициенты из расширения Q поля P. Следует заметить, однако, что при сделанных предположениях в виде (25) представляется общий член любой ЛРП из семейства $L_Q(F)$. Поэтому дополнительное условие $u \in L_Q(F) \cap P^\infty$ накладывает некоторые ограничения на набор коэффициентов $a_{sl} \in Q$. Смысл этих ограничений в случае, когда P — конечное поле, можно будет уяснить из результатов следующего параграфа (см. замечание 5).

Пример 9. Вычислим над полем $P = \mathbb{Z}_3$ значение определителя

$$d = \begin{vmatrix} 2 & 2 & 0 & 0 & \dots & 0 \\ 1 & 2 & 2 & 0 & \dots & 0 \\ 0 & 1 & 2 & 2 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 1 & 2 & 2 \\ 0 & \dots & 0 & 0 & 1 & 2 \end{vmatrix}_{12\times 12}.$$

Как отмечено в примере 5, d есть член $\Delta(11)$ ЛРП Δ над полем P с характеристическим многочленом $F(x) = x^2 - 2x + 2$ и начальным вектором $\Delta[\overline{0,1}] = (2, 2)$.

Многочлен $F(x)$ не имеет корней в P, и потому ввиду условия $\deg F(x) = 2$ он неприводим над P, а его минимальное поле разложения есть $Q = GF(3^2)$. В поле Q многочлен $F(x)$ имеет два разных корня: α_0 и α_1, удовлетворяющих соотношению $\alpha_0 + \alpha_1 = 2$. По следствию 2 теоремы 17 общий член ЛРП Δ имеет вид $\Delta(i) = c_0\alpha_0^i + c_1\alpha_1^i$, где коэффициенты c_0 и c_1 находятся из системы линейных уравнений

$$\begin{cases} c_0\alpha_0^0 + c_1\alpha_1^0 = \Delta(0), \\ c_0\alpha_0^1 + c_1\alpha_1^1 = \Delta(1). \end{cases}$$

Подставляя сюда значения начального вектора, получаем:

$$\begin{cases} c_0 + c_1 = 2, \\ c_0\alpha_0 + c_1\alpha_1 = 2. \end{cases}$$

Пользуясь условием $\alpha_0 + \alpha_1 = 2$, находим $c_0 = c_1 = 1$ и $\Delta(i) = \alpha_0^i + \alpha_1^i$. В частности, $d = \Delta(11) = \alpha_0^{11} + \alpha_1^{11}$. Так как $\alpha_s \in GF(3^2)$, то $\alpha_s^9 = \alpha_s$ для $s \in \overline{0,1}$. Поэтому $\alpha^{11} = \alpha_0^{9+2} + \alpha_1^{9+2} = \alpha_0^3 + \alpha_1^3$. Так как $\alpha_s^2 = 2\alpha_s - 2$, то

$$\alpha_s^3 = 2\alpha_s^2 - 2\alpha_s = \alpha_s - 1 - 2\alpha_s = 2\alpha_s - 1$$

для $s \in \overline{0,1}$. Окончательно получаем: $d = (2\alpha_0 - 1) + (2\alpha_1 - 1) = 2(\alpha_0 + \alpha_1) - 2 = 2$.

§ 6. ПРЕДСТАВЛЕНИЕ ЛРП НАД КОНЕЧНЫМ ПОЛЕМ С ПОМОЩЬЮ ФУНКЦИИ СЛЕД

1. Пусть $P = GF(q)$ — конечное поле характеристики p и $Q = GF(q^m)$ — его расширение степени m.

Определение 11. *Следом из поля Q в поле P* называется отображение $\mathrm{tr}_P^Q\colon Q \to P$, ставящее в соответствие произвольному элементу $\alpha \in Q$ элемент

$$\mathrm{tr}_P^Q(\alpha) = \alpha + \alpha^q + \ldots + \alpha^{q^{m-1}}.$$

Функция $\mathrm{tr}_P^Q(x)$ иногда обозначается также через $\mathrm{tr}_q^{q^m}(x)$ (если достаточно акцентировать внимание лишь на мощностях рассматриваемых полей) или просто — через $\mathrm{tr}(x)$ (если из контекста ясно, какие поля имеются ввиду).

Отметим сразу, что отображение tr_P^Q определено корректно, т. е. для любого $\alpha \in Q$ выполняется включение $\mathrm{tr}_P^Q(\alpha) \in P$, поскольку очевидно, что $\mathrm{tr}_P^Q(\alpha)^q = \mathrm{tr}_P^Q(\alpha)$. Основные свойства функции след перечисляет

Теорема 18. (а) *Функция tr_P^Q есть линейное отображение пространства Q_P на пространство P_P*;

(б) *если дана башня полей $Q = GF(q^m) \supset GF(q^k) \supset P$, то для любого $\alpha \in Q$ справедливо равенство*

$$\mathrm{tr}_q^{q^m}(\alpha) = \mathrm{tr}_q^{q^k}(\mathrm{tr}_{q^k}^{q^m}(\alpha));$$

(в) *если минимальный многочлен элемента* $\alpha \in Q$ *над полем* P *имеет вид* $m_{\alpha,P}(x) = x^k - c_{k-1}x^{k-1} - \ldots - c_0$, *то* $k \mid m$ *и*

$$\mathrm{tr}_q^{q^m}(\alpha) = \frac{m}{k}\, c_{k-1}.$$

□ (а) Для любых элементов $a, b \in P$ и $\alpha, \beta \in Q$ из известного равенства $(\alpha a + \beta b)^q = \alpha^q a + \beta^q b$ и определения 11 следует $\mathrm{tr}_P^Q(\alpha a + \beta b) = \mathrm{tr}(\alpha)a + \mathrm{tr}(\beta)b$. Следовательно, tr_P^Q — линейное отображение Q_P в P_P, и $\mathrm{tr}(Q)$ — подпространство пространства P_P. Так как $\dim P_P = 1$, то либо $\mathrm{tr}(Q) = P$, либо $\mathrm{tr}(Q) = 0$. Последнее равенство невозможно, так как оно означает, что все q^m элементов поля Q являются корнями многочлена $x + x^q + \ldots + x^{q^{m-1}}$ степени q^{m-1}. Следовательно, $\mathrm{tr}(Q) = P$, т. е. tr — отображение Q на P.

(б) Из условия и свойств конечных полей следует, что $k \mid m$. Пусть $m = kn$. Заметим, что справедливо равенство

$$\{0, 1, \ldots, m-1\} = \{ks + l\colon\ s \in \overline{0,\, n-1},\ l \in \overline{0,\, k-1}\}.$$

Теперь утверждение (б) доказывается следующим образом:

$$\mathrm{tr}_q^{q^m}(\alpha) = \sum_{i=0}^{m-1} \alpha^{q^i} = \sum_{l=0}^{k-1}\sum_{s=0}^{n-1} \alpha^{q^{ks+l}} = \sum_{l=0}^{k-1}\sum_{s=0}^{n-1} \alpha^{(q^k)^s \cdot q^l} =$$

$$= \sum_{l=0}^{k-1}\left(\sum_{s=0}^{n-1} \alpha^{(q^k)^s}\right)^{q^l} = \sum_{l=0}^{k-1}\left(\mathrm{tr}_{q^k}^{q^m}(\alpha)\right)^{q^l} = \mathrm{tr}_q^{q^k}(\mathrm{tr}_{q^k}^{q^m}(\alpha)).$$

(в) Рассмотрим расширение $P(\alpha)$ поля P в Q. Так как $[P(\alpha) : P] = \deg m_{\alpha,P}(x) = k$, то $P(\alpha) = GF(q^k)$ и $k \mid m$, т. е. $m = kn$ для подходящего $n \in \mathbb{N}$. Поскольку при сделанных предположениях $\alpha^{q^k} = \alpha$, то справедливы равенства:

$$\mathrm{tr}_{q^k}^{q^m}(\alpha) = \alpha + \alpha^{q^k} + \ldots + \alpha^{q^{k(n-1)}} = \alpha + \alpha + \ldots + \alpha = n\alpha.$$

Из свойств неприводимых многочленов над конечным полем следует равенство

$$m_{\alpha,P}(x) = x^k - c_{k-1}x^{k-1} - \ldots - c_0 = (x-\alpha)(x-\alpha^q)\ldots(x-\alpha^{q^{k-1}}),$$

которое дает соотношение

$$\mathrm{tr}_q^{q^k}(\alpha) = \alpha + \alpha^q + \ldots + \alpha^{q^{k-1}} = c_{k-1}.$$

Отсюда, пользуясь утверждениями (б) и (а), получаем

$$\mathrm{tr}_q^{q^m}(\alpha) = \mathrm{tr}_q^{q^k}(\mathrm{tr}_{q^k}^{q^m}(\alpha)) = \mathrm{tr}_q^{q^k}(n\alpha) = n \cdot \mathrm{tr}_q^{q^k}(\alpha) = nc_{k-1} = \frac{m}{k}\, c_{k-1}. \quad \square$$

2. Основной результат, позволяющий описывать любую ЛРП над конечным полем с помощью функции след, состоит в следующем.

Теорема 19. *Пусть $P = GF(q)$, $G(x) \neq x$ — неприводимый многочлен степени m над P, $Q = GF(q^m)$ — минимальное поле разложения $G(x)$ над P, и α — корень $G(x)$ в Q. Тогда для любой ЛРП $u \in L_P(G(x)^{k+1})$, $k \in \mathbb{N}_0$, существует единственный набор констант $a_0, \ldots, a_k \in Q$ такой, что*

$$u(i) = \operatorname{tr}_P^Q(a_0\alpha^i) + \binom{i}{1} \operatorname{tr}_P^Q(a_1\alpha^i) + \ldots + \binom{i}{k} \operatorname{tr}_P^Q(a_k\alpha^i) \tag{28}$$

при всех $i \in \mathbb{N}_0$. Любая последовательность $u \in P^\infty$ вида (28) *принадлежит $L_P(G(x)^{k+1})$.*

□ Пространство $L_P(G(x)^{k+1})$ имеет над P размерность $m(k+1)$ и потому состоит ровно из $q^{m(k+1)}$ последовательностей. Число различных наборов $(a_0, \ldots, a_k)$ элементов из Q также равно $q^{m(k+1)}$. Поэтому для доказательства теоремы достаточно показать, что любая последовательность вида (28) принадлежит $L_P(G(x)^{k+1})$ и различным наборам коэффициентов $(a_0, \ldots, a_k) \in Q^{(k+1)}$ соответствуют различные последовательности вида (28).

Любая последовательность u, удовлетворяющая условию (28) при некоторых $a_0, \ldots, a_k \in Q$, есть сумма последовательностей

$$u = u_0 + u_1 + \ldots + u_k, \tag{29}$$

где для $l \in \overline{0,k}$ последовательность u_l задается равенствами

$$u_l(i) = \binom{i}{l} \operatorname{tr}_P^Q(a_l\alpha^i), \quad i \in \mathbb{N}_0. \tag{30}$$

Введем обозначения $\alpha_0 = \alpha$, $\alpha_1 = \alpha^q$, $\ldots$, $\alpha_{m-1} = \alpha^{q^{m-1}}$. Тогда по определению 11

$$\operatorname{tr}_P^Q(a_l\alpha^i) = a_l\alpha_0^i + a_l^q\alpha_1^i + \ldots + a_l^{q^{m-1}}\alpha_{m-1}^i.$$

Отсюда и из (30), пользуясь обозначениями (24) и определением 9, получаем

$$u_l = a_l\alpha_0^{\langle l\rangle} + a_l^q\alpha_1^{\langle l\rangle} + \ldots + a_l^{q^{m-1}}\alpha_{m-1}^{\langle l\rangle},$$

и в силу (29)

$$u = \sum_{l=0}^{k} \sum_{s=0}^{m-1} a_l^{q^s} \alpha_s^{\langle l\rangle}. \tag{31}$$

Теперь заметим, что по теореме 7 главы 22 $\alpha_0, \ldots, \alpha_{m-1}$ суть все различные корни в Q неприводимого над P многочлена $G(x)$, т. е. $G(x) = (x-\alpha_0)\ldots(x-\alpha_{m-1})$, и каноническое разложение над Q многочлена $G(x)^{k+1}$ имеет вид

$$G(x)^{k+1} = (x-\alpha_0)^{k+1}\ldots(x-\alpha_{m-1})^{k+1}.$$

Поэтому из (31) и теоремы 17 следует, что $u \in L_Q(G(x)^{k+1})$. Так как, кроме того, $u \in P^\infty$ ввиду (28), то $u \in L_Q(G(x)^{k+1}) \cap P^\infty = L_P(G(x)^{k+1})$. Наконец, так как

элементы $\alpha_0, \ldots, \alpha_{m-1} \in Q$ попарно различны и отличны от нуля, то по теореме 17 система последовательностей

$$\{\alpha_s^{[l]} : \ s \in \overline{0, m-1}, \ l \in \overline{0, k}\}$$

линейно независима над Q. Поэтому различным наборам коэффициентов $(a_0, \ldots, a_k) \in Q^{(k+1)}$ соответствуют различные последовательности вида (31). $\square$

Замечание 5. Из доказательства теоремы 19 вытекает следующий способ представления знаков ЛРП $u \in L_P(G(x)^{k+1})$ в виде (28). Так как $u \in L_Q(G(x)^{k+1})$, то u однозначно представляется в виде

$$u = \sum_{s=0}^{m-1} \sum_{l=0}^{k} a_{sl} \alpha_s^{\langle l \rangle}, \quad \text{где} \quad a_{sl} \in Q, \quad s \in \overline{0, m-1}, \quad l \in \overline{0, k}. \tag{32}$$

Коэффициенты a_{sl} в этом представлении находятся путем решения системы линейных уравнений над Q (см. замечание 3). Из единственности представления (32) и существования для u представления вида (31) следует, что коэффициенты a_{sl} в (32) удовлетворяют соотношениям

$$a_{1l} = a_{0l}^q, \ a_{2l} = a_{0l}^{q^2}, \ \ldots, \ a_{m-1\,l} = a_{0l}^{q^{m-1}}, \quad l \in \overline{0, k}, \tag{33}$$

и искомые коэффициенты $a_0, \ldots, a_k$ в разложении (28) суть $a_0 = a_{00}$, $a_1 = a_{01}, \ldots, a_k = a_{0k}$. Соотношения (33) и представляют собой упомянутые в замечании 4 ограничения на коэффициенты a_{sl} разложения (32) произвольной ЛРП $u \in L_Q(G(x)^{k+1})$, которые накладываются условием $u \in P^\infty$.

Пример 10. Пусть u — ЛРП над полем $P = \mathbb{Z}_5$ с характеристическим многочленом $(x^2 - 2x - 2)^2$ и начальным вектором $u[\overline{0,3}] = (0, 0, 0, 1)$. Требуется представить общий член этой ЛРП с помощью функции след и вычислить $u(37)$. Непосредственной проверкой убеждаемся в том, что многочлен $G(x) = x^2 - 2x - 2$ не имеет корней в P и потому неприводим. Пусть $Q = GF(5^2)$ — минимальное поле разложения $G(x)$ над P, и $\alpha \in Q$ — корень $G(x)$. Тогда согласно теореме 19 общий член $u(i)$ ЛРП u однозначно представляется в виде

$$u(i) = \operatorname{tr}(a_0 \alpha^i) + i \operatorname{tr}(a_1 \alpha^i).$$

Для отыскания коэффициентов a_0, a_1 в этом представлении ищем коэффициенты $a_{00}, a_{01}, a_{10}, a_{11} \in Q$, удовлетворяющие равенству (32), которое в данном случае имеет вид:

$$u = a_{00} \alpha_0^{\langle 0 \rangle} + a_{01} \alpha_0^{\langle 1 \rangle} + a_{10} \alpha_1^{\langle 0 \rangle} + a_{11} \alpha_1^{\langle 1 \rangle},$$

где $\alpha_s = \alpha^{5^s}$, $\alpha_s^{\langle 0 \rangle} = (\ldots, \alpha_s^i, \ldots)$, $\alpha_s^{\langle 1 \rangle} = (\ldots, i\alpha_s^i, \ldots)$ для $s \in \overline{0,1}$. Согласно замечанию 5 $a_0 = a_{00}$, $a_1 = a_{01}$. Коэффициенты a_{sl} находятся из системы линейных уравнений

$$u[\overline{0,3}] = a_{00}\, \alpha_0^{\langle 0 \rangle}[\overline{0,3}] + a_{01}\, \alpha_0^{\langle 1 \rangle}[\overline{0,3}] + a_{10}\, \alpha_1^{\langle 0 \rangle}[\overline{0,3}] + a_{11}\, \alpha_1^{\langle 1 \rangle}[\overline{0,3}],$$

которая в рассматриваемом случае имеет следующую матричную запись:

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ \alpha & \alpha & \alpha^5 & \alpha^5 \\ \alpha^2 & 2\alpha^2 & \alpha^{10} & 2\alpha^{10} \\ \alpha^3 & 3\alpha^3 & \alpha^{15} & 3\alpha^{15} \end{pmatrix} \begin{pmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Составим расширенную матрицу системы:

$$A = \left(\begin{array}{cccc|c} 1 & 0 & 1 & 0 & 0 \\ \alpha & \alpha & \alpha^5 & \alpha^5 & 0 \\ \alpha^2 & 2\alpha^2 & \alpha^{10} & 2\alpha^{10} & 0 \\ \alpha^3 & 3\alpha^3 & \alpha^{15} & 3\alpha^{15} & 1 \end{array}\right)$$

и упростим ее элементарными преобразованиями строк. Вычитая последовательно из 4-й, 3-й, 2-й строки матрицы A предыдущую строку, умноженную на α, получаем

$$A \sim B = \left(\begin{array}{cccc|c} 1 & 0 & 1 & 0 & 0 \\ 0 & \alpha & \alpha^5 - \alpha & \alpha^5 & 0 \\ 0 & \alpha^2 & \alpha^{10} - \alpha^6 & 2\alpha^{10} - \alpha^6 & 0 \\ 0 & \alpha^3 & \alpha^{15} - \alpha^{11} & 3\alpha^{15} - 2\alpha^{11} & 1 \end{array}\right).$$

Повторяя ту же процедуру с 4-й и 3-й строками B, получаем

$$B \sim C = \left(\begin{array}{cccc|c} 1 & 0 & 1 & 0 & 0 \\ 0 & \alpha & \alpha^5 - \alpha & \alpha^5 & 0 \\ 0 & 0 & \alpha^{10} - 2\alpha^6 + \alpha^2 & 2\alpha^{10} - 2\alpha^6 & 0 \\ 0 & 0 & \alpha^{15} - 2\alpha^{11} + \alpha^7 & 3\alpha^{15} - 4\alpha^{11} + \alpha^7 & 1 \end{array}\right).$$

Вычитая из 4-й строки матрицы C 3-ю, умноженную на α^5, находим

$$C \sim D = \left(\begin{array}{cccc|c} 1 & 0 & 1 & 0 & 0 \\ 0 & \alpha & \alpha^5 - \alpha & \alpha^5 & 0 \\ 0 & 0 & \alpha^{10} - 2\alpha^6 + \alpha^2 & 2\alpha^{10} - 2\alpha^6 & 0 \\ 0 & 0 & 0 & \alpha^{15} - 2\alpha^{11} + \alpha^7 & 1 \end{array}\right).$$

Так как α — корень многочлена $x^2 - 2x - 2$, то справедливы соотношения

$$\begin{array}{lll} \alpha^2 = 2\alpha + 2, & \alpha^5 = 4\alpha + 2, & \alpha^{10} = 3\alpha + 1, \\ \alpha^3 = \alpha + 4, & \alpha^6 = 3, & \alpha^{11} = 2\alpha + 1, \\ \alpha^4 = \alpha + 2, & \alpha^7 = 3\alpha, & \alpha^{15} = 4\alpha + 1, \end{array}$$

пользуясь которыми, матрицу D можно записать в виде

$$D = \left(\begin{array}{cccc|c} 1 & 0 & 1 & 0 & 0 \\ 0 & \alpha & 3\alpha + 2 & 4\alpha + 2 & 0 \\ 0 & 0 & 2 & \alpha + 1 & 0 \\ 0 & 0 & 0 & 3\alpha + 4 & 1 \end{array}\right).$$

Так как $(3\alpha+4)^{-1}=\alpha$, то вычитая из 3-й строки матрицы D ее 4-ю строку, умноженную на $\alpha(\alpha+1)$, получаем

$$D\sim\left(\begin{array}{cccc|c}1&0&1&0&0\\0&\alpha&3\alpha+2&4\alpha+2&0\\0&0&2&0&2\alpha+3\\0&0&0&3\alpha+4&1\end{array}\right).$$

Теперь, как нетрудно видеть, в исходной системе линейных уравнений выделяется подсистема

$$\begin{pmatrix}1&1\\0&2\end{pmatrix}\begin{pmatrix}a_{00}\\a_{10}\end{pmatrix}=\begin{pmatrix}0\\2\alpha+3\end{pmatrix},$$

из которой находим: $a_{10}=\alpha+4$, $a_{00}=4\alpha+1$ и $a_0=a_{00}=4\alpha+1$. (Для проверки заметим, что $a_{00}^5=(4\alpha+1)^5=4\alpha^5+1=4(4\alpha+2)+1=\alpha+4=a_{10}$.) Отсюда для отыскания переменных a_{10}, a_{11} получаем следующую систему:

$$\begin{pmatrix}\alpha&4\alpha+2\\0&3\alpha+4\end{pmatrix}\begin{pmatrix}a_{01}\\a_{11}\end{pmatrix}=\begin{pmatrix}-(3\alpha+2)(\alpha+4)\\1\end{pmatrix}=\begin{pmatrix}1\\1\end{pmatrix}.$$

Решая ее, находим: $a_{11}=(3\alpha+4)^{-1}=\alpha$, $a_{01}=\alpha^{-1}(1-\alpha(4\alpha+2))=3\alpha^{-1}=$ $=3(3\alpha+4)=4\alpha+2=a_{11}^5$ и $a_1=a_{01}=4\alpha+2$.

Окончательно получаем, что искомое представление знаков ЛРП u имеет вид

$$u(i)=\operatorname{tr}((4\alpha+1)\alpha^i)+i\operatorname{tr}((4\alpha+2)\alpha^i),\quad i\in\mathbb{N}_0.$$

Теперь элемент $u(37)$ можно вычислить следующим образом. Так как $\alpha^{24}=\alpha^{5^2-1}=1$, то $\alpha^{37}=\alpha^{13}=\alpha^3\alpha^{10}=(\alpha+4)(3\alpha+1)=4\alpha$. Отсюда

$$\begin{aligned}u(37)&=\operatorname{tr}((4\alpha+1)4\alpha)+37\operatorname{tr}((4\alpha+2)4\alpha)=\\&=\operatorname{tr}(((4\alpha+1)+2(4\alpha+2))\cdot4\alpha)=\operatorname{tr}(3\alpha^2)=\operatorname{tr}(\alpha+1)=\operatorname{tr}(\alpha)+\operatorname{tr}(1).\end{aligned}$$

Так как α — корень неприводимого многочлена x^2-2x-2, то по теореме 18(в) $\operatorname{tr}(\alpha)=2$ и $\operatorname{tr}(1)=2$. В итоге $u(37)=4$.

Замечание 6. Теорема 19 позволяет вычислить с помощью функции след знаки линейной рекурренты не только с примарным, но и вообще с любым характеристическим многочленом $F(x)$ таким, что $F(0)\neq0$. Для этого достаточно найти каноническое разложение $F(x)$ и представить исходную ЛРП в виде суммы ЛРП с примарными характеристическими многочленами, пользуясь теоремой 15.

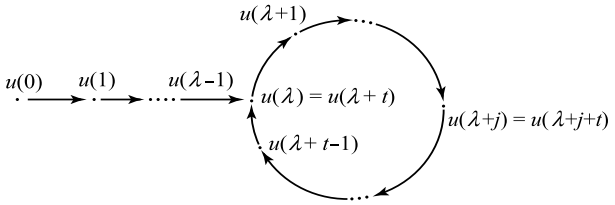
§ 7. ПЕРИОДИЧЕСКИЕ ПОСЛЕДОВАТЕЛЬНОСТИ

1. Пусть Ω — произвольное множество.

Определение 12. Последовательность $u\in\Omega^\infty$ называется *периодической*, если существуют параметры $\lambda\in\mathbb{N}_0$ и $t\in\mathbb{N}$ такие, что

$$\forall\, i\geqslant\lambda:\ \ u(i+t)=u(i).\tag{34}$$

Для наглядности периодическую последовательность u, удовлетворяющую условию (34), можно изобразить графически следующим образом:



Заметим, что если u — последовательность над кольцом R, то условие (34) эквивалентно условию

$$x^{\lambda}(x^t - e)u = (0). \tag{35}$$

В дальнейшем этот факт используется без дополнительных оговорок. В частности, отсюда следует

Утверждение 20. *Любая периодическая последовательность над кольцом R есть ЛРП.*

Если $u \in \Omega^{\infty}$ — периодическая последовательность, то пара чисел $(\lambda, t) \in \mathbb{N}_0 \times \mathbb{N}$, удовлетворяющая условию (34), определена неоднозначно. Для описания всех таких пар чисел введем

Определение 13. Если $u \in \Omega^{\infty}$ — периодическая последовательность, то наименьшее число $t \in \mathbb{N}$, для которого существует $\lambda \in \mathbb{N}_0$ такое, что выполняется (34), назовем *периодом* последовательности u и обозначим через $T(u)$. При этом наименьший параметр $\lambda \in \mathbb{N}_0$ такой, что

$$\forall\, i \geqslant \lambda\colon\ u(i + T(u)) = u(i),$$

назовем *длиной подхода* последовательности u и обозначим через $\Lambda(u)$.

Теорема 21. *Если u — периодическая последовательность элементов множества Ω, то числа $\lambda \in \mathbb{N}_0$, $t \in \mathbb{N}$ удовлетворяют условию* (34) *тогда и только тогда, когда*

$$\lambda \geqslant \Lambda(u), \quad T(u) \mid t.$$

□ Введем, для краткости, обозначения: $\Lambda(u) = \lambda_0$, $T(u) = t_0$. Пусть M — множество всех различных элементов из Ω, встречающихся в последовательности u. Так как u — периодическая последовательность, то M — конечное множество: $|M| \leqslant \lambda_0 + t_0$. Выберем произвольно поле P такое, что $|P| \geqslant |M|$, зададим инъективное отображение $\xi\colon M \to P$ и определим последовательность $\overline{u} \in P^{\infty}$ условием $\overline{u}(i) = \xi(u(i))$ для $i \in \mathbb{N}_0$. Ввиду инъективности отображения ξ очевидно, что для фиксированных $\lambda \in \mathbb{N}_0$ и $t \in \mathbb{N}$ условие (34) равносильно условию

$$x^{\lambda}(x^t - e)\overline{u} = (0). \tag{36}$$

Отсюда и из условия теоремы следует, что $\overline{u}$ — периодическая последовательность, причем $T(\overline{u}) = t_0$, $\Lambda(\overline{u}) = \lambda_0$, и нам достаточно доказать, что условие (36) равносильно условию

$$\lambda \geqslant \lambda_0, \quad t_0 \mid t. \tag{37}$$

Так как по определению 13

$$x^{\lambda_0}(x^{t_0} - e)\overline{u} = (0), \tag{38}$$

и из (37) следует, что $x^{\lambda_0}(x^{t_0} - e) \mid x^{\lambda}(x^t - e)$, то из (37) следует (36).

Наоборот, допустим, что параметры $\lambda \in \mathbb{N}_0$, $t \in \mathbb{N}$ удовлетворяют условию (36), и докажем (37). Заметим, что справедливо равенство

$$(x^{\lambda}(x^t - e),\ x^{\lambda_0}(x^{t_0} - e)) = x^l(x^d - e), \tag{39}$$

где $l = \min\{\lambda, \lambda_0\}$, $d = (t, t_0)$. Действительно, очевидно, что

$$(x^{\lambda}(x^t - e),\ x^{\lambda_0}(x^{t_0} - e)) = x^l(x^t - e,\ x^{t_0} - e),$$

и так как по определению 13 $t \geqslant t_0$, то $x^t - e = x^{t-t_0}(x^{t_0} - e) + (x^{t-t_0} - e)$, откуда $(x^t - e,\ x^{t_0} - e) = (x^{t-t_0} - e,\ x^{t_0} - e)$. Теперь равенство (39) легко доказывается индукцией по $t + t_0$.

Так как многочлен $x^l(x^d - e)$ есть линейная комбинация многочленов $x^{\lambda}(x^t - e)$ и $x^{\lambda_0}(x^{t_0} - e)$, то из (36) и (38) следует, что

$$x^l(x^d - e)\overline{u} = (0).$$

Отсюда по определению параметра $t_0 = T(u)$ следует, что $d \geqslant t_0$, а так как $d = (t, t_0) \mid t_0$, то $d = t_0$, $t_0 \mid t$, и верно равенство $x^l(x^{t_0} - e)u = (0)$. Но тогда по определению параметра $\lambda_0 = \Lambda(u)$ справедливо неравенство $l \geqslant \lambda_0$, т. е. верно (37). □

Следствие 1. *Если $u \in \Omega^{\infty}$ — периодическая последовательность, то $\Lambda(u)$ есть наименьшее $\lambda \geqslant \mathbb{N}_0$, для которого существует $t \in \mathbb{N}$ со свойством* (34).

Следствие 2. *Если u — периодическая последовательность над кольцом R, то для любого многочлена $H(x) \in R[x]$ последовательность $v = H(x)u$ также периодическая, причем $\Lambda(v) \leqslant \Lambda(u)$ и $T(v) \mid T(u)$.*

□ Достаточно заметить, что если $\Lambda(u) = \lambda_0$, $T(u) = t_0$, то

$$x^{\lambda_0}(x^{t_0} - e)v = H(x)x^{\lambda_0}(x^{t_0} - e)u = (0). \quad \square$$

В качестве важного приложения теоремы 21 докажем

Утверждение 22. *Если $u, v \in R^{\infty}$ — периодические последовательности, то $w = u + v$ — периодическая последовательность, и*

$$\Lambda(w) \leqslant \max\{\Lambda(u), \Lambda(v)\}, \quad T(w) \mid [T(u), T(v)]. \tag{40}$$

При этом:

(а) *если* $\Lambda(u) \neq \Lambda(v)$, *то*

$$\Lambda(w) = \max\{\Lambda(u),\, \Lambda(v)\}; \tag{41}$$

(б) *если* $(T(u),\, T(v)) = 1$, *то*

$$T(w) = [T(u),\, T(v)]; \tag{42}$$

(в) *если* u, v — *ЛРП, для которых можно указать взаимно простые характеристические многочлены, то справедливы равенства* (41) *и* (42).

□ Пусть $\lambda = \max\{\Lambda(u),\, \Lambda(v)\}$, $t = [T(u),\, T(v)]$. Тогда по теореме 21 $x^\lambda(x^t - e)u = (0)$ и $x^\lambda(x^t - e)v = (0)$. Следовательно, $x^\lambda(x^t - e)w = (0)$. Отсюда, опять по теореме 21, следуют соотношения (40).

(а) Если, например, $\Lambda(u) < \Lambda(v)$, то $\lambda = \Lambda(v)$. Предположим, что $\Lambda(w) < \lambda$. Тогда многочлен $x^{\lambda-1}(x^t - e)$ аннулирует последовательности u и w, а значит, и последовательность $v = w - u$. Но тогда по теореме 21 $\Lambda(v) \leqslant \lambda - 1$, что невозможно. Следовательно, $\Lambda(w) = \lambda$, т. е. верно (41).

(б) Пусть $(T(u),\, T(v)) = 1$ и $T(w) = \tau$. Заметим, что $[\tau, T(u)] = \tau k$, где $k = \dfrac{T(u)}{(\tau, T(u))} \geqslant 1$, и так как $\tau \mid \tau k$ и $T(u) \mid \tau k$, то по теореме 21 $x^\lambda(x^{\tau k} - e)w = (0)$, $x^\lambda(x^{\tau k} - e)u = (0)$. Но тогда $x^\lambda(x^{\tau k} - e)v = (0)$, и по теореме 21 $T(v) \mid \tau k$, а поскольку $(T(v), k) = 1$, то $T(v) \mid \tau$. Аналогично доказывается, что $T(u) \mid \tau$. Следовательно, $T(u)\,T(v) \mid T(w)$. Теперь (42) следует из (40).

(в) Пусть $u \in L_R(F)$, $v \in L_R(G)$ и $(F(x),\, G(x)) = e$. Тогда $w \in L_R(FG)$ и $L_R(FG) = L_R(F) \dotplus L_R(G)$. Отсюда, учитывая, что для любых $\lambda_1 \in \mathbb{N}_0$, $t_1 \in \mathbb{N}$ справедливы соотношения

$$x^{\lambda_1}(x^{t_1} - e)w = x^{\lambda_1}(x^{t_1} - e)u + x^{\lambda_1}(x^{t_1} - e)v,$$

$$x^{\lambda_1}(x^{t_1} - e)u \in L_R(F), \quad x^{\lambda_1}(x^{t_1} - e)v \in L_R(G),$$

получаем, что для любых $\lambda_1 \in \mathbb{N}_0$ и $t_1 \in \mathbb{N}$

$$\big(x^{\lambda_1}(x^{t_1} - e)w = (0)\big) \;\Leftrightarrow\; \big(x^{\lambda_1}(x^{t_1} - e)u = (0),\; x^{\lambda_1}(x^{t_1} - e)v = (0)\big).$$

Теперь равенства (41) и (42) следуют из теоремы 21. □

Определение 14. Периодическая последовательность u над кольцом R называется *чисто периодической*, или *реверсивной*, если $\Lambda(u) = 0$, и *вырождающейся*, если $u = (u(0), \dots, u(\lambda - 1), 0, 0, \dots, 0, \dots)$ для некоторого $\lambda \in \mathbb{N}_0$.

Очевидно, что u — чисто периодическая последовательность тогда и только тогда, когда $u \in L_R(x^t - e)$ для некоторого $t \in \mathbb{N}$, и u — вырождающаяся последовательность тогда и только тогда, когда $u \in L_R(x^\lambda)$ для некоторого $\lambda \in \mathbb{N}_0$. Единственная одновременно чисто периодическая и вырождающаяся последовательность — нулевая: $\Lambda((0)) = 0$, $T((0)) = 1$.

Теорема 23. *Любая периодическая последовательность $u \in R^\infty$ однозначно представляется в виде суммы*

$$u = u_0 + u_1, \tag{43}$$

где u_0 — вырождающаяся, u_1 — чисто периодическая последовательности. При этом

$$\Lambda(u) = \Lambda(u_0), \quad T(u) = T(u_1). \tag{44}$$

□ Пусть $\Lambda(u) = \lambda$, $T(u) = t$. Тогда $u \in L_R(x^\lambda(x^t - e))$. Из очевидного соотношения $(x,\, x^t - e) = e$ в силу утверждения 14(а) следует соотношение $(x^\lambda,\, x^t - e) = e$. Отсюда, пользуясь теоремой 15, получаем, что

$$L_R(x^\lambda(x^t - e)) = L_R(x^\lambda) \dotplus L_R(x^t - e), \tag{45}$$

и последовательность u единственным образом представляется в виде

$$u = u_0 + u_1, \quad u_0 \in L_R(x^\lambda), \quad u_1 \in L_R(x^t - e).$$

Это и есть искомое разложение (43). Равенства (44) легко следуют из утверждения 22.

Пусть имеется еще одно разложение $u = v_0 + v_1$, где v_0, v_1 — соответственно вырождающаяся и чисто периодическая последовательности. Тогда по утверждению 22 $\Lambda(v_0) = \Lambda(u) = \lambda$, $T(v_1) = T(u) = t$. Следовательно, $v_0 \in L_R(x^\lambda)$, $v_1 \in L_R(x^t - e)$, и ввиду (45) справедливы равенства $v_0 = u_0$, $v_1 = u_1$. □

Замечание 7. На практике для представления последовательности $u \in L_R(x^\lambda(x^t - e))$ в виде (43) достаточно подобрать $k \in \mathbb{N}$ такое, что $tk \geqslant \lambda$. Тогда $x^{tk}u_0 = (0)$, и из (43) следует, что $x^{tk}u = x^{tk}u_1 = u_1$. Теперь последовательность u_0 находится из равенств $u_0 = u - u_1 = u - x^{tk}u$. Например, для последовательности

$$u = (0\ 0\ 2\ 2\ 1\ \underbrace{3\ 1\ 2\ 0}\ \underbrace{3\ 1\ 2\ 0}\ \ldots)$$

над кольцом $\mathbb{Z}_4$ справедливы соотношения $\Lambda(u) = \lambda = 5$, $T(u) = t = 4$, $t \cdot 2 = 8 > \lambda$. Следовательно,

$$u_1 = x^8 u = (0\ 3\ 1\ 2\ 0\ 3\ 1\ 2\ \ldots),$$
$$u_0 = u - u_1 = (0\ 1\ 1\ 0\ 1\ 0\ 0\ 0\ \ldots).$$

§ 8. ПЕРИОДИЧЕСКИЕ МНОГОЧЛЕНЫ. ПЕРИОДИЧНОСТЬ ЛРП НАД КОНЕЧНЫМ КОЛЬЦОМ

Заметим, что если R — произвольное кольцо, то не любая ЛРП над R периодична, т. е. обращение утверждения 20 неверно. Простейший пример: ЛРП $u = (0, 1, 2, 3, \ldots) \in L_{\mathbb{Z}}((x-1)^2)$. Однако если R — конечное кольцо, то обращение утверждения 20 верно. Доказательство этого факта и методика расчета периода ЛРП над конечным кольцом опираются на следующие результаты.

Определение 15. Многочлен $F(x) \in R[x]$ назовем *периодическим*, если существуют параметры $\lambda \in \mathbb{N}_0$, $t \in \mathbb{N}$ такие, что

$$F(x) \mid x^{\lambda}(x^t - e). \tag{46}$$

При этом наименьшее $t \in \mathbb{N}$, для которого существует $\lambda \in \mathbb{N}_0$, удовлетворяющее условию (46), обозначим через $T(F)$ и назовем *периодом многочлена* $F(x)$, а наименьшее $\lambda \in \mathbb{N}_0$ такое, что $F(x) \mid x^{\lambda}(x^{T(F)} - e)$ обозначим через $\Lambda(F)$ и назовем *дефектом многочлена* $F(x)$. Унитарный периодический многочлен $F(x)$ со свойством $\Lambda(F) = 0$ назовем *реверсивным*.

Связь введенных понятий с понятием периодической последовательности устанавливает

Утверждение 24. *Унитарный многочлен $F(x) \in R[x]$ является периодическим тогда и только тогда, когда периодична последовательность $e^F \in L_R(F)$. Если $F(x)$ — периодический многочлен, то*

$$\Lambda(F) = \Lambda(e^F), \quad T(F) = T(e^F), \tag{47}$$

и любая ЛРП $u \in L_R(F)$ есть периодическая последовательность, для которой

$$\Lambda(u) \leqslant \Lambda(F), \quad T(u) \mid T(F). \tag{48}$$

□ Так как по следствию утверждения 9 $\operatorname{Ann}(e^F) = R[x]F(x)$, то

$$\forall\, \lambda \in \mathbb{N}_0,\ \forall\, t \in \mathbb{N}\colon\ (x^{\lambda}(x^t - e)e^F = (0)) \ \Leftrightarrow\ (F(x) \mid x^{\lambda}(x^t - e)). \tag{49}$$

Отсюда следуют первая часть утверждения и соотношения (47). Пусть $u \in L_R(F)$. Тогда $F(x)u = (0)$, и так как

$$F(x) \mid x^{\Lambda(F)}(x^{T(F)} - e), \quad \text{то} \quad x^{\Lambda(F)}(x^{T(F)} - e)u = (0).$$

Следовательно, u — периодическая последовательность, и по теореме 21 верно (48). □

Следствие 1. *Если $F(x) \in R[x]$ — унитарный периодический многочлен, то*

$$\forall\, \lambda \in \mathbb{N}_0,\ \forall\, t \in \mathbb{N}\colon\ (F(x) \mid x^{\lambda}(x^t - e)) \ \Leftrightarrow\ (\lambda \geqslant \Lambda(F),\ T(F) \mid t).$$

□ Достаточно воспользоваться соотношениями (49), (47) и теоремой 21. □

Следствие 2. *Если $F(x)$, $G(x) \in R[x]$ — унитарные периодические взаимно простые многочлены, то $H(x) = F(x)G(x)$ — периодический многочлен, причем*

$$\Lambda(H) = \max\{\Lambda(F), \Lambda(G)\}, \quad T(H) = [T(F), T(G)].$$

□ Пусть $\lambda = \max\{\Lambda(F), \Lambda(G)\}$, $t = [T(F), T(G)]$. Тогда по следствию 1 многочлен $x^{\lambda}(x^t - e)$ делится на $F(x)$ и $G(x)$, и по утверждению 14(в) $H(x) \mid x^{\lambda}(x^t - e)$. Таким образом, по определению 15 $H(x)$ — периодический многочлен, и по следствию 1 $\Lambda(H) \leqslant \lambda$, $T(x) \mid t$. Наоборот, так как многочлен $x^{\Lambda(H)}(x^{T(H)} - e)$ делится на $H(x) = F(x)G(x)$, то по следствию 1 $\Lambda(H) \geqslant \lambda$ и $T(F) \mid T(H)$, $T(G) \mid T(H)$, т. е. $t \mid T(H)$. □

Замечание 8. Если R — произвольное бесконечное кольцо, и $F(x)$, $G(x) \in R[x]$ — унитарные периодические, но не взаимно простые многочлены, то многочлен $H(x) = F(x)G(x)$ может не быть периодическим. Например, если $R = \mathbb{Q}$, $F(x) = G(x) = x - 1$, то $H(x) = (x-1)^2$ — многочлен с кратным корнем 1, и потому он не делит ни одного из многочленов $x^t - 1$, $t \in \mathbb{N}$. Иная картина имеет место, если R — конечное кольцо.

Теорема 25. *Пусть $F(x)$ — унитарный многочлен степени $m > 0$ над конечным кольцом R. Тогда*

(а) *$F(x)$ — периодический многочлен, причем если $|R|^m > 2$, то*

$$\Lambda(F) + T(F) \leqslant |R|^m - 1; \tag{50}$$

(б) *$F(x)$ — реверсивный многочлен в том и только в том случае, если $F(0) \in R^*$.*

□ (а) Рассмотрим факторкольцо $S = R[x]/F(x)$ и последовательность над S:

$$[e]_F,\ [x]_F,\ \ldots,\ [x^i]_F,\ \ldots\ . \tag{51}$$

Так как S — конечное кольцо, $|S| = |R|^m$, то в последовательности (51) есть повторения, т. е.

$$[x^{\lambda}]_F = [x^{\lambda+t}]_F \tag{52}$$

для некоторых $\lambda \in \mathbb{N}_0$, $t \in \mathbb{N}$. Но равенство (52), очевидно, эквивалентно условию

$$F(x) \mid x^{\lambda}(x^t - e). \tag{53}$$

Следовательно, $F(x)$ — периодический многочлен. Более того, из следствия 1 утверждения 24 и равносильности условий (52) и (53) следует, что $\Lambda(F) + T(F) = k$ — наибольшее натуральное число такое, что элементы кольца S

$$[e]_F,\ [x]_F,\ \ldots,\ [x^{k-1}]_F \tag{54}$$

попарно различны. Поэтому всегда $\Lambda(F) + T(F) \leqslant |S| = |R|^m$.

Покажем, что если $|S| > 2$, то $k \leqslant |S| - 1$. Допустим, что $k > |S| - 1$. Тогда $k = |S|$, и так как элементы (54) попарно различны, то

$$S = \{\, [e]_F,\ [x]_F,\ \ldots,\ [x]_F^{k-1}\}. \tag{55}$$

Так как $[0]_F \in S$, то из (55) следует, что $[0]_F = [x]_F^{k-1}$, $[x]_F$ — делитель нуля в S, и $[e]_F$ — единственный обратимый элемент в S. Но $[e-x]_F$ — также обратимый элемент в S, поскольку

$$[e-x]_F \cdot [e+x+\ldots+x^{k-1}]_F = [e-x^k]_F = [e]_F.$$

Следовательно, $[e-x]_F = [e]_F$, $[x]_F = [0]_F$, и ввиду (55) $S = \{[e]_F, [0]_F\}$, т. е. $|S| = 2$, что противоречит условию.

(б) Если $F(x)$ — реверсивный многочлен, то $x^{T(F)} - e = F(x)G(x)$ для подходящего $G(x) \in R[x]$. Тогда $F(0) \cdot (-G(0)) = e$, и потому $F(0) \in R^*$. Наоборот, так как $F(x)$ имеет вид $F(x) = F(0) + xU(x)$, то из условия $F(0) \in R^*$ очевидно следует, что $(F(x), x) = e$, и по утверждению 14(а) $(F(x), x^\lambda) = e$ для любого $\lambda \in \mathbb{N}$. Тогда, так как $F(x) \mid x^{\Lambda(F)}(x^{T(F)} - e)$, то по утверждению 14(б) $F(x) \mid x^{T(F)} - e$, т. е. $F(x)$ — реверсивный многочлен. $\square$

Следствие. *Если u — ЛРП порядка m над конечным кольцом R и $|R|^m > 2$, то* $\Lambda(u) + T(u) \leqslant |R|^m - 1$.

Замечание 9. При условии $|R|^m = 2$ существует единственный пример, опровергающий неравенство (50) и последнее следствие: $R = \mathbb{Z}_2$, $F(x) = x$, $u = (1, 0, 0, \ldots)$. В этой ситуации $\Lambda(F) = \Lambda(u) = 1$ и $T(F) = T(u) = 1$.

Ниже будет показано, что если R — конечное поле, то неравенство (50) может обращаться в равенство для некоторых многочленов $F(x)$.

§ 9. ВЫЧИСЛЕНИЕ ПЕРИОДА И ДЛИНЫ ПОДХОДА ЛРП НАД КОНЕЧНЫМ ПОЛЕМ

Прежде всего, сведем задачу к изучению минимального многочлена ЛРП.

Утверждение 26. *Если u — ЛРП над конечным полем, то*

$$\Lambda(u) = \Lambda(M_u(x)), \quad T(u) = T(M_u(x)).$$

$\square$ Достаточно заметить, что в силу теоремы 7

$$\forall\, \lambda \in \mathbb{N}_0,\ \forall\, t \in \mathbb{N}\colon\ (x^\lambda(x^t - e)u = (0)) \ \Leftrightarrow\ (M_u(x) \mid x^\lambda(x^t - e)). \quad \square$$

Описание параметров $\Lambda(F)$ и $T(F)$ для произвольного унитарного многочлена $F(x)$ над конечным полем сводится к построению его канонического разложения и вычислению периодов неприводимых сомножителей. Пусть $P = GF(q)$, $q = p^n$, p — простое. Как и в главе 22 (определение 3), для произвольного $F(x) \in P[x]$ определим параметр $O(F)$ как НОК порядков всех ненулевых корней многочлена $F(x)$ в его поле разложения над P и положим $O(F) = 1$, если $F(x) = x^l$, $l \in \mathbb{N}$.

Утверждение 27. *Если $F(x) \in P[x]$ — реверсивный неприводимый многочлен степени m, то $T(F) = O(F)$,*

$$T(F) \mid q^m - 1 \quad \textit{и} \quad T(F) \nmid q^k - 1 \ \textit{ для } \ k \in \overline{1, m-1}. \tag{56}$$

В частности, $(T(F), p) = 1$.

□ Пусть Q — минимальное поле разложения $F(x)$ над P.

Тогда $Q = GF(q^m)$ (теорема 7 главы 22), и если α — корень $F(x)$ в поле Q, то $O(F) = \operatorname{Ord}\alpha$ (следствие 1 теоремы 7 главы 22). Так как $F(x) \mid x^{T(F)} - e$, то $\alpha^{T(F)} = e$ и $O(F) \mid T(F)$.

С другой стороны, $\alpha^{O(F)} = e$ и $(F(x), x^{O(F)} - e) \neq e$. Поскольку $x^{O(F)} - e \in P[x]$ и многочлен $F(x)$ неприводим над P, отсюда следует, что $F(x) \mid x^{O(F)} - e$, т. е. $T(F) \mid O(F)$ и $T(F) = O(F)$.

Так как $\alpha \in Q^*$, то $\operatorname{Ord}\alpha \mid q^m - 1$, т. е. $T(F) \mid q^m - 1$. Наконец, если $T(F) \mid q^k - 1$, где $1 \leqslant k < m$, то $\alpha^{q^k - 1} = e$ и $\alpha^{q^k} = \alpha$, что противоречит следствию 1 теоремы 7 главы 22. □

Из (56) вытекает следующий способ вычисления периода реверсивного неприводимого многочлена $F(x) \in P[x]$ степени $m > 0$.

1. Перебрать все делители t числа $q^m - 1$, не являющиеся делителями чисел $q - 1, \ldots, q^{m-1} - 1$.

2. Для каждого выбранного t проверить условие

$$x^t \equiv e \,(\operatorname{mod} F(x)). \tag{57}$$

Наименьшее из таких t, для которых это условие выполнено, есть $T(F)$. Очевидно, при этом самый большой делитель, — число $t = q^m - 1$, — проверять не надо.

Пример 11. Вычислим период многочлена $F(x) = x^4 + x + 1$ над полем $P = \mathbb{Z}_2$. Так как $F(x)$ неприводим, то можно применить описанный выше алгоритм. Поскольку $2^4 - 1 = 15 = 3 \cdot 5$ и $3 \mid 2^2 - 1$, то нужно проверять условие (57) лишь для $t = 5$. Так как $x^4 \equiv x + 1 \,(\operatorname{mod} F(x))$, то $x^5 \equiv x^2 + x \,(\operatorname{mod} F(x))$ и $x^5 \not\equiv 1 \,(\operatorname{mod} F(x))$. Следовательно, $T(F) = 15$.

Теорема 28. *Если $P = GF(q)$ — поле характеристики p, унитарный многочлен $F(x) \in P[x]$ имеет каноническое разложение*

$$F(x) = x^l G_1(x)^{k_1} \ldots G_s(x)^{k_s}$$

и

$$k = \max\{k_1, \ldots, k_s\}, \tag{58}$$

то справедливы равенства

$$\Lambda(F) = l, \quad T(F) = [T(G_1), \ldots, T(G_s)] \cdot p^c = O(F) \cdot p^c,$$

где параметр $c \in \mathbb{N}_0$ находится из условия

$$p^{c-1} < k \leqslant p^c, \tag{59}$$

т. е. $c =]\log_p k[$.

□ Пусть $H(x) = G_1(x)^{k_1} \ldots G_s(x)^{k_s}$. Тогда по теореме 25 $H(x)$ — реверсивный многочлен, и по следствию 2 утверждения 24

$$\Lambda(F) = \Lambda(x^l) = l, \quad T(F) = T(H).$$

Пусть $G(x) = G_1(x) \dots G_s(x)$. Тогда очевидно, что

$$O(F) = O(G) = [O(G_1), \dots, O(G_s)],$$

и по утверждению 27 и следствию 2 утверждения 24

$$[O(G_1), \dots, O(G_s)] = [T(G_1), \dots, T(G_s)] = T(G).$$

Теперь остается доказать равенство $T(H) = T(G)p^c$.

Так как $G(x) \mid x^{T(G)} - e$, то в силу (58) $H(x) \mid (x^{T(G)} - e)^k$ и в силу (59) $H(x) \mid (x^{T(G)} - e)^{p^c}$. Отсюда, пользуясь равенством

$$(x^{T(G)} - e)^{p^c} = x^{T(G)p^c} - e,$$

получаем: $T(H) \mid T(G)p^c$. Более того, так как $T(G) \mid T(H)$ (поскольку $G(x) \mid H(x)$), то $T(H) = T(G)p^d$, где $d \leqslant c$.

Заметим теперь, что $(T(G), p) = 1$, поскольку по утверждению 27 $(T(G_i), p) = 1$ для $i \in \overline{1, s}$. Следовательно, многочлен $x^{T(G)} - e$ над P взаимно прост со своей производной и потому не имеет кратных множителей в каноническом разложении над P (следствие 2 теоремы 23 главы 9). Поэтому каждый неприводимый делитель многочлена $x^{T(H)} - e = (x^{T(G)} - e)^{p^d}$ имеет в его каноническом разложении кратность p^d, и так как $H(x) \mid x^{T(H)} - e$, то ввиду (58) $k \leqslant p^d$ и ввиду (59) $d \geqslant c$. Следовательно, $d = c$, т. е. $T(H) = T(G)p^c$. $\square$

Пример 12. Пусть $P = GF(p^n)$, и α — элемент из P^* порядка t. Вычислим период и длину подхода биномиальной последовательности $\alpha^{[s]}$. По утверждению 10 ее минимальный многочлен равен $(x - \alpha)^{s+1}$. Следовательно, по утверждению 26, $\alpha^{[s]}$ — чисто периодическая последовательность и $T(\alpha^{[s]}) = T((x - \alpha)^{s+1})$. Так как $T(x - \alpha) = t$, то по теореме 28 $T((x - \alpha)^{s+1}) = tp^c$, где $c = \,]\log_p(s + 1)[$. В частности, для последовательности $\alpha^{[0]} = (e, \alpha, \alpha^2, \dots)$ справедливо равенство $T(\alpha^{[0]}) = \operatorname{Ord}\alpha = t$, а для последовательности биномиальных коэффициентов над P: $e^{[s]} = \left(\binom{s}{0}e, \binom{s}{1}e, \dots, \binom{s}{i}e, \dots\right)$ — равенство $T(e^{[s]}) = p^{\,]\log_p(s+1)[}$. Теми же свойствами обладает сбалансированная биномиальная последовательность $\alpha^{\langle s \rangle}$.

Пример 13. Найдем период и длину подхода ЛРП u над $\mathbb{Z}_2$ с характеристическим многочленом $F(x) = x^8 + x^5 + x^3 + x^2 + x$ и начальным вектором $u[\overline{0, 7}] = (00001010)$. По формуле (11) находим генератор u относительно $F(x)$: $\Phi(x) = x^3 + x + 1$, и по теореме 11(а) — ее минимальный многочлен:

$$M_u(x) = \frac{F(x)}{(F(x),\, \Phi(x))} = x^5 + x^3 + x = x(x^2 + x + 1)^2.$$

Так как $x^2 + x + 1$ — неприводимый многочлен над $\mathbb{Z}_2$ и $T(x^2 + x + 1) = 3$, то по теореме 28 $\Lambda(M_u(x)) = 1$ и $T(M_u(x)) = 3 \cdot 2^1 = 6$. Таким образом, по утверждению 26 $\Lambda(u) = 1$, $T(u) = 6$.

§ 10. ЛРП МАКСИМАЛЬНОГО ПЕРИОДА НАД КОНЕЧНЫМ ПОЛЕМ

1. Пусть $P = GF(q)$ и u — ЛРП ранга m над P (определение 7). Тогда, согласно теореме 25 и утверждению 26, при условии $q^m > 2$ период и длина подхода последовательности u удовлетворяют неравенству $\Lambda(u) + T(u) \leqslant q^m - 1$. В связи с этим представляет естественный интерес изучение следующих последовательностей.

Определение 16. Последовательность u над полем $P = GF(q)$ называется *линейной рекуррентной последовательностью максимального периода над* P, если для некоторого $m \in \mathbb{N}$ последовательность u есть ЛРП ранга m и периода $q^m - 1$.

Очевидно, что при $q^m > 2$ ЛРП максимального периода $q^m - 1$ есть чисто периодическая последовательность, т. е. ее минимальный многочлен реверсивен.

Теорема 29. *Пусть u — ЛРП над полем $P = GF(q)$ с реверсивным минимальным многочленом $M_u(x) = F(x)$ степени m и $q^m > 2$. Тогда следующие утверждения эквивалентны*:

(а) *u — ЛРП максимального периода над P*;

(б) *любая ненулевая ЛРП $v \in L_P(F)$ есть сдвиг последовательности u, т. е. $v = x^k u$ для некоторого $k \in \mathbb{N}$*;

(в) *многочлен $F(x)$ неприводим над P, и его корень α в минимальном поле разложения $Q = GF(q^m)$ над P есть примитивный элемент поля Q, т. е. $F(x)$ — примитивный многочлен над P (см. определение 4 главы 22)*;

(г) $T(F) = q^m - 1$.

□ (а)⇒(б) Так как $T(u) = q^m - 1$, то все последовательности

$$u,\ xu,\ \ldots,\ x^{\tau-1}u, \quad \text{где } \tau = q^m - 1, \tag{60}$$

различны и принадлежат $L_P(F) \setminus \{(0)\}$. Поскольку $|L_P(F) \setminus \{(0)\}| = q^m - 1 = \tau$, то система (60) исчерпывает все множество $L_P(F) \setminus \{(0)\}$, следовательно, ей принадлежит и последовательность v.

(б)⇒(в) Так как ненулевая ЛРП $v \in L_P(F)$ имеет вид $v = x^k u$ и по условию $(M_u(x), x) = e$, то по теореме 11(б) $M_v(x) = M_u(x)$. Таким образом, минимальный многочлен любой ЛРП $v \in L_P(F) \setminus \{(0)\}$ равен $F(x)$, и по следствию теоремы 11 многочлен $F(x)$ неприводим над полем P. Тогда по утверждению 27 получаем $T(F) = O(F) = \operatorname{Ord}\alpha$, и из равенств $T(F) = T(u) = q^m - 1$ следует, что α — примитивный элемент поля Q.

(в)⇒(г) При условии (в) по утверждению 27 $T(F) = \operatorname{Ord}\alpha = q^m - 1$.

Импликация (г)⇒(а) очевидна. □

Замечание 10. Если u — ЛРП максимального периода $q^m - 1$ над полем $P = GF(q)$ и $P < P' = GF(q^t)$, то при $t > 1$ последовательность u уже не является ЛРП максимального периода над полем P', поскольку $T(u) < q^{tm} - 1$.

2. Следующее важное для практических приложений свойство ЛРП u максимального периода $\tau = q^m - 1$ над $P = GF(q)$ показывает, что она в некотором смысле хорошо «имитирует» случайную последовательность элементов поля P, в которой все элементы из P встречаются с одинаковой вероятностью $1/q$.

Зафиксируем числа $i_1, \ldots, i_r \in \overline{0, \tau - 1}$ и элементы $a_1, \ldots, a_r \in P$ и обозначим через $\mathfrak{N}_u\begin{pmatrix} i_1, \ldots, i_r \\ a_1, \ldots, a_r \end{pmatrix}$ число решений $i \in \overline{0, \tau - 1}$, системы уравнений

$$u(i + i_1) = a_1,\ u(i + i_2) = a_2,\ \ldots,\ u(i + i_r) = a_r. \tag{61}$$

Отметим, что если бы последовательность u была отмеченной выше случайной последовательностью, то при достаточно большом τ должно было бы выполняться приблизительное равенство

$$\frac{1}{\tau}\,\mathfrak{N}_u\begin{pmatrix} i_1, \ldots, i_r \\ a_1, \ldots, a_r \end{pmatrix} \approx \left(\frac{1}{q}\right)^r.$$

Оказывается, это равенство (при некоторых ограничениях) выполняется и для ЛРП u.

Теорема 30. *Пусть u — ЛРП максимального периода $\tau = q^m - 1$ над полем $P = GF(q)$ и $0 \leqslant i_1 < i_2 < \ldots < i_r \leqslant m - 1$. Тогда для любых $a_1, \ldots, a_r \in P$ справедливы равенства*:

$$\mathfrak{N}_u\begin{pmatrix} i_1, \ldots, i_r \\ a_1, \ldots, a_r \end{pmatrix} = \begin{cases} q^{m-r}, & \text{если } (a_1, \ldots, a_r) \neq \vec{0}, \\ q^{m-r} - 1, & \text{если } (a_1, \ldots, a_r) = \vec{0}. \end{cases} \tag{62}$$

□ Так как u — ЛРП ранга m и периода τ, то система векторов

$$u[\overline{0, m-1}],\ u[\overline{1, m}],\ \ldots,\ u[\overline{\tau - 1, \tau + m - 2}]$$

не содержит одинаковых векторов и нулевого вектора, следовательно, она совпадает с множеством $P^m \setminus \{\vec{0}\}$. Теперь легко видеть, что число решений $i \in \overline{0, \tau - 1}$ системы уравнений (61) равно числу ненулевых векторов из P^m, у которых координаты с номерами $i_1, \ldots, i_r$ равны соответственно $a_1, \ldots, a_r$. Это число, очевидно, описывается равенствами (62). □

3. Согласно теореме 29 задача построения ЛРП максимального периода $q^m - 1$ над полем $P = GF(q)$ сводится к построению реверсивного многочлена $F(x) \in P[x]$, удовлетворяющего условиям пункта (г) этой теоремы.

Определение 17. Реверсивный многочлен над полем $P = GF(q)$, имеющий степень m и период $q^m - 1$, называется *многочленом максимального периода* (или *примитивным* многочленом) над полем P.

Заметим, что ввиду эквивалентности утверждений (в) и (г) теоремы 29 любой многочлен, удовлетворяющий условиям определения 17, имеет в поле $Q = GF(q^m)$ m

корней, каждый из которых есть примитивный элемент Q, поэтому число многочленов максимального периода q^m-1 над Q равно $\dfrac{1}{m}\varphi(q^m-1)$, где φ — функция Эйлера.

Построение многочлена максимального периода над полем P осуществляется, как правило, путем перебора неприводимых многочленов $F(x)$ степени m над полем P (см. § 5 главы 22) с проверкой условия $T(F)=q^m-1$ по следующему критерию.

Утверждение 31. *Неприводимый многочлен $F(x)\in P[x]$ степени $m\geqslant 1$ является многочленом максимального периода над полем P тогда и только тогда, когда $F(x)\neq x$ и для каждого собственного простого делителя π числа q^m-1 выполняется условие*

$$x^{\frac{q^m-1}{\pi}}\not\equiv e\,(\mathrm{mod}\,F(x)). \tag{63}$$

□ Пусть $T(F)=t$. Так как $F(x)$ неприводим над $P=GF(q)$, то $t\mid q^m-1$, и условие $t<q^m-1$ равносильно тому, что для некоторого собственного простого делителя π числа q^m-1 выполняется соотношение $t\mid\dfrac{q^m-1}{\pi}$, т. е. не выполняется условие (63). □

Следствие. *Если 2^m-1 — простое число, то любой неприводимый над $GF(2)$ многочлен степени m есть многочлен максимального периода.*

Пример 14. Рассмотрим многочлен $F(x)=x^3-x-2$ над полем $P=GF(3)$. Так как $F(x)$ не имеет корней в P, то он неприводим. Число $q^m-1=3^3-1=26$ имеет простые делители 2 и 13. Очевидно, что

$$x^{\frac{3^3-1}{13}}=x^2\not\equiv 1\,(\mathrm{mod}\,F(x)).$$

Далее, из сравнений по модулю $F(x)$

$$x^3\equiv x+2,\quad x^4\equiv x^2+2x,\quad x^8\equiv(x^2+2x)^2\equiv 2x^2+2$$

находим

$$\begin{aligned}x^{\frac{3^3-1}{2}}=x^{13}=x\cdot x^4\cdot x^8&\equiv x(x^2+2x)(2x^2+2)\equiv\\&\equiv 2x^2(2x^2+2x+1)\equiv x^4+x^3+2x^2=2\not\equiv 1.\end{aligned}$$

Следовательно, x^3-x-2 — многочлен максимального периода над полем $GF(3)$.

Пример 15. Числа $2^2-1=3$, $2^3-1=7$, $2^5-1=31$ простые. Следовательно, все неприводимые многочлены степеней 2, 3, 5 над полем $GF(2)$ являются многочленами максимального периода. Например, такими будут многочлены

$$x^2+x+1,\quad x^3+x+1,\quad x^3+x^2+1,\quad x^5+x^2+1.$$

Последний многочлен неприводим, потому что он не имеет корней в $GF(2)$ и не делится на единственный неприводимый над $GF(2)$ многочлен второй степени x^2+x+1.

Как уже отмечалось в примере 4 главы 22, простые числа вида 2^m-1 называются числами Мерсенна. Таковы, например, числа 2^m-1 при $m\in\{2,3,5,7,13,17,19,31,127\}$. До сих пор неизвестно, конечно ли множество чисел Мерсенна. В 2013 г. энтузиастами проекта GIMPS было найдено 48-е число Мерсенна $2^{57885161}-1$.

§ 11. ЦИКЛОВОЙ ТИП СЕМЕЙСТВА ЛРП С РЕВЕРСИВНЫМ ХАРАКТЕРИСТИЧЕСКИМ МНОГОЧЛЕНОМ НАД КОНЕЧНЫМ КОЛЬЦОМ

1. Пусть R — конечное (коммутативное) кольцо с единицей и $F(x) \in R[x]$ — унитарный многочлен. Определим на $L_R(F)$ бинарное отношение $\sim$ условием

$$\forall\, u, v \in L_R(F):\ (u \sim v \ \Leftrightarrow\ \exists\, t \in \mathbb{N}_0\ (v = x^t u)).$$

Очевидно, что отношение $\sim$ рефлексивно и транзитивно при любом $F(x)$.

Утверждение 32. *Отношение $\sim$ на $L_R(F)$ есть отношение эквивалентности тогда и только тогда, когда $F(x)$ — реверсивный многочлен.*

□ Достаточно доказать, что реверсивность $F(x)$ равносильна симметричности отношения $\sim$.

Пусть $\sim$ — симметричное отношение. Рассмотрим последовательность $e^F \in L_R(F)$. Так как по определению $e^F \sim xe^F$, то в силу симметричности $\sim$ также и $xe^F \sim e^F$, т. е. $e^F = x^{t+1}e^F$ для некоторого $t \in \mathbb{N}_0$. Но в таком случае $(x^{t+1} - e)e^F = (0)$, т. е. по теореме 21 e^F — чисто периодическая последовательность. Отсюда по утверждению 24 следует, что $\Lambda(F) = \Lambda(e^F) = 0$, и $F(x)$ — реверсивный многочлен.

Наоборот, пусть $F(x)$ — реверсивный многочлен, $u, v \in L_R(F)$ и $u \sim v$, т. е. $v = x^t u$, $t \in \mathbb{N}_0$. Докажем, что $v \sim u$. Так как $F(x)$ — реверсивный многочлен, то по утверждению 24 u — чисто периодическая последовательность, т. е. $x^{T(u)}u = u$. Выберем $k \in \mathbb{N}$ так, что $kT(u) \geqslant t$. Тогда для $t_1 = kT(u) - t$ имеем

$$x^{t_1}v = x^{t_1+t}u = x^{kT(u)}u = u.$$

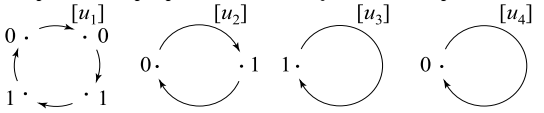
Следовательно, $v \sim u$. □

Определение 18. Для реверсивного многочлена $F(x) \in R[x]$ классы, на которые семейство $L_R(F)$ разбивается отношением $\sim$, называют *циклами* семейства $L_R(F)$. Если $u, v \in L_R(F)$ и $u \sim v$, то говорят, что *последовательности u и v лежат на одном цикле*. Класс $[u] = \{v \in L_R(F):\ v \sim u\}$ называют *циклом последовательности u* (или циклом, порождаемым u), а его мощность $|[u]|$ — *длиной* этого *цикла*.

Пример 16. Для многочлена $F(x) = x^3 + x^2 + x + 1$ над полем $P = \mathbb{Z}_2$ множество $L_P(F)$ разбивается на 4 цикла, которые порождаются последовательностями $u_1 = (00110011\ldots)$, $u_2 = (0101\ldots)$, $u_3 = (111\ldots)$, $u_4 = (0)$ и имеют соответственно вид:

$$[u_1] = \{(00110011\ldots),\ (01100110\ldots),\ (11001100\ldots),\ (10011001\ldots)\},$$
$$[u_2] = \{(0101\ldots),\ (1010\ldots)\},$$
$$[u_3] = \{(111\ldots)\},$$
$$[u_4] = \{(000\ldots)\}.$$

Эти циклы можно изобразить графически следующим образом:



Утверждение 33. *Пусть $F(x)$ — реверсивный многочлен над R и $u \in L_R(F)$. Тогда длина цикла $[u]$ равна $T(u)$, и для любой последовательности $v \in [u]$ справедливо равенство* $\mathrm{Ann}(v) = \mathrm{Ann}(u)$.

□ Очевидно, что если $T(u) = t$, то $[u] = \{u, xu, \ldots, x^{t-1}u\}$, т. е. $|[u]| = t$. Если $v \in [u]$, то $v = x^s u$ для некоторого $s \in \mathbb{N}$. Поэтому, если $G(x) \in \mathrm{Ann}(u)$, то $G(x)v = (0)$, т. е. $\mathrm{Ann}(u) \subset \mathrm{Ann}(v)$. Обратное включение следует из того, что $u \in [v]$. □

Таким образом, если для реверсивного $F(x) \in R[x]$ через $N_F^{(t)}$ обозначить количество ЛРП $u \in L_R(F)$ со свойством $T(u) = t$, а через $C_F^{(t)}$ — количество циклов длины t в $L_R(F)$, то $N_F^{(t)} = t \cdot C_F^{(t)}$.

Определение 19. Для реверсивного многочлена $F(x)$ над конечным кольцом R *цикловым типом многочлена* $F(x)$ (или *семейства* $L_R(F)$) назовем многочлен с целыми коэффициентами

$$\mathcal{C}_F(y) = \sum_{t \geqslant 1} C_F^{(t)} y^t.$$

Пример 17. Пусть $P = GF(q)$ и $F(x) \in P[x]$ — неприводимый реверсивный многочлен степени m и периода $T(F) = \tau$. Вычислим цикловой тип множества $L_P(F)$. Если $u \in L_P(F) \setminus \{(0)\}$, то по следствию теоремы 11 $M_u(x) = F(x)$ и по утверждениям 26, 27 $T(u) = \tau$, $\tau \mid q^m - 1$. Таким образом, множество $L_P(F) \setminus \{(0)\}$ разбивается на $\dfrac{q^m - 1}{\tau}$ циклов длины τ, и так как $[(0)]$ — цикл длины 1, то цикловой тип $L_P(F)$ имеет вид

$$\mathcal{C}_F(y) = \begin{cases} y + \dfrac{q^m - 1}{\tau}\, y^\tau, & \text{если } \tau > 1, \\ q^m \cdot y^1, & \text{если } \tau = 1. \end{cases}$$

Пример 18. Если $R = \mathbb{Z}_4$ и $F(x) = x - 3 \in R[x]$, то семейство $L_R(F)$ состоит из четырех последовательностей

$$u_1 = (0),\ u_2 = (2, 2\ldots),\ u_3 = (1, 3, 1, 3, \ldots),\ u_4 = (3, 1, 3, 1, \ldots)$$

и разбивается на 3 цикла: $[u_1]$, $[u_2]$, $[u_3] = [u_4]$. Цикловой тип этого семейства: $\mathcal{C}_{x-3}(y) = 2y + y^2$.

2. При вычислении циклового типа реверсивного многочлена часто оказываются полезными следующие результаты.

Определение 20. *Композицией многочленов* $a(y) = \sum_{i \geqslant 1} a_i y^i$ и $b(y) = \sum_{j \geqslant 1} b_j y^j$ над $\mathbb{Z}$ назовем многочлен $c(y) = a(y) * b(y)$, определяемый равенствами

$$c(y) = \sum_{t \geqslant 1} c_t y^t, \quad c_t = \sum_{i,j \in \mathbb{N},\, [i,j] = t} a_i b_j\, (i, j) \quad \text{для} \quad t \in \mathbb{N},$$

где (i, j) и $[i, j]$ — соответственно НОД и НОК чисел i и j. Иначе говоря,

$$c(y) = \sum_{i \geqslant 1} \sum_{j \geqslant 1} a_i b_j (i, j) y^{[i,j]} = \sum_{i \geqslant 1} \sum_{j \geqslant 1} a_i b_j (y^i * y^j). \tag{64}$$

Пусть $\mathbb{Z}_1[y]$ — совокупность всех многочленов над $\mathbb{Z}$ с нулевым свободным членом. Тогда, очевидно, $*$ — внутренняя операция на $\mathbb{Z}_1[y]$, и справедливо

Утверждение 34. *Алгебра $(\mathbb{Z}_1[y], *, +)$ есть коммутативное кольцо с единицей y. Если $\mathcal{C}^{(s)}(y) = \sum_{t\geqslant 1} c_t^{(s)} y^t \in \mathbb{Z}_1[y]$ для $s \in \overline{1,r}$, то*

$$\mathcal{C}^{(1)}(y) * \ldots * \mathcal{C}^{(r)}(y) = \sum_{t\geqslant 1}\left(\sum_{\substack{t_1,\ldots,t_r\in\mathbb{N}\\ [t_1,\ldots,t_r]=t}} \frac{t_1\ldots t_r}{[t_1,\ldots,t_r]}\, c_{t_1}^{(1)}\ldots c_{t_r}^{(r)}\right) y^t. \tag{65}$$

□ Коммутативность операции $*$ и ее дистрибутивность относительно сложения легко выводятся из (64). Поэтому для доказательства ассоциативности операции $*$ ввиду (64) достаточно доказать, что для любых $k, l, m \in \mathbb{N}$ выполняется равенство

$$(y^k * y^l) * y^m = y^k * (y^l * y^m). \tag{66}$$

Пользуясь определением 20, получаем

$$(y^k * y^l) * y^m = (k,l)\, y^{[k,l]} * y^m = ([k,l],m)(k,l)\, y^{[[k,l],m]} =$$

$$= \frac{[k,l]\cdot m}{[k,l,m]}\,(k,l)\, y^{[k,l,m]} = \frac{klm}{[k,l,m]}\, y^{[k,l,m]}.$$

Аналогично доказывается равенство

$$y^k * (y^l * y^m) = \frac{klm}{[k,l,m]}\, y^{[k,l,m]},$$

откуда и следует равенство (66).

Для доказательства равенства (65) ввиду (64) достаточно показать, что для любых $t_1, \ldots, t_r \in \mathbb{N}$ справедливо равенство

$$y^{t_1} * \ldots * y^{t_r} = \frac{t_1\ldots t_r}{[t_1,\ldots,t_r]}\, y^{[t_1,\ldots,t_r]}. \tag{67}$$

При $r = 2$ оно следует из определения 20, а при $r = 3$ доказано выше. Пусть $n > 3$ и для $r < n$ равенство (67) справедливо. Тогда при $r = n$, пользуясь предположением индукции и определением 20, получаем

$$y^{t_1} * \ldots * y^{t_r} = \frac{t_1\ldots t_{r-1}}{[t_1,\ldots,t_{r-1}]}\, y^{[t_1,\ldots,t_{r-1}]} * y^{t_r} =$$

$$= ([t_1,\ldots,t_{r-1}],\, t_r)\cdot \frac{t_1\ldots t_{r-1}}{[t_1,\ldots,t_{r-1}]}\, y^{[t_1,\ldots,t_r]} =$$

$$= \frac{[t_1,\ldots,t_{r-1}]\cdot t_r}{[[t_1,\ldots,t_{r-1}],\, t_r]} \cdot \frac{t_1\ldots t_{r-1}}{[t_1,\ldots,t_{r-1}]}\, y^{[t_1,\ldots,t_r]} = \frac{t_1\ldots t_r}{[t_1,\ldots,t_r]}\, y^{[t_1,\ldots,t_r]}. \quad \square$$

Теорема 35. *Пусть R — конечное кольцо и $F_1(x)$, $F_2(x)$ — взаимно простые реверсивные многочлены над R. Тогда $F(x) = F_1(x)F_2(x)$ — реверсивный многочлен, и его цикловой тип вычисляется по формуле*

$$\mathcal{C}_F(y) = \mathcal{C}_{F_1}(y) * \mathcal{C}_{F_2}(y).$$

□ Реверсивность многочлена $F(x)$ следует из теоремы 25(б). По определению 19 $\mathcal{C}_F(y) = \sum_{t\geqslant 1} C_F^{(t)} y^t$, где $tC_F^{(t)} = N_F^{(t)}$ — число различных ЛРП $u \in L_R(F)$, имеющих период t. Подсчитаем число $N_F^{(t)}$ другим способом. По теореме 15 каждая ЛРП $u \in L_R(F)$ однозначно представляется в виде суммы $u = u_1 + u_2$, где $u_s \in L_R(F_s)$ для $s \in \overline{1,2}$. При этом если $T(u) = t$, то по утверждению 22(в) $T(u_1) = t_1$, $T(u_2) = t_2$ и $[t_1, t_2] = t$. Наоборот, если $u_s \in L_R(F_s)$, $s \in \overline{1,2}$, — последовательности, удовлетворяющие трем последним равенствам, то $u = u_1 + u_2$ — ЛРП из $L_R(F)$ периода t. Следовательно,

$$N_F^{(t)} = \sum_{\substack{t_1,t_2\in\mathbb{N}\\ [t_1,t_r]=t}} N_{F_1}^{(t_1)} N_{F_2}^{(t_2)}. \tag{68}$$

Поскольку $N_{F_s}^{(t_s)} = t_s C_{F_s}^{(t_s)}$, то из (68) получаем

$$t \cdot C_F^{(t)} = \sum_{\substack{t_1,t_2\in\mathbb{N}\\ [t_1,t_2]=t}} C_F^{(t_1)} C_F^{(t_2)} \cdot t_1 t_2.$$

Отсюда, ввиду соотношения $t_1 t_2 = t \cdot (t_1, t_2)$, следует равенство

$$C_F^{(t)} = \sum_{[t_1,t_2]=t} C_{F_1}^{(t_1)} C_{F_2}^{(t_2)} \cdot (t_1, t_2),$$

которое по определению 20 и означает, что $\mathcal{C}_F(y) = \mathcal{C}_{F_1}(y) * \mathcal{C}_{F_2}(y)$. □

Пример 19. Пусть $P = \mathbb{Z}_2$ и $F(x) = (x^2 + x + 1)(x^4 + x^3 + x^2 + x + 1) \in P[x]$. Найдем цикловой тип семейства $L_P(F)$. Пользуясь результатом примера 17, получаем, что неприводимые многочлены $F_1(x) = x^2 + x + 1$ и $F_2(x) = x^4 + x^3 + x^2 + x + 1$ имеют цикловые типы соответственно

$$\mathcal{C}_{F_1}(y) = y + y^3, \quad \mathcal{C}_{F_2}(y) = y + 3y^5.$$

Так как $(F_1(x),\, F_2(x)) = 1$, то по теореме 35

$$\mathcal{C}_F(y) = \mathcal{C}_{F_1}(y) * \mathcal{C}_{F_2}(y) = y + y^3 + 3y^5 + 3y^{15}.$$

3. Теперь задача описания циклового типа произвольного реверсивного многочлена над конечным полем сводится к описанию циклового типа примарного многочлена. Последний выглядит следующим образом.

Теорема 36. *Пусть $P = GF(q)$ — поле характеристики p и $G(x) \in P[x]$ — реверсивный неприводимый многочлен степени m и периода τ. Тогда*

$$\mathcal{C}_G(y) = y + \frac{q^m - 1}{\tau}\, y^\tau,$$

и для любого $k > 1$

$$\mathcal{C}_{G^k}(y) = y + \frac{q^m - 1}{\tau}\, y^\tau + \sum_{\lambda=1}^{l-1} \frac{q^{mp^\lambda} - q^{mp^{\lambda-1}}}{\tau \cdot p^\lambda}\, y^{\tau p^\lambda} + \frac{q^{mk} - q^{mp^{l-1}}}{\tau \cdot p^l}\, y^{\tau p^l}, \qquad (69)$$

где $l =]\log_p k[$.

□ Докажем индукцией по k равенство

$$\mathcal{C}_{G^k}(y) = y + \sum_{t=1}^{k} \frac{q^{mt} - q^{m(t-1)}}{\tau \cdot p^{\lambda_t}}\, y^{\tau p^{\lambda_t}}, \qquad (70)$$

где $\lambda_t =]\log_p t[$. Для $k = 1$ оно совпадает с первым из утверждаемых теоремой 36 равенств и уже выведено в примере 17. Пусть $n > 1$, и для всех $k < n$ равенство (70) верно. Докажем его для $k = n$. Рассмотрим в $L_P(G^n)$ подмножество $L_P^*(G^n)$, состоящее из всех ЛРП u, для которых $G(x)^n$ — не только характеристический, но и минимальный многочлен. Тогда очевидны соотношения

$$L_P(G^n) = L_P(G^{n-1}) \cup L_P^*(G^n), \quad L_P(G^{n-1}) \cap L_P^*(G^n) = \varnothing, \qquad (71)$$

из которых следует, что

$$|L_P^*(G^n)| = |L_P(G^n)| - |L_P(G^{n-1})| = q^{mn} - q^{m(n-1)}.$$

Кроме того, так как по утверждению 33 все ЛРП из $L_P(G^n)$, принадлежащие одному циклу, имеют равные минимальные многочлены, то для любой ЛРП $u \in L_P^*(G^n)$ справедливо включение $[u]_\sim \subset L_P^*(G^n)$. Следовательно, $L_P^*(G^n)$ есть объединение некоторого числа N циклов длины $T(G^n) = \tau p^{\lambda_n}$, и

$$N = \frac{|L^*(G^n)|}{\tau \cdot p^{\lambda_n}} = \frac{q^{mn} - q^{m(n-1)}}{\tau \cdot p^{\lambda_n}}.$$

Теперь из (71), очевидно, следует равенство

$$\mathcal{C}_{G^n}(y) = \mathcal{C}_{G^{n-1}}(y) + \frac{q^{mn} - q^{m(n-1)}}{\tau \cdot p^{\lambda_n}}\, y^{\tau p^{\lambda_n}}.$$

Отсюда, пользуясь тем, что (70) верно для $k = n - 1$, получаем равенство (70) для $k = n$.

Для завершения доказательства теоремы остается заметить, что равенство (69) получается из (70) суммированием коэффициентов при одинаковых степенях y, поскольку для слагаемых из (70) справедливы соотношения

$$(\lambda_t = 0) \;\Leftrightarrow\; (t = 0),$$

для каждого $\lambda \in \overline{1,\, l-1}$:

$$(\lambda_t = \lambda) \;\Leftrightarrow\; (\lambda - 1 < \log_p t \leqslant \lambda) \;\Leftrightarrow\; (t \in \overline{p^{\lambda-1}+1,\, p^{\lambda}})$$

и, наконец,

$$(\lambda_t = l) \;\Leftrightarrow\; (t \in \overline{p^{l-1}+1,\, k}). \quad \square$$

§ 12. ЛРП НАД КОЛЬЦАМИ ВЫЧЕТОВ

В этом параграфе дается описание простейших свойств ЛРП над кольцом вычетов $R = \mathbb{Z}/M$. Указывается методика оценки периодов таких ЛРП и излагаются некоторые сведения о ЛРП максимально возможного периода (при данном ранге m) над примарным кольцом вычетов $R = \mathbb{Z}/p^n$, где p — простое.

1. Сведем все задачи к изучению многочленов и ЛРП над примарными кольцами вычетов. Пусть каноническое разложение числа M есть $M = p_1^{n_1} \dots p_k^{n_k}$. Положим $R_s = \mathbb{Z}/p_s^{n_s}$ для $s \in \overline{1,k}$. Согласно следствию теоремы 32 главы 20 кольцо $R = \mathbb{Z}/M$ изоморфно внешней прямой сумме $R_1 \oplus \dots \oplus R_k$. При этом изоморфизм

$$\varphi\colon R \to R_1 \oplus \dots \oplus R_k \tag{72}$$

устанавливается следующим образом: если $r \in R$ и $r = [a]_M$ — класс элементов, сравнимых с a по модулю M, то

$$\varphi(r) = (r^{(1)},\, \dots,\, r^{(k)}), \quad \text{где } r^{(s)} = [a]_{p_s^{n_s}} \text{ для } s \in \overline{1,k}. \tag{73}$$

Этот изоморфизм можно продолжить до изоморфизма кольца многочленов $\widehat{\varphi}\colon R[x] \to$ $\to R_1[x] \oplus \dots \oplus R_k[x]$ следующим образом: если $F(x) \in R[x]$ и $F(x) = \sum_{i \geqslant 0} f_i x^i$, то

$$\widehat{\varphi}(F(x)) = (F^{(1)}(x),\, \dots,\, F^{(k)}(x)), \tag{74}$$

где $F^{(s)}(x) = \sum_{i \geqslant 0} f_i^{(s)} x^i$ для $s \in \overline{1,k}$.

Для удобства элемент $r^{(s)}$ из (73) и многочлен $F^{(s)}(x)$ из (74) будем называть *компонентой в кольце* R_s (в кольце $R_s[x]$) или просто *s-й компонентой* соответственно элемента r и многочлена $F(x)$.

Перечислим некоторые важные в дальнейшем простейшие свойства изучаемых разложений колец R и $R[x]$:

1) если $e = [1]_M$ — единица кольца R, то ее компонента $e^{(s)} = [1]_{p_s^{n_s}}$ — единица кольца R_s;

2) элемент $r \in R$ обратим тогда и только тогда, когда все его компоненты $r^{(s)}$ обратимы;

3) многочлен $F(x) \in R[x]$ унитарен тогда и только тогда, когда все его компоненты $F^{(s)}(x)$ унитарны и имеют равные степени;

4) многочлен $H(x) \in R[x]$ делится на $F(x) \in R[x]$ тогда и только тогда, когда $F^{(s)}(x) \mid H^{(s)}(x)$ для $s \in \overline{1,k}$.

Напомним, что по теореме 25(а) любой унитарный многочлен над кольцом R является периодическим.

Утверждение 37. *Для любого унитарного многочлена $F(x) \in \mathbb{Z}/M[x]$ справедливы равенства*

$$\Lambda(F) = \max\{\Lambda(F^{(1)}), \ldots, \Lambda(F^{(k)})\}, \quad T(F) = [T(F^{(1)}), \ldots, T(F^{(k)})].$$

В частности, многочлен $F(x)$ является реверсивным тогда и только тогда, когда все его компоненты $F^{(s)}(x)$ являются реверсивными многочленами.

□ Выберем произвольно $\lambda \in \mathbb{N}_0$ и $t \in \mathbb{N}$ и рассмотрим многочлен $H(x) = x^\lambda(x^t - e) = ex^{\lambda+t} - ex^\lambda \in R[x]$. Его компоненты имеют вид $H^{(s)}(x) = e^{(s)}x^{\lambda+t} - e^{(s)}x^\lambda = x^\lambda(x^t - e^{(s)}) \in R_s[x]$ для $s \in \overline{1,k}$. Из сделанных выше замечаний следует, что

$$(F(x) \mid x^\lambda(x^t - e)) \;\Leftrightarrow\; (F^{(s)}(x) \mid x^\lambda(x^t - e^{(s)}) \text{ для } s \in \overline{1,k}).$$

Теперь остается воспользоваться определением 15 и следствием 1 утверждения 24. □

Пример 20. Вычислим период и длину дефект многочлена $F(x) = x^5 + 10x^4 + 9x + 7$ над кольцом $R = \mathbb{Z}/15$. Так как $(7, 15)=1$, то сразу можно утверждать, что $F(x)$ — реверсивный многочлен, т. е. $\Lambda(F) = 0$. Разложение кольца R на примарные компоненты имеет вид

$$R \cong R_1 \oplus R_2, \quad \text{где} \quad R_1 = \mathbb{Z}/3, \; R_2 = \mathbb{Z}/5,$$

соответствующие этому разложению компоненты многочлена $F(x)$ таковы:

$$F^{(1)}(x) = x^5 + x^4 + 1 = (x^3 + 2x + 1)(x - 1)^2 \in \mathbb{Z}/3[x],$$
$$F^{(2)}(x) = x^5 + 4x + 2 \in \mathbb{Z}/5[x].$$

Многочлен $F^{(1)}(x) = x^3+2x+1$ над полем $\mathbb{Z}/3$ неприводим и имеет период $3^3-1 = 26$. Поэтому

$$T(F^{(1)}(x)) = [T(x^3 + 2x + 1), T((x - 1)^2)] = [26, 3] = 2 \cdot 3 \cdot 13.$$

Многочлен $F^{(2)}(x)$ над полем $\mathbb{Z}/5$ неприводим и $T(F^{(2)}) = 5^5 - 1 = 4 \cdot 11 \cdot 71$. Окончательно получаем:

$$T(F) = [T(F^{(1)}), T(F^{(2)})] = 4 \cdot 3 \cdot 11 \cdot 13 \cdot 71.$$

Замечание 11. В условиях утверждения 37 из того, что $\deg F(x) = m$ и многочлен $F(x)$ имеет максимально возможный период среди всех многочленов степени m над $\mathbb{Z}/M$, вообще говоря, не следует, что каждая его компонента $F^{(s)}(x)$ имеет максимально возможный период среди всех многочленов степени m над $\mathbb{Z}/p_s^{n_s}$. Так, в условиях примера 20, если $G(x) \in R[x]$ — многочлен степени 5, компоненты которого $G^{(1)}(x)$, $G^{(2)}(x)$ имеют максимальные периоды над полями соответственно $\mathbb{Z}/3$ и $\mathbb{Z}/5$, то $T(G^{(1)}) = 3^5 - 1 = 2 \cdot 11^2$, $T(G^{(2)}) = 5^5 - 1 = 4 \cdot 11 \cdot 71$ и $T(G) = 4 \cdot 11^2 \cdot 71$. Последняя величина меньше периода многочлена $F(x)$ из примера 20.

Заметим теперь, что изоморфизм (72) может быть продолжен до изоморфизма абелевых групп

$$\widetilde{\varphi}\colon R^\infty \to R_1^\infty \oplus \ldots \oplus R_k^\infty, \tag{75}$$

ставящего в соответствие последовательности $u \in R^\infty$ набор последовательностей

$$\widetilde{\varphi}(u) = (u^{(1)}, \ldots, u^{(k)}), \quad u^{(s)} \in R_s^\infty, \quad s \in \overline{1,k},$$

в котором i-й член $u^{(s)}(i)$ последовательности $u^{(s)}$ есть s-я компонента i-го члена $u(i)$ последовательности u, т. е.

$$\widetilde{\varphi}(u)(i) = (u^{(1)}(i), \ldots, u^{(k)}(i)) = \varphi(u(i)).$$

Утверждение 38. *Пусть $u \in R^\infty$. Тогда при изоморфизме* (75) *справедливы следующие утверждения*:

(а) *последовательность u есть ЛРП с характеристическим многочленом $F(x) \in R[x]$ тогда и только тогда, когда каждая ее компонента $u^{(s)}$ есть ЛРП с характеристическим многочленом $F^{(s)}(x)$*;

(б) *u — периодическая последовательность тогда и только тогда, когда каждая ее компонента $u^{(s)}$ — периодическая последовательность. Если u — периодическая последовательность, то*

$$\Lambda(u) = \max\{\Lambda(u^{(1)}), \ldots, \Lambda(u^{(k)})\}, \quad T(u) = [T(u^{(1)}), \ldots, T(u^{(k)})].$$

□ (а) Легко видеть, что $\widetilde{\varphi}(F(x)u) = (F^{(1)}(x)\,u^{(1)}, \ldots, F^{(k)}(x)\,u^{(k)})$. Поэтому

$$(F(x)u = (0)) \;\Leftrightarrow\; (F^{(s)}(x)\,u^{(s)} = (0) \;\text{ для }\; s \in \overline{1,k}).$$

Утверждение (б) легко следует из (а), если взять $F(x) = x^\lambda(x^t - e)$. □

Следствие. *Для любого унитарного многочлена $F(x) \in R[x]$ имеет место изоморфизм абелевых групп*:

$$L_R(F) \cong L_{R_1}(F^{(1)}) \oplus \ldots \oplus L_{R_k}(F^{(k)}).$$

Если $F(x)$ — реверсивный многочлен, то цикловой тип $\mathcal{C}_F(y)$ семейства $L_R(F)$ (см. определение 19) *может быть вычислен по формуле*

$$\mathcal{C}_F(y) = \mathcal{C}_{F^{(1)}}(y) * \ldots * \mathcal{C}_{F^{(k)}}(y). \tag{76}$$

□ Первое утверждение следствия вытекает из изоморфизма (75) и утверждения 38(а). Равенство (76) доказывается точно так же, как равенство теоремы 35. □

Пример 21. В условиях примера 20 найдем период ЛРП $u \in L_R(F)$ с начальным вектором $u[\overline{0,4}] = (66011)$. Начальные векторы компонент u над полями $R_1 = \mathbb{Z}/3$ и $R_2 = \mathbb{Z}/5$ имеют соответственно вид $u^{(1)}[\overline{0,4}] = (00011)$, $u^{(2)}[\overline{0,4}] = (11010)$. ЛРП $u^{(1)}$

над R_1 имеет характеристический многочлен $F^{(1)}(x) = x^5 + x^4 + 1$, и ее генератор относительно $F^{(1)}(x)$ есть $\Phi^{(1)}(x) = x + 2$. Отсюда получаем:

$$M_{u^{(1)}}(x) = \frac{F^{(1)}(x)}{(F^{(1)}(x),\, \Phi^{(1)}(x))} = (x^3 + 2x + 1)(x - 1),$$

$$T(u^{(1)}) = T((x^3 + 2x + 1)(x - 1)) = T(x^3 + 2x + 1) = 26.$$

Последовательность $u^{(2)}$ над R_2 есть ЛРП с неприводимым характеристическим многочленом $F^{(2)}(x) = x^5 + 4x + 2$, и так как $u^{(2)} \neq (0)$, то $M_{u^{(2)}}(x) = F^{(2)}(x)$, $T(u^{(2)}) = T(F^{(2)}) = 5^5 - 1$. Окончательно находим:

$$T(u) = [T(u^{(1)}),\, T(u^{(2)})] = [26,\, 5^5 - 1] = 4 \cdot 11 \cdot 13 \cdot 71.$$

Пример 22. Вычислим цикловой тип $\mathcal{C}_F(y)$ семейства $L_R(F)$ из примера 20. По следствию из утверждения 38 $\mathcal{C}_F(y) = \mathcal{C}_{F^{(1)}}(y) * \mathcal{C}_{F^{(2)}}(y)$. По теореме 35 справедливо равенство $\mathcal{C}_{F^{(1)}}(y) = \mathcal{C}_G(y) * \mathcal{C}_H(y)$, где $G(x) = x^3 + 2x + 1$, $H(x) = (x - 1)^2$ — многочлены над $R_1 = \mathbb{Z}/3$. Так как $G(x)$ — многочлен максимального периода 26 над R_1, то $\mathcal{C}_G(y) = 1y^1 + 1y^{26}$. Цикловой тип многочлена $H(x)$, как легко проверить, имеет вид $\mathcal{C}_H(y) = 3y^1 + 2y^3$. Таким образом,

$$\mathcal{C}_{F^{(1)}}(y) = (1y + 1y^{26}) * (3y^1 + 2y^3) = 3y^1 + 2y^3 + 3y^{26} + 2y^{2\cdot 3\cdot 13}.$$

Так как $F^{(2)}(x)$ — многочлен максимального периода $4 \cdot 11 \cdot 71$ над кольцом $R_2 = \mathbb{Z}/5$, то $\mathcal{C}_{F^{(2)}}(y) = 1y^1 + 1y^{4\cdot 11\cdot 71}$. Окончательно получаем:

$$\begin{aligned}\mathcal{C}_F(y) &= (3y^1 + 2y^3 + 3y^{2\cdot 13} + 2y^{2\cdot 3\cdot 13}) * (1y^1 + 1y^{4\cdot 11\cdot 71}) = \\ &= 3y^1 + 3y^{4\cdot 11\cdot 71} + 2y^3 + 2y^{3\cdot 4\cdot 11\cdot 71} + 3y^{2\cdot 13} + \\ &\quad + 3 \cdot (2 \cdot 13,\ 4 \cdot 11 \cdot 71) \cdot y^{[2\cdot 13,\, 4\cdot 11\cdot 71]} + 2y^{2\cdot 3\cdot 13} + \\ &\quad + 2 \cdot (2 \cdot 3 \cdot 13,\ 4 \cdot 11 \cdot 17) \cdot y^{[2\cdot 3\cdot 13,\, 4\cdot 11\cdot 17]} = \\ &= 3y^1 + 2y^3 + 3y^{2\cdot 13} + 2y^{2\cdot 3\cdot 13} + 2y^{4\cdot 3\cdot 11\cdot 71} + 6y^{4\cdot 11\cdot 13\cdot 71} + 4y^{4\cdot 3\cdot 11\cdot 13\cdot 71}.\end{aligned}$$

2. Всюду далее в этом параграфе будем считать, что $R = \mathbb{Z}/p^n$, где p — простое и $n > 1$. Исследуем, чему равен максимально возможный период ЛРП порядка m над R и как строить такие ЛРП. Очевидно, что для этого надо прежде всего найти максимум периодов унитарных многочленов степени m над R.

Рассмотрим поле $\overline{R} = \mathbb{Z}/p$ и естественный эпиморфизм $\psi\colon R \to \overline{R}$, который ставит произвольному элементу $r = [a]_{p^n} \in R$ в соответствие элемент $\psi(r) = [a]_p \in \overline{R}$. В дальнейшем для краткости будем использовать обозначение $\psi(r) = \overline{r}$. Заметим сразу, что обратимость элемента r в кольце R равносильна условию $(a, p) = 1$, которое равносильно обратимости $\overline{r}$ в $\overline{R}$.

Для произвольного многочлена $F(x) = \sum f_i x^i \in R[x]$ положим $\overline{F}(x) = \sum \overline{f}_i x^i \in \overline{R}[x]$. Очевидно, что эпиморфизм $\psi\colon R \to \overline{R}$ можно продолжить до эпиморфизма $\widehat{\psi}\colon R[x] \to \overline{R}[x]$, действующего по закону $\widehat{\psi}(F(x)) = \overline{F}(x)$. При этом реверсивность

произвольного унитарного многочлена $F(x) \in R[x]$ равносильна реверсивности его образа $\overline{F}(x)$.

В дальнейшем нам понадобится

Лемма 39. *Если $F(x) \in R[x]$ — унитарный многочлен степени m и многочлены $A(x)$, $B(x) \in R[x]$ удовлетворяют условию*

$$p^t A(x) \equiv p^t B(x) \,(\mathrm{mod}\, F(x)),$$

где $0 \leqslant t < n$, то $\overline{A}(x) \equiv \overline{B}(x) \,(\mathrm{mod}\, \overline{F}(x))$.

□ Разделим многочлен $A(x) - B(x)$ на $F(x)$ с остатком:

$$A(x) - B(x) = Q(x)F(x) + C(x), \quad \deg C(x) < m. \tag{77}$$

Тогда $p^t(A(x) - B(x)) = (p^t Q(x))F(x) + p^t C(x)$, и так как $\deg p^t C(x) < m$, а по условию $F(x) \mid p^t(A(x) - B(x))$, то $p^t C(x) = 0$. Следовательно, все коэффициенты многочлена $C(x)$ делятся на p^{n-t}, и поскольку $n - t > 0$, они делятся на p, т. е. $\overline{C}(x) = \overline{0}$. В таком случае из (77) следует равенство $\overline{A}(x) - \overline{B}(x) = \overline{Q}(x)\overline{F}(x)$. □

Пусть теперь $F(x) \in R[x]$ — реверсивный многочлен степени $m > 0$, и $\tau_0 = T(\overline{F})$ — период $\overline{F}(x)$ над полем $\overline{R}$. Тогда $x^{\tau_0} \equiv \overline{e} \,(\mathrm{mod}\, \overline{F}(x))$, и, вычисляя остаток от деления в кольце $R[x]$ многочлена x^{τ_0} на $F(x)$, получаем:

$$x^{\tau_0} \equiv e + pU(x) \,(\mathrm{mod}\, F(x)), \quad \deg U(x) < m. \tag{78}$$

Это соотношение служит отправной точкой при решении всех задач, связанных с вычислениями периодов многочленов и соответствующих им ЛРП над кольцом R. Основным инструментом, позволяющим его использовать, является

Лемма 40. *Пусть $F(x) \in R[x]$ — реверсивный многочлен степени m, и для $t, l \in \mathbb{N}$ выполняются соотношения*

$$x^t \equiv e + p^l \Delta(x) \,(\mathrm{mod}\, F(x)), \quad \deg \Delta(x) < m. \tag{79}$$

Тогда существует многочлен $\Delta_1(x) \in R[x]$ такой, что

$$x^{tp} \equiv e + p^{l+1} \Delta_1(x) \,(\mathrm{mod}\, F(x)), \quad \deg \Delta_1(x) < m. \tag{80}$$

При этом если $l + 1 < n$, то любой многочлен $\Delta_1(x)$, удовлетворяющий соотношениям (80)*, удовлетворяет также соотношениям*:

$$\overline{\Delta}_1(x) = \overline{\Delta}(x), \qquad \text{если } p^l > 2; \tag{81}$$

$$\overline{\Delta}_1(x) \equiv \overline{\Delta}(x)^2 + \overline{\Delta}(x) \,(\mathrm{mod}\, \overline{F}(x)), \quad \text{если } p^l = 2. \tag{82}$$

□ Из (79) возведением в степень p получаем:

$$x^{tp} \equiv e + \binom{p}{1} p^l \Delta(x) + \binom{p}{2} p^{2l} \Delta(x)^2 + \ldots + \binom{p}{p} p^{pl} \Delta(x)^p \,(\mathrm{mod}\, F(x)).$$

Так как $\binom{p}{1}p^l = p^{l+1}$ и $p^{sl} \geqslant p^{l+1}$ для $s \in \overline{2,p}$, то последнее сравнение можно записать в виде

$$\begin{gathered} x^{tp} \equiv e + p^{l+1}K(x) \,(\mathrm{mod}\, F(x)), \quad \text{где} \\ K(x) = \Delta(x) + \binom{p}{2}p^{l-1}\Delta(x)^2 + \ldots + \binom{p}{p}p^{pl-(l+1)}\Delta(x)^p. \end{gathered} \tag{83}$$

Заменяя здесь $K(x)$ его остатком $\Delta_1(x)$ от деления на $F(x)$, получаем (80).

Пусть теперь $\Delta_1(x) \in R[x]$ — произвольный многочлен, удовлетворяющий условиям (80). Тогда из соотношений (80) и (83) следует, что $p^{l+1}\Delta_1(x) \equiv p^{l+1}K(x) \,(\mathrm{mod}\, F(x))$, и если $l+1 < n$, то по лемме 39

$$\overline{\Delta}_1(x) \equiv \overline{K}(x) \,(\mathrm{mod}\, \overline{F}(x)). \tag{84}$$

Если $p^l > 2$, то в выражении (83) для $K(x)$ коэффициенты всех слагаемых, начиная со второго, делятся на p. Следовательно, $\overline{K}(x) = \overline{\Delta}(x)$, и из (84) и условий $\deg\overline{\Delta}(x) < m$, $\deg\overline{\Delta}_1(x) < m$ следует (81).

Если $p^l = 2$, т. е. $p = 2$, $l = 1$, то соотношения (83) имеют вид

$$x^{t\cdot 2} \equiv e + 2^2K(x) \,(\mathrm{mod}\, F(x)), \quad K(x) = \Delta(x)^2 + \Delta(x),$$

и из (84) следует (82). □

Теорема 41. *Для любого реверсивного многочлена $F(x) \in R[x]$ справедливо равенство*

$$T(F) = T(\overline{F}) \cdot p^k, \quad \textit{где} \quad k \in \overline{0, n-1}. \tag{85}$$

Если $T(\overline{F}) = \tau_0$, то равенство $T(F) = \tau_0 \cdot p^{n-1}$ выполняется тогда и только тогда, когда многочлен $U(x)$ из соотношения (78) *удовлетворяет условию*:

$$\begin{aligned} &\overline{U}(x) \neq \overline{0}, && \textit{если } p > 2 \textit{ или } p = 2,\ n = 2; \\ &\overline{U}(x)^2 + \overline{U}(x) \not\equiv 0 \,(\mathrm{mod}\, \overline{F}(x)), && \textit{если } p = 2,\ n > 2. \end{aligned} \tag{86}$$

□ Пусть $T(F) = \tau$, $T(\overline{F}) = \tau_0$. Так как $F(x) \mid x^\tau - e$, то $\overline{F}(x) \mid x^\tau - \overline{e}$ и по следствию 1 утверждения 24 $\tau_0 \mid \tau$.

С другой стороны, из соотношения (78), применяя s раз лемму 40, получаем, что для каждого $s \in \mathbb{N}_0$ существует многочлен $U_s(x) \in R[x]$ такой, что выполняются соотношения

$$x^{\tau_0 p^s} \equiv e + p^{s+1}U_s(x) \,(\mathrm{mod}\, F(x)), \quad \deg U_s(x) < m. \tag{87}$$

Отсюда при $s = n-1$ получаем: $x^{\tau_0 p^{n-1}} \equiv e \,(\mathrm{mod}\, F(x))$, т. е.

$$F(x) \mid x^{\tau_0 p^{n-1}} - e \quad \text{и} \quad \tau \mid \tau_0 p^{n-1}.$$

В совокупности с условием $\tau_0 \mid \tau$ это дает равенство (85).

Ввиду (85) условие $T(F) = \tau_0 p^{n-1}$ равносильно условию $\tau > \tau_0 p^{n-2}$, которое опять-таки ввиду (85) равносильно тому, что

$$x^{\tau_0 p^{n-2}} \not\equiv e \,(\mathrm{mod}\, F(x)).$$

Последнее в силу (87) равносильно условию $\overline{U}_{n-2}(x) \neq \overline{0}$. Теперь остается заметить, что согласно лемме 40 из соотношения (78) вытекают следующие соотношения для многочленов $U_s(x)$ из (87):

если $p > 2$, то $\overline{U}_0(x) = \overline{U}_1(x) = \ldots = \overline{U}_{n-2}(x) = \overline{U}(x)$;

если $p = 2$, $n = 2$, то $U_0(x) = U_{n-2}(x) = U(x)$;

если $p = 2$, $n > 2$, то $\overline{U}_0(x) = \overline{U}(x)$, $\overline{U}_1(x) = \ldots = \overline{U}_{n-2}(x) \equiv \equiv \overline{U}(x)^2 + \overline{U}(x) \,(\mathrm{mod}\, F(x))$. □

Следствие. *Для любого реверсивного многочлена $F(x) \in R[x]$ степени m выполняется неравенство $T(F) \leqslant (p^m - 1)p^{n-1}$. Равенство $T(F) = (p^m - 1)p^{n-1}$ имеет место тогда и только тогда, когда*

(а) *$\overline{F}(x)$ — многочлен максимального периода $\tau_0 = p^m - 1$ над полем $\overline{R} = \mathbb{Z}/p$; и*

(б) *для многочлена $U(x)$ из* (78) *выполняется условие* (86).

□ Достаточно заметить, что для любого реверсивного многочлена $\overline{F}(x) \in \overline{R}[x]$ степени m верно неравенство $T(\overline{F}) \leqslant p^m - 1$, а равенство $T(\overline{F}) = p^m - 1$ означает, что $\overline{F}(x)$ — многочлен максимального периода. □

Определение 21. Реверсивный многочлен $F(x)$ степени m над кольцом $R = \mathbb{Z}/p^n$ называется *многочленом максимального периода*, если $T(F) = (p^m - 1)p^{n-1}$.

Теорема 42. *Для любого натурального $m \geqslant 2$ в кольце $R[x]$ существует многочлен максимального периода степени m.*

□ Выберем произвольно реверсивный многочлен $F(x) \in R[x]$ степени m так, чтобы многочлен $\overline{F}(x)$ имел максимальный период $\tau_0 = p^m - 1$. Если многочлен $U(x)$ из соотношения (78) удовлетворяет условию (86), то по следствию теоремы 41 $F(x)$ — искомый многочлен максимального периода. Допустим, что условие (86) для $U(x)$ не выполнено. Покажем, что в таком случае многочленом максимального периода будет многочлен $F_1(x) = F(x + pe)$.

Очевидно, что $\overline{F}_1(x) = \overline{F}(x)$, и потому для $F_1(x)$ выполнено условие (а) следствия теоремы 41. Пусть

$$x^{\tau_0} \equiv e + pU_1(x) \,(\mathrm{mod}\, F_1(x)), \quad \deg U_1(x) < m. \tag{88}$$

Остается показать, что многочлен $U_1(x)$ удовлетворяет условию (86). Для этого выразим $U_1(x)$ через $U(x)$. Заменяя в (78) x на $x + pe$, получаем:

$$(x + pe)^{\tau_0} \equiv e + pU(x + pe) \,(\mathrm{mod}\, F_1(x)).$$

Пользуясь формулой Ньютона (теорема 3 главы 2), находим

$$(x + pe)^{\tau_0} = x^{\tau_0} + p\tau_0 x^{\tau_0 - 1} + p^2 K(x)$$

для подходящего $K(x) \in R[x]$. Из двух последних соотношений имеем:

$$x^{\tau_0} \equiv e + p\big(U(x+ep) - \tau_0 x^{\tau_0-1} - pK(x)\big) \,(\mathrm{mod}\, F_1(x)).$$

Отсюда и из (88) получаем соотношение

$$pU_1(x) \equiv p\big(U(x+pe) - \tau_0 x^{\tau_0-1} - pK(x)\big) \,(\mathrm{mod}\, F_1(x)),$$

из которого в силу леммы 39 и очевидных соотношений $\overline{U}(x+pe) = \overline{U}(x)$, $\overline{\tau_0 x^{\tau_0-1}} = -\overline{e}x^{\tau_0-1}$, $\overline{pK(x)} = \overline{0}$ вытекает сравнение

$$\overline{U}_1(x) \equiv \overline{U}(x) - \overline{e}x^{\tau_0-1} \,(\mathrm{mod}\, \overline{F}_1(x)). \tag{89}$$

В случае $p > 2$ или $p = n = 2$ предположение о том, что многочлен $U(x)$ не удовлетворяет условию (86) означает: $\overline{U}(x) \equiv \overline{0} \,(\mathrm{mod}\, \overline{F}(x))$. Но тогда ввиду равенства $\overline{F}_1(x) = \overline{F}(x)$ из (89) следует, что

$$\overline{U}_1(x) \equiv -\overline{e}x^{\tau_0-1} \not\equiv \overline{0} \,(\mathrm{mod}\, \overline{F}_1(x)),$$

следовательно, $U_1(x)$ удовлетворяет условию (86).

В случае $p = 2$, $n \geqslant 3$ наше предположение означает, что

$$\overline{U}(x)^2 + \overline{U}(x) \equiv \overline{0} \,(\mathrm{mod}\, \overline{F}(x)).$$

Но тогда из (89) следует сравнение

$$\overline{U}_1(x)^2 + \overline{U}_1(x) \equiv x^{\tau_0-1}(x^{\tau_0-1} - \overline{e}) \,(\mathrm{mod}\, \overline{F}_1(x)),$$

и так как $T(\overline{F}_1(x)) = \tau_0$, то $x^{\tau_0-1}(x^{\tau_0-1} - \overline{e}) \not\equiv \overline{0} \,(\mathrm{mod}\, \overline{F}_1(x))$, т. е. $\overline{U}_1(x)$ удовлетворяет условию (86). $\square$

3. Теперь предположим, что $F(x)$ — многочлен степени m над кольцом $R = \mathbb{Z}/p^n$, имеющий максимально возможный период $T(F) = (p^m - 1)p^{n-1}$, и дадим описание периодов ЛРП из $L_R(F)$ и циклового типа семейства $L_R(F)$.

Заметим, что в кольце R можно выделить строго возрастающую цепочку идеалов:

$$\{0\} = p^n R \underset{\neq}{\lhd} p^{n-1}R \underset{\neq}{\lhd} \ldots \underset{\neq}{\lhd} pR \underset{\neq}{\lhd} R$$

(равенство $p^k R = p^{k+1}R$ при $k < n$ невозможно, так как из него следует равенство $p^k R = p^n R = \{0\}$).

Определение 22. *Нормой элемента* $r \in R$ назовем число $\|r\|$, равное наибольшему $k \in \overline{0,n}$ со свойством $r \in p^k R$. *Нормой последовательности* $u \in R^\infty$ и *нормой вектора* $u[\overline{0,m-1}]$ будем называть параметры

$$\|u\| = \min\{\|u(i)\| :\ i \in \mathbb{N}_0\}, \quad \|u[\overline{0,m-1}]\| = \min\{\|u(i)\| :\ i \in \overline{0,m-1}\}.$$

Из определения легко следует, что для любого элемента $r \in R$ справедливы соотношения

$$(\|r\| = 0) \Leftrightarrow (r \in R^*), \quad (\|r\| = n) \Leftrightarrow (r = 0).$$

Читателю предлагается самостоятельно убедиться в справедливости следующих фактов.

Лемма 43. *Для любых элементов $a, b \in R$ верны соотношения*:

(а) $\|a + b\| \geqslant \min\{\|a\|, \|b\|\}$, *и если* $\|a\| \neq \|b\|$, *то* $\|a + b\| = \min\{\|a\|, \|b\|\}$;

(б) $\|ab\| \leqslant \|a\| + \|b\|$, *и если* $\|a\| + \|b\| \leqslant n$, *то* $\|ab\| = \|a\| + \|b\|$.

(в) *Для любой ЛРП $u \in L_R(F)$ верно равенство* $\|u\| = \|u\overline{[0, m-1]}\|$.

В дальнейшем нам понадобится также

Лемма 44. *Многочлены $F(x), G(x) \in R[x]$ взаимно просты тогда и только тогда, когда взаимно просты их образы $\overline{F}(x)$, $\overline{G}(x)$ над полем $\overline{R} = \mathbb{Z}/p$.*

□ Пусть $(\overline{F}(x), \overline{G}(x)) = \overline{e}$. Тогда существуют такие многочлены $A(x)$, $B(x) \in R[x]$, что $\overline{A}(x)\overline{F}(x) + \overline{B}(x)\overline{G}(x) = \overline{e}$. Это означает, что в кольце $R[x]$ для подходящего $C(x) \in R[x]$ выполняется равенство

$$A(x)F(x) + B(x)G(x) = e + pC(x).$$

Так как $(e + pC(x))^{p^{n-1}} = e$, то $e + pC(x)$ — обратимый многочлен в кольце $R[x]$, и для $U(x) = (e + pC(x))^{-1}A(x)$, $V(x) = (e + pC(x))^{-1}B(x)$ выполняется равенство $U(x)F(x) + V(x)G(x) = e$, т. е. $(F(x), G(x)) = e$ (определение 10). Доказательство в обратную сторону очевидно. □

Теорема 45. *Если $F(x)$ — многочлен степени $m \geqslant 2$ максимального периода $(p^m - 1)p^{n-1}$ над кольцом R, $u \in L_R(F) \setminus (0)$, $\|u\| = k$, то $T(u) = (p^m - 1)p^{n-k-1}$. Цикловой тип семейства $L_R(F)$ имеет вид*

$$\mathcal{C}_F(y) = y^1 + \sum_{t=0}^{n-1} p^{(m-1)t} y^{(p^m-1)p^t}.$$

□ Рассмотрим сначала случай, когда $\|u\| = 0$. Пусть $\Phi_u(x)$ — генератор ЛРП u относительно характеристического многочлена $F(x)$. Покажем, что $(\Phi_u(x), F(x)) = e$. Из формулы (11) легко следует, что $\overline{\Phi}_u(x) = \Phi_{\overline{u}}(x)$ — генератор образа $\overline{u}$ ЛРП u над полем $\overline{R}$ относительно характеристического многочлена $\overline{F}(x)$. Так как $\|u\| = 0$, то $\overline{u} \neq (\overline{0})$ и $\Phi_{\overline{u}}(x) \neq \overline{0}$. Так как $F(x)$ — многочлен максимального периода над R, то по следствию теоремы 41 $\overline{F}(x)$ — неприводимый многочлен степени m над $\overline{R}$. Поскольку $\overline{\Phi}_u(x) \neq \overline{0}$ и $\deg \overline{\Phi}_u(x) < m$, то это дает соотношение $(\overline{\Phi}_u(x), \overline{F}(x)) = \overline{e}$, которое ввиду леммы 44 эквивалентно условию $(\Phi_u(x), F(x)) = e$.

По утверждению 14(б) последнее означает, что для любого $t \in \mathbb{N}$ условие $F(x) \mid (x^t - e)\Phi_u(x)$ эквивалентно условию $F(x) \mid x^t - e$. В силу утверждения 12 это означает, что

$$((x^t - e)u = (0)) \Leftrightarrow (F(x) \mid x^t - e),$$

т. е. $T(u) = T(F) = (p^m - 1)p^{n-1}$. Таким образом, в случае $\|u\| = 0$ теорема доказана.

Пусть теперь $\|u\| = k > 0$. Заметим, что $k < n$, так как $u \neq 0$. По лемме 43(в) $\|u[\overline{0, m-1}]\| = k$. По определению нормы вектора это означает, что все координаты $u(0), \ldots, u(m-1)$ делятся на p^k, и часть из них не делится на p^{k+1}. Следовательно, найдется вектор $v[\overline{0, m-1}]$ над R такой, что $\|v[\overline{0, m-1}]\| = 0$ и $u[\overline{0, m-1}] = p^k v[\overline{0, m-1}]$. Пусть $v \in L_R(F)$ — ЛРП с начальным вектором $v[\overline{0, m-1}]$. Тогда, очевидно, справедливы равенства $\|v\| = 0$ и $u = p^k v$.

Рассмотрим факторкольцо $\widetilde{R} = R/p^{n-k}R \cong \mathbb{Z}/p^{n-k}$. Обозначим через $\widetilde{v}$ и $\widetilde{F}(x)$ образы последовательности v и многочлена $F(x)$ при естественном эпиморфизме $R \to \widetilde{R}$ и докажем последовательно равенства $T(\widetilde{v}) = (p^m - 1)p^{n-k-1}$, $T(u) = T(\widetilde{v})$.

Очевидно, $\widetilde{v} \in L_{\widetilde{R}}(\widetilde{F})$ и $\|\widetilde{v}\| = 0$. Кроме того, так как $n - k > 0$, то $\widetilde{F}(x)$ — многочлен максимального периода $(p^m - 1)p^{n-k-1}$ над кольцом $\widetilde{R}$. Действительно, если $n - k = 1$, то $\widetilde{R} = \overline{R}$, $\widetilde{F}(x) = \overline{F}(x)$ и утверждение очевидно; если $n - k > 1$, то из соотношения (78) для $\tau_0 = T(\overline{F}) = p^m - 1$ следует соотношение

$$x^{\tau_0} \equiv \widetilde{e} + p\widetilde{U}(x) \,(\mathrm{mod}\, \widetilde{F}(x)),$$

где $\widetilde{U}(x)$ — образ $U(x)$ над $\widetilde{R}$. Так как $\overline{\widetilde{F}}(x) = \overline{F}(x)$ и $\overline{\widetilde{U}}(x) = \overline{U}(x)$, а $F(x)$ — многочлен максимального периода над R, то для $\overline{\widetilde{F}}$ и $\overline{\widetilde{U}}$ выполнены условия следствия теоремы 41, т. е. $\widetilde{F}(x)$ — многочлен максимального периода над $\widetilde{R}$. Поскольку $\|\widetilde{v}\| = 0$, то по доказанному выше это означает, что

$$T(\widetilde{v}) = T(\widetilde{F}) = (p^m - 1)p^{n-k-1}.$$

Из равенства $u = p^k v$ следует, что для каждого $t \in \mathbb{N}$ справедлива цепочка соотношений

$$\begin{aligned}(x^t - e)u = (0) \;&\Leftrightarrow\; p^k(x^t - e)v = (0) \;\Leftrightarrow \\ &\Leftrightarrow\; (x^t - e)v \equiv (0) \,(\mathrm{mod}\, p^{n-k}) \;\Leftrightarrow\; (x^t - \widetilde{e})\,\widetilde{v} = (\widetilde{0}).\end{aligned}$$

Эти импликации доказывают равенство $T(u) = T(\widetilde{v})$. Следовательно, $T(u) = (p^m - 1)p^{n-k-1}$, и первая часть теоремы доказана.

Теперь можно утверждать, что возможные длины циклов, на которые разбивается множество $L_R(F)$, суть 1, $(p^m - 1)$, $(p^m - 1)p$, $\ldots$, $(p^m - 1)p^{n-1}$, т. е. цикловой тип семейства $L_R(F)$ имеет вид

$$\mathcal{C}_F(y) = Cy^1 + \sum_{t=0}^{n-1} C_t y^{(p^m-1)p^t}, \tag{90}$$

где C_t — количество циклов длины $(p^m - 1)p^t$ в $L_R(F)$. ЛРП $u \in L_R(F)$ имеет период 1 тогда и только тогда, когда $u = (0)$, т. е. $\|u\| = n$. Таким образом, в (90) $C = 1$. Равенство $T(u) = (p^m - 1)p^t$, где $t \in \overline{0, n-1}$, эквивалентно равенству $\|u[\overline{0, m-1}]\| = n - t - 1$. Количество векторов длины m над кольцом R, имеющих норму $n - t - 1$, очевидно, равно $|p^{n-t-1}R|^m - |p^{n-t}R|^m = p^{(t+1)m} - p^{tm}$. Следовательно, количество последовательностей $u \in L_R(F)$, имеющих период $(p^m - 1)p^t$, равно $(p^m - 1)p^{tm}$, и они разбиваются на $C_t = (p^m - 1)p^{tm}/(p^m - 1)p^t = p^{(m-1)t}$ циклов. Подставляя найденное значение C_t в (90), получаем нужное равенство для $\mathcal{C}_F(y)$. $\square$

Следствие. *Если u — произвольная ЛРП над кольцом $R = \mathbb{Z}/p^n$ с характеристическим многочленом $G(x)$ степени m, то*

$$T(u) \leqslant (p^m - 1)p^{n-1}.$$

Равенство $T(u) = (p^m - 1)p^{n-1}$ достигается тогда и только тогда, когда $G(x)$ — многочлен максимального периода над R и $\|u\| = 0$.

□ Первое утверждение вытекает из неравенства $T(u) \leqslant T(G)$ и следствия теоремы 41. Второе — из того же следствия и доказанной только что теоремы. □

Определение 23. ЛРП u порядка m и периода $(p^m - 1)p^{n-1}$ над кольцом $\mathbb{Z}/p^n$ называется *линейной рекуррентной последовательностью максимального периода* над кольцом $\mathbb{Z}/p^n$.

§ 13. РАСПРЕДЕЛЕНИЕ ЭЛЕМЕНТОВ НА ЦИКЛАХ ЛИНЕЙНЫХ РЕКУРРЕНТ[37]

1. Пусть u — ненулевая реверсивная ЛРП над полем $P = GF(q)$ ранга $m \geqslant 1$ и периода $\tau = T(u) \leqslant q^m - 1$. Обозначим через $\mathfrak{N}_u(a)$ количество появлений элемента $a \in P$ на цикле ЛРП u, т. е. на отрезке $u[\overline{0, \tau - 1}]$. Как уже отмечалось в параграфе 10, для того, чтобы рассматривать u как имитацию случайной последовательности, необходимо, чтобы относительная частота $\nu_u(a) = \dfrac{1}{\tau}\mathfrak{N}_u(a)$ появления элемента a на отрезке $u[\overline{0, \tau - 1}]$ была близка к естественной средней величине $1/q$ для любого $a \in P$.

Здесь мы иллюстрируем возможности применения *метода тригонометрических сумм* Виноградова для получения оценок величин $\nu_u(a)$ и $\mathfrak{N}_u(a)$ с использованием свойств характеров конечного поля и сумм Гаусса.

Утверждение 46. *Для любого нетривиального аддитивного характера ψ (см.* § 6 главы 22) *поля P верно равенство*

$$\mathfrak{N}_u(a) = \frac{\tau}{q} + \frac{1}{q}\sum_{c \in P \setminus 0} \psi(-ca) \sum_{i=0}^{\tau-1} \psi(cu(i)).$$

□ Согласно соотношению ортогональности для характеров группы $(P, +)$ (см. теорему 12 главы 12) справедливы соотношения:

$$\frac{1}{q}\sum_{c \in P} \psi(c(u(i) - a)) = \begin{cases} 1, & \text{если } u(i) = a, \\ 0, & \text{если } u(i) \neq a. \end{cases}$$

Отсюда

$$\mathfrak{N}_u(a) = \sum_{i=0}^{\tau-1} \frac{1}{q}\sum_{c \in P} \psi(c(u(i) - a)).$$

[37] Авторы признательны О. В. Камловскому за помощь при подготовке материалов этого параграфа.

Поскольку ψ — аддитивный характер, то $\psi(c(u(i)-a)) = \psi(cu(i))\psi(-ca)$. Следовательно,

$$\mathfrak{N}_u(a) = \frac{1}{q}\sum_{c\in P}\sum_{i=0}^{\tau-1}\psi(cu(i))\,\psi(-ca).$$

Так как $\psi(0)=1$, то сумма слагаемых, соответствующих $c=0$, равна τ/q. Выделяя это слагаемое отдельно, получим требуемое соотношение. □

Из доказанного утверждения видна необходимость исследования сумм вида $\sum_{i=0}^{\tau-1}\psi(cu(i))$. Важное их свойство дает

Утверждение 47. *Пусть ψ — нетривиальный аддитивный характер поля P. Тогда*

$$\tau\left|\sum_{i=0}^{\tau-1}\psi(u(i))\right|^2 \leqslant \sum_{v\in L_P(F)\setminus(0)}\left|\sum_{i=0}^{\tau-1}\psi(v(i))\right|^2 = \tau(q^m-\tau).$$

□ Так как u — последовательность периода τ, то справедливо равенство

$$\tau\left|\sum_{i=0}^{\tau-1}\psi(u(i))\right|^2 = \sum_{j=0}^{\tau-1}\left|\sum_{i=0}^{\tau-1}\psi(u(i+j))\right|^2.$$

Так как u — реверсивная последовательность, то система последовательностей $v_j = x^j u,\ 0\leqslant j\leqslant \tau-1$, есть система попарно различных ЛРП из $L_P(F)\setminus 0$, и потому

$$\sum_{j=0}^{\tau-1}\left|\sum_{i=0}^{\tau-1}\psi(u(i+j))\right|^2 = \sum_{j=0}^{\tau-1}\left|\sum_{i=0}^{\tau-1}\psi(v_j(i))\right|^2 \leqslant \sum_{v\in L_P(F)\setminus 0}\left|\sum_{i=0}^{\tau-1}\psi(v(i))\right|^2,$$

откуда следует первое из доказываемых соотношений.

Для доказательства второго соотношения заметим, что

$$\sum_{v\in L_P(F)\setminus 0}\left|\sum_{i=0}^{\tau-1}\psi(v(i))\right|^2 = \Sigma - \tau^2,$$

где

$$\Sigma = \sum_{v\in L_P(F)}\left|\sum_{i=0}^{\tau-1}\psi(v(i))\right|^2.$$

Поэтому достаточно доказать, что $\Sigma = \tau q^m$. Пусть $F(x)$ — минимальный многочлен ЛРП u. Тогда по предположению $\deg F(x) = m$, и система последовательностей $v_0 = u$, $v_1 = xu$, …, $v_{m-1} = x^{m-1}u$ есть базис пространства $L_P(F)$. Отсюда

$$\Sigma = \sum_{a_0,\ldots,a_{m-1}\in P} \left| \sum_{i=0}^{\tau-1} \psi\big(a_0 v_0(i) + \ldots + a_{m-1} v_{m-1}(i)\big) \right|^2 =$$

$$= \sum_{a_0,\ldots,a_{m-1}\in P} \sum_{i=0}^{\tau-1} \psi\big(a_0 v_0(i) + \ldots + a_{m-1} v_{m-1}(i)\big) \overline{\sum_{j=0}^{\tau-1} \psi\big(a_0 v_0(j) + \ldots + a_{m-1} v_{m-1}(j)\big)},$$

где черта означает комплексное сопряжение. Перемножая две последние суммы и пользуясь равенством $\overline{\psi(c)} = \psi(-c)$, получим

$$\Sigma = \sum_{a_0,\ldots,a_{m-1}\in P} \sum_{i,j=0}^{\tau-1} \psi\big(a_0(v_0(i) - v_0(j))\big) \ldots \psi\big(a_{m-1}(v_{m-1}(i) - v_{m-1}(j))\big) =$$

$$= \sum_{i,j=0}^{\tau-1} \left(\sum_{a_0\in P} \psi\big(a_0(v_0(i) - v_0(j))\big) \right) \ldots \left(\sum_{a_{m-1}\in P} \psi\big(a_{m-1}(v_{m-1}(i) - v_{m-1}(j))\big) \right).$$

В силу соотношения ортогональности для характеров при любых фиксированных $i, j \in \overline{0,\, \tau-1}$ справедливо равенство

$$\sum_{a\in P} \psi(a(v(i) - v(j))) = q\delta_{v(i),v(j)},$$

где $\delta_{v(i),v(j)}$ — символ Кронекера. Отсюда

$$\Sigma = q^m \sum_{i,j=0}^{\tau-1} \delta_{v_0(i),v_0(j)} \ldots \delta_{v_{m-1}(i),v_{m-1}(j)}.$$

Слагаемое данной суммы отлично от 0 (и, следовательно, равно 1) тогда и только тогда, когда $(v_0(i), \ldots, v_{m-1}(i)) = (v_0(j), \ldots, v_{m-1}(j))$, т. е. тогда и только тогда, когда $u[\overline{i,\, i+m-1}] = u[\overline{j,\, j+m-1}]$. Так как u — ЛРП порядка m, то последнее равенство эквивалентно условию $x^i u = x^j u$. Так как $0 \leqslant i, j \leqslant \tau - 1$, где τ — период ЛРП u, то это условие равносильно условию $i = j$. Таким образом,

$$\Sigma = q^m \sum_{i=0}^{\tau-1} 1 = \tau q^m,$$

что и требовалось доказать. □

Теорема 48. *Пусть, по-прежнему, u — ненулевая реверсивная ЛРП ранга m и периода $\tau = T(u)$ над полем $P = GF(q)$. Тогда для любого $a \in P$*

$$\left| \nu_u(a) - \frac{1}{q} \right| \leqslant \frac{q-1}{q} \ \frac{\sqrt{q^m - \tau}}{\tau}.$$

□ Из определения $\nu_u(a)$ следует, что достаточно доказать неравенство

$$\left|\mathfrak{N}_u(a) - \frac{\tau}{q}\right| \leqslant \frac{q-1}{q}\sqrt{q^m - \tau}.$$

Используя утверждение 46 и равенство $|\psi(-ac)| = 1$ для $c \in P \setminus 0$, получаем

$$\left|\mathfrak{N}_u(a) - \frac{\tau}{q}\right| = \frac{1}{q}\left|\sum_{c\in P\setminus 0}\psi(-ca)\sum_{i=0}^{\tau-1}\psi(cu(i))\right| \leqslant \frac{1}{q}\sum_{c\in P\setminus 0}\left|\sum_{i=0}^{\tau-1}\psi(cu(i))\right|.$$

Теперь по утверждению 47, примененному к ЛРП cu, имеем:

$$\left|\mathfrak{N}_u(a) - \frac{\tau}{q}\right| \leqslant \frac{1}{q}\sum_{c\in P\setminus 0}(q^m-\tau)^{1/2} = \frac{q-1}{q}(q^m-\tau)^{1/2}. \quad \square$$

По теореме 30 если u — ЛРП максимального периода $\tau = q^m - 1$, то

$$\nu_u(a) - \frac{1}{q} = \begin{cases} \dfrac{1}{q\tau}, & \text{если } a \neq 0, \\ \dfrac{1-q}{q\tau}, & \text{если } a = 0. \end{cases} \tag{91}$$

Читателю предлагается самостоятельно вывести из теоремы 48

Следствие. *Если для некоторого $\varepsilon > 0$ выполняется равенство $\tau = q^{\frac{m}{2}+1+\varepsilon}$, то*

$$\left|\nu_u(a) - \frac{1}{q}\right| \leqslant \frac{1}{q^{1+\varepsilon}}.$$

Этот результат, по сути, указывает нижнюю оценку периода τ последовательности u, при которой оценку теоремы 48 можно рассматривать как нетривиальную.

2. Более точные оценки величин $\nu_u(a)$ можно получить, если наложить на характеристический многочлен ЛРП u дополнительные ограничения и использовать более сильный математический аппарат. Так, используя введенные в § 6 главы 22 *суммы Гаусса*

$$G(\chi,\psi) = \sum_{c\in P\setminus 0}\chi(c)\,\overline{\psi}(c),$$

где χ, ψ — характеры соответственно мультипликативной и аддитивной групп поля P, можно более точно описать частоты появления элементов поля P на цикле ЛРП u с произвольным неприводимым минимальным многочленом $F(x)$ степени m и периода $(q^m-1)/d$ при $d > 1$. Ниже соответствующий результат приводится при $d = 2$.

Нам понадобятся следующие свойства сумм Гаусса. Если e — единица поля $P = GF(q)$, то

$$G(\chi,\overline{\psi}) = \chi(-e)G(\chi,\psi), \quad G(\overline{\chi},\psi) = \chi(-e)\overline{G(\chi,\psi)}. \tag{92}$$

Читателю предлагается доказать эти равенства самостоятельно. Если характеры χ и ψ нетривиальны, то $|G(\chi,\psi)|^2 = q$ (см. теорему 21(в) главы 22).

Пусть $P = GF(q)$, q нечетно, и η — *квадратичный мультипликативный характер* поля P, определяемый соотношениями

$$\eta(a) = \begin{cases} 1, & \text{если } a \in P \text{ является квадратом,} \\ -1, & \text{в противном случае} \end{cases} \tag{93}$$

(см. задачу 73).

Утверждение 49. *Если η — квадратичный мультипликативный характер и ψ — нетривиальный аддитивный характер поля P, то*

$$G(\eta,\psi) = \begin{cases} \pm\sqrt{q}, & \textit{если } q \equiv 1 \pmod 4, \\ \pm i\sqrt{q}, & \textit{если } q \equiv 3 \pmod 4. \end{cases}$$

□ Пусть α — примитивный элемент поля $GF(q)$. Элемент $\alpha^{(q-1)/2}$ не равен единице и является решением уравнения $x^2 = e$. Это уравнение имеет в точности два корня e и $-e$, значит $\alpha^{(q-1)/2} = -e$.

В циклической группе $GF(q)^* = \langle\alpha\rangle$ элемент $\alpha^{(q-1)/2} = -e$ является квадратом, если $(q-1)/2$ четно, и не является квадратом, если $(q-1)/2$ нечетно. Действительно, если $(q-1)/2$ четно, то $\alpha^{(q-1)/2} = (\alpha^{(q-1)/4})^2$. Если же $(q-1)/2$ нечетно, то из равенства $\alpha^{(q-1)/2} = (\alpha^k)^2$ получаем, что четное число $\operatorname{ord}\alpha = q-1$ делит нечетное число $(q-1)/2 - 2k$, противоречие.

По определению (93) получаем, что $\eta(-e) = 1$, если $(q-1)/2$ четно, и $\eta(-e) = -1$, если $(q-1)/2$ нечетно. Другими словами,

$$\eta(-e) = \begin{cases} 1, & \text{если } q \equiv 1 \pmod 4, \\ -1, & \text{если } q \equiv 3 \pmod 4. \end{cases} \tag{94}$$

Так как $\eta = \overline{\eta}$, то ввиду (92)

$$G(\eta,\psi)^2 = G(\eta,\psi)G(\overline{\eta},\psi) = \eta(-e)G(\eta,\psi)\overline{G(\eta,\psi)} = \eta(-e)|G(\eta,\psi)|^2 = \eta(-e)q,$$

и требуемые равенства следуют из (94). □

По теореме 19 реверсивная ЛРП u с неприводимым минимальным многочленом $F(x)$ степени m имеет представление функцией след вида

$$u(i) = \operatorname{tr}_q^{q^m}(b\theta^i), \quad i \geqslant 0,$$

где θ — корень многочлена $F(x)$ в поле $Q = GF(q^m)$, и $b \in Q$ — некоторый элемент, однозначно определяемый начальным вектором ЛРП u. При этом параметр $\tau = T(u) = T(F)$ удовлетворяет также равенству $\tau = \operatorname{Ord}\theta$ (см. утверждение 27 и пример 3 главы 22).

Утверждение 50. *При заданных условиях для любых элементов $a \in P$ и нетривиального аддитивного характера ψ поля P справедливо равенство*

$$\mathfrak{N}_u(a) = \frac{\tau}{q} + \frac{\tau}{q(q^m-1)} \sum_{\chi:\ \chi(\theta)=1} G(\overline{\chi}, \psi^Q)\, G(\chi_P, \overline{\psi}_a)\chi(b),$$

где суммирование проводится по всем мультипликативным характерам χ поля $Q = GF(q^m)$ таким, что $\chi(\theta) = 1$, и использованы обозначения:

χ_P — *ограничение характера χ на поле P*;

$\psi^Q(x) = \psi(\mathrm{tr}_q^{q^m}(x))$ — *расширение характера ψ поля P на поле Q*;

$\psi_a(y) = \psi(ay)$ — *аддитивный характер поля P.*

□ Во-первых, отметим, что χ_P, ψ^Q и ψ_a — характеры. Это устанавливается непосредственной проверкой с использованием линейности функции след для характера ψ^Q. По утверждению 46

$$\mathfrak{N}_u(a) = \frac{\tau}{q} + \frac{1}{q} \sum_{c\in P\setminus 0} \psi(-ca) \sum_{i=0}^{\tau-1} \psi(c\ \mathrm{tr}_q^{q^m}(b\theta^i)) = \frac{\tau}{q} + \frac{1}{q} \sum_{c\in P\setminus 0} \overline{\psi}_a(c) \sum_{i=0}^{\tau-1} \psi^Q(cb\theta^i).$$

Согласно теореме 20 главы 22 характер ψ^Q поля Q выражается через его мультипликативные характеры с помощью сумм Гаусса:

$$\psi^Q(x) = \frac{1}{q^m-1} \sum_{\chi} G(\overline{\chi}, \psi^Q)\chi(x),$$

где суммирование проводится по всем мультипликативным характерам χ поля Q. Тогда

$$\sum_{i=0}^{\tau-1} \psi^Q(cb\theta^i) = \frac{1}{q^m-1} \sum_{\chi} G(\overline{\chi}, \psi^Q) \sum_{i=0}^{\tau-1} \chi(cb)\chi(\theta)^i.$$

Если $\chi(\theta) \neq 1$, то внутренняя сумма, которая после вынесения общего множителя $\chi(cb)$ вычисляется по формуле суммы геометрической прогрессии, равна $\chi(cb)(\chi(\theta)^\tau - 1)/(\chi(\theta) - 1) = 0$, поскольку $\chi(\theta)^\tau = \chi(\theta^\tau) = \chi(e) = 1$. Если же $\chi(\theta) = 1$, то внутренняя сумма равна $\tau\chi(cb)$. Отсюда

$$\mathfrak{N}_u(a) = \frac{\tau}{q} + \frac{1}{q} \sum_{c\in P\setminus 0} \overline{\psi}_a(c) \frac{\tau}{q^m-1} \sum_{\chi:\ \chi(\theta)=1} G(\overline{\chi}, \psi^Q)\chi(c)\chi(b) =$$

$$= \frac{\tau}{q} + \frac{\tau}{q(q^m-1)} \sum_{\chi:\ \chi(\theta)=1} G(\overline{\chi}, \psi^Q)\, G(\chi_P, \overline{\psi}_a)\chi(b).$$

Последнее равенство получается изменением порядка суммирования с использованием определения суммы $G(\chi_P, \overline{\psi}_a)$. □

Доказанное утверждение позволяет получать оценки для величины $|\nu_u(a) - 1/q|$ более точные, чем в следствии теоремы 48, а иногда — находить точные формулы для значений $\nu_u(a)$.

Заметим, что согласно утверждению 27 для некоторого делителя d числа q^m-1 справедливо равенство $\tau=(q^m-1)/d$. Читателю предлагается самостоятельно проверить, что в случае $d=1$ формула утверждения 50 дает равенства (91). Мы покажем в заключение, как эта формула позволяет рассчитать значения $\nu_u(a)$ в случае $d=2$ (заметим, что при этом q нечетно).

Теорема 51. *Пусть $P=GF(q)$, q нечетно, u — реверсивная ЛРП над P с неприводимым минимальным многочленом $F(x)$ степени m и периода*

$$\tau=T(F)=T(u)=(q^m-1)/2.$$

Тогда справедливы следующие утверждения: *если m нечетно, то*

$$\nu_u(0)=\frac{1}{q}\left(1-\frac{q-1}{q^m-1}\right),\quad \nu_u(a)=\frac{1}{q}\left(1+\frac{1\pm q^{\frac{m+1}{2}}}{q^m-1}\right)\ \textit{для всех}\ a\neq 0;$$

если m четно, то

$$\nu_u(0)=\frac{1}{q}\left(1-\frac{(q-1)(1\pm q^{\frac{m}{2}})}{q^m-1}\right),\quad \nu_u(a)=\frac{1}{q}\left(1+\frac{1\pm q^{\frac{m}{2}}}{q^m-1}\right)\ \textit{для}\ a\neq 0.$$

□ Пользуясь утверждением 50, мы получим соответствующие выражения для параметров $\mathfrak{N}_u(a)=\tau\nu_u(a)$.

Рассмотрим сначала случай $a=0$. Тогда в соответствующей формуле из утверждения 50 используется сумма Гаусса $G(\chi_P,\overline{\psi}_0)$ относительно тривиального аддитивного характера ψ_0, и согласно теореме 21(а) главы 22

$$G(\chi_P,\overline{\psi}_0)=\begin{cases}0, & \text{если } \chi_P \text{ — нетривиальный характер,}\\ q-1, & \text{в противном случае.}\end{cases}$$

Характеры χ, участвующие в сумме, обладают свойством $\chi(\theta)=1$, откуда $\chi(\theta^i)=1$, $i\geqslant 0$. Таким образом, характер χ тривиален на подгруппе $\langle\theta\rangle$ индекса 2 группы $GF(q^m)^*$. Существует точно два мультипликативных характера поля $GF(q^m)$ с указанным свойством: тривиальный характер χ_e и квадратичный характер η. При этом η_P — тривиальный характер поля P тогда и только тогда, когда $GF(q)^*\subseteq\langle\theta\rangle$, т. е. $q-1$ делит $(q^m-1)/2$. Это условие равносильно тому, что 2 делит $(q^m-1)/(q-1)=q^{m-1}+\ldots+q+1$, т. е. тому, что m четно.

Итак, если m нечетно, то характер η_P нетривиален, $G(\eta_P,\overline{\psi}_0)=0$, и по утверждению 50

$$\mathfrak{N}_u(0)=\frac{\tau}{q}+\frac{\tau}{q(q^m-1)}\,G(\overline{\chi}_e,\psi^Q)(q-1)\chi_e(b)=$$
$$=\frac{q^m-1}{2q}+\frac{1}{2q}(-1)(q-1)=\frac{q^{m-1}-1}{2},$$

где χ_e — тривиальный мультипликативный характер. Если же m четно, то характер η_P тривиален, $G(\eta_P,\overline{\psi}_0)=q-1$, и

$$\mathfrak{N}_u(0)=\frac{\tau}{q}+\frac{\tau}{q(q^m-1)}\,(q-1)\big(G(\overline{\chi}_e,\psi^Q)\chi_e(b)+G(\overline{\eta},\psi^Q)\eta(b)\big).$$

Так как $q^m \equiv 1 \pmod 4$ при четном m, то ввиду утверждения 49

$$\mathfrak{N}_u(0) = \frac{q^m-1}{2q} + \frac{q-1}{2q}(-1 \pm q^{m/2}) = \frac{q^{m-1} \pm (q-1)q^{\frac{m}{2}-1} - 1}{2}.$$

Рассмотрим теперь случай $a \neq 0$. Если m четно, то характер η_P тривиален, и

$$\mathfrak{N}_u(a) = \frac{\tau}{q} + \frac{\tau}{q(q^m-1)}(-1)\big(G(\overline{\chi}_e, \psi^Q)\chi_e(b) + G(\overline{\eta}, \psi^Q)\eta(b)\big) =$$

$$= \frac{q^m-1}{2q} - \frac{1}{2q}(-1 \pm q^{m/2}) = \frac{q^{m-1} \pm q^{\frac{m}{2}-1}}{2}.$$

Если же m нечетно, то

$$\mathfrak{N}_u(a) = \frac{\tau}{q} + \frac{\tau}{q(q^m-1)}\big(G(\overline{\chi}_e, \psi^Q)G(\chi_{eP}, \overline{\psi}_a)\chi_e(b) + G(\overline{\eta}, \psi^Q)G(\eta_P, \overline{\psi}_a)\eta(b)\big).$$

Обозначая $\varepsilon = 0$, если $q \equiv 1 \pmod 4$, и $\varepsilon = 1$, если $q \equiv 3 \pmod 4$, получаем с учетом утверждения 49

$$\mathfrak{N}_u(a) = \frac{q^m-1}{2q} + \frac{1}{2q}\left((-1)(-1) + (\pm i^{\varepsilon} q^{m/2})(\pm i^{\varepsilon} q^{1/2})(\pm 1)\right) =$$

$$= \frac{q^m-1}{2q} + \frac{1}{2q}\left(1 \pm q^{\frac{m+1}{2}}\right) = \frac{q^{m-1} \pm q^{\frac{m-1}{2}}}{2}. \quad \square$$

ЗАДАЧИ

1. Пусть u — ЛРП над кольцом R с характеристическим многочленом $F(x)$ степени m. Докажите, что если $G(x) \in R[x]$ — унитарный многочлен степени $k \geqslant m$, делящийся на $F(x)$, и ЛРП $v \in L_R(G)$ имеет начальный вектор $v[\overline{0, k-1}] = u[\overline{0, k-1}]$, то $v \in L_R(F)$ и $v = u$. (С помощью этого результата легко строить ЛРП $v \in L_R(G)$, у которых минимальный многочлен равен заданному делителю $F(x)$ многочлена $G(x)$.)

2. Пусть $A_{m\times m}$ — матрица над коммутативным кольцом R с единицей, $\alpha^{\downarrow} \in R^{(m)}$ и $A^i\alpha^{\downarrow} = (u_1(i), u_2(i), \ldots, u_m(i))^T$ для $i \in \mathbb{N}_0$. Докажите, что каждая из последовательностей $u_s = (u_s(0), u_s(1), \ldots)$, $s \in \overline{1, m}$, есть ЛРП над R, для которой характеристическим будет любой унитарный многочлен $F(x) \in R[x]$ со свойством $F(A)\alpha^{\downarrow} = 0^{\downarrow}$. В частности, таков характеристический многочлен $\chi_A(x)$ матрицы A.

3. В условиях задачи 2 пусть R — поле, $M(x) = M_{A,\alpha^{\downarrow}}(x)$ — минимальный многочлен вектора $\alpha^{\downarrow}$ относительно A, и $M_s(x) = M_{u_s}(x)$ — минимальный многочлен ЛРП u_s для $s \in \overline{1, m}$. Докажите равенство $M(x) = [M_1(x), \ldots, M_m(x)]$. Приведите примеры, показывающие, что возможны как соотношения $M_s(x) \neq M(x)$ для всех $s \in \overline{1, m}$, так и соотношения $M_s(x) = M(x)$ для всех $s \in \overline{1, m}$.

4. Докажите, что для любой ЛРП над кольцом целых чисел существует единственный минимальный многочлен.

5. Известно, что u — ЛРП порядка m над кольцом R, и дано $2m$ знаков этой последовательности: вектор $u[\overline{0,2m-1}]$. Докажите, что многочлен $F(x) = x^m - f_{m-1}x^{m-1} - \ldots - f_0$ будет характеристическим для ЛРП u тогда и только тогда, когда столбец его коэффициентов $(f_0, f_1, \ldots, f_{m-1})^T$ есть решение системы линейных уравнений

$$\begin{pmatrix} u(0) & u(1) & \ldots & u(m-1) \\ u(1) & u(2) & \ldots & u(m) \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ u(m-1) & u(m) & \ldots & u(2m-2) \end{pmatrix} x^{\downarrow} = \begin{pmatrix} u(m) \\ u(m+1) \\ \ldots\ldots \\ u(2m-1) \end{pmatrix}.$$

Приведите пример, доказывающий, что по $2m-1$ знакам ЛРП u ранга m ее характеристический многочлен не восстанавливается однозначно.

6. Известно, что u — ЛРП порядка m над полем P. Докажите, что $\operatorname{rang} u$ равен рангу матрицы

$$A = \begin{pmatrix} u(0) & u(1) & \ldots & u(m-1) \\ u(1) & u(2) & \ldots & u(m) \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ u(m-1) & u(m) & \ldots & u(2m-2) \end{pmatrix}$$

и равен наибольшему $r \in \overline{1,m}$ такому, что $M_A\binom{1,\ldots,r}{1,\ldots,r} \neq 0$.

7. Найдите минимальный многочлен ЛРП u порядка m над полем P в следующих случаях:

№	P	m	$u[\overline{0,2m-1}]$
1	$GF(2)$	6	(0 1 0 1 0 1 0 0 1 0 1 1)
2	$GF(2)$	6	(0 1 0 1 1 1 1 0 0 0 1 0)
3	$GF(5)$	5	(0 1 2 3 4 4 4 4 0 0)
4	$GF(5)$	6	(1 0 3 1 1 1 2 2 0 0 0 0)
5	$\mathbb{Q}$	4	(1 1 1 2 2 3 4 5)

8. Пусть u — ЛРП над кольцом R с характеристическим многочленом $F(x) = x^m - f_{m-1}x^{m-1} - \ldots - f_0$, и $S(F)$ — сопровождающая матрица для $F(x)$ (см. определение 21 главы 15). Докажите, что для любого $i \in \mathbb{N}_0$ вектор

$$u[\overline{i,\, i+m-1}] = (u(i), u(i+1), \ldots, u(i+m-1))$$

имеет вид $u[\overline{i,\, i+m-1}] = u[\overline{0,m-1}]S(F)^i$, и если $e^{\downarrow} = (e, 0, \ldots, 0)^T$, то $u(i) = u[\overline{0,m-1}]S(F)^i e^{\downarrow}$. Докажите равенство

$$\operatorname{Ann}(u) = \{H(x) \in R[x] :\ u[\overline{0,m-1}] \cdot H(S(F)) = \vec{0}\}.$$

9. Пусть u — ЛРП над кольцом R с характеристическим многочленом $F(x)$ степени m. Докажите, что идеал $\operatorname{Ann}(u)$ порождается многочленом $F(x)$ и всеми много-

членами $H(x) = h_0 + h_1 x + \ldots + h_{m-1}x^{m-1} \in R[x]$, удовлетворяющими условию

$$\begin{pmatrix} u(0) & u(1) & \ldots & u(m-1) \\ u(1) & u(2) & \ldots & u(m) \\ \ldots & \ldots & \ldots & \ldots \\ u(m-1) & u(m) & \ldots & u(2m-2) \end{pmatrix} \begin{pmatrix} h_0 \\ h_1 \\ \ldots \\ h_{m-1} \end{pmatrix} = 0^{\downarrow}.$$

10. Докажите, что если u — ЛРП порядка m над конечным кольцом R, то идеал $\mathrm{Ann}(u)$ в $R[x]$ порождается конечным числом многочленов. В случае, когда $R = \mathbb{Z}/N$, докажите, что идеал $\mathrm{Ann}(u)$ может быть порожден не более чем $m+1$ многочленами и приведите пример, доказывающий, что эту оценку числа образующих нельзя понизить. (*Указание*: воспользуйтесь результатом задачи 9 и тем, что множество многочленов $H(x) \in \mathrm{Ann}(u)$ степени меньшей, чем m, есть подгруппа группы $((\mathbb{Z}/N)^{(m)}, +)$. Для примера рассмотрите ЛРП u над кольцом $\mathbb{Z}/4$ с характеристическим многочленом $x - e$ и начальным вектором $u(0) = 2e$.)

11. Пусть u — ЛРП над полем P с характеристическим многочленом $F(x)$ степени m, и известен вектор $u[i_1, \ldots, i_k] = (u(i_1), \ldots, u(i_k))$. Для $s \in \overline{1,k}$ обозначим через $\Delta_s(x) = \mathrm{Res}(x^{i_s}, F(x))$ остаток от деления x^{i_s} на $F(x)$. Докажите, что по вектору $u[i_1, \ldots, i_k]$ можно однозначно восстановить начальный вектор $u[\overline{0, m-1}]$ ЛРП u тогда и только тогда, когда $k \geqslant m$ и система многочленов $\Delta_1(x), \ldots, \Delta_k(x)$ имеет над P ранг m (как система векторов пространства $P[x]$). *Указание*: решите задачу двумя способами.

а) Покажите, что если $\Delta_s(x) = a_{s,0} + a_{s,1}x + \ldots + a_{s,m-1}x^{m-1}$, то $u(i_s) = a_{s,0}u(0) + \ldots + a_{s,m-1}u(m-1)$ для $s \in \overline{1,k}$, и составьте соответствующую систему линейных уравнений.

б) Используя результат задачи 8, составьте систему линейных уравнений $u[i_1, \ldots, i_k] = u[\overline{0, m-1}] \cdot (S(F)^{i_1}e^{\downarrow}, \ldots, S(F)^{i_k}e^{\downarrow})$ и воспользуйтесь тем, что минимальный многочлен вектора $e^{\downarrow}$ относительно матрицы $S(F)$ равен $F(x)$.

12. В условиях предыдущей задачи покажите, что если $P = GF(q)$ и $\mathrm{rang}\{\Delta_1(x), \ldots, \Delta_k(x)\} = r$, то существует ровно q^{m-r} различных ЛРП $v \in L_P(F)$ со свойством $v[i_1, \ldots, i_k] = u[i_1, \ldots, i_k]$.

13. Найдите все возможные начальные векторы линейных рекуррент $u \in L_P(F)$ над полем $P = GF(2)$ по следующим данным:

№	$F(x)$	$u[i_1, \ldots, i_k]$
1	$x^3 + x + 1$	$u[3,5,6] = (1,1,0)$
2	$x^3 + x + 1$	$u[3,4,6] = (1,1,0)$
3	$x^3 + x + 1$	$u[3,4,6] = (1,1,1)$
4	$x^6 + x^5 + x^4 + x^3 + 1$	$u[1,2,4,5,8,10,15] = (0,0,0,0,0,0,0)$

Вычислите минимальные многочлены этих ЛРП.

14. Пусть u — ЛРП над кольцом R с характеристическим многочленом $F(x) = x^m - f_{m-1}x^{m-1} - \ldots - f_0$ и генератором $\Phi(x)$, и пусть для каждого $i \in \mathbb{N}_0$ $\Phi_i(x) = \operatorname{Res}(x^i\Phi(x), F(x))$ — остаток от деления $x^i\Phi(x)$ на $F(x)$. Докажите равенство

$$\Phi_i(x) = u(i)x^{m-1} + \sum_{s=1}^{m-1}(u(i+s) - f_{m-1}u(i+s-1) - \ldots - f_{m-s}u(i))x^{m-1-s}.$$

15. Найдите генератор и минимальный многочлен ЛРП u над полем P с характеристическим многочленом $F(x)$, если

№	P	$F(x)$	$u[\overline{0,m-1}]$
1	$GF(2)$	x^5+x^2+x+1	$(1,1,1,0,0)$
2	$GF(2)$	x^5+x^2+x+1	$(1,0,0,0,1)$
3	$GF(2)$	x^5+x^2+x+1	$(0,1,0,0,1)$
4	$GF(5)$	$x^4+2x^3+3x^2+4x+1$	$(0,1,2,3)$
5	$GF(5)$	$x^4+2x^3+3x^2+4x+1$	$(0,1,1,3)$
6	$GF(5)$	$x^4+2x^3+3x^2+4x+1$	$(1,2,0,3)$

16. Пусть $P = GF(q)$ и $F(x) \in P[x]$ — унитарный многочлен степени m с каноническим разложением

$$F(x) = G_1(x)^{k_1} \ldots G_t(x)^{k_t}, \quad \deg G_s(x) = n_s \ \text{ для } \ s \in \overline{1,t}.$$

Докажите, что число $\varphi_P(F)$ линейных рекуррент над P с минимальным многочленом $F(x)$ вычисляется по формуле

$$\varphi_P(F(x)) = q^m \cdot \prod_{s=1}^{t}\left(1 - \left(\frac{1}{q}\right)^{n_s}\right) = |P|^{\deg F} \cdot \prod_{s=1}^{t}\left(1 - \left(\frac{1}{|P|}\right)^{\deg G_s}\right).$$

Обратите внимание на то, что это — аналог формулы для функции Эйлера. (*Указание*: сведите задачу к подсчету числа многочленов $\Phi(x) \in P[x]$ со свойствами $\deg\Phi(x) < m$, $(\Phi(x), F(x)) = e$. Обратите внимание, что это число равно $|(P[x]/F(x))^*|$, и воспользуйтесь разложением

$$P[x]/F(x) \cong \bigoplus_{s=1}^{t} P[x]/G_s(x)^{k_s}. \ )$$

17. Докажите, что если $F(x) \in R[x]$ — (единственный) минимальный многочлен ЛРП $u \in R^\infty$ и $F(x) = G(x)H(x)$, то $G(x)$ — (единственный) минимальный многочлен ЛРП $v = H(x)u$.

18. Пусть u — ЛРП над кольцом R с характеристическим многочленом $F(x)$ степени m и генератором $\Phi(x)$. Докажите, что равенство

$$L_R(F) = \{G(x)u : \ G(x) \in R[x], \ \deg G(x) < m\}$$

выполняется тогда и только тогда, когда $(\Phi(x),\ F(x)) = e$.

19. Пусть u — ЛРП над кольцом R с характеристическим многочленом $F(x)$ степени m и $v = G(x)u$ для некоторого $G(x) \in R[x]$. Докажите, что если $(F(x), G(x)) = e$, то последовательность u может быть однозначно восстановлена по v, и для этого достаточно иметь вектор $v[\overline{0, m-1}]$.

20. Пусть в условиях задачи 19 R — поле, и для заданного $G(x)$ последовательность u восстанавливается по v однозначно. Докажите, что $(G(x), F(x)) = e$.

21. Пусть $P = GF(q)$, $F(x) \in P[x]$ — унитарный многочлен степени m и $G(x) \in P[x]$. Известно, что последовательность v получена по закону $v = G(x)u$, где $u \in L_P(F)$, и дано k знаков $v(i_1) = a_1, \ldots, v(i_k) = a_k$ ЛРП v. Докажите, что число различных ЛРП $u \in L_P(F)$, удовлетворяющих выписанным условиям, равно q^{m-r}, где r — ранг системы многочленов $\Delta_1(x), \ldots, \Delta_k(x)$; $\Delta_s(x) = \operatorname{Res}(x^{i_s}G(x), F(x))$ для $s \in \overline{1,k}$. При каких условиях для любого набора констант $a_1, \ldots, a_k \in P$ существует ЛРП $u \in L_P(F)$, удовлетворяющая заданным равенствам?

22. В условиях задачи 21 найдите все возможные начальные векторы ЛРП $u \in L_P(F)$ над полем $P = GF(2)$, если

№	$F(x)$	$G(x)$	$v[i_1, \ldots, i_k]$
1	$x^4 + x + 1$	$x^2 + x + 1$	$v[1,2,5,6] = (0\ 0\ 0\ 0)$
2	$x^4 + x + 1$	$x^2 + x + 1$	$v[0,2,5,6] = (0\ 0\ 0\ 0)$
3	$x^4 + x + 1$	$x^2 + x + 1$	$v[0,2,4,8] = (1\ 0\ 1\ 1)$
4	$x^5 + x^2 + x + 1$	$x^2 + 1$	$v[1,2,3,6] = (1\ 1\ 1\ 1)$
5	$x^5 + x^2 + x + 1$	$x^2 + 1$	$v[0,2,4,8] = (0\ 1\ 0\ 1)$
6	$x^5 + x^2 + x + 1$	$x^2 + 1$	$v[0,4,5] = (0\ 0\ 0)$

23. Пусть u — ЛРП ранга m над полем P с минимальным многочленом $F(x)$. Докажите, что последовательность $v \in P^\infty$ представляется в виде $v = G(x)u$ для некоторого $G(x) \in P[x]$ тогда и только тогда, когда она есть ЛРП, удовлетворяющая условию $M_v(x) \mid F(x)$. При выполнении последнего условия для соответствующего многочлена $G(x)$ должно выполняться неравенство $\deg G(x) \geqslant m - \operatorname{rang} v$.

24. Пусть u — ЛРП над полем P, $H(x) \in P[x]$ и $v = H(x)u$. Докажите, что если неприводимый многочлен $G(x) \in P[x]$ входит в каноническое разложение многочлена $M_v(x)$ над P с кратностью $k > 0$ и кратность $G(x)$ в каноническом разложении $H(x)$ равна $l \geqslant 0$, то кратность $G(x)$ в каноническом разложении $M_u(x)$ равна $k + l$.

25. Найдите минимальный многочлен ЛРП u над полем P по следующей информации:

а) $P = \mathbb{Q}$, $(x-1)^k u = (5, 5, 5, \ldots)$,
б) $P = \mathbb{Q}$, $(x-1)^k u = (0, 1, 2, \ldots)$,
в) $P = GF(2)$, $(x+1)(x^4 + x^2 + 1)u = (1, 1, 1, \ldots)$,
г) $P = GF(2)$, $(x+1)^2(x^2 + x + 1)u = (0, 1, 1, 0, 1, 1, \ldots)$,
д) $P = GF(2)$, $(x+1)^2(x^3+x+1)(x^3+x^2+1)u = (00000010000001\ldots)$,
е) $P = GF(3)$, $(x-1)^2(x^2 + x + 2)u = (1, 1, 1, \ldots)$,
ж) $P = GF(3)$, $(x+1)(x^2 + x + 2)u = (1012202110122021\ldots)$.

26. Пусть u — ЛРП над полем P с характеристическим многочленом $F(x) = (x-\alpha_1)^{k_1+1}\dots(x-\alpha_t)^{k_t+1}$, $\alpha_1,\dots,\alpha_t \in P$ и $\alpha_i \neq \alpha_j$ для $i \neq j$. Докажите, что если разложение u по биномиальному базису пространства $L_P(F)$ имеет вид

$$u = \sum_{s=1}^{t}\sum_{j=0}^{k_s} c_{sj}\alpha_s^{[j]}, \quad c_{sj} \in P,$$

то минимальный многочлен ЛРП u имеет вид

$$M_u(x) = (x-\alpha_1)^{\nu_1+1}\dots(x-\alpha_t)^{\nu_t+1},$$

где для каждого $s \in \overline{1,t}$

$$\nu_s = \begin{cases} -1, & \text{если } c_{s,0} = c_{s,1} = \dots = c_{s,k_s} = 0, \\ \max\{j \in \overline{0,k_s} :\ c_{sj} \neq 0\} & \text{в противном случае.} \end{cases}$$

27. Пусть P — поле, и $\sigma\colon P^\infty \to P^\infty$ — преобразование, определяемое равенством $\sigma(u) = xu$. Докажите, что конечномерное подпространство L пространства P^∞ инвариантно относительно σ тогда и только тогда, когда $L = L_P(F)$ для некоторого унитарного многочлена $F(x) \in P[x]$. Таким образом, все σ-инвариантные конечномерные подпространства в P^∞ — циклические. (*Указание*: если $u \in L$, то u — ЛРП, и при условии $M_u(x) = G(x)$ выполняется включение $L_P(G) \subseteq L$.)

28. Приведите примеры собственных бесконечномерных подпространств в P^∞, инвариантных относительно преобразования σ из задачи 27. Докажите, что их бесконечно много.

29. Пусть $f(x) \in R[x]$ — многочлен степени k, $\alpha \in R$ и $u \in R^\infty$ — последовательность вида $u(i) = f(i)\alpha^i$ для $i \in \mathbb{N}_0$. Докажите, что $u \in L_R((x-\alpha)^{k+1})$.

30. Докажите, что для любого $k \in \mathbb{N}$ последовательность $s_k \in \mathbb{Z}^\infty$, определяемая равенствами

$$s_k(i) = \sum_{n=0}^{i} n^k \quad \text{для } i \in \mathbb{N}_0,$$

есть ЛРП ранга $k+2$, и ее общий член представляется в виде полинома от i степени $k+1$ с коэффициентами из $\mathbb{Q}$. Укажите характеристические многочлены для s_k и указанные представления для $k \in \{2,3,4\}$. Сравните с результатами задачи 11 главы 1.

31. (Задача о размножении кроликов.) Каждая пара зрелых кроликов через месяц рожает новую пару кроликов, которая еще через месяц достигает зрелости. Сколько пар зрелых кроликов можно получить из одной зрелой пары за n лет, $n \in \overline{1,10}$?

32. Пусть Q — расширение поля P, и $F(x) \in P[x]$ — унитарный многочлен. Докажите, что $L_P(F) = P^\infty \cap L_Q(F)$. Заметьте, что базис $e_1^F, \dots, e_m^F$ пространства $L_P(F)$ будет базисом и для $L_Q(F)$.

33. Определите произведение последовательностей u и v над полем P равенством $uv = w \in P^\infty$, где $w(i) = u(i)v(i)$ для $i \in \mathbb{N}_0$. Для произвольного набора подпространств $L_1,\dots,L_r$ из P^∞ определите произведение $L_1\dots L_r$ как подпространство

в P^∞, порожденное всеми произведениями вида $u_1 \dots u_r$, где $u_s \in L_s$ для $s \in \overline{1,r}$. Докажите равенства:

$$L_1(L_2 + L_3) = L_1L_2 + L_1L_3, \quad L_1L_2 = L_2L_1.$$

34. Докажите, что для любых унитарных многочленов $F_1(x), \dots, F_r(x)$ над полем P существует унитарный многочлен $F(x) \in P[x]$ такой, что

$$L_P(F_1) \cdot \dots \cdot L_P(F_r) = L_P(F);$$

этот многочлен называется *дизъюнкцией многочленов* F_1, ..., F_r и обозначается $F(x) = F_1(x) \vee \dots \vee F_r(x)$. (*Указание*: покажите, что $L = L_P(F_1) \cdot \dots \cdot L_P(F_r)$ — конечномерное подпространство в P^∞, инвариантное относительно преобразования сдвига σ, и воспользуйтесь результатом задачи 27.)

35. Для линейных рекуррент из задач 7, 13, 15 выясните, какие из них являются периодическими, и найдите их периоды и длины подходов.

36. Докажите, что период многочлена $F(x) = (x - e)^2$ над конечным кольцом R с единицей равен характеристике этого кольца (т. е. равен $\exp(R, +)$, или, что тоже самое, порядку элемента e группы $(R, +)$). Отсюда следует, что $(T(F) = |R|) \Leftrightarrow (\exists\, n \in \mathbb{N}:\ R \cong \mathbb{Z}/n)$.

37. Докажите, что если ЛРП u над кольцом R имеет единственный минимальный многочлен $G(x)$, то она периодична тогда и только тогда, когда $G(x) \mid x^\lambda(x^t - e)$ для некоторых $\lambda \in \mathbb{N}_0$ и $t \in \mathbb{N}$. При этом наименьшие λ и t с указанным свойством суть $\Lambda(u)$ и $T(u)$.

38. Элемент $c \in R$ называют *мультипликатором* последовательности $u \in R^\infty$, если для некоторого $t \in \mathbb{N}$ выполняется равенство $x^t u = cu$. Пусть $\mathfrak{M}(u)$ — множество всех мультипликаторов последовательности u. Докажите, что если $\mathfrak{M}(u) \neq \varnothing$, то $\mathfrak{M}(u)$ — подполугруппа полугруппы $(R, \cdot)$. Приведите пример периодической последовательности u над конечным кольцом, для которой $\mathfrak{M}(u) \neq \varnothing$. Покажите, что если u — чисто периодическая последовательность, то $\mathfrak{M}(u) \ni e$.

39. Пусть u — последовательность над конечным коммутативным кольцом R с единицей, и множество ее мультипликаторов $\mathfrak{M}(u)$ не пусто. Докажите, что:

а) u — периодическая последовательность;

б) u — вырождающаяся последовательность тогда и только тогда, когда $\mathfrak{M}(u) \ni 0$;

в) u — чисто периодическая последовательность тогда и только тогда, когда $\mathfrak{M}(u) \ni e$. (*Указание*: покажите, что для каждого $r \in R$ существует $t \in \mathbb{N}$ такое, что $r^t = \varepsilon$ — идемпотент, т. е. $\varepsilon^2 = \varepsilon$.)

40. Пусть $u \in R^\infty$ — чисто периодическая последовательность с периодом t, удовлетворяющая условию $\operatorname{Ann}(u) \cap R = 0$. Докажите, что $\mathfrak{M}(u)$ — подгруппа в R^*, и для каждого $c \in \mathfrak{M}(u)$ выполняется равенство $c^t = e$.

41. Пусть $u \in R^\infty$ — чисто периодическая последовательность. *Приведенным периодом* или *предпериодом* последовательности u называется наименьшее $t \in \mathbb{N}$, для которого существует $c \in R$ со свойством $x^t u = cu$. Предпериод последовательности u обозначается через $T_\Pi(u)$. Докажите, что если $x^{T_\Pi(u)} u = cu$ и $\operatorname{Ann}(u) \cap R = 0$,

то $T_\Pi(u) \mid T(u)$, $\mathfrak{M}(u)$ — циклическая подгруппа в R^*, порождаемая элементом c, и $T(u) = T_\Pi(u) \cdot |\mathfrak{M}(u)| = T_\Pi(u) \cdot \operatorname{Ord} c$.

42. Пусть $P = GF(q)$, и u — ЛРП максимального периода над P с минимальным многочленом $F(x)$, $\deg F(x) = m$. Докажите, что приведенный период и группа мультипликаторов ЛРП u удовлетворяют равенствам

$$T_\Pi(u) = \frac{q^m - 1}{q - 1}, \quad \mathfrak{M}(u) = P^*, \quad x^{\frac{q^m-1}{q-1}} \cdot u = (-1)^m F(0) \cdot u.$$

(Используйте представление ЛРП u с помощью функции след.)

43. Пусть $P = GF(2)$ и $u \in P^\infty \setminus (0)$ — такая последовательность, что для любого $k \in \mathbb{N}$ либо $u + x^k u = (0)$, либо существует $l \in \mathbb{N}$ со свойством $u + x^k u = x^l u$. Докажите, что либо $u = (1, 0, 0, 0, \ldots)$, либо u — ЛРП максимального периода над полем P.

44. Докажите, что если $P = GF(q)$, то неприводимый многочлен $F(x) \in P[x]$ степени m является многочленом максимального периода тогда и только тогда, когда выполняются следующие условия:

а) $(-1)^m F(0)$ — примитивный элемент поля P;

б) для любого простого делителя π числа $N = \dfrac{q^m - 1}{q - 1}$ такого, что $\pi \nmid q - 1$, справедливо соотношение

$$x^{N/\pi} \not\equiv \text{const} \pmod{F(x)}.$$

45. Пользуясь методикой, изложенной в § 10, и результатом задачи 44, проверьте, какие из перечисленных ниже неприводимых многочленов $F(x)$ над полем $GF(q)$ имеют максимальный период над этим полем. Вычислите периоды остальных многочленов:

P	$GF(2)$	$GF(3)$	$GF(5)$	$GF(7)$
$F(x)$	$x^4 + x^3 + x^2 + 1$	$x^2 + 1$	$x^2 + x + 2$	$x^2 + 1$
	$x^4 + x + 1$	$x^2 + x + 2$	$x^2 + 2x + 4$	$x^2 + 4$
	$x^6 + x + 1$	$x^3 + 2x + 2$	$x^2 + 2$	$x^2 + x + 3$
	$x^6 + x^3 + 1$	$x^4 + x + 2$	$x^3 + 3x + 2$	
		$x^4 + 2x + 2$		

46. Докажите, что если $F(x)$ — периодический многочлен над полем P и его период $T(F)$ делится на некоторое простое число $\pi \neq \operatorname{Char} P$, то существует неприводимый многочлен $G(x) \in P[x]$ такой, что $G(x) \mid F(x)$ и $\pi \mid T(G)$.

47. Пусть $P = GF(q)$ и $t \in \mathbb{N}$. Докажите, что над P существует неприводимый многочлен $F(x)$, имеющий период t, тогда и только тогда, когда $(q, t) = 1$. Покажите, что при условии $(q, t) = 1$ степени всех неприводимых многочленов из $P[x]$, имеющих период t, равны

$$m = \min\{k \in \mathbb{N} : \ t \mid q^k - 1\}.$$

48. Докажите, что многочлен вида $F(x^k)$, $k > 1$, над конечным полем не может быть многочленом максимального периода.

49. Докажите, что для любого конечного поля P характеристики p и для любого $t \in \mathbb{N}$ ($t > 2$, если $p = 2$) существует чисто периодическая ЛРП над P ранга $r \leqslant t-1$ с периодом t. Приведите примеры, доказывающие, что в общем случае указанная оценка для r не может быть понижена даже при $t > 1$. Рассмотрите следующие случаи:

а) $|P| = 2$, $t = 3, 5, 11, 13, 19$;

б) $|P| = 3$, $t = 2, 5, 7, 19$;

в) $|P| = 5$, $t = 2, 3, 7, 17, 23$;

г) $|P| = 7$, $t = 2, 5, 11, 13, 17, 23$.

50. Укажите наименьший возможный ранг ЛРП u над полем $GF(q)$, имеющей период t, и постройте примеры таких ЛРП в следующих ситуациях:

q	2				4			5		
t	5	10	6	11	5	10	9	31	40	248

51. Укажите число различных ЛРП над полем $GF(2)$, имеющих порядок m и период, делящий t, в следующих случаях:

m	4	5	8	6	8	3	4	7
t	5	5	5	10	10	15	15	15

(*Указание*: опишите возможные минимальные многочлены таких ЛРП и воспользуйтесь результатом задачи 16.)

52. Пусть $F(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0 \in R[x]$ — реверсивный многочлен. *Двойственным к* $F(x)$ называется многочлен

$$F^*(x) = F(0)^{-1}x^m F(1/x) = x^m + a_0^{-1}a_1 x^{m-1} + \ldots + a_0^{-1}a_{m-1}x + a_0^{-1}.$$

Докажите следующие утверждения:

а) $F^{**}(x) = F(x)$;

б) для любого унитарного $G(x) \in R[x]$ условие $G(x) \mid F(x)$ равносильно тому, что $G(x)$ — реверсивный многочлен и $G^*(x) \mid F^*(x)$;

в) многочлен $F(x)$ неприводим над R тогда и только тогда, когда $F^*(x)$ неприводим;

г) элемент $\alpha \in R$ является корнем $F(x)$ тогда и только тогда, когда $\alpha \in R^*$, и α^{-1} — корень $F^*(x)$;

д) если R — поле, и каноническое разложение $F(x)$ над R имеет вид $F(x) = G_1(x)^{k_1} \ldots G_t(x)^{k_t}$, то каноническое разложение $F^*(x)$ над R имеет вид $F^*(x) = G_1^*(x)^{k_1} \ldots G_t^*(x)^{k_t}$;

е) $F(x)$ — периодический многочлен тогда и только тогда, когда $F^*(x)$ периодический, и в случае периодичности $T(F) = T(F^*)$.

53. Пусть u — чисто периодическая последовательность над кольцом R и $T(u) = t$. Для каждого $i \in \mathbb{N}_0$ через $r_t(i)$ обозначим остаток от деления i на t и определим *двойственную к* u *последовательность* u^* условием

$$\forall\, i \in \mathbb{N}_0 : \; u^*(i) = u(t - r_t(i)).$$

Докажите следующие утверждения:

а) если $u = (u(0), u(1), \ldots, u(t-1),\ u(0), \ldots)$, то

$$u^* = (u(0), u(t-1), \ldots, u(1),\ u(0), \ldots)$$

и $T(u^*) = T(u)$;

б) реверсивный многочлен $F(x) \in R[x]$ является характеристическим для ЛРП u тогда и только тогда, когда $F^*(x)$ — характеристический для ЛРП u^*.

54. Реверсивный многочлен $F(x) \in R[x]$ называется *самодвойственным*, если $F^*(x) = F(x)$. Докажите, что неприводимый самодвойственный многочлен $F(x)$ степени m над полем $P = GF(q)$:

а) является многочленом максимального периода тогда и только тогда, когда $q = 2$ и $m = 2$ (т. е. $F(x) = x^2 + x + 1$);

б) существует тогда и только тогда, когда m — четное число. (*Указание*: воспользуйтесь результатом задачи 52 г).)

55. Вычислите цикловой тип семейства $L_P(F)$ в следующих случаях:

а) $P = GF(2),\ F(x) = x^4 + x^3 + x^2 + x + 1$;
б) $P = GF(2),\ F(x) = x^5 + x^2 + x + 1$;
в) $P = GF(2),\ F(x) = x^6 + x^3 + 1$;
г) $P = GF(3),\ F(x) = x^5 + 2x^4 + 2$;
д) $P = GF(3),\ F(x) = x^5 + x^3 + 2x^2 + x + 1$;
е) $P = GF(5),\ F(x) = x^4 + 2x^3 + 3x^2 + 4x + 2$;
ж) $P = GF(5),\ F(x) = x^3 + 3x + 2$.

56. Пусть w — конгруэнтная последовательность над конечным кольцом R:

$$w(0) = a, \quad w(i+1) = cw(i) + b \ \text{ для } \ i \in \mathbb{N}_0.$$

Докажите, что $T(w) \leqslant |R|$, и если $c \notin R^*$, то $T(w) \leqslant |R| - |R^*|$, а если $c \in R^*$ и $c - e \in R^*$, то $T(w) \leqslant |R^*|$. Таким образом, для выполнения равенства $T(w) = |R|$ необходимо выполнение условий $c \in R^*$, $c - e \notin R^*$. (Покажите, что во втором случае $(x - e,\ x - c) = e$, и воспользуйтесь результатами примера 3.)

57. В условиях задачи 56 выведите формулу

$$w(i) = c^i a + (e + c + \ldots + c^{i-1})b \ \text{ для } \ i \in \mathbb{N}$$

и, пользуясь ею, докажите, что если $T(w) = |R|$, то $b \in R^*$. (Заметьте, что если $T(w) = |R|$, то на отрезке последовательности w длины $|R|$ лежат все элементы кольца R, и можно считать, что $a = 0$.)

58. В условиях задачи 56 пусть $R = \mathbb{Z}/p^n$, где p — простое, и выполнены условия $(b, p) = 1$, $c \equiv 1 \pmod p$, а если $p = 2$ и $n \geqslant 2$, то $c \equiv 1 \pmod 4$. Докажите, что тогда $T(w) = p^n$. Каким будет период последовательности w, если $p = 2$, $n \geqslant 3$, $c \equiv 3 \pmod 4$?

59. В условиях задачи 56 пусть $R = \mathbb{Z}/N$, где $N \in \mathbb{N}$. Докажите, что равенство $T(w) = N$ выполняется тогда и только тогда, когда

а) $(b, N) = 1$,

б) $c-1$ делится на любой простой делитель числа N,

в) $4 \mid c-1$, если $4 \mid N$.

(*Указание*: используйте разложение $R \cong \mathbb{Z}/p_1^{n_1} \oplus \ldots \oplus \mathbb{Z}/p_t^{n_t}$.)

60. Вычислите период $T(F)$ и длину подхода $\Lambda(F)$ многочлена $F(x)$ над кольцом $R = \mathbb{Z}/M$ в следующих случаях:

а) $M = 10,\ F(x) = x^4 + 6x^3 + 2x^2 + 5x + 5$;

б) $M = 15,\ F(x) = x^4 + 6x^3 + 14x^2 + 8x + 8$;

в) $M = 30,\ F(x) = x^4 + 6x^3 + 14x^2 + 23x + 23$.

61. Вычислите период и длину подхода ЛРП $u \in L_R(F)$ в следующих случаях:

№	R	$F(x)$	$u[\overline{0, m-1}]$
1	$\mathbb{Z}/6$	$x^5 + 4x^3 + 2x^2 + 3x + 1$	(14140)
2	$\mathbb{Z}/6$	$x^5 + 4x^3 + 2x^2 + 3x + 1$	(13124)
3	$\mathbb{Z}/10$	$x^5 + 7x^4 + 2x^2 + 2x + 1$	(17079)
4	$\mathbb{Z}/10$	$x^5 + 7x^4 + 2x^2 + 2x + 1$	(66141)
5	$\mathbb{Z}/10$	$x^5 + 7x^4 + 2x^2 + 2x + 1$	(61616)

62. Постройте многочлен $F(x)$ степени m над кольцом $\mathbb{Z}/N$, имеющий максимально возможный период, и найдите число линейных рекуррент $u \in L_R(F)$, имеющих период $T(F)$, в следующих случаях:

N	6		10			15			23		30		
m	4	5	4	5	6	3	4	5	2	3	2	3	4

63. Пусть $F(x) \in R[x]$ — реверсивный периодический многочлен. Докажите равенство (см. задачи 53 и 54)

$$L_R(F^*) = \{u^* :\ u \in L_R(F)\}.$$

Покажите, что цикловые типы семейств $L_R(F)$ и $L_R(F^*)$ равны.

64. Пусть $R = \mathbb{Z}/p^n$, p — простое число, $n \geqslant 2$, $F(x) \in R[x]$ — реверсивный многочлен и $T(\overline{F}) = \tau_0$. Докажите, что для некоторых $l \in \overline{1, n}$ и $V(x) \in R[x]$ выполняются соотношения

$$x^{\tau_0} \equiv e + p^l V(x) \,(\mathrm{mod}\, F(x)), \quad \deg V(x) < \deg F(x), \quad \overline{V}(x) \neq \overline{0},$$

и в таком случае

а) если $p^l > 2$ или $p^l = 2$, $n = 2$, то $T(F) = \tau_0 p^{n-l}$,

б) если $p^l = 2$, $n > 2$, то для некоторых $l_1 \in \overline{2, n}$, $V_1(x) \in R[x]$ выполняются соотношения

$$x^{2\tau_0} \equiv e + 2^{l_1} V_1(x) \,(\mathrm{mod}\, F(x)), \quad \deg V_1(x) < \deg F(x), \quad \overline{V}_1(x) \neq \overline{0},$$

и справедливо равенство $T(F) = \tau_0 \cdot 2^{n-l_1+1}$.

65. Вычислите период многочлена $F(x)$ над кольцом $R = \mathbb{Z}/p^n$ в следующих ситуациях:
а) $R = \mathbb{Z}/2^n,\ F(x) = x^5 - x - 1$;
б) $R = \mathbb{Z}/2^n,\ F(x) = x^5 - 2x^3 + x + 1$;
в) $R = \mathbb{Z}/2^n,\ F(x) = x^5 - 4x^4 + 6x^3 - 4x^2 + x - 1$;
г) $R = \mathbb{Z}/2^n,\ F(x) = x^5 - 2x^3 + x + 3$;
д) $R = \mathbb{Z}/5^n,\ F(x) = x^3 + 2x + 1$.

66. Постройте многочлен максимального периода степени m над кольцом R, если
а) $R = \mathbb{Z}/2^n,\ m = 3, 4, 5$;
б) $R = \mathbb{Z}/3^n,\ m = 2, 3, 4$;
в) $R = \mathbb{Z}/5^n,\ m = 2, 3$.

67. Докажите, что если $F(x)$ — многочлен максимального периода над кольцом $R = \mathbb{Z}/p^n$, $n \geqslant 3$, то любой унитарный многочлен $G(x) \in R[x]$ со свойством $G(x) \equiv F(x) \pmod{p^2}$ также будет многочленом максимального периода над R.

68. Для многочленов из задачи 60 вычислите цикловой тип семейства $L_R(F)$.

69. Вычислите цикловой тип семейства $L_R(F)$ в следующих случаях:
а) $R = \mathbb{Z}/p^n,\ \ F(x) = x - (p+1)$;
б) $R = \mathbb{Z}/p^n,\ \ F(x) = (x-1)^2$;
в) $R = \mathbb{Z}/5^n,\ \ F(x) = (x-2)$;
г) $R = \mathbb{Z}/2^n,\ \ F(x) = x^2 + x + 1$;
д) $R = \mathbb{Z}/2^n,\ \ F(x) = x^2 - x - 1$;
е) $R = \mathbb{Z}/10^n,\ F(x) = (x-7)$;
ж) $R = \mathbb{Z}/10^n,\ F(x) = (x-1)^2$.

70. Найдите цикловой тип семейства $L_R(F)$ в следующих ситуациях:
а) $R = \mathbb{Z}/8,\ \ F(x) = x^2 + x + 1$;
б) $R = \mathbb{Z}/8,\ \ F(x) = x^3 - 2x^2 + x - 1$;
в) $R = \mathbb{Z}/2^n,\ F(x) = x^3 - x - 1$;
г) $R = \mathbb{Z}/9,\ \ F(x) = x^3 + 2x + 1$;
д) $R = \mathbb{Z}/9,\ \ F(x) = x^3 + 3x^2 + 2x + 1$;
е) $R = \mathbb{Z}/36,\ F(x) = x^3 + 27x^2 + 20x + 19$.

71. Докажите, что если u — ЛРП над кольцом $R = \mathbb{Z}/p^n$ максимального периода $(p^m - 1)p^{n-1}$, то ее предпериод удовлетворяет равенству

$$T_{\Pi}(u) = \frac{p^m - 1}{p - 1}\, p^k, \quad 1 \leqslant k \leqslant n - 1,$$

причем в случаях $p = 2$, $n > 2$ обязательно $k \geqslant 2$. (Воспользуйтесь тем, что $\overline{u}$ — ЛРП максимального периода над полем $\mathbb{Z}/p$, и используйте результаты задачи 42, теоремы 45 и следствия из теоремы 41.)

72. Докажите соотношения (92) для сумм Гаусса $G(\chi, \psi)$.

73. Пусть $P = GF(q)$, q нечетно, и отображение $\eta\colon P^* \to \mathbb{C}^*$ определяется соотношениями (93). Докажите, что η — мультипликативный характер поля P. Он называется квадратичным характером. Докажите, что η — единственный мультипликативный характер порядка 2, а также единственный нетривиальный мультипликативный характер, тривиальный на подгруппе индекса 2 циклической группы P^*.

74. Пусть u — реверсивная ЛРП над полем $P = GF(q)$ ранга m и периода $\tau \in \{q^m - 1, (q^m - 1)/2\}$, причем q нечетно если $\tau = (q^m - 1)/2$. Выясните, насколько точна оценка теоремы 48 в этих двух случаях, т. е. насколько она отличается от точных значений величин $\nu_u(a)$, указанных в (91) и в теореме 51.

75. Выведите из утверждения 50 формулы (91) для ЛРП максимального периода ранга m над полем $GF(q)$.

Глава 26

ГРАФ ЛИНЕЙНОГО ПРЕОБРАЗОВАНИЯ КОНЕЧНОГО ВЕКТОРНОГО ПРОСТРАНСТВА

§ 1. ПЕРИОД И ДЛИНА ПОДХОДА ЛИНЕЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ

Пусть V_P — *конечное векторное пространство*, т. е. пространство конечной размерности n над конечным полем $P = GF(q)$. Для произвольного линейного преобразования $\varphi \in \mathfrak{L}(V_P)$ и любого вектора $\alpha \in V_P$ можно построить последовательность $\alpha^\varphi \in V^\infty$ вида

$$\alpha^\varphi = (\alpha, \varphi(\alpha), \ldots, \varphi^i(\alpha), \ldots). \tag{1}$$

Определение 1. Последовательность (1) называется *линейной последовательностью*, порождаемой вектором α и преобразованием φ.

Пример 1. Пусть $V = P^n$ — пространство векторов-строк, $F(x) = x^n - f_{n-1}x^{n-1} - \ldots - f_0$ — многочлен над P, и $\varphi \in \mathfrak{L}(P_P^n)$ — линейное преобразование, матрица которого в единичном базисе $\vec{e}$ пространства P_P^n есть сопровождающая матрица для многочлена $F(x)$ (см. определение 21 главы 15), т. е. $A_{\vec{e}}(\varphi) = S(F)$. Тогда для любого вектора $\alpha = (u(0), \ldots, u(n-1)) \in P^n$ справедливо равенство $\varphi(\alpha) = \alpha S(F)$, и линейная последовательность α^φ есть последовательность векторов длины n вида

$$\alpha^\varphi(i) = \varphi^i(\alpha) = (u(i), u(i+1), \ldots, u(i+n-1)) = u[\overline{i, i+n-1}],$$

где u — ЛРП с характеристическим многочленом $F(x)$ и начальным вектором $u[\overline{0, n-1}] = \alpha$.

В этой главе дается описание периода и длины подхода произвольной линейной последовательности и изучаются параметры совокупности всех линейных последовательностей, порождаемых данным преобразованием φ. В частности, для случая, когда φ — обратимое линейное преобразование, т. е. подстановка на V, указывается способ расчета цикловой структуры подстановки φ.

Из примера 1 видно, что, изучая в предыдущей главе ЛРП над полем P, мы, по сути дела, изучали частный случай рассматриваемой ситуации, когда V_P — пространство, циклическое относительно преобразования φ.

Теорема 1. *Пусть V — конечное векторное пространство над полем P, $\varphi \in \mathfrak{L}(V_P)$, и α — вектор из V с минимальным многочленом $m_{\alpha,\varphi}(x) = F(x)$. Тогда линейная последовательность α^φ есть периодическая последовательность, и*

$$\Lambda(\alpha^\varphi) = \Lambda(F), \quad T(\alpha^\varphi) = T(F). \tag{2}$$

□ По определению 12 главы 25 периодичность последовательности α^φ равносильна существованию параметров $\lambda \in \mathbb{N}_0$ и $t \in \mathbb{N}$ таких, что

$$\forall\, i \geqslant \lambda\colon\ \varphi^{i+t}(\alpha) = \varphi^i(\alpha). \tag{3}$$

Последнее условие, очевидно, эквивалентно равенству $\varphi^{\lambda+t}(\alpha) = \varphi^\lambda(\alpha)$, которое, в свою очередь, равносильно соотношению

$$F(x) \mid x^\lambda(x^t - e). \tag{4}$$

Так как $F(x)$ — унитарный многочлен над конечным полем, то по теореме 25 главы 25 он является периодическим, т. е. существуют параметры $\lambda \in \mathbb{N}_0$ и $t \in \mathbb{N}$, удовлетворяющие условию (4). Следовательно, α^φ — периодическая последовательность.

Равенства (2) теперь легко следуют из определений ввиду эквивалентности соотношений (3) и (4). □

Следствие 1. *Если в обозначениях теоремы* 1 *минимальный многочлен преобразования φ есть $m_\varphi(x) = G(x)$, то для любого вектора $\alpha \in V_P$ справедливы соотношения*

$$\Lambda(\alpha^\varphi) \leqslant \Lambda(G), \quad T(\alpha^\varphi) \mid T(G), \tag{5}$$

и существуют векторы $\alpha \in V_P$, для которых

$$\Lambda(\alpha^\varphi) = \Lambda(G), \quad T(\alpha^\varphi) = T(G). \tag{6}$$

□ Соотношения (5) следуют из (2) и условия $F(x) \mid G(x)$.

В качестве вектора α, для которого выполняются равенства (6), можно выбрать любой вектор $\alpha \in V$ со свойством $m_{\alpha,\varphi}(x) = G(x)$ (по теореме 33 главы 15 такие векторы существуют). □

Замечание 1. Равенства (6) могут выполняться и для такого вектора $\alpha \in V$, у которого минимальный многочлен $F(x)$ является собственным делителем многочлена $G(x)$. Соответствующий пример читателю предлагается подобрать самостоятельно.

Следствие 2. *Если V_P — пространство из $q^n > 2$ элементов, то для любых $\varphi \in \mathfrak{L}(V)$ и $\alpha \in V$ последовательность α^φ удовлетворяет условию*

$$\Lambda(\alpha^\varphi) + T(\alpha^\varphi) \leqslant q^n - 1.$$

□ Если $F(x) = m_{\alpha,\varphi}(x)$, то $\deg F(x) = m \leqslant n$, и ввиду теоремы 1 $\Lambda(\alpha^\varphi) + T(\alpha^\varphi) = \Lambda(F) + T(F)$. Остается заметить, что по теореме 25 главы 25 $\Lambda(F) + T(F) \leqslant q^m - 1$, если $q^m > 2$, и $\Lambda(F) + T(F) \leqslant q^m$, если $q^m = 2$ (см. замечание к указанной теореме), причем в последнем случае $q^m < q^n - 1$. □

Определение 2. В пространстве V из q^n элементов линейная последовательность (1), удовлетворяющая условию $T(\alpha^\varphi) = q^n - 1$, называется *линейной последовательностью максимального периода*.

Очевидно, что α^{φ} — последовательность максимального периода тогда и только тогда, когда $\alpha \neq \theta$ и $\chi_{\varphi}(x)$ — многочлен максимального периода над P. При выполнении последнего условия φ — подстановка на V, для которой разложение на независимые циклы имеет вид

$$\varphi = (\theta) \cdot (\alpha,\, \varphi(\alpha),\, \ldots,\, \varphi^{q^n-2}(\alpha)).$$

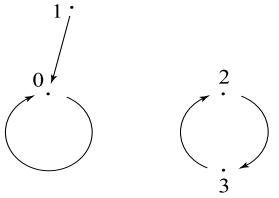
§ 2. ГРАФЫ ПРЕОБРАЗОВАНИЙ И ИХ ЧИСЛОВЫЕ ХАРАКТЕРИСТИКИ

Определение 3. *Графом* с множеством *вершин* Ω называется пара объектов $\Gamma = (\Omega, R)$, где $R \subset \Omega \times \Omega$. Множество R называют множеством *ребер*, или *дуг* графа Γ. При этом говорят, что $(a, b) \in R$ есть ребро из вершины a в вершину b графа Γ.

Наглядно граф можно представить как некоторое множество точек плоскости (вершин), некоторые из которых соединены стрелками (ребрами).

Пример 2. На следующем рисунке изображен граф

$$\Gamma = (\{0,1,2,3\},\ \{(0,0),\ (1,0),\ (2,3),\ (3,2)\}).$$



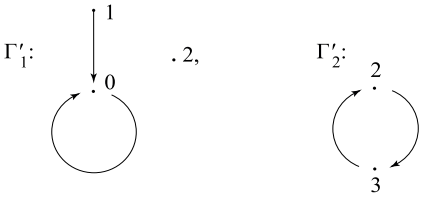
1. В дальнейшем нам понадобятся следующие отношения между графами и операции над ними.

Определение 4. Говорят, что граф $\Gamma = (\Omega', R')$ есть *подграф* графа $\Gamma = (\Omega, R)$ и пишут $\Gamma' \subset \Gamma$, если $\Omega' \subset \Omega$ и $R' \subset R$. Граф $\Gamma = (\Omega, R)$ называется *объединением графов* $\Gamma_1 = (\Omega_1, R_1)$, $\ldots$, $\Gamma_t = (\Omega_t, R_t)$, если $\Omega = \Omega_1 \cup \ldots \cup \Omega_t$ и $R = R_1 \cup \ldots \cup R_t$. Если при этом $\Omega_i \cap \Omega_j = \varnothing$, то говорят, что графы Γ_i и Γ_j *не пересекаются*.

Пример 3. Граф Γ из примера 2 есть объединение непересекающихся подграфов $\Gamma_1 = (\{0,1\},\ \{(0,0),\ (1,0)\})$ и $\Gamma_2 = (\{2,3\},\ \{(2,3),\ (3,2)\})$. Но тот же граф можно представить и как объединение пересекающихся подграфов

$$\Gamma_1' = (\{0,1,2\},\ \{(0,0),\ (1,0)\}) \quad \text{и} \quad \Gamma_2' = (\{2,3\},\ \{(2,3),\ (3,2)\}),$$

которые изображаются следующим образом:



Определение 5. Графы $\Gamma = (\Omega, R)$ и $\Gamma' = (\Omega', R')$ называют *изоморфными* и пишут $\Gamma \cong \Gamma'$, если существует биекция $\tau\colon \Omega \to \Omega'$ такая, что

$$\forall\, a, b \in \Omega\colon\ (a,b) \in R \ \Leftrightarrow\ (\tau(a), \tau(b)) \in R'.$$

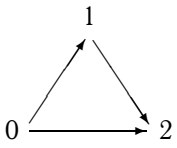
Отображение τ при этом называют *изоморфизмом графа* Γ *на граф* Γ'.

2. В дальнейшем мы будем предполагать всегда, что Ω — конечное множество, и изучать графы следующего специального типа.

Определение 6. *Графом преобразования* $f\colon \Omega \to \Omega$ множества Ω называют граф $\Gamma(f) = (\Omega, R_f)$, в котором

$$R_f = \{(a, f(a))\colon\ a \in \Omega\}.$$

Пример 4. Граф Γ из примера 2 есть граф преобразования $f = \left(\begin{smallmatrix} 0 & 1 & 2 & 3 \\ 0 & 0 & 3 & 2 \end{smallmatrix}\right)$. Граф Γ_1' из примера 3 не является графом преобразования. Не будет графом преобразования, например, и граф



Утверждение 2. *Произвольный граф* $\Gamma = (\Omega, R)$ *есть граф некоторого преобразования* $f\colon \Omega \to \Omega$ *тогда и только тогда, когда для каждой вершины* $a \in \Omega$ *существует единственная вершина* $b \in R$ *такая, что* $(a,b) \in R$.

□ Соответствующее преобразование f задается условием: $f(a) = b$, если $(a,b) \in R$. □

Утверждение 3. *Граф* $\Gamma(f')$ *преобразования* $f'\colon \Omega' \to \Omega'$ *является подграфом графа* $\Gamma(f)$ *преобразования* $f\colon \Omega \to \Omega$ *тогда и только тогда, когда* Ω' *— подмножество множества* Ω, *инвариантное относительно преобразования* f (*т. е. такое, что* $f(\Omega') \subset \Omega'$), *и* $f\big|_{\Omega'} = f'$.

□ Если $\Omega' \subset \Omega$, $f(\Omega') \subset \Omega'$ и $f' = f\big|_{\Omega'}$, то для любых $a, b \in \Omega'$ справедливы импликации:

$$(a,b) \in R_{f'} \ \Rightarrow\ f'(a) = b \ \Rightarrow\ f(a) = b \ \Rightarrow\ (a,b) \in R_f.$$

Поэтому $R_{f'} \subset R_f$, и $\Gamma(f')$ — подграф $\Gamma(f)$. Наоборот, если $\Gamma(f') \subset \Gamma(f)$, то по определению 4 $\Omega' \subset \Omega$, $R_{f'} \subset R_f$, и по определению 6 для любого $a \in \Omega$ справедливы импликации:

$$a \in \Omega' \ \Rightarrow\ (a, f'(a)) \in R_{f'} \ \Rightarrow\ (a, f'(a)) \in R_f \ \Rightarrow\ f(a) = f'(a) \in \Omega'.$$

Следовательно, $f(\Omega') \subset \Omega'$ и $f\big|_{\Omega'} = f'$. □

Утверждение 4. *Графы* $\Gamma(f)$ *и* $\Gamma(f')$ *преобразований соответственно* $f\colon \Omega \to \Omega$ *и* $f'\colon \Omega' \to \Omega'$ *изоморфны тогда и только тогда, когда существует биекция* $\tau\colon \Omega \to \Omega'$ *такая, что*

$$\forall\, a \in \Omega:\ \ f'(\tau(a)) = \tau(f(a)),$$

т. е. $\tau^{-1} \circ f' \circ \tau = f$.

□ По определению 5 биекция $\tau\colon \Omega \to \Omega'$ является изоморфизмом графа $\Gamma(f)$ на $\Gamma(f')$ тогда и только тогда, когда

$$\forall\, a, b \in \Omega:\ \ (a,b) \in R_f \ \Leftrightarrow\ (\tau(a), \tau(b)) \in R_{f'},$$

т. е. тогда и только тогда, когда

$$\forall\, a, b \in \Omega:\ \ b = f(a) \ \Leftrightarrow\ \tau(b) = f'(\tau(a)).$$

Последнее условие, очевидно, равносильно условию на τ из формулировки утверждения 4. □

Определение 7. Точки $a, b \in \Omega$ назовем *связанными преобразованием* $f\colon \Omega \to \Omega$, или *$f$-связанными*, если $f^i(a) = f^j(b)$ для некоторых $i, j \in \mathbb{N}_0$. В этом случае будем писать $a \underset{f}{\sim} b$ (при этом $a \underset{f}{\sim} a$, так как $f^0(a) = a$).

Нетрудно видеть, что отношение $\underset{f}{\sim}$ есть отношение эквивалентности на Ω.

Замечание 2. Если f — подстановка на Ω и $G = \langle f \rangle$ — порождаемая ею подгруппа в $S(\Omega)$, то отношение $\underset{f}{\sim}$ совпадает с отношением $\underset{G}{\sim}$, введенным в определении 24 главы 11. Таким образом, определение 7 есть обобщение определения 24 главы 11 (для $G = \langle f \rangle$) на случай произвольного преобразования f.

Определение 8. Граф $\Gamma(f)$ преобразования $f\colon \Omega \to \Omega$ называют *связным*, если любые две его вершины связаны преобразованием f.

Заметим, что в частном случае, когда f — подстановка на Ω, связность графа $\Gamma(f)$ означает, что f — цикл длины $|\Omega|$.

Утверждение 5. *Для произвольного преобразования* $f\colon \Omega \to \Omega$ *классы* $\Omega_1, \ldots, \Omega_t$, *на которые множество* Ω *разбивается отношением* $\underset{f}{\sim}$, *инвариантны относительно* f. *Если* $f_s = f\big|_{\Omega_s}$, $s \in \overline{1,t}$, *то каждый граф* $\Gamma(f_s)$ *связен и*

$$\Gamma(f) = \Gamma(f_1) \cup \ldots \cup \Gamma(f_t). \tag{7}$$

□ Так как по определению 7 $f(a) \underset{f}{\sim} a$ для любого $a \in \Omega$, то из включения $a \in \Omega_s$ следует включение $f(a) \in \Omega_s$, т. е. $f(\Omega_s) \subset \Omega_s$.

Пусть $a, b \in \Omega_s$. Тогда $f^i(a) = f^j(b)$ для подходящих $i, j \in \mathbb{N}_0$, и так как $f_s = f\big|_{\Omega_s}$, то $f_s^i(a) = f_s^j(b)$, т. е. $a \underset{f_s}{\sim} b$. Следовательно, граф $\Gamma(f_s)$ связен.

Равенство (7) доказывается следующим образом. Для любых $a, b \in \Omega$ включение $(a,b) \in R_f$ равносильно условию $b = f(a)$. А последнее означает, что $a, b \in \Omega_s$ для подходящего $s \in \overline{1,t}$, и $b = f_s(a)$, т. е. $(a,b) \in R_{f_s}$. Следовательно, $R_f = R_{f_1} \cup \ldots \cup R_{f_t}$. □

Определение 9. В условиях утверждения 5 графы $\Gamma(f_1), \ldots, \Gamma(f_t)$ называются *компонентами связности* графа $\Gamma(f)$.

3. Теперь для описания возможного строения произвольного графа $\Gamma(f)$ достаточно описать его строение при условии, что он связный. Для этого введем следующую классификацию вершин и подграфов графа $\Gamma(f)$.

Определение 10. Вершина a графа $\Gamma(f)$ называется *циклической*, или *регулярной*, если

$$\exists\, t \in \mathbb{N}: \ f^t(a) = a,$$

точкой подхода, если

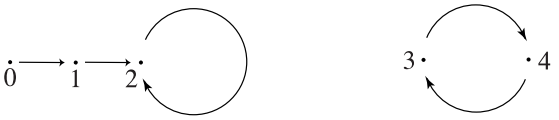
$$\forall\, t \in \mathbb{N}: \ f^t(a) \neq a,$$

начальной, если на Ω не разрешимо уравнение $f(x) = a$.

Граф называется *регулярным*, если все его вершины регулярны.

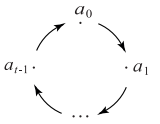
Очевидно, любая начальная вершина в графе $\Gamma(f)$ является точкой подхода, но обратное, вообще говоря, неверно. Регулярность графа $\Gamma(f)$ равносильна биективности преобразования f.

Пример 5. Граф преобразования $f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 2 & 4 & 3 \end{pmatrix}$ имеет вид



На этом рисунке: 2, 3, 4 — регулярные вершины графа, 0, 1 — точки подхода, 0 — начальная вершина.

Определение 11. *Циклом длины* $t \in \mathbb{N}$ в графе $\Gamma(f) = (\Omega, R_f)$ называется любой подграф вида $\Gamma(f') = (\Omega', R_{f'})$, в котором Ω' — подмножество множества Ω мощности t, инвариантное относительно f, и $f' = f\big|_{\Omega'}$ — подстановка, являющаяся полным циклом на Ω', т. е. любой подграф вида



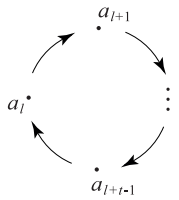
Очевидно, вершина a графа $\Gamma(f)$ является циклической тогда и только тогда, когда она принадлежит некоторому циклу в графе $\Gamma(f)$.

Пример 6. Граф $\Gamma(f)$ из примера 5 имеет один цикл длины 1 и один цикл длины 2:

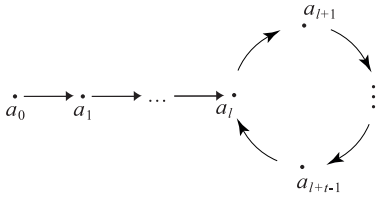
Определение 12. *Подходом длины* l в графе $\Gamma(f)$ называют любой подграф вида

$$\underset{a_0}{\bullet} \longrightarrow \underset{a_1}{\bullet} \longrightarrow \ldots \longrightarrow \underset{a_{l-1}}{\bullet} \longrightarrow \underset{a_l}{\bullet}, \tag{8}$$

в котором a_0 — начальная точка, $a_1, \ldots, a_{l-1}$ — точки подхода, a_l — циклическая точка. Если при этом вершина a_l принадлежит циклу



то подграф (8) называют *подходом к циклу* (9) из начальной вершины a_0, а подграф



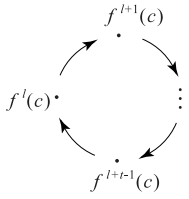
называют *циклом с подходом*.

Утверждение 6. *Если* $\Gamma(f)$ *— связный граф, то он есть либо цикл, либо цикл с подходами к нему.*

□ В графе $\Gamma(f)$ есть по крайней мере один цикл. Действительно, если $c \in \Omega$, то ввиду конечности Ω последовательность элементов из Ω:

$$c,\ f(c),\ \ldots,\ f^i(c),\ \ldots$$

периодична. Если l и t — соответственно длина подхода и период этой последовательности, то в графе $\Gamma(f)$ есть цикл



Из приведенных рассуждений следует также, что любая вершина $c \in \Omega$ принадлежит либо циклу графа $\Gamma(f)$, либо подходу к циклу.

Остается показать, что в графе $\Gamma(f)$ есть лишь один цикл. Действительно, пусть a, b — две циклические вершины графа. Тогда $f^t(a) = a$ для подходящего $t \in \mathbb{N}$, и

так как $\Gamma(f)$ связен, то $f^i(a) = f^j(b)$ для подходящих $i, j \in \mathbb{N}_0$. Выбирая $k \in \mathbb{N}$ из условия $kt \geqslant i$, получаем равенства

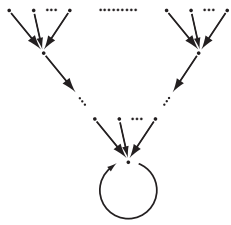
$$a = f^{kt}(a) = f^{kt-i}(f^i(a)) = f^{kt-i}(f^j(b)) = f^{kt-i+j}(b),$$

из которых следует, что a и b лежат на одном цикле. □

Важный частный тип графов преобразований описывает

Определение 13. Связный граф $\Gamma(f)$ с единственной циклической вершиной a называется *деревом с корнем* a.

Общий вид дерева можно изобразить следующим образом:



Утверждение 7. *Граф* $\Gamma(f)$ *является деревом тогда и только тогда, когда он имеет единственную циклическую вершину.*

□ Так как по утверждениям 5 и 6 число компонент связности графа $\Gamma(f)$ не превосходит числа его циклических вершин, то граф с единственной циклической вершиной связен и удовлетворяет определению 13. □

Непосредственно из утверждений 5 и 6 следует

Теорема 8. *Граф* $\Gamma(f)$ *произвольного преобразования* f *конечного множества* Ω *есть объединение конечного числа попарно не пересекающихся циклов с подходами.*

Очевидно, что в случае, когда граф $\Gamma(f)$ регулярен (т. е. f — подстановка на Ω), утверждение теоремы 8 эквивалентно утверждению теоремы 27 главы 11 о разложении подстановок в произведение независимых циклов.

4. В дальнейшем мы будем изучать следующие числовые характеристики графов преобразований.

Определение 14. *Цикловым типом* графа $\Gamma(f)$ преобразования f конечного множества Ω (или просто цикловым типом преобразования f) назовем многочлен над $\mathbb{Z}$ вида

$$\mathcal{C}_f(y) = \sum_{t \geqslant 1} C_f^{(t)} y^t,$$

в котором $C_f^{(t)}$ — количество циклов длины t в графе $\Gamma(f)$. В случае, если f — подстановка на Ω, цикловой тип f есть лишь другая форма записи цикловой структуры f.

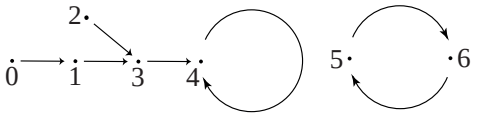
Отметим, что цикловой тип графа $\Gamma(f)$ не определяет его однозначно с точностью до изоморфизма, поскольку в $\mathcal{C}_f(y)$ нет информации о подходах к циклам. Цикловые типы изоморфных графов равны. Обратное утверждение, вообще говоря, неверно. Однако если f и g — подстановки, то

$$\Gamma(f) \cong \Gamma(g) \;\Leftrightarrow\; \mathcal{C}_f(y) = \mathcal{C}_g(y).$$

Для нерегулярных графов важны следующие характеристики.

Определение 15. *Расстоянием от вершины* c графа $\Gamma(f)$ *до цикла* этого графа назовем параметр $\lambda_f(c)$, равный наименьшему $l \in \mathbb{N}_0$ такому, что $f^l(c)$ — циклическая вершина. *Степенью вершины* c в графе $\Gamma(f)$ назовем общее число $\sigma_f(c)$ дуг, входящих в вершину c и выходящих из нее.

Пример 7. Граф преобразования $f = \begin{pmatrix} 0&1&2&3&4&5&6 \\ 1&3&3&4&4&6&5 \end{pmatrix}$ имеет вид



Его числовые характеристики таковы: $\mathcal{C}_f(y) = y + y^2$,

$$\lambda_f(0) = 3, \quad \lambda_f(1) = \lambda_f(2) = 2, \quad \lambda_f(3) = 1, \quad \lambda_f(4) = \lambda_f(5) = \lambda_f(6) = 0;$$

$$\sigma_f(0) = \sigma_f(2) = 1, \quad \sigma_f(3) = \sigma_f(4) = 3, \quad \sigma_f(1) = \sigma_f(5) = \sigma_f(6) = 2.$$

Отметим, что в графе произвольного преобразования $f\colon \Omega \to \Omega$ из любой вершины $c \in \Omega$ выходит ровно одна дуга, поэтому число дуг, входящих в c, равно $\sigma_f(c) - 1$, и начальные вершины характеризуются равенством $\sigma_f(c) = 1$. Циклические вершины характеризуются равенством $\lambda_f(c) = 0$. Для любой вершины $c \in \Omega$ длина подхода последовательности

$$c,\, f(c),\, \ldots,\, f^i(c),\, \ldots$$

равна $\lambda_f(c)$, а ее период равен длине соответствующего цикла в графе.

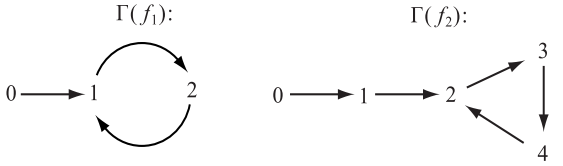
§ 3. ДЕКАРТОВО ПРОИЗВЕДЕНИЕ ГРАФОВ ПРЕОБРАЗОВАНИЙ

Определение 16. Пусть $f_i\colon \Omega_i \to \Omega_i$, $i \in \overline{1,k}$, — преобразования конечных множеств. Их *декартовым произведением* называют преобразование $f = f_1 \times \ldots \times f_k$ множества $\Omega = \Omega_1 \times \ldots \times \Omega_k$, определяемое условием

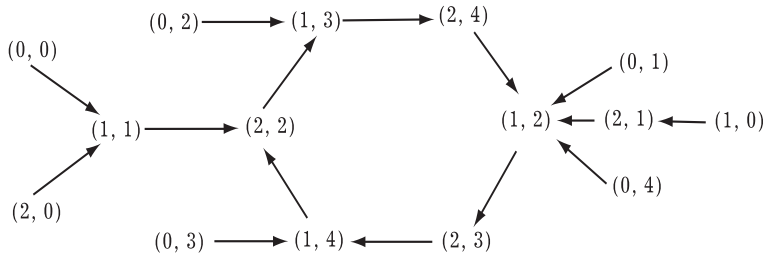
$$\forall\, (a_1, \ldots, a_k) \in \Omega_1 \times \ldots \times \Omega_k\colon \;\; f((a_1, \ldots, a_k)) = (f_1(a_1), \ldots, f_k(a_k)).$$

Тогда граф $\Gamma(f)$ называют *декартовым произведением* графов $\Gamma(f_1), \ldots, \Gamma(f_k)$ и обозначают $\Gamma(f) = \Gamma(f_1) \times \ldots \times \Gamma(f_k)$.

Пример 8. Пусть f_1 и f_2 — преобразования множеств $\Omega_1 = \{0,1,2\}$ и $\Omega_2 = \{0,1,2,3\}$, описываемые графами, соответственно



Тогда граф $\Gamma(f_1) \times \Gamma(f_2)$ имеет вид



Теорема 9. *При обозначениях из определения* 16 *пусть* $\Gamma(f) = \Gamma(f_1) \times \ldots \times \Gamma(f_k)$ *и* $\vec{a} = (a_1, \ldots, a_k) \in \Omega$. *Тогда справедливы свойства*:

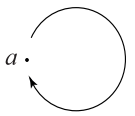
(а) $\lambda_f(\vec{a}) = \max\{\lambda_{f_1}(a_1), \ldots, \lambda_{f_k}(a_k)\}$, *в частности,* $\vec{a}$ *— циклическая вершина в* $\Gamma(f)$ *тогда и только тогда, когда* a_i *— циклическая вершина в* $\Gamma(f_i)$ *для* $i \in \overline{1,k}$;

(б) $\sigma_f(\vec{a}) = 1 + (\sigma_{f_1}(a_1) - 1)(\sigma_{f_2}(a_2) - 1) \ldots (\sigma_{f_k}(a_k) - 1)$, *в частности* $\vec{a}$ *— начальная вершина в* $\Gamma(f)$ *тогда и только тогда, когда хотя бы одна ее компонента* a_i *— начальная вершина в* $\Gamma(f_i)$;

(в) $\mathcal{C}_f(y) = \mathcal{C}_{f_1}(y) * \ldots * \mathcal{C}_{f_k}(y)$, *где* $*$ *— операция композиции цикловых типов* (*определение* 20 главы 25).

□ Доказательства утверждений (а) и (б) предоставляются читателю в качестве упражнений. Доказательство утверждения (в) проводится с помощью тех же рассуждений, которые использовались в доказательстве теоремы 35 главы 25. □

Полезно заметить, что если $f_1 \colon \Omega_1 \to \Omega_1$ — единственное преобразование одноэлементного множества $\Omega_1 = \{a\}$, то граф $\Gamma(f_1)$ имеет вид:



и для любого преобразования $f_2 \colon \Omega_2 \to \Omega_2$ граф $\Gamma(f_1) \times \Gamma(f_2)$ изоморфен $\Gamma(f_2)$.

§ 4. ПАРАМЕТРЫ ГРАФА ЛИНЕЙНОГО ПРЕОБРАЗОВАНИЯ

При доказательствах приводимых ниже теорем используются результаты главы 15, ссылки на которые читателю предлагается подобрать самостоятельно.

1. Пусть φ — линейное преобразование пространства V_P размерности n, и $|P| = q$. Опишем сначала некоторые общие свойства графа $\Gamma(\varphi)$.

Теорема 10. (а) *Если* $\operatorname{rang}\varphi = r$, *то в графе* $\Gamma(\varphi)$ *существует ровно* $q^n - q^r$ *начальных вершин, а степень каждой не начальной вершины равна* $q^{n-r}+1$;

(б) *в графе* $\Gamma(\varphi)$ *расстояние* $\lambda_\varphi(\alpha)$ *от вершины* α *до цикла и длина* t *этого цикла удовлетворяют равенствам*

$$\lambda_\varphi(\alpha) = \Lambda(m_{\alpha,\varphi}(x)), \quad t = T(m_{\alpha,\varphi}(x));$$

(в) *граф* $\Gamma(\varphi)$ *является деревом с петлей тогда и только тогда, когда* $\chi_\varphi(x) = x^n$.

□ (а) Множество начальных вершин графа $\Gamma(\varphi)$ есть, очевидно, $V \setminus \varphi(V)$, и $|V \setminus \varphi(V)| = |V| - |\varphi(V)| = q^n - q^r$. Если $\alpha \in \varphi(V)$, то число дуг, входящих в вершину α, равно $|\varphi^{-1}(\alpha)| = |\operatorname{Ker}\varphi| = q^{n-r}$.

(б) Параметры $\lambda_\varphi(\alpha)$ и t равны соответственно длине подхода и периоду последовательности α^φ, поэтому нужные равенства следуют из теоремы 1.

(в) Вершина θ является циклической в любом графе $\Gamma(\varphi)$ (она принадлежит циклу длины 1). Поэтому согласно утверждению 7 граф $\Gamma(\varphi)$ — дерево тогда и только тогда, когда θ — его единственная циклическая вершина, т. е. тогда и только тогда, когда любой вектор $\alpha \in V$ удовлетворяет условию $\varphi^{\lambda_\varphi(\alpha)}(\alpha) = \theta$ (см. определение 13). Последнее, очевидно, равносильно тому, что минимальный многочлен каждого вектора α имеет вид x^l, т. е. $\chi_\varphi(x) = x^n$. □

Пример 9. Пусть $\chi_\varphi(x) = m_\varphi(x) = x^n$. Тогда $\Gamma(\varphi)$ — дерево с корнем θ, и так как $\operatorname{rang}\varphi = n-1$, то в $\Gamma(\varphi)$ существует ровно $q^n - q^{n-1}$ начальных вершин; в каждую неначальную вершину входит ровно q дуг, и расстояние от каждой начальной вершины до корня θ равно n. Множество начальных вершин этого графа есть множество всех векторов $\alpha \in L$ со свойством $m_{\alpha,\varphi}(x) = x^n$. Дерево с описанными здесь числовыми параметрами назовем *деревом типа* $D_q(n)$.

2. Дальнейшее уточнение строения графа $\Gamma(\varphi)$ основано на следующих результатах.

Теорема 11. *Пусть пространство* V_P *раскладывается в прямую сумму подпространств, инвариантных относительно преобразования* φ:

$$V = V_1 \dotplus V_2, \quad \varphi(V_s) \subset V_s, \quad s \in \overline{1,2},$$

и пусть $\varphi_s = \varphi\big|_{V_s}$, $s \in \overline{1,2}$. *Тогда*

$$\Gamma(\varphi) \cong \Gamma(\varphi_1) \times \Gamma(\varphi_2).$$

□ Каждый вектор $\alpha \in V$ однозначно представляется в виде $\alpha = \alpha_1 + \alpha_2$, где $\alpha_1 \in V_1$, $\alpha_2 \in V_2$. Поэтому отображение $\tau\colon V \to V_1 \times V_2$ по правилу $\tau(\alpha) = (\alpha_1, \alpha_2)$ есть корректно заданная биекция. Остается заметить, что для любых $\alpha, \beta \in V$ справедливы импликации

$$\begin{aligned}(\alpha,\beta) \in R_\varphi \;&\Leftrightarrow\; \beta = \varphi(\alpha) \;\Leftrightarrow\; (\beta_1 = \varphi_1(\alpha_1),\ \beta_2 = \varphi_2(\alpha_2)) \;\Leftrightarrow\\ &\Leftrightarrow\; (\beta_1,\beta_2) = (\varphi_1 \times \varphi_2)((\alpha_1,\alpha_2)) \;\Leftrightarrow\; (\tau(\alpha),\tau(\beta)) \in R_{\varphi_1\times\varphi_2},\end{aligned}$$

и потому, согласно определениям 5 и 16, τ — изоморфизм графов $\Gamma(\varphi)$ и $\Gamma(\varphi_1) \times \Gamma(\varphi_2)$. □

Теперь вспомним, что согласно теореме 17 главы 16 пространство V_P раскладывается в прямую сумму циклических относительно преобразования φ подпространств:

$$V = V_1 \dotplus \ldots \dotplus V_k, \tag{10}$$

т. е. подпространств V_s, инвариантных относительно φ и таких, что преобразование $\varphi_s = \varphi\big|_{V_s}$ удовлетворяет условию $\chi_{\varphi_s}(x) = m_{\varphi_s}(x)$. Более того, разложение (10) можно выбрать так, что либо $\chi_{\varphi_s}(x) = x^{n_s}$, либо χ_{φ_s} — реверсивный многочлен. В таком случае по теореме 11

$$\Gamma(\varphi) \cong \Gamma(\varphi_1) \times \ldots \times \Gamma(\varphi_k),$$

и с учетом примера 9 нам остается научиться описывать строение графа $\Gamma(\varphi)$ в случае, когда $\chi_\varphi(x) = m_\varphi(x) = F(x)$ — реверсивный многочлен. В этом случае по теореме 10(а) граф $\Gamma(\varphi)$ регулярен, и потому он однозначно, с точностью до изоморфизма, описывается своим цикловым типом $\mathcal{C}_\varphi(y)$.

Теорема 12. *Если φ — такое линейное преобразование пространства V_P, что $\chi_\varphi(x) = m_\varphi(x) = F(x)$ — реверсивный многочлен, то цикловой тип графа $\Gamma(\varphi)$ совпадает с цикловым типом пространства $L_P(F)$, т. е. $\mathcal{C}_\varphi(y) = \mathcal{C}_F(y)$.*

□ Рассмотрим преобразование $\sigma\colon L_P(F) \to L_P(F)$, определяемое правилом

$$\forall\, u \in L_P(F):\ \ \sigma(u) = x \cdot u. \tag{11}$$

Как уже отмечалось в главе 25, σ — линейное преобразование пространства $L_P(F)$, и поскольку минимальный многочлен относительно σ вектора $e^F \in L_P(F)$ равен $F(x)$ и $\deg F(x) = \dim L_P(F)$, то $\chi_\sigma(x) = m_\sigma(x) = F(x)$.

Заметим, что цикловой тип $\mathcal{C}_\sigma(y)$ графа $\Gamma(\sigma)$ равен цикловому типу $\mathcal{C}_F(y)$ семейства $L_P(F)$, поскольку ввиду (11) очевидно, что вершины u, v из $L_P(F)$ лежат в графе $\Gamma(\sigma)$ на одном цикле тогда и только тогда, когда одному циклу в $L_P(F)$ принадлежат последовательности u и v. Остается заметить, что $\mathcal{C}_\sigma(y) = \mathcal{C}_\varphi(y)$, поскольку справедлива

Лемма. *Если матрица преобразования $\varphi \in \mathfrak{L}(V_P)$ (в каком-либо базисе пространства V) подобна матрице преобразования $\psi \in \mathfrak{L}(W_P)$, то $\Gamma(\varphi) \cong \Gamma(\psi)$.*

□ Из условия следует, что $\dim V_P = \dim W_P$, и в рассматриваемых пространствах можно выбирать базисы $\vec{e} = (e_1, \ldots, e_n)$ и $\vec{f} = (f_1, \ldots, f_n)$ так, что

$$A_{\vec{e}}(\varphi) = A_{\vec{f}}(\psi). \tag{12}$$

Зададим отображение $\tau\colon V \to W$ по правилу

$$\forall\, \alpha \in V:\ \ \tau(\alpha) = \vec{f} \cdot \alpha^{\downarrow}_{\vec{e}} \quad (\text{т. е. } \tau(\alpha)^{\downarrow}_{\vec{f}} = \alpha^{\downarrow}_{\vec{e}}). \tag{13}$$

Очевидно, что τ — биекция. Если $\varphi(\alpha) = \beta$, то $\beta^{\downarrow}_{\vec{e}} = A_{\vec{e}}(\varphi)\alpha^{\downarrow}_{\vec{e}}$, и в силу соотношений (13) и (12)

$$\psi(\tau(\alpha)) = \vec{f}\cdot A_{\vec{f}}(\psi)\cdot\tau(\alpha)^{\downarrow}_{\vec{f}} = \vec{f}\cdot A_{\vec{f}}(\psi)\,\alpha^{\downarrow}_{\vec{e}} = \\ = \vec{f}\cdot A_{\vec{e}}(\varphi)\,\alpha^{\downarrow}_{\vec{e}} = \vec{f}\,\beta^{\downarrow}_{\vec{e}} = \tau(\beta) = \tau(\varphi(\alpha)).$$

По утверждению 4, τ — изоморфизм графа $\Gamma(\varphi)$ на $\Gamma(\psi)$. □

Теорема 12 доказана. □

Суммируя результаты этого параграфа, можно сформулировать следующий результат.

Теорема 13. *Пусть пространство V_P есть прямая сумма циклических относительно преобразования $\varphi \in \mathfrak{L}(V)$ подпространств:*

$$V = V_1 \dotplus \ldots \dotplus V_k$$

таких, что для $s \in \overline{1,k}$ преобразование $\varphi_s = \varphi\big|_{V_s}$ имеет характеристический многочлен вида

$$\chi_{\varphi_s}(x) = x^{l_s}G_s(x), \quad G_s(0) \neq 0.$$

Тогда граф $\Gamma(\varphi)$ изоморфен прямому произведению деревьев типов $D_q(l_1), \ldots, D_q(l_k)$ и регулярных графов с цикловыми типами $\mathcal{C}_{G_1}(y), \ldots, \mathcal{C}_{G_k}(y)$.

Пример 10. Опишем граф линейного преобразования φ пространства V размерности 4 над полем $P = \mathbb{Z}/2$, матрица которого в некотором базисе $\vec{e}$ имеет вид

$$A_{\vec{e}}(\varphi) = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

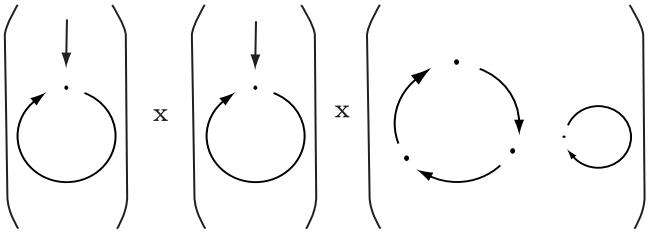
Элементарными преобразованиями находим, что канонический вид матрицы $xE - A_{\vec{e}}(\varphi)$ есть

$$\operatorname{diag}(e,\, e,\, x,\, x(x^2 + x + 1)).$$

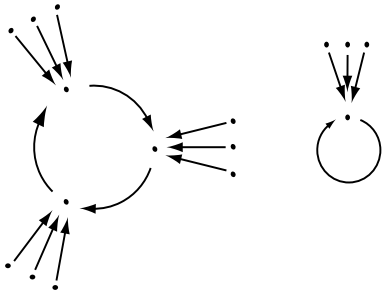
Следовательно, пространство V есть прямая сумма циклических относительно φ подпространств V_1 и V_2 таких, что линейные преобразования $\varphi_s = \varphi\big|_{V_s}$ удовлетворяют равенствам

$$\chi_{\varphi_1} = m_{\varphi_1}(x) = x,$$
$$\chi_{\varphi_2} = m_{\varphi_2}(x) = x(x^2 + x + 1).$$

Отсюда по теореме 13 следует, что граф $\Gamma(\varphi)$ изоморфен прямому произведению деревьев типов $D_2(1)$, $D_2(1)$ и регулярного графа с цикловым типом $\mathcal{C}_{x^2+x+1}(y) = y + y^3$, т. е. прямому произведению графов



Следовательно, граф $\Gamma(\varphi)$ имеет вид



ЗАДАЧИ

1. Вычислите длину подхода и период линейной последовательности α^{φ}, порождаемой вектором $\alpha = (0, \ldots, 0, 1)^T \in P^{(n)}$ и преобразованием $\varphi\colon P^{(n)} \to P^{(n)}$ с матрицей

$$A(\varphi) = \begin{pmatrix} 1 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 1 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & \ldots & 0 & 1 & 1 \\ 1 & 0 & \ldots & 0 & 0 & 1 \end{pmatrix}$$

в следующих ситуациях:

а) $P = GF(2),\ n = 3,\ 4,\ 5$;

б) $P = GF(3),\ n = 4$;

в) $P = GF(5),\ n = 3$.

2. В условиях задачи 1 опишите графы $\Gamma(\varphi)$.

3. Опишите с точностью до изоморфизма все возможные графы линейных преобразований $\varphi\colon P^{(n)} \to P^{(n)}$ при условиях:

а) $P = GF(2),\ n = 2,\ 3,\ 4$;

б) $P = GF(3),\ n = 3$;

в) $P = GF(5),\ n = 2$.

4. Вычислите экспоненту и максимум порядков элементов группы $GL(m, p^t)$.

5. Пусть R — конечное коммутативное кольцо с единицей e и $\psi\colon R^{(m)} \to R^{(m)}$ — аффинное преобразование, определяемое условием

$$\forall\, \alpha^{\downarrow} \in R^{(m)}:\ \psi(\alpha^{\downarrow}) = A\alpha^{\downarrow} + \beta^{\downarrow},$$

где $A \in R_{m,m}$, $b^{\downarrow} \in R^{(m)}$. Докажите, что граф $\Gamma(\psi)$ изоморфен подграфу графа $\Gamma(\varphi)$ линейного преобразования $\varphi\colon R^{(m+1)} \to R^{(m+1)}$, определяемого условием

$$\forall\, \beta^{\downarrow} \in R^{(m+1)}:\ \varphi(\beta^{\downarrow}) = B\beta^{\downarrow},\quad \text{где}\quad B = \begin{pmatrix} A & b^{\downarrow} \\ 0\ \ldots\ 0 & e \end{pmatrix}.$$

6. Пусть $P = GF(q)$, $\alpha \in P^{(m)}$ и $\psi\colon P^{(m)} \to P^{(m)}$ — аффинное преобразование. Докажите, что последовательность $\alpha^{\psi} = (\alpha, \psi(\alpha), \psi^2(\alpha), \ldots)$ удовлетворяет условию $\Lambda(\alpha^{\psi}) + T(\alpha^{\psi}) \leqslant q^m - 1$.

7. Вычислите экспоненту и максимум порядков элементов группы $AGL(m, p^t)$.

ЛИТЕРАТУРА

Учебники и учебные пособия

1. *Алексеев В. Б.* Теорема Абеля в задачах и решениях. — М.: МЦНМО, 2001.
2. *Бухштаб А. А.* Теория чисел. — СПб.: Лань, 2015.
3. *Винберг Э. Б.* Курс алгебры. Изд. 3. — М.: Факториал, 2002.
4. *Виноградов И. М.* Основы теории чисел. — СПб.: Лань, 2009.
5. *Воеводин В. В.* Линейная алгебра. — СПб.: Лань, 2009.
6. *Елизаров В. П., Нечаев А. А.* Высшая алгебра, чч. I, III. — М.: 1976; чч. II, IV. — М.: 1977.
7. *Ильин В. А., Позняк Э. Г.* Линейная алгебра. — М.: Наука, 1984.
8. *Калужнин Л. А.* Введение в общую алгебру. — М.: Наука, 1973.
9. *Кострикин А. И.* Введение в алгебру. — М.: Наука, 1977.
10. *Кострикин А. И.* Введение в алгебру, чч. I–III. — М.: Гос. изд-во физ.-мат. литературы, 2000; 2002.
11. *Кострикин А. И., Манин Ю. И.* Линейная алгебра и геометрия. — СПб.: Лань, 2008.
12. *Куликов Л. Я.* Алгебра и теория чисел. — М.: Высшая школа, 1979.
13. *Курош А. Г.* Курс высшей алгебры. — СПб.: Лань, 2013.
14. *Лидл Р., Пильц Г.* Прикладная абстрактная алгебра. — Екатеринбург: Изд-во Уральского ун-та, 1996.
15. *Ляпин Е. С., Евсеев А. Е.* Алгебра и теория чисел, чч. I, II. — М.: Просвещение, 1974; 1978.
16. *Мальцев А. И.* Основы линейной алгебры. — СПб.: Лань, 2009.
17. *Окунев Л. Я.* Высшая алгебра. — СПб.: Лань, 2009.
18. *Скорняков Л. А.* Элементы алгебры. — М.: Наука, 1980.
19. *Скорняков Л. А.* Элементы общей алгебры. — М.: Наука, 1983.
20. *Узков А. И.* Группы и теория Галуа. — М., 1971.
21. *Узков А. И.* Поля. — М., 1969.
22. *Фаддеев Д. К.* Лекции по алгебре. — СПб.: Лань, 2007.
23. *Шафаревич И. Р.* Основные понятия алгебры. — М.; Ижевск: R&C «Dynamics», 2001.

Сборники задач

1. *Икрамов Х. Д.* Сборник задач по линейной алгебре. — М.: Наука, 1975.
2. *Ляпин Е. С., Айзенштат А. Я., Лесохин М. М.* Упражнения по теории групп. — СПб.: Лань, 2010.
3. *Проскуряков И. В.* Сборник задач по линейной алгебре. — СПб.: Лань, 2010.
4. Сборник задач по алгебре / Под ред. Кострикина А. И. — М.: Наука, 1987.
5. *Фаддеев Д. К., Соминский И. С.* Сборник задач по высшей алгебре. — М.: Наука, 1977.

Научная литература

1. *Биркгоф Г., Барти Т.* Современная прикладная алгебра. — М.: Мир, 1976.
2. *Ван-дер-Варден Б. Л.* Алгебра. — М.: Наука, 1976.
3. *Гантмахер Ф. Р.* Теория матриц. — М.: Наука, 1988.
4. *Горенстейн Д.* Конечные простые группы. Введение в их классификацию. — М.: Мир, 1985.
5. *Елизаров В. П.* Конечные кольца. — М.: Гелиос АРВ, 2006.
6. *Каргаполов М. И., Мерзляков Ю. И.* Основы теории групп. — СПб.: Лань, 2009.
7. *Каш Ф.* Модули и кольца. — М.: Мир, 1981.
8. *Клиффорд А., Престон Г.* Алгебраическая теория полугрупп, тт. 1, 2. — М.: Мир, 1972.
9. *Кон П.* Универсальная алгебра. — М.: Мир, 1968.
10. *Курош А. Г.* Лекции по общей алгебре. — СПб.: Лань, 2007.
11. *Курош А. Г.* Теория групп. — СПб.: Лань, 2005.
12. *Кэртис Ч., Райнер И.* Теория представлений конечных групп и ассоциативных алгебр. — М.: Наука, 1969.
13. *Ламбек И.* Кольца и модули. — М.: Мир, 1971.
14. *Ленг С.* Алгебра. — М.: Мир, 1968.
15. *Лидл Р., Нидеррайтер Г.* Конечные поля, тт. 1, 2. — М.: Мир, 1988.
16. *Линдон Р., Шупп П.* Комбинаторная теория групп. — М.: Мир, 1980.
17. *Ляпин Е. С.* Полугруппы. — М.: Гос. изд-во физ.-мат. литературы, 1960.
18. *Магнус В., Каррас А., Солитэр Д.* Комбинаторная теория групп. — М.: Наука, 1974.
19. *Мальцев А. И.* Алгебраические системы. — М.: Наука, 1970.
20. *Ольшанский А. Ю.* Геометрия определяющих соотношений в группах. — М.: Наука, 1989.
21. *Плоткин Б. И.* Группы автоморфизмов алгебраических систем. — М.: Наука, 1966.
22. *Погорелов Б. А.* Основы теории групп подстановок. — М.: 1985.
23. *Прасолов В. В.* Многочлены. — М.: МЦНМО, 1999.
24. *Фукс Л.* Бесконечные абелевы группы, тт. 1, 2. — М.: Мир, 1974, 1977.
25. *Холл М.* Теория групп. — М.: ИЛ, 1962.

ИМЕННОЙ УКАЗАТЕЛЬ

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

Д

Н

C

Михаил Михайлович ГЛУХОВ
Виктор Павлович ЕЛИЗАРОВ
Александр Александрович НЕЧАЕВ

АЛГЕБРА

Учебник

Издание второе,
исправленное и дополненное

Зав. редакцией
физико-математической литературы *Н. Р. Нигмадзянова*
Верстка *А. Г. Сандомирская*
Выпускающие *Н. А. Крылова, О. В. Шилкова*

ЛР № 065466 от 21.10.97
Гигиенический сертификат 78.01.07.953.П.007216.04.10
от 21.04.2010 г., выдан ЦГСЭН в СПб

Издательство «ЛАНЬ»
lan@lanbook.ru; www.lanbook.com
192029, Санкт-Петербург, Общественный пер., 5.
Тел./факс: (812) 412-29-35, 412-05-97, 412-92-72.
Бесплатный звонок по России: 8-800-700-40-71

Подписано в печать 24.07.15.
Бумага офсетная. Гарнитура Школьная. Формат 70×100 $^{1}/_{16}$.
Печать офсетная. Усл. п. л. 49,40. Тираж 700 экз.

Заказ № .

Отпечатано в полном соответствии
с качеством предоставленных материалов
в АО «ИПК “Чувашия”».
428019, г. Чебоксары, пр. И. Яковлева, д. 13.
Тел.: (8352) 56-00-23