М. П. ТРОПИН

ОСНОВЫ ПРИКЛАДНОЙ АЛГЕБРЫ

УЧЕБНОЕ ПОСОБИЕ

Издание второе, стереотипное

ЛАНЬ®
· САНКТ-ПЕТЕРБУРГ ·
· МОСКВА ·
· КРАСНОДАР ·
2020

УДК 512
ББК 22.144я73

Т 74 **Тропин М. П.** Основы прикладной алгебры : учебное пособие / М. П. Тропин. — 2-е изд., стер. — Санкт-Петербург : Лань, 2020. — 288 с. : ил. — (Учебники для вузов. Специальная литература). — Текст : непосредственный.

ISBN 978-5-8114-5327-6

В пособие вошли такие разделы, как целые числа, элементы общей алгебры, общая теория многочленов, расширения полей, конечные поля, многочлены над конечными полями, эллиптические кривые. Эти разделы играют важную роль в приложениях. Уровень сложности изложения невысокий, однако предполагается, что читатель имеет математическую подготовку. В конце каждой главы предлагаются задачи для самостоятельного решения. Они направлены на освоение основных понятий и базовых алгоритмов.

Учебное пособие предназначено для студентов, обучающихся по направлениям «Математика и механика», «Компьютерные и информационные науки», «Информационная безопасность», «Образование и педагогические науки», другим направлениям и специальностям математического и технического профилей.

Учебное пособие может быть использовано как для преподавания прикладной алгебры как самостоятельной дисциплины, так и как основа для различных курсов по алгебре, теории кодирования и криптографии.

УДК 512
ББК 22.144я73

Рецензенты:

М. В. НЕЩАДИМ — доктор физико-математических наук, ведущий научный сотрудник Института математики им. С. Л. Соболева Сибирского отделения РАН;

Ю. В. СОСНОВСКИЙ — кандидат физико-математических наук, доцент, директор Института физико-математического и информационно-экономического образования Новосибирского государственного педагогического университета.

Обложка
Е. А. ВЛАСОВА

Предисловие

В результате развития информационных систем приобрели большую роль вопросы безопасности и надёжности передачи информации на большие расстояния. Как следствие, стали развиваться теория (помехоустойчивого) кодирования и криптография. Эти дисциплины, во-первых, сформировались как отдельные разделы математики, со своим аппаратом, своими основными проблемами и задачами, во-вторых, они стали генераторами новых содержательных математических задач. Можно согласиться с утверждением (см. [5, 21]), что криптография и теория кодирования – это один из источников развития математики в настоящее время.

Многие классические математические дисциплины, на которых основаны криптография и теория кодирования, такие как алгебра, теория чисел, дискретная математика и др., получили серьёзные и востребованные обществом приложения. Возникла необходимость преподавания основ криптографии и кодирования в высшей школе как в рамках специализированных направлений («Криптография», «Информационная безопасность» и пр.), так и в качестве курсов по выбору на других математических направлениях.

Можно сказать больше. Интенсивное развитие прикладных разделов алгебры, а также повсеместное распространение компьютеров сместило центр тяжести математики от «непрерывной математики» к «дискретной математике». Назрела необходимость сформировать в учебных планах некоторых математических направлений (как прикладных, так и теоретических) модуль «Прикладная алгебра», который может включать следующие дисциплины:

1) «Линейная алгебра» (1 или 2 семестра),

2) «Основы теории чисел» отдельно (1 семестр) или в рамках предмета «Дискретная математика» (2 семестра),

3) «Основы прикладной алгебры» в объёме данной книги (2 семестра),

4) «Методы теории чисел в криптографии» (1 семестр),

5) «Вычислительные алгоритмы алгебры и теории чисел» (1 семестр),

6) «Основы криптографии» (1 семестр),

7) «Основы теории кодирования» (1 или 2 семестра).

Учебная литература по этим дисциплинам достаточно обширна, однако не является легкодоступной. Кроме того, её изучение подразумевает достаточно высокую математическую культуру. Явно не хватает учебных пособий *начального* уровня. Не хватает также пособий, которые готовят почву для преподавания теории кодирования и криптографии.

Настоящее пособие направлено на решение этих проблем для студентов-математиков классического университета или педагогического вуза. Подразумевается, что курс линейной алгебры уже освоен. В пособие входят разделы: «Целые числа», «Элементы общей алгебры», «Общая теория многочленов», «Расширения полей», «Конечные поля», «Многочлены над конечными полями», «Эллиптические кривые».

При изучении данного учебного пособия читатель может воспользоваться книгами [1-4]. Они могут быть рекомендованы тем, кто хочет расширить свои знания вышеупомянутых разделов, т.к. существенно больше по объёму. Учебники [6-11] изданы в Новосибирском государственном педагогическом университете, они – результат многолетнего опыта преподавания алгебры и теории чисел коллективом кафедры алгебры. В них входят основы теории чисел, теория многочленов, алгебраические числа.

Книги [12-22] – это учебники или монографии по теории кодирования и криптографии, которые содержат разделы, частично покрывающие содержание данного пособия. Их можно использовать как источник альтернативной информации. Список литературы ни в коем случае не претендует на полноту. Достаточно обширный библиографический список можно найти, например, в [1] и [16]. При написании данного пособия использовались книги [1-4, 8-10].

Автор выражает признательность Ю.В. Сосновскому, который несколько раз внимательно прочитал рукопись и высказал ряд полезных замечаний.

ГЛАВА 1. ЦЕЛЫЕ ЧИСЛА

§1. Отношение делимости и деление с остатком

1.1. Определение. Говорят, что целое число a *делится* на целое число b, если существует такое $q \in \mathbb{Z}$, что $a = bq$. Коротко этот факт записывается так:

$$a \vdots b .$$

Другой вариант записи: $b \mid a$ (читается: b *делит* a). Число a называется *делимым*, b *– делителем*, а q *– частным.*

N.B. В данной главе, если не оговорено противное, все числа будут предполагаться целыми.

1.2. Теорема (свойства делимости). *Для любых целых чисел* a, b, c *выполняются следующие свойства:*

1) $a \vdots a$ *(рефлексивность);*

2) если $a \vdots b$, $b \vdots c$, *то* $a \vdots c$ *(транзитивность);*

3) если $a \vdots c$, $b \vdots c$, *то* $(a \pm b) \vdots c$;

4) если $a \vdots c$, *то* $ab \vdots c$;

5) если $a \vdots b$, *то* $\pm a \vdots \pm b$ *(делимость не зависит от сомножителя* ± 1*);*

6) $0 \vdots a$, $a \vdots \pm 1$, $a \vdots \pm a$ *(тривиальные делимости);*

7) если $a \vdots b$, $a \neq 0$, *то* $|a| \geq |b|$.

Доказательство этих свойств проводится по одной схеме: сначала нужно воспользоваться определением делимости, затем выполнить необходимые преобразования. Докажем некоторые из них.

2) Если $a \vdots b$ и $b \vdots c$, то соответственно $a = bq_1$ и $b = cq_2$. Подставляя b из второго равенства в первое, получаем $a = (cq_2)q_1 = c(q_2 q_1)$. Следовательно, a делится на c.

3) Если a и b делятся на c, то соответственно $a = cq_1$ и $b = cq_2$. Почленно складывая эти равенства, получаем $a + b = cq_1 + cq_2 = c(q_1 + q_2)$. Следовательно, $a + b$ делится на c.

5) Если a делится на b, то $a = bq$. Согласно свойствам противоположного элемента выполняются равенства $a = (-b)(-q)$, $-a = b(-q) = (-b)q$. В результате a делится на $(-b)$, $(-a)$ делится на b, $(-a)$ делится на $(-b)$.

7) Если $a \vdots b$, $a \neq 0$, то $a = bq$, причём $q \neq 0$. Так как q – целое число, то $|q| \geq 1$. Взяв модуль от обеих частей равенства, получаем

$$|a| = |bq| = |b| \cdot |q| \geq |b| \cdot 1 = |b|.$$

1.3. Следствия (из свойства 7).

а) Если $a \vdots b$, $b \vdots a$, *то* $a = b$ *или* $a = -b$.

б) Если $1 \vdots a$, *то* $a = \pm 1$.

1.4. Замечание. Так как всякое целое число a (согласно свойству 6) делится на ± 1, $\pm a$, то такие делители в дальнейшем будут называться *тривиальными*.

1.5. Пример. Доказать, что число $\left(7 \cdot 129^{301} + 3 \cdot 301^{129}\right)$ делится на 43.

Заметим, что $129 \vdots 43$, $301 \vdots 43$, т.к. $129 = 43 \cdot 3$, $301 = 43 \cdot 7$. После этого, пользуясь свойством 4 делимости, последовательно получаем следующее:

$$129 \vdots 43,\ 129^{301} \vdots 43,\ 7 \cdot 129^{301} \vdots 43;$$

$$301 \vdots 43,\ 301^{129} \vdots 43,\ 3 \cdot 301^{129} \vdots 43.$$

Складывая полученные делимости, по свойству 3, получаем

$$\left(7 \cdot 129^{301} + 3 \cdot 301^{129}\right) \vdots 43.$$

1.6. Пример. Доказать, что для любого натурального n число $\left(4^n+6n+8\right)$ делится на 9.

Данное свойство удобнее всего доказать по индукции.

Если $n=1$, то $4^1+6\cdot 1+8=18\vdots 9$.

Предположим, что для $n=k$ свойство выполняется. Докажем его для $n=k+1$.

$$4^{k+1}+6(k+1)+8=4\cdot 4^k+6k+14=$$

$$=4\cdot\left(4^k+6k+8\right)-4\cdot 6k-4\cdot 8+6k+14=$$

$$=4\cdot\left(4^k+6k+8\right)-18k-18.$$

Первое слагаемое делится на 9 по предположению, остальные делятся на 9, т.к. у них легко выделить сомножитель 9. По свойствам 4 и 3 полученное выражение делится на 9.

Рассмотрим деление с остатком.

1.7. Теорема (о делении с остатком целых чисел). *Для любых целых чисел a и b, $b\neq 0$, существуют единственные целые числа q, r такие, что*

$$\begin{cases} a=bq+r, \\ 0\le r<|b|. \end{cases}$$

1.8. Определение. Число q называется *неполным частным*, а число r – *остатком* от деления a на b. *Разделить число a на число b с остатком* – это значит найти неполное частное q и остаток r.

Самым важным результатом деления с остатком является равенство вида $a=bq+r$. Именно это равенство обычно используется при решении задач.

Доказательство теоремы. 1) Существование.

1-й случай: $b>0$. В этом случае $|b|=b$. Рассмотрим множество M чисел, кратных b: bk, $k\in\mathbb{Z}$ и удовлетворяющих условию $bk\le a$. Выберем среди них наибольшее bk_0. Положим $q=k_0$, $r=a-bq$, тогда q, r – целые числа и $a=bq+r$.

Так как $bq\le a$, то $r=a-bq\ge 0$.

Так как $b>0$, то $bq<b(q+1)$. Так как bq – наибольший элемент в M, то $b(q+1)\not\le a$. Следовательно, $b(q+1)>a$, $bq+b>a$, $b>a-bq=r$ и, наконец, $|b|=b>r$.

В результате найдены числа q и r, удовлетворяющие всем условиям теоремы.

2-й случай: $b<0$. В этом случае $|b|=-b$. Рассмотрим число $-b>0$. Воспользовавшись предыдущим случаем, найдём для пары чисел $a, -b$ частное и остаток:

$$\begin{cases} a=(-b)q+r, \\ 0\le r<|-b|=|b|. \end{cases}$$

Преобразовав, получаем

$$\begin{cases} a=b(-q)+r, \\ 0\le r<|b|. \end{cases}$$

Числа $-q$ и r удовлетворяют всем условиям теоремы.

2) Единственность.

Пусть

$$a=bq_1+r_1,\ a=bq_2+r_2,\ 0\le r_1<|b|,\ 0\le r_2<|b|,$$

тогда

$$bq_1+r_1=bq_2+r_2,$$

$$bq_1-bq_2=r_2-r_1,$$

$$b(q_1-q_2)=r_2-r_1.$$

Если $q_1 - q_2 \neq 0$, то $r_2 - r_1 \neq 0$. Сделаем оценку абсолютной величины левой и правой части полученного равенства:

$$|b| \leq |b| \cdot |q_1 - q_2| = |b(q_1 - q_2)| = |r_2 - r_1| < |b|.$$

Противоречие. Следовательно, этот случай невозможен.

Если $q_1 - q_2 = 0$, то $r_2 - r_1 = 0$ и тогда $q_1 = q_2$, $r_1 = r_2$.

1.9. Следствие. *Целое число a делится на целое число b тогда и только тогда, когда остаток от деления a на b равен 0.*

Доказательство. Если $a \vdots b$, то $a = bq = bq + 0$. В силу единственности частного и остатка получаем, что q – это частное, а $r = 0$ – это остаток.

Если остаток от деления числа a на число b равен 0, то $a = bq + 0 = bq$ и, следовательно, $a \vdots b$.

1.10. Пример. Разделить числа (-834) и $7^n - 3$ на 7 с остатком.

Число 834 на 7 с остатком можно разделить столбиком:

$$834 = 7 \cdot 119 + 1.$$

После этого умножаем полученное равенство на -1 и преобразуем так, чтобы выполнялись все условия деления с остатком.

$$-834 = -(7 \cdot 119) - 1 = 7 \cdot (-119) - 1 = \ldots$$

Число -1 остатком быть не может, т.к. оно отрицательно. Чтобы исправить это, возьмём частное на единицу меньше.

$$\ldots = 7 \cdot (-120) + 7 - 1 = 7 \cdot (-120) + 6.$$

Теперь все условия выполняются:

$$\begin{cases} -834 = 7 \cdot (-120) + 6, \\ 0 \leq 6 < 7. \end{cases}$$

Неполное частное при делении (-834) на 7 равно (-120), а остаток равен 6.

Во втором случае, т.к. остаток должен быть положительным, добавим и отнимем от данного выражения 7.

$$7^n - 3 = 7^n - 7 + 7 - 3 = 7^n - 7 + 4 = 7 \cdot \left(7^{n-1} - 1\right) + 4 .$$

В результате частное равно $\left(7^{n-1} - 1\right)$, а остаток равен 4. Отметим, что в данной и предыдущей задаче мы пользовались единственностью частного и остатка: подобрав подходящие q и r, можно прекращать поиски, т.к. других частного и остатка быть не может.

1.11. Замечание. Остаток при делении на b должен удовлетворять условию $0 \le r < |b|$. Таких чисел конечное множество: $0, 1, 2, \ldots, |b| - 1$. Поэтому можно применять *метод перебора всех возможных остатков.*

1.12. Пример. Доказать, что при делении числа n^2 на 3 не может получиться остаток 2.

При делении числа n на 3 могут получиться остатки 0,1 и 2. Рассмотрим эти случаи отдельно, и в каждом из них найдём остаток от деления числа n^2 на 3.

$n = 3k,\ n^2 = 9k^2 = 3 \cdot 3k^2 + 0$, остаток равен 0;

$n = 3k + 1,\ n^2 = 9k^2 + 6k + 1 = 3 \cdot \left(3k^2 + 2k\right) + 1$,

остаток равен 1;

$n = 3k + 2,\ n^2 = 9k^2 + 12k + 4 = 3 \cdot \left(3k^2 + 4k + 1\right) + 1$,

остаток равен 1.

Ни в одном из случаев остаток 2 не получился.

1.13. Пример. Доказать, что число $2017^{2017} + 1$ не может быть квадратом натурального числа.

Так как $2017 = 3 \cdot 672 + 1$, то по биному Ньютона можно получить, что

$$2017^{2017} = (3 \cdot 672 + 1)^{2017} = 3(\ldots) + 1 .$$

В результате число $2017^{2017} + 1$ при делении на 3 будет давать остаток 2 и по предыдущей задаче не может быть квадратом натурального числа.

§2. Наибольший общий делитель и его свойства

1.14. Определение. Целое число m называется *общим делителем* чисел a и b, если $a \vdots m$, $b \vdots m$.

Число m называется *наибольшим общим делителем* чисел a и b, если оно является их общим делителем и делится на любой другой их общий делитель, т.е. если

1) $a \vdots m$, $b \vdots m$,

2) для любого целого числа k, если $a \vdots k$ и $b \vdots k$, то $m \vdots k$.

1.15. Замечание. Так как наибольший общий делитель делится на любой другой общий делитель, то он, согласно свойству делимости 7 (теорема 1.2), будет действительно наибольшим по абсолютной величине. Таких чисел ровно два: m и $-m$, т.к. по свойству делимости 5 (теорема 1.2) делимость не зависит от знака. Кроме того, их не может быть больше двух, т.к. если m_1 и m_2 два наибольших общих делителя, то по определению они делятся друг на друга и, следовательно:

$$|m_1| = |m_2| .$$

Условимся положительный наибольший общий делитель обозначать

$$НОД(a, b) .$$

1.16. Замечание. $НОД(0,0)$ *не существует*, т.к. общим делителем пары 0,0 является любое целое число. Ниже будет доказано, что во всех остальных случаях *НОД* существует.

1.17. Лемма. *Если целые числа a и b не равны нулю одновременно и a делится на b, то $НОД(a,b)$ существует и равен $|b|$.*

Доказательство. Заметим, что если $b \vdots k$, то и $a \vdots k$. Поэтому общие делители чисел a и b – это в точности все делители b. Число $|b|$ делится на все делители b, поэтому $|b| = НОД(a,b)$.

1.18. Лемма. *Если $a = bq + r$, то $НОД(a,b)$ существует тогда и только тогда, когда существует $НОД(b,r)$ и*

$$НОД(a,b) = НОД(b,r).$$

Доказательство. Заметим, что множество общих делителей пары a, b и пары b, r совпадают. Действительно, если $a \vdots k$, $b \vdots k$, то $r = a - bq \vdots k$. Если $b \vdots k, r \vdots k$, то $a = (bq + r) \vdots k$.

В результате оба *НОД* либо не существуют, либо существуют и равны.

1.19. Теорема (Евклид). *НОД любых двух не равных одновременно нулю целых чисел a и b существует.*

Доказательство. Так как числа a, b входят в условие равноправно, то, не уменьшая общности рассуждений, можно считать, что $b \neq 0$. Если $a \vdots b$, то $НОД(a,b) = |b|$ и теорема доказана.

Если $a \not\vdots b$, то разделим a на b с остатком, затем b разделим на полученный остаток и далее аналогично по принципу: на каждом шаге делим делитель на остаток из предыдущего деления. В результате получим соотношения:

$$a = bq_1 + r_1,\ 0 \le r_1 < |b|;$$

$$b = r_1 q_2 + r_2,\ 0 \le r_2 < r_1;$$

$$r_1 = r_2 q_3 + r_3,\ 0 \le r_3 < r_2;\ \ldots$$

Данный алгоритм называется *алгоритмом Евклида*.

1) Алгоритм Евклида обрывается.

Действительно, последовательность остатков удовлетворяет неравенствам:

$$|b| > r_1 > r_2 > r_3 > \ldots \geq 0 .$$

Эта последовательность не может быть бесконечной, т.к. между числами $|b|$ и 0 лишь конечное количество различных натуральных чисел. С другой стороны, алгоритм оборвётся только в том случае, если его следующий шаг невозможно выполнить, а это произойдёт только тогда, когда получится нулевой остаток, на который разделить нельзя. В результате, получим следующий набор условий:

$$a = bq_1 + r_1,\ 0 < r_1 < |b| ;$$

$$b = r_1 q_2 + r_2,\ 0 < r_2 < r_1 ;$$

$$r_1 = r_2 q_3 + r_3,\ 0 < r_3 < r_2 ;$$

$$\ldots$$

$$r_{n-2} = r_{n-1} q_n + r_n,\ 0 < r_n < r_{n-1} ;$$

$$r_{n-1} = r_n q_{n+1} + 0 .$$

1.20. Определение. Последовательность $a, b, r_1, r_2, \ldots, r_n$ называется *последовательностью Евклида*. Для единообразия можно считать, что $a = r_{-1}, b = r_0$.

2) Если $a \not\vdots b$, то $НОД(a,b)$ *существует и равен последнему ненулевому остатку в алгоритме Евклида:*

$$НОД(a,b) = r_n .$$

Применим сначала n раз лемму 1.18, а затем – лемму 1.17.

$$НОД(a,b) \overset{1.18}{=} НОД(b, r_1) \overset{1.18}{=} НОД(r_1, r_2) \overset{1.18}{=}$$

$$= НОД(r_2, r_3) \overset{1.18}{=} \ldots = НОД(r_{n-2}, r_{n-1}) \overset{1.18}{=} НОД(r_{n-1}, r_n) \overset{1.17}{=} r_n .$$

1.21. Следствие. *НОД двух не делящихся друг на друга целых чисел равен последнему ненулевому остатку в алгоритме Евклида для этих чисел.*

1.22. Теорема (тождество Безу). *Для любых двух не равных одновременно нулю целых чисел a и b существуют такие целые числа u, v, что*

$$au + bv = НОД(a,b).$$

Доказательство. Пусть $НОД(a,b) = m$. Если одно из чисел делится на другое, например $a \vdots b$, то

$$НОД(a,b) = |b|, \quad b = a \cdot 0 + b \cdot 1,$$

и, следовательно, $u = 0$, а $v = 1$ или -1 в зависимости от знака b.

Если a не делится на b, то применим к этим числам алгоритм Евклида и выразим в каждом равенстве остатки:

$$\begin{aligned} a &= bq_1 + r_1, & r_1 &= a - bq_1, \\ b &= r_1q_2 + r_2, & r_2 &= b - r_1q_2, \\ r_1 &= r_2q_3 + r_3, & r_3 &= r_1 - r_2q_3, \\ &\ldots, & &\ldots, \\ r_{n-2} &= r_{n-1}q_n + r_n; & r_n &= r_{n-2} - r_{n-1}q_n. \end{aligned}$$

В первом равенстве остаток r_1 выражается в виде линейной комбинации чисел a, b. Если подставить эту линейную комбинацию во второе равенство и привести подобные члены, то остаток r_2 представится в виде линейной комбинации чисел a, b. Если полученные представления для r_1 и r_2 подставить в третье равенство и привести подобные члены, то в виде линейной комбинации чисел a, b будет представлен остаток r_3. Продолжая этот процесс, в конечном счёте получим представление в виде линейной комбинации чисел a, b остатка $r_n = НОД(a,b)$, т.е. найдём такие числа u, v, что

$$au + bv = НОД(a,b).$$

1.23. Пример. Найти $НОД(13,5)$ и составить для чисел 13 и 5 тождество Безу.

Применим алгоритм Евклида к числам 13 и 5:

$$13 = 5 \cdot 2 + 3,$$

$$5 = 3 \cdot 1 + 2,$$

$$3 = 2 \cdot 1 + 1,$$

$$2 = 1 \cdot 2 + 0.$$

Получилось, что $НОД(13,5) = 1$. Далее выражаем из полученных равенств остатки и подставляем их так, как описано в доказательстве теоремы. Чтобы числа не перепутались, всё, кроме частных, обозначим буквами:

$$\begin{aligned} a &= b \cdot 2 + r_1, & r_1 &= a - b \cdot 2, \\ b &= r_1 \cdot 1 + r_2, & r_2 &= b - r_1 \cdot 1, \\ r_1 &= r_2 \cdot 1 + r_3; & r_3 &= r_1 - r_2 \cdot 1. \end{aligned}$$

$$r_1 = a - 2b,\ r_2 = b - r_1 = b - (a - 2b) = -a + 3b,$$

$$r_3 = r_1 - r_2 = (a - 2b) - (-a + 3b) = 2a - 5b.$$

В результате

$$НОД(13,5) = 1 = a \cdot 2 + b \cdot (-5) = 13 \cdot 2 + 5(-5).$$

Коэффициенты u, v в тождестве Безу удобнее находить при помощи следующих рекуррентных соотношений.

1.24. Теорема. *Пусть* $u_{-1} = 1, v_{-1} = 0, u_0 = 0,\ v_0 = 1$. *Для любого* $1 \le i \le n$ *обозначим коэффициенты в линейном выражении остатка* r_i *через* a *и* b *как соответственно* u_i, v_i*:*

$$r_i = au_i + bv_i.$$

Эти коэффициенты могут быть последовательно найдены при помощи рекуррентных соотношений:

$$u_i = u_{i-2} - u_{i-1}q_i,\ v_i = v_{i-2} - v_{i-1}q_i,\ 1 \le i \le n.$$

Доказательство. Заметим, что:

$$a = r_{-1} = a \cdot 1 + b \cdot 0 = au_{-1} + bv_{-1},$$

$$b = r_0 = a \cdot 0 + b \cdot 1 = au_0 + bv_0.$$

Предположим теперь, что для двух соседних элементов последовательности Евклида требуемое представление получено:

$$r_{i-2} = au_{i-2} + bv_{i-2},\ r_{i-1} = au_{i-1} + bv_{i-1}.$$

Выразив r_i из алгоритма Евклида, получаем

$$r_i = r_{i-2} - r_{i-1}q_i = \left(au_{i-2} + bv_{i-2}\right) - \left(au_{i-1} + bv_{i-1}\right)q_i =$$

$$= a\left(u_{i-2} - u_{i-1}q_i\right) + b\left(v_{i-2} - v_{i-1}q_i\right).$$

В результате можно считать, что

$$u_i = u_{i-2} - u_{i-1}q_i,\ v_i = v_{i-2} - v_{i-1}q_i.$$

Алгоритм по одновременному нахождению наибольшего общего делителя двух чисел и тождества Безу для них называется *расширенным алгоритмом Евклида*. Этот алгоритм широко используется в приложениях. Он является эффективным, т.к. позволяет вычислять $НОД(a,b)$ и u_n, v_n для весьма больших чисел.

1.25. Пример. Найти наибольший общий делитель и составить тождество Безу для чисел 1006 и 823.

Вычисления удобно записать в виде таблицы.

r_i	u_i	v_i	
$a = 1006 = r_{-1}$	1	0	
$b = 823 = r_0$	0	1	
$r_1 = 183$	$1 - 0 \cdot \mathbf{1} = 1$	$0 - 1 \cdot \mathbf{1} = -1$	$1006 = 823 \cdot \mathbf{1} + 183$
$r_2 = 91$	$0 - 1 \cdot \mathbf{4} = -4$	$1 - (-1) \cdot \mathbf{4} = 5$	$823 = 183 \cdot \mathbf{4} + 91$
$r_3 = 1$	$1 - (-4) \cdot \mathbf{2} = 9$	$-1 - 5 \cdot \mathbf{2} = -11$	$183 = 91 \cdot \mathbf{2} + 1$

Ответ: $НОД(1006,823) = 1$, $1 = 1006 \cdot 9 + 823 \cdot (-11)$.

1.26. Теорема (основное свойство *НОД*). *НОД двух не равных одновременно нулю целых чисел – это наибольший по абсолютной величине натуральный общий делитель этих чисел.*

В одну сторону Доказательство проведено в замечании 1.15.

Докажем теорему в обратную сторону. Пусть $m = НОД(a,b)$, а k – наибольший по абсолютной величине натуральный общий делитель чисел a, b, в частности $m \le k$.

Из определения *НОД* следует, что $m \vdots k$. По свойству делимости 7 (теорема 1.2) из этого получаем $|m| = m \ge |k| = k$. В результате $k = m$.

При изучении делимости чисел большую роль играет свойство взаимной простоты.

1.27. Определение. Целые числа a и b называются *взаимно простыми,* если их наибольший общий делитель равен 1, т.е. числа не имеют других общих делителей, кроме ± 1.

1.28. Теорема (признак взаимной простоты). *Целые числа a и b взаимно просты тогда и только тогда, когда существуют такие целые u, v, что $au + bv = 1$.*

Доказательство. Пусть $au + bv = 1$. Если число k делит числа a и b, то k делит и $au + bv = 1$. Делителями 1 являются только числа ± 1.

1.29. Следствие. *Числа* $\dfrac{a}{НОД(a,b)}$ *и* $\dfrac{b}{НОД(a,b)}$ *взаимно просты.*

Доказательство. Пусть $au + bv = НОД(a,b)$, тогда

$$\frac{a}{НОД(a,b)}u + \frac{b}{НОД(a,b)}v = 1.$$

После этого можно воспользоваться признаком 1.28.

Докажем ещё два очень важных свойства делимости, в которых используется свойство взаимной простоты.

1.30. Теорема (свойства делимости).

1) Если $ab \vdots c$ *и числа* a *и* c *взаимно просты, то* $b \vdots c$.

2) Если $a \vdots b$, $a \vdots c$ *и числа* b, c *взаимно просты, то* $a \vdots bc$.

Доказательство. 1) Так как числа a и c взаимно просты, то существуют такие $u, v \in \mathbb{Z}$, что $au + cv = 1$. Умножим это равенство на b:

$$aub + cvb = b.$$

Так как по условию $ab \vdots c$, то левая, а значит, и правая части равенства делятся на c.

2) Из первых двух условий следует, что существуют такие целые числа q_1, q_2, что

$$a = bq_1 = cq_2.$$

Правая часть этого равенства делится на c, следовательно $bq_1 \vdots c$. Так как числа b, c взаимно просты, то по предыдущему свойству $q_1 \vdots c$ и, следовательно, для подходящего целого числа q_3:

$$q_1 = cq_3.$$

Подставляя это выражение в первое равенство, получаем $a = bq_1 = bcq_3$ и, следовательно, $a \vdots bc$.

§3. Простые числа

В этом параграфе будет рассматриваться задача разложения целого числа на сомножители. Чтобы не возиться со знаками, мы ограничимся случаем **натуральных чисел.**

1.31. Определение. Натуральное число p называется *простым*, если оно больше 1 и не имеет других (натуральных) делителей, кроме p и 1. В противном случае оно называется *составным.*

1.32. Замечания. Всякое натуральное число n делится на n и 1. Это *тривиальные делители*. Очевидно, *нетривиальный натуральный делитель d должен удовлетворять неравенству* $1 < d < n$.

Простое число не имеет нетривиальных делителей. Если число n составное, то оно имеет нетривиальный делитель d:

$$n \vdots d,\ 1 < d < n.$$

В этом случае $n = dq$ и q также будет нетривиальным делителем числа n, т.к. если $q = 1$, то $d = n$, если $q = n$, то $d = 1$, что невозможно по условию.

В результате *число n является составным тогда и только тогда, когда существуют такие d, q, что*

$$n = dq,\ 1 < d < n,\ 1 < q < n.$$

Часть неравенств можно опустить.

1.33. Признак (составного числа). *Число n является составным тогда и только тогда, когда выполняется одно из двух условий:*

1) $n = dq,\ 1 < d,\ 1 < q$;

2) $n = dq,\ d < n,\ q < n$.

Это связано с тем, что $q = 1 \Leftrightarrow d = n$, и наоборот: $q = n \Leftrightarrow d = 1$.

Докажем характеристические свойства простых чисел.

1.34. Теорема (свойства простых чисел). *1) Пусть p – простое число. Произвольное натуральное число n либо взаимно просто с p, либо делится на p.*

2) Всякое натуральное число $n > 1$ имеет (наименьший) простой делитель.

Доказательство. 1) У простого числа p всего два натуральных делителя: 1 и p. Поэтому $НОД(n, p) = 1$ или p.

В первом случае n и p взаимно просты, во втором – $n \vdots p$.

2) Рассмотрим все натуральные числа, большие 1 и меньшие n. Их конечное число. Начнём подряд проверять, делят ли они число n. Если делители найдутся, то меньший их них будет простым. Если нет, то число не имеет нетривиальных делителей, является простым и само будет своим (наименьшим) простым делителем.

1.35. Следствие (основное свойство простых чисел). *Если произведение двух натуральных чисел делится на простое число p, то один из сомножителей делится на p.*

ДЕЙСТВИТЕЛЬНО, пусть $ab \vdots p$. Если $a \vdots p$, то доказывать нечего. Если $a \not\vdots p$, то a и p – взаимно просты и по свойству делимости (теорема 1.30) получаем, что $b \vdots p$.

При помощи метода математической индукции это свойство можно обобщить на случай произвольного количества сомножителей: *если произведение натуральных чисел делится на простое число, то хотя бы один из сомножителей делится на это простое число.*

1.36. Следствие. *Натуральное число n является составным тогда и только тогда, когда оно имеет простой делитель p, удовлетворяющий условию $p \le \sqrt{n}$.*

Доказательство. Согласно замечанию 1.32, $n = dq$, $1 < d < n$, $1 < q < n$. Не уменьшая общности, можно считать, что $d \le q$. Умножая это неравенство на d, получаем, что $dd \le qd = n$ и $d \le \sqrt{n}$. Любой простой делитель p числа d будет делителем n и будет удовлетворять условию $p \le \sqrt{n}$.

В обратную сторону. Если число имеет простой делитель $p \le \sqrt{n}$, то этот делитель будет нетривиальным, т.к.

$$1 < p \le \sqrt{n} < n,$$

а число n – составным.

1.37. Следствие. *Натуральное число* $n>1$ *является простым тогда и только тогда, когда оно не имеет простых делителей, меньших или равных числу* $\sqrt{n}$.

Следствие 1.37 является контрапозицией к следствию 1.36.

1.38. Следствие (решето Эратосфена). *Если в натуральном ряду зачеркнуть 1 и все числа, кратные первым k простым числам* $2, 3, 5, \ldots, p_k$, *то все оставшиеся незачёркнутыми числа вплоть до* $(p_{k+1})^2$ *являются простыми* (здесь p_k – *это k-е простое число*).

Действительно, если $n<(p_{k+1})^2$, то

$$\sqrt{n} < p_{k+1} .$$

Если n осталось незачёркнутым, то оно не делится на простые числа $2, 3, 5, \ldots, p_k$, в частности оно не делится на простые числа, меньшие или равные $\sqrt{n}$.

1.39. Теорема (основная теорема арифметики). *Всякое натуральное число* $n>1$ *может быть разложено в произведение простых сомножителей. Это разложение единственно с точностью до порядка сомножителей.*

Доказательство будет проведено индукцией по n .

Существование. Если $n=2$, то n очевидно представимо в виде произведения одного простого сомножителя 2.

Пусть для всех чисел, меньших некоторого n , существование разложения доказано. Докажем существование разложения для n .

Если n – простое, то, как уже отмечалось, n представимо в виде произведения одного простого сомножителя, равного n . Если n – составное, то

$$n=n_1 n_2,\ 1<n_1<n,\ 1<n_2<n .$$

По предположению индукции числа n_1, n_2 раскладываются в произведение простых сомножителей:

$$n_1 = p_1 p_2 \cdot \ldots \cdot p_k,\ n_2 = q_1 q_2 \cdot \ldots \cdot q_s .$$

В результате

$$n = p_1 p_2 \cdot \ldots \cdot p_k q_1 q_2 \cdot \ldots \cdot q_s .$$

Единственность. Если $n = 2$, то единственность разложения очевидна.

Пусть для всех чисел, меньших некоторого n, единственность разложения доказана. Докажем единственность для n.

Пусть есть два разложения числа n в произведение простых сомножителей:

$$n = p_1 p_2 \cdot \ldots \cdot p_k = q_1 q_2 \cdot \ldots \cdot q_s .$$

Так как произведение $p_1 p_2 \cdot \ldots \cdot p_k$ делится на простое число q_1, то по следствию 1.35 один из сомножителей (пусть для простоты обозначений это будет p_1) делится на q_1. В силу простоты чисел p_1 и q_1 получаем $p_1 = q_1$. Сокращаем равенство на $p_1 = q_1$:

$$p_2 \cdot \ldots \cdot p_k = q_2 \cdot \ldots \cdot q_s = n_1 < n .$$

По индукционному предположению полученные два разложения числа n_1 отличаются только порядком сомножителей. Домножая на $p_1 = q_1$, получаем, что разложения

$$n = p_1 p_2 \cdot \ldots \cdot p_k = q_1 q_2 \cdot \ldots \cdot q_s$$

также отличаются только порядком сомножителей.

Теорема доказана.

В разложении числа в произведение простые сомножители могут повторяться. Объединив их в степень, получим

1.40. Следствие (каноническое разложение). *Всякое натуральное число $n > 1$ может быть разложено в произведение степеней простых сомножителей:*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} ,$$

где $p_1, p_2, \ldots, p_k$ *– попарно различные простые числа.*

Это разложение единственно с точностью до порядка сомножителей.

1.41. Пример. Разложить на простые сомножители число 71981.

Начинаем поиск наименьшего делителя. Для этого перебираем все простые числа, меньшие $\sqrt{71981} < 269$, и проверяем, являются ли они делителями данного числа.

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots < 269;$$

$$71981 \not\vdots 2,\ 71981 \not\vdots 3,\ 71981 \not\vdots 5,\ 71981 \vdots 7;$$

$$71981 = 7 \cdot 10283.$$

Если делитель найден, то вычисляем частное и повторяем данную процедуру для него. Проверку делимости можно начать с 7, т.к. уже проверено, что на 2, 3, 5 данное число не делится.

$$\sqrt{10283} < 102;\ 2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots < 102;$$

$$10283 \vdots 7;\ 10283 = 7 \cdot 1469;$$

$$\sqrt{1469} < 39;\ 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37 < 39;$$

$$1469 \not\vdots 7,\ 1469 \not\vdots 11,\ 1469 \vdots 13;\ 1469 = 13 \cdot 113;$$

$$\sqrt{113} < 11.$$

В этом месте алгоритм завершается, т.к. уже проверено, что число 113 не делится на простые числа, меньшие $\sqrt{113}$, и, следовательно (следствие 1.37), является простым.

Ответ: $71981 = 7^2 \cdot 13 \cdot 113$.

Разберём простейшие случаи применения канонического разложения.

1.42. Теорема (формула для делителей). *Если число* $n > 1$ *представлено в каноническом виде* $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ *и* d *–*

некоторый его натуральный делитель, то $d = p_1^{\beta_1} p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$ *для подходящих* $0 \le \beta_i \le \alpha_i$, $1 \le i \le k$. *Количество различных натуральных делителей числа n равно* $(\alpha_1 + 1)(\alpha_2 + 1) \cdot \ldots \cdot (\alpha_k + 1)$.

Доказательство. Пусть d – делитель числа n и найдено его каноническое разложение

$$d = q_1^{\gamma_1} q_2^{\gamma_2} \cdot \ldots \cdot q_s^{\gamma_s} .$$

Тогда будет выполняться равенство

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} = q_1^{\gamma_1} q_2^{\gamma_2} \cdot \ldots \cdot q_s^{\gamma_s} h .$$

Правая, а, следовательно, и левая части этого равенства делятся на простые числа $q_1, q_2, \ldots, q_s$. По следствию 1.35, каждое из чисел q_i совпадает с одним из чисел p_j, а так как по определению числа $q_1, q_2, \ldots, q_s$ попарно различны, то равенство можно переписать так:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} = p_1^{\beta_1} p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k} h$$

(чтобы индексы шли по-порядку сомножители в правой части нужно соответствующим образом переставить; если среди чисел $q_1, q_2, \ldots, q_s$ нет какого-то простого сомножителя p_i, то его записываем в нулевой степени).

Если $\alpha_i < \beta_i$, то после сокращения на $p_i^{\alpha_i}$ получится равенство, правая часть которого делится на p_i, а левая – нет, что невозможно. Следовательно, $\alpha_i \ge \beta_i$ для всех i.

Чтобы подсчитать количество делителей, заметим, что делители отличаются друг от друга только набором степеней β_i. Для каждой степени имеется $(\alpha_i + 1)$ вариантов значений: $0,1,2,\ldots,\alpha_i$. Всего различных наборов степеней будет $(\alpha_1 + 1)(\alpha_2 + 1) \cdot \ldots \cdot (\alpha_k + 1)$. Это и есть количество различных натуральных делителей числа n.

1.43. Пример. Найти все делители числа 71981.

Каноническое разложение этого числа было получено выше:

$$71981 = 7^2 \cdot 13 \cdot 113 .$$

Согласно теореме, оно имеет $(2+1)(1+1)(1+1) = 12$ различных натуральных делителей. Пользуясь формулой, их все легко перечислить:

$$7^0 13^0 113^0 = 1,\ 7^1 13^0 113^0,\ 7^2 13^0 113^0 ,$$

$$7^0 13^1 113^0,\ 7^1 13^1 113^0,\ 7^2 13^1 113^0 ,$$

$$7^0 13^0 113^1,\ 7^1 13^0 113^1,\ 7^2 13^0 113^1 ,$$

$$7^0 13^1 113^1,\ 7^1 13^1 113^1,\ 7^2 13^1 113^1 = 71981 .$$

Целых делителей будет в два раза больше, т.к. добавятся отрицательные делители.

1.44. Замечание. Для любых двух натуральных чисел $n, m > 1$ можно считать, что в их каноническое разложение входят одинаковые простые числа, т.к. недостающие числа всегда можно дописать в нулевой степени. Такие канонические разложения будем называть *согласованными*.

Например, для чисел $4732 = 2^2 \cdot 7 \cdot 13^2$, $1287 = 3^2 \cdot 11 \cdot 13$ согласованные канонические разложения будут выглядеть так:

$$4732 = 2^2 \cdot 7 \cdot 13^2 = 2^2 \cdot 3^0 \cdot 7 \cdot 11^0 \cdot 13^2 ,$$

$$1287 = 3^2 \cdot 11 \cdot 13 = 2^0 \cdot 3^2 \cdot 7^0 \cdot 11 \cdot 13 .$$

1.45. Теорема (формула для вычисления *НОД*). *Пусть заданы два произвольных натуральных числа* $n, m > 1$ *и их согласованные канонические разложения*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k},\ \ m = p_1^{\beta_1} p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k} .$$

Пусть $\gamma_i = \min(\alpha_i, \beta_i)$, *тогда* $НОД(n, m) = p_1^{\gamma_1} p_2^{\gamma_2} \cdot \ldots \cdot p_k^{\gamma_k}$.

Доказательство. Согласно формуле 1.42 всякий общий делитель чисел n и m имеет вид

$$a = p_1^{x_1} p_2^{x_2} \cdot \ldots \cdot p_k^{x_k},\ 0 \le x_i \le \alpha_i, \beta_i .$$

Из этого сразу следует, что $0 \le x_i \le \min(\alpha_i, \beta_i) = \gamma_i$, число $d = p_1^{\gamma_1} p_2^{\gamma_2} \cdot \ldots \cdot p_k^{\gamma_k}$ является общим делителем чисел n и m и делится на любой их общий делитель.

Кроме наибольшего общего делителя часто возникает необходимость в наименьшем общем кратном.

1.46. Определение. Число K называется *наименьшим общим кратным* чисел n и m, если оно является их общим кратным и любое другое их общее кратное делится на него, т.е. если:

1) K делится на n и m;

2) любое целое число k, которое делится на n и m, делится также и на K.

Если наименьшее общее кратное существует, то, как и в случае с наибольшим общим делителем, их будет ровно два: равных по абсолютной величине и отличающихся знаком. При помощи *НОК* будем обозначать *неотрицательное* наименьшее общее кратное.

1.47. Замечание. $НОК(n, 0) = 0$ для любого целого n, т.к. единственным кратным числа 0 является 0. Кроме того, $НОК(n, 1) = |n|$, т.к. $n \vdots 1$. В остальных случаях можно воспользоваться следующей теоремой.

1.48. Теорема (о формулах для вычисления *НОК*). *1) Пусть заданы два натуральных числа* $n, m > 1$ *и их согласованные канонические разложения*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k},\ m = p_1^{\beta_1} p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k} .$$

Пусть $\gamma_i = \max(\alpha_i, \beta_i)$, *тогда* $НОК(n, m) = p_1^{\gamma_1} p_2^{\gamma_2} \cdot \ldots \cdot p_k^{\gamma_k}$.

В частности $НОК(n,m)$ *существует.*

2) $НОК(n,m)=\dfrac{nm}{НОД(n,m)}$.

Доказательство. 1) Общее кратное чисел n,m имеет иметь вид

$$p_1^{s_1}p_2^{s_2}\cdot\ldots\cdot p_k^{s_k}h\,,$$

где h – произвольное целое число, а $s_i\geq\alpha_i,\beta_i$ для любого $1\leq i\leq k$.

Число $K=p_1^{\gamma_1}p_2^{\gamma_2}\cdot\ldots\cdot p_k^{\gamma_k}$ будет удовлетворять всем условиям определения $НОК(n,m)$.

2) Пусть $\gamma_i=\max(\alpha_i,\beta_i)$, $\delta_i=\min(\alpha_i,\beta_i)$. Так как из любых двух чисел одно будет максимальным, а другое – минимальным, то $\{\alpha_i,\beta_i\}=\{\gamma_i,\delta_i\}$. Из этого следует, что

$$nm=\left(p_1^{\alpha_1}p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}\right)\left(p_1^{\beta_1}p_2^{\beta_2}\cdot\ldots\cdot p_k^{\beta_k}\right)=$$

$$=\left(p_1^{\gamma_1}p_2^{\gamma_2}\cdot\ldots\cdot p_k^{\gamma_k}\right)\left(p_1^{\delta_1}p_2^{\delta_2}\cdot\ldots\cdot p_k^{\delta_k}\right)=$$

$$=НОД(n,m)\cdot НОК(n,m).$$

1.49. Замечание. Вторая часть теоремы 1.48 даёт другой способ вычисления *НОК*:

1) вычисляем по алгоритму Евклида $НОД(n,m)$;

2) вычисляем $НОК(n,m)=\dfrac{nm}{НОД(n,m)}$.

§4. Функция Эйлера и её свойства

1.50. Определение. Пусть m – натуральное число. Количество натуральных чисел, взаимно простых с m и не

превосходящих m, обозначается $\varphi(m)$. Функция φ называется *функцией Эйлера.*

1.51. Пример. 1) Пусть $m=15$. Величину $\varphi(15)$ можно вычислить по определению. Для этого выпишем все натуральные числа, не превосходящие 15, и вычеркнем те из них, которые имеют с ним нетривиальные общие делители:

$$1, 2, \sout{3}, 4, \sout{5}, \sout{6}, 7, 8, \sout{9}, \sout{10}, 11, \sout{12}, 13, 14, \sout{15}.$$

Остались не зачёркнутыми восемь чисел, поэтому $\varphi(15)=8$.

2) Пусть p – простое число, тогда в последовательности $1, 2, 3, \ldots, p$ все числа, кроме последнего, взаимно просты с p и, следовательно, $\varphi(p)=p-1$.

Выведем формулу для вычисления $\varphi(m)$, т.к. для больших m способ вычисления по определению становится громоздким. Для получения формулы понадобится

1.52. Теорема (о мультипликативности функции Эйлера). *Если натуральные числа a, b взаимно просты, то* $\varphi(ab)=\varphi(a)\cdot\varphi(b)$.

Доказательство. Подсчитаем напрямую $\varphi(ab)$. Для этого запишем все числа от 1 до ab в таблицу так, как показано ниже, и будем зачёркивать те из них, которые не являются взаимно простыми с ab.

$$\begin{array}{ccccccc}
1, & 2, & 3, & \ldots, & a-1, & & a, \\
a+1, & a+2, & a+3, & \ldots, & a+a-1, & & 2a, \\
\ldots & \ldots & \ldots & \ldots & \ldots & & \ldots \\
a(b-1)+1, & a(b-1)+2, & & \ldots, & & & a(b-1)+a=ab.
\end{array}$$

Любое число в данном списке имеет вид

$$aq+r,\ 0\le q\le b-1,\ 1\le r\le a.$$

В r-м столбце при $r\neq a$ записаны все натуральные числа, меньшие ab, которые при делении на a дают остаток r.

В последнем столбце записаны все числа, меньшие ab, которые при делении на a дают остаток 0.

Согласно лемме 1.18, $НОД(aq+r,\ a) = НОД(r, a)$, поэтому если число r взаимно просто с a, то и все элементы его столбца взаимно просты с a, и наоборот. Вычеркнем все столбцы, элементы которых не являются взаимно простыми с a и, следовательно, с произведением ab. Останется $\varphi(a)$ столбцов.

Каждый столбец состоит из чисел

$$a\cdot 0+r,\ a\cdot 1+r,\ a\cdot 2+r,\ \ldots,\ a(b-1)+r\ .$$

Эти числа имеют попарно различные остатки при делении на b. Действительно, если числа aq_1+r и aq_2+r, $0\le q_1<q_2\le b-1$, имеют одинаковый остаток при делении на b, то их разность $(aq_2+r)-(aq_1+r)=a(q_2-q_1)$ делится на b. Так как по условию a и b взаимно просты, то по свойству делимости 1 (теорема 1.30) разность (q_2-q_1) делится на b. Последнее невозможно, т.к. $0<q_2-q_1<b$. Противоречие.

В результате среди чисел r-го столбца столько же чисел взаимно простых с b, сколько и среди чисел $0,1,2,\ldots,b-1$, т.е. $\varphi(b)$ штук. Вычеркнем в каждом столбце числа, не являющиеся взаимно простыми с b. Получится список, состоящий из $\varphi(a)\varphi(b)$ чисел. Каждое из них одновременно взаимно просто и с a, и с b.

В заключение осталось доказать, что *целое число c взаимно просто с произведением ab двух чисел тогда и только тогда, когда оно взаимно просто с каждым из них.*

Докажем это методом «от противного». Пусть c взаимно просто с ab и, напротив, не взаимно просто, например, с a. Тогда числа c и a имеют общий простой делитель p. Это же число будет общим простым делителем чисел c и ab. Противоречие.

В обратную сторону. Пусть c взаимно просто с каждым из чисел a и b, но, напротив, не взаимно просто с произведением

ab. Тогда числа c и ab имеют общий простой делитель p. По следствию 1.35 одно из чисел a или b делится на p. Число p будет общим делителем c и одного из чисел a или b, что противоречит предположению.

В результате в списке чисел от 1 до ab осталось ровно $\varphi(a)\varphi(b)$ чисел, которые взаимно просты с ab. По определению их количество равно $\varphi(ab)$, поэтому

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

1.53. Следствие (формулы для вычисления φ).

1) Если p – простое число, то $\varphi(p^n)=p^n-p^{n-1}$.

2) Если $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}$ – *каноническое разложение числа n, то*

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\cdot\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right).$$

Доказательство. 1) Свойство взаимной простоты некоторого числа x с данным простым числом p равносильно тому, что $x\not\vdots p$.

Вычислим значение функции Эйлера по определению. Для этого выпишем все числа от 1 до p^n:

$$1,\ 2,\ 3,\ \ldots,\ p,\ p+1,\ p+2,\ \ldots,\ p^2,\ p^2+1,\ \ldots,\ p^n.$$

В этой последовательности каждое p-е число делится на p и таких чисел $\dfrac{p^n}{p}$ штук. Остальные числа взаимно просты с p. Их количество равно

$$\varphi(p^n)=p^n-\frac{p^n}{p}=p^n-p^{n-1}.$$

2) В каноническом представлении $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ любая степень $p_i^{\alpha_i}$ взаимно проста с произведением остальных сомножителей. Применяем $(k-1)$ раз теорему 1.52 о мультипликативности функции φ, а затем применяем только что доказанную формулу.

$$\varphi(n) = \varphi\left(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}\right) = \text{ (по свойству мультипликативности)}$$

$$= \varphi\left(p_1^{\alpha_1}\right) \cdot \varphi\left(p_2^{\alpha_2}\right) \cdot \ldots \cdot \varphi\left(p_k^{\alpha_k}\right) = \text{ (по формуле 1)}$$

$$= \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \cdot \left(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}\right) \cdot \ldots \cdot \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right) =$$

(выносим степени p_i)

$$= p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right) =$$

$$= n\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right).$$

1.54. Замечание. В последней формуле не участвуют показатели степеней α_i. Поэтому, чтобы применить формулу, достаточно лишь знать простые числа, которые входят в каноническое разложение числа n.

1.55. Пример. Вычислим $\varphi(1000000)$. Очевидно, в каноническое разложение числа 1000000 входят только числа 2 и 5, поэтому

$$\varphi(1000000) = 1000000 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) = 1000000 \cdot \frac{2}{5} = 400000.$$

В дальнейшем нам понадобится следующая

1.56. Теорема (Гаусс). $\sum\limits_{n:d} \varphi(d) = n$.

Доказательство. Разложим число n согласно основной теореме арифметики в произведение степеней различных простых чисел:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}.$$

По теореме 1.42 о строении делителя числа n и по свойству мультипликативности функции Эйлера имеем для произвольного делителя d:

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k},\ 0 \le \beta_i \le \alpha_i,$$

$$\varphi(d) = \varphi\left(p_1^{\beta_1}\right)\varphi\left(p_2^{\beta_2}\right)\cdot \ldots \cdot \varphi\left(p_k^{\beta_k}\right).$$

Всевозможные произведения такого типа получаются после раскрытия скобок в произведении

$$\prod_{i=1}^{n}\left(\varphi\left(p_i^0\right)+\varphi\left(p_i^1\right)+\ldots+\varphi\left(p_i^{\alpha_i}\right)\right).$$

Поэтому это произведение равно $\sum_{n:d}\varphi(d)$. С другой стороны, вычисляя $\varphi\left(p_i^j\right)$ по формуле, получаем, что оно равно

$$\prod_{i=1}^{n}\left(1+(p_i-1)+\left(p_i^2-p_i\right)+\ldots+\left(p_i^{\alpha_i}-p_i^{\alpha_i-1}\right)\right)=\prod_{i=1}^{n}p_i^{\alpha_i}=n.$$

Задачи для самостоятельного решения

1. Докажите, используя свойства делимости:

а) $\left(333^{444}+555^{666}\right)\vdots 37$; б) $\left(31^{10}-1\right)\vdots 10$;

в) $\left(54^{33}-24^{33}\right)\vdots 1080$; г) $\left(62^3+38^3\right)\vdots 400$.

2. Докажите, что для любого натурального n:

а) $\left(7^{2n}-1\right)\vdots 48$; б) $\left(6^{2n-1}+1\right)\vdots 7$;

в) $\left(9^n - 8n - 1\right) \vdots 64$; г) $\left(3^{3n+2} + 2^{4n+1}\right) \vdots 11$.

3. Докажите для произвольных целых чисел n, m, что:

а) если $(3n + 5m) \vdots 11$, то $(30n + 6m) \vdots 11$;

б) если $(19n + 3m) \vdots 13$, то $(9n + 24m) \vdots 13$;

в) если $(5n + 7m) \vdots 19$, то $(43n + 64m) \vdots 19$;

г) если $(3n + 8m) \vdots 17$, то $(35n + 65m) \vdots 17$.

4. Докажите, что:

а) $\left(26^{30} - 1\right) \vdots 3 \cdot 5 \cdot 7 \cdot 11$; б) $\underbrace{77\ldots7}_{27} \vdots 189,\ 333,\ 567$.

5. Докажите, что для любого натурального n:

а) $\left(n^3 - n\right) \vdots 6$; б) $\left(n^5 - n\right) \vdots 5$;

в) $\left(n^5 - 5n^3 + 4n\right) \vdots 120$; г) $\left(n^{13} - n\right) \vdots 2730$;

д) $\left(3^{2n+3} + 40n - 27\right) \vdots 64$; е) $\left(2n^3 + 3n^2 + n\right) \vdots 6$.

6. Найдите остаток от деления a на b:

а) $a = 11218,\ b = 23$; б) $a = 127,\ b = 11$;

в) $a = -127,\ b = 11$; г) $a = 127,\ b = -11$;

д) $a = -127,\ b = -11$; е) $a = -1211,\ b = 9$.

7. Разделите с остатком:

а) $5n + 3$ на 5; б) $7n - 5$ на 7;

в) $6^n - 4$ на 2; г) $-9n - 4$ на 9.

8. Какой день недели будет через 100 дней после сегодняшнего?

9. Найдите все натуральные числа, которые:

а) при делении на 7 дают неполное частное 12;

б) не превосходят 100 и при делении на 14 и 19 дают соответственно остатки 0 и 11;

в) при делении на 6 дают неполное частное равное остатку;

г) при делении на 7 дают неполное частное и остаток, в полтора раза большие, чем соответственно частное и остаток при делении на 11.

10. Найдите все такие целые числа n, m, что:

а) при делении числа 434 на n получится неполное частное 27 и остаток m;

б) при делении числа 262 на n получится неполное частное 17 и остаток m.

11. Докажите, что квадрат натурального числа при делении:

а) на 4 может давать только остатки 0 и 1;

б) на 5 может давать только остатки 0, 1 и 4.

12. Докажите, что не может быть квадратом натурального числа число:

а) $2021^{2021}+1$; б) $2016^{2016}+1$.

13. Найдите наибольшее натуральное число, которое при делении на 11 даёт неполное частное 7.

14. Докажите, что для любого целого числа m:

а) $m\left(m^2+5\right)\vdots 6$; б) $m(m+1)(2m+1)\vdots 6$.

15. Известно, что число n при делении на 5 даёт остаток 1, а при делении на 3 – остаток 2. Найдите остаток от деления этого числа на 15.

16. В корзине лежат 5 листов бумаги. Можно взять из корзины любой лист и, разрезав его на 4 части, положить обратно. Может ли в корзине получиться 2009 кусков бумаги? 2010? 2011?

17. Докажите, что не могут быть квадратами целых чисел числа вида:

а) $3n+2$; б) $4n+2$;

в) $4n+3$; г) $5n+2$.

18. Определите, какие остатки при делении на 6,7 и 8 могут давать квадраты натуральных чисел.

19. Найдите *НОД* чисел по определению:

а) 100 и 124; б) 1001 и 169;

в) 2940 и 84; г) 1021 и 77.

20. Найдите при помощи расширенного алгоритма Евклида *НОД* и тождество Безу для чисел:

а) 156 и 462; б) 521 и 231;

в) 594 и 481; г) 17765 и 438.

21. Известно что $НОД(a,b)=1$. Вычислите при помощи свойств:

а) $НОД(a,2a+b)$; б) $НОД(a+b,3a+2b)$;

в) $НОД(5a+3b,8a+5b)$; г) $НОД(2b-5a,3a-b)$.

22. Определите, при каких значениях целого числа n данная дробь является несократимой:

а) $\frac{14n+3}{21n+4}$; б) $\frac{5n+4}{9n+7}$;

в) $\dfrac{41n+33}{9n+7}$; г) $\dfrac{6n+1}{4n+9}$.

23. Найдите количество натуральных чисел:

а) не превосходящих 400 и делящихся на 7;

б) не превосходящих 400 и не делящихся на 11;

в) не превосходящих 900 и делящихся на 5 или на 7;

г) не превосходящих 900 и не делящихся ни на 11, ни на 13;

д) не превосходящих 133 и взаимно простых с 36;

е) не превосходящих 800 и взаимно простых с 30.

24. Решите в целых числах системы уравнений:

а) $\begin{cases} \dfrac{a}{b}=\dfrac{5}{9}, \\ НОД(a,b)=28; \end{cases}$ б) $\begin{cases} ab=20, \\ НОД(a,b)=2; \end{cases}$

в) $\begin{cases} a+b=150, \\ НОД(a,b)=30; \end{cases}$ г) $\begin{cases} a+b=85, \\ 102\cdot НОД(a,b)=ab. \end{cases}$

25. От прямоугольника 324×141 мм отрезают квадраты со стороной 141 мм, пока это возможно. Затем от полученного прямоугольника снова отрезают квадраты со стороной, равной меньшей стороне прямоугольника, и т.д. Какова длина стороны последнего отрезанного квадрата? Выясните то же самое для прямоугольника размером 12606×6494 мм.

26. Докажите, что:

а) если несократимая рациональная дробь $\dfrac{n}{m}$ равна рациональной дроби $\dfrac{a}{b}$, $a,n\neq0$, то $a\vdots n$, $b\vdots m$;

б) две ненулевые несократимые рациональные дроби с натуральными знаменателями равны тогда и только тогда, когда равны их числители и соответственно знаменатели;

в) если несократимая дробь $\frac{n}{m}$ является корнем многочлена $a_k x^k + a_{k-1} x^{k-1} + \ldots + a_1 x + a_0$ с целыми коэффициентами, то $a_0 \vdots n,\ a_k \vdots m$;

г) сумма двух несократимых дробей с разными знаменателями не может быть целым числом.

27. Найдите наименьший простой делитель чисел:

а) 1001; б) 1927;

в) 1991; г) 181.

28. Разложите на простые сомножители числа:

а) 3135; б) 2431;

в) 43771; г) 5491.

29. Найдите все простые числа в промежутке:

а) от 130 до 230; б) от 150 до 350.

30. Докажите, что все простые числа ≥ 5 представимы в виде:

а) $4k+1$ или $4k+3$; б) $6k+1$ или $6k-1$.

31. Докажите, что следующие числа не могут быть одновременно простыми:

а) $p+5$ и $p+10$; б) p, $p+2$ и $p+5$;

в) 2^n-1 и 2^n+1 при $n>2$.

32. Докажите, что натуральные числа вида $6n+1$ не могут быть представлены в виде разности двух простых чисел.

33. Докажите, что

а) если $p>3$ – простое число, то $\left(p^2-1\right) \vdots 24$;

б) если числа p и $2p+1$ – простые и $p>3$, то число $4p+1$ не может быть простым;

в) если число $2^n - 1$ является простым, то и число n также является простым;

г) если число $2^n + 1$ является простым, то $n = 2^m$.

34. Запишите формулу для делителей числа. Найдите все целые делители чисел:

а) $5^2 \cdot 7^3$; б) $2 \cdot 5 \cdot 11^2$;

в) 12^3; г) 991.

35. Найдите наименьшее число, имеющее:

а) ровно 7 различных натуральных делителей;

б) ровно 30 различных натуральных делителей;

в) ровно 5 различных простых делителей.

36. Найдите все целые числа, удовлетворяющие уравнению:

а) $(n+1)(m-1) = 15$; б) $n(m-3) = 38$;

в) $nm + m - 3n = 11$; г) $3nm - 12 + n = 0$.

37. Найдите все простые числа, удовлетворяющие для подходящего n равенству:

а) $5p + 9 = n^2$; б) $7p + 4 = n^2$.

38. Докажите, что не имеет целых решений уравнение:

а) $x^2 - 3y^2 = 14$; б) $y^2 = 5x^2 + 6$;

в) $8y = x^2 + 4x - 11$; г) $2x^2 - 1 = 5y$.

39. Найдите *НОД* и *НОК* чисел по их каноническому разложению:

а) $2^2 \cdot 5^3 \cdot 11^4$ и $2^3 \cdot 3^3 \cdot 11^2$; б) $2^3 \cdot 3^4 \cdot 5^6$ и $3^3 \cdot 4^4 \cdot 6^6$;

в) $5^3 \cdot 11^2 \cdot 7^2$ и 1648801; г) $7^3 \cdot 9^2 \cdot 13$ и 2790207.

40. Вычислите по определению $\varphi(21), \varphi(22), \varphi(23)$.

41. Вычислите:

а) $\varphi(370)$; б) $\varphi(100100)$;

в) $\varphi\left(2^3 \cdot 3^4 \cdot 5^6\right)$; г) $\varphi\left(3^2 \cdot 4^2 \cdot 5 \cdot 6\right)$.

42. Найдите количество натуральных чисел, которые:

а) не превосходят 120 и взаимно просты с 30;

б) не превосходят 1035 и имеют с 1035 наибольший общий делитель, равный 9;

в) находятся в промежутке от 1000 до 1400 и имеют с числом 180 наибольший общий делитель, равный 20;

г) меньше 300 и имеют с ним наибольший общий делитель, равный 20.

ГЛАВА 2. ЭЛЕМЕНТЫ ОБЩЕЙ АЛГЕБРЫ

Сложение и умножение может быть определено для целых чисел, для действительных чисел, для квадратных матриц определённого размера, для многочленов, функций и т.д. и т.п. При этом многие исходные свойства этих операций (аксиомы) могут совпадать. Например, в перечисленных выше примерах обе операции удовлетворяют сочетательному закону, умножение относительно сложения удовлетворяет распределительному закону, сложение удовлетворяет переместительному закону и т.д.

В этих случаях имеет смысл рассматривать ситуацию в общем виде. Например, в классической алгебре и её приложениях используются такие общие понятия, как группа, кольцо, поле, векторное пространство.

§1. Понятие группы, простейшие свойства групп

2.1. Определения. *Группой* называется непустое множество G, на котором определена двуместная операция $\circ$, удовлетворяющая следующим условиям:

1) для любых $a,b,c \in G$ выполняется равенство

$$(a \circ b) \circ c = a \circ (b \circ c);$$

это свойство *ассоциативности* (или сочетательный закон);

2) существует такой элемент $e \in G$, что для любого $a \in G$ выполняется

$$a \circ e = e \circ a = a;$$

этот элемент называется *нейтральным*;

3) для любого $a \in G$ существует такое $a' \in G$, что

$$a \circ a' = a' \circ a = e;$$

элемент a' называется *симметричным* к a.

Можно доказать, что в произвольной группе нейтральный элемент и симметричный для каждого $a \in G$ элемент являются единственными.

Если группа дополнительно удовлетворяет равенству $a \circ b = b \circ a$ для любых $a, b \in G$, то она называется *коммутативной* или *абелевой* группой. В приложениях в основном используются абелевы группы.

При отсутствии свойства коммутативности элементы $a \circ b$ и $b \circ a$ могут не совпадать. Поэтому в свойствах приходится рассматривать два случая расположения элементов, например: в аксиоме 2 $a \circ e$ и $e \circ a$; в аксиоме 3 $a \circ a'$ и $a' \circ a$ и т.д. Иногда, чтобы различать эти случаи, говорят о правом или левом варианте некоторого свойства (см., например, теорему 2.3).

По традиции в теории групп используются две разновидности обозначений: *аддитивная* и *мультипликативная*. В аддитивной форме записи операция $\circ$ обозначается знаком $+$ и называется *сложением*, нейтральный элемент обозначается 0 и называется *нулём*, симметричный элемент обозначается $(-a)$ и называется *противоположным к* a.

В мультипликативной форме записи операция обозначается знаком $\times$ или $\cdot$ и называется *умножением*, нейтральный элемент обозначается 1 и называется *единицей*, симметричный элемент обозначается a^{-1} и называется *обратным к* a. В дальнейшем, как правило, будет использоваться одна из этих форм записи.

Запись $\langle G; \circ \rangle$ означает, что рассматривается непустое множество G с заданной на нём операцией $\circ$. Кроме этого, на множестве могут задаваться отношения и выделенные элементы (константы). Такая конструкция называется *алгебраической системой*. Например, запись $\langle \mathbb{Z}; +, \times; <; 0, 1 \rangle$ означает, что рассматривается множество целых чисел $\mathbb{Z}$ с операциями сложения и умножения, с отношением «меньше» $<$ и выделенными элементами 0 и 1.

2.2. Примеры. Коммутативной группой являются:

а) целые числа с операцией сложения: $\langle \mathbb{Z}; + \rangle$,

б) ненулевые действительные числа относительно операции умножения $\langle \mathbb{R}^*; \cdot \rangle$.

Целые числа относительно операции умножения $\langle \mathbb{Z}; \cdot \rangle$ группой не являются, т.к. обратные элементы имеют только числа ± 1.

Квадратные матрицы размера $n \times n$ при $n > 1$ образуют группу относительно операции умножения матриц, которая не является коммутативной.

2.3. Теорема (простейшие свойства групп). *Пусть* $\langle G; \circ \rangle$ – *группа. Тогда выполняются следующие свойства.*

1) Если $c \circ a = c \circ b$, *то* $a = b$. *Если* $a \circ c = b \circ c$, *то* $a = b$. *(левый и правый законы сокращения).*

2) Если $a \circ b = a$ *или* $c \circ a = a$, *то* $b = e$ *или соответственно* $c = e$.

3) $(a')' = a$, *т. е. симметричный к* a' *есть* a.

4) Если $a \circ b = e$, *то* $b = a'$ *и* $a = b'$.

5) $(a \circ b)' = b' \circ a'$.

Доказательство. 1) Пусть $c \circ a = c \circ b$. Умножив слева на c' и воспользовавшись аксиомами 1,3,2, последовательно получаем:

$$c' \circ (c \circ a) = c' \circ (c \circ b),\ (c' \circ c) \circ a = (c' \circ c) \circ b,$$

$$e \circ a = e \circ b,\ a = b.$$

Это свойство сокращения слева. Аналогично доказывается вторая половина свойства (сокращение справа).

2) Если $a \circ b = a$, то $a \circ b = a \circ e$ и, сократив на a слева, получаем $b = e$.

3) По определению симметричного элемента, для a' и $(a')'$ должны выполняться равенства $a' \circ (a')' = e$ и $a' \circ a = e$. Приравняв левые части и сократив слева на a', получаем $(a')' = a$.

4) По условию $a \circ b = e = a \circ a'$. Сокращая слева на a, получаем $b = a'$. Вторая половина доказывается аналогично.

5) В силу единственности симметричного элемента достаточно проверить, что $(a \circ b) \circ (b' \circ a') = e$:

$$(a \circ b) \circ (b' \circ a') \overset{\text{акс.1}}{=} a \circ (b \circ b') \circ a' \overset{\text{акс.3}}{=}$$

$$= a \circ e \circ a' \overset{\text{акс.2}}{=} a \circ a' \overset{\text{акс.3}}{=} e.$$

Перепишем теорему 2.3 в привычном виде.

2.4. Следствие (простейшие свойства групп в мультипликативном виде). *Пусть* $\langle G; \cdot \rangle$ *– группа. Тогда выполняются следующие свойства.*

1) Если $ac = bc$, *то* $a = b$. *Если* $ca = cb$, *то* $a = b$ *(закон сокращения).*

2) Если $ab = a$, *то* $b = 1$. *Если* $ca = a$, *то* $c = 1$.

3) $\left(a^{-1}\right)^{-1} = a$.

4) Если $ab = 1$, *то* $b = a^{-1}$ *и* $a = b^{-1}$.

5) $(ab)^{-1} = b^{-1}a^{-1}$.

2.5. Следствие (простейшие свойства групп в аддитивном виде). *Пусть* $\langle G; + \rangle$ *– группа. Тогда выполняются следующие свойства.*

1) Если $a + c = b + c$, *то* $a = b$. *Если* $c + a = c + b$, *то* $a = b$ *(закон сокращения).*

2) Если $a+b=a$, *то* $b=0$. *Если* $c+a=a$, *то* $c=0$.

3) $-(-a)=a$.

4) Если $a+b=0$, *то* $b=-a$ *и* $a=-b$.

5) $-(a+b)=(-b)+(-a)$.

Следствия 2.4 и 2.5 получены из теоремы 2.3 простой заменой обозначений.

2.6. Определение. *Подгруппой* группы $\langle G;\ \circ \rangle$ называется непустое подмножество H группы G, которое само является группой относительно той же операции $\circ$. Обозначение: $H \le G$.

Это частный случай такого понятия, как «подобъект». Так как аксиомы группы должны выполняться для всех элементов, то непустое подмножество группы является её подгруппой тогда и только тогда, когда оно замкнуто относительно операции, содержит нейтральный элемент и для всякого элемента содержит симметричный к нему. Часть из этих условий можно опустить.

2.7. Теорема (критерий подгруппы). *Непустое подмножество H группы* $\langle G;\circ \rangle$ *является её подгруппой, тогда и только тогда, когда оно замкнуто относительно операции* $\circ$ *и взятия симметричного, т.е. если для любых элементов* a, b *из* H *элементы* $a\circ b$ *и* a' *снова принадлежат* H.

Доказательство. В прямую сторону утверждение очевидно. Докажем его в обратную сторону.

Пусть непустое подмножество $H \subseteq G$ замкнуто относительно основной операции и взятия симметричного. Так как $H \neq \varnothing$, то существует $a \in H$. Из условий следует, что $a' \in H$, $a\circ a' \in H$, и т.к. $a\circ a' = e$, то $e \in H$.

2.8. Пример. 1) Множество всех целых чётных чисел по сложению является подгруппой группы всех целых чисел по сложению.

2) Множество всех целых неотрицательных чисел по сложению не является подгруппой целых чисел по сложению,

т.к. оно не является замкнутым относительно взятия противоположного элемента.

2.9. Определение. Группа $\langle G; * \rangle$ *изоморфна* группе $\langle H; \circ \rangle$, если существует взаимно однозначное отображение f множества G на множество H такое, что для любых элементов $a, b \in G$ выполняется равенство

$$f(a * b) = f(a) \circ f(b).$$

Обозначение: $G \cong H$.

Отношение изоморфизма – это аналог равенства для алгебраических систем. Изоморфные системы можно считать копиями друг друга.

2.10. Пример (показывающий, что копии могут быть не похожи друг на друга). Группа $\langle \mathbb{R}^+; \cdot \rangle$ всех положительных действительных чисел с операцией умножения изоморфна группе $\langle \mathbb{R}; + \rangle$ действительных чисел с операцией сложения. В качестве взаимно однозначного отображения множества $\mathbb{R}^+$ на $\mathbb{R}$ можно взять логарифмическую функцию по любому основанию и свойство логарифмов:

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

§2. Порядок элемента

Пусть G – некоторая (мультипликативная) группа. Для произвольного элемента a из G и натурального числа n определим натуральную степень:

$$\underbrace{a \cdot a \cdot a \cdot \ldots \cdot a}_{n} = a^n.$$

Используя понятие обратного элемента, степень можно определить для любого целого показателя, положив по определению:

$$a^0 = 1,\ \ a^{-n} = \left(a^{-1}\right)^n .$$

Обыкновенные дроби вводятся при помощи равенства

$$\frac{a}{b} = ab^{-1} .$$

После этого можно доказать

2.11. Свойства степеней. *Для любых элементов a,b некоторой мультипликативной группы и любых целых чисел n,m выполняются следующие равенства:*

а) $a^n \cdot a^m = a^{n+m}$;

б) $\left(a^n\right)^m = a^{nm}$;

в) $a^n \cdot b^n = (ab)^n$;

г) $\dfrac{a^n}{a^m} = a^{n-m}$;

д) $\left(\dfrac{a}{b}\right)^n = \dfrac{a^n}{b^n}$.

Аналогичное понятие в аддитивной группе называется *кратным элемента:*

$$\underbrace{a + a + \ldots + a}_{n} = n * a,\ \ n \in \mathbb{N} .$$

При помощи противоположных элементов понятие кратного распространяется на целые числа:

$$0 * a = 0,\ \ (-n) * a = -(n * a) .$$

2.12. Свойства кратных. *Для любых элементов a,b некоторой аддитивной группы и целых чисел n,m выполняются следующие равенства*:

а) $n * a + m * a = (n + m) * a$;

б) $m*(n*a)=(mn)*a$;

в) $n*a+n*b=n*(a+b)$;

г) $n*a-m*a=(n-m)*a$;

д) $n*(a-b)=n*a-n*b$;

е) $(n*a)b=n*(ab)$.

Доказательство этих свойств не представляет сложности и оставляется в качестве упражнения читателю.

Рассмотрим последовательность степеней некоторого элемента a в мультипликативной группе:

$$a^0=1,\ a^1,\ a^2,\ a^3,\ \ldots \qquad (1)$$

Возможны два случая.

1) Существуют такие натуральные $n\neq m$, что $a^n=a^m$.

2) Все элементы последовательности (1) попарно различны.

2.13. Замечание. *Равенство $a^n=a^m$ справедливо для некоторых натуральных $n\neq m$ тогда и только тогда, когда существует такое натуральное k, что $a^k=1$.*

Действительно, пусть $a^n=a^m$ и, для определённости, пусть $n>m$. Тогда можно сократить на a^m и получить равенство $a^{n-m}=1$.

В обратную сторону, если $a^k=1,\ k\neq 0$, то $a^{k+1}=a^1$.

Ввиду замечания элементы последовательности (1) попарно различны тогда и только тогда, когда $a^k\neq 1$ для любого натурального k.

2.14. Определение. *Порядком элемента a* группы G называется такое наименьшее натуральное число k, что $a^k=1$. Если такого числа не существует, то говорят, что a является *элементом бесконечного порядка.*

Обозначение: $ord(a)$.

N.B. Количество элементов в конечной группе также называется её *порядком*. Если группа бесконечна, то говорят, что она имеет *бесконечный порядок*.

2.15. Пример. 1) В группе $\langle \mathbb{Z}; + \rangle$ целых чисел по сложению порядки всех ненулевых элементов бесконечны, т.к. сумма $\underbrace{a+a+a+\ldots+a}_{k}$ отлична от нуля для любого целого $a \neq 0$ и для любого натурального k.

2) В группе $\langle \mathbb{C}^*; \cdot \rangle$ ненулевых комплексных чисел по умножению есть как элементы произвольного конечного порядка k (это корни k-й степени из 1), так и элементы бесконечного порядка (все остальные числа).

2.16. Свойства (порядков). *Пусть $\langle G; \cdot \rangle$ – некоторая группа и дан её элемент a порядка k. Для любых целых чисел n, m справедливы следующие утверждения.*

1) Равенство $a^m = 1$ выполняется тогда и только тогда, когда $m \vdots k$.

2) Равенство $a^n = a^m$ выполняется тогда и только тогда, когда $(n-m) \vdots k$.

3) Элементы $a^0 = 1$, a^1, a^2, a^3, …, a^{k-1} попарно различны.

4) $ord\left(a^m\right) = \dfrac{k}{НОД(m,k)}$.

5) $a^{-1} = a^{k-1}$.

6) Если элемент b группы G перестановочен с элементом a и имеет порядок s, взаимно простой с k, то $ord(ab) = ord(a)ord(b)$.

Доказательство. 1) Разделим m с остатком на k:

$$m = kq + r,\ 0 \le r < k\ .$$

Если $r \neq 0$, то

$$1 = a^m = a^{kq+r} = \left(a^k\right)^q a^r = (1)^q a^r = a^r\ .$$

Получилось, что $a^r = 1$ и $r < k$. Это противоречит определению порядка, поэтому $r = 0$ и $m = kq$.

2) Равенство $a^n = a^m$ равносильно тому, что $a^{n-m} = 1$. Воспользовавшись предыдущим пунктом, получаем $(n-m) \vdots k$.

3) Если $a^n = a^m$ для некоторых $0 \le m < n < k$, то $(n-m) \vdots k$ и $0 < n - m < k$, что невозможно.

4) Во-первых, для этой степени выполняется нужное свойство:

$$\left(a^m\right)^{\frac{k}{НОД(m,k)}} = \left(a^k\right)^{\frac{m}{НОД(m,k)}} = (1)^{\frac{m}{НОД(m,k)}} = 1\ .$$

Во-вторых, если для некоторого натурального n выполняется равенство $\left(a^m\right)^n = 1$, то, согласно пункту 1), это равносильно тому, что произведение mn делится на k, а это, в свою очередь, равносильно тому, что $\dfrac{mn}{НОД(m,k)}$ делится на $\dfrac{k}{НОД(m,k)}$.

Так как числа $\dfrac{m}{НОД(m,k)}$ и $\dfrac{k}{НОД(m,k)}$ взаимно просты, то по свойству делимости 1.30 получаем, что последнее соотношение равносильно тому, что число n делится на $\dfrac{k}{НОД(m,k)}$ и, следовательно, $n \ge \dfrac{k}{НОД(m,k)}$.

В результате наименьшее натуральное n с условием $\left(a^m\right)^n = 1$ равно $\dfrac{k}{НОД(m,k)}$.

5) Так как $a^k = a \cdot a^{k-1} = 1$, то по определению обратного элемента $a^{-1} = a^{k-1}$.

6) Пусть $m = ord(ab)$, пользуясь равенством $ab = ba$, получаем

$$(ab)^{sk} = a^{sk} b^{sk} = \left(a^k\right)^s \left(b^s\right)^k = 1^s 1^k = 1.$$

Согласно пункту 1), это означает, что произведение sk делится на m.

С другой стороны, так как $(ab)^m = 1 = a^m b^m$, то $a^m = b^{-m}$ и $ord\left(a^m\right) = ord\left(b^{-m}\right) = ord\left(b^m\right)$. Согласно пункту 4), получаем, что $\dfrac{k}{НОД(m,k)} = \dfrac{s}{НОД(m,s)}$. Поскольку числа k и s взаимно просты по условию, то

$$\frac{k}{НОД(m,k)} = \frac{s}{НОД(m,s)} = 1.$$

Тогда $k = НОД(m,k)$, $s = НОД(m,s)$, $m \vdots k$, $m \vdots s$ и, следовательно, $m \vdots sk$.

Наконец, совмещая соотношения $sk \vdots m$ и $m \vdots sk$, получаем, что $m = sk$.

Если обобщить понятие порядка на все элементы группы, то получим понятие экспоненты группы.

2.17. Определение. *Экспонентой группы* G называется такое наименьшее натуральное число m, что для любого элемента a из G справедливо равенство

$$a^m = 1.$$

Если натурального числа с таким свойством не существует, то экспоненту полагают равной бесконечности.

Обозначение: $\exp G$.

2.18. Теорема (об экспоненте конечной группы). *Экспонента конечной группы* $G=\{a_1,a_2,\ldots,a_n\}$ *конечна и удовлетворяет равенству*

$$\exp G = НОК\big(\operatorname{ord}(a_1),\operatorname{ord}(a_2),\ldots,\operatorname{ord}(a_n)\big).$$

Если G *– конечная абелева группа, то существует такой элемент* g *из* G, *что* $\operatorname{ord}(g)=\exp G$.

Доказательство. Пусть

$$k = НОК\big(\operatorname{ord}(a_1),\operatorname{ord}(a_2),\ldots,\operatorname{ord}(a_n)\big).$$

По свойству порядков 2.16.1) для любого i выполняется равенство $(a_i)^k=1$, поэтому $\exp G\le k$. Пусть $\exp G=m$, тогда $(a_i)^m=1$ и, снова по свойству 1), число m делится на $\operatorname{ord}(a_i)$ для любого i. Из определения наименьшего общего кратного 1.46 получаем тогда, что $m\vdots k$ и, следовательно, $m\ge k$. В результате $m=k$.

Пусть G – абелева группа. Найдём каноническое разложение числа m:

$$m = p_1^{k_1} p_2^{k_2}\ldots p_t^{k_t}.$$

Из определения НОК следует, что для каждого i, $1\le i\le t$, в группе G существует такой элемент h_i, что $\operatorname{ord}(h_i)\vdots p_i^{k_i}$. Пусть $\operatorname{ord}(h_i)=p_i^{k_i}n_i$. Очевидно, числа p_i и n_i взаимно просты. Положим $f_i=(h_i)^{n_i}$, тогда по свойству порядков 2.16.4) получаем, что $\operatorname{ord}(f_i)=p_i^{k_i}$, $1\le i\le t$. Воспользовавшись коммутативностью группы и свойством 2.16.6), получаем, что искомым является элемент $g=f_1f_2\ldots f_t$.

§3. Циклические группы

Множество степеней некоторого элемента $a \neq 1$ мультипликативной группы G замкнуто относительно умножения и взятия обратного, поэтому образует подгруппу в G. Такая подгруппа называется *циклической*. Можно рассматривать циклические группы отдельно.

2.19. Определение. Группа G называется *циклической*, если её основное множество состоит из степеней некоторого элемента a. Этот элемент называется *порождающим (образующим) элементом группы*. Говорят, что он *порождает* группу G и пишут $G = gr(a)$.

Очевидно, что *порядок порождающего элемента циклической группы совпадает с порядком группы*.

Если рассматривается аддитивная форма записи, то вместо степеней рассматриваются элементы вида

$$\underbrace{a + a + \ldots + a}_{n} = n * a .$$

2.20. Примеры. 1) Множество комплексных корней степени n из единицы относительно операции умножения образуют циклическую группу порядка n. В качестве порождающего элемента можно взять

$$u_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} .$$

Действительно,

$$(u_1)^k = \left(\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}\right)^k = \left(\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}\right) = u_k .$$

$$(u_1)^n = \left(\cos\frac{2\pi n}{n} + i\sin\frac{2\pi n}{n}\right) = 1 .$$

2) Множество целых чисел с операцией сложения образуют бесконечную циклическую группу. Порождающим элементом является единица, т.к. для любого $n \in \mathbb{Z}$ выполняется

$$n = \pm\underbrace{(1+1+\ldots+1)}_{|n|}.$$

2.21. Теорема (свойства циклических групп).

1) Все циклические группы коммутативны.

2) Циклические группы одного порядка изоморфны между собой.

3) Всякая подгруппа циклической группы сама является циклической.

4) Конечная циклическая группа порядка m имеет $\varphi(m)$ различных порождающих элементов.

Доказательство. 1) Пусть $G = gr(a)$ и x, y – некоторые элементы G. Тогда $x = a^n$, $y = a^m$ и

$$xy = a^n \cdot a^m = a^{n+m} = a^{m+n} = a^m \cdot a^n = yx .$$

2) Пусть $G = gr(a)$, $H = gr(b)$ – две циклические группы конечного порядка n. Заметим, что $G = \{1, a, a^1, a^2, \ldots, a^{n-1}\}$, т.к. для любого целого числа m мы можем вычислить степень a^m по следующему правилу. Делим m на n с остатком и вычисляем a^m:

$$m = nq + r,\ 0 \le r < n ,$$

$$a^m = a^{nq+r} = \left(a^n\right)^q a^r = (1)^q a^r = a^r,\ 0 \le r < n .$$

После этого можно задать отображение $f : G \to H$ по правилу

$$f\left(a^m\right) = b^m .$$

Оно будет взаимно однозначным отображением G на H, т.к., во-первых, эти группы имеют одинаковое количество элементов. И, во-вторых, по свойству порядка 2.16.3) элементы

$1, a, a^1, a^2, \ldots, a^{n-1}$ попарно различны. Элементы $1, b, b^1, b^2, \ldots, b^{n-1}$ также попарно различны.

Кроме того, выполняется характеристическое свойство изоморфизма:

$$f\left(a^m \cdot a^k\right) = f\left(a^{m+k}\right) = b^{m+k} = b^m \cdot b^k = f\left(a^m\right) \cdot f\left(a^k\right).$$

Для групп бесконечного порядка доказательство аналогично.

3) Пусть $G = gr(a)$ и H – её подгруппа. Если $H = \{1\}$, то доказывать нечего. Пусть H содержит какую-нибудь неединичную степень $a^m \neq 1$. Можно считать, что $m > 0$, т.к. если $m < 0$, то по критерию подгруппы $\left(a^m\right)^{-1} = a^{-m} \in H$ и $(-m) > 0$. Выберем такое наименьшее положительное s, что $a^s \in H$, и докажем, что H – циклическая группа, порождённая a^s.

Действительно, если $a^k \in H$, то по теореме о делении с остатком $k = sq + r$, $0 \leq r < s$, и

$$a^r = a^{k-sq} = a^k \cdot \left(a^s\right)^{-q} \in H.$$

Если $r \neq 0$, то получится противоречие с выбором степени s. Поэтому $r = 0$, $k = sq$ и $a^k = \left(a^s\right)^q$.

4) Элементы конечной циклической группы порядка m могут быть записаны в виде

$$a^0 = 1, a^1, a^2, \ldots, a^{m-1},$$

кроме того, $a^m = 1$. Рассмотрим все числа $1 \leq k \leq m$ взаимно простые с m. Их ровно $\varphi(m)$ штук. По свойству порядков 2.16.4) элементы вида a^k будут порождающими. Остальные элементы

порождающими не будут, т.к. их порядок равен $\frac{m}{НОД(m,k)}$ и строго меньше m. Теорема доказана.

§4. Отношение эквивалентности и фактор-множество

Понятие фактор-множества широко используется в алгебре и её приложениях. В рамках этого параграфа будут рассмотрены основные определения и доказаны простейшие факты.

2.22. Определение. Пусть дано непустое множество A. *Отношением эквивалентности* на множестве A называется всякое отношение $\sim$, которое для любых $a,b,c \in A$ удовлетворяет следующим свойствам (аксиомам):

а) $a \sim a$ (*рефлексивность*);

б) если $a \sim b$, то $b \sim a$ (*симметричность*);

в) если $a \sim b$ и $b \sim c$, $a \sim c$ (*транзитивность*).

2.23. Примеры. 1) Простейшим отношением эквивалентности является отношение равенства элементов некоторого множества.

2) Можно рассмотреть также отношение равенства некоторых свойств элементов, например: на множестве всех людей – отношение «иметь одинаковую национальность».

Аксиомы отношения эквивалентности для этих примеров очевидно выполняются. Менее очевидные примеры будут рассмотрены ниже.

2.24. Определение. Пусть A – некоторое непустое множество, на котором задано отношение эквивалентности $\sim$. *Классом эквивалентности* элемента $a \in A$ называется множество

$$[a]_{\sim} = \{x \in A \mid x \sim a\}.$$

Согласно определению, класс эквивалентности – это множество всех элементов, эквивалентных данному.

2.25. Свойства (классов эквивалентности). *Пусть* A – *некоторое непустое множество, на котором задано отношение эквивалентности* $\sim$. *Для любых элементов* a,b,x,y *множества* A *выполняются следующие свойства:*

1) $a \in [a]_{\sim}$;

2) если $x,y \in [a]_{\sim}$, *то* $x \sim y$;

3) если $b \in [a]_{\sim}$, *то* $[a]_{\sim} = [b]_{\sim}$;

4) любые два класса эквивалентности либо совпадают, либо не пересекаются;

5) $A = \bigcup\limits_{a \in A} [a]_{\sim}$.

Доказательство. 1) следует из определения класса эквивалентности и того, что $a \sim a$.

2) Если $x,y \in [a]_{\sim}$, то $x \sim a$ и $y \sim a$. Из соотношения $y \sim a$ по свойству симметричности получаем $a \sim y$. После этого применяем транзитивность к соотношениям $x \sim a$ и $a \sim y$ и получаем $x \sim y$.

3) Пусть $b \in [a]_{\sim}$, тогда $a \sim b$. Если $x \in [a]_{\sim}$, то $x \sim a \sim b$. По свойству транзитивности тогда $x \sim b$ и, следовательно, $x \in [b]_{\sim}$. В обратную сторону. Если $x \in [b]_{\sim}$, то $x \sim b$. Из соотношения $a \sim b$ по свойству симметричности получаем $b \sim a$. После этого применяем транзитивность к соотношениям $x \sim b$ и $b \sim a$ и получаем $x \sim a$, $x \in [a]_{\sim}$.

4) Если $[a]_{\sim} \cap [b]_{\sim} = \varnothing$, то $[a]_{\sim} \neq [b]_{\sim}$. Если существует $x \in [a]_{\sim} \cap [b]_{\sim}$, то по свойству 2) $[a]_{\sim} = [x]_{\sim} = [b]_{\sim}$ и, следовательно, $[a]_{\sim} = [b]_{\sim}$.

5) Так как $a \in [a]_{\sim}$, то $A \subseteq \bigcup\limits_{a \in A} [a]_{\sim}$. Обратное включение очевидно.

2.26. Определение. *Фактор-множеством* множества A по отношению эквивалентности $\sim$ называется множество, состоящее из всех классов эквивалентности по этому отношению:

$$A/_{\sim} = \{[a]_{\sim},\ a \in A\}.$$

2.27. Определение. *Разбиением* непустого множества A называется такая совокупность его подмножеств A_i, $i \in I$, что:

1) подмножества A_i попарно не пересекаются;

2) объединение подмножеств A_i совпадает с A.

2.28. Замечания. 1) Из свойств 1)–3) следует, что классы эквивалентности являются непустыми, каждый класс состоит из попарно эквивалентных элементов и однозначно определяется любым своим элементом (представителем). Оперировать с множествами во многих случаях не совсем удобно, поэтому в классах эквивалентности обычно выбираются «канонические» (самые удобные) представители и все вычисления производятся над ними.

2) Из свойств 4) и 5) следует, что классы эквивалентности образуют разбиение данного множества.

Можно установить и обратную связь.

2.29. Теорема. *Пусть дано некоторое непустое множество A и его разбиение A_i, $i \in I$. На множестве A можно определить такое отношение эквивалентности, что разбиение совпадёт с фактор-множеством.*

Доказательство. Определим отношение $\sim$ на A по правилу:

$$a \sim b \ \Leftrightarrow\ a, b \in A_i \text{ для некоторого подходящего } i \in I.$$

После этого по определению легко проверяется, что это отношение рефлексивно, симметрично, транзитивно и для любого $a \in A$:

$$a \in A_i \;\Leftrightarrow\; [a]_{\sim} = A_i\,.$$

§5. Теорема Лагранжа

Рассмотрим понятие фактор-группы. Пусть даны группа G и её подгруппа H. Рассмотрим подмножества вида

$$gH = \left\{ gh \,\middle|\, h \in H \right\} \subseteq G\,,$$

которые называются *(левыми) смежными классами* группы G по подгруппе H. Аналогично можно рассматривать *правые смежные классы* Hg. Для определённости будем рассматривать только левые смежные классы.

2.30. Теорема (свойства смежных классов). *1) Смежные классы по любой подгруппе образуют разбиение множества G.*

2) Отношение эквивалентности $\sim_H$, которое определяется этим разбиением, может быть задано так: $a \sim_H b \;\Leftrightarrow\; a^{-1}b \in H$.

3) Все смежные классы по данной конечной подгруппе имеют одинаковое количество элементов.

Доказательство. 1) Докажем, что если два смежных класса пересекаются, то они полностью совпадают.

Пусть $a \in g_1H \cap g_2H$, тогда $a = g_1h_1 = g_2h_2$ для некоторых $h_1,\ h_2 \in H$ и, следовательно, $g_1 = g_2h_2\left(h_1\right)^{-1}$.

Если $x \in g_1H$, то $x = g_1h$ для некоторого $h \in H$ и

$$x = g_1h = \left(g_2h_2\left(h_1\right)^{-1}\right)h = g_2\left(h_2\left(h_1\right)^{-1}h\right) \in g_2H\,,$$

т.к. $\left(h_2\left(h_1\right)^{-1}h\right) \in H$. Аналогично доказывается, что $g_1H \supseteq g_2H$.

Докажем, что объединение смежных классов даёт всё множество G:

$$\bigcup_{g\in G} gH = G\,.$$

Действительно, $g\in gH$, т.к. $g = g\cdot 1$ и $1\in H$. Поэтому $G\subseteq \bigcup\limits_{g\in G} gH$. Обратное включение следует из того, что $gH\subseteq G$ и, следовательно,

$$\bigcup_{g\in G} gH \subseteq G\,.$$

2) Согласно 2.29, отношение эквивалентности, задаваемое разбиением, нужно определять так:

$$a\sim_H b \;\Leftrightarrow\; a,b\in gH \text{ для некоторого } g\in G\,.$$

Пусть $a,b\in gH$, тогда $a = g h_1$, $b = g h_2$ и

$$a^{-1}b = \left(h_1^{-1}g^{-1}\right)(gh_2) = h_1^{-1}h_2 \in H\,.$$

В обратную сторону. Если $a^{-1}b\in H$, то $a^{-1}b = h\in H$, $b = a h$ и, следовательно, $a,b\in a\,H$.

3) Если подгруппа H имеет n элементов, то все смежные классы по этой подгруппе также имеют по n элементов. Для доказательства достаточно заметить, что отображение $t_g(x) = gx$ является взаимно однозначным отображением подгруппы H на смежный класс gH.

Теорема доказана.

Напомним, что *порядком группы* называется количество элементов (мощность) группы. Оно может быть как конечным, так и бесконечным. Наибольший интерес это понятие представляет для конечных групп ввиду следующего

2.31. Следствия (теорема Лагранжа). *Порядок конечной группы делится на порядок любой её подгруппы.*

Для доказательства нужно воспользоваться пунктами 1) и 3) предыдущей теоремы.

2.32. Следствие. *Порядок n конечной группы G делится на порядок любого её элемента a, делится на экспоненту группы и, кроме того, выполняется равенство $a^n = 1$.*

Действительно, пусть $a \in G$ и $ord(a) = m$. Тогда $a^m = 1$ и элементы $a^0 = 1, a^1, a^2, \ldots, a^{m-1}$ образуют циклическую подгруппу в G порядка m. По теореме Лагранжа порядок n делится на m.

Остальные утверждения следуют из описания экспоненты 2.18 и свойства порядков 2.16.1).

2.33. Определение. Множество всех смежных классов по заданной подгруппе называется *фактор-множеством по подгруппе* и обозначается G / H.

Для любых подмножеств $A, B \subseteq G$ можно определить произведение:

$$AB = \left\{ ab \,\middle|\, a \in A,\ b \in B \right\}.$$

Выясним, при каких условиях это фактор-множество будет группой относительно этого умножения.

2.34. Определение. Подгруппа H группы G называется *нормальной,* если для любого элемента $g \in G$ выполняется равенство $gH = Hg$, т.е. левые и правые смежные классы по подгруппе H совпадают.

В абелевых группах это понятие теряет смысл, т.к. все подгруппы оказываются нормальными.

2.35. Теорема. *Фактор-множество по нормальной подгруппе является группой относительно определённого выше умножения множеств и называется фактор-группой.*

Доказательство. Так как H – это подгруппа, то она замкнута относительно умножения и, следовательно, $H \cdot H = H$. Звездочкой будем помечать равенства, в которых использовалась нормальность подгруппы H.

1) Докажем, что произведение смежных классов снова будет смежным классом, т.е. умножение смежных классов является алгебраической операцией на фактор-множестве.

Действительно,

$$g_1H \cdot g_2H \overset{*)}{=} Hg_1 \cdot g_2H = H(g_1g_2) \cdot H \overset{*)}{=}$$

$$= (g_1g_2)H \cdot H = (g_1g_2)H .$$

2) Докажем ассоциативность операции умножения смежных классов.

$$(g_1H \cdot g_2H) \cdot g_3H \overset{1)}{=} (g_1g_2)H \cdot g_3H \overset{1)}{=} ((g_1g_2)g_3)H \overset{acc.}{=}$$

$$= (g_1(g_2g_3))H \overset{1)}{=} g_1H \cdot (g_2g_3)H \overset{1)}{=} g_1H \cdot (g_2H \cdot g_3H) .$$

3) Докажем существование единичного элемента. Им будет смежный класс $1H = H$. Действительно,

$$gH \cdot H = gH,\ H \cdot gH \overset{*)}{=} H \cdot Hg = Hg \overset{*)}{=} gH .$$

4) Докажем существование обратного элемента. Для смежного класса gH обратным будет смежный класс $g^{-1}H$. Действительно,

$$gH \cdot g^{-1}H \overset{1)}{=} \left(g \cdot g^{-1}\right)H = 1H = H ,$$

$$g^{-1}H \cdot gH \overset{1)}{=} H\left(g^{-1} \cdot g\right) = H1 = H .$$

Теорема доказана.

Используя свойства порядка и теорему Лагранжа, можно предложить

2.36. АЛГОРИТМ ВЫЧИСЛЕНИЯ ПОРЯДКА ЭЛЕМЕНТА. Пусть G – конечная мультипликативная группа порядка n и необходимо вычислить порядок некоторого элемента $a \in G$. Пусть удалось

найти каноническое разложение числа $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ в произведение попарно различных простых чисел $p_1, p_2, \ldots, p_k$. Тогда, воспользовавшись формулой для делителей 1.42 и тем, что порядок любого элемента является делителем числа n, можно предложить следующий алгоритм.

1) Перебирая последовательно $s_1 = 0,1,2,\ldots$, находим наименьшее $m_1 = \dfrac{n}{p_1^{s_1}}$, для которого выполняется равенство

$$a^{m_1} = 1.$$

2) Затем, перебирая последовательно $s_2 = 0,1,2,\ldots$, находим наименьшее $m_2 = \dfrac{m_1}{p_2^{s_2}}$, для которого выполняется равенство

$$a^{m_2} = 1.$$

3) Далее действуем аналогично и на k-м шаге найдём $m_k = ord(a)$.

В некоторых случаях для поиска элемента нужного порядка можно применять метод случайного перебора. Например,

2.37. Алгоритм поиска порождающего элемента в циклической группе. Пусть G – конечная мультипликативная циклическая группа порядка n и необходимо найти порождающий элемент $a \in G$. Порядок порождающего элемента равен n. Пусть удалось найти каноническое разложение порядка группы $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, где $p_1, p_2, \ldots, p_k$ – попарно различные простые числа.

1) Выбираем случайным образом элемент $a \in G$.

2) Перебирая последовательно значения i от 1 до k, вычисляем $b = a^{n/p_i}$. Если оказывается, что $b = 1$, то переходим к пункту 1).

3) Элемент b, прошедший проверку в пункте 2), является порождающим элементом данной циклической группы, т.к. его порядок равен n.

Эффективность этого алгоритма основана на том, что, согласно свойству 2.21.4) циклических групп, количество порождающих элементов равно $\varphi(n)$. Вероятность того, что случайно выбранный элемент окажется порождающим, равна $\frac{\varphi(n)}{n}$. Эта величина достаточно велика. Например, можно доказать, что $\frac{\varphi(n)}{n} > \frac{1}{6\ln\ln n}$.

Поиск методом случайного перебора элементов маленьких порядков неэффективен.

Как дополнение к теореме Лагранжа можно рассматривать следующую теорему, которая является частным случаем теоремы Коши.

2.38. Теорема (Коши). *Если G – конечная абелева группа порядка n и p – простой делитель числа n, то в G существует элемент порядка p.*

Доказательство. Индукция по n. Если $n=2$, то $G=\{1,a\}$, очевидно $a^2=1$ и $ord(a)=2$. Можно утверждать большее: *если порядок группы является простым числом, то эта группа будет циклической* и любой её порождающий элемент будет иметь нужный порядок.

Пусть дано некоторое $n>1$ и для всех $k<n$ утверждение теоремы выполняется. Докажем его для произвольной группы G, порядок которой равен n и делится на простое число p. Выберем произвольно $b\in G, b\neq 1$. Пусть $ord(b)=m$. Возможны два случая.

1-й случай: $m \vdots p$. В этом случае подходящим элементом будет $a=b^k$, где $k=\frac{m}{p}$.

2-й случай: m взаимно прост с p. Рассмотрим циклическую подгруппу $H = gr(b)$, порождённую элементом b, и фактор-группу G/H. Так как $|H| = m$, то $|G/H| = \frac{n}{m}$. Так как m и p взаимно просты, то $\frac{n}{m} \vdots p$. Так как $\frac{n}{m} < n$, то по предположению индукции фактор-группа G/H имеет элемент cH порядка p. Если $c^s = 1$, то $(cH)^s = H = 1$. Согласно свойству порядков 2.16.1), получаем $s \vdots p$ и, следовательно, $ord(c) \vdots p$. В результате нашелся элемент c, для которого имеет место 1-й случай.

§6. Кольца

2.39. Определение. Непустое множество K с заданными на нем двумя бинарными алгебраическими операциями + и · называется *кольцом*, если выполняются свойства:

1) $\langle K;\ + \rangle$ – коммутативная (абелева) группа;

2) для любых $a, b, c \in K$:

$$(a+b)c = ac + bc \quad \text{и} \quad a(b+c) = ab + ac$$

(это свойство *дистрибутивности* или *распределительный закон*).

Операции + и · называются *сложением* и *умножением* соответственно. Знак операции умножения (точку) для краткости договариваются не писать.

Пользуясь существованием противоположного элемента, в каждом кольце можно определить *разность*:

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

Кольцо называется *ассоциативным*, если операция умножения ассоциативна на K; *коммутативным* – если операция умножения коммутативна; *кольцом с единицей* – если

существует нейтральный элемент относительно умножения $1 \in K$.

N.B. В дальнейшем будут рассматриваться только ассоциативные кольца с единицей.

Элементы $a, b \in K$ называются *делителями нуля*, если $a \neq 0$, $b \neq 0$, но $ab = 0$ или $ba = 0$. Кольцо $\langle K;\ +;\ \cdot \rangle$ называется *областью целостности*, если оно коммутативно, $0 \neq 1$ и в нём нет делителей нуля, т.е. для любых $a, b \in K$ из условия $ab = 0$ следует $a = 0$ или $b = 0$.

Так как всякое кольцо является абелевой группой относительно сложения, то все аддитивные свойства групп автоматически выполняются.

2.40. Примеры. 1) Множества целых, рациональных и действительных чисел относительно обычных операций сложения и умножения $\langle \mathbb{Z};\ +;\ \cdot \rangle$, $\langle \mathbb{Q};\ +;\ \cdot \rangle$, $\langle \mathbb{R};\ +;\ \cdot \rangle$ являются областями целостности.

2) Множество всех отображений из $\mathbb{R}$ в $\mathbb{R}$ с операциями:

$$(f+g)(x) = f(x) + g(x), \quad (f \cdot g)(x) = f(x) \cdot g(x)$$

образует коммутативное, ассоциативное кольцо с делителями нуля и с единицей.

3) Множество всех квадратных матриц размерности $n \times n$ с обычными операциями сложения и умножения образует ассоциативное, но не коммутативное (при $n \geq 2$) кольцо с делителями нуля.

Например, при $n = 2$ следующие две матрицы являются делителями нуля и не являются перестановочными:

$$\begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ -3 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 0 \\ -3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 5 & 0 \end{pmatrix}.$$

2.41. Теорема (простейшие свойства колец). *Пусть* $\langle K;\ +;\ \cdot \rangle$ *– некоторое кольцо. Тогда для любых его элементов выполняются следующие свойства.*

1) $a0 = 0a = 0$.

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

3) $-(a+b) = (-a) + (-b)$.

4) $-a = (-1)a$ *(если в кольце есть единица).*

5) $(a-b)c = ac - bc$, $a(b-c) = ab - ac$.

6) свойство отсутствия делителей нуля равносильно свойству сокращения: $\forall a,b,c\big(ac = bc, c \neq 0 \Rightarrow a = b\big)$.

7) если кольцо не имеет делителей нуля, то частное любых двух элементов a,b, $b \neq 0$, *единственно.*

Доказательство. 1) Заметим, что $a0 + a0 = a(0+0) = a0$, т.е. $a0 + a0 = a0$. По свойству групп 2.5.2) получаем, что $a0 = 0$. Аналогично доказывается, что $0a = 0$.

2) $a(-b) + ab = a(-b+b) = a0 = 0$. По свойству 2.5.4) $a(-b) = -ab$. Аналогично доказывается, что $(-a)b = -ab$. Далее, воспользовавшись этими равенствами и свойством 2.5.3), получаем $(-a)(-b) = -a(-b) = -(-ab) = ab$.

3) Так как

$$(a+b) + (-a) + (-b) = (a+b) + (-b) + (-a) =$$

$$= a + (b + (-b)) + (-a) = a + 0 + (-a) = a + (-a) = 0,$$

то элемент $(-a) + (-b)$ является противоположным к $(a+b)$.

4) Действуем так, как и в предыдущем пункте:

$$a + (-1)a = 1a + (-1)a = (1 + (-1))a = 0a = 0.$$

5) Воспользуемся определением разности и аддитивными свойствами групп:

$$(a-b)c=\big(a+(-b)\big)c=ac+(-b)c=\ ac+\big(-bc\big)=ac-bc\,.$$

Вторая часть доказывается аналогично.

6) Пусть выполняется свойство отсутствия делителей нуля и для некоторых a,b и $c\neq 0$ выполняется $ac=bc$. Тогда $(a-b)c=0$, и т.к. $c\neq 0$, то $a-b=0$ и $a=b$.

В обратную сторону. Пусть свойство сокращения выполняется и $ab=0$. Если $b=0$, то доказывать нечего. Если $b\neq 0$, то $ab=0=0b$ и, сократив на b, получаем $a=0$.

7) Пусть $a=bq_1=bq_2$, сократив на $b\neq 0$, получаем $q_1=q_2$.

При рассмотрении свойств делимости важно знать: имеет кольцо K делители нуля или нет.

Разберём конструкцию фактор-кольца, ограничившись случаем коммутативно-ассоциативных колец с единицей. Большая часть излагаемого материала в неизменном виде подходит для случая некоммутативных колец.

2.42. Определение. Пусть K – некоторое кольцо и дано непустое множество $I\subseteq K$. Говорят, что I является *идеалом* кольца K, если оно замкнуто относительно вычитания и умножения на элементы кольца K, т.е. если для любых $a,b\in I$ и любого $k\in K$ выполняется $a-b\in I$ и $kb,\ bk\in I$.

2.43. Примеры. 1) Тривиальные идеалы: $O=\{0\}$ – *нулевой идеал*, $I=K$ – *единичный идеал*. Заметим, что всякий идеал содержит ноль, т.к. если $a\in I$, то $a-a=0\in I$.

2) *Главный идеал,* порождённый элементом $a\in K$:

$$(a)=\big\{ka\,\big|\ k\in K\big\}\,.$$

3) *Идеал, порождённый элементами* $a_1,a_2,\ldots,a_n\in K$:

$$\big(a_1,a_2,\ldots,a_n\big)=\big\{k_1a_1+k_2a_2+\ldots+k_na_n\,\big|\ k_1,k_2,\ldots,k_n\in K\big\}\,.$$

4) Пусть для любого натурального n запись nk обозначает сумму $\underbrace{k+k+\ldots+k}_{n}$, $k\in K$. Тогда идеалом будет множество

$$nK=\left\{nk\,\middle|\,k\in K\right\}.$$

Для колец (как и для групп) можно определить понятие фактор-кольца.

2.44. Определение. Пусть $I\subseteq K-$ некоторый идеал. Определим *отношение сравнимости элементов по идеалу* I:

$$a\equiv b\pmod I \Leftrightarrow a-b\in I.$$

2.45. Теорема. *1) Отношение сравнимости элементов кольца по идеалу является отношением эквивалентности.*

2) Класс эквивалентности любого элемента a по отношению $\equiv$ представим в виде $a+I$.

Доказательство. 1) Отношение $\equiv$ рефлексивно, т.к. $a-a=0\in I$. Отношение $\equiv$ симметрично, т.к. если $a\equiv b\pmod I$, то $a-b\in I$. Элемент $b-a=(-1)(a-b)$ будет принадлежать I согласно определению идеала. Следовательно, по определению $b\equiv a\pmod I$.

Отношение $\equiv$ транзитивно, т.к. если $a\equiv b\pmod I$, $b\equiv c\pmod I$, то $a-b\in I$, $b-c\in I$. Воспользовавшись определением идеала, получаем, что

$$(-1)(b-c)\in I \text{ и}$$

$$(a-b)-(-1)(b-c)=(a-b)+(b-c)=a-c\in I.$$

2) Следующие соотношения являются равносильными: $x\equiv a\pmod I$, $x-a\in I$, $x-a=u\in I$, $x=a+u$, $u\in I$, $x\in a+I$.

2.46. Определение. Классы эквивалентности по отношению $\equiv$ называются *классами вычетов по идеалу* I или *смежными классами по идеалу* I. Множество всех смежных классов по

данному идеалу называется *фактор-множеством* кольца K по идеалу I и обозначается K/I.

Определим на этом множестве операции:

$$(a+I)+(b+I)=(a+b)+I,$$

$$(a+I)\cdot(b+I)=ab+I,$$

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

В качестве единицы будем рассматривать класс $1+I$, а в качестве нуля – класс $0+I=I$.

2.47. Теорема. *Если K – коммутативно-ассоциативное кольцо с единицей и $I\subseteq K$ – его идеал, то фактор-множество K/I относительно определённых выше операций также является коммутативно-ассоциативным кольцом с единицей, которое называется фактор-кольцом кольца K по идеалу I.*

Для доказательства достаточно проверить все аксиомы кольца (оставляется в качестве упражнения).

2.48. Основной пример (кольцо вычетов). Пусть $m>1$ – некоторое натуральное число. Рассмотрим идеал $m\mathbb{Z}=\{ma, a\in\mathbb{Z}\}\subseteq\mathbb{Z}$ (см. пример 2.43.4).

Рассмотрим фактор-кольцо

$$\mathbb{Z}_m=\mathbb{Z}/m\mathbb{Z},$$

которое называется *кольцом вычетов по модулю m*. Очевидно, соотношение $a\equiv b(\mathrm{mod}\, m\mathbb{Z})$ выполняется тогда и только тогда, когда $a-b\in m\mathbb{Z}$ или $(a-b)\vdots m$.

Обозначение: $a\equiv b(\mathrm{mod}\, m)$.

2.49. Предложение (признаки сравнимости). *Для любых целых чисел a,b и целого $m>1$ следующие условия равносильны:*

1) $a\equiv b(\mathrm{mod}\, m)$;

2) $a=b+mt$ для подходящего целого t;

3) числа a и b имеют одинаковые остатки при делении на m.

Доказательство. 1) $\Leftrightarrow$ 2), т.к. равносильны условия

$$a \equiv b \pmod{m},\ (a-b) \vdots m,\ a-b=mt,\ a=b+mt.$$

2) $\Rightarrow$ 3). Если $a=b+mt$. Разделим b на m с остатком. Тогда $b=mq+r$ и $0 \le r < m$. Подставляя b в первое равенство, получаем $a=m(q+t)+r$, причём $0 \le r < m$.

2) $\Leftarrow$ 3). Если $a=mq_1+r$, $b=mq_2+r$, то $a=b+m(q_1-q_2)$ и $t=q_1-q_2$.

2.50. Следствие. *Класс вычетов по модулю m состоит из всех чисел, которые при делении на m имеют данный остаток.*

Наиболее удобным представлением классов вычетов является представление вида $r+m\mathbb{Z}$, где $0 \le r < m$. В этом случае в каждом классе вычетов в качестве представителя выбирается наименьшее неотрицательное число (*наименьший неотрицательный вычет*).

2.51. Следствие. *Кольцо вычетов по модулю m содержит ровно m элементов: $0+m\mathbb{Z}$, $1+m\mathbb{Z}$,..., $(m-1)+m\mathbb{Z}$.*

Если число m фиксировано, то классы вычетов для краткости обозначают $\overline{0},\overline{1},\overline{2},\ldots,\overline{m-1}$. Операции в кольце вычетов удобнее всего выполнять «по модулю m», т.е. после умножения или сложения нужно находить остаток от деления на m. Например, для $m=7$:

$$\overline{5}+\overline{4}=\overline{9}=\overline{2},\ \overline{5}\cdot\overline{4}=\overline{20}=\overline{6},\ -\overline{4}=\overline{3}.$$

§7. Отношение делимости в кольцах

Рассмотрим отношение делимости в произвольном (ассоциативном) кольце K:

$$\forall a,b \in K\ \left(a \vdots b \Leftrightarrow \exists q \in K\ (a=bq)\right).$$

Докажем простейшие свойства делимости в общем случае, действуя по аналогии со случаем целых чисел (см. свойства 1.2, 1.30).

2.52. Свойства. *Пусть K – ассоциативное кольцо с единицей. Для любых $a,b,c \in K$ выполняются следующие свойства:*

1) $a \vdots a$ (рефлексивность),

2) если $a \vdots b$, $b \vdots c$, то $a \vdots c$ (транзитивность),

3) если $a \vdots c$, $b \vdots c$, то $(a \pm b) \vdots c$,

4) если $a \vdots c$, то $ab \vdots c$.

И формулировка и доказательства этих свойств для общего случая и для случая целых чисел не отличаются.

В следующих двух свойствах участвуют *обратимые элементы*. Как известно, не все элементы кольца могут иметь обратный элемент, т.е. являются обратимыми. Например, в кольце целых чисел обратимыми являются только $+1$ и -1. Это предельный случай, т.к. в любом кольце элементы ± 1 обратимы. Другим предельным случаем является случай кольца, в котором все отличные от нуля элементы обратимы. В таком кольце отношение делимости вырождается, т.к. каждый элемент делится на любой ненулевой элемент.

Действительно, если элементы a, b, $b \neq 0$ принадлежат некоторому кольцу K и элемент b имеет обратный элемент b^{-1}, то $a \vdots b$, т.к. существует $q = b^{-1}a \in K$, для которого выполняется равенство

$$a = bq = b\left(b^{-1}a\right).$$

Обратимые элементы дают так называемые тривиальные делимости и тривиальные делители, т.е. делители таких типов, которые есть у любого элемента.

Множество обратимых элементов кольца K будет обозначаться как K_*.

2.53. Свойства. *Пусть K – коммутативное, ассоциативное кольцо с единицей. Для любых элементов a,b из K и любого обратимого элемента $\beta \in K_*$ выполняются следующие свойства:*

1) если $a \vdots b$, то $a \vdots \beta b$ и $\beta a \vdots b$ (делимость не зависит от обратимых сомножителей);

2) $0 \vdots a$, $a \vdots \beta$, $a \vdots \beta a$ (тривиальные делимости).

Для доказательства просто укажем частные в каждом случае. 1) Если $a = bq$, то $a = \beta b \cdot \left(\beta^{-1} q\right)$ и $\beta a = b \cdot (\beta q)$.

2) $0 = a \cdot 0$, $a = \beta \cdot \left(\beta^{-1} a\right)$, $a = \beta a \cdot \beta^{-1}$.

Для элемента a из K *тривиальными делителями* называются все элементы вида β, βa, где $\beta \in K_*$.

В силу свойств 1) и 2) многие понятия и результаты, связанные с делимостью, должны определяться с точностью до обратимого сомножителя. Для удобства дадим следующее

2.54. Определение. Элементы a, b кольца K называются *ассоциированными*, если существует такой обратимый элемент β, что $a = \beta b$.

Отношение ассоциированности обозначается так: $a \sim b$.

2.55. Теорема (свойства ассоциированных элементов). *Пусть K – коммутативное, ассоциативное кольцо с единицей. Для любых a, b, c из K выполняются следующие свойства:*

1) $a \sim a$;

2) если $a \sim b$, то $b \sim a$;

3) если $a \sim b$, $b \sim c$, то $a \sim c$;

4) если кольцо K не имеет делителей нуля, то соотношение $a \sim b$ выполняется тогда и только тогда, когда $a \vdots b$ и $b \vdots a$;

5) ассоциированные элементы имеют одинаковые делители.

Доказательство. 1) Следует из того, что $a = 1 \cdot a$.

2) Если $a = \beta b$ для некоторого обратимого элемента β, то $b = \beta^{-1} a$.

3) Если $a = \beta b$, $b = \gamma c$ для некоторых $\beta, \gamma \in K_*$, то $a = (\beta\gamma)c$, причём $\beta\gamma \in K_*$.

4) Так как $a = \beta b$, то $a \vdots b$. Так как $b = \beta^{-1} a$, то $b \vdots a$.

В обратную сторону. Если $a = 0$, то и $b = 0$ и тогда $a = 1 \cdot b$, $1 \in K_*$. Если $a \neq 0$, то из условия следует, что $a = bq_1$, $b = aq_2$, и тогда $a = aq_2q_1$. Пользуясь свойством отсутствия делителей нуля, сокращаем на $a \neq 0$ и получаем $1 = q_2q_1$. По определению, элементы q_1, q_2 обратимы, и так как $a = bq_1$, то $a \sim b$.

5) Действительно, если $a = \beta b$ и $a \vdots d$, то по свойству делимости 2.52.4) получаем, что $\beta^{-1} a = b \vdots d$, и наоборот.

§8. Поля

2.56. Определение. Коммутативное, ассоциативное кольцо $\langle P;\ +;\ \cdot \rangle$ с единицей, в котором $0 \neq 1$ и для каждого ненулевого элемента $a \in P$ существует обратный элемент a^{-1}, называется *полем*.

Для наглядности перечислим все

2.57. Аксиомы поля.

1) $(\forall a, b \in P)(a + b = b + a)$ – коммутативность сложения.

2) $(\forall a, b, c \in P)\Big(a + (b + c) = (a + b) + c\Big)$ –

ассоциативность сложения.

3) $(\forall a \in P)(a+0=a)$ – характеристическое свойство нуля.

4) $(\forall a \in P)(\exists b \in P)(a+b=0)$ – существование противоположного элемента.

5) $(\forall a,b \in P)(ab=ba)$ – коммутативность умножения.

6) $(\forall a,b,c \in P)\left(a(bc) =(ab)c\right)$ – ассоциативность умножения.

7) $(\forall a \in P)(a \cdot 1=a)$ – характеристическое свойство единицы.

8) $(\forall a \neq 0)(\exists b \in P)(ab=1)$ – существование обратного.

9) $(\forall a,b,c \in P)\left(a(b+c) =ab+ac\right)$ – дистрибутивность.

10) $0 \neq 1$.

Из аксиом следует, что всякое поле P образует относительно сложения коммутативную группу (*аддитивная группа поля*). Множество ненулевых элементов P^* относительно операции умножения также образует группу (*мультипликативная группа поля*).

Подполем поля $\langle P;\ +,\ \cdot \rangle$ называется непустое подмножество F, замкнутое относительно операций сложения и умножения и само являющееся полем. При этом поле P называется *расширением* поля F. Подполе поля $\langle P;\ +;\ \cdot \rangle$, отличное от P, называется его *собственным подполем*.

2.58. Теорема (критерий подполя). *Подмножество M поля P является его подполем тогда и только тогда, когда оно содержит хотя бы один ненулевой элемент, замкнуто относительно сложения, умножения, взятия противоположного и вместе с каждым ненулевым элементом содержит обратный к нему.*

Доказательство этого утверждения аналогично доказательству критерия подгруппы.

Заметим, что поле является кольцом, а значит, все свойства колец выполняются для любого поля. Ограничение $a \neq 0$ в аксиоме 8 связано с тем, что элемент 0 не имеет обратного. Ведь если, напротив, 0^{-1} существует, то, по определению обратного, $0 \cdot 0^{-1} = 1$. С другой стороны, по свойству колец 2.41.1) получим $0 \cdot 0^{-1} = 0$. Это противоречит аксиоме 10. По этой же причине обратный элемент всякого ненулевого элемента поля также не равен нулю.

Если $\langle P;\ +;\ \cdot \rangle$ – поле, то для любых его элементов a, b, $b \neq 0$, можно определить частное:

$$\frac{a}{b} = a \cdot b^{-1},\ b \neq 0.$$

Всюду в дальнейшем будет предполагаться, что знаменатель не равен нулю.

2.59. Теорема (простейшие свойства полей). *Пусть* $\langle P;\ +;\ \cdot \rangle$ *– некоторое поле. Тогда для любых его элементов* a, b, c *выполняются свойства:*

1) Если $ac = bc$ и $c \neq 0$, *то* $a = b$.

2) Если $ab = 0$, *то* $a = 0$ или $b = 0$ *(в поле нет делителей нуля).*

3) При условии $b \neq 0, d \neq 0$, *равенство* $\frac{a}{b} = \frac{c}{d}$ *равносильно равенству* $ad = bc$.

4) $\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd}$.

5) $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.

6) $\frac{a}{b} + \frac{(-a)}{b} = 0$ и $-\frac{a}{b} = \frac{-a}{b}$.

7) Если $a \neq 0$ и $b \neq 0$, *то* $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$.

8) $\frac{ac}{bc} = \frac{a}{b}$, *если* $b \neq 0$ и $c \neq 0$.

Доказательство. Так как P^* – это коммутативная группа относительно операции умножения, то свойство 1) – это свойство групп.

2) согласно свойствам колец (см. 2.41.6), равносильно свойству 1).

3) Пусть $\frac{a}{b} = \frac{c}{d}$, тогда $b \neq 0$, $d \neq 0$ и $ab^{-1} = cd^{-1}$. Домножаем это равенство на bd и преобразуем, пользуясь аксиомами поля:

$$\left(ab^{-1}\right)\cdot(bd) = \left(cd^{-1}\right)\cdot bd,$$

$$a\cdot\left(b^{-1}b\right)\cdot d = cd^{-1}\cdot bd = c\cdot\left(d^{-1}d\right)\cdot b,$$

$$a\cdot 1\cdot d = c\cdot 1\cdot b,$$

$$ad = cb.$$

Обратно, пусть $ad = cb$ и $b \neq 0$, $d \neq 0$. Тогда, умножив это равенство на $b^{-1}d^{-1}$, получаем:

$$ad\cdot b^{-1}d^{-1} = cb\cdot b^{-1}d^{-1},$$

$$a\cdot b^{-1} = c\cdot d^{-1}.$$

4) Так как $\frac{a}{b} = ab^{-1}$ и $\frac{c}{d} = cd^{-1}$, то

$$\frac{a}{b} \pm \frac{c}{d} = ab^{-1} \pm cd^{-1} = a\left(dd^{-1}\right)b^{-1} \pm c\left(bb^{-1}\right)d^{-1} =$$

$$= \left(ad \pm bc\right)\cdot b^{-1}d^{-1} = \left(ad \pm bc\right)\cdot\left(db\right)^{-1} = \frac{ad \pm bc}{bd}.$$

5) При $b \neq 0$ и $d \neq 0$ имеем

$$\frac{a}{b} \cdot \frac{c}{d} = ab^{-1} \cdot cd^{-1} = ac \cdot b^{-1}d^{-1} = ac \cdot \left(db\right)^{-1} = \frac{ac}{bd}.$$

6) При $b \neq 0$

$$\frac{a}{b} + \frac{(-a)}{b} = ab^{-1} + \left(-a\right)b^{-1} = \left(a - a\right)b^{-1} = 0b^{-1} = 0.$$

7) Если $a \neq 0$ и $b \neq 0$, то

$$\left(\frac{a}{b}\right)^{-1} = \left(ab^{-1}\right)^{-1} = \left(b^{-1}\right)^{-1} a^{-1} = ba^{-1} = \frac{b}{a}.$$

8) При $b \neq 0$ и $c \neq 0$

$$\frac{ac}{bc} = ac \cdot \left(bc\right)^{-1} = ac \cdot c^{-1}b^{-1} = ab^{-1} = \frac{a}{b}.$$

2.60. Примеры. Множества рациональных и действительных чисел относительно обычных операций сложения и умножения $\left\langle \mathbb{Q};\ +;\ \cdot \right\rangle$, $\left\langle \mathbb{R};\ +;\ \cdot \right\rangle$ являются полями, причём $\left\langle \mathbb{Q};\ +;\ \cdot \right\rangle$ является подполем поля $\left\langle \mathbb{R};\ +;\ \cdot \right\rangle$, т.к. $\mathbb{Q} \subset \mathbb{R}$. Между полями $\mathbb{Q}$ и $\mathbb{R}$ имеется бесконечное множество промежуточных полей F (таких, что $\mathbb{Q} \subset F \subset \mathbb{R}$). Например, полем будет множество $F = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$ с обычными операциями сложения и умножения чисел.

Для классификации полей используется понятие характеристики.

2.61. Определение. *Характеристикой поля* P называется такое наименьшее натуральное число p, что $p * 1 = 0$. Если такого p не существует, то говорят, что поле имеет характеристику 0.

Появление этого понятия связано с тем, что всякое поле содержит единицу и, следовательно, подполе, порождаемое этой единицей. При этом возможны два различных случая:

1) $n*1=0$ для некоторого натурального n;

2) $n*1\neq 0$ для любого натурального n.

2.62. Предложение. *Если натуральное число $p\neq 0$ является характеристикой поля P, то для любого элемента a из P выполняется равенство $p*a=0$. Если $0<n<p$, то $n*a\neq 0$ для любого ненулевого элемента a из P.*

Действительно, достаточно воспользоваться свойством кратных 2.12.e):

$$p*a=p*(1a)\overset{e)}{=}(p*1)a=0a=0.$$

Если, напротив, $n*a=0$ для некоторого $0<n<p$, то $0=n*a=n*(1a)\overset{e)}{=}(n*1)a$. В поле нет делителей нуля, $a\neq 0$, поэтому $n*1=0$, что противоречит определению p (тому, что оно наименьшее).

Для простоты элементы вида $n*1=\underbrace{1+..+1}_{n}$ обозначают просто как n:

$$n=\underbrace{1+..+1}_{n}.$$

Эти элементы – аналог целых чисел в произвольном поле. При помощи них можно более просто и более привычно записывать кратные:

$$n*a=\underbrace{a+..+a}_{n}=\underbrace{1a+..+1a}_{n}=\left(\underbrace{1+..+1}_{n}\right)a=na.$$

2.63. Следствие. *Характеристика поля – это аддитивный порядок множества ненулевых элементов поля.*

Можно пользоваться свойствами порядка 2.16, доказанными в §2.

2.64. Замечание. *Понятие характеристики и предложение 2.62 можно обобщить на случай (ассоциативных) колец с единицей и без делителей нуля.*

Действительно, если проанализировать 2.61 и 2.62, то можно заметить, что в них используется существование единицы, общие свойства колец (теорема 2.41, свойства кратных 2.12) и отсутствие делителей нуля. Поэтому в определении 2.61 и предложении 2.62 можно просто заменить поле на кольцо с единицей без делителей нуля.

Уточним понятие изоморфизма для случая полей. Для простоты обозначений операции в каждом поле будем обозначать одинаково: + и ·.

Поле $\langle P;\ +;\ \cdot \rangle$ называется *изоморфным* полю $\langle F;\ +;\ \cdot \rangle$, если существует взаимно однозначное отображение f множества P на множество F такое, что для любых $a,b \in P$ выполняются равенства:

$$f(a+b)=f(a)+f(b),\ f(a\cdot b)=f(a)\cdot f(b).$$

Изоморфизм полей обозначается, как обычно, $P \cong F$. Изоморфные поля можно считать копиями друг друга.

2.65. Основной пример (поле вычетов). Кольца вычетов $\mathbb{Z}_m$ в случае, когда m является простым числом, дают важнейшие для приложений примеры конечных полей.

2.66. Теорема. *Кольцо вычетов $\mathbb{Z}_m$ является полем тогда и только тогда, когда число m является простым.*

Доказательство. Пусть, напротив, кольцо $\mathbb{Z}_m$ является полем, но число m – составное:

$$m=m_1m_2,\ 1<m_1<m,\ 1<m_2<m.$$

В этом случае $\mathbb{Z}_m$ имеет делители нуля:

$$\overline{m_1}\cdot\overline{m_2}=\overline{m}=\overline{0},\quad \overline{m_1}\neq\overline{0},\ \overline{m_2}\neq\overline{0},$$

что невозможно для поля.

Обратно. Если m – простое число, то оно взаимно просто с любым числом $1\le r<m$. Составим для чисел m, r тождество Безу 1.22 (по алгоритму Евклида): $mu+rv=1$.

Тогда в кольце $\mathbb{Z}_m$ имеем равенство $\bar{r}\cdot\bar{v}=\bar{1}$, из которого следует, что элемент $\bar{r}$ имеет обратный элемент $\bar{v}$. После этого осталось заметить, что элементы вида $\bar{r}$, $1\le r<m$, исчерпывают все ненулевые элементы кольца $\mathbb{Z}_m$.

Задачи для самостоятельного решения

1. Пусть $GL_n(\mathbb{R})$ – множество невырожденных матриц размерности $n\times n$ с действительными коэффициентами. Докажите, что относительно умножения матриц это группа.

2. Вычислите в группе $GL_2(\mathbb{R})$:

а) $\begin{pmatrix}2 & 1\\ 3 & 2\end{pmatrix}\cdot\begin{pmatrix}-1 & 0\\ 1 & 2\end{pmatrix}$; б) $\begin{pmatrix}2 & 1\\ 3 & 1\end{pmatrix}^{-1}$;

в) $\begin{pmatrix}1 & 3\\ 0 & 2\end{pmatrix}^{4}$.

3. Найдите в группе $GL_2(\mathbb{R})$ порядок элемента:

а) $\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$; б) $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$;

в) $\begin{pmatrix}0 & 1\\ -1 & 1\end{pmatrix}$; г) $\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}$.

4. Найдите в группе $GL_2(\mathbb{R})$ три элемента бесконечного порядка.

5. Пусть $A=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$, $B=\begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix}$. Найдите порядки элементов A, B и AB.

6. В группе $GL_2(\mathbb{R})$ найдите все элементы:

а) порядка 2; б) порядка 3;

в) порядка 4.

7. Пусть $m>1$ – целое число, которое мы будем называть модулем. Докажите, что множество $m\mathbb{Z}=\{km \mid k\in\mathbb{Z}\}$ является идеалом в кольце целых чисел.

8. Найдите все классы вычетов кольца целых чисел $\mathbb{Z}$ по идеалу $m\mathbb{Z}$:

а) для $m=3$; б) для $m=4$;

в) для $m=5$; г) для произвольного m.

Сколько классов эквивалентности в общем случае?

9. Пусть $\mathbb{Z}_m$ обозначает фактор-кольцо кольца целых чисел по идеалу $m\mathbb{Z}$. Составьте таблицы сложения и умножения для случая:

а) $m=5$; б) $m=10$;

в) $m=7$; г) $m=9$.

10. Какой элемент называется обратимым? Какой элемент называется делителем нуля? Найдите все обратимые элементы и делители нуля в фактор-кольцах из предыдущего примера.

11. Найдите делители всех элементов кольца $\mathbb{Z}_{10}$. Какие из этих делителей являются нетривиальными?

12. Найдите все пары ассоциированных элементов кольца $\mathbb{Z}_{10}$.

13. Найдите в $\mathbb{Z}_{10}$ все тройки элементов, для которых не выполняется свойство сокращения: $ac=bc,\ a\neq b,\ c\neq 0$.

Определение. Числа вида $a+bi$, где $a,b\in\mathbb{Z}$, называются *целыми гауссовыми*. Множество всех гауссовых чисел обозначается $\mathbb{Z}[i]$.

14. Докажите, что $\mathbb{Z}[i]$ образует подкольцо поля комплексных чисел $\mathbb{C}$.

15. Вычислите в кольце $\mathbb{Z}[i]$:

а) $(1-3i)+(2+5i)$; б) $(1-3i)+(2+5i)$;

в) $(1-3i)(2+5i)$; г) $\dfrac{2+5i}{1-3i}$.

16. Докажите, что в $\mathbb{Z}[i]$:

а) $(7+4i)\vdots(3-2i)$; б) $(-1+8i)\vdots(2-3i)$;

в) $(5+15i)\vdots(1-3i)$; г) $(1+4i)\not\vdots(3-i)$.

Определение. Для всякого $z=a+bi\in\mathbb{Z}[i]$ определяется *сопряжённый элемент* $\bar{z}=a-bi\in\mathbb{Z}[i]$ и *норма* $N(z)=a^2+b^2\in\mathbb{Z}$.

Для любых z,u выполняются следующие свойства операции взятия сопряжённого: $\overline{z+u}=\bar{z}+\bar{u}$, $\overline{zu}=\bar{z}\cdot\bar{u}$.

17. Докажите основные свойства нормы для любых $z,u\in\mathbb{Z}[i]$:

а) $N(z)=z\cdot\bar{z}$; б) $N(z)=0\Leftrightarrow z=0$;

в) $N(zu)=N(z)N(u)$; г) если $z\vdots u$, то $N(z)\vdots N(u)$.

18. Найдите все обратимые элементы кольца $\mathbb{Z}[i]$.

19. Какие элементы будут ассоциированными в кольце $\mathbb{Z}[i]$? Как устроены тривиальные делители произвольного элемента $z\in\mathbb{Z}[i]$?

20. Используя свойства нормы и метод перебора, докажите, что:

а) являются простыми в кольце $\mathbb{Z}[i]$ числа 3 и $2+3i$;

б) не являются простыми числа 5 и $2i$.

21. Докажите в кольце $\mathbb{Z}[i]$ теорему о делении с остатком, взяв для чисел $z,u\in\mathbb{Z}[i]$, $u\neq 0$, в качестве неполного частного

ближайшее к числу $\frac{z}{u}$ на комплексной плоскости гауссово число h, а в качестве остатка – число $r = z - uh$. Для каких чисел неполное частное и остаток определяются неоднозначно? Сколько неполных частных и остатков может быть у пары чисел $z, u \in \mathbb{Z}[i],\ u \neq 0$?

22. Разделите с остатком в кольце $\mathbb{Z}[i]$:

а) $(4+3i)$ на $(2-i)$;

б) $(14-5i)$ на $(1+2i)$;

в) $(13+3i)$ на 2;

г) $(4+3i)$ на $(1+3i)$.

23. Найдите *НОД* целых гауссовых чисел:

а) $(18+4i)$ и $(7-i)$;

б) $(27-4i)$ и $(11+8i)$;

в) $(48+14i)$ и $(2-3i)$;

г) $(77-43i)$ и $(4+5i)$.

24. Найдите все простые гауссовы числа среди простых целых чисел от 2 до 30.

25. Докажите, что любое простое гауссово число является делителем ровно одного натурального простого числа.

26. Докажите, что являются простыми гауссовыми:

а) все четыре числа вида $\pm 1 \pm i$;

б) все натуральные простые числа вида $p = 4k + 3$;

в) все делители вида $a + bi$ натуральных простых чисел $p = a^2 + b^2$ вида $4k + 1$.

27. Докажите, что предыдущая задача даёт все простые гауссовы числа.

28. Найдите каноническое разложение гауссовых чисел:

а) $3 + 24i$;

б) $-28 + 231i$;

в) $-16 - 2i$;

г) $34 + 19i$.

29. Докажите, что множество ненулевых элементов некоторого поля относительно операции умножения образует группу.

30. Воспользовавшись следствием 2.32, найдите в мультипликативной группе поля вычетов $\mathbb{Z}_{31}$ элементы порядков $5, 6, 15, 30$.

31. Воспользовавшись расширенным алгоритмом Евклида, найдите:

а) в поле вычетов $\mathbb{Z}_{71}$ обратные элементы для $\overline{4}, \overline{33}, \overline{51}$;

б) в поле вычетов $\mathbb{Z}_{101}$ обратные элементы для $\overline{7}, \overline{31}, \overline{84}$.

ГЛАВА 3. ОБЩАЯ ТЕОРИЯ МНОГОЧЛЕНОВ

§1. Кольцо многочленов от одной переменной

Везде в данном разделе будет предполагаться, что K – коммутативное, ассоциативное кольцо с единицей без делителей нуля. Типичным примером такого кольца является кольцо целых чисел.

3.1. Определение. *Многочленом* (или *полиномом*) от x с коэффициентами из K называется выражение вида

$$f(x)=a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 , \qquad (1)$$

где n – неотрицательное целое число и $a_n, a_{n-1}, \ldots, a_1, a_0$ – элементы кольца K. Элемент a_i называется *коэффициентом многочлена* (1) *при* x^i. Для удобства обозначений будем считать, что для всех $i > n$ коэффициенты $a_i = 0$. Выражение $a_i x^i$ называется *одночленом.*

Многочлены $f(x)$ и $g(x)$ называются *равными,* если для любого $i \geq 0$ коэффициенты многочленов при x^i равны. Многочлен называется *нулевым,* если все его коэффициенты равны нулю.

3.2. Определение. Пусть даны многочлены

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

$$g(x)=b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0 \text{ и } k=\max(n,m).$$

Суммой многочленов $f(x)$ и $g(x)$ называется многочлен

$$f(x)+g(x)=$$

$$=(a_k+b_k)x^k + (a_{k-1}+b_{k-1})x^{k-1} + \ldots + (a_1+b_1)x + (a_0+b_0).$$

Чтобы вычислить сумму многочленов, достаточно записать два многочлена в виде суммы и привести подобные члены.

Произведением многочленов $f(x)$ *и* $g(x)$ называется многочлен, который равен сумме всевозможных произведений одночленов из $f(x)$ *и* $g(x)$:

$$f(x)g(x)=c_{n+m}x^{n+m}+c_{n+m-1}x^{n+m-1}+\ldots+c_1x+c_0,$$

где $c_i=a_0b_i+a_1b_{i-1}+a_2b_{i-2}+\ldots+a_{i-1}b_1+a_ib_0$, $0\le i\le n+m$.

3.3. Замечание. Запись вида (1) называется *стандартной* или *канонической* формой записи многочлена. Обычно при записи многочлена используются следующие соглашения.

1) Одночлены вида $0x^i$ *не записываются.*

2) Одночлены вида $1x^i$ *записываются как* x^i.

3) Одночлены вида $(-a_i)x^i$ *записываются как* $-a_ix^i$.

Если переменная x зафиксирована, то вместо $f(x)$ можно использовать сокращённую запись f.

3.4. Пример. Найти сумму и произведение многочленов:

$$f(x)=3x^3+2x^2-x+3,\ g(x)=x^2-3x-1.$$

Действуем согласно определению.

$$f(x)+g(x)=\left(3x^3+2x^2-x+3\right)+\left(x^2-3x-1\right)=$$

$$=3x^3+(2+1)x^2+(-1-3)x+(3-1)=3x^3+3x^2-4x+2.$$

$$f(x)g(x)=\left(3x^3+2x^2-x+3\right)\left(x^2-3x-1\right)=$$

$$=3x^5+2x^4-x^3+3x^2-9x^4-6x^3+3x^2-9x-$$

$$-3x^3-2x^2+x-3=3x^5-7x^4-10x^3+4x^2-8x-3.$$

Непосредственной проверкой доказывается

3.5. Теорема. *Многочлены с коэффициентами из* K *образуют коммутативное, ассоциативное кольцо с единицей* $K[x]$.

Доказательство состоит в проверке всех аксиом.

В дальнейшем под многочленом подразумевается любой элемент кольца $K[x]$. Он не обязательно записан в стандартной форме. Однако если раскрыть скобки и привести подобные члены, то стандартную форму можно получить.

3.6. Определение. Если дан многочлен $f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$ и $a_n\neq 0$, то число n называется его *степенью* и обозначается $\deg(f)$ или $cm(f)$. Коэффициент a_n в этом случае называется *старшим коэффициентом*.

Таким образом, степень многочлена – это наибольшая из степеней его ненулевых одночленов. *Степень нулевого многочлена не определяется.*

3.7. Теорема (свойства степени). *1) Степень суммы многочленов не превосходит максимальной степени слагаемых, т.е. если* $f, g\neq 0$, $f+g\neq 0$, *то*

$$cm(f+g)\leq \max\big(cm(f),cm(g)\big).$$

2) Степень произведения многочленов равна сумме степеней сомножителей, т.е. если $f, g\neq 0$, *то*

$$cm(fg)=cm(f)+cm(g).$$

Доказательство. 1) Следует из определения суммы.

2) Пусть

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0,\ a_n\neq 0,$$

$$g(x)=b_mx^m+b_{m-1}x^{m-1}+\ldots+b_1x+b_0,\ b_m\neq 0,$$

тогда

$$f(x)g(x)=a_nb_mx^{n+m}+(a_nb_{m-1}+a_{n-1}b_m)x^{n+m-1}+\ldots+a_0b_0.$$

Так как K не содержит делителей нуля, то $a_nb_m\neq 0$ и

$$cm(fg) = n + m = cm(f) + cm(g).$$

3.8. Следствие. *Если кольцо K не имеет делителей нуля, то кольцо $K[x]$ также не имеет делителей нуля.*

Доказательство. Из условия $a_n b_m \neq 0$ следует, что $f(x)g(x) \neq 0$.

Для уточнения свойств делимости нужно выяснить, какие многочлены являются обратимыми.

3.9. Теорема (об обратимых элементах кольца многочленов). *Многочлен $f(x) \in K[x]$ обратим тогда и только тогда, когда он является многочленом нулевой степени и обратим в кольце K, т.е. $f(x) = a_0 \in K_*$.*

Доказательство. Пусть некоторый ненулевой многочлен $f(x)$ имеет обратный элемент, т.е. существует $g(x) \in K[x]$, $g(x) \neq 0$ такой, что $f(x)g(x) = 1$. Вычисляя степень правой и левой частей этого равенства и применяя свойство степени, получаем

$$cm(fg) = cm(f) + cm(g) = 0.$$

Из этого следует, что $cm(f) = cm(g) = 0$, т.е. $f, g \in K$. Причём по условию они обратимы.

В обратную сторону теорема очевидна.

Используя эту теорему, можно уточнить свойства делимости 1)–6) для кольца многочленов. Кроме того, можно доказать аналог свойства делимости 7).

3.10. Свойство делимости. *7) Если $f \neq 0$ и $f \vdots g$, то $cm(f) \geq cm(g)$.*

Доказательство. По условию $f(x)$ делится на $g(x)$, поэтому существует такой многочлен $h(x)$ из кольца $K[x]$, что

$$f(x) = g(x)h(x).$$

Так как $f \neq 0$, то $g \neq 0$ и $h \neq 0$. Вычислим степень обеих частей равенства и применим свойство степени:

$$cm(f) = cm(gh) = cm(g) + cm(h) \geq cm(g).$$

Что и требовалось доказать.

3.11. Пример. Найти действительные числа a, b, для которых выполняется соотношение

$$\left(x^2 + ax + b\right) \vdots (x + 2).$$

Чтобы данное соотношение выполнялось, должен существовать такой многочлен $h(x) \in \mathbb{R}[x]$, что

$$\left(x^2 + ax + b\right) = (x + 2) \cdot h(x).$$

Согласно свойствам степени, $cm\left(h(x)\right) = 1$. Воспользуемся так называемым *методом неопределённых коэффициентов* и будем искать $h(x)$ в стандартной форме с неопределёнными коэффициентами:

$$h(x) = cx + d.$$

Подставляем $h(x)$ в равенство и приводим правую часть к стандартной форме:

$$x^2 + ax + b = (x + 2)(cx + d) = cx^2 + (2c + d)x + 2d.$$

Согласно определению равенства многочленов, коэффициенты стандартной формы при одинаковых степенях x в левой и правой частях должны совпадать. Приравниваем их и находим a, b.

$$\begin{cases} 1 = c, \\ a = 2c + d, \\ b = 2d; \end{cases} \Leftrightarrow \begin{cases} a = 2 + d, \\ b = 2d; \end{cases} \quad d \text{ – свободная переменная.}$$

Она может принимать любые значения. Данная задача имеет бесконечно много решений.

§2. Многочлены как функции

Если вместо переменной x в многочлен подставить некоторый элемент $c \in K$ и произвести вычисления, то получится элемент кольца K. Ввиду этого многочлены можно рассматривать как функции из K в K и использовать для их изучения приёмы теории функций.

3.12. Определение. Пусть дан некоторый многочлен $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$. *Значением многочлена* $f(x)$ в точке $c \in K$ называется элемент

$$f(c) = a_n c^n + a_{n-1}c^{n-1} + \ldots + a_1 c + a_0 \in K.$$

Если $f(c) = 0$, то c называется *корнем* многочлена $f(x)$.

Нахождение корней – одна из основных задач теории многочленов. Исходной для неё является задача решения уравнений вида $f(x) = g(x)$ или $f(x) = c$, однако если все слагаемые перенести в левую часть, то уравнения приобретут более простой вид $F(x) = 0$. В левой части уравнения стоит многочлен $F(x)$, и задача нахождения всех решений этого уравнения равносильна задаче нахождения всех корней многочлена.

3.13. Теорема (Безу). *Для любого многочлена* $f(x)$ *из кольца* $K[x]$ *и элемента* $c \in K$ *существуют и единственные многочлен* $h(x) \in K[x]$ *и элемент* $r \in K$ *такие, что*

$$f(x) = (x - c)h(x) + r. \qquad (2)$$

Доказательство. Если $f(x) \in K$, то $h(x) = 0$, $r = f(x)$ и доказательство закончено. Пусть $cm(f) = n \geq 1$, тогда

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0,\ a_n \neq 0.$$

Согласно свойству степеней, $cm(h) = n - 1$. Будем искать многочлен $h(x)$ методом неопределённых коэффициентов.

$$h(x)=b_{n-1}x^{n-1}+b_{n-2}x^{n-2}+\ldots+b_1x+b_0,$$

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0=$$

$$=(x-c)\left(b_{n-1}x^{n-1}+b_{n-2}x^{n-2}+\ldots+b_1x+b_0\right)+r=$$

$$=b_{n-1}x^n+(b_{n-2}-cb_{n-1})x^{n-1}+(b_{n-3}-cb_{n-2})x^{n-2}+\ldots$$

$$\ldots+(b_0-cb_1)x+(r-cb_0).$$

Приравниваем коэффициенты при одинаковых степенях x и выражаем неизвестные коэффициенты b_i и r.

$$\begin{cases} a_n=b_{n-1}, \\ a_{n-1}=b_{n-2}-cb_{n-1}, \\ a_{n-2}=b_{n-3}-cb_{n-2}, \\ \ldots \\ a_1=b_0-cb_1, \\ a_0=r-cb_0; \end{cases} \Leftrightarrow \begin{cases} b_{n-1}=a_n, \\ b_{n-2}=a_{n-1}+cb_{n-1}, \\ b_{n-3}=a_{n-2}+cb_{n-2}, \\ \ldots \\ b_0=a_1+cb_1, \\ r=a_0+cb_0. \end{cases} \qquad (3)$$

Полученная система легко решается сверху вниз. Из первого уравнения находим b_{n-1}, подставляем его значение во второе уравнение и находим b_{n-2}, подставляем полученное значение b_{n-2} в третье уравнение и находим b_{n-3}, и так до тех пор, пока не будут найдены все коэффициенты b_i и r.

Так как решение системы находится однозначно, то многочлен $h(x)$ из $K[x]$ и элемент r из K, удовлетворяющие условию теоремы, существуют и единственны.

3.14. Следствия. *1)* $r=f(c)$.

2) Элемент $c\in K$ *является корнем многочлена* $f(x)$ *тогда и только тогда, когда* $f(x)\vdots(x-c)$.

Доказательство. 1) Воспользуемся тем, что многочлен задаёт функцию, и подставим $c\in K$ в равенство (2):

$$f(c)=(c-c)\cdot h(c)+r=r.$$

2) Если $f(c)=0$, то

$$f(x)=(x-c)\cdot h(x)+f(c)=(x-c)\cdot h(x)$$

и, следовательно, $f(x)\vdots(x-c)$. Если $f(x)\vdots(x-c)$, то $f(x)=(x-c)\cdot h(x)$, и если подставить элемент c в это равенство, то

$$f(c)=(c-c)\cdot h(c)=0.$$

3.15. Схема Горнера. При решении системы (3) каждый коэффициент b_i, начиная с b_{n-2}, вычисляется по предыдущему коэффициенту по одной и той же схеме, которая называется *схемой Горнера*. Вычисления можно компактно записывать в таблицу. Поясним это на примере ниже.

Схема Горнера, фактически, позволяет делить с остатком произвольный многочлен на многочлен вида $(x-c)$. Многочлен $h(x)$ при этом является неполным частным, а r – остатком.

При помощи схемы Горнера можно:

а) вычислять значение многочлена,

б) проверять делимость на многочлены первой степени.

3.16. Пример. Вычислить значение многочлена $f(x)=2x^4-5x^2-4x+1$ при $c=2$.

Запишем все коэффициенты $f(x)$ в таблицу, как показано ниже. При этом необходимо отметить, что в вычислениях участвуют все коэффициенты, включая те, которые равны нулю.

	2	0	–5	–4	1
$c=2$	2	4	3	2	5

Во вторую строку будем вписывать коэффициенты b_i по мере их вычисления. Так как $b_3=a_4=2$, то число из первой клетки просто переносим вниз. Далее вычисления выполняются по принципу $b_{i-1}=cb_i+a_i$, т.е. чтобы заполнить некоторую клетку второй строки, нужно взять число из клетки слева (там

значение предшествующего коэффициента), умножить его на $c=2$ и добавить число из клетки выше (там соответствующее значение a_i). В последней клетке таблицы будет находиться r.

$$2\cdot 2+0=4,\ 2\cdot 4-5=3,\ 2\cdot 3-4=2,\ 2\cdot 2+1=5.$$

Важно правильно расшифровать результат, записанный в таблице. В верхней строке записаны коэффициенты многочлена $f(x)$, в нижней – сначала коэффициенты многочлена $h(x)$, а затем – элемент r. Результат можно записать так:

$$2x^4-5x^2-4x+1=(x-2)\left(2x^3+4x^2+3x+2\right)+5.$$

Если в правой части равенства раскрыть скобки и привести подобные члены, то получится многочлен из левой части равенства (это доказано в теореме Безу).

3.17. Теорема (о количестве корней). *Если кольцо K не содержит делителей нуля, то всякий ненулевой многочлен степени n в кольце $K[x]$ имеет не более n различных корней.*

Доказательство. Индукция по степени n. Если $n=0$, то многочлен $f(x)=a\in K,\ a\neq 0$, имеет 0 корней и, следовательно, утверждение теоремы выполняется.

Пусть для некоторого $n=k$ утверждение теоремы выполняется. Докажем, что оно верно также для произвольного многочлена $f(x)$ степени $k+1$.

Если многочлен не имеет корней, то их количество равно $0\le k+1$ и доказывать нечего. Пусть $f(x)$ имеет хотя бы один корень $c\in K$. Тогда по теореме Безу многочлен делится на $(x-c)$ и, следовательно,

$$f(x)=(x-c)h(x).$$

Докажем вспомогательное утверждение: *элемент $d\neq c$ является корнем $f(x)$ тогда и только тогда, когда d – корень многочлена $h(x)$.*

Действительно, если $f(d)=0$, то $(d-c)h(d)=0$. Так как $d-c\neq 0$, то ввиду отсутствия делителей нуля $h(d)=0$. Обратно, если $h(d)=0$, то $f(d)=(d-c)h(d)=(d-c)\cdot 0=0$.

В результате получилось, что корнями $f(x)$ будут все корни многочлена $h(x)$ и элемент c. По предположению многочлен $h(x)$ имеет $\leq k$ корней. Следовательно, многочлен $f(x)$ будет иметь $\leq k+1$ корней. Теорема доказана.

3.18. Следствие. *Если многочлен вида*

$$f(x)=a_n x^n+a_{n-1}x^{n-1}+\ldots+a_1 x+a_0$$

имеет более чем n корней, то он равен нулю.

Действительно, если $a_n\neq 0$, то получится противоречие с теоремой. Поэтому $a_n=0$. Аналогично доказываем, что

$$a_{n-1}=0,\ a_{n-2}=0,\ \ldots,\ a_1=0,\ a_0=0.$$

3.19. Следствие. *Всякий ненулевой многочлен степени, не превосходящей n, однозначно определяется своими значениями в $(n+1)$ точке.*

Доказательство. Предположим, что есть два многочлена:

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

$$g(x)=b_n x^n+b_{n-1}x^{n-1}+\ldots+b_1 x+b_0,$$

и попарно различные элементы $c_1,c_2,\ldots,c_n,c_{n+1}\in K$ такие, что $f(c_i)=g(c_i)$ для любого $1\leq i\leq n+1$.

Рассмотрим многочлен $h(x)=f(x)-g(x)$. Степень его не превосходит n, а элементы $c_1,c_2,\ldots,c_n,c_{n+1}$ будут его корнями, т.к.

$$h(c_i)=f(c_i)-g(c_i)=0.$$

Согласно следствию 3.18, $h(x)=f(x)-g(x)=0$ и поэтому $f(x)=g(x)$.

Кроме обычного равенства многочленов как выражений, можно рассматривать равенство многочленов как функций. Возникает вопрос: как связаны эти понятия?

3.20. Определение. Говорят, что многочлены $f(x), g(x)\in K$ *функционально равны*, если для любого элемента $c\in K$ выполняется равенство $f(c)=g(c)$.

Обозначение: $f(x)\equiv g(x)$.

3.21. Теорема (о равносильности алгебраического и функционального равенства). *Если K – бесконечное кольцо без делителей нуля, то многочлены над K равны тогда и только тогда, когда они функционально равны.*

Доказательство. В прямую сторону теорема очевидна, т.к. если многочлены равны, то и их соответствующие значения будут равными.

Докажем теорему в обратную сторону. Пусть $f(x)\equiv g(x)$ и степени этих многочленов не превосходят некоторого n. Так как K – бесконечное кольцо, то в нём можно выбрать $(n+1)$ попарно различных элементов $c_1, c_2, \ldots, c_n, c_{n+1}\in K$. По условию $f(c_i)=g(c_i)$ для любого $1\le i\le n+1$. Так как степень этих многочленов не превосходит n, то по следствию 3.19 $f(x)=g(x)$.

§3. Многочлены над полем

Перейдём к рассмотрению основного случая, когда $K=P$ является полем. Все ненулевые элементы поля являются обратимыми. По теореме 3.9 об обратимых элементах они дадут все обратимые элементы в кольце $P[x]$.

3.22. Теорема (о делении с остатком). *Для любого многочлена $f(x)$ и любого ненулевого многочлена $g(x)$ из*

кольца $P[x]$ *существуют такие единственные многочлены* $h(x)$ *и* $r(x)$ *из* $P[x]$, *что*

$$f(x)=g(x)h(x)+r(x) \text{ и}$$

либо $r=0$, *либо* $cm(r)<cm(g)$.

Доказательство. Существование.

Если $f=0$, то $f=g\cdot 0+0$ и $h=0,\ r=0$.

Если $f\neq 0,\ cm(f)<cm(g)$, то $f=g\cdot 0+f$ и $h=0,\ r=f$.

Пусть $f\neq 0,\ cm(f)=n\geq cm(g)=m$. Доказательство в этом случае проведём индукцией по степени n. Если $n=0$, то $m=0$ и данные многочлены просто элементы поля P, причём g обратим. В этом случае $f=g\cdot\left(g^{-1}f\right)+0$, т.е. $h=g^{-1}f,\ r=0$.

Предположим, что для всех многочленов степени меньше некоторого n теорема выполняется. Докажем её для многочлена $f(x)$ степени n.

Рассмотрим данные многочлены в стандартной форме:

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0,$$

$$g(x)=b_mx^m+b_{m-1}x^{m-1}+\ldots+b_1x+b_0,\ b_m\neq 0.$$

Вычтем из $f(x)$ многочлен $g(x)$, умноженный на такой сомножитель, чтобы старшие коэффициенты сократились и степень разности уменьшилась.

$$A(x)=f(x)-\frac{a_n}{b_m}\cdot x^{n-m}g(x).$$

Степень многочлена A строго меньше n, поэтому по предположению существуют такие $h_1(x), r_1(x)$, что $A(x)=g(x)h_1(x)+r_1(x)$, причём либо $r_1=0$, либо $cm(r_1)<cm(g)$. Подставляем этот результат в предыдущее равенство и получаем:

$$f(x)-\frac{a_n}{b_m}\cdot x^{n-m}g(x)=g(x)h_1(x)+r_1(x),$$

$$f(x)=g(x)\left(\frac{a_n}{b_m}x^{n-m}+h_1(x)\right)+r_1(x).$$

В результате $h(x)=\left(\frac{a_n}{b_m}x^{n-m}+h_1(x)\right)$, $r(x)=r_1(x)$.

Единственность. Пусть

$$f(x)=g(x)h_1(x)+r_1(x)=g(x)h_2(x)+r_2(x)$$

и для $i=1,2$ либо $r_i=0$, либо $cm(r_i)<cm(g)$. Преобразовав равенство, получаем

$$g(x)\big(h_1(x)-h_2(x)\big)=r_2(x)-r_1(x).$$

Если $h_1(x)-h_2(x)\neq 0$, то $r_2(x)-r_1(x)\neq 0$. Оценим степень левой и правой части полученного равенства.

$$cm\big(r_2(x)-r_1(x)\big)<cm(g),$$

$$cm\big(g(x)\big(h_1(x)-h_2(x)\big)\big)=$$

$$=cm\big(g(x)\big)+cm\big(h_1(x)-h_2(x)\big)\geq cm(g).$$

Полученное противоречие говорит о том, что данный случай невозможен.

Если $h_1(x)-h_2(x)=0$, то $r_2(x)-r_1(x)=0$ и

$$r_2(x)=r_1(x),\ h_1(x)=h_2(x).$$

Теорема полностью доказана.

Теорема о делении с остатком является одним из основных инструментов исследования в теории многочленов.

3.23. Определение. Пусть даны многочлены f и g из кольца $K[x]$, причём $g\neq 0$. *Разделить с остатком многочлен*

$f(x)$ *на многочлен* $g(x)$ – значит найти такие многочлены $h, r \in K[x]$, что

$$f(x) = g(x)h(x) + r(x)$$

и либо $r = 0$, либо $cm(r) < cm(g)$.

3.24. Следствие. *Пусть* f *и* g *– два многочлена над некоторым полем* P *и* $g \neq 0$. *Многочлен* f *делится на многочлен* g *тогда и только тогда, когда остаток от деления* f *на* g *равен нулю.*

Доказательство. Если $f \vdots g$, то $f = gh = gh + 0$ и в силу единственности частного и остатка частное равно h, а остаток равен 0.

Если остаток от деления f на g равен нулю, то $f = gh + 0$ и $f \vdots g$ по определению.

Единственность частного и остатка позволяет решать некоторые задачи методом подбора, ведь если $h(x), r(x)$, удовлетворяющие условиям теоремы, каким-либо образом найдены, то поиски можно прекратить, т.к. других частного и остатка нет.

3.25. Пример. Разделить с остатком многочлен $f(x) = \left(x^2+1\right)^{331} - 7x^5 + 3x - 31$ на $\left(x^2+1\right)^3$.

Заметим, что

$$f(x) = \left(x^2+1\right)^3 \left(x^2+1\right)^{328} - 7x^5 + 3x - 31 \text{ и}$$

$$cm\left(-7x^5 + 3x - 31\right) = 5 < cm\left(\left(x^2+1\right)^3\right) = 6.$$

По теореме о делении с остатком частное равно $\left(x^2+1\right)^{328}$, а остаток – $\left(-7x^5 + 3x - 31\right)$.

Из доказательства теоремы о делении с остатком извлекается алгоритм деления многочленов «в столбик». Он применяется, если многочлены отличны от нуля и $cm(f) \geq cm(g)$.

Чтобы найти частное и остаток, нужно из многочлена $f(x)$ вычитать многочлен $g(x)$, умноженный на такие одночлены, чтобы степень разности понижалась. Это делается до тех пор, пока степень разности не станет строго меньше степени делителя $g(x)$ или не получится ноль.

3.26. Пример. Разделить с остатком многочлен $2x^5+4x^4+7x^3+2x^2+3x+1$ на многочлен $2x^3+x-1$.

Оформим решение в виде деления «столбиком».

$$\begin{array}{r|l} 2x^5+4x^4+7x^3+2x^2+3x+1 & \underline{2x^3+x-1} \\ \underline{-\,2x^5+x^3-x^2} & x^2+2x+3 \\ 4x^4+6x^3+3x^2+3x+1 & \\ \underline{-\,4x^4+2x^2-2x} & \\ 6x^3+x^2+5x+1 & \\ \underline{-\,6x^3+3x-3} & \\ x^2+2x+4 & \end{array}$$

Разность, полученная на третьем шаге, имеет степень, меньшую степени делителя. Поэтому деление закончено и результат можно записать в виде равенства

$$2x^5+4x^4+7x^3+2x^2+3x+1 = \left(2x^3+x-1\right)\left(x^2+2x+3\right)+\left(x^2+2x+4\right).$$

По поводу особенностей отношения делимости в кольце многочленов можно сделать следующие

3.27. Замечания. *1) Обратимыми элементами являются ненулевые многочлены степени 0*, т.е. ненулевые элементы поля P.

2) Тривиальными делителями произвольного ненулевого многочлена $f(x)$ *являются многочлены вида* a *и* $af(x)$, *где* a – *ненулевой элемент поля* P. Степень тривиальных делителей первого вида равна 0; степень тривиальных делителей второго вида совпадает со степенью исходного многочлена.

3) Если $d(x)$ – *нетривиальный делитель произвольного ненулевого многочлена* $f(x)$, *то* $0 < cm(d) < cm(f)$.

4) Ассоциированными являются многочлены, которые отличаются постоянным множителем $a \in P$, $a \neq 0$ *:*

$$f(x) \sim af(x).$$

5) Ассоциированные многочлены имеют одинаковое множество делителей (см. свойства 2.55) и с точки зрения делимости ведут себя одинаково. Ввиду этого некоторые понятия определяются с точностью до сомножителей из P.

Таковым является, например, наибольший общий делитель. Для определённости, среди всех наибольших общих делителей некоторой пары многочленов можно выделить наибольший общий делитель со старшим коэффициентом, равным единице, и обозначить его *НОД*.

3.28. Определение. Ненулевой многочлен называется *нормированным*, если его старший коэффициент равен 1. В качестве $НОД(f, g)$ будем обозначать нормированный наибольший общий делитель многочленов f, g. Если многочлен разделить на его старший коэффициент, то получится нормированный многочлен, ассоциированный с данным многочленом.

Перечислим кратко основные свойства, связанные с делимостью. Они доказываются при помощи теоремы о делении с остатком. Доказательства для случая многочленов аналогичны доказательствам для случая целых чисел (см. гл. 1).

3.29. Теорема (Евклид). *НОД любых двух не равных одновременно нулю многочленов* $f(x)$ *и* $g(x)$ *в кольце* $P[x]$

существует. Если $f(x)$ *не делится на* $g(x)$, *то НОД*(f,g) *ассоциирован с последним ненулевым остатком в алгоритме Евклида.*

3.30. Теорема (тождество Безу). *Для любых двух не равных одновременно нулю многочленов* $f(x)$ *и* $g(x)$ *в кольце* $P[x]$ *существуют такие многочлены* $u(x), v(x)$, *что*

$$f(x)u(x)+g(x)v(x)=НОД(f,g).$$

Эти многочлены могут быть найдены при помощи рекуррентных соотношений расширенного алгоритма Евклида с одним следующим существенным отличием.

Пусть последний ненулевой остаток в алгоритме Евклида равен $r_n(x)$, а его старший коэффициент равен a. *НОД* получается из этого остатка делением на a. Рекуррентные соотношения дадут равенство

$$f(x)u_n(x)+g(x)v_n(x)=r_n(x).$$

После этого делим равенство почленно на a и получаем тождество Безу:

$$f(x)\left(\frac{u_n(x)}{a}\right)+g(x)\left(\frac{v_n(x)}{a}\right)=\frac{r_n(x)}{a}=НОД(f,g).$$

3.31. Теорема (признак взаимной простоты). *Многочлены* $f(x)$ *и* $g(x)$ *взаимно просты тогда и только тогда, когда существуют такие* $u(x), v(x)\in P[x]$, *что*

$$f(x)u(x)+g(x)v(x)=1.$$

3.32. Свойства делимости. *1) Если произведение многочленов* $f(x)g(x)$ *делится на некоторый многочлен* $h(x)$ *и* $h(x)$ *взаимно прост с одним из сомножителей, то второй сомножитель делится на* $h(x)$.

2) Если многочлен $f(x)$ делится на многочлены $g(x)$ и $h(x)$, которые взаимно просты друг с другом, то он делится на их произведение.

Некоторые утверждения теории делимости, пользуясь спецификой многочленов, можно усилить.

3.33. Следствие (модифицированное тождество Безу). *Если $f(x), g(x)$ – ненулевые многочлены, которые не делятся друг на друга, то существуют такие многочлены $u(x), v(x)$, что*

$$f(x)u(x)+g(x)v(x)=НОД\big(f,g\big),$$

причём $cm(u)<cm(g)$, $cm(v)<cm(f)$.

Доказательство. Пусть $НОД\big(f,g\big)=d$. По теореме Безу существуют такие многочлены u_0, v_0, что $fu_0+gv_0=d$. Пусть u – это остаток от деления u_0 на g:

$$u_0=gh+u\ .$$

Заметим, что $u\neq 0$, т.к. если $u=0$, то u_0 делится на g, $fu_0+gv_0=d$ делится на g и, следовательно, f делится на g. Это противоречит условию. По теореме о делении с остатком $cm(u)<cm(g)$, и одно из требуемых неравенств выполняется. Подставим полученное равенство в тождество Безу:

$$d=fu_0+gv_0=f\big(gh+u\big)+gv_0=fu+g\big(fh+v_0\big)\ .$$

Положим $v=fh+v_0$ и попытаемся оценить степень gv.

$$cm\big(gv\big)=cm\big(d-fu\big)\le cm\big(f\big)+cm\big(u\big)<cm\big(f\big)+cm\big(g\big),$$

т.к. $cm\big(u\big)<cm\big(g\big)$.

С другой стороны, $cm\big(gv\big)=cm\big(g\big)+cm\big(v\big)$. Поэтому, $\underline{cm\big(g\big)}+cm\big(v\big)<cm\big(f\big)+\underline{cm\big(g\big)}$ и, следовательно, $cm\big(v\big)<cm\big(f\big)$.

Так как степени многочленов u, v ограничены, то их можно находить методом неопределённых коэффициентов.

3.34. Пример. Составить тождество Безу для многочленов $f(x)=x^2+1,\ g(x)=x+2$, если известно, что $НОД\left(f, g\right)=1$.

Тождество Безу имеет вид $fu+gv=1$, причём $cm(u)<cm(g)=1,\ cm(v)<cm(f)=2$. Пользуясь этим, будем искать многочлены u, v в следующем виде:

$$u(x)=a,\ v(x)=bx+c.$$

Подставляем эти выражения в тождество, приводим обе части тождества к стандартной форме и приравниваем коэффициенты при одинаковых степенях переменного.

$$\left(x^2+1\right)\cdot a+(x+2)\cdot(bx+c)=1,$$

$$(a+b)x^2+(2b+c)x+(a+2c)=1,$$

$$\begin{cases} a+b=0, \\ 2b+c=0, \\ a+2c=1. \end{cases}$$

Решаем полученную систему. Из первого и второго уравнения получам $a=-b,\ c=-2b$. Подставляем это в третье уравнение, находим b, а затем a и c:

$$a+2c=-b+2(-2b)=1,\ -5b=1,$$

$$b=-\frac{1}{5},\ a=\frac{1}{5},\ c=\frac{2}{5}.$$

Тождество Безу имеет вид

$$\left(x^2+1\right)\frac{1}{5}+(x+2)\left(-\frac{1}{5}x+\frac{2}{5}\right)=1.$$

Если раскрыть скобки и привести подобные, то, естественно, в левой части всё, кроме единицы, сократится.

§4. Неприводимые многочлены

3.35. Определение. Ненулевой многочлен положительной степени $f(x) \in P[x]$ называется *неприводимым над полем* P (*простым* элементом кольца $P[x]$), если он не имеет нетривиальных делителей. В противном случае он называется *приводимым*.

Многочлены нулевой степени и нулевой многочлен не являются ни приводимыми, ни неприводимыми.

3.36. Теорема (основное свойство неприводимых многочленов). *Пусть* $p(x)$ *– неприводимый многочлен в кольце* $P[x]$. *Произвольный многочлен* $f(x)$ *из этого кольца либо делится на* $p(x)$, *либо взаимно прост с ним.*

Доказательство. Многочлен $p(x)$ имеет только тривиальные делители: a, $ap(x)$, $a \in P$, $a \neq 0$. Если общими делителями многочленов $p(x)$ и $f(x)$ являются только делители первого типа, то $НОД(f, p) = 1$. Если среди общих делителей есть многочлены второго типа, то $f(x) \vdots p(x)$.

3.37. Следствие. П*роизведение многочленов* $f(x)g(x)$ *делится на неприводимый многочлен* $p(x)$ *тогда и только тогда, когда на* $p(x)$ *делится хотя бы один из сомножителей.*

Доказательство. Если $f(x) \vdots p(x)$, то доказывать нечего. Если $f(x) \not\vdots p(x)$, то многочлены $f(x)$ и $p(x)$ взаимно просты по теореме 3.36 и по свойству делимости 3.32.8) второй сомножитель будет делиться на $p(x)$.

3.38. Теорема (признак приводимости). *Ненулевой многочлен* $f(x)$ *приводим в кольце* $P[x]$ *тогда и только тогда, когда он раскладывается в произведение двух многочленов меньшей степени:*

$$f(x) = d(x)h(x),\ cm(d), cm(h) < cm(f).$$

Доказательство. Если многочлен приводим, то он имеет нетривиальный делитель $d(x)$:

$$f(x)=d(x)h(x),\ 0<cm(d)<cm(f).$$

Частное $h(x)$ также будет нетривиальным делителем многочлена $f(x)$, т.к. из равенства $cm(f)=cm(d)+cm(h)$ следует, что если $cm(h)=cm(f)$, то $cm(d)=0$; если $cm(h)=0$, то $cm(d)=cm(f)$. В обратную сторону доказательство аналогично.

3.39. Следствие. *Ненулевой многочлен $f(x)$ приводим в кольце $P[x]$ тогда и только тогда, когда он раскладывается в произведение двух многочленов положительной степени:*

$$f(x)=d(x)h(x),\ cm(d),cm(h)>0.$$

3.40. Теорема (простейшие случаи неприводимости**).**

1) Многочлен первой степени всегда является неприводимым.

2) Если многочлен степени 2 или выше имеет корень, то он приводим.

3) Многочлен второй или третьей степени приводим тогда и только тогда, когда он имеет корень.

Доказательство. 1) Если многочлен приводим, то он раскладывается в произведение многочленов положительной степени:

$$f(x)=d(x)h(x),\ cm(d),cm(h)>0.$$

Отсюда получаем, что $cm(d),cm(h)\geq 1$ и

$$cm(f)=cm(d)+cm(h)\geq 2.$$

В результате приводимый многочлен не может быть степени меньше 2. Следовательно, многочлен первой степени всегда неприводим.

2) Если ненулевой многочлен имеет корень $c \in P$, то по теореме Безу он делится на $(x-c)$. Отсюда $f(x)=(x-c)h(x)$, причём $cm(h)=cm(f)-1\geq 1>0$. В результате многочлен $f(x)$ имеет два нетривиальных делителя $(x-c)$ и $h(x)$ и является приводимым.

3) Пусть многочлен второй или третьей степени имеет нетривиальное разложение

$$f(x)=d(x)h(x),\ cm(d), cm(h)>0.$$

По свойству степеней

$$cm(f)=cm(d)+cm(h)=2 \text{ или } 3.$$

Очевидно, степень одного из сомножителей равна единице. Многочлен первой степени всегда имеет один корень, который будет и корнем исходного многочлена.

3.41. Замечание. Для многочлена четвёртой степени свойство, аналогичное 3.40.3), не верно, т.к., например, многочлен $f(x)=\left(x^2+1\right)^2$ приводим в кольце $\mathbb{R}[x]$, но действительных корней не имеет.

3.42. Теорема. *Всякий многочлен положительной степени $f \in P[x]$ представим в виде*

$$f(x)=Ap_1^{k_1}(x)\,p_2^{k_2}(x)\cdot\ldots\cdot p_s^{k_s}(x),$$

где $A \in P$, а $p_1(x), p_2(x), \ldots, p_s(x)$ – попарно различные нормированные неприводимые в $P[x]$ многочлены. Данное представление единственно с точностью до порядка сомножителей. Будем называть его *каноническим.*

Доказательство этой теоремы аналогично доказательству основной теоремы арифметики. Сначала многочлен раскладываем на два нетривиальных сомножителя, потом каждый сомножитель – снова на нетривиальные сомножители и т.д. Так как степени многочленов являются целыми неотрицательными числами и при разложении строго убывают,

то этот процесс оборвётся. В результате получится разложение вида

$$f(x)=q_1(x)q_2(x)\cdot\ldots\cdot q_m(x),$$

где $q_1(x),q_2(x),\ldots,q_m(x)$ – неприводимые многочлены. Эти сомножители могут быть ассоциированы. Вынесем старшие коэффициенты всех многочленов и запишем их в начале разложения в виде общего сомножителя A. Одинаковые сомножители соберём в степень. В результате получится требуемое разложение.

Чтобы различать случаи разных степеней k_i, вводится понятие *кратности*.

3.43. Определение. Неприводимый (нормированный) многочлен $p(x)$ называется *неприводимым множителем кратности* $k>0$ многочлена $f(x)$, если

$$f(x)\vdots p^k(x) \quad \text{и} \quad f(x)\not\vdots p^{k+1}(x).$$

Кратность – это степень, в которой неприводимый многочлен входит в каноническое разложение данного многочлена. Будем считать, что кратность равна нулю, если неприводимый многочлен не входит в каноническое разложение. Неприводимый многочлен называют *кратным множителем* данного многочлена, если его кратность больше или равна 2.

3.44. Предложение. *Неприводимый (нормированный) многочлен* $p(x)$ *является неприводимым множителем кратности* $k>0$ *многочлена* $f(x)$ *тогда и только тогда, когда*

$$f(x)=p^k(x)h(x) \quad и \quad h(x)\not\vdots p(x).$$

Доказательство. Первые условия данного предложения и определения равносильны по определению делимости. Докажем равносильность вторых условий при условии выполнимости первых.

Пусть $f(x)\not\vdots p^{k+1}(x)$, но, напротив, $h(x)\vdots p(x)$. Тогда $h(x)=p(x)q(x)$, $f(x)=p^k(x)h(x)=p^{k+1}(x)q(x)$ и, следовательно, $f(x)\vdots p^{k+1}(x)$. Противоречие.

Пусть $h(x)\not\vdots p(x)$, но, напротив, $f(x)\vdots p^{k+1}(x)$. Тогда $f(x)=p^{k+1}(x)q(x)=p^k(x)h(x)$. Сократив на $p^k(x)$, получим $p(x)q(x)=h(x)$ и, следовательно, $h(x)\vdots p(x)$. Противоречие.

3.45. Пример. Найти в кольце $\mathbb{R}[x]$ многочленов с действительными коэффициентами кратность неприводимого множителя x^2+x+1 в разложении многочлена

$$f(x)=2x^5+7x^4+12x^3+13x^2+8x+3\,.$$

Во-первых, многочлен x^2+x+1 действительно неприводим в кольце $\mathbb{R}[x]$ по теореме 3.40, т.к. он второй степени и не имеет действительных корней. Согласно предложению 3.44, достаточно делить данный многочлен, а затем получаемые частные на $\left(x^2+x+1\right)$ до тех пор, пока деление выполнимо без остатка. Подсчитав количество делений без остатка, мы определим искомую кратность.

$$\begin{array}{r|l}
2x^5+7x^4+12x^3+13x^2+8x+3 & x^2+x+1 \\
\underline{-\,2x^5+2x^4+2x^3} & \hline
5x^4+10x^3+13x^2+8x+3 & 2x^3+5x^2+5x+3 \\
\underline{-\,5x^4+5x^3+5x^2} & \\
5x^3+8x^2+8x+3 & \\
\underline{-\,5x^3+5x^2+5x} & \\
3x^2+3x+3 & \\
\underline{-\,3x^2+3x+3} & \\
0 &
\end{array}$$

$$\begin{array}{r|l} 2x^3+5x^2+5x+3 & x^2+x+1 \\ \underline{-\,2x^3+2x^2+2x} & \overline{2x+3} \\ 3x^2+3x+3 & \\ \underline{-\,3x^2+3x+3} & \\ 0 & \end{array}$$

Очевидно, $(2x+3)\nmid\left(x^2+x+1\right)$. Поэтому искомая кратность равна двум. Кроме этого, получено разложение

$$f(x)=2x^5+7x^4+12x^3+13x^2+8x+3=\left(x^2+x+1\right)^2(2x+3).$$

Наиболее важным является случай, когда неприводимый множитель имеет вид $(x-c)$, т.е. имеет первую степень. В этом случае элемент $c\in P$ является корнем многочлена, и поэтому говорят о кратности корня.

3.46. Определение. Элемент $c\in P$ называется *корнем кратности* $k>0$ многочлена $f(x)$, если

$$f(x)\vdots(x-c)^k \quad \text{и} \quad f(x)\nmid(x-c)^{k+1}.$$

3.47. Предложение. *Элемент* $c\in P$ *является корнем кратности* $k>0$ *многочлена* $f(x)$ *тогда и только тогда, когда*

$$f(x)=(x-c)^k h(x) \quad \textit{и} \quad h(c)\neq 0.$$

Доказательство следует из предложения 3.44 и теоремы Безу.

3.48. Пример. Определить кратность корня $c=1$ многочлена $f(x)=3x^4-11x^3+15x^2-9x+2$.

Выполним деление по схеме Горнера.

	3	–11	15	–9	2
$c=1$	3	–8	7	–2	0

	3	−8	7	−2
$c=1$	3	−5	2	0

	3	−5	2
$c=1$	3	−2	0

	3	−2
$c=1$	3	$-1\neq 0$

В четвёртом делении получился ненулевой остаток, следовательно, кратность равна трём. Запишем результаты всех делений.

$$f(x)=3x^4-11x^3+15x^2-9x+2=(x-1)\left(3x^3-8x^2+7x-2\right),$$

$$3x^3-8x^2+7x-2=(x-1)\left(3x^2-5x+2\right),$$

$$3x^2-5x+2=(x-1)(3x-2).$$

Окончательное разложение имеет вид

$$f(x)=(x-1)^3(3x-2)=3(x-1)^3\left(x-\frac{2}{3}\right).$$

Для определения кратности может использоваться производная. Дадим алгебраическое определение производной (так называемая *формальная производная*), в котором не участвует понятие предела, т.к. предел в поле P может быть не определён.

3.49. Определение. *Производной многочлена*

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0\in P[x]$$

называется многочлен

$$f'(x)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\ldots+a_2x+a_1\in P[x].$$

В данной записи n используется для обозначения элемента $\underbrace{1+1+\ldots+1}_{n} \in P$.

3.50. Теорема (свойства производной). *Для любых многочленов f, g над некоторым полем P и для любого элемента $a \in P$ выполняются следующие свойства.*

1) $(f+g)' = f' + g'$,

2) $(fg)' = f'g + fg'$,

3) $(af)' = af'$,

4) $(f^m)' = mf^{m-1}f'$.

Доказательство может быть проведено непосредственно по определению. В случае, когда P – поле действительных чисел, можно сослаться на общие свойства из курса анализа.

Разберём сначала случай поля характеристики ноль.

3.51. Теорема (о кратности неприводимых множителей). *Если P – поле характеристики ноль, а $p(x)$ – неприводимый множитель кратности $k \geq 1$ ненулевого многочлена $f(x)$ из кольца $P[x]$, то $p(x)$ – неприводимый множитель кратности $(k-1)$ производной $f'(x)$.*

Доказательство. По условию

$$f(x) = p^k(x)h(x) \quad и \quad h(x) \not\vdots p(x).$$

Пользуясь свойствами производной, получаем

$$f'(x) = kp^{k-1}(x)p'(x)h(x) + p^k(x)h'(x) =$$

$$= p^{k-1}(x) \cdot \left[kp'(x)h(x) + p(x)h'(x)\right] = p^{k-1}(x) \cdot H(x),$$

где $H(x)=kp'(x)h(x)+p(x)h'(x)$. Если, напротив, $H(x)$ делится на $p(x)$, то первое слагаемое $\left(kp'(x)h(x)\right)$ делится на $p(x)$. Так как P – это поле характеристики ноль, то $k\neq 0$ и, следовательно, $\left(p'(x)h(x)\right)$ делится на неприводимый многочлен $p(x)$. Согласно следствию 3.37, один из сомножителей должен делиться на $p(x)$. Однако $p'(x)$ не может делиться на $p(x)$, т.к. его степень на единицу меньше степени $p(x)$, а $h(x)$ не может делиться на $p(x)$ по условию. Противоречие.

В результате частное не может делиться на $p(x)$, оба условия предложения 3.44 проверены и теорема доказана.

3.52. Следствие (признак наличия кратных множителей). *Ненулевой многочлен $f(x)$ над полем характеристики ноль имеет кратные множители тогда и только тогда, когда $НОД\left(f,f'\right)\neq 1$.*

Задача разложения многочлена на неприводимые множители является весьма сложной. Во многих случаях для неё нет общего алгоритма. Данное же следствие позволяет определить наличие кратных множителей при помощи алгоритма Евклида, который сводится к делению многочленов.

3.53. Следствие. *Элемент c поля характеристики ноль будет корнем кратности $k\geq 1$ многочлена $f(x)$ тогда и только тогда, когда*

$$f(c)=0,\ f'(c)=0,\ f''(c)=0,\ \ldots,\ f^{(k-1)}(c)=0,\ f^{(k)}(c)\neq 0.$$

Доказательство. Пусть c – корень кратности $k\geq 1$ многочлена $f(x)$, тогда по предложению 3.47 имеем

$$f(x)=(x-c)^k h(x)\ \ и\ \ h(c)\neq 0.$$

Все производные многочлена $f(x)$, начиная с нулевой и заканчивая производной $(k-1)$-го порядка, содержат в качестве сомножителя $(x-c)$. Поэтому

$$f(c)=0,\ f'(c)=0,\ f''(c)=0,\ \ldots,\ f^{(k-1)}(c)=0.$$

Производная k-го порядка в точке c равна

$$f^{(k)}(c)=k!\cdot h(c)\neq 0.$$

В обратную сторону. Многочлен $(x-c)$ будет неприводимым множителем многочленов $f(x), f'(x),\ldots, f^{(k-1)}(x)$. По предложению 3.44 он будет множителем кратности 1 многочлена $f^{(k-1)}(x)$. После этого $(k-1)$ раз применяем теорему:

$(x-c)$ множитель кратности 2 многочлена $f^{(k-2)}(x)$;

$(x-c)$ множитель кратности 3 многочлена $f^{(k-3)}(x)$;

...

$(x-c)$ множитель кратности k многочлена $f^{(k-k)}(x)=f(x)$.

Перейдём к случаю полей ненулевой характеристики. Некоторый аналог теоремы 3.51 выполняется только для неприводимых множителей степени один.

3.54. Теорема (признак кратного корня). *Корень c некоторого ненулевого многочлена $f(x)$ над произвольным полем является его кратным корнем тогда и только тогда, когда он также является корнем производной $f'(x)$.*

Доказательство. Пусть $f(x)=(x-c)^k h(x)$ и $k\geq 2$. Пользуясь свойствами производной, получаем

$$f'(x)=k(x-c)^{k-1}h(x)+(x-c)^k h'(x)=$$

$$=(x-c)^{k-1}\cdot\left[kh(x)+(x-c)h'(x)\right].$$

Так как $k-1\geq 1$, то производная $f'(x)$ делится на $(x-c)$.

В обратную сторону. Пусть, напротив, производная $f'(x)$ делится на $(x-c)$, но c является однократным корнем многочлена $f(x)$:

$$f(x)=(x-c)h(x),\ h(c)\neq 0.$$

По свойствам производной $f'(x)=h(x)+(x-c)h'(x)$. Так как по условию $f'(x)$ делится на $(x-c)$, то и $h(x)$ делится на $(x-c)$. Противоречие с условием $h(c)\neq 0$.

Аналог следствия 3.52 будет доказан в следующей главе.

3.55. Следствие. *Если ненулевой многочлен взаимно прост со своей производной, то он не имеет кратных корней.*

Действительно, если ненулевой многочлен $f(x)$ имеет кратный корень β, то этот корень будет общим для него и его производной. В этом случае $НОД(f,f')$ делится на многочлен $(x-\beta)$ и не может равняться 1.

3.56. Пример. Определить кратность корня $c=1$ многочлена $f(x)=3x^4-11x^3+15x^2-9x+2$ над полем действительных чисел.

Действуем согласно следствию 3.53.

$f(1)=3-11+15-9+2=0$;

$f'(x)=12x^3-33x^2+30x-9,\ f'(1)=12-33+30-9=0$;

$f''(x)=36x^2-66x+30,\ f''(1)=36-66+30=0$;

$f'''(x)=72x-66,\ f'''(1)=72-66=6\neq 0$.

Кратность корня $c=1$ равна 3.

§5. Многочлены над полями комплексных и действительных чисел

В прикладных задачах часто используются поля $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$ соответственно рациональных, действительных и комплексных чисел. Для многочленов над этими полями основной является задача отыскания корней многочлена.

Рассматривая многочлены над различными полями, нетрудно заметить, что они далеко не всегда имеют корни. Например, многочлен $x^2+2x-1\in\mathbb{Q}[x]$ не имеет (рациональных) корней, хотя имеет действительные корни $-1\pm\sqrt{2}$. Многочлен $x^2+1\in\mathbb{R}[x]$ не имеет действительных корней (хотя имеет комплексные корни $\pm i$). Возникает вопрос: а существуют ли кольца многочленов, в которых всякий многочлен положительной степени имеет корень?

3.57. Определение. Поле P называется *алгебраически замкнутым*, если всякий ненулевой многочлен положительной степени в кольце многочленов $P[x]$ имеет корень.

Один из основных примеров алгебраически замкнутого поля даёт

3.58. Теорема (основная алгебры многочленов). *Всякий многочлен положительной степени с комплексными коэффициентами имеет комплексный корень.*

Доказательство этой теоремы здесь не приводится, т.к. оно достаточно громоздко и для него необходимы некоторые нетривиальные факты из теории функций комплексного переменного.

3.59. Следствие. *Неприводимыми многочленами в кольце* $\mathbb{C}[x]$ *являются только многочлены первой степени.*

Действительно, многочлены первой степени всегда неприводимы. Многочлены больших степеней, согласно теореме, имеют корень и будут приводимы по одному из свойств неприводимости (3.40).

3.60. Следствие. *Всякий многочлен положительной степени из* $\mathbb{C}[x]$ *может быть единственным способом представлен в виде*

$$f(x)=a_n(x-c_1)(x-c_2)\ldots(x-c_n),$$

где a_n *– старший коэффициент, а* $c_1, c_2, \ldots, c_n$ *– корни многочлена* $f(x)$.

Доказательство следует из теоремы о разложении на простые (неприводимые) сомножители и следствия 3.59.

Можно собрать одинаковые сомножители первой степени в степень. В результате получится *каноническое разложение* данного многочлена в кольце $\mathbb{C}[x]$.

3.61. Следствие. *Всякий многочлен положительной степени в* $\mathbb{C}[x]$ *может быть единственным способом представлен в виде*

$$f(x)=a_n(x-c_1)^{\alpha_1}(x-c_2)^{\alpha_2}\ldots(x-c_k)^{\alpha_k},$$

где a_n *– старший коэффициент, а* $c_1, c_2, \ldots, c_k$ *– различные корни многочлена* $f(x)$.

Степени α_i – это, как легко заметить, кратности соответствующих корней.

3.62. Следствие. *Всякий многочлен положительной степени n из* $\mathbb{C}[x]$ *имеет ровно n корней, если каждый его корень считать столько раз, какова его кратность.*

3.63. Теорема (Виет). *Пусть дан нормированный многочлен* $f(x)=x^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$ *из кольца* $\mathbb{C}[x]$. *Пусть* $c_1, c_2, \ldots, c_n$ *– все его корни, причём каждый корень взят столько раз, какова его кратность. Тогда*

$$\begin{cases} a_{n-1} = -(c_1 + c_2 + \ldots + c_n), \\ a_{n-2} = c_1c_2 + c_1c_3 + \ldots + c_{n-1}c_n, \\ \ldots \\ a_0 = (-1)^n (c_1 c_2 \ldots c_n). \end{cases}$$

Доказательство. Возьмём разложение исходного многочлена согласно следствию 3.60, учитывая, что $a_n = 1$:

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = (x - c_1)(x - c_2)\ldots(x - c_n).$$

Согласно утверждению теоремы, коэффициент a_{n-k} равен сумме всевозможных произведений k корней многочлена со знаком $(-1)^k$. Если в правой части равенства раскрыть скобки, привести подобные и приравнять коэффициенты при одинаковых степенях x, то получатся все эти равенства.

3.64. Замечание. В теореме Виета рассматривается многочлен со старшим коэффициентом, равным 1. В общем случае нужно предварительно пронормировать многочлен, т.е. разделить его на старший коэффициент. Корни при этом не изменяются.

Смысл теоремы Виета в том, что коэффициенты многочлена вычисляются как некоторые выражения от корней.

3.65. Пример. Пусть x_1, x_2, x_3 – комплексные корни многочлена $f(x) = x^3 + x^2 + 1$. Найти многочлен третьей степени, корнями которого будут суммы $x_1 + x_2$, $x_2 + x_3$, $x_1 + x_3$.

Искомый многочлен $g(x)$ будет иметь третью степень, т.к. должен иметь три корня. Можно считать, что он нормированный. Запишем его с неопределёнными коэффициентами:

$$g(x) = x^3 + ax^2 + bx + c.$$

По теореме Виета для многочлена $g(x)$ должны выполняться следующие равенства:

$$\begin{cases} a=-(x_1+x_2)-(x_2+x_3)-(x_1+x_3), \\ b=(x_1+x_2)(x_2+x_3)+(x_1+x_2)(x_1+x_3)+(x_2+x_3)(x_1+x_3), \\ c=-(x_1+x_2)(x_2+x_3)(x_1+x_3). \end{cases} \quad (4)$$

По теореме Виета для исходного многочлена имеем:

$$\begin{cases} 1=-(x_1+x_2+x_3), \\ 0=x_1x_2+x_2x_3+x_1x_3, \\ 1=-x_1x_2x_3. \end{cases} \quad (5)$$

После этого вычисляем последовательно коэффициенты искомого многочлена, выражая правые части системы (4) через правые части системы (5).

$$a=-(x_1+x_2)-(x_2+x_3)-(x_1+x_3)=-2(x_1+x_2+x_3)=2.$$

$$b=(x_1+x_2)(x_2+x_3)+(x_1+x_2)(x_1+x_3)+(x_2+x_3)(x_1+x_3)=$$

$$=(x_1x_2+x_1x_3+x_2x_2+x_2x_3)+(x_1x_1+x_1x_3+x_2x_1+x_2x_3)+$$

$$+(x_2x_1+x_3x_1+x_2x_3+x_3x_3)=$$

$$=3(x_1x_2+x_1x_3+x_2x_3)+x_1^2+x_2^2+x_3^2=$$

$$=(x_1x_2+x_1x_3+x_2x_3)+(x_1+x_2+x_3)^2=0+(-1)^2=1.$$

$$c=-(x_1+x_2)(x_2+x_3)(x_1+x_3)=$$

$$=-(x_1x_2+x_1x_3+x_2x_2+x_2x_3)(x_1+x_3)=$$

$$=-\left(x_1^2x_2+x_1x_2^2+x_1^2x_3+x_1x_3^2+x_2^2x_3+x_2x_3^2+2x_1x_2x_3\right)=$$

$$=-(x_1+x_2+x_3)(x_1x_2+x_1x_3+x_2x_3)+x_1x_2x_3=-(-1)\cdot 0+(-1)=-1.$$

В результате искомый многочлен будет равен

$$g(x)=x^3+ax^2+bx+c=x^3+2x^2+x-1.$$

Рассмотрим кольцо многочленов с действительными коэффициентами $\mathbb{R}[x]$. Каждый многочлен этого кольца можно рассматривать как многочлен с комплексными коэффициентами и пользоваться тем, что он имеет комплексные корни. Ниже будет

доказано, что если комплексное число $a+bi$ является корнем многочлена с действительными коэффициентами, то и сопряжённое с ним число $a-bi$ также является корнем этого многочлена. Для этого нам понадобится следующее

3.66. Предложение. *Для любого многочлена $f(x)$ с действительными коэффициентами и любого комплексного числа и выполняется равенство $\overline{f(u)}=f\left(\overline{u}\right)$.*

Доказательство. Пусть

$$f=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0\,.$$

Рассмотрим левую часть равенства и, пользуясь свойствами сопряжения, преобразуем её к правой части.

$$\overline{f(u)}=\overline{a_nu^n+a_{n-1}u^{n-1}+\ldots+a_1u+a_0}=\ \text{(т.к. } \overline{u+v}=\overline{u}+\overline{v}\text{)}$$

$$=\overline{a_nu^n}+\overline{a_{n-1}u^{n-1}}+\ldots+\overline{a_1u}+\overline{a_0}=\ \text{(т.к. } \overline{u\cdot v}=\overline{u}\cdot\overline{v}\text{)}$$

$$=\overline{a_n}\cdot\overline{u}^n+\overline{a_{n-1}}\cdot\overline{u}^{n-1}+\ldots+\overline{a_1}\cdot\overline{u}+\overline{a_0}=\ \text{(т.к. } a_i\in\mathbb{R}\ \text{ и }\ \overline{a_i}=a_i\text{)}$$

$$=a_n\cdot\overline{u}^n+a_{n-1}\cdot\overline{u}^{n-1}+\ldots+a_1\cdot\overline{u}+a_0=f\left(\overline{u}\right).$$

3.67. Теорема (о комплексных корнях многочленов с действительными коэффициентами). *Если $f(x)$ – многочлен с действительными коэффициентами и комплексное число $a+bi$ является его корнем, то число $a-bi$ также будет корнем многочлена $f(x)$.*

Доказательство. По условию $f(a+bi)=0$. Применим операцию сопряжения к этому равенству и воспользуемся предложением 3.66.

$$\overline{f(a+bi)}=\overline{0}=0=f\left(\overline{a+bi}\right)=f(a-bi)\,.$$

Теорема доказана.

Заметим, что если $b\neq0$, то $a+bi$ и $a-bi$ – различные числа, и теорема позволяет находить новые корни.

3.68. Предложение. *Коэффициенты произведения* $\big(x-(a+bi)\big)\big(x-(a-bi)\big)$ *являются действительными числами.*

Доказательство. $\big(x-(a+bi)\big)\big(x-(a-bi)\big)=$

$$=x^2-(a+bi)x-(a-bi)x+(a+bi)(a-bi)=$$

$$=x^2-2ax+\left(a^2+b^2\right).$$

3.69. Теорема (о неприводимых многочленах в кольце $\mathbb{R}[x]$). *Неприводимыми над* $\mathbb{R}$ *являются все многочлены первой степени, а также все многочлены второй степени с отрицательным дискриминантом. Других неприводимых многочленов в кольце* $\mathbb{R}[x]$ *нет.*

Доказательство. Многочлены первой степени неприводимы над любым полем согласно свойствам неприводимости. Согласно другому свойству, многочлены второй степени неприводимы тогда и только тогда, когда они не имеют действительных корней, а это имеет место только в том случае, когда дискриминант является отрицательным.

Пусть $f(x)\in\mathbb{R}[x]$ – неприводимый многочлен степени больше 2. Согласно свойствам неприводимых многочленов 3.40, он не имеет действительных корней. Следовательно, по основной теореме алгебры многочленов (3.58) он имеет комплексный корень $a+bi$, $b\neq 0$. Согласно теореме 3.67 о комплексных корнях, число $a-bi$ также будет корнем этого многочлена. По теореме Безу $f(x)$ делится на многочлены $\big(x-(a+bi)\big)$ и $\big(x-(a-bi)\big)$. Нетрудно проверить, что эти многочлены первой степени являются взаимно простыми. Тогда по свойству делимости 3.32, $f(x)$ делится на их произведение, которое по предложению 3.68 будет многочленом с действительными коэффициентами: $x^2-2ax+\left(a^2+b^2\right)$. По теореме о делении с остатком частное также будет многочленом с действительными коэффициентами:

$$f(x)=\left(x^2-2ax+\left(a^2+b^2\right)\right)h(x),\quad h(x)\in\mathbb{R}[x].$$

Степень $h(x)$ больше нуля, а это противоречит неприводимости исходного многочлена $f(x)$. Следовательно, неприводимых многочленов степени >2 в кольце $\mathbb{R}[x]$ нет.

Теорема доказана.

3.70. Следствие. *Ненулевой многочлен с действительными коэффициентами имеет чётное число комплексных, недействительных корней.*

Доказательство. Каждый комплексный корень $a+bi$ имеет «парный» (сопряжённый) корень $a-bi$. Если разделить исходный многочлен на многочлен $\left(x^2-2ax+\left(a^2+b^2\right)\right)$, то можно перейти к частному, у которого эта пара корней «изъята», причём по теореме о делении с остатком частное будет многочленом с действительными коэффициентами. Продолжая этот процесс, мы выделим пары комплексных корней исходного многочлена и докажем, что таких корней чётное число. Остальные корни многочлена должны быть действительными.

3.71. Следствие. *Ненулевой многочлен нечётной степени с действительными коэффициентами имеет хотя бы один действительный корень.*

Доказательство. Всего корней нечётное число. Комплексных корней чётное число. Следовательно, действительных корней будет нечётное число: 1, 3, 5 и т.д. штук.

§6. Многочлены с рациональными коэффициентами

Многие задачи для многочленов с рациональными коэффициентами можно сводить к задачам для многочленов с целыми коэффициентами. Для этого достаточно многочлен умножить на *НОК* знаменателей его коэффициентов. В результате получится многочлен с целыми коэффициентами, отличающийся от исходного многочлена числовым множителем.

У этого многочлена практически те же свойства: те же корни, то же множество делителей и т.д. При этом для изучения свойств многочленов с целыми коэффициентами можно привлекать теорию делимости целых чисел, что, как будет показано ниже, даёт существенный выигрыш.

Мы сразу будем рассматривать многочлены с целыми коэффициентами.

3.72. Теорема (о рациональных корнях многочленов с целыми коэффициентами). *Пусть дан многочлен положительной степени с целыми коэффициентами:*

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

Если несократимая дробь $\frac{k}{m}$, $k \in \mathbb{Z}$, $m \in \mathbb{N}$, *является корнем многочлена* $f(x)$, *то свободный член* a_0 *делится на числитель* k, *а старший коэффициент* a_n *– на знаменатель* m *этой дроби.*

Доказательство. Подставим число $\frac{k}{m}$ в многочлен $f(x)$ и приведём к общему знаменателю.

$$f\left(\frac{k}{m}\right) = a_n\left(\frac{k}{m}\right)^n + a_{n-1}\left(\frac{k}{m}\right)^{n-1} + \ldots + a_1\left(\frac{k}{m}\right) + a_0 = 0,$$

$$a_n k^n + a_{n-1} k^{n-1} m + \ldots + a_1 k m^{n-1} + a_0 m^n = 0.$$

Выразим из этого равенства последнее слагаемое:

$$a_0 m^n = -k\left(a_n k^{n-1} + a_{n-1} k^{n-2} m + \ldots + a_1 m^{n-1}\right).$$

Очевидно, оно делится на k. Так как числа m и k взаимно просты, то по свойству делимости 8 (см. **1.30**) a_0 делится на k.

Выразим первое слагаемое:

$$a_n k^n = -m\left(a_{n-1} k^{n-1} + \ldots + a_1 k m^{n-2} + a_0 m^{n-1}\right).$$

Очевидно, оно делится на m. Аналогично, по свойству делимости 8 (см. 1.30) получаем, что a_n делится на m. Теорема доказана.

При помощи этой теоремы можно составить

3.73. Алгоритм поиска рациональных корней многочлена с рациональными коэффициентами.

1) Умножить многочлен на общий знаменатель его коэффициентов и перейти к многочлену с целыми коэффициентами.

2) Найти все целые делители k свободного члена a_0 и все натуральные делители m старшего коэффициента a_n.

3) Составить список всех несократимых дробей вида $\frac{k}{m}$. Это список «претендентов» в рациональные корни данного многочлена.

4) Проверить всех претендентов на выполнимость условия $f\left(\frac{k}{m}\right)=0$ и найти среди них рациональные корни, если они есть.

Рациональных корней у данного многочлена может не оказаться. Проверку условия можно делать подстановкой числа в многочлен по схеме Горнера или каким-нибудь иным способом.

3.74. Пример. Найти рациональные корни многочлена

$$f(x)=x^2-\frac{7}{2}x+3.$$

Действуем согласно алгоритму.

1) $2f(x)=2x^2-7x+6$.

2) Делители свободного члена: ±1, ±2, ±3, ±6. Натуральные делители старшего коэффициента: 1, 2.

3) Претенденты в рациональные корни: ±1, ±2, ±3, ±6, $\pm\frac{1}{2}$, $\pm\frac{3}{2}$.

4) Получилось 12 чисел, которые могут оказаться рациональными корнями данного многочлена. Можно заметить, что отрицательные числа не могут быть корнями, т.к. при подстановке в многочлен отрицательного числа все три слагаемых окажутся больше нуля и сумма будет также строго больше нуля. В результате останется 6 чисел: 1, 2, 3, 6, $\frac{1}{2}$, $\frac{3}{2}$. Проверку можно делать подстановкой.

$$2f(1)=2\cdot 1^2-7\cdot 1+6=1\neq 0.$$

Число 1 не является корнем.

Проверку можно также делать по схеме Гонера.

	2	– 7	6
$c=2$	2	– 3	0

Число 2 оказалось корнем. Кроме того, получено разложение

$$2f(x)=(x-2)(2x-3),$$

из которого находится второй рациональный корень $\left(\frac{3}{2}\right)$. В общем случае, после отыскания первого корня можно от исходного многочлена перейти к частному и повторить для него процедуру. Выигрыш состоит в том, что список претендентов в рациональные корни частного будет меньше. Например, в нашем случае для частного $h(x)=2x-3$ претендентами останутся числа 1, 3, $\frac{1}{2}$, $\frac{3}{2}$, т.е. числа 2 и 6 можно не проверять.

Итак, задача решена: данный многочлен имеет степень 2, у него не может быть более двух корней, а два корня мы уже нашли.

Ответ: рациональными корнями данного многочлена являются числа 2 и $-\frac{3}{2}$.

3.75. Теорема. *Многочлен с целыми коэффициентами неприводим в кольце* $\mathbb{Q}[x]$ *тогда и только тогда, когда он неприводим в кольце* $\mathbb{Z}[x]$.

Эту теорему мы приводим без доказательства.

3.76. Теорема (критерий Эйзенштейна). *Пусть дан многочлен положительной степени с целыми коэффициентами* $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, $a_n \neq 0$. *Если нашлось такое простое число* p, *что*

$$a_n \not\vdots p,\ \ a_{n-1} \vdots p,\ a_{n-2} \vdots p,\ \ldots,\ a_1 \vdots p,\ a_0 \vdots p,\ a_0 \not\vdots p^2,$$

то $f(x)$ *неприводим в* $\mathbb{Q}[x]$.

Доказательство. Пусть, напротив, такое простое число p существует, но данный многочлен раскладывается в произведение двух многочленов положительной степени с целыми коэффициентами.

$$f(x) = \left(b_k x^k + b_{k-1}x^{k-1} + \ldots + b_0\right)\left(c_m x^m + c_{m-1}x^{m-1} + \ldots + c_0\right) =$$

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

$$b_k \neq 0,\ c_m \neq 0,\ k, m > 0.$$

Очевидно, что свободный член произведения равен произведению свободных членов сомножителей: $a_0 = b_0 c_0$. По условию $a_0 \vdots p,\ a_0 \not\vdots p^2$. Отсюда следует, что либо $b_0 \vdots p,\ c_0 \not\vdots p$, либо $b_0 \not\vdots p,\ c_0 \vdots p$. Эти случаи аналогичны, поэтому пусть для определённости $\boxed{b_0 \vdots p,\ c_0 \not\vdots p}$.

Рассмотрим старший коэффициент $a_n = b_k c_m$. По условию $a_n \not\vdots p$, поэтому $b_k \not\vdots p,\ c_m \not\vdots p$.

Рассмотрим коэффициенты первого сомножителя $b_k, \ldots, b_1, b_0$. Так как $b_0 \vdots p$, а $b_k \not\vdots p$, то существует наименьшее $1 \leq s \leq k$ такое, что

$$b_0 \vdots p,\ \ldots,\ b_{s-1} \vdots p,\ \boxed{b_s \not\vdots p}.$$

Вычислим коэффициент

$$a_s = b_s c_0 + b_{s-1} c_1 + \ldots + b_1 c_{s-1} + b_0 c_s .$$

Так как $1 \le s \le k < n$, то по условию $a_s \vdots p$. Сумма $(b_{s-1} c_1 + \ldots + b_1 c_{s-1} + b_0 c_s)$ также делится на p, т.к. в ней, согласно выбору индекса s, все сомножители $b_i \vdots p$. Отсюда следует, что $b_s c_0 \vdots p$ и, значит, $b_s \vdots p$ или $c_0 \vdots p$. Противоречие с полученными ранее условиями (они выделены выше).

Предположение о том, что данный многочлен является приводимым, ведёт к противоречию. Следовательно, $f(x)$ неприводим в $\mathbb{Q}[x]$.

3.77. Следствие. *В кольце* $\mathbb{Q}[x]$ *есть неприводимые многочлены сколь угодно больших степеней.*

Действительно, согласно теореме, все многочлены вида $x^n + p$, где $n \ge 1$, p – простое число, будут неприводимыми в кольце $\mathbb{Q}[x]$.

Возможности для применения критерия Эйзенштейна довольно ограничены, т.к. вероятность найти простое число, удовлетворяющее всем условиям, невелика. Например, многочлен $x^2 + 3x + 1$ неприводим в $\mathbb{Q}[x]$, т.к. он второй степени и не имеет рациональных корней. Однако найти подходящее простое число p невозможно потому, что свободный член равен 1 и не может делиться на простые числа. Расширить возможности применения критерия позволяет следующее

3.78. Предложение. *Пусть* P *– некоторое поле,* $x = ay + b$, $a, b \in P$, $a \ne 0$. *Многочлен* $f(x)$ *неприводим в* $P[x]$ *тогда и только тогда, когда многочлен* $f(ay + b)$ *неприводим в* $P[y]$.

Доказательство. Достаточно проверить, что $f(x)$ приводим в $P[x]$ тогда и только тогда, когда $f(ay+b)$ приводим в $P[y]$.

Пусть $f(x)=u(x)v(x)$, $cm(u), cm(v)>0$, – некоторое нетривиальное разложение многочлена $f(x)$. Тогда

$$f(ay+b)=u(ay+b)\cdot v(ay+b)$$

будет нетривиальным разложением многочлена $f(ay+b)$ в $P[y]$.

Пусть $f(ay+b)=u(y)v(y)$, $cm(u), cm(v)>0$, – некоторое нетривиальное разложение многочлена $f(ay+b)$ в $P[y]$. Тогда $y=\frac{1}{a}x-\frac{b}{a}$ и

$$f(x)=u\left(\frac{1}{a}x-\frac{b}{a}\right)v\left(\frac{1}{a}x-\frac{b}{a}\right)$$

будет нетривиальным разложением многочлена $f(x)$ в $P[x]$.

3.79. Пример. Доказать, что многочлен $f(x)=x^2+3x+1$ неприводим в $\mathbb{Q}[x]$.

Критерий Эйзенштейна к данному многочлену неприменим. Сделаем замену $x=y-1$:

$$f(x)=x^2+3x+1=(y-1)^2+3(y-1)+1=$$

$$=y^2-2y+1+3y-3+1=y^2+y-1=g(y).$$

К многочлену $g(y)$ критерий Эйзенштейна также неприменим. Сделаем замену $x=y+1$.

$$f(x)=x^2+3x+1=(y+1)^2+3(y+1)+1=$$

$$=y^2+2y+1+3y+3+1=y^2+5y+5=h(y).$$

Многочлен $h(y)$ неприводим по критерию Эйзенштейна, т.к. все условия критерия выполняются для простого числа $p=5$. По предложению 3.78 неприводимым будет и многочлен $f(x)$.

Как видно из данного примера, далеко не каждая линейная замена позволяет применить критерий. Более того, неизвестно, существует ли для некоторого данного неприводимого многочлена линейная замена, позволяющая применить критерий.

Рассмотрим ещё один способ доказательства неприводимости в кольце $\mathbb{Q}[x]$, который основан на делимости целых чисел.

3.80. Пример. Доказать неприводимость в кольце $\mathbb{Q}[x]$ многочлена x^4+1.

Во-первых, проверяем, что данный многочлен не имеет рациональных корней (числа ± 1 не являются его корнями). Поэтому он не имеет делителей первой степени. Пусть тем не менее он приводим и раскладывается на два сомножителя меньшей степени.

$$x^4+1=f(x)g(x).$$

Согласно теореме 3.75, можно считать, что эти многочлены имеют целые коэффициенты. Как было отмечено выше, они не могут быть первой степени. Из свойств степени следует, что они оба должны быть второй степени. Применим метод неопределённых коэффициентов.

$$x^4+1=f(x)g(x)=\left(ax^2+bx+c\right)\left(dx^2+ex+h\right),$$

$$a,b,c,d,e,h\in\mathbb{Z}.$$

Раскрываем скобки, приводим подобные члены и приравниваем коэффициенты при одинаковых степенях.

$$\begin{cases} ad=1, \\ ae+bd=0, \\ ah+be+cd=0, \\ bh+ce=0, \\ ch=1. \end{cases}$$

Теперь можно пользоваться тем, что коэффициенты являются целыми числами, и применить свойства делимости.

Из первого уравнения следует, что либо $a=d=1$, либо $a=d=-1$. Второй случай сводится к первому, т.к., не нарушая условия разложимости $x^4+1=f(x)g(x)$, можно поменять знаки всех коэффициентов f,g на противоположные. Будем считать, что $a=d=1$. После подстановки полученная система приобретает вид

$$\begin{cases} e+b=0, \\ h+be+c=0, \\ bh+ce=0, \\ ch=1. \end{cases}$$

Из первого уравнения выражаем $e=-b$ и подставляем в остальные уравнения.

$$\begin{cases} h-b^2+c=0, \\ b(h-c)=0, \\ ch=1. \end{cases}$$

Из последнего уравнения получаем два случая: $c=h=1$ и $c=h=-1$. Рассматриваем эти случаи.

1-й случай: $c=h=1$.

$$\begin{cases} -b^2+2=0, \\ b\cdot 0=0; \end{cases} \quad b=\pm\sqrt{2}.$$

2-й случай: $c=h=-1$.

$$\begin{cases} -b^2-2=0, \\ b\cdot 0=0; \end{cases} \quad b=\pm i\sqrt{2}\,.$$

Во всех случаях получилось, что система не имеет целых решений. Следовательно, многочлен x^4+1 не может раскладываться в произведение многочленов с целыми коэффициентами и является неприводимым в кольце $\mathbb{Q}[x]$.

Задачи для самостоятельного решения

1. Найдите числа a, b из равенства:

а) $x^4+2x^3-16x^2-2x+15=(x+1)\left(x^3+ax^2-17x+b\right)$;

б) $x^5+x^3-2=(x-1)\left(x^4-ax^3+2x^2+2x+b\right)$;

в) $x^5+3x^4+3x^3+3x^2+x+1=$

$$=\left(x^2+x+1\right)\left(x^3+ax^2+bx+1\right);$$

г) $x^6-x^5+3x^4-5x^3+3x^2-5x+2=$

$$=\left(x^3+2x-1\right)\left(x^3+ax^2+bx-2\right).$$

2. Найдите числа a, b из данного условия:

а) $\left(2x^3-x^2+ax+b\right)\vdots\left(x^2-1\right)$;

б) $\left(x^4+3x^3+ax^2-5x+b\right)\vdots\left(x^2+2x-1\right)$;

в) $\left(x^4+2x^2+ax+b\right)\vdots\left(x^2+x+2\right)$.

3. Найдите частное от деления $f(x)$ на $g(x)$:

а) $f(x)=x^4-x^3-6x^2+5x-1$, $g(x)=x^2-3x+1$;

б) $f(x)=x^5-9x^4+26x^3-18x^2-27x+27$,

$g(x)=x^2-4x+3$.

4. Методом неопределённых коэффициентов найдите неполное частное и остаток от деления $f(x)$ на $g(x)$:

а) $f(x)=x^3-19x-30,\ g(x)=x^2+1$;

б) $f(x)=5x^4-x^3-x-4,\ g(x)=x^2-4$;

в) $f(x)=3x^5-x^4-2x^3+x^2+4x+5,\ g(x)=x^2-2x+2$.

5. Дан многочлен с натуральными коэффициентами $f(x)=ax^2+bx+c$. Известно, что для любого натурального x значение многочлена $f(x)$ делится на 3. Докажите, что все числа a,b,c делятся на 3.

6. Разделите с остатком, используя схему Горнера:

а) $f(x)=x^4-2x^3-x^2-4x+1$ на $(x+1)$;

б) $f(x)=x^4-2x^3-x^2-4x+1$ на $(-x+1)$;

в) $f(x)=2x^5-3x^3-x^2-5$ на $(-x-2)$;

г) $f(x)=2x^5-3x^3-x^2-5$ на $(3x+3)$.

7. Вычислите значение $f(c)$:

а) $f(x)=x^4-3x^3-5x^2+8x-14,\ c=4$;

б) $f(x)=x^5-5x^4+7x^3-3x^2+4x-1,\ c=2$.

8. Составьте таблицу значений многочлена:

а) $x^3+\overline{2}x^2+\overline{3}\in\mathbb{Z}_5[x]$; б) $x^3+\overline{2}x^2+\overline{3}\in\mathbb{Z}_7[x]$.

Нарисуйте графики этих многочленов.

9. Найдите в кольце $\mathbb{R}[x]$ многочлен $f(x)$, удовлетворяющий условиям:

а) $cm(f)=2$, $f(-3)=-2$, $f(-2)=-4$, $f(1)=2$;

б) $cm(f)=2$, $f(3)=2$, $f(-1)=6$;

в) $cm(f)=3$, $f(2)=4$, $f(3)=17$, $f(1)=1$, $f(-1)=1$;

г) $cm(f)=3$, $f(1)=2$, $f(3)=3$, $f(4)=1$.

10. Докажите, что:

а) $\left(80x^{70}-60x^{50}+40x^{30}-20x^{10}+x-41\right)\vdots(x-1)$;

б) $\left((x+5)^{25}-(x+3)^{13}+x+2\right)\vdots(x+4)$.

11. Найдите все такие a,b что:

а) $\left(x^4+ax^3+bx+1\right)\vdots(x+1)^2$;

б) $\left(x^5-x^4-4x^3+ax^2+bx+1\right)\vdots(x-1)^3$;

в) $\left(ax^{n+1}+bx^n+1\right)\vdots(x-1)^2$.

12. Разделите «уголком» многочлен $f(x)$ на $g(x)$:

а) $f(x)=2x^4-3x^3+4x^2-5x+6$, $g(x)=x^2-x+1$;

б) $f(x)=x^3-2x^2-2x-1$, $g(x)=3x^2-2x+1$;

в) $f(x)=x^2-x-1$, $g(x)=x^3+x^2-2x+1$;

г) $f(x)=3x^5+x^3+x+1$, $g(x)=x^2+2x-1$;

д) $f(x)=2x^4+4x^3-3x^2$, $g(x)=2x^2-x+1$.

13. Найдите делитель, если известны делимое, неполное частное и остаток:

а) $f(x)=2x^5+x^4+3x^3-1$, $h(x)=x^2+3x+3$, $r(x)=27x+62$;

б) $f(x)=x^5-2x^4-x^3-x^2-2x+3$,

$h(x)=x^2-x-2$, $r(x)=-2x^2-3x+1$;

в) $f(x)=x^4+2x^3+x^2+x+1$, $h(x)=x+4$, $r(x)=9x^2+2x+5$;

г) $f(x)=x^6+2x^5-5x^4-2x^3-4x^2+17x-11$,

$h(x)=x^2+2x-5$, $r(x)=x^3-2x-1$.

14. Разделите с остатком:

а) x^2+3 на x^3-2;

б) $(x+7)^{10}+4$ на $(x+7)^3$;

в) $(x+6)^{12}$ на $(x+6)^8+1$;

г) $(x-5)^{20}$ на $(x-5)^6+1$;

д) $(x+4)^{30}$ на $(x+4)^7-1$.

15. Найдите остаток от деления некоторого многочлена $f(x)$ на многочлен $g(x)$, если:

а) $f(1)=1, f(2)=3, f(3)=5,\ g(x)=(x-1)(x-2)(x-3)$;

б) $f(-1)=3, f(2)=4, f(1)=1,\ g(x)=(x+1)(x-2)(x-1)$.

16. Найдите *НОД* данных многочленов и составьте тождество Безу, используя расширенный алгоритм Евклида:

а) $f(x)=2x^4+x^3-3x^2+5x-2$, $g(x)=2x^3+3x^2-4x+1$;

б) $f(x)=4x^4-2x^3-16x^2+5x+9$, $g(x)=2x^3-x^2-5x+4$;

в) $f(x)=x^5+2x^4-3x^3+6x^2-3x+2$, $g(x)=x^4-x^2+2x-1$;

г) $f(x)=x^5+3x^4+x^3+x^2+3x+1$, $g(x)=x^4+2x^3+x+2$;

д) $f(x)=x^5+2x^2-3x+1$, $f(x)=x^5+3x^4+4x^3+2x^2-2x-1$.

17. Составьте тождество Безу при помощи метода неопределённых коэффициентов:

а) $f(x)=x^2+x-1$, $g(x)=x^2+2x-1$;

б) $f(x)=x^3-2x+3$, $g(x)=x^2-x-1$;

в) $f(x)=(x+1)(x-2)$, $g(x)=x(x-1)(x+2)$;

г) $f(x)=x^3-4x^2+x+6$,

$$g(x)=x^3+2x^2+2x+1,\ НОД(f,g)=x+1;$$

д) $f(x)=x^4-4x^3+1$, $g(x)=x^3-3x^2+1$, $НОД(f,g)=1$.

18. Найдите *НОД* многочленов:

а) $f(x)=(x-1)^{20}+4$, $g(x)=(x-1)^5$;

б) $f(x)=(x-1)^{20}$, $g(x)=(x-1)^5+4$;

в) $f(x)=2x^5-3x^4-5x^3+x^2+6x+3$,

$$g(x)=3x^4+2x^3-3x^2-5x-2.$$

19. Определите, являются ли приводимыми над полями $\mathbb{Q},\mathbb{R}$ и $\mathbb{C}$ следующие многочлены:

а) $f(x)=x^2-9x+20$; б) $f(x)=2x^2-x-3$;

в) $f(x)=3x^2+x+2$; г) $f(x)=x^2+2x-2$.

20. Определите, приводимы ли в кольце $\mathbb{Q}[x]$ данные многочлены. Если да, то разложите их на неприводимые множители.

а) $f(x)=x^4-5x^2+6$; б) $g(x)=2x+6$;

в) $h(x)=x^3+27$; г) $\varphi(x)=x^3-2$.

21. Найдите каноническое разложение многочлена $f(x)$ в кольце $\mathbb{C}[x]$:

а) $f(x)=x^3+x^2-2$; б) $f(x)=x^4+x^2+1$;

в) $f(x)=x^4+4$; г) $f(x)=x^4-10x^2+1$.

22. Найдите каноническое разложение многочлена $f(x)$ в кольце $\mathbb{R}[x]$:

а) $f(x)=x^3+x+2$; б) $f(x)=x^4+8x^3+8x-1$;

в) $f(x)=x^5-5x^4+7x^3-2x^2+4x-8,\ f(2)=0$;

г) $f(x)=x^5+7x^4+16x^3+8x^2-16x-16,\ f(-2)=0$.

23. Найдите в кольце $\mathbb{Q}[x]$ *НОД* и *НОК* многочленов по их каноническому разложению:

$$f(x)=x\left(x^3-3\right)^2\left(x^2-3\right),\ \ g(x)=x^3\left(x^2+1\right)^2\left(x^3-3\right).$$

24. Найдите в кольце $\mathbb{Q}[x]$ *НОД* многочленов:

$$f(x)=\left(x^3-2\right)^2\left(x^2+1\right)(x+1)^2,\ \ g(x)=x^9-3x^3-2.$$

25. Найдите в кольце $\mathbb{C}[x]$ *НОД* многочленов:

а) $f(x)=(x-1)^2(x-2)^2(x+i)$,

$$g(x)=x^5-2x^3+2x^2-3x+2;$$

б) $f(x)=(x-1)^8(x+1)^8$, $g(x)=x^{20}-10x^{11}+10x^2-1$;

в) $f(x)=x^6-1,\ g(x)=x^{14}-x+1$.

26. Найдите в кольце $\mathbb{Q}[x]$ все делители следующих многочленов:

а) $f(x)=\left(x^2+1\right)^3(x-2)^2(x+1)$;

б) $f(x)=\left(x^2-1\right)^2\left(x^2-2\right)(x+1)$.

Найдите все делители этих многочленов в кольцах $\mathbb{R}[x]$ и $\mathbb{C}[x]$.

27. Докажите, что являются взаимно простыми в кольце $\mathbb{Q}[x]$ многочлены:

а) $f(x)=(x+1)(x+3),\ g(x)=x^4+x-1$;

б) $f(x)=(x-1)(x-3),\ g(x)=x^3+x^2-3$.

28. Найдите кратность корня c многочлена $f(x)$:

а) $f(x)=x^5-7x^4+19x^3-26x^2+20x-8,\ c=2$;

б) $f(x)=x^5+9x^4+32x^3+56x^2+48x+16,\ c=-2$;

в) $f(x)=x^5+\overline{2}x^4-\overline{2}x^2-\overline{3}x-\overline{1}\in\mathbb{Z}_7[x],\ c=\overline{2}$;

г) $f(x)=\overline{2}x^4+x^3-\overline{2}x^2-\overline{1}\in\mathbb{Z}_5[x],\ c=-\overline{2}$.

29. В кольце $\mathbb{Q}[x]$ при помощи производной найдите кратные множители многочлена:

а) $f(x)=x^5-6x^4+16x^3-24x^2+20x-8$;

б) $f(x)=x^4+7x^3+17x^2+17x+6$;

в) $f(x)=x^6-15x^4+8x^3+51x^2-72x+27$;

г) $f(x)=x^5-10x^3-20x^2-15x-4$.

30. Найдите все такие a,b, чтобы корень $x=1$ имел кратность не ниже k:

а) $f(x)=x^5-x^4-4x^3+ax^2+bx+1,\ \ k=3$;

б) $f(x)=x^4+(a-2)x^3+(2-2a)x^2+(a-2)x+1,\ \ k=2$.

31. Определите, при каких значениях параметров a,b,c многочлен $f(x)\in\mathbb{R}[x]$ имеет ненулевой корень кратности k:

а) $f(x)=x^5+ax^3+b,\ k=2$;

б) $f(x)=x^5+10ax^3+5bx+c,\ k=3$.

32. Разложите следующие многочлены в произведение линейных множителей над полем $\mathbb{C}$:

а) x^4+4x^3-x-4; б) $x^4-6x^3-2x^2-11x+6$;

в) x^4+6x^2+8; г) x^4+7x^2+10.

33. Составьте многочлен с комплексными коэффициентами, корнями которого являются следующие числа:

а) $2,-1,3+i$; б) $1+2i,2+i$;

в) $3-2i,-1+3i,-3-3i$; г) $1,-1+i,1+i,-1-2i$.

34. Найдите такое значение параметра a, чтобы выполнялось следующее условие:

а) один из корней многочлена $f(x)=x^3-7x+a$ равняется удвоенному другому;

б) сумма двух корней многочлена $f(x)=x^3-4x^2+6x+a$ равняется третьему корню;

в) один из корней многочлена $f(x)=x^3+3x^2+2x+a$ равняется удвоенной сумме двух других корней;

г) сумма двух корней многочлена $f(x)=2x^3-x^2-7x+a$ равняется 1.

35. Разложите данные многочлены в произведение неприводимых множителей над полем $\mathbb{R}$:

а) x^3+3x-4; б) x^3+x-2;

в) $x^3-5x-12$; г) $x^3+7x^2+11x+5$;

д) x^4+4x^2+10; е) x^4+6x^2+9;

ж) x^4+4x^2-21; з) x^6-64.

36. Составьте многочлен наименьшей степени с действительными коэффициентами, корнями которого являлись бы следующие числа:

а) $-2,\ \sqrt{2}-i$; б) $1+2i,\ -1+2i$;

в) двукратный корень i и однократный корень $1+2i$;

г) $2+i, 1+2i, 2i-1$.

37. Найдите корни многочлена $f(x)$, если известно, что $f(c)=0$:

а) $f(x)=2x^3-7x^2+16x-15,\ c=1+2i$;

б) $f(x)=3x^4-5x^3+3x^2+4x-2,\ c=1+i$;

в) $f(x)=2x^4-7x^3+17x^2-17x+5,\ c=1-2i$;

г) $f(x)=x^6+x^5+3x^4+2x^3+3x^2+x+1,\ c=i$.

38. Найдите рациональные корни многочленов:

а) $4x^4+3x^3-1$;

б) $6x^4+x^3+11x^2+2x-2$;

в) $6x^5+x^4-x^3-6x^2-x+1$;

г) $x^5-\frac{1}{6}x^4-\frac{1}{3}x^3+x^2-\frac{1}{6}x-\frac{1}{3}=0$;

д) $3x^4 - 2x^3 + 4x^2 - x + 2;$

е) $x^5 + \frac{1}{6}x^4 - \frac{5}{6}x^3 - \frac{5}{6}x^2 - \frac{11}{6}x - 1 = 0;$

ж) $x^5 - \frac{5}{6}x^4 - x^3 - x^2 + \frac{5}{6}x + 1 = 0.$

39. Докажите при помощи метода неопределённых коэффициентов неприводимость над $\mathbb{Q}$ следующих многочленов:

а) $x^3 + 3x^2 + 1;$ б) $x^3 + 5x^2 + 2;$

в) $x^4 + 3x^3 + 3;$ г) $x^4 + 5x + 7.$

40. Докажите с помощью критерия Эйзенштейна неприводимость над $\mathbb{Q}$ следующих многочленов:

а) $x^5 - 12x^3 + 3;$ б) $x^8 - 10x - 10;$

в) $x^{10} - 8x^5 + 4x^2 + 2;$ г) $5x^3 - 15x^2 + 18x - 5;$

д) $x^4 - 4x^3 + 6x^2 + x + 1;$

е) $x^5 - 5x^4 + 10x^3 - 7x^2 - x + 8;$

ж) $4x^4 + 16x^3 + 24x^2 + 22x + 13.$

ГЛАВА 4. РАСШИРЕНИЯ ПОЛЕЙ

§1. Простые расширения полей

В данной главе рассматриваются расширения так называемых *числовых полей,* т.е. таких полей, которые содержатся в поле комплексных чисел $\mathbb{C}$. Наличие поля, которое содержит все рассматриваемые поля, существенно упрощает рассмотрение, т.к. избавляет от необходимости доказывать, что поле с определёнными свойствами существует. Ниже, если не оговорено противное, будут всегда рассматриваться числовые поля. Подавляющее большинство результатов выполняется и в общем случае, который будет рассмотрен в главах 5 и 6.

Так как числовое поле содержит единицу и замкнуто относительно сложения и взятия противоположного, то оно содержит все элементы вида $\pm\left(\underbrace{1+1+\ldots+1}_{m}\right)=\pm m$, т.е. целые числа. Так как поле замкнуто относительно умножения и взятия обратного, то оно содержит все дроби вида $\frac{n}{m}$, $n\in\mathbb{Z}, m\in\mathbb{N}$, т.е. все рациональные числа. Таким образом, *наименьшим числовым полем является поле рациональных чисел* $\mathbb{Q}$*, а все остальные числовые поля лежат между* $\mathbb{Q}$ *и* $\mathbb{C}$. Например, один из важнейших примеров числового поля – поле действительных чисел $\mathbb{R}$:

$$\mathbb{Q}\subset\mathbb{R}\subset\mathbb{C}.$$

Кроме полей, будут рассматриваться также *числовые кольца*.

4.1. Пример. Рассмотрим множество

$$\mathbb{Q}\left[\sqrt{2}\right]=\left\{a+b\sqrt{2}\,\middle|\, a,b\in\mathbb{Q}\right\}.$$

Оно содержит $0,1$ и замкнуто относительно операций сложения, умножения и взятия противоположного. Согласно критерию подкольца, это множество будет числовым кольцом.

Ниже будет доказано, что оно является полем, т.к. всякий ненулевой элемент в нём имеет обратный. Например:

$$\left(1+\sqrt{2}\right)^{-1}=\frac{1}{1+\sqrt{2}}=\frac{1-\sqrt{2}}{\left(1+\sqrt{2}\right)\left(1-\sqrt{2}\right)}=-1+\sqrt{2}\,.$$

4.2. Определение. Пусть P – некоторое числовое поле. Элемент β называется *алгебраическим над* P, если он является корнем некоторого ненулевого многочлена с коэффициентами из P. В противном случае элемент называется *трансцендентным над* P.

Если поле P не указывается, то подразумевается, что алгебраичность или трансцендентность элемента рассматривается над полем $\mathbb{Q}$ рациональных чисел.

4.3. Пример. Числа $\sqrt{2}$ и i будут алгебраическими над $\mathbb{Q}$, т.к. они соответственно являются корнями многочленов $x^2-2,\ x^2+1\in\mathbb{Q}[x]$.

4.4. Пример. Доказать, что число $\beta=\sqrt{2}+\sqrt{3}$ является алгебраическим.

Рассмотрим равенство $\beta=\sqrt{2}+\sqrt{3}$ и при помощи возведения в квадрат избавимся в нём от иррациональности:

$$\beta^2=2+2\sqrt{6}+3\,,\quad \beta^2-5=2\sqrt{6}\,,$$

$$\left(\beta^2-5\right)^2=24\,,\quad \beta^4-10\beta^2+1=0\,.$$

В результате получилось, что β – корень многочлена x^4-10x^2+1 с рациональными коэффициентами. Что и требовалось доказать. Способ доказательства, применённый в этом примере, достаточно универсален.

4.5. Определение. *Минимальным многочленом* алгебраического над полем P элемента β называется ненулевой, нормированный многочлен наименьшей степени из кольца $P[x]$, корнем которого является β.

Минимальный многочлен будет обозначаться как $m_\beta(x)$. Степень его называется *степенью элемента* β.

4.6. Пример. *Все элементы* β *поля* P *являются алгебраическими над* P *элементами степени 1,* т.к. они – корни многочленов первой степени $x-\beta \in P[x]$, которые и будут минимальными, т.к. первую степень понижать некуда: ненулевые многочлены нулевой степени корней не имеют. Обратное также верно: *любой алгебраический над* P *элемент степени 1 принадлежит* P.

Числа $\sqrt{2}$ и i будут алгебраическими над $\mathbb{Q}$ числами степени 2, т.к. они являются корнями многочленов степени 2 с рациональными коэффициентами (см. пример выше) и не могут иметь степень 1, т.к. не принадлежат $\mathbb{Q}$.

4.7. Теорема (о свойствах минимального многочлена). *Пусть* β *– некоторый алгебраический над полем* P *элемент.*

1) Минимальный многочлен элемента β *существует и единственен.*

2) Минимальный многочлен $m_\beta(x)$ *неприводим в* $P[x]$.

3) Если β *корень некоторого многочлена* $f(x)$ *из* $P[x]$, *то* $f(x)$ *делится на* $m_\beta(x)$.

Доказательство. 1) Пусть M – множество ненулевых многочленов из $P[x]$, для которых β является корнем. Так как β алгебраический над P элемент, то $M \neq \varnothing$. Следовательно, в нём найдётся многочлен наименьшей степени. Можно предполагать, что этот многочлен является нормированным, т.к. нормирование не изменяет степени и множества корней.

Пусть в множестве M имеются два многочлена минимальной степени $f(x)$ и $g(x)$. Тогда $cm(f)=cm(g)$. Разделим один многочлен на другой с остатком:

$$f(x)=g(x)h(x)+r(x).$$

Если $r \neq 0$, то $cm(r) < cm(g)$ и

$$0 = f(\beta) = g(\beta)h(\beta) + r(\beta) = 0 \cdot h(\beta) + r(\beta) = r(\beta),$$

что противоречит выбору многочленов $f(x)$ и $g(x)$. Следовательно, $r = 0$, $f(x) = g(x)h(x)$. Так как $cm(f) = cm(g)$, то $cm(h) = 0$ и $h \in P$.

Из условия $f(x) = g(x) \cdot h$ и нормированности f и g следует, что $h = 1$ и $f(x) = g(x)$.

2) Пусть, напротив, многочлен $m_\beta(x)$ раскладывается в произведение многочленов меньшей степени.

$$m_\beta(x) = u(x)v(x),\ cm(u), cm(v) < cm\left(m_\beta\right),\ u, v \in P[x].$$

Подставим в это равенство элемент β:

$$m_\beta(\beta) = u(\beta)v(\beta) = 0.$$

Получится, что $u(\beta) = 0$ или $v(\beta) = 0$, а это противоречит минимальности многочлена $m_\beta(x)$.

3) Разделим многочлен $f(x)$ на многочлен $m_\beta(x)$ с остатком:

$$f(x) = m_\beta(x)h(x) + r(x).$$

Если $r \neq 0$, то $cm(r) < cm\left(m_\beta\right)$ и

$$0 = f(\beta) = m_\beta(\beta)h(\beta) + r(\beta) = 0 \cdot h(\beta) + r(\beta) = r(\beta),$$

что противоречит выбору многочлена $m_\beta(x)$. Следовательно, $r = 0$ и $f(x) = m_\beta(x)h(x)$.

Минимальный многочлен играет большую роль в изучении алгебраических чисел. Проверку того, что данный многочлен является минимальным для данного элемента, можно производить по следующему признаку минимальности.

4.8. Теорема (признак минимальности). *Пусть* β – *алгебраический над полем* P *элемент. Если* $f(x)\in P[x]$ – *ненулевой, нормированный, неприводимый в* $P[x]$ *многочлен, для которого* β *является корнем, то он и будет для* β *минимальным многочленом.*

Доказательство. Так как $f(\beta)=0$, то по свойству 4.7.3) многочлен $f(x)$ делится на минимальный многочлен $m_\beta(x)$:

$$f(x)=m_\beta(x)h(x).$$

Так как многочлен $f(x)$ неприводим, то степень частного h не может быть положительной, поэтому $cm(h)=0,\ h\in P$. После этого приравниваем старшие коэффициенты в правой и левой частях равенства и получаем, что $1=1\cdot h$. В результате $h=1$, $f(x)=m_\beta(x)$ и теорема доказана.

4.9. Определение. Пусть P – числовое поле и дано комплексное число β, не принадлежащее P. *Расширением поля* P *при помощи элемента* β называется

$$P[\beta]=\left\{a_n\beta^n+a_{n-1}\beta^{n-1}+\ldots+a_1\beta+a_0 \,\middle|\, a_i\in P,\ n\geq 0\right\}.$$

Очевидно, это множество замкнуто относительно сложения и умножения, поэтому, по критерию подкольца, является числовым кольцом. Кроме того,

$$P\subset P[\beta]\subseteq\mathbb{C}.$$

Расширение при помощи элемента – это в точности числовое кольцо, состоящее из чисел, представимых в виде многочленов от β с коэффициентами из P. С некоторыми оговорками такое представление единственно.

4.10. Теорема (о каноническом представлении чисел в $P[\beta]$). *1) Если* β – *алгебраическое над* P *число степени* m, *то всякий элемент* γ *из* $P[\beta]$ *имеет единственное представление вида*

$$\gamma = a_{m-1}\beta^{m-1} + a_{m-2}\beta^{m-2} + \ldots + a_1\beta + a_0,$$

для подходящих коэффициентов $a_{m-1}, a_{m-2}, \ldots, a_1, a_0$ *из* P.

2) Если β *– трансцендентное над* P *число, то всякий элемент* γ *из* $P[\beta]$ *имеет единственное представление вида*

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

для некоторого натурального n *и подходящих коэффициентов* $a_n, a_{n-1}, \ldots, a_1, a_0$ *из* P.

Отличие первого случая от второго состоит в том, что в первом случае степень многочлена от β строго меньше степени числа β. Во втором случае она не ограничена.

Доказательство. 1) Пусть $\gamma = f(\beta)$. Разделим многочлен $f(x)$ на $m_\beta(x)$ с остатком:

$$f(x) = m_\beta(x)h(x) + r(x),$$

$$r(x) = 0 \text{ или } cm(r) < cm(m_\beta) = m.$$

Подставляя β в это равенство, получаем

$$\gamma = f(\beta) = m_\beta(\beta)h(\beta) + r(\beta) = r(\beta).$$

Это и есть требуемое представление.

Если

$$\gamma = g_1(\beta) = a_{m-1}\beta^{m-1} + a_{m-2}\beta^{m-2} + \ldots + a_1\beta + a_0 =$$

$$= g_2(\beta) = b_{m-1}\beta^{m-1} + b_{m-2}\beta^{m-2} + \ldots + b_1\beta + b_0$$

– два представления одного и того же числа γ, то $g_1(\beta) - g_2(\beta) = 0$ и β является корнем многочлена $g_1(x) - g_2(x)$, степень которого не выше $m - 1 < m$. Если этот многочлен ненулевой, то получится противоречие с тем, что β имеет степень m. Следовательно, $g_1(x) - g_2(x) = 0$ и $g_1(x) = g_2(x)$.

2) Необходимое представление существует по определению расширения $P[\beta]$. Докажем единственность. Пусть

$$\gamma = g_1(\beta) = a_n\beta^n + a_{n-1}\beta^{n-1} + \ldots + a_1\beta + a_0 =$$

$$= g_2(\beta) = b_m\beta^m + b_{m-1}\beta^{m-1} + \ldots + b_1\beta + b_0\,,$$

тогда $g_1(\beta) - g_2(\beta) = 0$ и β является корнем многочлена $g_1(x) - g_2(x)$. Если этот многочлен ненулевой, то получится противоречие с тем, что β трансцендентное над P число. Следовательно, $g_1(x) - g_2(x) = 0$ и $g_1(x) = g_2(x)$.

Пусть $K \subset \mathbb{C}$ – некоторое числовое кольцо. Оно замкнуто относительно сложения, вычитания, умножения. Для того чтобы оно было полем, не хватает замкнутости относительно взятия обратных элементов или, что равносильно, деления на ненулевые элементы. Рассмотрим множество

$$K_1 = \left\{ \frac{a}{b} \,\middle|\, a, b \in K,\ b \neq 0 \right\}.$$

По свойствам полей 2.59, K_1 будет замкнуто относительно сложения, умножения, вычитания и деления на ненулевые элементы. По критерию подполя K_1 является числовым полем. Кроме того, K_1 содержит K, т.к. любое $a \in K$ можно представить в виде дроби: $a = \frac{a}{1}$.

Можно заметить, что K_1 – это наименьшее числовое поле, содержащее K, т.к. если K содержится в некотором числовом поле P, то P обязано содержать все элементы вида $\frac{a}{b},\ a, b \in K,\ b \neq 0$, т.е. $K_1 \subseteq P$.

Поле K_1 называется *полем частных* кольца K. Можно доказать, что *для любого кольца без делителей нуля поле частных существует и единственно с точностью до изоморфизма.*

4.11. Определение. Пусть $P[\beta]$ – расширение числового поля при помощи элемента β. Обозначим при помощи $P(\beta)$ поле частных кольца $P[\beta]$. Поле $P(\beta)$ называется *простым алгебраическим расширением* поля P, если β – алгебраическое над P число, и *простым трансцендентным расширением* поля P, если β – трансцендентное над P число.

4.12. Теорема (об избавлении от иррациональности в знаменателе). *Если β – алгебраическое над P число, то* $P(\beta)=P[\beta]$.

Доказательство. Включение $P[\beta]\subseteq P(\beta)$ было получено выше. Докажем обратное включение $P(\beta)\subseteq P[\beta]$. Пусть $a\in P(\beta)$, тогда

$$a=\frac{f(\beta)}{g(\beta)},\ g(\beta)\neq 0,\ f,g\in P[x].$$

Рассмотрим минимальный многочлен $m_\beta(x)$. Он является неприводимым над P. Согласно основному свойству неприводимых многочленов **3.36**, либо $g(x)\vdots m_\beta(x)$, либо многочлены $g(x), m_\beta(x)$ – взаимно просты. Первый случай невозможен, т.к. если $g(x)\vdots m_\beta(x)$, то $g(x)=m_\beta(x)h(x)$ и $g(\beta)=m_\beta(\beta)h(\beta)=0\cdot h(\beta)=0$, что невозможно по условию. Следовательно, $g(x), m_\beta(x)$ – взаимно просты.

Составим для них тождество Безу:

$$g(x)u(x)+m_\beta(x)v(x)=1,\ u(x),v(x)\in P[x]$$

и подставим в него $x=\beta$:

$$g(\beta)u(\beta)+m_\beta(\beta)v(\beta)=g(\beta)u(\beta)+0\cdot v(\beta)=g(\beta)u(\beta)=1.$$

Из последнего равенства следует, что $\dfrac{1}{g(\beta)}=u(\beta)$, поэтому

$$a=\frac{f(\beta)}{g(\beta)}=f(\beta)u(\beta)\in P[\beta].$$

Теорема доказана.

4.13. Следствие. *Если β – алгебраическое над P число, то $P[\beta]$ – поле.*

4.14. Замечание. Так называемое «избавление от иррациональности в знаменателе» состоит в том, что мы получаем равенство вида

$$\frac{f(\beta)}{g(\beta)}=f(\beta)u(\beta).$$

В левой его части есть иррациональность в знаменателе, а в правой этой иррациональности нет.

4.15. Пример. Избавиться от иррациональности в знаменателе дроби $\dfrac{1}{1+\sqrt{2}}$.

Положим $\beta=\sqrt{2},\ a=\dfrac{1}{1+\sqrt{2}}$. Тогда

$$m_{\sqrt{2}}(x)=x^2-2,\ g(x)=1+x.$$

Составим для этих многочленов тождество Безу методом неопределённых коэффициентов.

$$(1+x)u(x)+\left(x^2-2\right)v(x)=1,\ cm(u)<2,\ cm(v)<1;$$

$$(1+x)(ax+b)+\left(x^2-2\right)c=1,$$

$$(a+c)x^2+(a+b)x+(b-2c)=1,$$

$$\begin{cases} a+c=0, \\ a+b=0, \\ b-2c=1. \end{cases}$$

Решаем систему и находим $u(x)$: $c=-a$, $b=-a$, $(-a)-2(-a)=1$; отсюда $a=1$, $c=b=-1$ и $u(x)=x-1$.

В результате $\dfrac{1}{1+\sqrt{2}}=\sqrt{2}-1$.

§2. Конечные расширения полей

Пусть P – некоторое поле и кольцо $K \supseteq P$. Кольцо K с обычными операциями является векторным пространством над полем P. Для того чтобы понять это, достаточно рассмотреть аксиомы векторного пространства над полем P. Согласно этим аксиомам, для любых элементов (векторов) a,b,c из K и любых элементов (скаляров) β, γ из P должны выполняться следующие тождества:

1) $a+b=b+a$,

2) $a+(b+c)=(a+b)+c$,

3) $a+0=a$,

4) $\beta(a+b)=\beta a+\beta b$,

5) $(\beta+\gamma)a=\beta a+\gamma a$,

6) $(\beta\gamma)a=\beta(\gamma a)$,

7) $1\cdot a=a$.

Кроме того, 8) для любого $a \in K$ должно существовать такое $b \in K$, что $a+b=0$.

Замечаем, что 1)–3) и 7), 8) совпадают с соответствующими аксиомами кольца, 4), 5) являются частными случаями распределительного закона, а 6) – частный случай ассоциативности умножения.

Такое векторное пространство обозначается как K/P. Оно может быть как конечномерным, так и бесконечномерным. Уточним определения для случая бесконечного множества векторов.

4.16. Определение. Множество $a_1, a_2, a_3, \ldots$ элементов K (конечное или бесконечное) называется *линейно независимым*, если линейная комбинация конечного множества этих элементов равна нулю только в том случае, когда все коэффициенты равны нулю.

Множество $B = \{a_1, a_2, a_3, \ldots\}$ будет называться *базисом пространства* K, если

1) оно линейно независимо и

2) каждый элемент K линейно выражается через элементы множества B, т.е. равен линейной комбинации конечного множества векторов из B.

Так как к линейной комбинации всегда можно дописать слагаемые с нулевыми коэффициентами, то для простоты обозначений можно считать, что в линейную комбинацию входят подряд все элементы от a_1 до некоторого a_k, где k – это наибольший индекс векторов, входящих в данную линейную комбинацию с ненулевым коэффициентом:

$$\beta_1 a_1 + \beta_{21} a_2 + \ldots + \beta_k a_k, \ k \in \mathbb{N}.$$

После этого свойства 1) и 2) из определения базиса можно записать следующим образом.

1) Для любых скаляров $\beta_1, \beta_2, \ldots, \beta_k$ из P и любого натурального k, если $\beta_1 a_1 + \beta_2 a_2 + \ldots + \beta_k a_k = 0$, то $\beta_1 = \beta_2 = \ldots = \beta_k = 0$.

2) Для любого $a \in K$ существует такое натуральное k и такие скаляры $\beta_1, \beta_2, \ldots, \beta_k$ из P, что $a = \beta_1 a_1 + \beta_2 a_2 + \ldots + \beta_k a_k$.

4.17. Свойство. *Если векторное пространство K имеет бесконечный базис, то оно не может быть конечномерным.*

Доказательство. Пусть пространство K имеет бесконечный базис $B = \{a_1, a_2, a_3, \ldots\}$ и, напротив, имеет ещё конечный базис $b_1, b_2, \ldots, b_n$. Так как B – базис, то все элементы b_j линейно выражаются через него. Пусть b_j линейно

выражается через $a_1, a_2, \ldots, a_{k_j}$. Положим $k = \max\limits_{j=1,2,\ldots,n} k_j$, тогда все элементы $b_1, b_2, \ldots, b_n$ линейно выражаются через $a_1, a_2, \ldots, a_k$.

В свою очередь, все элементы пространства K линейно выражаются через векторы $b_1, b_2, \ldots, b_n$. Следовательно, по свойству транзитивности, все элементы K будут линейно выражаться через $a_1, a_2, \ldots, a_k$. В частности, элемент a_{k+1} линейно выражается через $a_1, a_2, \ldots, a_k$, что противоречит линейной независимости базиса B.

Перейдём к векторным пространствам вида $P[\beta]/P$. Это основной случай конечномерных векторных пространств, которые используются в приложениях.

4.18. Теорема (о размерности расширения). *Элемент β является алгебраическим над полем P тогда и только тогда, когда пространство $P[\beta]/P$ конечномерно. Размерность этого пространства равна степени числа β.*

Доказательство. Пусть β – алгебраический над P элемент степени m. Докажем, что элементы $1, \beta, \beta^2, \ldots, \beta^{m-1}$ образуют базис пространства $P[\beta]/P$. Действительно, все элементы кольца $P[\beta]$ линейно выражаются через эти степени β по теореме 4.10 о каноническом представлении. Кроме того, элементы $1, \beta, \beta^2, \ldots, \beta^{m-1}$ будут линейно независимыми, т.к. если

$$a_{m-1}\beta^{m-1} + a_{m-2}\beta^{m-2} + \ldots + a_1\beta + a_0 = 0$$

для некоторых $a_{m-1}, a_{m-2}, \ldots, a_1, a_0 \in P$, то все эти коэффициенты должны равняться нулю, в противном случае будет найден многочлен из $P[x]$ степени меньше чем m, корнем которого является β. Это противоречит выбору числа m.

Размерность пространства $P[\beta]/P$ равна m, т.к. построенный базис содержит в точности m элементов: $1, \beta, \beta^2, \ldots, \beta^{m-1}$.

Если β трансцендентный над P элемент, то аналогично доказывается, что бесконечное множество

$$1, \beta, \beta^2, \beta^3, \ldots$$

образует базис пространства $P[\beta]/P$. По свойству 4.17, доказанному выше, это пространство не может быть конечномерным, что доказывает теорему в обратную сторону.

4.19. Следствие. *Пусть K – числовое кольцо, содержащее поле P. Если пространство K/P конечномерно, то всякий элемент K является алгебраическим над P.*

Доказательство. Пусть $\beta \in K$, тогда $P[\beta] \subseteq K$ будет его подпространством и, как подпространство конечномерного пространства, само является конечномерным. По теореме о размерности расширения β – алгебраический над P элемент. Степень β будет совпадать с размерностью пространства $P[\beta]/P$.

4.20. Предложение. *Если кольцо K конечномерно над полем P, то оно является полем.*

Для доказательства достаточно для произвольного ненулевого элемента $\beta \in K, \beta \notin P$ найти обратный элемент. По предыдущему следствию β является алгебраическим над P.

Пусть $m_\beta(x) = x^n + a_{n-1}x^{n-1} \ldots + a_1 x + a_0$ – его минимальный многочлен. Так как $\beta \notin P$, то $n > 1$. Свободный член $a_0 \neq 0$, т.к. в противном случае многочлен раскладывается на нетривиальные сомножители

$$m_\beta(x) = \left(x^{n-1} + a_{n-1}x^{n-2} \ldots + a_1\right)x,$$

что противоречит его неприводимости.

Подставляем β в минимальный многочлен и находим β^{-1}.

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

$$\left(\beta^{n-1} + a_{n-1}\beta^{n-2} \ldots + a_1\right)\beta = -a_0,$$

$$\beta^{-1} = -\frac{1}{a_0}\left(\beta^{n-1} + a_{n-1}\beta^{n-2} \ldots + a_1\right) \in K.$$

4.21. Определение. Поле K называется *конечным расширением поля* P, если $P \subseteq K$ и пространство K/P конечномерно.

В этом определении учтён результат предыдущей теоремы, т.к. сразу предполагается, что K – поле.

4.22. Теорема (о транзитивности конечных расширений). *Пусть даны три поля* $P \subseteq K \subseteq L$. *Если* K – *конечное расширение* P, *а* L – *конечное расширение* K, *то* L *является конечным расширением* P. *Причём*

$$\dim(L/P) = \dim(L/K) \cdot \dim(K/P).$$

Доказательство. Пусть $a_1, a_2, \ldots, a_n$ – базис пространства K/P, а $b_1, b_2, \ldots, b_m$ – базис пространства L/K. Для доказательства достаточно указать базис пространства L/P, состоящий из (nm) элементов. Докажем, что это будет множество всевозможных произведений

$$a_i b_j,\ 1 \le i \le n,\ 1 \le j \le m.$$

Любой элемент $a \in L$ линейно выражается через b_j:

$$a = \sum_j \beta_j b_j,\ \beta_j \in K.$$

Все элементы β_j выражаются через a_i:

$$\beta_j = \sum_i \gamma_{ij} a_i,\ \gamma_{ij} \in P.$$

Подставляя выражение для всех β_j в предыдущее равенство, получаем, что

$$a = \sum_j \beta_j b_j = \sum_j \left(\sum_i \gamma_{ij} a_i \right) b_j = \sum_j \sum_i \gamma_{ij} \left(a_i b_j \right),\ \gamma_{ij} \in P,$$

т.е. $a \in L$ линейно выражается через $a_i b_j$.

Докажем линейную независимость элементов $a_i b_j$. Пусть

$$\sum_j \sum_i \gamma_{ij} \left(a_i b_j \right) = 0,\ \gamma_{ij} \in P.$$

Изменяя порядок суммирования, получаем $\sum_j \left(\sum_i \gamma_{ij} a_i \right) b_j = 0$. Так как элементы b_j линейно независимы, а коэффициенты $\sum_i \gamma_{ij} a_i \in K$, то все они равны нулю: $\sum_i \gamma_{ij} a_i = 0$. Так как элементы a_i линейно независимы, то снова все коэффициенты $\gamma_{ij} = 0$. Теорема доказана.

Рассмотрим множество $\overline{P}$ всех алгебраических над P чисел.

4.23. Теорема. *Множество $\overline{P}$ замкнуто относительно сложения, умножения, взятия противоположного и обратного, извлечения корней любой степени. В частности, $\overline{P}$ является числовым полем.*

Доказательство. Действительно, пусть β – корень многочлена $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in P[x]$. Тогда $(-\beta)$ будет корнем многочлена $g(x) = f(-x) \in P[x]$, т.к. $g(-\beta) = f(-(-\beta)) = f(\beta) = 0$.

Число $\frac{1}{\beta}$, $\beta \neq 0$, будет корнем многочлена $h(x) = x^n \cdot f\left(\frac{1}{x} \right) \in P[x]$, т.к.

$$h\left(\frac{1}{\beta}\right)=\frac{1}{\beta^n}\cdot f\left(\frac{1}{\frac{1}{\beta}}\right)=\frac{1}{\beta^n}\cdot f(\beta)=0.$$

Число $\sqrt[m]{\beta}$ будет корнем многочлена $u(x)=f\left(x^m\right)\in P[x]$, т.к. $u\left(\sqrt[m]{\beta}\right)=f\left(\left(\sqrt[m]{\beta}\right)^m\right)=f(\beta)=0$.

Множество $\overline{P}$ замкнуто относительно умножения на элементы из P и относительно добавления элементов из P, т.к. для любого $a\in P$ число $a\beta$ будет корнем многочлена $f\left(\frac{x}{a}\right)\in P[x]$, а число $\beta+a$ – корнем многочлена $f(x-a)\in P[x]$.

Замкнутость относительно сложения и умножения доказывается сложнее. Пусть α,β – алгебраические над полем P числа, пусть $\alpha_1=\alpha,\alpha_2,\ldots,\alpha_n$ – все (комплексные) корни многочлена $m_\alpha(x)$, а $\beta_1=\beta,\beta_2,\ldots,\beta_m$ – все корни многочлена $m_\beta(x)$. В качестве многочлена, корнем которого является $\alpha+\beta$, нужно взять многочлен $f(x)=\prod\limits_{i=1}^{n}\prod\limits_{j=1}^{m}\left(x-\alpha_i-\beta_j\right)$. В качестве многочлена, корнем которого является $\alpha\beta$, нужно взять многочлен $g(x)=\prod\limits_{i=1}^{n}\prod\limits_{j=1}^{m}\left(x-\alpha_i\beta_j\right)$. Правда, достаточно трудно доказать, что эти многочлены принадлежат кольцу $P[x]$. Для этого понадобятся результаты о симметрических многочленах и теоремы Виета для $m_\alpha(x)$ и $m_\beta(x)$.

Разберём другой способ, основанный на свойствах конечных расширений.

Пусть числа $\beta,\gamma\in\overline{P}$. Рассмотрим цепочку расширений

$$P\subseteq P(\beta)\subseteq P(\beta)(\gamma).$$

Число γ является алгебраическим над полем P, поэтому оно – корень некоторого многочлена $f(x)$ с коэффициентами из P. Так как $P \subseteq P(\beta)$, то можно считать, что коэффициенты $f(x)$ лежат в $P(\beta)$, а γ является алгебраическим над полем $P(\beta)$.

По теореме о размерности расширения каждое звено цепочки $P \subseteq P(\beta) \subseteq P(\beta)(\gamma)$ является конечным расширением. По теореме о транзитивности расширений поле $P(\beta)(\gamma)$ будет конечным расширением поля P. Так как

$$P \subseteq P(\beta+\gamma) \subseteq P(\beta)(\gamma),\ P \subseteq P(\beta\gamma) \subseteq P(\beta)(\gamma),$$

то поля $P(\beta+\gamma)$, $P(\beta\gamma)$ также являются конечными расширениями P. По следствию 4.19 из теоремы о размерности числа $\beta+\gamma$ и $\beta\gamma$ будут алгебраическими над P. Теорема доказана.

4.24. Пример. Найти многочлен с рациональными коэффициентами, корнем которого является число $\sqrt{2}+\sqrt{3}$.

Вычислим многочлены, указанные в доказательстве теоремы 4.23. В нашем случае $P = \mathbb{Q}$.

Пусть

$$\alpha = \sqrt{2},\ m_\alpha(x) = x^2 - 2,\ \alpha_1, \alpha_2 - \text{ корни } m_\alpha;$$

$$\beta = \sqrt{3},\ m_\beta(x) = x^2 - 3,\ \beta_1, \beta_2 - \text{корни } m_\beta.$$

Рассмотрим многочлен

$$f(x) = (x-\alpha_1-\beta_1)(x-\alpha_1-\beta_2)(x-\alpha_2-\beta_1)(x-\alpha_2-\beta_2).$$

Нужно раскрыть скобки и представить выражение в виде многочлена от β_1, β_2 (привести подобные члены). Затем, пользуясь теоремой Виета, вычислить значения всех коэффициентов, которые должны оказаться рациональными числами. Затем процедуру повторить для полученного многочлена.

На первом шаге можно съэкономить. Так как по условию $m_\alpha(x)=(x-\alpha_1)(x-\alpha_2)$, то в определении $f(x)$ сомножители можно сгруппировать по парам и получить:

$$f(x)=m_\alpha(x-\beta_1)m_\alpha(x-\beta_2)=\Big((x-\beta_1)^2-2\Big)\Big((x-\beta_2)^2-2\Big).$$

В результате α_1,α_2 уже исчезли. После этого раскрываем скобки и приводим подобные члены.

$$f(x)=\Big(x^2-2\beta_1x+\beta_1^2-2\Big)\Big(x^2-2\beta_2x+\beta_2^2-2\Big)=$$

$$=x^4-2(\beta_1+\beta_2)x^3+\Big(\beta_1^2-2+\beta_2^2-2+4\beta_1\beta_2\Big)x^2+$$

$$+\Big(-2\beta_1\Big(\beta_2^2-2\Big)-2\beta_2\Big(\beta_1^2-2\Big)\Big)x+\Big(\beta_1^2-2\Big)\Big(\beta_2^2-2\Big).$$

По теореме Виета для многочлена $m_\beta(x)=x^2-3$ имеем

$$\beta_1+\beta_2=0,\ \beta_1\beta_2=-3.$$

После этого последовательно вычисляем коэффициенты многочлена $f(x)$, выражая их через числа $\beta_1+\beta_2$ и $\beta_1\beta_2$ и подставляя значения из теоремы Виета.

$$-2(\beta_1+\beta_2)=-2\cdot0=0,$$

$$\beta_1^2-2+\beta_2^2-2+4\beta_1\beta_2=\Big(\beta_1^2+\beta_2^2\Big)-4+4\cdot(-3)=$$

$$=\Big((\beta_1+\beta_2)^2-2\beta_1\beta_2\Big)-16=\Big(0^2-2\cdot(-3)\Big)-16=-10,$$

$$-2\beta_1\Big(\beta_2^2-2\Big)-2\beta_2\Big(\beta_1^2-2\Big)=-2\beta_1\beta_2(\beta_1+\beta_2)+4(\beta_1+\beta_2)=0,$$

$$\Big(\beta_1^2-2\Big)\Big(\beta_2^2-2\Big)=\beta_1^2\beta_2^2-2\Big(\beta_1^2+\beta_2^2\Big)+4=(-3)^2-2\cdot6+4=1.$$

В результате получилось, что $f(x)=x^4-10x^2+1$.

4.25. Теорема. *Корни любого ненулевого многочлена, коэффициенты которого алгебраичны над полем P, сами являются алгебраическими над полем P.*

Доказательство. Пусть $\alpha_n, \alpha_{n-1}, \ldots, \alpha_1, \alpha_0$ – некоторые алгебраические над полем P элементы и β – (комплексный) корень многочлена $f(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \ldots + \alpha_1 x + \alpha_0$. Рассмотрим цепочку расширений:

$$P_0 = P(\alpha_n),$$

$$P_1 = P_0(\alpha_{n-1}),$$

$$P_2 = P_1(\alpha_{n-2}),$$

$$\ldots$$

$$P_n = P_{n-1}(\alpha_0),$$

$$P_{n+1} = P_n(\beta).$$

Так как элемент α_{n-k} является алгебраическим над P, то оно является алгебраическим и над P_{k-1}. По теореме о размерности расширения получаем, что поле P_k является конечным расширением поля P_{k-1}. Элемент β является алгебраическим над полем P_n, следовательно, P_{n+1} также является конечным расширением P_n. Многократно применяя теорему о транзитивности конечных расширений ко всем звеньям цепочки, получаем, что поле $P_{n+1} = P_n(\beta)$ является конечным расширением поля P. Согласно следствию 4.19 из теоремы о размерности расширения, элемент β будет алгебраическим над P.

4.26. Следствие. *Поле $\overline{P}$ для всякого числового поля P является алгебраически замкнутым, т.е. любой многочлен положительной степени с коэффициентами из $\overline{P}$ имеет в $\overline{P}$ корень.*

Доказательство. Пусть $f(x)$ – некоторый многочлен положительной степени с коэффициентами из $\overline{P}$. Так как поле комплексных чисел алгебраически замкнуто, то он имеет комплексный корень β. По только что доказанной теореме $\beta \in \overline{P}$.

В предыдущих двух теоремах рассматривались цепочки последовательных простых алгебраических расширений. Можно задаться вопросом: при каких условиях $P(\alpha)(\beta)=P(\gamma)$, т.е. многократное расширение является простым? Ответ на этот вопрос даёт

4.27. Теорема (о простоте конечного расширения). *Всякое конечное расширение K числового поля P является простым алгебраическим расширением.*

Сначала докажем лемму, которая имеет самостоятельный интерес.

4.28. Лемма (о простоте двукратного алгебраического расширения). *Для любых алгебраических над числовым полем P чисел α,β существует такое алгебраическое над P число γ, что $P(\alpha)(\beta)=P(\gamma)$.*

Доказательство. Пусть α,β – алгебраические над P числа. Число γ будем искать в виде $\gamma=\alpha+c\beta$, где c – параметр из P.

Пусть $m_\alpha(x)$, $m_\beta(x)$ – минимальные многочлены чисел α и β соответственно. Рассмотрим многочлен

$$q(x)=m_\alpha(\gamma-cx)\in P(\gamma).$$

Число β является корнем этого многочлена, т.к.

$$q(\beta)=m_\alpha(\gamma-c\beta)=m_\alpha(\alpha)=0.$$

Основной случай: многочлены $m_\beta(x)$ и $q(x)$ не имеют других общих корней, кроме β.

В этом случае $НОД\left(m_\beta,q\right)=x-\beta$. Так как $НОД$ может быть найден по алгоритму Евклида и коэффициенты исходных многочленов принадлежат $P(\gamma)$, то его коэффициенты также принадлежат $P(\gamma)$. Отсюда следует, что $\beta\in P(\gamma)$. Кроме того, $\alpha=\gamma-c\beta\in P(\gamma)$. Следовательно, $P(\alpha)(\beta)\subseteq P(\gamma)$.

С другой стороны, $\gamma = \alpha + c\beta \in P(\alpha)(\beta)$, поэтому $P(\gamma) \subseteq P(\alpha)(\beta)$ и в результате $P(\gamma) = P(\alpha)(\beta)$.

Докажем, что параметр $c \in P$ всегда можно выбрать так, чтобы имел место основной случай, т.е. чтобы многочлены $m_\beta(x)$ и $q(x)$ не имели других общих корней, кроме β.

Пусть $\alpha_1, \alpha_2, \ldots, \alpha_n$ – все комплексные корни $m_\alpha(x)$, а $\beta_1 = \beta, \beta_2, \ldots, \beta_m$ – все корни многочлена $m_\beta(x)$. Число β_j, $j \neq 1$, будет корнем многочлена $q(x)$, если $\gamma - c\beta_j = \alpha_i$ для некоторого $1 \leq i \leq n$.

По условию $\gamma = \alpha + c\beta$, поэтому

$$\gamma - c\beta_j = \alpha_i = (\alpha + c\beta) - c\beta_j .$$

Отсюда $\alpha_i - \alpha = c(\beta - \beta_j)$ и $c = \dfrac{\alpha_i - \alpha}{\beta - \beta_j}$.

Так как поле P является бесконечным, то всегда можно выбрать параметр c так, чтобы $c \neq \dfrac{\alpha_i - \alpha}{\beta - \beta_j}$ для любых $1 \leq i \leq n$, $1 < j \leq m$. При таком выборе будет иметь место основной случай и, следовательно, равенство $P(\gamma) = P(\alpha)(\beta)$.

Доказательство теоремы 4.27. Индукция по $n = \dim(K / P)$.

Если $n = \dim(K / P) = 1$, то это означает, что $K = P$ и утверждение теоремы очевидно выполняется (например, $K = P(1)$).

Пусть для всех случаев, когда $\dim(K / P) < m$, утверждение теоремы выполняется. Докажем теорему для случая $\dim(K / P) = m$.

Пусть α – алгебраическое над P число и $\alpha \notin P$. В этом случае $\dim\big(P(\alpha)/P\big) > 1$ и по теореме о транзитивности

$$\dim\big(K/P(\alpha)\big) = \frac{\dim(K/P)}{\dim\big(P(\alpha)/P\big)} = \frac{m}{\dim\big(P(\alpha)/P\big)} < m\ .$$

По индукционному предположению $K = P(\alpha)(\beta)$, а по лемме 4.28 о простоте двухкратного расширения $P(\alpha)(\beta) = P(\gamma)$. Теорема доказана.

4.29. Замечание. 1) Так как неподходящих значений параметра c конечное число, а поле P содержит бесконечное множество элементов, то на практике «почти для любого» $c \in P$ выполняется $P(\alpha)(\beta) = P(\alpha + c\beta)$. Можно брать $c = 1$ и почти всегда будет выполняться равенство

$$P(\alpha)(\beta) = P(\alpha + \beta)\,.$$

2) На основе доказательства теоремы можно предложить способ нахождения представления числа β в расширении $P(\gamma)$. Действительно, в теореме представление β через γ получилось, когда мы вычислили по алгоритму Евклида $НОД\big(m_\beta, q\big)$. Поэтому для решения данной задачи нужно по алгоритму Евклида вычислить этот $НОД$, и воспользоваться тем, что он равен $x - \beta$. Свободный член этого делителя с противоположным знаком и будет представлением числа β в $P(\gamma)$.

4.30. Пример. Найти представление числа $\sqrt{3}$ в расширении $P\big(\sqrt{2} + \sqrt{3}\big)$.

Сначала убедимся, что $P\big(\sqrt{2}\big)\big(\sqrt{3}\big) = P\big(\sqrt{2} + \sqrt{3}\big)$. Для этого достаточно, чтобы $c = 1$ удовлетворяло условиям из теоремы. Проверяем эти условия.

$$m_{\sqrt{2}}(x) = x^2 - 2,\ \alpha_1 = \sqrt{2},\ \alpha_2 = -\sqrt{2}\,;$$

$$m_{\sqrt{3}}(x) = x^2 - 3,\ \beta_1 = \sqrt{3},\ \beta_2 = -\sqrt{3}\,.$$

Необходимо, чтобы $1 \neq \dfrac{\alpha_1 - \alpha_i}{\beta_1 - \beta_2}$, $i = 1, 2$, или чтобы $1 \neq \dfrac{\alpha_1 - \alpha_1}{\beta_1 - \beta_2} = 0$, $1 \neq \dfrac{\alpha_1 - \alpha_2}{\beta_1 - \beta_2} = \dfrac{\sqrt{2} - \left(-\sqrt{2}\right)}{\sqrt{3} - \left(-\sqrt{3}\right)} = \dfrac{\sqrt{2}}{\sqrt{3}}$.

Так как эти условия выполняются, то $P\left(\sqrt{2}\right)\left(\sqrt{3}\right) = P\left(\sqrt{2} + \sqrt{3}\right)$ и можно переходить к нахождению наибольшего общего делителя многочленов $m_{\sqrt{3}}(x) = x^2 - 3$ и $q(x) = (\gamma - x)^2 - 2$, $\gamma = \sqrt{2} + \sqrt{3}$. Можно пользоваться тем, что заранее известно, что *НОД* – это многочлен первой степени.

$$\begin{array}{r|l} x^2 - 2\gamma x + \gamma^2 - 2 & x^2 - 3 \\ \underline{-\ x^2 - 3} & \hline 1 \\ -2\gamma x + \gamma^2 + 1 & \end{array}$$

Получился остаток первой степени, следовательно, это и будет искомый *НОД* после того, как мы его пронормируем. В результате $x - \beta = x - \dfrac{\gamma^2 + 1}{2\gamma}$, а $\beta = \dfrac{\gamma^2 + 1}{2\gamma}$ или $\sqrt{3} = \dfrac{\left(\sqrt{2} + \sqrt{3}\right)^2 + 1}{2\left(\sqrt{2} + \sqrt{3}\right)}$. Последнее равенство легко проверить непосредственными вычислениями.

Чтобы найти каноническое представление, можно избавиться от иррациональности в знаменателе полученной дроби.

Пусть β – некоторое алгебраическое над полем P число. Разберём ещё один способ получения многочлена, корнем которого является алгебраический элемент вида $\gamma = a_m \beta^m + \ldots + a_1 \beta + a_0$, $a_i \in P$.

4.31. Метод Чирнгауза (подстановка Чирнгауза).

Пусть степень числа β равна n. Рассмотрим элементы $\gamma, \gamma\beta, \gamma\beta^2, \ldots, \gamma\beta^{n-1}$ и найдём их каноническое представление в $P(\beta)$.

$$\gamma = b_{0,n-1}\beta^{n-1} + \ldots + b_{0,1}\beta + b_{0,0},$$

$$\gamma\beta = b_{1,n-1}\beta^{n-1} + \ldots + b_{1,1}\beta + b_{1,0},$$

$$\gamma\beta^2 = b_{2,n-1}\beta^{n-1} + \ldots + b_{2,1}\beta + b_{2,0},$$

$$\ldots$$

$$\gamma\beta^{n-1} = b_{n-1,n-1}\beta^{n-1} + \ldots + b_{n-1,1}\beta + b_{n-1,0}.$$

Перенесём всё в правую часть и, считая число γ параметром, приведём подобные члены.

$$b_{0,n-1}\beta^{n-1} + \ldots + b_{0,1}\beta + \left(b_{0,0} - \gamma\right) = 0,$$

$$b_{1,n-1}\beta^{n-1} + \ldots + \left(b_{1,1} - \gamma\right)\beta + b_{1,0} = 0,$$

$$b_{2,n-1}\beta^{n-1} + \ldots + \left(b_{2,1} - \gamma\right)\beta^2 + b_{2,1}\beta + b_{2,0} = 0,$$

$$\ldots$$

$$\left(b_{n-1,n-1} - \gamma\right)\beta^{n-1} + \ldots + b_{n-1,1}\beta + b_{n-1,0} = 0.$$

Очевидно, упорядоченный набор чисел $\left(\beta^{n-1}, \beta^{n-2}, \ldots, \beta, 1\right)$ является ненулевым решением однородной системы

$$b_{0,n-1}x_{n-1} + \ldots + b_{0,1}x_1 + \left(b_{0,0} - \gamma\right)x_0 = 0,$$

$$b_{1,n-1}x_{n-1} + \ldots + \left(b_{1,1} - \gamma\right)x_1 + b_{1,0}x_0 = 0,$$

$$b_{2,n-1}x_{n-1} + \ldots + \left(b_{2,1} - \gamma\right)x_2 + b_{2,1}x_1 + b_{2,0}x_0 = 0,$$

$$\ldots$$

$$\left(b_{n-1,n-1} - \gamma\right)x_{n-1} + \ldots + b_{n-1,1}x_1 + b_{n-1,0}x_0 = 0.$$

Однородная система имеет ненулевое решение тогда и только тогда, когда её определитель равен нулю:

$$\begin{vmatrix} b_{0,n-1} & \cdots & b_{0,1} & (b_{0,0}-\gamma) \\ b_{1,n-1} & \cdots & (b_{1,1}-\gamma) & b_{1,0} \\ b_{2,n-1} & \cdots & b_{2,1} & b_{2,0} \\ \cdots & \cdots & \cdots & \cdots \\ (b_{n-1,n-1}-\gamma) & \cdots & b_{n-1,1} & b_{n-1,0} \end{vmatrix} = 0 .$$

Вычислив этот определитель, получим многочлен от γ с коэффициентами из P, равный нулю или, что то же самое, многочлен из кольца $P[x]$, корнем которого является данное число γ.

4.32. Пример. Пусть β – алгебраическое число, минимальным многочленом которого является $m_\beta(x) = x^3 - x - 1$. Найти многочлен, корнем которого является $\gamma = \beta^2 + \beta + 1$.

По умолчанию $P = \mathbb{Q}$. Для нахождения канонического представления в $\mathbb{Q}(\beta)$ будем использовать равенство $\beta^3 - \beta - 1 = 0$, выразив из него старшую степень: $\beta^3 = \beta + 1$.

Действуем согласно описанному методу:

$$\gamma = \beta^2 + \beta + 1,$$

$$\gamma\beta = (\beta^2 + \beta + 1)\beta = \beta^3 + \beta^2 + \beta =$$

$$= (\beta + 1) + \beta^2 + \beta = \beta^2 + 2\beta + 1,$$

$$\gamma\beta^2 = (\beta^2 + 2\beta + 1)\beta = \beta^3 + 2\beta^2 + \beta =$$

$$= (\beta + 1) + 2\beta^2 + \beta = 2\beta^2 + 2\beta + 1.$$

Составляем определитель системы и вычисляем его:

$$\begin{vmatrix} 1 & 1 & 1-\gamma \\ 1 & 2-\gamma & 1 \\ 2-\gamma & 2 & 1 \end{vmatrix} = 0;$$

$$(2-\gamma)+2(1-\gamma)+(2-\gamma)-(2-\gamma)^2(1-\gamma)-2-1=0,$$

$$6-4\gamma-\left(4-4\gamma+\gamma^2-4\gamma+4\gamma^2-\gamma^3\right)-3=0,$$

$$\gamma^3-5\gamma^2+4\gamma-1=0.$$

В результате получилось, что число γ является корнем многочлена $x^3-5x^2+4x-1\in\mathbb{Q}[x]$.

§3*. Разрешимость уравнений в радикалах

Одним из применений теории расширений числовых полей является решение некоторых классических задач на построение.

4.33. Задача о квадратуре круга. *При помощи циркуля и линейки построить квадрат, равновеликий данному кругу.*

4.34. Задача об удвоении куба. *При помощи циркуля и линейки построить куб, объём которого в два раза больше данного.*

4.35. Задача о трисекции угла. *При помощи циркуля и линейки разделить произвольный угол на три равные части.*

Эти задачи пытались решить ещё древние греки. В XIX в. удалось доказать, что эти задачи неразрешимы. В доказательстве используются расширения полей.

4.36. Определение. Будем говорить, что число β *представляется в квадратных радикалах над полем* P, если оно может быть получено из элементов P при помощи извлечения квадратных корней и четырёх арифметических действий: сложения, вычитания, умножения и деления. Более точно, если существует такая последовательность чисел

$$\beta_1, \beta_2, \ldots, \beta_m,$$

что $\beta_m = \beta$ и каждый элемент последовательности либо принадлежит P, либо получается из предыдущих элементов как сумма, как произведение, разность, частное или как квадратный корень.

Алгебраическое уравнение n-й степени с коэффициентами из поля P называется *разрешимым в (квадратных) радикалах над* P, если все его решения представляются в (квадратных) радикалах над P.

4.37. Теорема (необходимое условие разрешимости в квадратных радикалах). *Пусть* $f(x)$ – *нормированный неприводимый многочлен степени* n *в* $P[x]$. *Если один из корней уравнения* $f(x)=0$ *представим в квадратных радикалах над* P, *то число* n *является степенью 2.*

Доказательство. Пусть β – корень уравнения $f(x)=0$, представимый в квадратных радикалах над P. Согласно определению, существует последовательность

$$\beta_1, \beta_2, \ldots, \beta_m = \beta,$$

в которой каждый элемент либо принадлежит P, либо получается из предыдущих элементов как сумма, как произведение, разность, частное или как корень второй степени.

Рассмотрим цепочку расширений

$$P_0 = P,\ P_1 = P_0(\beta_1),\ P_2 = P_1(\beta_2),\ \ldots,\ P_m = P_{m-1}(\beta_m).$$

Если β_k принадлежит P или получается из предыдущих элементов при помощи арифметических операций, то $\beta_k \in P_{k-1}$ и $P_k = P_{k-1}$. Если β_k равен квадратному корню одного из предыдущих элементов, то либо $\beta_k \in P_{k-1}$ и $P_k = P_{k-1}$, либо $\beta_k \notin P_{k-1}$ и тогда $\dim(P_k / P_{k-1}) = 2$. Таким образом,

$$\dim(P_k / P_{k-1}) = 1 \text{ или } 2.$$

Многократно применяя теорему 4.22 о транзитивности конечных расширений, получаем, что

$$\dim\left(P_m / P\right) =$$

$$= \dim\left(P_m / P_{m-1}\right) \cdot \dim\left(P_{m-1} / P_{m-2}\right) \cdot \ldots \cdot \dim\left(P_1 / P\right) = 2^s,$$

где s – это количество случаев, когда $\beta_k \notin P_{k-1}$.

Рассмотрим теперь расширение $P(\beta)$. Так как $f(x)$ – неприводимый многочлен и β – его корень, то $f(x)$ будет минимальным многочленом для β. По теореме о размерности $\dim\left(P(\beta) / P\right) = n$. Так как $P(\beta) \subseteq P_m$, то

$$2^s = \dim\left(P_m / P\right) =$$

$$= \dim\left(P_m / P(\beta)\right) \cdot \dim\left(P(\beta) / P\right) = \dim\left(P_m / P(\beta)\right) \cdot n.$$

В результате получилось, что число 2^s делится на n и, следовательно, $n = 2^q$, $q \le s$. Теорема доказана.

4.38. Следствие. *Кубическое уравнение $f(x) = 0$ для многочлена $f(x)$ из кольца $P[x]$ разрешимо в квадратных радикалах тогда и только тогда, когда имеет хотя бы одно решение в P.*

Доказательство. Если многочлен $f(x)$ не имеет корней в P, то он будет неприводимым в $P[x]$ и по теореме 4.37 данное уравнение неразрешимо в квадратных радикалах над P.

Если многочлен $f(x)$ имеет корень $c \in P$, то его можно разделить на $(x - c)$ и свести решение данного уравнения к квадратному уравнению, которое очевидно разрешимо в квадратных радикалах.

Рассмотрим теперь процедуру построения циркулем и линейкой. Её можно свести к последовательности действий следующего типа:

Д1) нахождение точки пересечения двух прямых;

Д2) нахождение точек пересечения прямой и окружности;

Д3) нахождение точек пересечения двух окружностей;

Д4) построение прямой, проходящей через две точки;

Д5) построение окружности с данным центром и проходящей через заданную точку.

Точка на плоскости задаётся своими двумя координатами, прямая задаётся своими двумя различными точками, окружность задаётся своим центром и некоторой точкой на ней. Будем говорить, что *точка на плоскости представима в квадратных радикалах над полем* P, если представимы в квадратных радикалах над полем P обе её координаты. Будем говорить, что *прямая представима в квадратных радикалах над полем* P, если представимы в квадратных радикалах над полем P две различные точки на ней. И, наконец, будем говорить, что *окружность представима в квадратных радикалах над полем* P, если представимы в квадратных радикалах над полем P её центр и какая-нибудь точка на ней.

4.39. Предложение. *а) Если прямая представима в квадратных радикалах над полем* P, *то она может быть задана уравнением вида* $ax+by=c$, *коэффициенты которого представимы в квадратных радикалах над* P.

б) Если окружность представима в квадратных радикалах над полем P, *то она может быть задана уравнением вида* $x^2+y^2+px+qy+r=0$, *коэффициенты которого представимы в квадратных радикалах над* P.

Доказательство. а) Пусть (x_1, y_1), (x_2, y_2) – две различные точки на данной прямой, представимые в квадратных радикалах над P. Тогда уравнение прямой может быть записано в виде $\dfrac{x-x_1}{x_2-x_1}=\dfrac{y-y_1}{y_2-y_1}$ или, после преобразований, в виде

$$(y_2-y_1)x+(x_2-x_1)y=x_1y_2-x_2y_1.$$

Коэффициенты последнего уравнения представимы в квадратных радикалах над P.

б) Пусть (x_0, y_0), (x_1, y_1) – соответственно центр окружности и точка на ней, представимые в квадратных радикалах над P. Уравнение данной окружности может быть записано в виде

$$(x - x_0)^2 + (y - y_0)^2 = (x_1 - x_0)^2 + (y_1 - y_0)^2$$

и после преобразований может быть приведено к требуемому виду.

4.40. Предложение. *Пусть дано множество M точек, прямых и окружностей на плоскости, представимых в квадратных радикалах над полем P. Если точка, прямая или окружность построена при помощи циркуля и линейки на основе множества M, то она также представима в квадратных радикалах над полем P.*

Доказательство. Для доказательства достаточно убедиться, что каждое из приведённых выше пяти действий сохраняет представимость в квадратных радикалах над полем P.

Действия Д4) и Д5) этому условию очевидно удовлетворяют. В случае Д1)–Д3) прямые и окружности можно задать уравнениями из предложения 4.39. Нахождение точки пересечения сведётся к решению системы одного из следующих видов:

$$\begin{cases} a_1 x + b_1 y = c_1, \\ a_2 x + b_2 y = c_2; \end{cases}$$

$$\begin{cases} a_1 x + b_1 y = c_1, \\ x^2 + y^2 + px + qy + r = 0; \end{cases}$$

$$\begin{cases} x^2 + y^2 + p_1 x + q_1 y + r_1 = 0, \\ x^2 + y^2 + p_2 x + q_2 y + r_2 = 0. \end{cases}$$

Коэффициенты этих систем представимы в квадратных радикалах над полем P.

Система первого типа решается методом исключения неизвестных, её решение выражается через коэффициенты и поэтому представимо в квадратных радикалах над полем P.

Система второго типа сводится к квадратному уравнению, её решение по формуле корней выражается через коэффициенты и квадратные корни из коэффициентов, и поэтому представимо в квадратных радикалах над полем P.

Система третьего типа после вычитания уравнений сводится к системе второго типа.

Строгое доказательство должно проводиться индукцией по количеству действий.

Теперь можно дать решение указанных выше задач.

4.41. Квадратура круга. *При помощи циркуля и линейки невозможно построить квадрат, равновеликий данному кругу.*

Пусть, напротив, эта задача разрешима. Возьмём радиус круга за единицу измерения и выберем прямоугольную декартову систему координат с началом в центре круга. Данная окружность представима в квадратных радикалах над полем рациональных чисел $\mathbb{Q}$, т.к. её центр имеет координаты $(0,0)$ и она содержит точку $(1,0)$.

Площадь круга равна π, поэтому сторона равновеликого квадрата равна $\sqrt{\pi}$. Отложим сторону этого квадрата по горизонтальной оси и построим точку $(\sqrt{\pi},0)$. Согласно предложению 4.40, число $\sqrt{\pi}$ представимо в квадратных радикалах над полем рациональных чисел, в частности является алгебраическим.

Однако известно, что число π и, следовательно, $\sqrt{\pi}$ являются трансцендентными (Линдеман, 1872). Противоречие.

4.42. Удвоение куба. *При помощи циркуля и линейки невозможно построить куб, объём которого в два раза больше объёма данного куба.*

Предполагается, что на плоскости дана сторона некоторого куба и нужно построить сторону куба вдвое большего объёма.

Пусть эта задача разрешима, тогда, как и выше, можно сторону данного куба взять за единицу измерения и выбрать систему координат, в которой рёбра куба параллельны осям, а одна из его вершин лежит в начале координат. Все его вершины будут иметь целые координаты, т.е., в частности, представимы в квадратных радикалах над полем рациональных чисел. По предложению 4.40 получится, что число $\sqrt[3]{2}$ представимо в квадратных радикалах над полем рациональных чисел. Это противоречит следствию 4.38, т.к. уравнение $x^3-2=0$ не имеет рациональных корней.

4.43. Трисекция угла. *При помощи циркуля и линейки невозможно разделить произвольный угол на три равные части.*

Укажем конкретный угол, который невозможно разделить на три равные части при помощи циркуля и линейки. Сначала рассмотрим задачу в общем виде. Пусть есть угол $\widehat{AOB}=\varphi$ (см. рис. 1) и угол $\widehat{AOB_1}=\frac{\varphi}{3}$.

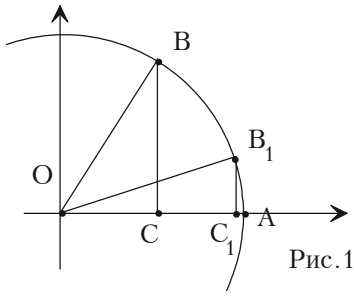

Рис.1

Задачу можно представить так. По точкам A, O, B построить точку B_1, или, что равносильно, по отрезку OC построить отрезок OC_1. Можно считать, что данная на рис. 1 окружность является единичной, тогда $OC=\cos\varphi$, $OC_1=\cos\frac{\varphi}{3}$, причём по формуле косинуса тройного угла

$$\cos\varphi=4\cos^3\left(\frac{\varphi}{3}\right)-3\cos\frac{\varphi}{3}.$$

Положим $\varphi = \frac{\pi}{3}$, тогда $\cos\varphi = \frac{1}{2}$ и число $\cos\frac{\varphi}{3} = \cos\frac{\pi}{9}$ является корнем многочлена третьей степени $f(x) = 4x^3 - 3x - \frac{1}{2}$.

Если задача трисекции для данного угла разрешима, то можно построить отрезок длины $\cos\frac{\pi}{9}$ и, согласно предложению 4.40, это число представимо в квадратных радикалах над полем рациональных чисел.

С другой стороны, легко проверить, что многочлен $f(x)$ не имеет рациональных корней, поэтому неприводим над $\mathbb{Q}$ и, по следствию 4.38, любой его корень не может быть представим в квадратных радикалах над $\mathbb{Q}$. Снова получилось противоречие, которое говорит о неразрешимости трисекции угла $\varphi = \frac{\pi}{3} = 60^\circ$.

Задачи для самостоятельного решения

1. Докажите, что являются алгебраическими над полем $\mathbb{Q}$ следующие числа:

а) $\alpha = \sqrt{5}$;

б) $\alpha = \sqrt[3]{7}$;

в) $\alpha = \sqrt{7} - 2$;

г) $\alpha = i + 1$;

д) $\alpha = \sqrt[3]{3} + 4$;

е) $\alpha = -1 + i\sqrt{3}$;

ж) $\alpha = \sqrt{5} - \sqrt{7}$;

з) $\alpha = 2\sqrt{3} + \sqrt{5}$;

и) $\alpha = \sqrt[3]{5} - \sqrt{2}$;

к) $\alpha = 3\sqrt{3} + \sqrt[3]{2}$;

л) $\alpha = \sqrt[4]{1 + \sqrt{2}}$;

м) $\alpha = \sqrt[3]{5} + 2\sqrt[3]{2}$;

н) $\frac{1}{\sqrt[3]{2} + \sqrt[3]{3}}$;

о) $\alpha = \cos\frac{5\pi}{8} + i\sin\frac{5\pi}{8}$.

2. Докажите, что:

а) число $\sqrt{2}+\sqrt{3}$ алгебраично над полем $\mathbb{Q}\left[\sqrt{2}\right]$;

б) число $\sqrt{3}+\sqrt[3]{3}$ алгебраично над полем $\mathbb{Q}\left[\sqrt{3}\right]$;

в) число $\sqrt{2}+i\sqrt[3]{5}-\sqrt{3}$ алгебраично над полем $\mathbb{Q}\left[\sqrt[3]{5}\right]$;

г) число $\sqrt[4]{2}$ алгебраично над полем $\mathbb{Q}\left[\sqrt{2}\right]$.

3. Найдите минимальный многочлен числа α над полем рациональных чисел $\mathbb{Q}$, если:

а) $\alpha=\sqrt{3}-2$; б) $\alpha=\sqrt{5}-\sqrt{3}$;

в) $\alpha=2\sqrt{5}-3\sqrt{2}$; г) $\alpha=\sqrt[3]{9}+2\sqrt[3]{3}$.

4. Докажите, что:

а) $\sqrt{7}\notin\mathbb{Q}\left[\sqrt{2}\right]$; б) $\sqrt{2}\notin\mathbb{Q}\left[\sqrt[3]{3}\right]$.

5. Найдите каноническое представление следующих чисел:

а) $\left(\sqrt{2}-1\right)^4$ в $\mathbb{Q}\left[\sqrt{2}\right]$;

б) $\left(\sqrt[3]{3}\right)^5-\left(\sqrt[3]{3}\right)^4-2\left(\sqrt[3]{3}\right)^2+3\left(\sqrt[3]{3}\right)+1$ в $\mathbb{Q}\left[\sqrt[3]{3}\right]$;

в) $\alpha^5-2\alpha^4+\alpha^3-3\alpha^2-4\alpha+1$ в $\mathbb{Q}[\alpha]$, если $m_\alpha(x)=x^3-x-1$;

г) $\alpha^6+2\alpha^4-3\alpha^3-\alpha^2-2\alpha+4$ в $\mathbb{Q}[\alpha]$, если $m_\alpha(x)=x^2-x+3$.

6. Избавьтесь от иррациональности в знаменателе дроби:

а) $\dfrac{1}{\sqrt{3}-1}$; б) $\dfrac{1}{\sqrt{5}+2}$;

в) $\dfrac{1}{\sqrt{5}+2\sqrt{3}}$; г) $\dfrac{1}{\sqrt[3]{3}-2}$;

д) $\dfrac{1}{2\sqrt[3]{5}+3}$;

е) $\dfrac{1}{2\sqrt[3]{9}-\sqrt[3]{3}+1}$;

ж) $\dfrac{1}{\sqrt[3]{4}-\sqrt[3]{2}+2}$;

з) $\dfrac{7}{1-\sqrt[4]{2}+\sqrt{2}}$;

и) $\dfrac{1}{1+\sqrt{2}-\sqrt{3}}$;

к) $\dfrac{23}{1+\sqrt[3]{2}+2\sqrt[3]{4}}$.

7. Избавьтесь от иррациональности в знаменателе дроби:

а) $\dfrac{1}{\alpha^2+2}$, где $\alpha^3+\alpha+1=0$;

б) $\dfrac{1}{\alpha^2+\alpha+1}$, где $\alpha^3-2\alpha+2=0$;

в) $\dfrac{1}{\alpha^2+\alpha+1}$, где $\alpha^3+2\alpha^2-1=0$;

г) $\dfrac{1}{3\alpha^3+\alpha^2-2\alpha-1}$, где $\alpha^4-\alpha^3+2\alpha+1=0$.

8. Избавьтесь от иррациональности в знаменателе следующих дробей и найдите их каноническое представление в расширении $\mathbb{Q}[\alpha]$:

а) $\dfrac{17\alpha^2}{\alpha^4+1}$, где $\alpha^4+2\alpha+2=0$;

б) $\dfrac{13\alpha}{\alpha^3+5}$, где $\alpha^3-2\alpha+2=0$;

в) $\dfrac{\alpha^2-3\alpha-1}{\alpha^2+2\alpha+1}$, где $\alpha^3+\alpha^2+3\alpha+4=0$.

9. Даны минимальные многочлены $m_\alpha(x), m_\beta(x)\in\mathbb{Q}[x]$ алгебраических чисел α и β. Пользуясь доказательством теоремы о том, что алгебраические числа образуют поле, найдите многочлены с рациональными коэффициентами, корнями которых являются числа c_1 и c_2:

а) $m_\alpha(x)=x^2+x+1$, $m_\beta(x)=x^2+2x+3$, $c_1=-\alpha$, $c_2=\alpha+\beta$;

б) $m_\alpha(x)=x^3-2$, $m_\beta(x)=x^2-5$, $c_1=\dfrac{1}{\alpha}$, $c_2=\alpha\beta$;

в) $m_\alpha(x)=x^3-2$, $m_\beta(x)=x^2-3x+1$, $c_1=\sqrt[3]{\beta}$, $c_2=\alpha+\beta$;

г) $m_\alpha(x)=x^3+x+1$, $m_\beta(x)=x^2+2x+3$, $c_1=-\dfrac{1}{\alpha}$, $c_2=\alpha\beta$;

д) $m_\alpha(x)=x^3+x+1$, $m_\beta(x)=x^2-5$, $c_1=-\sqrt[5]{\alpha}$, $c_2=\alpha+\beta$.

10. Пусть β,γ – трансцендентные числа, а числа a,b – алгебраические. Определите, какие из следующих чисел обязательно будут трансцендентными, какие алгебраическими, а какие могут быть как трансцендентными, так и алгебраическими:

$$a+b,\ a+\beta,\ a\beta,\ \frac{\beta}{a},\ \sqrt{a},\ \sqrt{\beta},\ \beta+\gamma,\ \beta\gamma,\ \frac{\beta}{\gamma},\ a^n,\ \beta^n,\ ab.$$

11. Найдите размерность и базис расширения:

а) $\mathbb{Q}\left(\sqrt[5]{5}\right)$ над $\mathbb{Q}$;

б) $\mathbb{Q}\left(\sqrt{3}\right)\left(\sqrt{5}\right)$ над $\mathbb{Q}\left(\sqrt{3}\right)$;

в) $\mathbb{C}$ над $\mathbb{R}$;

г) $\mathbb{Q}\left(\sqrt[3]{3}\right)\left(\sqrt{3}\right)\left(\sqrt[4]{3}\right)$ над $\mathbb{Q}$;

д) $\mathbb{Q}\left(\sqrt[3]{3}\right)\left(\sqrt[4]{3}\right)\left(\sqrt{3}\right)$ над $\mathbb{Q}$.

12. Докажите, что выполняется равенство $\mathbb{Q}\left(\sqrt[3]{p}\right)\left(\sqrt[3]{q}\right)=\mathbb{Q}\left(\sqrt[3]{p}+\sqrt[3]{q}\right)$. Выразите в поле $\mathbb{Q}\left(\sqrt[3]{p}+\sqrt[3]{q}\right)$ число $\sqrt[3]{p}$ через $\left(\sqrt[3]{p}+\sqrt[3]{q}\right)$ (найдите каноническое представление), если:

а) $p=3,\ q=7$;

б) $p=5,\ q=12$.

13. Найдите многочлен с рациональными коэффициентами, корнем которого является число:

а) $\sqrt[3]{4}+3\sqrt[3]{2}+2$;

б) $2\sqrt[3]{4}+\sqrt[3]{2}+1$;

в) $\sqrt[3]{16}+2\sqrt[3]{4}-1$; г) $3\sqrt[3]{16}+\sqrt[3]{4}-2$.

14. Известно, что число α является корнем многочлена $f(x)\in\mathbb{Q}[x]$. Найдите многочлен с рациональными коэффициентами, корнем которого является число β, если:

а) $f(x)=x^2+2x+2,\ \beta=\alpha^2+1$;

б) $f(x)=x^2+x+3,\ \beta=\alpha^2+\alpha+1$;

в) $f(x)=x^3+2x^2+2,\ \beta=\alpha^2+1$;

г) $f(x)=x^3-x+2,\ \beta=\alpha^2+\alpha$;

д) $f(x)=x^3-x^2-2x+1,\ \beta=-\alpha^2+2$.

ГЛАВА 5. КОНЕЧНЫЕ ПОЛЯ

§1. Характеристика поля. Конечные поля

Конечные поля находят применение в таких весьма важных прикладных разделах алгебры, как теория кодирования и криптография. При описании и классификации конечных полей одним из основных параметров является характеристика поля. Во второй главе было показано (2.61, 2.62), что *характеристика поля – это аддитивный порядок ненулевых элементов поля.*

5.1. Теорема. *Характеристика конечного поля не может равняться нулю. Если поле не является полем характеристики 0, то его характеристика – простое число.*

Доказательство. Рассмотрим все элементы вида $n*1$. Так как поле конечно, то эти элементы не могут быть попарно различными. Следовательно, существуют такие натуральные $n>m$, что $n*1=m*1$. Перенеся всё в левую часть и применив свойство кратных 2.12.г), получим $(n-m)*1=0$. Из этого равенства следует, что характеристика не может равняться нулю.

Пусть характеристика поля равна p и, напротив, $p=nm$ для некоторых натуральных чисел $n<p, m<p$. Тогда

$$0=p*1=(nm)*1 \overset{2.12.б)}{=} n*(m*1).$$

Если $m*1\neq 0$, то аддитивный порядок элемента $m*1$ меньше p, что противоречит условию. Если $m*1=0$, то аддитивный порядок элемента $1\neq 0$ меньше p, что также противоречит условию. Теорема доказана.

5.2. Следствие. *Пусть P – поле характеристики $p\neq 0$. а) Для любых элементов $a,b\in P$ и любого натурального k справедливы равенства*:

$$(a+b)^{p^k}=a^{p^k}+b^{p^k},\ (a-b)^{p^k}=a^{p^k}-b^{p^k}.$$

б) Для любого многочлена $f(x)=a_nx^n+\ldots+a_1x+a_0$ *с коэффициентами из* P *справедливо равенство*

$$\left(f(x)\right)^{p^k}=\left(a_nx^n\right)^{p^k}+\ldots+\left(a_1x\right)^{p^k}+\left(a_0\right)^{p^k}.$$

Доказательство. а) Пусть $k=1$. Применим бином Ньютона:

$$(a+b)^p=\sum_{i=0}^{p}C_p^ia^{p-i}b^i.$$

При $i\neq 0,p$ биномиальные коэффициенты $C_p^i=\dfrac{p(p-1)\ldots(p-i+1)}{1\cdot 2\cdot 3\cdot\ldots\cdot i}$ содержат простой сомножитель p, который не может сократиться, т.к. в знаменателе все простые сомножители меньше p. Поле имеет характеристику p, поэтому $C_p^ia^{p-i}b^i=0$ при $i\neq 0,p$, и в результате в биноме Ньютона останутся только первое и последнее слагаемое: $(a+b)^p=a^p+b^p$.

Аналогично $(a-b)^p=a^p+(-1)^pb^p$. Если p – нечётное число, то $(a-b)^p=a^p+(-1)^pb^p=a^p-b^p$. Если $p=2$, то в таком поле $c=-c$ для любого $c\in P$, поэтому

$$(a-b)^p=a^p+(-1)^pb^p=a^p+b^p=a^p-b^p.$$

Для произвольного k доказательство следствия проводится по индукции.

б) Доказательство аналогично доказательству а).

5.3. Определение. Поле называется *простым*, если оно не содержит собственных подполей.

Как следует из определения, простые поля – это в некотором смысле самые «маленькие» и самые «простые» поля. Класс простых полей легко поддаётся описанию.

5.4. Теорема. *Поле является простым тогда и только тогда, когда оно изоморфно полю* $\mathbb{Z}_p$ *для некоторого простого* p *или полю* $\mathbb{Q}$ *рациональных чисел.*

Доказательство. Пусть P – простое поле.

1-й случай: поле P имеет характеристику p для некоторого простого p.

Пользуясь свойствами кратных, легко доказать, что для любых целых n, m, k:

1) $n*1 = m*1 \Leftrightarrow n \equiv m \pmod p$;

2) $(n*1)+(m*1) = k*1 \Leftrightarrow n+m \equiv k \pmod p$;

3) $(n*1)(m*1) = k*1 \Leftrightarrow nm \equiv k \pmod p$.

Докажем, например, 3). Во-первых замечаем, что

$$(n*1)(m*1) \overset{2.12.е)}{=} n*(1(m*1)) = n*(m*1) \overset{2.12.б)}{=} (nm)*1.$$

Воспользовавшись этим, получаем, что $(n*1)(m*1) = k*1$ тогда и только тогда, когда $(nm)*1 = k*1$, а это, согласно пункту 1), равносильно сравнению $nm \equiv k \pmod p$.

Затем определяем отображение $f : \mathbb{Z}_p \to P$ по правилу:

$$f([n]_p) = n*1,$$

где $[n]_p$ – класс вычетов числа n по модулю p.

Свойство 1) гарантирует, что это отображение будет взаимно однозначным, а свойства 2), 3) соответственно – что будут сохраняться операции сложения и умножения. Таким образом, поле P содержит изоморфную копию $f(\mathbb{Z}_p)$ поля $\mathbb{Z}_p$ в качестве подполя. В силу простоты поля P получаем, что $P = f(\mathbb{Z}_p) \cong \mathbb{Z}_p$.

2-й случай: поле P имеет характеристику 0.

В этом случае элементы вида $n*1 \in P$ будут попарно различными. Пользуясь свойствами кратных 2.12 опять доказываем, что для любых целых n, m :

1) $n*1 = m*1 \Leftrightarrow n = m$;

2) $(n*1)+(m*1)=(n+m)*1$;

3) $(n*1)(m*1)=(nm)*1$.

Действительно, если $n > m$ и $n*1 = m*1$, то $(n-m)*1 = 0$ и это противоречит тому, что характеристика поля равна 0. Свойство 2) – это частный случай свойства 2.12.а) кратных. Доказательство свойства 3) дано при рассмотрении случая 1.

После этого определяем отображение $f : \mathbb{Z} \to P$ по правилу:

$$f(n) = n*1 .$$

Свойство 1) гарантирует, что это отображение будет взаимно однозначным, а свойства 2), 3) соответственно – что будут сохраняться операции сложения и умножения. Таким образом, поле P содержит кольцо $f(\mathbb{Z})$, изоморфное кольцу $\mathbb{Z}$, а следовательно, и поле частных кольца $f(\mathbb{Z})$. Поскольку поле частных любого кольца без делителей нуля единственно с точностью до изоморфизма и полем частных кольца $\mathbb{Z}$ является поле $\mathbb{Q}$, то P содержит подполе F, изоморфное полю $\mathbb{Q}$. Ввиду простоты поля P имеем $P = F \cong \mathbb{Q}$.

5.5. Следствие. *Всякое конечное поле характеристики p содержит простое подполе, состоящее из p элементов.*

5.6. Теорема (о количестве элементов в конечном поле). *Всякое конечное поле F характеристики p содержит $q = p^k$ элементов, где k – некоторое натуральное число.*

Доказательство. Выберем в F простое подполе P из p элементов. Рассмотрим расширение $P \subseteq F$. В силу конечности F

оно является *конечным* (конечномерным) расширением поля P некоторой размерности $k \in \mathbb{N}$.

Пусть $\beta_1, \beta_2, \ldots, \beta_k$ – произвольный базис этого расширения. Каждый элемент поля F единственным образом представим в виде линейной комбинации:

$$a_1\beta_1 + a_2\beta_2 + \ldots + a_k\beta_k,$$

где $a_1, a_2, \ldots, a_k \in P$. Так как $|P| = p$, то таких линейных комбинаций ровно p^k штук. Теорема доказана.

5.7. Следствие. *Порядок конечного поля является степенью порядка любого его подполя. Другими словами, если* $P \le F$ *и* $|P| = q = p^m$, *то* $|F| = q^k$, *причём* $k = \dim(F/P)$.

Доказательство. Если $P \le F$ и $|P| = q$, то, как и в доказательстве теоремы 5.6, получаем, что поле F является конечным расширением поля P некоторой размерности k и $|F| = q^k$.

5.8. Теорема (критерий конечного подполя для полей характеристики p). *Конечное подмножество M поля характеристики p является его подполем тогда и только тогда, когда оно содержит хотя бы один ненулевой элемент и замкнуто относительно сложения и умножения.*

Доказательство. Замкнутость относительно взятия противоположного можно опустить, т.к. вычисление противоположного в поле характеристики p сводится к сложению. Действительно, т.к. $p * a = 0$, то $a + (p-1) * a = 0$ и, следовательно, $-a = (p-1) * a$.

Замкнутость относительно взятия обратного также можно опустить, т.к. вычисление обратного сводится к умножению. Действительно, если M замкнуто относительно умножения и конечно, то (мультипликативный) порядок любого элемента $a \in M$ также конечен и тогда $a^{-1} = a^{ord(a)-1}$.

5.9. Обозначение. Конечные поля обычно называют *полями Галуа* и обозначают $GF(q)$ или, для краткости, F_q. Ниже всегда будет предполагаться, что q является степенью некоторого простого числа: $q = p^k$, которое является характеристикой поля.

Рассмотрим мультипликативную группу ненулевых элементов $F_q^* = F_q \setminus \{0\}$ поля Галуа. Порядок этой группы равен $q-1$. *Порядок элемента поля* $a \in F_q$ определяется как его (мультипликативный) порядок в группе F_q^*.

5.10. Определение. Элемент $a \in F_q$ называется *примитивным элементом поля* F_q, если все ненулевые элементы поля являются степенями этого элемента.

Равносильными условиями являются:

а) элемент a порождает мультипликативную группу F_q^*;

б) $ord(a) = q-1$.

5.11. Теорема (о примитивном элементе). *Во всяком конечном поле* F_q *существует примитивный элемент.*

Доказательство. Мультипликативная группа F_q^* является конечной абелевой группой. По теореме 2.18 об экспоненте конечной группы существует такой элемент $a \in F_q^*$, что $ord(a) = \exp F_q^*$. Это означает, что любой элемент $b \in F_q^*$ удовлетворяет равенству $b^{ord(a)} = 1$ или, другими словами, всякий элемент $b \in F_q^*$ является корнем ненулевого многочлена $f(x) = \left(x^{ord(a)} - 1\right)$. Если $ord(a) < \left|F_q^*\right| = q-1$, то многочлен $f(x)$ имеет корней больше, чем его степень, что невозможно, согласно теореме 3.18. Следовательно, $ord(a) = q-1$ и a является примитивным элементом данного поля.

5.12. Следствие. *Мультипликативная группа поля Галуа является циклической.*

5.13. Следствие (тождество Ферма). *Все ненулевые элементы поля* F_q *удовлетворяют тождеству* $a^{q-1}=1$. *Все элементы поля* F_q *удовлетворяют тождеству* $a^q=a$. *Или, более общо, тождеству* $a^{qs}=a^s$ *для любого натурального* s.

5.14. Замечание. Из свойства порядка 2.16.4) следует, что *если* a *является примитивным элементом поля* F_q, *то примитивными являются также все элементы вида* a^k, *где* $НОД(k,q-1)=1$. Таких элементов $\varphi(q-1)$ штук.

Используя свойства порядков, можно также доказать

5.15. Теорему (о количестве элементов данного порядка в поле). *Если* m *– натуральный делитель числа* $q-1$, *то число элементов порядка* m *в поле* F_q *равно* $\varphi(m)$.

§2. Универсальная конструкция для построения конечных полей

Пусть P – произвольное поле. Рассмотрим кольцо многочленов $P[x]$ и возьмём в нём произвольный многочлен $f(x)$. Идеал, порождённый этим многочленом, состоит из многочленов, делящихся на $f(x)$, и может быть записан как $I=f(x)P[x]$. Рассмотрим фактор-кольцо кольца $P[x]$ по этому идеалу. Оно обычно обозначается как $P[x]/f(x)$. Фактор-кольцо состоит из классов эквивалентности вида

$$\left[a(x)\right]_{f(x)}=\left\{b(x)\in P[x] \;\middle|\; a(x)-b(x)\in f(x)P[x]\right\}=$$

$$=\left\{b(x)\in P[x] \;\middle|\; a(x)-b(x)\vdots f(x)\right\},$$

где $a(x)\in P[x]$. Другими словами, $\left[a(x)\right]_{f(x)}=a(x)+I$.

Если $f(x)=0$, то $a(x)-b(x)\in 0P[x]=\{0\}$ тогда и только тогда, когда $a(x)=b(x)$. Поэтому $P[x]/0=P[x]$.

Если $f(x)=f\in P, f\neq 0$, то $f\cdot P[x]=P[x]$ и соотношение $a(x)-b(x)\in f\cdot P[x]$ выполняется для любых многочленов $a(x),b(x)\in P[x]$. В этом случае $P[x]/f$ – кольцо из одного элемента.

Если $cm(f(x))=n>0$, то, взяв произвольный многочлен $a(x)$ из $P[x]$, можно разделить его с остатком на $f(x)$ и получить, что $a(x)=f(x)q(x)+r(x)$, причём либо $r=0$, либо $cm(r(x))<n$. Так как $a(x)-r(x)\in I=f(x)P[x]$, то в каждом классе эквивалентности либо есть нулевой элемент, либо многочлен степени меньшей, чем степень $f(x)$. Такой элемент в каждом классе единственен, т.к. разность двух различных многочленов степени меньше $cm(f(x))$ не может делиться на $f(x)$.

В результате, фактор-кольцо представимо в виде

$$P[x]/f(x)=\left\{\left[a_{n-1}x^{n-1}+\ldots+a_1x^1+a_0\right]_{f(x)}\,\middle|\,a_i\in P\right\}.$$

Если $|P|<\infty$, то $|P[x]/f(x)|=|P|^n$.

Данная конструкция используется как (универсальный) способ для построения конечных полей ввиду следующей теоремы.

5.16. Теорема. *Если $f(x)$ – многочлен положительной степени над некоторым полем P, то фактор-кольцо $P[x]/f(x)$ является полем тогда и только тогда, когда многочлен $f(x)$ неприводим над P.*

Доказательство. $\boxed{\Rightarrow}$ Пусть, напротив, кольцо $P[x]/f(x)$ является полем, но $f(x)=u(x)v(x)$, $u(x),v(x)\in P[x]$ и

$cm(u) < cm(f)$, $cm(v) < cm(f)$. В кольце $P[x]/f(x)$ будет выполняться равенство

$$\left[u(x)\right]_{f(x)}\left[v(x)\right]_{f(x)} = \left[f(x)\right]_{f(x)} = 0,$$

из которого следует, что в нём есть делители нуля, т.к. $\left[u(x)\right]_{f(x)}, \left[v(x)\right]_{f(x)} \neq 0$. Противоречие.

$\boxed{\Leftarrow}$ Пусть многочлен $f(x)$ неприводим над P и $\left[g(x)\right]_{f(x)} \neq 0$ произвольный ненулевой элемент кольца $P[x]/f(x)$. Для доказательства достаточно доказать существование обратного элемента.

Так как $\left[g(x)\right]_{f(x)} \neq 0 = \left[f(x)\right]_{f(x)}$, то многочлен $g(x)$ не делится на $f(x)$. Так как $f(x)$ неприводим, то многочлены $f(x)$ и $g(x)$ взаимно просты (3.36). Следовательно, существуют такие многочлены $u(x), v(x)$ из $P[x]$, что

$$g(x)u(x) + f(x)v(x) = 1.$$

Переходя к фактор-кольцу $P[x]/f(x)$, получаем:

$$\left[g(x)\right]_{f(x)}\left[u(x)\right]_{f(x)} + \left[f(x)\right]_{f(x)}\left[v(x)\right]_{f(x)} =$$

$$= \left[g(x)\right]_{f(x)}\left[u(x)\right]_{f(x)} + 0\left[v(x)\right]_{f(x)} = \left[g(x)\right]_{f(x)}\left[u(x)\right]_{f(x)} = 1.$$

В результате $\left(\left[g(x)\right]_{f(x)}\right)^{-1} = \left[u(x)\right]_{f(x)}$.

Теорема доказана.

5.17. Замечание (о том, что фактор-кольцо совпадает с простым алгебраическим расширением).

1) Всякий элемент кольца $P[x]/f(x)$ однозначно представим в виде

$$a_{n-1}x^{n-1} + \ldots + a_1x^1 + a_0 + I,\ a_i \in P,\ n = cm(f).$$

2) Кольцо $P[x]/f(x)$ содержит в качестве подкольца изоморфную копию $P_1 = \{a + I \mid a \in P\}$ поля P.

Можно заменить P_1 на P, переопределить операции на множестве $\left(\left(P[x]/f(x)\right) \setminus P_1\right) \cup P$ и получить кольцо, содержащее P в явном виде в качестве подкольца (см., например, [2]).

Ввиду этого можно считать, что фактор-кольцо $P[x]/f(x)$ содержит поле P в качестве подкольца.

3) Обозначим $\beta = x + I$. Тогда, пользуясь определением идеала, получаем, что всякий элемент кольца $P[x]/f(x)$ однозначно представим в виде:

$$a_{n-1}x^{n-1} + \ldots + a_1 x^1 + a_0 + I =$$

$$= a_{n-1}(x + I)^{n-1} + \ldots + a_1 (x + I)^1 + a_0 =$$

$$= a_{n-1}\beta^{n-1} + \ldots + a_1\beta + a_0,\ a_i \in P.$$

Это представление будет называться *каноническим*. Кроме того, элемент $\beta \in P[x]/f(x)$ является корнем многочлена $f(x)$. Действительно, если

$$f(x) = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_1 x^1 + b_0,\ b_i \in P,$$

то

$$f(\beta) = b_n\beta^n + b_{n-1}\beta^{n-1} + \ldots + b_1\beta^1 + b_0 =$$

$$= b_n (x + I)^n + b_{n-1}(x + I)^{n-1} + \ldots + b_1 (x + I)^1 + b_0 =$$

$$= b_n x^n + b_{n-1}x^{n-1} + \ldots + b_1 x^1 + b_0 + I = f(x) + I = 0 + I.$$

С учётом замечания 5.17.2), можно считать, что коэффициенты многочлена $f(x)$ принадлежат $P \subseteq P[x]/f(x)$.

В результате доказана

5.18. Теорема (о строении фактор-кольца). *Для любого поля P и любого неприводимого над P многочлена $f(x) \in P[x]$ степени n существует такое поле F, а в нём такой элемент β, что $F = P(\beta)$ и $f(\beta) = 0$. Кроме того, если поле P – конечно, то поле F также конечно и $|F| = |P|^n$.*

Данная теорема позволяет в реальных вычислениях использовать для представления элементов не классы эквивалентности, а многочлены от β степени меньше n с коэффициентами из P:

$$\gamma = a_{n-1}\beta^{n-1} + \ldots + a_1\beta + a_0 .$$

Такое представление для каждого элемента $\gamma \in P[x]/f(x)$ единственно, согласно теореме 4.10 о каноническом представлении. Все вычисления осуществляются «по модулю $f(x)$». Для этого используется теорема о делении с остатком и равенство $f(\beta) = 0$.

5.19. Следствие (Кронекер). *Для любого поля P и любого многочлена $f(x) \in P[x]$ положительной степени существует поле F, содержащее поле P и корень β многочлена $f(x)$.*

Достаточно взять каноническое разложение многочлена $f(x)$ на неприводимые над P сомножители

$$f(x) = b_n g_1(x)^{k_1} g_2(x)^{k_2} \cdot \ldots \cdot g_s(x)^{k_s} ,$$

один из неприводимых многочленов $g_i(x)$, и построить фактор-кольцо $F = P[x]/g_i(x)$. Согласно теореме 5.18, $F = P(\beta)$, а β – один из корней многочлена $g_i(x)$ и, следовательно, многочлена $f(x)$.

Следующая теорема говорит о том, что конструкции фактор-поля и простого алгебраического расширения являются универсальными для построения конечных полей.

5.20. Теорема. *Всякое конечное поле F является простым алгебраическим расширением любого своего подполя P при помощи корня неприводимого многочлена.*

Действительно, пусть $P \subseteq F$. Пусть β – примитивный элемент поля F. Тогда очевидно, что $P(\beta) \subseteq F$. С другой стороны, поле $P(\beta)$ содержит 0 и все степени элемента β, а значит, и все элементы поля F. В результате $P(\beta) = F$. Так как расширение F/P конечномерно, то (согласно 4.18) всякий его элемент является алгебраическим. Взяв минимальный многочлен для элемента β, получим неприводимый многочлен $f(x) \in P[x]$ с условием $f(\beta) = 0$. Размерность расширения F/P совпадает со степенью n этого минимального многочлена.

В результате для случая $P \subseteq F$ всегда будет иметь место следующая ситуация:

1) $P = F_q$;

2) $F = F_{q^n} = F_q(\beta)$ – конечное расширение поля F_q при помощи алгебраического над F_q элемента β степени n;

3) базис пространства F_{q^n} над полем $F_q(\beta)$ состоит из степеней β:

$$1, \beta^1, \beta^2, \ldots, \beta^{n-1};$$

4) всякий элемент $\gamma \in F_{q^n}$ единственным образом линейно выражается через этот базис (*каноническое представление*):

$$\gamma = c_{n-1}\beta^{n-1} + c_{n-2}\beta^{n-2} + \ldots + c_1\beta + c_0,\ c_i \in F_q.$$

5.21. Алгоритмы вычислений в конечных полях. Пусть $F = P(\beta)$ – конечное поле, являющееся простым алгебраическим расширением своего подполя P. Пусть $f(x)$ – минимальный многочлен элемента β и пусть $cm(f) = n$. Произвольные

элементы γ_1, γ_2 из поля F имеют вид $\gamma_1 = g_1(\beta)$, $\gamma_2 = g_2(\beta)$, где $g_1(x), g_2(x) \in P[x]$ и $cm(g_1) < cm(f)$, $cm(g_2) < cm(f)$.

1) Для вычисления $\gamma_1 \pm \gamma_2$ достаточно в выражении $g_1(\beta) \pm g_2(\beta)$ привести подобные члены.

2) Чтобы найти каноническое представление произведения $\gamma_1\gamma_2 = g_1(\beta)g_2(\beta)$, нужно многочлен $g_1(x)g_2(x)$ разделить в кольце $P[x]$ на многочлен $f(x)$ с остатком:

$$g_1(x)g_2(x) = f(x)h(x) + r(x),$$

$r(x) = 0$ или $cm(r) < cm(f) = n$, и подставить в полученное равенство $x = \beta$. Тогда

$$\gamma_1\gamma_2 = g_1(\beta)g_2(\beta) = \underbrace{f(\beta)}_{=0}h(\beta) + r(\beta) = r(\beta)$$

– искомое представление.

3) Для вычисления частного

$$\frac{\gamma_1}{\gamma_2} = \frac{g_1(\beta)}{g_2(\beta)} = g_1(\beta)\Big(g_2(\beta)\Big)^{-1},\ g_2(\beta) \neq 0,$$

достаточно вычислить $\Big(g_2(\beta)\Big)^{-1}$ и умножить его на $g_1(\beta)$.

4) Для вычисления обратного элемента можно воспользоваться расширенным алгоритмом Евклида. Так как $g_2(\beta) \neq 0$, то многочлен $g_2(x)$ не делится на $f(x)$. Так как многочлен $f(x)$ неприводим, то многочлены $f(x)$ и $g_2(x)$ взаимно просты (см. 3.36). Следовательно (см. 3.31), существуют такие многочлены $u(x), v(x) \in P[x]$, что

$$f(x)u(x) + g_2(x)v(x) = 1.$$

Если подставить в это равенство элемент β, то получим

$$\underbrace{f(\beta)}_{=0}u(\beta) + g_2(\beta)v(\beta) = g_2(\beta)v(\beta) = 1,$$

откуда $\left(g_2(\beta)\right)^{-1} = v(\beta)$.

5) Для вычисления обратного элемента можно воспользоваться методом неопределённых коэффициентов, подставив в определение обратного $g_2(\beta)v(\beta)=1$ его каноническое представление с неопределёнными коэффициентами:

$$v(\beta) = c_{n-1}\beta^{n-1} + c_{n-2}\beta^{n-2} + \ldots + c_1\beta + c_0,\ c_i \in P.$$

Если привести после этого правую часть равенства к каноническому виду, то можно, в силу единственности, приравнять коэффициенты при одинаковых степенях β слева и справа и найти $c_i \in P$ из полученной системы.

5.22. Пример. Пусть $f(x) = x^3 + 2x + 1 \in F_3[x]$. Он неприводим над F_3, т.к. не имеет в F_3 корней. Пусть β – один из его корней в поле $F_{3^3} = F_3(\beta)$. Вычислить сумму, разность и частное элементов $\gamma_1 = \beta + 1$ и $\gamma_2 = \beta^2 + \beta + 2$.

Ясно, что

$$\gamma_1 + \gamma_2 = (\beta + 1) + \left(\beta^2 + \beta + 2\right) = \beta^2 + 2\beta;$$

$$\gamma_1 - \gamma_2 = (\beta + 1) - \left(\beta^2 + \beta + 2\right) = -\beta^2 - 1 = 2\beta^2 + 2.$$

Напомним рекуррентную схему вычисления сомножителя $u(x)$ из тождества Безу в расширенном алгоритме Евклида (см. 1.24):

$$f(x)u(x) + g_2(x)v(x) = 1.$$

1) Сначала вычисляем последовательность Евклида: $r_{-1}(x) = f(x), r_0(x) = g_2(x), r_1(x), r_2(x), \ldots$

2) Затем каждый её элемент выражаем через многочлены $f(x)$ и $g_2(x)$:

$$f(x)u_k(x) + g_2(x)v_k(x) = r_k(x).$$

Последний ненулевой остаток r_n ассоциирован с *НОД* и имеет нулевую степень, поэтому делим равенство почленно на r_n и получаем тождество Безу:

$$f(x)\left(\frac{u_n(x)}{r_n}\right)+g_2(x)\left(\frac{v_n(x)}{r_n}\right)=1.$$

3) При этом если два соседних сомножителя $v_{k-2}(x)$ и $v_{k-1}(x)$ найдены, то следующий сомножитель $v_k(x)$ вычисляется по правилу:

$$v_k(x)=v_{k-2}(x)-v_{k-1}(x)q_k(x),$$

где $q_k(x)$ – частное на k-м шаге алгоритма Евклида. Сомножители $u_k(x)$ вычисляются аналогично, хотя их можно не вычислять, т.к. они не влияют на искомый обратный элемент.

4) Так как

$$f(x)\cdot 1+g_2(x)\cdot 0=f(x),\ f(x)\cdot 0+g_2(x)\cdot 1=g_2(x),$$

то можно считать, что $v_{-1}(x)=0, v_0(x)=1$, и остальные сомножители $v_k(x)$ вычислить, используя правило из п. 3).

В нашем примере получится следующее.

$$\begin{array}{r|l} x^3+2x+1 & x^2+x+2 \\ \underline{-\,x^3+x^2+2x} & \underbrace{x+2}_{q_1(x)} \\ -2x^2+1 & \\ \underline{-\,2x^2+2x+1} & \\ x & \end{array}$$

$$v_1(x)=v_{-1}(x)-v_0(x)q_1(x)=0-1\cdot(x+2)=2x+1;$$

$$x^2+x+2=\underbrace{x(x+1)}_{q_2(x)}+\underbrace{2}_{r_2(x)},$$

$$v_2(x)=1-(2x+1)(x+1)=x^2.$$

В результате $\left(\beta^2+\beta+2\right)\left(\beta^2\right)=2$ и, следовательно,

$$\left(\beta^2+\beta+2\right)^{-1}=\frac{\beta^2}{2}=2\beta^2.$$

Сделаем проверку: $\left(\beta^2+\beta+2\right)\left(2\beta^2\right)=1$. При умножении воспользуемся тем, что $f(\beta)=\beta^3+2\beta+1=0$ или $\beta^3=-2\beta-1=\beta+2$:

$$\left(\beta^2+\beta+2\right)\left(2\beta^2\right)=2\beta^4+2\beta^3+\beta^2=$$

$$=2\beta(\beta+2)+2(\beta+2)+\beta^2=\cancel{2\beta^2}+\cancel{4\beta}+\cancel{2\beta}+4+\cancel{\beta^2}=1.$$

Обратный элемент можно также находить методом неопределённых коэффициентов. Для этого искомый обратный элемент запишем в каноническом виде с неопределёнными коэффициентами $a\beta^2+b\beta+c$, $a,b,c\in F_3$, и подставим в определение обратного элемента:

$$\left(\beta^2+\beta+2\right)\left(a\beta^2+b\beta+c\right)=1.$$

Раскрываем скобки и приводим подобные члены:

$$a\beta^4+(a+b)\beta^3+(2a+b+c)\beta^2+(2b+c)\beta+2c=1.$$

Затем приводим левую (и правую) часть последнего равенства к каноническому виду:

$$a\beta(\beta+2)+(a+b)(\beta+2)+(2a+b+c)\beta^2+(2b+c)\beta+2c=1,$$

$$(3a+b+c)\beta^2+(3a+3b+c)\beta+2c+2a+2b=1,$$

$$(b+c)\beta^2+c\beta+2c+2a+2b=1=0\beta^2+0\beta+1.$$

Из единственности канонической формы следует равенство коэффициентов при степенях β слева и справа в равенстве:

$$\Leftrightarrow \begin{cases} b+c=0, \\ c=0, \\ 2c+2a+2b=1; \end{cases} \Leftrightarrow \begin{cases} b=0, \\ c=0, \\ a=2. \end{cases}$$

Обратный элемент, естественно, получился таким же, как и в предыдущем решении:

$$a\beta^2+b\beta+c=2\beta^2 .$$

Наконец, после этого вычисляем частное:

$$\frac{\gamma_1}{\gamma_2}=\frac{\beta+1}{\beta^2+\beta+2}=(\beta+1)2\beta^2=2\beta^3+2\beta^2=$$

$$=2(\beta+2)+2\beta^2=2\beta^2+2\beta+1 .$$

5.23. Пример. Пусть, как и в предыдущем примере, $f(x)=x^3+2x+1\in F_3[x]$ и β – один из его корней в поле $F_{3^3}=F_3(\beta)$. Вычислить порядок β.

Согласно свойствам порядков (см. 2.32), можно утверждать, что порядок элемента должен быть делителем порядка мультипликативной группы $\left(F_{3^3}\right)^*$, который равен $3^3-1=26$, т.е. может оказаться равным 1, 2, 13 и 26. Согласно теореме 5.15, элементов порядка 1 всего $\varphi(1)=1$ штук. Очевидно, этим элементом является единица. Элементов порядка 2 будет ровно $\varphi(2)=1$. Очевидно – это элемент $(-1)=2$. Элементов порядков 13 и 26 будет по $\varphi(13)=\varphi(26)=12$ штук.

Начнём последовательно вычислять степени β, приводить их к каноническому виду $\beta^k=a_k\beta^2+b_k\beta+c_k$ и проверять равенство $\beta^k=1$. Так как мы перебираем степени подряд, начиная с единицы, то первое натуральное k, удовлетворяющее условию $\beta^k=1$, и будет искомым порядком. Чтобы получить каноническое представление для степени β^{k+1}, достаточно равенство для β^k умножить на β и избавиться в нём от β^3:

$$\beta^3 = -2\beta - 1 = \underline{\beta + 2}\ ,\ \beta^4 = \underline{\beta^2 + 2\beta}\ ,$$

$$\beta^5 = \beta^3 + 2\beta^2 = \beta + 2 + 2\beta^2 = \underline{2\beta^2 + \beta + 2}\ .$$

Результаты вычислений занесём в таблицу.

$\beta^1 = \beta$	$\beta^{10} = \beta^2 + \beta$	$\beta^{19} = 2\beta^2 + 2\beta + 2$
$\beta^2 = \beta^2$	$\beta^{11} = \beta^2 + \beta + 2$	$\beta^{20} = 2\beta^2 + \beta + 1$
$\beta^3 = \beta + 2$	$\beta^{12} = \beta^2 + 2$	$\beta^{21} = \beta^2 + 1$
$\beta^4 = \beta^2 + 2\beta$	$\beta^{13} = 2$	$\beta^{22} = 2\beta + 2$
$\beta^5 = 2\beta^2 + \beta + 2$	$\beta^{14} = 2\beta$	$\beta^{23} = 2\beta^2 + 2\beta$
$\beta^6 = \beta^2 + \beta + 1$	$\beta^{15} = 2\beta^2$	$\beta^{24} = 2\beta^2 + 2\beta + 1$
$\beta^7 = \beta^2 + 2\beta + 2$	$\beta^{16} = 2\beta + 1$	$\beta^{25} = 2\beta^2 + 1$
$\beta^8 = 2\beta^2 + 2$	$\beta^{17} = 2\beta^2 + \beta$	$\beta^{26} = 1$
$\beta^9 = \beta + 1$	$\beta^{18} = \beta^2 + 2\beta + 1$	

В результате получилось, что $ord(\beta) = 26$, т.е. β является примитивным элементом поля F_{3^3}.

Воспользовавшись этим фактом и свойством порядков 2.16.4), можно найти все примитивные элементы в поле F_{3^3}. Примитивными будут все степени β^k, если число k взаимно просто с числом 26:

$$\beta^1, \beta^3, \beta^5, \beta^7, \beta^9, \beta^{11}, \beta^{15}, \beta^{17}, \beta^{19}, \beta^{21}, \beta^{23}, \beta^{25}.$$

Для вычисления порядков элементов и для поиска примитивных элементов можно воспользоваться алгоритмами 2.36 и 2.37. Например, согласно 2.37, чтобы доказать, что элемент β является примитивным, достаточно проверить, что $\beta^2 \neq 1$ и $\beta^{13} \neq 1$.

Кроме того, для вычисления степени можно применять

5.24. Бинарный алгоритм возведения в степень. Для того чтобы в некотором поле вычислить степень a^n, нужно:

а) найти двоичное представление показателя степени

$$n = b_k 2^k + b_{k-1} 2^{k-1} + \ldots + b_1 2^1 + b_0,\ b_i \in \{0, 1\};$$

б) вычислить степени a^{2^i}, $1 \le i \le k$;

в) вычислить $a^n = \left(a^{2^k}\right)^{b_k} \left(a^{2^{k-1}}\right)^{b_{k-1}} \cdot \ldots \cdot \left(a^{2^1}\right)^{b_1} \left(a^{2^0}\right)^{b_0}$.

Этот алгоритм эффективнее последовательного вычисления степени, т.к. для вычислений в пункте б) понадобится k умножений (возведений в квадрат), а в пункте в) – не более k умножений. В результате, всего не более $2k$ умножений. Так как $2^{k+1} > n \ge 2^k$, то $k+1 > \log_2 n \ge k$ и, следовательно, $k = [\log_2 n]$. Окончательно оценку сложности бинарного алгоритма можно сформулировать так:

Вычисление степени a^n при помощи бинарного алгоритма требует не более $2[\log_2 n]$ умножений в данном поле.

Последовательное же вычисление степени потребует $(n-1)$ умножений, что для больших n существенно больше.

5.25. Пример. В условиях примера 5.23 проверить, что элемент $\gamma = \beta^2 + \beta + 2$ является примитивным в поле F_{3^3}.

Согласно тождеству Ферма 5.13, $\gamma^{26} = 1$. Так как $26 = 2 \cdot 13$, то для решения задачи достаточно проверить, что $\gamma^2 \ne 1$ и $\gamma^{13} \ne 1$. Для этого нужно вычислить γ^2 и γ^{13}. Ниже это будет проделано при помощи бинарного алгоритма.

Кроме того, можно заметить, что т.к. многочлен однозначно определяется последовательностью коэффициентов своей

стандартной формы, то стандартную форму можно записывать как последовательность. Умножение, сложение, вычитание и деление можно выполнять «столбиком», учитывая, что в случае многочленов перенос данных между разрядами не производится. Например:

$$\gamma^2=\left(\beta^2+\beta+2\right)\left(\beta^2+\beta+2\right)=$$

$$=\beta^4+\beta^3+2\beta^2+\beta^3+\beta^2+2\beta+2\beta^2+2\beta+1=$$

$$=\beta^4+2\beta^3+2\beta^2+\beta+1;$$

$$\begin{array}{r} 112 \\ \times\ \underline{112} \\ 221 \\ 112 \\ \underline{112} \\ 12211 \end{array}$$

$$\begin{array}{l} \beta^4+2\beta^3+2\beta^2+\beta+1 \\ \underline{\beta^4+2\beta^2+\beta} \\ 2\beta^3+1 \\ \underline{2\beta^3+\beta+2} \\ 2\beta+2 \end{array} \Bigg| \begin{array}{l} \beta^3+2\beta+1 \\ \beta+2 \end{array}$$

$$\begin{array}{l} 12211 \\ \underline{1021} \\ 2001 \\ \underline{2012} \\ 22 \end{array} \Bigg| \begin{array}{l} \underline{1021} \\ 12 \end{array}$$

В результате $\gamma^2=2\beta+2\neq 1$.

Далее вычисляем γ^4, γ^8 и $\gamma^{13}=\gamma^8\gamma^4\gamma$.

$$\begin{array}{r} 22 \\ \times\ \underline{22} \\ 11 \\ \underline{11} \\ 121 \end{array} ; \quad \gamma^4=\beta^2+2\beta+1.$$

$$\begin{array}{r} 121 \\ \times\ \underline{121} \\ 121 \\ 212 \\ \underline{121} \\ 11011 \end{array} ; \quad \begin{array}{l} 11011 \\ \underline{1021} \\ 1101 \\ \underline{1021} \\ 110 \end{array} \Bigg| \begin{array}{l} \underline{1021} \\ 11 \end{array} ; \quad \gamma^8=\beta^2+\beta.$$

$$\begin{array}{r} \times\ 121 \\ \underline{\quad 110} \\ 121 \\ \underline{121} \\ 10010 \end{array};\qquad \begin{array}{r} \times\ 10010 \\ \underline{\quad 112} \\ 20020 \\ 10010 \\ \underline{10010} \\ 1121120 \end{array};\qquad \begin{array}{r|l} 1121120 & \underline{1021} \\ \underline{1021} & 1101 \\ 1001 & \\ \underline{1021} & \\ 1020 & \\ \underline{1021} & \\ 2 & \end{array};\quad \gamma^{13}=\gamma^8\gamma^4\gamma\,.$$

Получилось, что $\gamma^{13}=2\neq 1$ и, следовательно, $\gamma=\beta^2+\beta+2$ является примитивным элементом поля F_{3^3}. Этот результат согласуется с выводами из примера 5.23, т.к. $\gamma=\beta^{11}$.

5.26. Определение. Поле F называется *полем разложения многочлена* $f(x)\in P[x]$, если F является наименьшим полем, которое содержит P и над которым многочлен $f(x)$ раскладывается на линейные сомножители.

5.27. Теорема (о существовании поля разложения). *Для любого поля P и любого многочлена $f(x)\in P[x]$ положительной степени существует поле разложения этого многочлена над P.*

Доказательство. Рассмотрим каноническое разложение многочлена $f(x)$ над полем P:

$$f(x)=b_n g_1^{k_1}(x)\cdot g_2^{k_2}(x)\cdot\ldots\cdot g_s^{k_s}(x)\,.$$

Возьмём один из неприводимых многочленов $g_i(x)$ степени не ниже 2 из этого разложения и положим $F_1=P[x]/g_i(x)$. Согласно теореме 5.18, $F_1=P(\beta_1)$, где β_1 – корень многочленов $g_i(x)$ и $f(x)$ в поле F_1.

В каноническом разложении $f(x)$ над F_1 суммарная степень нелинейных неприводимых сомножителей уменьшится по крайней мере на единицу, т.к. $g_i(x)=(x-\beta_1)h(x)$, и в разложении появится неприводимый над F_1 сомножитель первой степени $(x-\beta_1)$. Продолжая этот процесс, находим расширение

$F_s \supseteq P$, в котором многочлен $f(x)$ разлагается на линейные сомножители.

Если $\beta_1, \beta_2, \ldots, \beta_n \in F_s$ – все корни многочлена $f(x)$, то искомым полем разложения будет, очевидно, поле $P(\beta_1, \beta_2, \ldots, \beta_n)$.

Без доказательства сформулируем

5.28. Теорему (о единственности поля разложения). *Для любого поля P и любого многочлена $f(x) \in P[x]$ положительной степени поле разложения этого многочлена единственно с точностью до изоморфизма.*

§3. Строение конечных полей

Конструкция из предыдущего параграфа позволяет получить любое конечное поле.

5.29. Теорема (о строении конечных полей). *Если F – конечное поле характеристики p, а P – его простое подполе и $k = \dim(F/P)$, то F является полем разложения над P многочлена $x^{p^k} - x \in P[x]$ и совпадает с множеством всех его корней.*

Доказательство. Согласно 5.4 и 5.6, простое подполе P изоморфно полю $\mathbb{Z}_p$ и $|F| = p^k$. Порядок группы ненулевых элементов F^* равен $p^k - 1$, поэтому для всех $a \in F^*$ выполняется равенство $a^{p^k - 1} = 1$. Из этого следует, что все элементы поля F являются корнями многочлена $f(x) = x\left(x^{p^k - 1} - 1\right) = x^{p^k} - x$. Так как $cm(f) = |F|$, то у многочлена $f(x)$ нет других корней, кроме тех, что лежат в поле F. Следовательно, F – поле разложения многочлена $x^{p^k} - x$. Теорема доказана.

5.30. Теорема (о существовании и единственности конечного поля с данным количеством элементов). *Для любого простого числа p и любого натурального k существует единственное с точностью до изоморфизма поле, состоящее из p^k элементов.*

Доказательство. Рассмотрим многочлен $f(x)=x^{p^k}-x$ как многочлен над полем $\mathbb{Z}_p$. Пусть F – поле разложения этого многочлена над полем $\mathbb{Z}_p$. Оно имеет характеристику p.

Так как $f'(x)=p^k x^{p^k-1}-1=-1$, то многочлены $f(x)$ и $f'(x)$ взаимно просты, не имеют общих корней и, согласно теореме 3.54, многочлен $f(x)$ не имеет кратных корней. В результате, в своём поле разложения F многочлен $f(x)$ будет иметь ровно p^k различных корней. Пусть $M=\left\{\beta_1,\beta_2,\ldots,\beta_{p^k}\right\}$ – множество этих корней. Для них справедливы равенства $(\beta_i)^{p^k}=\beta_i$, $1\le i\le p^k$.

Докажем, что множество M замкнуто относительно сложения и умножения, воспользовавшись следствием 5.2. Действительно, т.к. $\left(\beta_i\beta_j\right)^{p^k}=\beta_i{}^{p^k}\beta_j{}^{p^k}=\beta_i\beta_j$ и $\left(\beta_i+\beta_j\right)^{p^k}=\beta_i{}^{p^k}+\beta_j{}^{p^k}=\beta_i+\beta_j$, то $\beta_i\beta_j\in M$ и $\beta_i+\beta_j\in M$.

Согласно критерию конечного подполя 5.8, множество M является подполем поля F и содержит в точности p^k элементов. Поля F и M должны совпадать в силу минимальности поля разложения.

Если F_1 и F_2 – два поля, содержащие p^k элементов, то они оба будут полями разложения конкретного многочлена над простым полем из p элементов. Согласно описанию простых полей, такое поле единственно с точностью до изоморфизма – это поле $\mathbb{Z}_p$. Следовательно, F_1 и F_2 изоморфны в силу единственности поля разложения.

5.31. Теорема (о существовании и единственности подполя). *Если* $F = F_{p^n}$ *и* $n \vdots k$, *то поле* F *имеет единственное подполе* P, *изоморфное* F_{p^k}.

Доказательство. Пусть $n = ks$. Равенство

$$p^n - 1 = p^{ks} - 1 = \left(p^k - 1\right)\left(p^{k(s-1)} + p^{k(s-2)} + \ldots + p^k + 1\right)$$

показывает, что $p^n - 1$ делится на $p^k - 1$.

По аналогичной причине многочлен $x^{p^n-1} - 1$ делится на многочлен $x^{p^k-1} - 1$ и, следовательно, многочлен $f(x) = x^{p^n} - x$ делится на многочлен $g(x) = x^{p^k} - x$. По теореме 5.29 о строении конечных полей, F – поле разложения многочлена $f(x)$ над простым полем и $f(x)$ разлагается над F на линейные сомножители. Следовательно, многочлен $g(x)$ также разлагается над полем F на линейные сомножители.

Затем, как и в доказательстве предыдущей теоремы, получаем, что корни многочлена $g(x)$ образуют внутри F подполе P, состоящее из p^k элементов.

Задачи для самостоятельного решения

1. Пусть дан неприводимый многочлен $f(x) = x^4 + x^3 + x^2 + x + 1 \in F_2[x]$. Пусть β – один из его корней в поле $F_{2^4} = F_2(\beta)$. Найти в этом поле:

а) произведение и частное элементов $\gamma_1 = \beta^3 + \beta + 1$ и $\gamma_2 = \beta^2 + \beta + 1$;

б) порядки элементов β, $\beta^3 + \beta^2 + 1$ и $\beta^2 + \beta + 1$;

в) три примитивных элемента;

г) представление всех элементов поля в виде степеней примитивного элемента.

2. Пусть дан неприводимый многочлен $f(x)=x^2+3x+1\in F_7[x]$. Пусть β – один из его корней в поле $F_{7^2}=F_7(\beta)$. Найти в этом поле:

а) произведение и частное элементов $\gamma_1=2\beta+1$ и $\gamma_2=\beta^2+\beta+1$;

б) порядки элементов $3\beta+1$, $5\beta+1$ и $\beta+2$;

в) три примитивных элемента;

г) представление всех элементов поля в виде степеней примитивного элемента.

3. Пусть дан неприводимый многочлен $f(x)=x^6+x+1\in F_2[x]$. Пусть β – один из его корней в поле $F_{2^6}=F_2(\beta)$. Найти в этом поле:

а) произведение и частное элементов $\gamma_1=\beta^3+\beta+1$ и $\gamma_2=\beta^5+\beta^4+\beta^2+\beta+1$;

б) порядки элементов $\beta+1$, $\beta^3+\beta+1$ и $\beta^5+\beta^4+\beta^3+\beta+1$;

в) три примитивных элемента.

4. Пусть дан неприводимый многочлен $f(x)=x^4+x^2+x+1\in F_3[x]$. Пусть β – один из его корней в поле $F_{3^4}=F_3(\beta)$. Найти в этом поле:

а) произведение и частное элементов $\gamma_1=2\beta^3+\beta+1$ и $\gamma_2=\beta^2+2\beta+2$;

б) порядки элементов β, $2\beta+1$ и $2\beta^2+\beta+1$;

в) три примитивных элемента.

ГЛАВА 6. МНОГОЧЛЕНЫ НАД КОНЕЧНЫМИ ПОЛЯМИ

§1. Неприводимые многочлены над конечными полями

Неприводимые многочлены над конечными полями необходимы для построения новых конечных полей. Важнейшими являются вопросы существования неприводимых многочленов данного вида, признаки неприводимости, количество неприводимых многочленов, а также способы их нахождения.

6.1. Теорема (о существовании неприводимых многочленов над конечным полем). *Над полем* F_q *существуют неприводимые многочлены произвольной натуральной степени* n.

Доказательство. Пусть $q = p^k$. Рассмотрим поле разложения $F_{p^{kn}} = F_{q^n}$ многочлена $f(x) = x^{p^{kn}} - x$ над F_p. Оно является конечным и, согласно теореме 5.31, содержит F_q в качестве подполя. Согласно теореме 5.20, поле F_{q^n} является простым алгебраическим расширением поля F_q при помощи корня β некоторого неприводимого многочлена $g(x) \in F_q[x]$:

$$F_{q^n} = F_q(\beta).$$

С одной стороны,

$$\dim\left(F_{q^n} / F_q\right) = \dim\left(F_q(\beta) / F_q\right) = cm\left(g(x)\right).$$

С другой стороны, по следствию 5.7, $\dim\left(F_{q^n} / F_q\right) = n$. В результате $cm\left(g(x)\right) = n$.

6.2. Теорема (о корнях неприводимого многочлена над конечным полем). *Пусть* $f(x)$ *– неприводимый многочлен степени* n *над полем* F_q *и* $F = F_q(\beta)$ *– простое алгебраическое расширение поля* F_q *при помощи корня* β *многочлена* $f(x)$. *Тогда:*

а) F *– поле разложения многочлена* $f(x)$ *над* F_q, *причём* $f(x)$ *имеет в* F *ровно* n *различных корней:*

$$\beta, \beta^q, \beta^{q^2}, \ldots, \beta^{q^{n-1}};$$

б) $\left(x^{q^n} - x\right) \vdots f(x)$.

Доказательство. а) Пусть $f(x) = \sum_{i=0}^{n} b_i x^i$. Так как $b_i \in F_q$, то $(b_i)^q = b_i$, $(b_i)^{q^s} = b_i$ для любого натурального s. Подставим элементы вида β^{q^s} в многочлен $f(x)$ и воспользуемся следствием 5.2:

$$f\left(\beta^{q^s}\right) = \sum_{i=0}^{n} b_i \left(\beta^{q^s}\right)^i = \sum_{i=0}^{n} b_i \left(\beta^i\right)^{q^s} =$$

$$= \sum_{i=0}^{n} \left(b_i \beta^i\right)^{q^s} = \left(\sum_{i=0}^{n} b_i \beta^i\right)^{q^s} = \left(f(\beta)\right)^{q^s} = 0.$$

В результате все элементы $\beta, \beta^q, \beta^{q^2}, \ldots, \beta^{q^{n-1}}$ являются корнями многочлена $f(x)$.

Докажем, что они различны. Пусть, напротив, $\beta^{q^s} = \beta^{q^t}$, $s < t$. Тогда

$$\beta^{q^t} - \beta^{q^s} = \left(\beta^{q^{t-s}}\right)^{q^s} - \beta^{q^s} = \left(\beta^{q^{t-s}} - \beta\right)^{q^s} = 0$$

и, следовательно, $\beta^{q^{t-s}} = \beta$, $0 < t-s < n$. Произвольный элемент b поля F имеет вид $b = \sum_{i=1}^{n-1} b_i \beta^i$, $b_i \in F_q$, поэтому

$$b^{q^{t-s}} = \left(\sum_{i=1}^{n-1} b_i \beta^i \right)^{q^{t-s}} = \sum_{i=1}^{n-1} \left(b_i \beta^i \right)^{q^{t-s}} =$$

$$= \sum_{i=1}^{n-1} b_i^{q^{t-s}} \left(\beta^i \right)^{q^{t-s}} = \sum_{i=1}^{n-1} b_i \beta^i = b .$$

В результате все q^n элементов поля F являются корнями многочлена $x^{q^{t-s}} - x$, что невозможно, т.к. его степень меньше q^n.

б) Так как $\dim\left(F / F_q\right) = n = cm(f)$, то $|F| = q^n$. По теореме 5.29 о строении конечных полей все элементы поля F являются корнями многочлена $g(x) = x^{q^n} - x \in F_q[x]$. Следовательно многочлены $f(x)$ и $g(x)$ имеют общие корни и не являются взаимно простыми над полем F. Так как $f(x), g(x) \in F_q[x]$, то они не являются взаимно простыми и над F_q. Наконец, т.к. многочлен $f(x)$ неприводим над F_q, то по основному свойству неприводимых многочленов 3.36 многочлен $g(x)$ делится на $f(x)$.

6.3. Следствие (о порядках корней неприводимого многочлена). *Если $f(x)$ – неприводимый многочлен степени n над полем F_q, а β_1, β_2 – различные корни $f(x)$ в его поле разложения, то:*

а) $ord(\beta_1) = ord(\beta_2)$,

б) $\left(q^n - 1\right) \vdots ord(\beta_1)$,

в) $\left(q^m-1\right)\nmid ord(\beta_1)$, *для любого* $0<m<n$.

Доказательство. а) Если $ord(\beta_1)=k$, то β_1 – корень многочлена $x^k-1\in F_q[x]$. Так как многочлены $f(x)$ и x^k-1 имеют общие корни, то они не являются взаимно простыми. Так как $f(x)$ неприводим над F_q, то $\left(x^k-1\right)\vdots f(x)$. Так как $f(\beta_2)=0$, то $(\beta_2)^k-1=0$ и, согласно свойству порядков 2.16.1), $ord(\beta_1)\vdots ord(\beta_2)$.

Аналогично доказывается, что $ord(\beta_2)\vdots ord(\beta_1)$.

б) Согласно утверждению б) теоремы 6.2, $\left(x^{q^n}-x\right)=x\left(x^{q^n-1}-1\right)\vdots f(x)$. По условию многочлен $f(x)$ неприводим и имеет степень $n\geq 2$, поэтому $f(x)$ взаимно прост с x и, согласно свойствам неприводимых многочленов, $\left(x^{q^n-1}-1\right)\vdots f(x)$. Так как $f(\beta_1)=0$, то $(\beta_1)^{q^n-1}-1=0$. По свойствам порядков из этого следует, что $\left(q^n-1\right)\vdots ord(\beta_1)$.

в) Если, напротив, $\left(q^m-1\right)\vdots ord(\beta_1)$ и $0<m<n$, то так же, как и в пункте а) теоремы 6.2, доказывается, что количество различных корней многочлена $\left(x^{q^m-1}-1\right)$ превосходит его степень. Противоречие.

6.4. Следствие. *Неприводимый многочлен над конечным полем* P *взаимно прост со своей производной.*

Действительно, согласно теореме 6.2а), такой многочлен в своём поле разложения F не имеет кратных корней, следовательно, он не имеет со своей производной общих корней (теорема 3.54). Следовательно, в кольце $F[x]$ он взаимно прост со своей производной. Так как многочлены $f(x)$ и $f'(x)$ лежат в кольце $P[x]$, то по теореме о делении с остатком и алгоритму

Евклида их *НОД* также лежит в $P[x]$ и совпадает с *НОД* в кольце $F[x]$, т.е. равен 1.

6.5. Следствие. *Неприводимый над* F_q *многочлен* $g(x)$ *степени* m *делит многочлен вида* $\left(x^{q^n}-x\right)$ *тогда и только тогда, когда* $n \vdots m$.

Доказательство. Если $n \vdots m$, то $\left(x^{q^n-1}-1\right) \vdots \left(x^{q^m-1}-1\right)$ и $\left(x^{q^n}-x\right) \vdots \left(x^{q^m}-x\right)$. Если $g(x) \in F_q[x]$ – неприводимый многочлен степени m, то по теореме $\left(x^{q^m}-x\right) \vdots g(x)$. В результате $\left(x^{q^n}-x\right) \vdots g(x)$.

Пусть теперь $\left(x^{q^n}-x\right) \vdots g(x)$ и β – корень многочлена $g(x)$. Тогда β – корень многочлена $\left(x^{q^n}-x\right)$ и, следовательно, принадлежит полю F_{q^n}. Запишем условие на размерность для цепочки расширений $F_q \subseteq F_q(\beta) \subseteq F_{q^n}$:

$$n = \dim\left(F_{q^n} / F_q\right) = \dim\left(F_{q^n} / F_q(\beta)\right)\dim\left(F_q(\beta) / F_q\right) =$$

$$= \dim\left(F_{q^n} / F_q(\beta)\right) \cdot m .$$

В результате $n \vdots m$.

6.6. Следствие. *Пусть* $f(x)$ *– неприводимый многочлен степени* n *над полем* F_q *и пусть* $F = F_q(\beta)$ *– простое алгебраическое расширение поля* F_q *при помощи корня* β *многочлена* $f(x)$. *Тогда любой неприводимый над* F_q *многочлен*

$g(x)$ с условием $n \vdots cm(g)$ раскладывается в кольце $F[x]$ на линейные сомножители. Кроме того, поле F не содержит корней неприводимых над F_q многочленов, степени которых не делят n.

Доказательство. Если $g(x) \in F_q[x]$ – неприводимый многочлен степени m и $n \vdots m$, то по следствию 6.5 $\left(x^{q^n} - x\right) \vdots g(x)$. По теореме 5.29 о строении конечных полей многочлен $\left(x^{q^n} - x\right)$ раскладывается над полем F на линейные сомножители. Следовательно, и многочлен $g(x)$ также раскладывается над F на линейные сомножители.

Если неприводимый над F_q многочлен степени m имеет корень $\gamma \in F_q(\beta)$, то $\dim\left(F_q(\gamma)/F_q\right) = m$ и по теореме о транзитивности конечных расширений для цепочки расширений $F_q \subseteq F_q(\gamma) \subseteq F_q(\beta)$ получаем:

$$n = \dim\left(F_q(\beta)/F_q\right) = \dim\left(F_q(\beta)/F_q(\gamma)\right) \cdot \dim\left(F_q(\gamma)/F_q\right) =$$

$$= \dim\left(F_q(\beta)/F_q(\gamma)\right) \cdot m \ .$$

Откуда $n \vdots m$.

6.7. Теорема. *Произведение всех нормированных неприводимых над полем F_q многочленов, степени которых делят число n, равно $\left(x^{q^n} - x\right)$.*

Доказательство. Многочлен $f(x) = x^{q^n} - x$ в кольце $F_q[x]$, согласно 6.5, делится на все нормированные неприводимые многочлены, степени которых делят число n. Так как эти многочлены попарно взаимно просты, то он делится и на их произведение. Согласно 6.5, других многочленов в каноническом разложении быть не может. В результате каноническое

разложение многочлена $f(x)=x^{q^n}-x$ в кольце $F_q[x]$ является произведением всех нормированных неприводимых многочленов, степени которых делят число n. Каждый неприводимый множитель может входить в разложение в некоторой степени, т.е. быть кратным.

Многочлен $f(x)$ взаимно прост со своей производной $f'(x)=-1$, поэтому (см. 3.55) не имеет кратных корней. Если бы $f(x)$ имел кратный неприводимый множитель, то в своём поле разложения он бы имел кратные корни. Ввиду этого многочлены канонического разложения $f(x)$ должны входить в него в первой степени.

6.8. Теорема (М. Батлер, 1954). *Многочлен $f(x)$ положительной степени из кольца $F_q[x]$ неприводим над полем F_q тогда и только тогда, когда выполнены два условия:*

а) $НОД\big(f(x), f'(x)\big)=1$;

б) уравнение $z^q-z=0$ имеет в кольце $F_q[x]/f(x)$ ровно q различных решений.

Доказательство (см., например, [2]).

Используя теорему Батлера, можно предложить следующий

6.9. Алгоритм проверки неприводимости многочлена над конечным полем.

1) Так как многочлены первой степени всегда неприводимы, то можно считать, что $n=cm(f)>1$.

2) Проверяем условие $НОД\big(f(x), f'(x)\big)=1$ по алгоритму Евклида.

3) Если $НОД\big(f(x), f'(x)\big)=1$, то попытаемся подсчитать количество решений уравнения $z^q-z=0$ в кольце $F_q[x]/f(x)$.

Произвольный элемент этого кольца можно записать в виде $h(x) \equiv c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \ldots + c_1 x^1 + c_0 \left(\mathrm{mod} f(x)\right)$, $c_i \in F_q$. Он будет решением уравнения $z^q - z = 0$, если:

$$h(x)^q \equiv h(x)\left(\mathrm{mod} f(x)\right) \Leftrightarrow$$

$$\left(c_{n-1}\right)^q x^{(n-1)q} + \left(c_{n-2}\right)^q x^{(n-2)q} + \ldots + \left(c_1\right)^q x^q + \left(c_0\right)^q \equiv$$

$$\equiv c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \ldots + c_1 x^1 + c_0 \left(\mathrm{mod} f(x)\right).$$

Переносим все слагаемые в левую часть, учитываем, что по тождеству Ферма $\left(c_i\right)^q = c_i$, и получаем:

$$c_{n-1}\left(x^{(n-1)q} - x^{n-1}\right) + \ldots + c_1\left(x^q - x^1\right) \equiv 0\left(\mathrm{mod} f(x)\right).$$

Находим каноническое представление всех многочленов вида $\left(x^{iq} - x^i\right)$, $1 \le i \le n-1$, в кольце $F_q[x]/f(x)$:

$$\left(x^{iq} - x^i\right) \equiv a_{i,n-1}x^{n-1} + a_{i,n-2}x^{n-2} + .. + a_{i,1}x^1 + a_{i,0}$$

и подставляем в предыдущее сравнение. Слева получится многочлен степени меньше $n = cm(f)$, сравнимый с 0 по модулю $f(x)$. Следовательно, этот многочлен равен нулю. Приравнивая коэффициенты при одинаковых степенях, получаем однородную систему линейных уравнений относительно неизвестных c_i:

$$\begin{cases} a_{n-1,n-1}c_{n-1} + a_{n-2,n-1}c_{n-2} + \ldots + a_{1,n-1}c_1 + 0c_0 = 0, \\ a_{n-1,n-2}c_{n-1} + a_{n-2,n-2}c_{n-2} + \ldots + a_{1,n-2}c_1 + 0c_0 = 0, \\ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n-1,0}c_{n-1} + a_{n-2,0}c_{n-2} + \ldots + a_{1,0}c_1 + 0c_0 = 0. \end{cases} \quad (1)$$

Её можно записать в матричном виде $A\bar{c} = \bar{0}$, если положить

$$A=\begin{pmatrix} a_{n-1,n-1} & a_{n-2,n-1} & \cdots & a_{1,n-1} & 0 \\ a_{n-1,n-2} & a_{n-2,n-2} & \cdots & a_{1,n-2} & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n-1,0} & a_{n-2,0} & \cdots & a_{1,0} & 0 \end{pmatrix},\quad \bar{c}=\begin{pmatrix} c_{n-1} \\ c_{n-2} \\ \cdots \\ c_0 \end{pmatrix}.$$

Заметим, что столбцами матрицы A являются коэффициенты из представления многочленов $\left(x^{iq}-x^{i}\right)$, записанные в порядке убывания числа i от $(n-1)$ к 1.

Количество решений уравнения $z^q-z=0$ в кольце $F_q[x]/f(x)$ совпадает с количеством решений системы (1). Так как система имеет $\left(n-rang\,A\right)$ свободных неизвестных, то количество решений будет равно $q^{\left(n-rang\,A\right)}$. По теореме Батлера многочлен $f(x)$ неприводим тогда и только тогда, когда $n-rang\,A=1$, т.е. когда $rang\,A=n-1$.

6.10. Пример. Проверить неприводимость многочлена $f(x)=x^4+x+2$ над полем F_3.

В нашем случае $q=3, n=4$, $f'(x)=x^3+1$. Так как $f(x)=xf'(x)+2$, то многочлены $f(x)$ и $f'(x)$ взаимно просты.

Находим представление многочленов $\left(x^{i3}-x^{i}\right)$, $1\le i\le 3$, в кольце $F_3[x]/f(x)$. Вместо деления можно воспользоваться тем, что $x^4+x+2\equiv 0\left(\mathrm{mod}\,f(x)\right)$ или $x^4\equiv -x-2=2x+1\left(\mathrm{mod}\,f(x)\right)$.

$$x^9-x^3\equiv x(2x+1)^2-x^3\equiv x\left(x^2+x+1\right)-x^3\equiv$$

$$\equiv x^2+x\equiv 0x^3+x^2+x+0\left(\mathrm{mod}\,f(x)\right);$$

$$x^6-x^2\equiv x^2(2x+1)-x^2\equiv 2x^3\left(\mathrm{mod}\,f(x)\right);$$

$$x^3-x\equiv x^3+0x^2+2x+0\left(\mathrm{mod}\,f(x)\right);$$

$$A=\begin{pmatrix}0&2&1&0\\1&0&0&0\\1&0&2&0\\0&0&0&0\end{pmatrix}.$$

$rang\,A$ равен 3, так как

$$\begin{pmatrix}0&2&1\\\mathbf{1}&0&0\\1&0&2\end{pmatrix}\sim\begin{pmatrix}0&2&1\\\mathbf{1}&0&0\\0&0&\mathbf{2}\end{pmatrix}\sim\begin{pmatrix}0&\mathbf{2}&0\\\mathbf{1}&0&0\\0&0&\mathbf{2}\end{pmatrix}.$$

По теореме Батлера данный многочлен неприводим над полем F_3.

Одним из простейших способов поиска неприводимых многочленов над конечным полем является метод перебора, который состоит в следующем:

1) случайным образом выбирается произвольный многочлен;

2) производится его проверка на неприводимость; если многочлен оказывается приводимым, то выбирается следующий многочлен.

Эффективность этого метода обеспечивается тем, что неприводимых многочленов данной степени над конечным полем достаточно много. Выведем формулу для определения *числа* $\Phi_P(d)$ *неприводимых нормированных многочленов степени* d *над полем* P.

6.11. Определение. Пусть дано каноническое разложение натурального числа $n=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$. Значением *функции Мёбиуса* от n называется величина

$$\mu(n)=\begin{cases}1, \text{ если } n=1,\\(-1)^k, \text{ если } \alpha_1=\alpha_2=\ldots=\alpha_k=1,\\0, \text{ если } \exists\alpha_i>1.\end{cases}$$

6.12. Предложение. *Для любого натурального n выполняется равенство*

$$\sum_{n:d}\mu(d)=\begin{cases}1, \text{ если } n=1,\\ 0, \text{ если } n\neq 1.\end{cases}$$

Доказательство. При $n=1$, согласно определению, $\mu(1)=1$.

Пусть $n\neq 1$. Слагаемое в сумме $\sum\limits_{n:d}\mu(d)$ является ненулевым, если $d=1$ или $d=p_{i_1}\ldots p_{i_s}$, где простые числа p_{i_j} попарно различны. Делителей вида $d=p_{i_1}\ldots p_{i_s}$ ровно C_k^s штук. Вычислим данную сумму, воспользовавшись биномом Ньютона:

$$\sum_{n:d}\mu(d)=1-C_k^1+C_k^2-\ldots+(-1)^s C_k^s+\ldots+(-1)^k C_k^k=$$

$$=(1-1)^k=0.$$

6.13. Теорема (формула обращения Мёбиуса). *Для функций натурального аргумента $F(n)$ и $f(n)$ при всех натуральных n справедливо равенство*

$$\sum_{n:d}f(d)=F(n)$$

тогда и только тогда, когда при всех натуральных n справедливо равенство

$$\sum_{n:d}F\left(\frac{n}{d}\right)\cdot\mu(d)=f(n).$$

Доказательство. Воспользовавшись условием теоремы, левую часть требуемого равенства можно записать в виде

$$\sum_{n:d}\left(\sum_{\frac{n}{d}:d_1}f(d_1)\right)\cdot\mu(d).$$

Заметим, что имеют место равносильности:

$$n \vdots d,\ \frac{n}{d} \vdots d_1 \ \Leftrightarrow\ n = dd_1q \ \Leftrightarrow\ n \vdots d_1,\ \frac{n}{d_1} \vdots d\ .$$

Поэтому

$$\sum_{n \vdots d}\left(\sum_{\frac{n}{d} \vdots d_1} f(d_1)\right)\cdot\mu(d) = \sum_{n \vdots d}\left(\sum_{\frac{n}{d} \vdots d_1}\left(f(d_1)\mu(d)\right)\right) =$$

$$= \sum_{n \vdots d_1}\left(\sum_{\frac{n}{d_1} \vdots d}\mu(d)\right)\cdot f(d_1)\ .$$

Вычисляем коэффициент при $f(d_1)$:

$$\sum_{\frac{n}{d_1} \vdots d}\mu(d) \overset{\text{утв.1}}{=} \begin{cases} 1, \text{ при } \dfrac{n}{d_1} = 1, \text{ т.е. при } n = d_1; \\ 0, \text{ при } \dfrac{n}{d_1} \neq 1, \text{ т.е. при } n \neq d_1. \end{cases}$$

Таким образом, в полученной сумме будет только одно ненулевое слагаемое (при $d_1 = n,\ d = 1$), которое равно $1 \cdot f(n)$.

Обратное утверждение доказывается аналогично.

6.14. Следствие (формула обращения Мёбиуса в мультипликативной форме).

$$\prod_{n \vdots d} f(d) = F(n) \ \Leftrightarrow\ \prod_{n \vdots d} F\left(\frac{n}{d}\right)^{\mu(d)} = f(n) = \prod_{n \vdots d} F(d)^{\mu\left(\frac{n}{d}\right)}.$$

Для доказательства достаточно в формуле обращения в аддитивной форме заменить сложение на умножение, а умножение – на возведение в степень.

6.15. Предложение. *Для любого конечного поля* $P = F_q$ *и для любого натурального числа* n *выполняется равенство*

$$q^n = \sum_{n:d} d\Phi_P(d).$$

Доказательство. Если $f(x) \in P[x]$ – неприводимый многочлен степени n и β – его корень, то, согласно теореме 6.2 о корнях неприводимого многочлена, поле $P(\beta)$ является полем разложения $f(x)$ и содержит n его различных корней. Кроме того (см. 6.6), поле $P(\beta)$ содержит все корни всех неприводимых многочленов, степени которых являются делителями числа n. Так как различные нормированные неприводимые многочлены не могут иметь одинаковых корней, то поле $P(\beta)$ содержит не менее $\sum_{n:d} d\Phi_P(d)$ различных элементов и, значит,

$$q^n \geq \sum_{n:d} d\Phi_P(d).$$

С другой стороны, поле $P(\beta)$ содержит q^n элементов, каждый из которых является корнем многочлена $F(x) = \left(x^{q^n} - x\right)$ и, следовательно, корнем некоторого нормированного неприводимого многочлена $g(x)$, который делит $F(x)$. Согласно следствию 6.5, $n \vdots cm(g)$. Так как различные нормированные неприводимые многочлены не могут иметь одинаковых корней, то

$$q^n \leq \sum_{n:d} d\Phi_P(d).$$

6.16. Теорема (о числе неприводимых многочленов данной степени). *Для любого конечного поля* $P = F_q$ *и для любого натурального числа* n *выполняется равенство*

$$\Phi_P(n)=\frac{1}{n}\sum_{n:d}\mu(d)q^{n/d}.$$

Доказательство. Если положить $F(n)=q^n$, $f(d)=d\Phi_P(d)$, то равенство из предложения 6.15 будет иметь вид условия теоремы 6.13:

$$F(n)=q^n=\sum_{n:d}d\Phi_P(d)=\sum_{n:d}f(d).$$

Воспользовавшись теоремой 6.13, получаем:

$$f(n)=n\Phi_P(n)=\sum_{n:d}F\left(\frac{n}{d}\right)\cdot\mu(d)=\sum_{n:d}q^{n/d}\cdot\mu(d).$$

Теорема доказана.

6.17. Теорема. *Пусть* $q=p^k$. *Тогда произведение* $I(q,n)$ *всех нормированных неприводимых многочленов степени* n *в кольце* $F_q[x]$ *равно*

$$I(q,n)=\prod_{n:d}\left(x^{q^d}-x\right)^{\mu\left(\frac{n}{d}\right)}=\prod_{n:d}\left(x^{q^{n/d}}-x\right)^{\mu(d)}.$$

Доказательство. Согласно теореме 6.7, произведение всех нормированных неприводимых в кольце $F_q[x]$ многочленов равно $x^{q^n}-x=\prod_{n:d}I(q,d)$. Применение формулы обращения Мёбиуса в мультипликативном варианте для функций $F(n)=x^{q^n}-x$, $f(n)=I(q,n)$ доказывает требуемое равенство.

Теперь можно уточнить, почему метод случайного перебора является достаточно эффективным для нахождения нормированного неприводимого многочлена некоторой степени n.

Нормированный многочлен степени n над полем F_q имеет вид

$$f(x)=x^n+b_{n-1}x^{n-1}+\ldots+b_1x^1+b_0,$$

причём должно выполняться условие $b_0\neq 0$. Таких многочленов $(q-1)q^{n-1}$ штук. Из них неприводимых, согласно теореме 6.16, будет

$$\Phi_P(n)=\frac{1}{n}\sum_{n:d}\mu(d)q^{\frac{n}{d}}=$$

$$=\frac{1}{n}\left(q^n-q^{\frac{n}{p_1}}-q^{\frac{n}{p_2}}-\ldots+q^{\frac{n}{p_1p_2}}+q^{\frac{n}{p_1p_3}}+\ldots\right),$$

где $p_1,p_2,\ldots$ – различные простые делители числа n.

Вероятность случайно найти неприводимый многочлен равна $\frac{\Phi_P(n)}{(q-1)q^{n-1}}$. Для достаточно больших чисел q это число приблизительно равно $\frac{q}{n(q-1)}$ или, ещё проще, – $\frac{1}{n}$. Таким образом, проделав n испытаний, можно надеяться найти хотя бы один неприводимый многочлен данной степени. Проверку неприводимости по признаку, указанному ранее, и перебор вариантов целесообразно производить на ЭВМ.

6.18. Алгоритм нахождения неприводимых многочленов, состоящий в вычислении минимальных многочленов элементов поля F_{q^n}.

Пусть $F_{q^n}=F_q(\beta)$ – простое алгебраическое расширение при помощи алгебраического над F_q элемента β степени n. Базисом расширения будет множество $\left\{1,\beta,\beta^2,\ldots,\beta^{n-1}\right\}$. Степень минимального многочлена $m_\gamma(x)$ некоторого элемента $\gamma\in F^*_{q^n}$,

согласно следствию 6.6, является делителем n и, в частности, меньше n. Ввиду этого многочлен $m_\gamma(x)$ можно искать в виде

$$m_\gamma(x) = c_n x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0 ,\ c_i \in F_q .$$

По определению это многочлен наименьшей степени с коэффициентами из поля F_q, корнем которого является γ, т.е. справедливо равенство

$$m_\gamma(\gamma) = c_n \gamma^n + c_{n-1}\gamma^{n-1} + \ldots + c_1\gamma + c_0 = 0 .$$

Выразим через базис пространства элементы γ^k, $0 \le k \le n$:

$$\gamma^k = \sum_{i=0}^{n-1} b_{ki}\beta^i ,$$

подставим эти выражения в равенство $m_\gamma(\gamma) = 0$ и приведём подобные члены. Получится линейная комбинация базисных элементов, равная нулю. Так как базис линейно независим, то все коэффициенты линейной комбинации должны равняться нулю.

В результате получится однородная система линейных уравнений от неизвестных коэффициентов $c_n, c_{n-1}, \ldots, c_1, c_0$:

$$\begin{cases} c_n b_{n,n-1} + c_{n-1}b_{n-1,n-1} + \ldots + c_0 b_{0,n-1} = 0, \\ c_n b_{n,n-2} + c_{n-1}b_{n-1,n-2} + \ldots + c_0 b_{0,n-2} = 0, \\ \qquad\qquad \ldots\ldots\ldots\ldots\ldots\ldots \\ c_n b_{n,0} + c_{n-1}b_{n-1,0} + \ldots + c_0 b_{0,0} = 0. \end{cases}$$

Можно заметить, что *столбцами матрицы системы являются коэффициенты канонического представления элементов* γ^k, $0 \le k \le n$, *в поле* $F_q(\beta)$. Ввиду этого матрицу можно выписывать сразу.

Матрица системы имеет размеры $n \times (n+1)$. Система всегда имеет ненулевое решение, т.к. количество неизвестных больше количества уравнений.

Минимальный многочлен существует и, следовательно, существует такое наименьшее $r \geq 1$ и решение системы $c_n, c_{n-1}, \ldots, c_0$, что $c_n = 0, c_{n-1} = 0, \ldots, c_{r+1} = 0, c_r = 1$ и

$$m_\gamma(\gamma) = \gamma^r + c_{r-1}\gamma^{r-1} + \ldots + c_1\gamma + c_0 = 0.$$

При этом коэффициенты $c_{r-1}, c_{r-2}, \ldots, c_0$ определяются из системы однозначно. Кроме того, для любых не равных нулю одновременно значений $c_{r-1}, c_{r-2}, \ldots, c_0$ равенство $c_{r-1}\gamma^{r-1} + \ldots + c_1\gamma + c_0 = 0$ невозможно.

Обозначим столбец коэффициентов матрицы системы при неизвестной c_i как B_i. Тогда предыдущие рассуждения говорят о том, что столбцы $B_{r-1}, B_{r-2}, \ldots, B_0$ линейно независимы, а столбец B_r линейно выражается через них. Остальные столбцы также линейно выражаются через столбцы $B_{r-1}, B_{r-2}, \ldots, B_0$.

Действительно, рассмотрим степень γ^k для $r < k \leq n$. Разделим её как многочлен от γ на $m_\gamma(\gamma)$ с остатком:

$$\gamma^k = m_\gamma(\gamma)h(\gamma) + s(\gamma),\ cm(s) < r.$$

Учитывая, что в поле F_{q^n} имеет место равенство $m_\gamma(\gamma) = 0$, получаем равенство $\gamma^k = s(\gamma)$, которое и даст требуемое линейное выражение столбца B_k через столбцы $B_{r-1}, B_{r-2}, \ldots, B_0$.

В результате доказано, что ранг матрицы нашей системы в точности совпадает со степенью r искомого минимального многочлена. Причём неизвестные $c_{r-1}, c_{r-2}, \ldots, c_0$ можно считать зависимыми, а неизвестные $c_n, c_{n-1}, \ldots, c_r$ – независимыми неизвестными.

Ввиду этого можно предложить следующий алгоритм:

1) находим ранг r матрицы системы;

2) подставляем в систему $c_n = 0, c_{n-1} = 0, \ldots, c_{r+1} = 0, c_r = 1$;

3) находим из системы $c_{r-1}, c_{r-2}, \ldots, c_0$.

В результате многочлен $m_\gamma(x) = x^r + c_{r-1}x^{r-1} + \ldots + c_1 x + c_0$ будет найден.

6.19. Пример. Пусть $f(x) = x^3 + 2x + 1 \in F_3[x]$ и β – один из его корней в поле $F_{3^3} = F_3(\beta)$ (см. пример 5.22). Найти минимальный многочлен элемента $\gamma = \beta^2 + 1$.

По условию $\beta^3 + 2\beta + 1 = 0$, поэтому

$$\beta^3 = -2\beta - 1 = \beta + 2.$$

Мы будем использовать это тождество в преобразованиях. Согласно алгоритму 6.18, выражаем степени γ через базис $\{1, \beta, \beta^2\}$:

$$\gamma^0 = 1 = 0\beta^2 + 0\beta + 1;$$

$$\gamma^1 = \beta^2 + 1 = 1\beta^2 + 0\beta + 1;$$

$$\gamma^2 = \left(\beta^2 + 1\right)^2 = \beta^4 + 2\beta^2 + 1 = \beta(\beta + 2) + 2\beta^2 + 1 =$$

$$= 2\beta + 1 = 0\beta^2 + 2\beta + 1;$$

$$\gamma^3 = (2\beta + 1)\left(\beta^2 + 1\right) = 2\beta^3 + \beta^2 + 2\beta + 1 =$$

$$= 2\beta + 1 + \beta^2 + 2\beta + 1 = \beta^2 + \beta + 2.$$

Минимальный многочлен находится из условия

$$m_\gamma(\gamma) = c_3\gamma^3 + c_2\gamma^2 + c_1\gamma + c_0 = 0.$$

Подставляем в это условие каноническое представление степеней γ в $F_3(\beta)$ и переходим к системе:

$$c_3\left(\beta^2 + \beta + 2\right) + c_2(2\beta + 1) + c_1\left(\beta^2 + 1\right) + c_0 = 0.$$

$$\begin{cases} c_3 + c_1 = 0, \\ c_3 + 2c_2 = 0, \\ 2c_3 + c_2 + c_1 + c_0 = 0. \end{cases}$$

Решаем систему, преобразуя её матрицу. Чтобы свободными неизвестными оказались первые коэффициенты, ведущие элементы выбираем в последних столбцах.

$$\begin{pmatrix} 1 & 0 & \mathbf{1} & 0 \\ 1 & 2 & 0 & 0 \\ 2 & 1 & 1 & \mathbf{1} \end{pmatrix} \begin{matrix} \\ \\ \leftarrow \end{matrix} (-1) \sim \begin{pmatrix} 1 & 0 & \mathbf{1} & 0 \\ 1 & 2 & 0 & 0 \\ 1 & 1 & 0 & \mathbf{1} \end{pmatrix} (2) \sim \begin{pmatrix} 1 & 0 & \mathbf{1} & 0 \\ 2 & \mathbf{1} & 0 & 0 \\ 1 & 1 & 0 & \mathbf{1} \end{pmatrix} \begin{matrix} \\ \\ \leftarrow \end{matrix} (-1) \sim$$

$$\sim \begin{pmatrix} 1 & 0 & \mathbf{1} & 0 \\ 2 & \mathbf{1} & 0 & 0 \\ 2 & 0 & 0 & \mathbf{1} \end{pmatrix} \begin{matrix} \\ \leftarrow \\ \leftarrow \end{matrix} \sim \begin{pmatrix} 2 & \mathbf{1} & 0 & 0 \\ 1 & 0 & \mathbf{1} & 0 \\ 2 & 0 & 0 & \mathbf{1} \end{pmatrix}.$$

В результате преобразований получилось решение:

$$\begin{cases} c_2 = -2c_3, \\ c_1 = -c_3, \\ c_0 = -2c_3. \end{cases}$$

Если положить $c_3 = 1$, то решением будет вектор $(1, -2, -1, -2) = (1, 1, 2, 1)$. Искомый минимальный многочлен имеет вид

$$m_\gamma(x) = x^3 + x^2 + 2x + 1.$$

Можно сделать проверку:

$$\gamma^3 + \gamma^2 + 2\gamma + 1 = \left(\beta^2 + \beta + 2\right) + (2\beta + 1) + 2\left(\beta^2 + 1\right) + 1 =$$

$$= 3\beta^2 + 3\beta + 6 = 0.$$

Другой метод нахождения неприводимых многочленов основан на следующей теореме.

6.20. Теорема (характеристическое свойство минимального многочлена элемента конечного поля). *Пусть γ – некоторый*

элемент расширения $F_{q^n} = F_q(\beta)$ *поля* F_q *при помощи алгебраического над* F_q *элемента* β *степени* n. *Пусть* $m_\gamma(x) \in F_q[x]$ – *минимальный многочлен элемента* γ *и пусть степень его равна* m. *Тогда* $n \vdots m$ *и элементы* $\gamma, \gamma^q, \gamma^{q^2}, \ldots, \gamma^{q^{m-1}}$ *являются корнями многочлена* $m_\gamma(x)$, *причём* $m_\gamma(x)$ *является минимальным многочленом для каждого из этих элементов.*

Верно и обратное. Если $\gamma \in F_{q^n}$, $\gamma \notin F_q$ *и* m – *наименьшая степень, для которой* $\gamma^{q^m} = \gamma$, *то* $n \vdots m$ *и многочлен* $g(x) = (x-\gamma)\left(x-\gamma^q\right)\ldots\left(x-\gamma^{q^{m-1}}\right)$ *является минимальным для элемента* γ.

Доказательство. В поле $F_{q^n} = F_q(\beta)$ многочлены $\left(x^{q^n} - x\right)$ и $m_\gamma(x)$ имеют общие корни, многочлен $m_\gamma(x)$ неприводим, следовательно, $\left(x^{q^n} - x\right)$ делится на $m_\gamma(x)$ и, согласно следствию 6.5, $n \vdots m$. По теореме 6.2 корнями многочлена $m_\gamma(x)$ в поле $F_{q^m} \subseteq F_{q^n}$ являются элементы $\gamma, \gamma^q, \gamma^{q^2}, \ldots, \gamma^{q^{m-1}}$, и только они. Кратных корней этот многочлен не имеет. Кроме того (см. 4.8), любой неприводимый многочлен является минимальным для любого из своих корней.

Обратно. Если многочлен $m_\gamma(x)$ из $F_q[x]$ является минимальным для элемента γ, то $g(x) \vdots m_\gamma(x)$, т.к. у них есть общий корень γ. Если γ – корень $m_\gamma(x)$, то (см. 6.2) его корнями также будут элементы $\gamma, \gamma^q, \gamma^{q^2}, \ldots, \gamma^{q^{m-1}}$. Поэтому $m_\gamma(x) \vdots g(x)$ и, следовательно, $m_\gamma(x) = g(x)$.

6.21. Определение. Пусть дано поле F_{q^n} и элемент $\gamma \in F_{q^n}$. Элементы $\gamma, \gamma^q, \gamma^{q^2}, \ldots, \gamma^{q^{n-1}}$ называются *сопряженными* с элементом γ относительно поля F_q.

Очевидно, что элементы, сопряженные с данным элементом γ, будут различны, если минимальный многочлен γ имеет степень n. В противном случае они будут повторяться с некоторым периодом, который является делителем числа n.

6.22. Алгоритм нахождения минимального многочлена по его корням.

Пусть $\gamma \in F_{q^n}$. Вычисляем степени $\gamma, \gamma^q, \gamma^{q^2}, \gamma^{q^3}, \ldots$, до тех пор, пока не найдётся такое m, что $\gamma^{q^m} = \gamma$. Это число будет степенью искомого многочлена, а сам многочлен равен

$$g(x) = (x-\gamma)\left(x-\gamma^q\right)\left(x-\gamma^{q^2}\right)\ldots\left(x-\gamma^{q^{m-1}}\right).$$

Из теоремы 6.20 следует, что коэффициенты $g(x)$ принадлежат полю F_q. При нахождении числа m можно руководствоваться тем, что $n \vdots m$, т.к. это существенно сокращает количество его возможных значений.

6.23. Пример. Пусть $f(x) = x^3 + 2x + 1 \in F_3[x]$ и β – один из его корней в поле $F_{3^3} = F_3(\beta)$. Найти минимальный многочлен элемента $\gamma = \beta^2 + 1$.

Вычисляем степени γ^{q^k}. Предварительно можно заметить, что $3 \vdots k$ и $k \neq 1$, т.к. элемент γ не принадлежит полю F_3. В результате $k = 3$. При вычислениях удобно воспользоваться представлением всех ненулевых элементов поля F_{3^3} как степеней β (см. пример 5.23):

$$\gamma = \beta^2 + 1 = \beta^{21};\ \gamma^3 = \left(\beta^{21}\right)^3 = \beta^{11};\ \gamma^{3^2} = \left(\beta^{11}\right)^3 = \beta^7;$$

$$\gamma^{3^3} = \left(\beta^7\right)^3 = \beta^{21} = \gamma\ .$$

Утверждение о том, что $k = 3$, подтвердилось, корни многочлена $m_\gamma(x)$ найдены, записываем его через корни и вычисляем коэффициенты, пользуясь таблицей из примера 5.23:

$$m_\gamma(x) = \left(x - \beta^{21}\right)\left(x - \beta^{11}\right)\left(x - \beta^7\right) =$$

$$= x^3 - \left(\beta^{21} + \beta^{11} + \beta^7\right)x^2 + \left(\beta^{32} + \beta^{18} + \beta^{28}\right)x - \beta^{21+11+7} =$$

$$= x^3 - \left(\beta^2 + 1 + \beta^2 + \beta + 2 + \beta^2 + 2\beta + 2\right)x^2 +$$

$$+ \left(\beta^6 + \beta^{18} + \beta^2\right)x - \beta^{13} =$$

$$= x^3 - 2x^2 + \left(\beta^2 + \beta + 1 + \beta^2 + 2\beta + 1 + \beta^2\right)x - 2 =$$

$$= x^3 - 2x^2 + 2x - 2 = x^3 + x^2 + 2x + 1\ .$$

Этот многочлен является минимальным для элементов $\beta^{21} = \gamma, \beta^{11}, \beta^7$.

Многочлен $f(x) = x^3 + 2x + 1$ является минимальным для элементов β, β^3, β^9.

6.24. Замечание. Если взять степени β, отличные от $\beta^{21}, \beta^{11}, \beta^7, \beta, \beta^3, \beta^9$, и найти их минимальные многочлены, то будет найдено ещё несколько неприводимых многочленов. Можно найти минимальные многочлены всех элементов данного поля.

6.25. Пример. Найдём минимальные многочлены для некоторых (оставшихся) элементов поля F_{3^3}.

Для элементов $0, 1, 2 = \beta^{13}$ минимальными, очевидно, будут соответственно $x, x-1, x-2$. Это алгебраические элементы степени 1 над полем F_3.

Найдём последовательности сопряженных элементов для остальных степеней β:

$$\beta^2, \beta^6, \beta^{18}, \beta^{54} = \beta^2;$$

$$\beta^4, \beta^{12}, \beta^{36} = \beta^{10}, \beta^{30} = \beta^4;$$

$$\beta^5, \beta^{15}, \beta^{45} = \beta^{19}, \beta^{57} = \beta^5;$$

$$\beta^8, \beta^{24}, \beta^{72} = \beta^{20}, \beta^{69} = \beta^8;$$

$$\beta^{14}, \beta^{42} = \beta^{16}, \beta^{48} = \beta^{22}, \beta^{66} = \beta^{14};$$

$$\beta^{17}, \beta^{51} = \beta^{25}, \beta^{75} = \beta^{23}, \beta^{69} = \beta^{17}.$$

Например, найдём минимальный многочлен для последней тройки сопряжённых элементов.

$$\left(x-\beta^{17}\right)\left(x-\beta^{25}\right)\left(x-\beta^{23}\right)=$$

$$=x^3-\left(\beta^{17}+\beta^{25}+\beta^{23}\right)x^2+\left(\beta^{42}+\beta^{40}+\beta^{48}\right)x-\beta^{17+25+23}=$$

$$=x^3-\left(2\beta^2+\beta+2\beta^2+1+2\beta^2+2\beta\right)x^2+$$

$$+\left(\beta^{16}+\beta^{14}+\beta^{22}\right)x-\beta^{13}=$$

$$=x^3-x^2+(2\beta+1+2\beta+2\beta+2)x-2=$$

$$=x^3-x^2-2=x^3+2x^2+1.$$

Остальные минимальные многочлены находятся аналогично.

§2. Разложение многочленов на сомножители

Способ проверки неприводимости многочлена над полем F_q, основанный на теореме 6.8. Батлера, позволяет не только проверить, неприводим ли данный многочлен, но и получить

нетривиальное разложение в случае, если многочлен приводим над F_q.

6.26. Алгоритм Берлекэмпа разложения многочлена $f(x) \in F_q[x]$, $q = p^k$, степени n на сомножители.

1) Если $d(x) = НОД(f(x), f'(x)) \neq 1$ и $f'(x) \neq 0$, то тогда $1 < cm(d(x)) \leq cm(f'(x)) < n$ и искомым нетривиальным разложением многочлена $f(x)$ будет равенство

$$f(x) = d(x)g(x),$$

где $g(x)$ – частное от деления $f(x)$ на $d(x)$.

2) Пусть $d(x) = НОД(f(x), f'(x)) \neq 1$ и $f'(x) = 0$. Запишем многочлен $f(x)$ в стандартной форме: $f(x) = \sum_{i=0}^{n} b_i x^i$. Тогда $f'(x) = \sum_{i=1}^{n} i b_i x^{i-1} = 0$ и, следовательно, все коэффициенты производной равны нулю: $ib_i = 0$. Если $b_i \neq 0$, то необходимо, чтобы число i делилось на характеристику p поля F_q. Ввиду этого многочлен $f(x)$ можно записать в виде

$$f(x) = \sum_{\substack{i=0 \\ b_i \neq 0}}^{n} b_i x^{p \cdot \frac{i}{p}}.$$

Так как $b_i = (b_i)^{p^k} = \left((b_i)^{p^{k-1}} \right)^p$, то, положив $c_i = (b_i)^{p^{k-1}}$, получаем разложение $f(x)$ на p сомножителей:

$$f(x) = \sum_{\substack{i=0 \\ b_i \neq 0}}^{n} b_i x^{p \cdot \frac{i}{p}} = \sum_{\substack{i=0 \\ b_i \neq 0}}^{n} c_i{}^p x^{p \cdot \frac{i}{p}} = \left(\sum_{\substack{i=0 \\ b_i \neq 0}}^{n} c_i x^{\frac{i}{p}} \right)^p.$$

3) Пусть $НОД\big(f(x),f'(x)\big)=1$ и многочлен $f(x)$ приводим над F_q. Тогда ранг матрицы A системы (1) (см. 6.9) меньше, чем $n-1$, и, следовательно, существует решение $\bar{c}=(c_{n-1},c_{n-2},\ldots,c_0)$ этой системы, в котором одна из компонент $c_1,c_2,\ldots,c_{n-1}$ отлична от нуля. По решению системы находим решение $h(x)=c_{n-1}x^{n-1}+c_{n-2}x^{n-2}+\ldots+c_1x^1+c_0$ уравнения $z^q-z=0$ в кольце $F_q[x]/f(x)$. Это решение удовлетворяет условию $0<cm\big(h(x)\big)<n$. После этого нужно воспользоваться следующей теоремой.

6.27. Теорема (Берлекэмп, 1967). *Если* $f(x)$ – *нормированный многочлен из* $F_q[x]$ *и известно решение* $h(x)$ *уравнения* $z^q-z=0$ *в кольце* $F_q[x]/f(x)$ *с условием* $0<cm\big(h(x)\big)<n$, *то*

$$f(x)=\prod_{\alpha\in F_q} НОД\big(f(x),h(x)-\alpha\big),$$

причём это разложение нетривиально, т.е. существует такое $\alpha\in F_q$, *что* $0<cm\Big(НОД\big(f(x),h(x)-\alpha\big)\Big)<n$.

Доказательство. Сомножители в правой части равенства делят многочлен $f(x)$. Так как многочлены вида $h(x)-\alpha$ для разных $\alpha\in F_q$ попарно взаимно просты, то попарно взаимно просты и все $НОД\big(f(x),h(x)-\alpha\big)$. По свойству делимости 3.32.9) многочлен $f(x)$ делится на их произведение $\prod\limits_{\alpha\in F_q} НОД\big(f(x),h(x)-\alpha\big)$.

Согласно теореме 5.29, множество корней многочлена z^q-z совпадает с F_q. Ввиду этого $z^q-z=\prod\limits_{\alpha\in F_q}(z-\alpha)$. Подставляя в это равенство вместо z многочлен $h(x)$, получаем

$$\left(h(x)\right)^q - h(x) = \prod_{\alpha \in F_q} \left(h(x) - \alpha\right).$$

По условию теоремы левая часть этого равенства делится на $f(x)$. Следовательно, правая часть также делится на $f(x)$. Разложим многочлен $f(x)$ на неприводимые сомножители:

$$f(x) = \left(g_1(x)\right)^{s_1} \left(g_2(x)\right)^{s_2} \cdot \ldots \cdot \left(g_m(x)\right)^{s_m}.$$

Каждый многочлен $g_i(x)$ делит подходящий сомножитель $h(x) - \alpha_i$. Так как сомножители вида $h(x) - \alpha$ попарно взаимно просты, то многочлен $\left(g_i(x)\right)^{s_i}$ также делит $h(x) - \alpha_i$ и, следовательно, делит $НОД\left(f(x), h(x) - \alpha_i\right)$. В результате многочлен $f(x)$ делит произведение $\prod_{\alpha \in F_q} НОД\left(f(x), h(x) - \alpha\right)$.

После этого заключаем, что

$$f(x) = \prod_{\alpha \in F_q} НОД\left(f(x), h(x) - \alpha\right),$$

т.к. эти многочлены оба нормированные и делят друг друга.

6.28. Пример. Проверить неприводимость над полем F_3 многочлена $f(x) = x^4 + x^3 + x + 2$ или разложить его на сомножители.

Воспользуемся алгоритмом 6.9 при $q = 3, n = 4$. Так как $f'(x) = x^3 + 1$, $f(x) = xf'(x) + x + 2$ и $f'(x) \vdots (x + 2)$, то многочлены $f(x)$ и $f'(x)$ взаимно просты.

Находим представление многочленов $\left(x^{i3} - x^i\right), 1 \le i \le 3$, в кольце $F_3[x]/f(x)$:

$$x^3 - x \equiv x^3 + 0x^2 + 2x + 0 \left(\mathrm{mod}\, f(x)\right);$$

$x^6 - x^2 \equiv x^3 + x^2 + x + 1 \pmod{f(x)}$, т.к.

$$\begin{array}{r|l} x^6 - x^2 & x^4 + x^3 + x + 2 \\ \underline{-\,x^6 + x^5 + x^3 + 2x^2} & x^2 - x + 1 \\ -x^5 - x^3 & \\ \underline{-\,-x^5 - x^4 - x^2 - 2x} & \\ x^4 - x^3 + x^2 + 2x & \\ \underline{-\,x^4 + x^3 + x + 2} & \\ -2x^3 + x^2 + x - 2 \equiv x^3 + x^2 + x + 1 & \end{array}$$

$$x^9 - x^3 \equiv x^3\left(x^6 - 1\right) \equiv x^3\left(x^3 + 2x^2 + x\right) \equiv x^6 + 2x^5 + x^4 \equiv$$

$$\equiv 2x^3 + x \equiv 2x^3 + 0x^2 + x + 0 \pmod{f(x)}, \text{ т.к.}$$

$$\begin{array}{r|l} x^6 + 2x^5 + x^4 & x^4 + x^3 + x + 2 \\ \underline{-\,x^6 + x^5 + x^3 + 2x^2} & x^2 + x \\ x^5 + x^4 - x^3 - 2x^2 & \\ \underline{-\,x^5 + x^4 + x^2 + 2x} & \\ -x^3 - 2x \equiv 2x^3 + x & \end{array}$$

Матрица системы (1) получается, если записать коэффициенты канонических представлений многочленов $x^9 - x^3$, $x^6 - x^2$, $x^3 - x^1$ и нулевой столбец как её столбцы:

$$A = \begin{pmatrix} 2 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 2 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Ранг матрицы A равен $2 < n - 1 = 4 - 1$, т.к.

$$\begin{pmatrix} 2 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 2 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 2 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 2 \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} -1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 2 \end{pmatrix} \sim \begin{pmatrix} -1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 2 & 0 \end{pmatrix} \sim \begin{pmatrix} -1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Следовательно, данный многочлен приводим. Общим решением системы будут векторы вида $(c_3, 0, c_3, c_0)$. Для простоты можно взять $(1, 0, 1, 0)$, тогда $h(x) = x^3 + x$.

По теореме Берлекэмпа многочлен $f(x)$ раскладывается в произведение трёх сомножителей:

$$НОД\left(x^4 + x^3 + x + 2, x^3 + x\right),$$

$$НОД\left(x^4 + x^3 + x + 2, x^3 + x - 1\right),$$

$$НОД\left(x^4 + x^3 + x + 2, x^3 + x - 2\right).$$

Последовательно вычисляя их по алгоритму Евклида, находим, что:

$$НОД\left(x^4 + x^3 + x + 2, x^3 + x\right) = x^2 + 1,$$

$$НОД\left(x^4 + x^3 + x + 2, x^3 + x - 1\right) = 1,$$

$$НОД\left(x^4 + x^3 + x + 2, x^3 + x - 2\right) = x^2 + x + 2.$$

В результате получаем искомое разложение $f(x) = \left(x^2 + 1\right)\left(x^2 + x + 2\right)$.

6.29. Замечание. Так как неприводимый многочлен $f(x)$ степени n над конечным полем делит многочлен

$x^{q^n} - x = \left(x^{q^n - 1} - 1 \right) x$, то для изучения свойства неприводимости большую роль играют многочлены вида $x^{q^n} - x$ и их разложение на сомножители.

6.30. Определение. Пусть F – произвольное поле. Поле разложения многочлена $x^n - 1$ над полем F называется *n-круговым* (или *n-циклотомическим*) *полем* над F и обозначается $F^{(n)}$. Корни многочлена $x^n - 1$ в поле $F^{(n)}$ называются *корнями n-й степени из единицы* над F, их множество обозначается $E^{(n)}$.

Основным для приложений является случай поля характеристики $p \neq 0$. Это будет предполагаться в дальнейшем, хотя многие результаты данного параграфа верны и для случая $p = 0$.

6.31. Предложение. *Пусть F – поле характеристики p и n – натуральное число. Тогда справедливы следующие утверждения.*

а) Если n не делится на p, то множество $E^{(n)}$ образует циклическую подгруппу порядка n в мультипликативной группе поля $F^{(n)}$.

б) Если $n = p^k m$ для некоторых $k \geq 1$ и $m \backslash p$, то $E^{(n)} = E^{(m)}$, $F^{(n)} = F^{(m)}$ и корнями многочлена $x^n - 1$ являются элементы $E^{(m)}$, каждый из которых имеет кратность p^k.

Доказательство. а) Докажем, что множество $E^{(n)}$ замкнуто относительно произведения и взятия обратных элементов. Если $a, b \in E^{(n)}$, то $(ab)^n = a^n b^n = 1 \cdot 1 = 1$ и, следовательно, $ab \in E^{(n)}$. Аналогично $\left(a^{-1}\right)^n = \left(a^n\right)^{-1} = 1^{-1} = 1$, и поэтому $a^{-1} \in E^{(n)}$.

В результате множество $E^{(n)}$ образует подгруппу в мультипликативной группе поля $F^{(n)}$. Она будет циклической, как подгруппа циклической группы. Кроме того, все корни многочлена x^n-1 различны, т.к. из условия, что n не делится на p, следует, что x^n-1 взаимно прост со своей производной $f'(x)=nx^{n-1}$, которая имеет единственный корень 0.

б) Утверждение вытекает из равенства

$$x^n-1=x^{mp^k}-1=\left(x^m-1\right)^{p^k}.$$

6.32. Определение. *Порядком* корня a n-й степени из единицы называется его мультипликативный порядок в группе $E^{(n)}$, т.е. такое наименьшее натуральное число k, что $a^k=1$. Корень n-й степени из единицы называется *первообразным* (или *примитивным*) над F, если его порядок равен n, т.е. он порождает группу $E^{(n)}$.

Для того чтобы не было путаницы, порождающие элементы мультипликативной группы поля будем называть примитивными элементами, а порождающие элементы подгруппы $E^{(n)}$ корней n-й степени из единицы – первообразными корнями.

6.33. Предложение. *Круговое поле $F^{(n)}$ является простым алгебраическим расширением поля F.*

Доказательство. Если n и p взаимно просты, то по предыдущему предложению в поле $F^{(n)}$ существуют первообразные корни n-й степени из единицы. Пусть β – один из них, тогда, очевидно, $F^{(n)}=F(\beta)$.

Если n делится на p, то $n=p^km$ для некоторых $k\geq 1$, $m\nmid p$ и по предыдущему утверждению $F^{(n)}=F^{(m)}$. В этом случае в поле $F^{(n)}$ существует первообразный корень m-й степени из единицы и снова $F^{(n)}=F^{(m)}=F(\beta)$.

В дальнейшем мы будем в основном рассматривать случай, когда n и p взаимно просты. Поэтому первообразные корни n-й степени из единицы над F будут давать все порождающие элементы группы $E^{(n)}$. Степени любого первообразного корня дадут все остальные корни многочлена x^n-1 в поле $F^{(n)}$. Согласно свойствам порядков, если $\beta \in F^{(n)}$ и β – первообразный корень, то все остальные первообразные корни n-й степени из единицы над полем F могут быть получены как степени β^s, где $1<s<n$ и s взаимно просто с n. Различных первообразных корней степени n ровно $\varphi(n)$ штук.

Большую роль играют многочлены, корнями которых являются все первообразные корни n-й степени из единицы над полем F.

6.34. Определение. Пусть F – поле характеристики p и n – натуральное число, которое не делится на p. Пусть β – первообразный корень n-й степени из единицы над F. Тогда *n-круговым* (или *n-циклотомическим*) *многочленом* над F называется многочлен

$$Q_n(x)=\left(\prod_{\substack{s=1\\ НОД(s,n)=1}}^{n}\left(x-\beta^s\right)\right)\in F(\beta)[x].$$

6.35. Теорема (циклотомическое разложение x^n-1). *Пусть F – поле характеристики p и n – натуральное число, не делящееся на p. Тогда*

а) $x^n-1=\prod\limits_{n\vdots d} Q_d(x)$;

б) коэффициенты n-кругового многочлена принадлежат простому подполю поля F.

Доказательство. а) Пусть β – первообразный корень степени n из единицы над F. Согласно свойствам порядков,

элемент β^m имеет порядок $d=\dfrac{n}{НОД(n,m)}$, т.е. он будет первообразным корнем порядка d для единственного делителя d числа n. Так как

$$x^n-1=\prod_{m=1}^{n}\left(x-\beta^m\right),$$

то, собирая в одно произведение все сомножители вида $\left(x-\beta^m\right)$, для которых β^m является первообразным корнем степени d, получаем Q_d. Проделав это для всех натуральных делителей числа n, получим требуемую формулу.

Утверждение б) доказывается индукцией по n.

Если $n=1$, то $Q_1(x)=x-1$ удовлетворяет утверждению б). Если утверждение б) выполняется для всех $k<n$, то, положив $f(x)=\prod\limits_{\substack{n:d\\ d<n}} Q_d(x)$, получаем $Q_n(x)=\dfrac{x^n-1}{f(x)}$. Коэффициенты многочленов x^n-1 и $f(x)$ принадлежат простому подполю поля F. При делении с остатком это свойство сохранится.

6.36. Следствие. *Если r – простое число, отличное от p, то*

$$Q_{r^k}=1+x^{r^{k-1}}+x^{2r^{k-1}}+\ldots+x^{(r-1)r^{k-1}}.$$

Доказательство. Достаточно воспользоваться тем, что делителями числа r^k являются степени r^s, $0\le s\le k$, и формулой 6.35а):

$$Q_{r^k}(x)=\frac{x^{r^k}-1}{Q_{r^0}(x)Q_{r^1}(x)\ldots Q_{r^{k-1}}(x)}=\frac{x^{r^k}-1}{x^{r^{k-1}}-1}.$$

6.37. Следствие.

$$Q_n(x)=\prod_{n:d}\left(x^{\frac{n}{d}}-1\right)^{\mu(d)}=\prod_{n:d}\left(x^d-1\right)^{\mu\left(\frac{n}{d}\right)}.$$

Пусть $F(n)=x^n-1$ и $f(n)=Q_n(x)$, тогда выполняется условие $\prod_{n:d} f(d)=F(n)$ и можно применить формулу обращения Мёбиуса в мультипликативной форме (см. 6.14).

Эта формула позволяет напрямую вычислять n-циклотомические многочлены для произвольного n.

6.38. Замечание. Из следствия 6.37 следует, что многочлены $Q_n(x)$ практически не зависят от поля, над которым они рассматриваются. Их коэффициенты всегда целые числа (по модулю характеристики поля F). Не все многочлены $Q_n(x)$ являются неприводимыми не только над F, но даже над простым подполем поля F. Для практического применения можно заранее вычислить все $Q_n(x)$ до некоторого n_0.

6.39. Пример. Вычислить Q_{10}.

Согласно определению функции Мёбиуса, степень сомножителя будет ненулевой, если число $\frac{n}{d}$ равно 1 или свободно от квадратов, т.е. все простые сомножители в его каноническом разложении имеют кратность 1. Для $n=10$ таких чисел четыре: 1, 2, 5, 10. Соответственно для них $d=10,5,2,1$ и

$$Q_{10}=\left(x^{10}-1\right)^1\left(x^5-1\right)^{-1}\left(x^2-1\right)^{-1}(x-1)^1=$$

$$=\frac{\left(x^{10}-1\right)(x-1)}{\left(x^5-1\right)\left(x^2-1\right)}=\frac{\left(x^5-1\right)\left(x^5+1\right)(x-1)}{\left(x^5-1\right)(x-1)(x+1)}=$$

$$=\frac{x^5+1}{x+1}=x^4-x^3+x^2-x+1.$$

6.40. Теорема (о свойствах n-кругового поля). *Пусть натуральное число n не делится на простое число p и $q = p^k$. Тогда:*

1) размерность n-кругового поля $F_q^{(n)}$ над полем F_q равна наименьшему натуральному числу m, для которого справедливо сравнение $q^m \equiv 1 (\mathrm{mod}\, n)$;

2) круговой многочлен $Q_n(x)$ разлагается в произведение $\frac{\varphi(n)}{m}$ различных нормированных неприводимых многочленов из F_q степени m, причём поле $F_q^{(n)}$ является полем разложения каждого из этих многочленов.

Доказательство. Пусть β – первообразный корень n-й степени из единицы над F_q. Тогда справедливы равносильности:

$$\beta \in F_{q^s} \Leftrightarrow \beta^{q^s} = \beta \Leftrightarrow q^s \equiv 1 (\mathrm{mod}\, n).$$

По условию наименьшее такое s равно m. Следовательно, $\beta \in F_{q^m}$, но не принадлежит никакому собственному подполю поля F_{q^m}. Минимальный многочлен $m_\beta(x)$ элемента β над полем F_q имеет степень m. Согласно предложению 6.33, $F_q^{(n)} = F_q(\beta)$, поэтому

$$\dim\left(F_q^{(n)} / F_q\right) = \dim\left(F_q(\beta) / F_q\right) = m.$$

Так как все первообразные корни n-й степени из единицы над полем F_q являются корнями n-циклотомического многочлена $Q_n(x)$, то $Q_n(x) \vdots m_\beta(x)$ для любого первообразного корня β над полем F. Многочлены вида $m_\beta(x)$ попарно взаимно просты. Степень многочлена $Q_n(x)$ равна $\varphi(n)$, поэтому в разложении будет $\frac{\varphi(n)}{m}$ различных сомножителей.

Так как $F_q^{(n)} = F_q(\beta)$ для любого первообразного корня n-й степени β, то поле $F_q^{(n)}$ является полем разложения любого многочлена вида $m_\beta(x)$.

6.41. Замечание. Используя доказанные свойства, можно раскладывать на неприводимые над полем F_p сомножители многочлены вида $x^n - 1$, $Q_d(x)$ в случае, если степени этих многочленов не делятся на p.

Действительно:

1) корнями $Q_d(x)$ являются в точности все элементы поля F_{p^n} порядка d;

2) степень минимального многочлена элемента порядка d в любом расширении поля F_p – это наименьшее число m с условием $\left(p^m - 1\right) \vdots d$; его можно легко найти;

3) так как всего элементов порядка d имеется $\varphi(d)$ штук, то всего неприводимых многочленов степени m над F_p ровно $\dfrac{\varphi(d)}{m}$ штук;

4) Q_d раскладывается в произведение всех этих многочленов; можно записать разложение, используя метод неопределённых коэффициентов, и найти сомножители методом перебора.

6.42. Пример. Найти разложение на неприводимые сомножители над F_3 многочлена $Q_{10} = x^4 - x^3 + x^2 - x + 1$.

$d = 10$, $\varphi(10) = 10\left(1 - \dfrac{1}{2}\right)\left(1 - \dfrac{1}{5}\right) = 4$. Наименьшее m с условием $\left(3^m - 1\right) \vdots 10$ равно 4. Неприводимых многочленов

степени 4 над F_3 ровно $\frac{4}{4}=1$ штук. Следовательно, Q_{10} неприводим над F_3.

6.43. Пример. Найти разложение на неприводимые сомножители над F_2 многочлена Q_7.

Согласно формуле

$$Q_7=\frac{x^7-1}{x-1}=x^6+x^5+x^4+x^3+x^2+x+1,$$

$d=7$, $\varphi(7)=6$. Наименьшее m с условием $\left(2^m-1\right)\vdots 7$ равно 3. Количество неприводимых многочленов степени 3 над F_2 равно $\frac{\varphi(7)}{3}=\frac{6}{3}=2$. Следовательно, Q_7 разлагается над F_2 на два многочлена третьей степени. Можно считать, что многочлены нормированные и со свободным членом, равным 1: $f(x)=x^3+ax^2+bx+1$. Так как $a,b\in\{0,1\}$, то таких многочленов всего 4:

$$x^3+x^2+x+1,\ x^3+x+1,\ x^3+x^2+1,\ x^3+1.$$

Первый и последний многочлены не являются неприводимыми, т.к. имеют корень $1\in F_2$. Следовательно, остаются второй и третий многочлены. Их произведение равно

$$\left(x^3+x+1\right)\left(x^3+x^2+1\right)=$$

$$=x^6+x^4+\cancel{x^3}+x^5+\cancel{x^3}+x^2+x^3+x+1=Q_7.$$

6.44. Теорема. *Произвольное конечное поле F_q является $\left(q^n-1\right)$-круговым полем над любым из своих подполей, в частности над простым подполем F_p.*

Доказательство. Многочлен $x^{q-1}-1$ разлагается в кольце $F_q[x]$ на линейные сомножители, т.к. его корнями являются все

ненулевые элементы поля F_q. С другой стороны, этот многочлен не может полностью разлагаться над собственным подполем поля F_q, т.к. его степень будет больше количества элементов подполя. Следовательно, поле F_q является полем разложения многочлена $x^{q-1}-1$ над любым из его подполей, в частности над простым подполем F_p.

6.45. Следствие. *В поле* F_{p^n} *имеет место разложение*

$$x^{p^n-1}-1=\prod_{\left(p^n-1\right):d} Q_d(x).$$

§3. Примитивные многочлены

Как показывает примеры 5.23, 6.23, 6.25, вычисления в конечном поле F_{q^n} существенно упрощаются, если найден примитивный элемент данного поля, каноническое представление всех элементов поля и представление всех элементов в виде степеней примитивного элемента.

Можно предложить следующий

6.46. Алгоритм поиска примитивного элемента конечного поля.

1) Найти разложение числа $q^n-1=\prod_{i=1}^{k} p_i^{\alpha_i}$ в произведение различных простых чисел.

2) Если найти элементы порядков $p_i^{\alpha_i}$, то их произведение β и будет искомым примитивным элементом поля.

3) Остальные примитивные элементы будут иметь вид β^s, где степень s взаимно проста с q^n-1.

6.47. Пример. Найти примитивный элемент поля F_{3^3}.

Так как $3^3-1=26=2\cdot 13$, то достаточно найти элементы порядков 2 и 13 и взять их произведение.

Элементы порядка 2 являются корнями кругового многочлена $Q_2=\prod\limits_{2:d}\left(x^{2/d}-1\right)^{\mu(d)}=\dfrac{x^2-1}{x-1}=x+1$. Его единственный корень 2 и будет единственным элементом порядка 2.

Наименьшее k с условием $3^k\equiv 1(\mathrm{mod}13)$ равно 3. Многочлен

$$Q_{13}=\prod_{13:d}\left(x^{13/d}-1\right)^{\mu(d)}=\frac{x^{13}-1}{x-1}=$$

$$=x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1.$$

Он разлагается на $\dfrac{\varphi(13)}{3}=\dfrac{12}{3}=4$ неприводимых многочлена степени 3. Каждый корень любого из этих многочленов является элементом порядка 13 в поле F_{3^3}. Всего элементов порядка 13 будет ровно 12.

Аналогично, наименьшее k с условием $3^k\equiv 1(\mathrm{mod}26)$ равно 3. Многочлен

$$Q_{26}=\prod_{26:d}\left(x^{26/d}-1\right)^{\mu(d)}=\frac{\left(x^{26}-1\right)(x-1)}{\left(x^{13}-1\right)\left(x^2-1\right)}=\frac{x^{13}+1}{x+1}=$$

$$=x^{12}-x^{11}+x^{10}-x^9+x^8-x^7+x^6-x^5+x^4-x^3+x^2-x+1.$$

Он разлагается на $\dfrac{\varphi(26)}{3}=\dfrac{12}{3}=4$ неприводимых многочлена степени 3. Каждый корень любого из этих многочленов является элементом порядка 26 в поле F_{3^3}. Таких элементов ровно 12 штук.

В результате в поле F_{3^3} из 26 ненулевых элементов есть один элемент порядка 1 – это единица. Один элемент порядка 2 – это 2. Двенадцать элементов порядка 13 и двенадцать элементов порядка 26.

Как известно, многочлен третьей степени неприводим тогда и только тогда, когда он не имеет корней в данном поле. Если этот многочлен делит Q_{13}, то его корни имеют порядок 13. В противном случае он делит Q_{26} и его корни имеют порядок 26, т.е. являются примитивными элементами. В любом случае будет найден примитивный элемент.

Рассмотрим, например, многочлен $x^3 + x^2 + x + 2$. Перебором элементов поля F_3 убеждаемся, то он не имеет в F_3 корней. Разделим многочлен Q_{13} на него, записывая только коэффициенты.

$$
\begin{array}{l|l}
1111111111111 & \underline{\quad 1112 \quad} \\
\underline{1112} & 1002201212 \\
\quad 2111 & \\
\quad \underline{2221} & \\
\quad\ 2201 & \\
\quad\ \underline{2221} & \\
\quad\quad 1011 & \\
\quad\quad \underline{1112} & \\
\quad\quad\ 2021 & \\
\quad\quad\ \underline{2221} & \\
\quad\quad\quad 1001 & \\
\quad\quad\quad \underline{1112} & \\
\quad\quad\quad\ 2221 & \\
\quad\quad\quad\ \underline{2221} & \\
\quad\quad\quad\quad 0 &
\end{array}
$$

Многочлены разделились без остатка. Частное равно

$$x^9 + 2x^6 + 2x^5 + x^3 + 2x^2 + x + 2 .$$

В результате любой корень θ многочлена x^3+x^2+x+2 будет элементом порядка 13. Элементом порядка 26 (примитивным элементом) будет элемент 2θ.

Для поиска примитивных элементов можно использовать также их минимальные многочлены.

6.48. Определение. Многочлен $f(x)\in F_q[x]$ степени n называется *примитивным многочленом* над полем F_q, если он является минимальным многочленом некоторого примитивного элемента расширения F_{q^n} поля F_q.

Очевидно, примитивный многочлен является неприводимым над F_q. Для данного примитивного элемента его примитивный многочлен можно найти по одному из алгоритмов построения минимальных многочленов.

6.49. Пример. Найти примитивный многочлен над полем F_3.

Согласно определению, достаточно найти минимальный многочлен элемента 2θ из примера 6.47:

$$(x-2\theta)\left(x-(2\theta)^3\right)\left(x-(2\theta)^9\right)=$$

$$=x^3-2\left(\theta+\theta^3+\theta^9\right)x^2+\left(\theta^4+\theta^{10}+\theta^{12}\right)x-2\theta^{13}.$$

Находим представление коэффициентов этого многочлена в поле $F_{3^3}=F_3(\theta)$. Для этого делим многочлены $\left(x^9+x^3+x\right)$ и $\left(x^{12}+x^{10}+x^4\right)$ на многочлен $\left(x^3+x^2+x+2\right)$ с остатком (см. деление столбиком на следующей странице).

В результате получится искомый примитивный многочлен:

$$m_{2\theta}(x)=x^3-4x^2+x-2=x^3+2x^2+x+1.$$

Заметим, что в примере 5.23 уже был найден примитивный элемент β поля F_{3^3}. Его минимальный многочлен равен

x^3+2x+1. Всякий элемент поля F_{3^3} представим в виде степени β, это представление было также найдено в 5.23.

Аналогично можно найти представление всех ненулевых элементов поля F_{3^3} в виде степеней элемента 2θ. Возникают вопросы: как связаны эти представления и как от одного представления переходить к другому?

Самый простой (и прямой способ) состоит в том, чтобы найти представление элемента 2θ в виде степени β.

```
1000001010 | 1112
1112       | 1202012
 2210
 2221
  2201
  2221
   1001
   1112
    2220
    2221
       2
```

```
1010000010000 | 1112
1112          | 1211001211
 2010
 2221
  1220
  1112
   1110
   1112
     1010
     1112
      2010
      2221
       1220
       1112
        1110
        1112
           1
```

6.50. Пример. Выразить $\alpha=2\theta$ через β и наоборот в поле F_{3^3}.

По сути 2θ и β – это обозначение некоторых элементов поля F_{3^3}, которые заданы при помощи своего минимального

многочлена. Найдём элемент, записанный через β, который является корнем минимального многочлена для 2θ:

$$m_{2\theta}(x) = x^3 + 2x^2 + x + 1.$$

Так как $1 = \beta^{26} = \left(\beta^2\right)^{13}$, то элемент β^2 имеет порядок 13 и можно проверить элемент $2\beta^2$:

$$m_{2\theta}\left(2\beta^2\right) = \left(2\beta^2\right)^3 + 2\left(2\beta^2\right)^2 + \left(2\beta^2\right) + 1 =$$

$$= 2\beta^6 + 2\beta^4 + 2\beta^2 + 1 = \left(2\beta^2 + 2\beta + 2\right) + \left(2\beta^2 + \beta\right) + 2\beta^2 + 1 = 0.$$

Поскольку $2\beta^2$ является корнем многочлена $m_{2\theta}(x)$, то можно считать, что $\alpha = 2\theta = 2\beta^2 = \beta^{15}$.

Чтобы выразить β через α, достаточно возвести полученное равенство $\alpha = \beta^{15}$ в такую натуральную степень k, что $15k \equiv 1 (\mathrm{mod}\, 26)$. Решаем полученное сравнение при помощи преобразований:

$$15k \equiv 1(\mathrm{mod}\, 26) \Leftrightarrow 15k \equiv 27(\mathrm{mod}\, 26) \Leftrightarrow$$

$$\Leftrightarrow 5k \equiv 9(\mathrm{mod}\, 26) \Leftrightarrow 5k \equiv 35(\mathrm{mod}\, 26) \Leftrightarrow k \equiv 7(\mathrm{mod}\, 26).$$

В итоге получаем равенство $\beta = \alpha^7$.

После этого элементы поля F_{3^3} можно представлять в виде степеней α и степеней β, в виде многочленов степени не выше 2 от α и многочленов степени не выше 2 от β, легко переходить от одного представления к другому при помощи равенств $\alpha = \beta^{15}$ и $\alpha^7 = \beta$.

6.51. Пример. Найти все примитивные элементы поля F_{3^3}. Найти все примитивные многочлены степени 3 над полем F_3.

Примитивные элементы можно получить, возводя элемент β в степени, взаимно простые с числом $3^3-1=26$. Они будут разбиваться на группы сопряжённых элементов:

$$\beta,\ \beta^3,\ \beta^9;$$

$$\alpha=\beta^{15},\ \beta^{45}=\beta^{19},\ \beta^{19\cdot 3}=\beta^5;$$

$$\beta^7,\ \beta^{21},\ \beta^{63}=\beta^{11};$$

$$\beta^{17},\ \beta^{51}=\beta^{25},\ \beta^{75}=\beta^{23}.$$

Примитивные многочлены для первых двух троек уже найдены. Это соответственно x^3+2x+1 и x^3+2x^2+x+1. Найдём остальные два, пользуясь таблицей из примера 5.23.

$$\left(x-\beta^7\right)\left(x-\beta^{21}\right)\left(x-\beta^{11}\right)=x^3-\left(\beta^7+\beta^{21}+\beta^{11}\right)x^2+$$

$$+\left(\beta^{28}+\beta^{32}+\beta^{18}\right)x-\beta^{39}=$$

$$=x^3-\left(\beta^2+2\beta+2+\beta^2+1+\beta^2+\beta+2\right)x^2+$$

$$+\left(\beta^2+\beta^2+\beta+1+\beta^2+2\beta+1\right)x-2=$$

$$=x^3-2x^2+2x-2=x^3+x^2+2x+1.$$

$$\left(x-\beta^{17}\right)\left(x-\beta^{25}\right)\left(x-\beta^{23}\right)=x^3-\left(\beta^{17}+\beta^{25}+\beta^{23}\right)x^2+$$

$$+\left(\beta^{16}+\beta^{22}+\beta^{14}\right)x-\beta^{13}=$$

$$=x^3-\left(2\beta^2+\beta+2\beta^2+1+2\beta^2+2\beta\right)x^2+$$

$$+\left(2\beta+1+2\beta+2+2\beta\right)x-2=$$

$$=x^3-x^2-2=x^3+2x^2+1.$$

Примитивные многочлены степени 3 над полем F_3 в принципе можно пытаться найти как элементы разложения кругового многочлена $Q_{3^3-1}=Q_{26}$ на сомножители.

Это следует из того, что, согласно теореме 6.44, поле F_{q^n} является $\left(q^n-1\right)$-круговым полем над F_q. Можно вычислить $\left(q^n-1\right)$-круговой многочлен $Q_{q^n-1}(x)$ и разложить его на неприводимые над F_q сомножители, пользуясь тем, что их количество и степень легко вычисляются. Любой корень каждого из этих многочленов является первообразным корнем $\left(q^n-1\right)$-й степени из единицы над F_q, т.е. примитивным элементом поля F_{q^n}.

Для поиска примитивных многочленов можно воспользоваться понятием порядка многочлена, которое основано на следующей теореме.

6.52. Теорема. *Для всякого многочлена $f(x)$ из $F_q[x]$ степени $n\geq 1$ с условием $f(0)\neq 0$ существует такое натуральное число k, что многочлен $\left(x^k-1\right)$ делится на $f(x)$ и $k\leq q^n-1$.*

Доказательство. Фактор-кольцо $F_q[x]/f(x)$ содержит q^n-1 ненулевых элементов (классов вычетов по модулю $f(x)$). Следовательно, среди классов вычетов

$$\left[x^0\right]_{f(x)},\left[x^1\right]_{f(x)},\left[x^2\right]_{f(x)},\ldots,\left[x^{q^n-1}\right]_{f(x)},$$

порождённых степенями x, найдутся по крайней мере два совпадающих. В результате для некоторых натуральных s и t, удовлетворяющих неравенствам $0\leq s<t\leq q^n-1$, будет

выполняться сравнение $x^s \equiv x^t \left(\mathrm{mod} f(x)\right)$, т.е. многочлен $x^s - x^t = x^t\left(x^{s-t} - 1\right)$ делится на $f(x)$.

Поскольку $f(0) \neq 0$, то многочлены $f(x)$ и x взаимно просты, и по свойству делимости 3.32 получится, что $\left(x^{s-t} - 1\right)$ делится $f(x)$.

В результате нашлось натуральное число $k = t - s,\ 0 \leq k \leq q^n - 1$, для которого $\left(x^k - 1\right) \vdots f(x)$.

6.53. Определение. Пусть $f(x)$ – ненулевой многочлен из $F_q[x]$. Если $f(0) \neq 0$, то наименьшее натуральное число $k \leq q^n - 1$, удовлетворяющее условию $\left(x^k - 1\right) \vdots f(x)$, называется *порядком многочлена* $f(x)$ и обозначается $ord\left(f(x)\right)$. Если $f(0) = 0$, то многочлен можно представить в виде $f(x) = x^s g(x), g(0) \neq 0$, и тогда порядок многочлена $f(x)$ полагается равным $ord\left(g(x)\right)$.

Условие положительности степени в определении опущено, т.к. многочлен $\left(x^1 - 1\right)$ делится на любой ненулевой многочлен нулевой степени.

6.54. Теорема (о порядке неприводимого многочлена). *Пусть $f(x)$ – неприводимый многочлен степени n из $F_q[x]$ и $f(0) \neq 0$. Порядок многочлена $f(x)$ совпадает с порядком любого его корня в поле F_{q^n}.*

Доказательство. Согласно теореме 6.2, поле F_{q^n} является полем разложения многочлена $f(x)$. Все его корни имеют одинаковый порядок k. Пусть $\beta \in F_{q^n}$ – один из корней многочлена $f(x)$. Условие $\beta^k = 1$ влечёт наличие общего корня у

многочленов $f(x)$ и $\left(x^k-1\right)$. В результате они не являются взаимно простыми, а т.к. многочлен $f(x)$ неприводим, то по основному свойству неприводимых многочленов 3.36 многочлен $\left(x^k-1\right)$ делится на $f(x)$.

6.55. Следствие. *Если $f(x)$ – неприводимый многочлен степени n из кольца $F_q[x]$ и $f(0)\neq 0$, то его порядок является делителем числа q^n-1.*

Доказательство. Применяем теорему 6.54 и следствие 6.3.

Заметим, что для приводимых многочленов данное следствие не верно (см. [3]).

Понятие порядка подходит для поиска примитивных многочленов. Кроме того, вычисление порядка многочлена, основанное на делении многочленов, может оказаться проще вычисления порядка его корней в мультипликативной группе поля. Рассмотрим

6.56. Алгоритм нахождения порядка неприводимого многочлена, основанный на алгоритме вычисления порядка элемента группы 2.36.

Пусть $f(x)$ – неприводимый многочлен степени n из $F_q[x]$ и $f(0)\neq 0$. Согласно теореме 6.2.б),

$$x^{q^n-1}\equiv 1\left(\bmod f(x)\right).$$

Пусть найдено каноническое разложение числа q^n-1 на простые сомножители:

$$q^n-1=\prod_{i=1}^{k} p_i^{\alpha_i}\ .$$

Поскольку многочлен $f(x)$ неприводим $F_q[x]$, то его порядок является делителем числа q^n-1. В каноническом

разложении любого делителя числа q^n-1 участвуют те же простые числа p_i, что и в разложении исходного числа, но в меньших или равных степенях.

Проверяя справедливость сравнений

$$x^{\frac{q^n-1}{p_1}} \equiv 1\left(\operatorname{mod} f(x)\right),\ x^{\frac{q^n-1}{p_1^2}} \equiv 1\left(\operatorname{mod} f(x)\right),$$

$$x^{\frac{q^n-1}{p_1^3}} \equiv 1\left(\operatorname{mod} f(x)\right),\ ...,$$

находим наименьшее $m_1 = \dfrac{q^n-1}{p_1^{s_1}}$, $0 \le s_1 \le \alpha_1$, для которого выполняется сравнение $x^{m_1} \equiv 1\left(\operatorname{mod} f(x)\right)$.

Затем находим наименьшее $m_2 = \dfrac{m_1}{p_2^{s_2}}$, $0 \le s_2 \le \alpha_2$, для которого выполняется сравнение $x^{m_2} \equiv 1\left(\operatorname{mod} f(x)\right)$. Выполнив эту процедуру для всех простых делителей числа q^n-1, найдём $m_k = ord\left(f(x)\right)$.

Если нужно проверить, что данный неприводимый многочлен является примитивным, то, согласно теореме 6.54, достаточно проверить, что $x^{\frac{q^n-1}{p_i}} \not\equiv 1\left(\operatorname{mod} f(x)\right)$ для всех p_i, $1 \le i \le k$. Проверка осуществляется при помощи деления многочленов.

6.57. Пример. Проверить, что многочлен $f(x) = x^3 + 2x + 1 \in F_3[x]$ является примитивным над полем F_3.

Этот многочлен неприводим над полем F_3, т.к. он имеет степень 3 и не имеет корней в F_3.

Так как $3^3-1=26=2\cdot 13$, то достаточно проверить, что $x^2 \not\equiv 1 \pmod{f(x)}$ и $x^{13} \not\equiv 1 \pmod{f(x)}$. Первое условие выполняется, т.к. многочлен x^2-1 имеет степень меньшую, чем степень многочлена $f(x)$. Проверяем второе условие делением:

$$
\begin{array}{l|l}
10000000000002 & \overline{1021} \\
\underline{1021} & 1012112011 \\
1200 & \\
\underline{1021} & \\
2120 & \\
\underline{2012} & \\
1110 & \\
\underline{1021} & \\
1220 & \\
\underline{1021} & \\
2020 & \\
\underline{2012} & \\
1100 & \\
\underline{1021} & \\
1120 & \\
\underline{1021} & \\
1022 & \\
\underline{1021} & \\
1 &
\end{array}
$$

Так как получился ненулевой остаток, то многочлен $\left(x^{13}-1\right)$ не делится на $f(x)$ и, следовательно, $f(x)$ является примитивным многочленом над полем F_3.

Задачи для самостоятельного решения

1. Проверить по теореме Батлера неприводимость:

а) многочлена $g(x)=x^4+x^3+1$ над полем F_2;

б) многочлена $g(x)=x^3+2x^2+x+6$ над полем F_7;

в) многочлена $g(x)=x^4+3x^3+2x^2+2x+1$ над полем F_5;

г) многочлена $g(x)=x^5+x^4+x^3+2x^2+x+1$ над полем F_3.

2. Пусть дан неприводимый многочлен $f(x)=x^4+x^3+x^2+x+1\in F_2[x]$. Пусть β – один из его корней в поле $F_{2^4}=F_2(\beta)$. Найти минимальный многочлен:

а) элемента $\left(\beta^3+\beta+1\right)$ методом неопределённых коэффициентов;

б) элемента $\left(\beta^3+\beta+1\right)$ по его корням.

3. Пусть дан неприводимый многочлен $f(x)=x^2+3x+1\in F_7[x]$. Пусть β – один из его корней в поле $F_{7^2}=F_7(\beta)$. Найти минимальный многочлен:

а) элемента $(3\beta+5)$ методом неопределённых коэффициентов;

б) элемента $(3\beta+5)$ по его корням.

4. Пусть дан неприводимый многочлен $f(x)=x^6+x+1\in F_2[x]$. Пусть β – один из его корней в поле $F_{2^6}=F_2(\beta)$. Найти минимальный многочлен:

а) элемента $\left(\beta^5+\beta^4+\beta^2+\beta+1\right)$ методом неопределённых коэффициентов;

б) элемента $\left(\beta^5+\beta^4+\beta^2+\beta+1\right)$ по его корням.

5. Пусть дан неприводимый многочлен $f(x)=x^4+x^2+x+1\in F_3[x]$. Пусть β – один из его корней в поле $F_{3^4}=F_3(\beta)$. Найти минимальный многочлен:

а) элемента $\left(2\beta^3+\beta+1\right)$ методом неопределённых коэффициентов;

б) элемента $\left(2\beta^3+\beta+1\right)$ по его корням.

6. Используя теорему Берлекэмпа, разложить на сомножители многочлен:

а) $g(x)=x^7+x^4+x^2+x+1\in F_2[x]$;

б) $g(x)=x^5+2x^2+2x+2\in F_3[x]$;

в) $g(x)=x^4+3x^3+2x^2+2x+1\in F_5[x]$;

г) $g(x)=x^5+3x^3+2x^2+2x+1\in F_7[x]$.

7. Используя теорему Берлекэмпа, разложить на сомножители многочлен:

а) $g(x)=x^5+x^4+1\in F_2[x]$;

б) $g(x)=x^5+2x^2+2x+2\in F_3[x]$;

в) $g(x)=x^4+3x^3+2x^2+2x+1\in F_5[x]$;

г) $g(x)=x^5+3x^3+2x^2+2x+1\in F_7[x]$.

ГЛАВА 7. ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ

§1. Основные определения

Эллиптические кривые находят применение в криптографии, т.к. на множестве их точек может быть определена группа, которая при соответствующем выборе параметров имеет достаточный уровень сложности. Кроме того, операция в ней допускает эффективное вычисление. Ниже, после небольшого вступления, мы рассмотрим конкретные разновидности таких групп.

Пусть дано некоторое поле F. Рассмотрим многочлен $f(x,y)$ степени n от двух переменных над полем F. Множество точек $(x,y), x,y \in F$, координаты которых удовлетворяют уравнению $f(x,y)=0$, называется *алгебраической кривой степени n* над полем F.

Точка (x_0,y_0) называется *неособой*, если в ней не равны нулю одновременно обе частные производные многочлена $f(x,y)$. Естественно, при этом рассматриваются формальные производные. Для поля действительных чисел это означает, что в точке (x_0,y_0) существует касательная к кривой. Касательная задаётся уравнением

$$(x-x_0)\frac{df(x_0,y_0)}{dx}+(y-y_0)\frac{df(x_0,y_0)}{dy}=0.$$

Кривая называется *гладкой*, если она не имеет особых точек. *Эллиптической кривой* над полем F называется всякая гладкая алгебраическая кривая третьего порядка, которая имеет хотя бы одну точку.

Если характеристика поля F не равна 2, то эллиптическую кривую можно привести к так называемой *форме Вейерштрасса*:

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6,\ a_i\in F. \qquad (1)$$

Условие гладкости означает, что в поле F ни одна из точек кривой не удовлетворяет системе уравнений

$$\begin{cases} a_1 y - 3x^2 - 2a_2 x - a_4 = 0, \\ 2y + a_1 x + a_3 = 0. \end{cases}$$

Ниже всегда предполагается, что условие гладкости кривой выполняется не только над данным полем, но и над его алгебраическим замыканием.

При помощи специального вида замен координат уравнение эллиптической кривой в форме Вейерштрасса можно подвергнуть дальнейшему упрощению. В результате в зависимости от характеристики поля получатся следующие основные случаи.

7.1. Если характеристика поля F не равна 2 и 3, то кривая может быть задана уравнением

$$y^2 = x^3 + a_4 x + a_6,\ a_i \in F\ .$$

Для выполнения условия гладкости нужно потребовать, чтобы не имела решений система

$$\begin{cases} y^2 = x^3 + a_4 x + a_6, \\ -3x^2 - a_4 = 0, \\ 2y = 0. \end{cases}$$

После очевидных преобразований система приобретает следующий вид:

$$\begin{cases} g(x) = x^3 + a_4 x + a_6 = 0, \\ g'(x) = 3x^2 + a_4 = 0. \end{cases}$$

Неразрешимость последней системы над алгебраическим замыканием F означает, что многочлен $g(x)$ не имеет кратных корней, т.е. его дискриминант $\Delta = \left(\frac{a_4}{3}\right)^3 + \left(\frac{a_6}{2}\right)^2$ отличен от нуля.

Другой вариант проверки условия гладкости кривой – это условие $НОД\big(g(x),g'(x)\big)=1$.

7.2. Если характеристика поля F равна 3, то кривая может быть задана уравнением

$$y^2=x^3+a_2x^2+a_4x+a_6,\ a_i\in F.$$

Как и в предыдущем случае, условие гладкости равносильно тому, что следующая система не имеет решений:

$$\begin{cases} y^2=x^3+a_2x^2+a_4x+a_6, \\ -2a_2x-a_4=0, \\ 2y=0; \end{cases} \Leftrightarrow \begin{cases} x^3+a_2x^2+a_4x+a_6=0, \\ a_2x=a_4. \end{cases}$$

7.3. Если характеристика поля F равна 2, то кривая может быть задана уравнением одного из следующих двух видов:

а) $y^2+a_3y=x^3+a_4x+a_6,\ a_i\in F$ (суперсингулярная кривая);

б) $y^2+xy=x^3+a_2x^2+a_6,\ a_i\in F$ (несуперсингулярная кривая).

К множеству точек некоторой кривой E добавим фиктивную бесконечно удалённую точку O и обозначим полученное множество $E(F)$. На этом множестве будет определяться операция сложения.

§2. Определение группы точек эллиптической кривой

Пусть E – некоторая эллиптическая кривая над полем F. Для каждой точки $(x,y)\in E(F)$ полагаем по определению

$$(x,y)+O=O+(x,y)=(x,y),\ O+O=O.$$

Точка O будет играть роль нуля – нейтрального элемента по сложению. Определение, данное выше, гарантирует выполнение соответствующей аксиомы.

7.4. Предложение (формула противоположного элемента). *С каждой точкой* (x,y) *эллиптическая кривая содержит точку* $\widetilde{(x,y)}=(x,-a_1x-a_3-y)$.

Доказательство. Утверждение можно проверить, подставив координаты точки $\widetilde{(x,y)}$ в уравнение (1). Можно отдельно проверять утверждение в каждом из случаев 7.1–7.3.

Действительно, если кривая имеет уравнение $y^2=x^3+a_4x+a_6$ или $y^2=x^3+a_2x^2+a_4x+a_6$, то $a_1=a_3=0$, $\widetilde{(x,y)}=(x,-a_1x-a_3-y)=(x,-y)$ и утверждение следует из того, что y входит в оба уравнения в чётной степени.

Если поле F имеет характеристику 2 и кривая задаётся уравнением вида $y^2+a_3y=x^3+a_4x+a_6$, то $a_1=0$, $\widetilde{(x,y)}=(x,-a_1x-a_3-y)=(x,y+a_3)$ и

$$(y+a_3)^2+a_3(y+a_3)=y^2+\cancel{a_3^2}+a_3y+\cancel{a_3^2}=y^2+a_3y.$$

Если поле F имеет характеристику 2 и кривая задаётся уравнением вида $y^2+xy=x^3+a_2x^2+a_6$, то $a_1=1, a_3=0$, $\widetilde{(x,y)}=(x,-a_1x-a_3-y)=(x,x+y)$ и

$$(x+y)^2+x(x+y)=\cancel{x^2}+y^2+\cancel{x^2}+xy=y^2+xy.$$

После этого положим $(x,y)+\widetilde{(x,y)}=\widetilde{(x,y)}+(x,y)=O$, т.е.

$$-(x,y)=\widetilde{(x,y)}.$$

В результате для каждой точки определена противоположная точка.

7.5. Сложение двух разных точек, не являющихся противоположными. Пусть $P=(x_1,y_1)$ и $Q=(x_2,y_2)$ – две точки на эллиптической кривой и $x_1\neq x_2$. Определим сумму $P+Q$. Для этого рассмотрим прямую, содержащую эти точки. Её уравнение имеет вид $y-y_1=k(x-x_1)$ или $y=kx-(kx_1-y_1)=kx-b$.

Коэффициент k находится из условия, что точка Q также удовлетворяет уравнению прямой:

$$y_2 - y_1 = k(x_2 - x_1) \Leftrightarrow k = \frac{y_2 - y_1}{x_2 - x_1}.$$

Если подставить в уравнение эллиптической кривой вместо y выражение $kx - b$, то получится уравнение третьей степени от x, которое уже имеет два решения – x_1 и x_2. Очевидно, что в этом случае уравнение имеет и третье решение – x_3. Точка (x_3, y_3), где $y_3 = kx_3 - (kx_1 - y_1)$ по построению принадлежит данной эллиптической кривой (и данной прямой). Элемент x_3 можно найти по теореме Виета 3.63, т.к. коэффициент при x^2 в уравнении третьей степени равен сумме корней с противоположным знаком.

1) Случай поля характеристики, не равной 2 и 3.

$$y^2 = x^3 + a_4 x + a_6 \Leftrightarrow (kx - b)^2 = x^3 + a_4 x + a_6 \Leftrightarrow$$

$$\Leftrightarrow x^3 - k^2 x^2 + \ldots = 0;$$

$$x_3 = k^2 - x_1 - x_2.$$

2) Случай поля характеристики 3.

$$y^2 = x^3 + a_2 x^2 + a_4 x + a_6 \Leftrightarrow$$

$$\Leftrightarrow (kx - b)^2 = x^3 + a_2 x^2 + a_4 x + a_6 \Leftrightarrow$$

$$\Leftrightarrow x^3 - \left(k^2 - a_2\right) x^2 + \ldots = 0;$$

$$x_3 = k^2 - a_2 - x_1 - x_2.$$

3) Случай суперсингулярной кривой над полем характеристики 2.

$$y^2 + a_3 y = x^3 + a_4 x + a_6 \Leftrightarrow$$

$$\Leftrightarrow (kx - b)^2 + a_3 (kx - b) = x^3 + a_4 x + a_6 \Leftrightarrow$$

$$\Leftrightarrow\ x^3 - k^2x^2 + \ldots = 0\,;$$

$$x_3 = k^2 - x_1 - x_2 = k^2 + x_1 + x_2\,.$$

4) Случай несуперсингулярной кривой над полем характеристики 2.

$$y^2 + xy = x^3 + a_2x^2 + a_6\ \Leftrightarrow$$

$$\Leftrightarrow\ \big(kx - b\big)^2 + x\big(kx - b\big) = x^3 + a_2x^2 + a_6\ \Leftrightarrow$$

$$\Leftrightarrow\ x^3 - \Big(k^2 + k - a_2\Big)x^2 + \ldots = 0\,;$$

$$x_3 = k^2 + k - a_2 - x_1 - x_2 = \Big(k^2 + k + a_2\Big) + x_1 + x_2\,.$$

По определению полагаем $P + Q = -\big(x_3, y_3\big)$.

Пусть теперь $P = \big(x_1, y_1\big)$ и $Q = \big(x_2, y_2\big)$ – две точки на эллиптической кривой, для которых $x_1 = x_2$. Так как правые части уравнения (1) для этих точек совпадают, приравняем левые части уравнения:

$$y_1^2 + a_1x_1y_1 + a_3y_1 = y_2^2 + a_1x_2y_2 + a_3y_2\ \Leftrightarrow$$

$$\Leftrightarrow\ y_1^2 - y_2^2 = a_1x_2y_2 + a_3y_2 - a_1x_1y_1 - a_3y_1\ \Leftrightarrow$$

$$\Leftrightarrow\ \big(y_1 - y_2\big)\big(y_1 + y_2\big) = \big(y_2 - y_1\big)\big(a_1x_1 + a_3\big)\ .$$

В результате возникают два случая.

1) $y_1 = y_2$. Это случай когда точки P и Q совпадают.

2) $y_2 = -y_1 - a_1x_1 - a_3$. Это случай, когда данные точки являются противоположными. Их сумма была определена выше. Поэтому осталось определить сумму в первом случае.

7.6. Сложение двух одинаковых точек. Пусть дана точка $P = \big(x_1, y_1\big)$ на эллиптической кривой, которая не совпадает со своей противоположной точкой: $P \neq -P$, $y_1 \neq -a_1x_1 - a_3 - y_1$.

Определим $P+P=2P$. Для этого рассмотрим касательную к кривой в данной точке. Её уравнение имеет вид:

$$y=kx-b\text{, где } b=kx_1-y_1,$$

$$k=-\left.\frac{df(x,y)/dx}{df(x,y)/dy}\right|_{x=x_1,y=y_1}=-\frac{a_1y_1-3x_1^2-2a_2x_1-a_4}{2y_1+a_1x_1+a_3}.$$

Заметим, что знаменатель не может обратиться в ноль, т.к. по условию $y_1\neq -a_1x_1-a_3-y_1$.

Для доказательства существования точки (x_3,y_3), лежащей одновременно на касательной и на эллиптической кривой, подставим $y=kx-b$ в уравнение (1) и докажем, что $x_1=x_2$ является кратным решением полученного уравнения:

$$(kx-b)^2+a_1x(kx-b)+a_3(kx-b)=x^3+a_2x^2+a_4x+a_6.$$

Для этого достаточно доказать, что $x_1=x_2$ является корнем производной, т.е. решением уравнения

$$2k(kx-b)+a_1(kx-b)+a_1kx+a_3k=3x^2+2a_2x+a_4.$$

Подставляем $x=x_1$, $y_1=kx_1-b$:

$$2ky_1+a_1y_1+a_1kx_1+a_3k=3x_1^2+2a_2x_1+a_4\ \Leftrightarrow$$

$$\Leftrightarrow\ k(2y_1+a_1x_1+a_3)=-a_1y_1+3x_1^2+2a_2x_1+a_4.$$

Последнее равенство выполняется по определению k.

Для вычисления координат точки (x_3,y_3) достаточно вычислить угловой коэффициент k по новой формуле и воспользоваться формулами из пункта 7.5.

1) Характеристика поля не равна 2 и 3.

Уравнение имеет вид $y^2=x^3+a_4x+a_6$, поэтому

$$k=-\frac{a_1y_1-3x_1^2-2a_2x_1-a_4}{2y_1+a_1x_1+a_3}=-\frac{-3x_1^2-a_4}{2y_1}=\frac{3x_1^2+a_4}{2y_1}.$$

2) Характеристика поля равна 3.

Уравнение кривой имеет вид $y^2=x^3+a_2x^2+a_4x+a_6$, поэтому

$$k=-\frac{-3x_1^2-2a_2x_1-a_4}{2y_1}=\frac{a_2x_1-a_4}{y_1}.$$

3) Характеристика поля равна 2. Случай суперсингулярной кривой.

$$y^2+a_3y=x^3+a_4x+a_6;$$

$$k=-\frac{a_1y_1-3x_1^2-2a_2x_1-a_4}{2y_1+a_1x_1+a_3}=-\frac{-3x_1^2-a_4}{2y_1+a_3}=\frac{x_1^2+a_4}{a_3}.$$

4) Характеристика поля равна 2. Случай несуперсингулярной кривой.

$$y^2+xy=x^3+a_2x^2+a_6;$$

$$k=-\frac{a_1y_1-3x_1^2-2a_2x_1-a_4}{2y_1+a_1x_1+a_3}=-\frac{y_1-3x_1^2}{x_1}=\frac{y_1+x_1^2}{x_1}.$$

По определению полагаем $2P=-(x_3,y_3)$.

В результате на множестве $E(F)$ определена бинарная операция $+$, для которой справедлива следующая

7.7. Теорема (А. Пуанкаре). *Множество $E(F)$ относительно операции $+$ является коммутативной группой.*

Наличие нейтрального элемента O и противоположных элементов было обеспечено ещё в процессе определения операции сложения точек. Коммутативность следует из того, что суммируемые точки (x_1,y_1) и (x_2,y_2) входят в формулы симметрично. Ассоциативность операции сложения можно проверить непосредственными вычислениями. Однако эти

вычисления весьма громоздки, и мы их приводить не будем. Существуют и другие доказательства этой теоремы (см. [14]).

7.8. Пример. Пусть $F = F_5$. Рассмотрим кривую над полем F, заданную уравнением $y^2 = x^3 + 2x + 1$. Проверим, что она является гладкой:

$$\Delta = \left(\frac{2}{3}\right)^3 + \left(\frac{1}{2}\right)^2 = 4^3 + 3^2 = 64 + 9 = 4 + 4 = 3 \neq 0 .$$

Найдём точку на этой кривой. Пусть, например, $x = 0$, тогда $y = \pm 1$. Вычислим $2(0,1)$.

$$k = \frac{3x_1^2 + a_4}{2y_1} = \frac{3 \cdot 0 + 2}{2 \cdot 1} = 1 ; \; x_3 = k^2 - 2x_1 = 1 - 2 \cdot 0 = 1 ;$$

$$y_3 = kx_3 - b = kx_3 - (kx_1 - y_1) = 1 \cdot 1 - (1 \cdot 0 - 1) = 2 .$$

Следовательно,

$$2(0,1) = -(1,2) = (1,-2) .$$

Проверим, что точка $(1,-2)$ удовлетворяет уравнению кривой:

$$y^2 = x^3 + 2x + 1; \; (-2)^2 = 4 = 1^3 + 2 \cdot 1 + 1 .$$

Вычислим $(0,1) + (1,-2)$.

$$k = \frac{y_2 - y_1}{x_2 - x_1} = \frac{-2 - 1}{1 - 0} = -3 = 2 ;$$

$$x_3 = k^2 - x_1 - x_2 = 2^2 - 0 - 1 = 3 ;$$

$$y_3 = kx_3 - b = kx_3 - (kx_1 - y_1) = 2 \cdot 3 - (2 \cdot 0 - 1) + 1 = 7 = 2 .$$

В результате

$$(0,1) + (1,-2) = -(3,2) = (3,-2) .$$

7.9. Пример. Пусть $F = F_{3^3}$. Это поле было рассмотрено в примере 5.23. Оно изоморфно расширению $F = F_3(\beta)$, где β – корень многочлена $f(x) = x^3 + 2x + 1$. В вычислениях мы будем использовать представление элементов поля F, полученное в примере 5.23. Рассмотрим кривую над полем F, заданную уравнением $y^2 = x^3 + 2x + \beta$. Кривая является гладкой, т.к. второе уравнение системы из 7.2 решений не имеет:

$$\begin{cases} x^3 + a_2x^2 + a_4x + a_6 = 0, \\ a_2x = a_4; \end{cases} \Leftrightarrow \begin{cases} x^3 + 2x + \beta = 0, \\ 0 \cdot x = 2. \end{cases}$$

Методом подбора найдём точку на кривой. Пусть, например, $x = \beta^2$, тогда

$$x^3 + 2x + \beta = \beta^6 + 2\beta^2 + \beta = \beta^2 + \beta + 1 + 2\beta^2 + \beta =$$

$$= 2\beta + 1 = \beta^{16} = y^2.$$

Отсюда

$$y = \beta^8, \; y = -\beta^8 = -\left(2\beta^2 + 2\right) = \beta^2 + 1 = \beta^{21}.$$

Вычислим $2\left(\beta^2, \beta^8\right)$:

$$k = \frac{a_2x_1 - a_4}{y_1} = \frac{-2}{\beta^8} = -2\beta^{18} = \beta^{18};$$

$$x_3 = k^2 - 2x_1 = \beta^{36} + \beta^2 = \beta^{10} + \beta^2 = \beta^2 + \beta + \beta^2 = \beta^{17};$$

$$y_3 = kx_3 - (kx_1 - y_1) = \beta^{18}\beta^{17} - \left(\beta^{18}\beta^2 - \beta^8\right) =$$

$$= \beta^9 - \beta^{20} + \beta^8 = \beta + \cancel{1} - \cancel{2\beta^2} - \beta - \cancel{1} + \cancel{2\beta^2} + 2 = 2;$$

$$2\left(\beta^2, \beta^8\right) = -\left(\beta^{17}, 2\right) = \left(\beta^{17}, -2\right).$$

Проверка:

$$x^3 + 2x + \beta = \beta^{51} + 2\beta^{17} + \beta = 2\beta^2 + 1 + 2\left(2\beta^2 + \beta\right) + \beta = 1 = (-2)^2.$$

В общем случае, когда нет заранее вычисленного представления элементов данного поля F, все вычисления нужно производить в фактор-кольце $F[x]/f(x)$.

§3. Порядок группы точек эллиптической кривой

В приложениях основными являются следующие задачи.

1) Определение порядка q группы точек эллиптической кривой. Необходимо, чтобы этот порядок либо был простым числом $q = p$, либо, в крайнем случае, имел «большой» простой делитель: $q = sp,\ s \ll p$.

2) Вычисление (случайной) точки на кривой.

3) Определение порядка точки эллиптической кривой. Отыскание точки кривой заданного порядка p.

Для полей с небольшим количеством элементов порядок группы точек эллиптической кривой можно вычислить, перебрав в качестве x все элементы данного поля.

7.10. Пример. Найти порядок группы $E(F_7)$ кривой $y^2 = x^3 + x + 1$.

Во-первых, проверяем, что кривая является гладкой:

$$\Delta = \left(\frac{1}{3}\right)^3 + \left(\frac{1}{2}\right)^2 = \frac{1}{27} + \frac{1}{4} = \frac{1}{6} + 2 = 6 + 2 = 1 \neq 0 \pmod 7.$$

Во-вторых, вычисляем квадраты всех элементов по модулю 7, т.к. нам понадобится извлекать квадратный корень:

$$0^2 = 0,\ 1^2 = 1,\ 2^2 = 4,\ 3^2 = 2,\ 4^2 = 2,\ 5^2 = 4,\ 6^2 = 1 \pmod 7.$$

Затем перебираем все элементы $x \in \mathbb{Z}_7$ и находим соответствующие им y:

если $x = 0$, то $y^2 = 0^3 + 0 + 1 = 1$ и $y = 0,\ y = 6$;

если $x = 1$, то $y^2 = 1^3 + 1 + 1 = 3$ и y не существует;

если $x=2$, то $y^2=2^3+2+1=4$ и $y=2, y=5$;

если $x=3$, то $y^2=3^3+3+1=3$ и y не существует;

если $x=4$, то $y^2=4^3+4+1=6$ и y не существует;

если $x=5$, то $y^2=5^3+5+1=5$ и y не существует;

если $x=6$, то $y^2=6^3+6+1=6$ и y не существует.

В результате, с учётом бесконечно удалённой точки получилось пять элементов.

7.11. Формула для вычисления порядка группы точек эллиптической кривой на основе символа Лежандра. Пусть $p>2$. Рассмотрим эллиптическую кривую над полем F_p. Как показывает предыдущий пример, нужно подсчитать количество решений квадратичного сравнения вида

$$y^2=f(x)(\mathrm{mod}\,p).$$

Любое такое сравнение имеет $1+\left(\frac{f(x)}{p}\right)$ решений, где $\left(\frac{f(x)}{p}\right)$ – символ Лежандра. Учитывая бесконечно удалённую точку, получаем общее количество точек эллиптической кривой над полем F_p, $p>2$:

$$1+\sum_{x=0}^{p-1}\left(1+\left(\frac{f(x)}{p}\right)\right)=p+1+\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right).$$

С использованием свойств символа Лежандра по этой формуле можно вычислять $\left|E\left(F_p\right)\right|$ для случая относительно небольших p. Для больших простых чисел, которые используются на практике, трудоёмкость этого алгоритма становится неприемлемой.

Общей формулы для вычисления порядка группы точек эллиптической кривой не найдено. Однако для большинства

случаев есть алгоритмы. Основным является алгоритм Шуфа (R. Schoof, 1985) и различные его модификации. Этот алгоритм имеет сложность порядка $O\left(\log^6 p\right)$ операций по модулю p и позволяет вычислять порядок группы для чрезвычайно больших $\left(p \approx 10^{500}\right)$ простых чисел. Сам алгоритм и его доказательство весьма громоздки, и мы не будем его здесь рассматривать (см. [14, 17]).

Общую оценку порядка группы точек эллиптической кривой даёт

7.12. Теорема (Хассе). *Порядок N группы точек некоторой эллиптической кривой E над конечным полем F_q удовлетворяет неравенству*

$$|N - q - 1| \le 2\sqrt{q} \ .$$

Доказательство см. в [14]. Неравенство является точным. Его можно переписать в виде

$$q + 1 - 2\sqrt{q} \le N \le q + 1 + 2\sqrt{q} \ .$$

7.13. Пример. Для кривой, которая рассматривалась в примере 7.10, неравенство имеет вид:

$$7 + 1 - 2\sqrt{7} \le N \le 7 + 1 + 2\sqrt{7} \ \Leftrightarrow \ 3 \le N \le 13 \ .$$

Найденное значение $N = 5$ лежит в данном промежутке. Однако видно, что промежуток достаточно большой.

Если рассматривать кривые над полем F_{q^n}, то можно воспользоваться

7.14. Теоремой (Хассе-Вейль). Если N *– порядок группы точек некоторой эллиптической кривой E над конечным полем F_q, то для порядка $N(n)$ группы этой же кривой над полем F_{q^n} справедлива формула*

$$N(n) = q^n + 1 - x_1^n - x_2^n \ ,$$

где x_1, x_2 *– (комплексные) корни квадратного уравнения* $x^2 - tx + q = 0$, $t = q + 1 - N$.

7.15. Пример. Найти порядок группы точек кривой $y^2 = x^3 + x + 1$ над полем F_{7^5}.

Воспользуемся теоремой Хассе-Вейля и примером 7.10:

$$N = 5\ ,\ t = 7 + 1 - 5 = 3\ ;$$

$$x^2 - 3x + 7 = 0 \Leftrightarrow x_{1,2} = \frac{3 \pm \sqrt{9 - 28}}{2} = \frac{3 \pm i\sqrt{19}}{2}\ .$$

Выражение $x_1^5 + x_2^5$ вычисляем при помощи бинома Ньютона. При этом слагаемые на чётных местах сократятся, а на нечётных – удвоятся:

$$x_1^5 + x_2^5 = \frac{2}{32}\left(3^5 + C_5^2 \cdot 3^3 \cdot i^2 19 + C_5^4 \cdot 3 \cdot i^4 19^2\right) =$$

$$= \frac{1}{16}\left(3^5 - 10 \cdot 27 \cdot 19 + 5 \cdot 3 \cdot 19^2\right) = \frac{528}{16} = 33\ ;$$

$$N(5) = 7^5 + 1 - 33 = 16775 = 5^2 \cdot 11 \cdot 61\ .$$

7.16. Пример. Найти порядок группы точек кривой $y^2 = x^3 + 2x + 1$ над полем F_{3^3}.

Гладкость кривой проверяется так же, как и в примере 7.9: второе уравнение соответствующей системы несовместно. Найдём порядок кривой над полем F_3 методом перебора:

если $x = 0$, то $y^2 = 1$ и $y = \pm 1$;

если $x = 1$, то $y^2 = 1 + 2 + 1 = 1$ и $y = \pm 1$;

если $x = 2$, то $y^2 = 8 + 4 + 1 = 1$ и $y = \pm 1$.

С учётом бесконечно удалённой точки $\left|E(F_3)\right| = 7$. Затем воспользуемся теоремой Хассе-Вейля:

$$N = 7\ ;\ t = 3 + 1 - 7 = -3\ ;$$

$$x^2+3x+3=0\ ,\ x_{1,2}=\frac{-3\pm\sqrt{9-12}}{2}=\frac{-3\pm i\sqrt{3}}{2}\ .$$

$$x_1^3+x_2^3=\frac{2}{8}\left((-3)^3+3\cdot(-3)^1\cdot i^2 3\right)=\frac{1}{4}(-27+27)=0\ ;$$

$$N(3)=3^3+1-0=28=2^2\cdot 7\ .$$

7.17. Пример. Для кривой из примера 7.16 найти точку, лежащую на ней. Найти её порядок. Найти точку максимального простого порядка.

Будем перебирать значения x и пытаться вычислить y. В приложениях x выбирается случайным образом. Для вычислений в поле F_{3^3} будем использовать результаты примера 5.23. Для полей с очень большим количеством элементов вычисление такой таблицы становится невозможным, и поэтому используются непосредственные вычисления в фактор-кольце многочленов.

$$x=\beta;\ y^2=x^3+2x+1=\beta^3+2\beta+1=(\beta+2)+2\beta+1=0\ .$$

Точка $P=(\beta,0)$ имеет порядок 2, т.к. она противоположна сама себе и по определению сложения $2P=O$.

$$x=\beta+1;\ y^2=x^3+2x+1=(\beta+1)^3+2(\beta+1)+1=$$

$$=\beta^3+1+2(\beta+1)+1=(\beta+2)+1+2(\beta+1)+1=0\ .$$

Аналогично $ord(\beta+1,0)=2$.

$$x=\beta^2;\ y^2=\beta^6+2\beta^2+1=\left(\beta^2+\beta+1\right)+2\beta^2+1=\beta+2=\beta^3\ .$$

Корень квадратный из β^3 не существует.

$$x=\beta^5;\ y^2=\beta^{15}+2\beta^5+1=\left(2\beta^2\right)+2\left(2\beta^2+\beta+2\right)+1=$$

$$=2\beta+2=\beta^{22}\ ;\ \ y=\pm\beta^{11}\ .$$

Вычислим порядок точки $P=\left(\beta^5,\beta^{11}\right)$ в группе точек эллиптической кривой $y^2=x^3+2x+1$ над полем F_{3^3}. Так как группа имеет 28 элементов, то порядок может быть равен 1, 2, 4, 7, 14 или 28. Порядок 1 имеет только точка O, поэтому начинаем с 2. Пользуемся формулами для поля характеристики 3.

Вычисляем $2P=2\left(\beta^5,\beta^{11}\right)$.

$$k=\frac{a_2x_1-a_4}{y_1}=\frac{-2}{y_1}=\frac{1}{y_1}=\frac{1}{\beta^{11}}=\beta^{15};$$

$$x_3=k^2-2x_1=\beta^{30}-2\beta^5=\left(\beta^2+2\beta\right)-2\left(2\beta^2+\beta+2\right)=2;$$

$$y_3=k\left(x_3-x_1\right)+y_1=\beta^{15}\left(2-\beta^5\right)+\beta^{11}=2\beta^{15}-\beta^{20}+\beta^{11}=$$

$$=2\left(2\beta^2\right)-\left(2\beta^2+\beta+1\right)+\left(\beta^2+\beta+2\right)=1;\ -y_3=-1;$$

$$2P=\left(2,-1\right).$$

Вычисляем $4P=2\left(2,-1\right)$.

$$k=\frac{1}{y_1}=\frac{1}{-1}=2;\ x_3=k^2-2x_1=4-2\cdot2=0;$$

$$y_3=2(0-2)-1=1;\ 4P=\left(0,-1\right).$$

Вычисляем $6P=4P+2P=\left(0,-1\right)+\left(2,-1\right)$.

$$k=\frac{y_2-y_1}{x_2-x_1}=\frac{-1-(-1)}{2-0}=0;\ x_3=k^2-x_1-x_2=0-0-2=1;$$

$$y_3=0(1-0)-1=-1=2;\ 6P=\left(1,-2\right)=\left(1,1\right).$$

Вычисляем $7P=6P+P=\left(1,1\right)+\left(\beta^5,\beta^{11}\right)$.

$$k=\frac{y_2-y_1}{x_2-x_1}=\frac{\beta^{11}-1}{\beta^5-1}=\frac{\beta^2+\beta+1}{2\beta^2+\beta+1}=\frac{\beta^6}{\beta^{20}}=\beta^{12};$$

$$x_3 = \beta^{24} - 1 - \beta^5 = \left(2\beta^2 + 2\beta + 1\right) - 1 - \left(2\beta^2 + \beta + 2\right) = \beta + 1;$$

$$y_3 = \beta^{12}\left(\beta + 1 - 1\right) + 1 = \beta^{13} + 1 = 2 + 1 = 0;\ 7P = \left(\beta + 1, 0\right).$$

Точка $7P$ является обратной к самой себе, поэтому, согласно правилам сложения, $14P = O$ и $ord(P) = 14$.

Максимальный простой порядок имеет, например, точка $Q = 2P = \left(2, -1\right)$. Согласно свойству порядков 2.16.4), другими точками порядка 7 будут $2Q, 3Q, 4Q, 5Q, 6Q$.

В общем случае для вычисления кратных точек используется

7.18. Аддитивный вариант алгоритма вычисления степени. Для вычисления кратной точки nP нужно сделать следующее.

1) Представить в двоичной системе число n:

$$n = x_k 2^k + x_{k-1} 2^{k-1} + \ldots + x_1 2^1 + x_0,\ x_i \in \left\{0, 1\right\}.$$

2) Вычислить $2^i P$ для всех $1 \le i \le k$.

3) Вычислить $\left(x_k 2^k\right)P + \left(x_{k-1} 2^{k-1}\right)P + \ldots + \left(x_1 2^1\right)P + x_0 P$.

Для реализации алгоритма понадобится k операций удвоения (в п. 2) и не более k сложений (в п. 3).

Для полей с большим количеством элементов построение таблицы умножения или представление каждого элемента в каноническом виде и в виде степени примитивного элемента становится практически невозможным, поэтому при поиске точки на эллиптической кривой необходимо уметь вычислять квадратные корни. Для этого разработаны различные алгоритмы (см., например, [1]).

Ниже будут рассмотрены некоторые алгоритмы извлечения квадратного корня в конечных полях с нечётным количеством элементов.

7.19. Утверждение. *В произвольном конечном поле* F_q, *q – нечётно, ненулевой элемент a представим в виде квадрата другого элемента тогда и только тогда, когда* $a^{\frac{q-1}{2}} = 1$.

Доказательство. Если $a = x^2$, $x \in F_q$, то

$$a^{\frac{q-1}{2}} = \left(x^2\right)^{\frac{q-1}{2}} = x^{q-1} = 1 .$$

Пусть $a^{\frac{q-1}{2}} = 1$ и g – примитивный элемент поля F_q. Тогда $a = g^k$ для некоторого k и $a^{\frac{q-1}{2}} = \left(g^k\right)^{\frac{q-1}{2}} = g^{\frac{k(q-1)}{2}} = 1$. Согласно свойствам порядка, показатель степени $\frac{k(q-1)}{2}$ делится на $(q-1)$ и, следовательно, $k \vdots 2$, $k = 2m$. В этом случае

$$a = g^k = g^{2m} = \left(g^m\right)^2 ,$$

т.е. элемент a представим в поле F_q в виде квадрата.

7.20. Теорема. *Пусть F_q – конечное поле и $q \equiv 3 (\mathrm{mod}\, 4)$. Если корни квадратные из ненулевого элемента $a \in F_q$ существуют, то они равны* $\pm a^{\frac{q+1}{4}}$.

Доказательство. Заметим, что $\frac{q+1}{4}$ – целое число. Проверяем утверждение теоремы, воспользовавшись 7.19:

$$\left(\pm a^{\frac{q+1}{4}}\right)^2 = a^{\frac{q+1}{2}} = a^{\frac{q-1}{2}+1} = a^{\frac{q-1}{2}} \cdot a \overset{(7.19)}{=} 1 \cdot a = a .$$

Алгоритм вычисления корня квадратного в таком поле состоит в том, чтобы вычислить степень $x = a^{\frac{q+1}{4}}$ и проверить, что

$x^2 = a$. Если последнее равенство выполняется, то корень квадратный из $a \in F_q$ существует и равен $\pm a^{\frac{q+1}{4}}$, если нет, то корень квадратный не существует.

7.21. Теорема. *Пусть F_q – конечное поле и $q \equiv 5 (\mathrm{mod} 8)$. Если корни квадратные из ненулевого элемента $a \in F_q$ существуют, то они равны $\pm\left(a^{\frac{q+3}{8}} \cdot b^{\frac{(q-1)s}{4}} \right)$, где $b \in F_q$ – элемент, который не может быть представлен в виде квадрата, а s равно 0 или 1.*

Доказательство. Из 7.19. следует, что $b^{\frac{q-1}{2}} = -1$. Пусть $x^2 = a$. Проверяем элементы из теоремы по определению квадратного корня:

$$\left(a^{\frac{q+3}{8}} \cdot b^{\frac{(q-1)s}{4}} \right)^2 = a^{\frac{q+3}{4}} \cdot b^{\frac{(q-1)s}{2}} = a^{\frac{q-1}{4}} \cdot a \cdot b^{\frac{(q-1)s}{2}} =$$

$$= x^{\frac{q-1}{2}} \cdot a \cdot b^{\frac{(q-1)s}{2}}.$$

Если $x^{\frac{q-1}{2}} = 1$, то подходит случай $s = 0$.

Если $x^{\frac{q-1}{2}} = -1$, то подходит случай $s = 1$.

Алгоритм вычисления корня квадратного в данном поле состоит в том, чтобы вычислить элементы $x = \pm\left(a^{\frac{q+3}{8}} \cdot b^{\frac{(q-1)s}{4}} \right)$, $s = 0,1$, и проверить для них условие $x^2 = a$. Если ни один не подойдёт, то корней квадратных из элемента a не существует.

Остался последний случай: $q \equiv 1 (\mathrm{mod} 8)$. В этом случае компактную формулу корня квадратного записать трудно, т.к. она получается как результат выполнения некоторого алгоритма.

7.22. Теорема. *Пусть* F_q *– конечное поле,* $q \equiv 1 (\mathrm{mod} 8)$, $q = 2^k h + 1$, $k \geq 3$, h *– нечётное число. Пусть* $b \in F_q$ *– элемент, который не является квадратом. Если корни квадратные из ненулевого элемента* $a \in F_q$ *существуют, то они равны* $\pm\left(a^{\frac{h+1}{2}} \cdot b^{sh} \right)$, *где* $0 \leq s \leq 2^{k-1} - 1$ *– некоторое подходящее число.*

Доказательство. Согласно 7.19, $a^{2^{k-1}h} = 1$, $b^{2^{k-1}h} = -1$. Извлекая квадратный корень, получаем, что $a^{2^{k-2}h} = \pm 1$. Чтобы компенсировать возможный «минус», домножаем правую часть этого равенства на $b^{s_0 2^{k-1}h}$, где $s_0 = 0$, если $a^{2^{k-2}h} = +1$, и $s_0 = 1$, если $a^{2^{k-2}h} = -1$. В результате

$$a^{2^{k-2}h} \cdot b^{s_0 2^{k-1}h} = 1.$$

Снова извлекаем квадратный корень и получаем $a^{2^{k-3}h} \cdot b^{s_0 2^{k-2}h} = \pm 1$. Чтобы компенсировать возможный «минус», снова домножаем правую часть последнего равенства на $b^{(s_1 2)2^{k-2}h} = b^{s_1 2^{k-1}h}$, где $s_1 = 0$, если $a^{2^{k-3}h} \cdot b^{s_0 2^{k-2}h} = +1$, и $s_1 = 1$, если $a^{2^{k-3}h} \cdot b^{s_0 2^{k-2}h} = -1$. В результате

$$a^{2^{k-3}h} \cdot b^{s_0 2^{k-2}h} \cdot b^{(s_1 2)2^{k-2}h} = a^{2^{k-3}h} \cdot b^{(s_0 + 2s_1)2^{k-2}h} = 1.$$

Далее продолжаем аналогично и на $(k-1)$-м шаге получаем

$$a^h \cdot b^{\left(s_0 + 2s_1 + 2^2 s_2 + \ldots + 2^{k-2} s_{k-2}\right)2h} = 1.$$

Положим $s = s_0 + 2s_1 + 2^2 s_2 + \ldots + 2^{k-2} s_{k-2}$, тогда $0 \leq s \leq 2^{k-1} - 1$ и $a^h \cdot b^{s2h} = 1$.

После этого по определению проверяется, что квадратными корнями из элемента a будут элементы $\pm\left(a^{\frac{h+1}{2}}\cdot b^{sh}\right)$.

В этом случае алгоритм вычисления корня квадратного сложнее. Сначала нужно вычислить все степени $a^{2^i h}, 0\le i\le k-1$, $b^{2^j h}, 1\le j\le k-1$. Если $a^{2^{k-1}h}\ne 1$, то корней нет. Затем, перемножая соответствующие степени и определяя знак соответствующего произведения, нужно вычислить коэффициенты s_i и s. И, наконец, вычислить значения корней.

7.23. Пример. Записать формулу для вычисления квадратного корня в поле F_{3^3}. Вычислить квадратные корни из 2β и $\beta+1$.

Так как $q=27\equiv 3(\mathrm{mod}\,4)$, то нужно воспользоваться теоремой 7.20:

$$a^{\frac{q+1}{4}}=a^{\frac{28}{4}}=a^7.$$

Пусть $a=2\beta$, тогда $a^7=(2\beta)^7=2\beta^7=2\beta^2+\beta+1$. Делаем проверку, используя пример 5.23:

$$\left(\pm 2\beta^7\right)^2=\beta^{14}=2\beta.$$

В результате $\sqrt{2\beta}=\pm 2\beta^7=\pm\left(2\beta^2+\beta+1\right)$.

Пусть $a=\beta+1$, тогда

$$a^7=(\beta+1)^7=\left(\beta^9\right)^7=\beta^{11}=\beta^2+\beta+2.$$

Проверка: $\left(\pm\beta^{11}\right)^2=\beta^{22}=2\beta+2\ne\beta+1$. В результате корень квадратный из элемента $\beta+1$ в поле F_{3^3} не существует.

Задачи для самостоятельного решения

1. Проверить условие гладкости эллиптической кривой над полем P, вычислить все элементы группы её точек и порядок группы.

а) $y^2+\left(\beta^2+\beta+1\right)y=x^3+\left(\beta^3+1\right)x+1$, $P=F_{2^4}=F_2(\beta)$;

б) $y^2=x^3+3x+2$, $P=F_{5^2}$;

в) $y^2=x^3+2x^2+x+1$, $P=F_{3^3}$.

2. На каждой кривой из предыдущей задачи выбрать произвольно точки A, B и C. Для каждого случая вычислить:

а) $A+B, B+C, A+C$;

б) $ord(A), ord(B), ord(C)$.

3. Пользуясь теоремой Хассе-Вейля, вычислить порядок группы точек данной кривой над полем P:

а) $y^2=x^3+3x+2$, $P=F_{5^4}$;

б) $y^2=x^3+2x^2+x+1$, $P=F_{3^7}$.

4. Вычислить корень квадратный из элемента a в поле F_q:

а) $a=29 \quad q=67$; б) $a=38 \quad q=53$;

в) $a=3 \quad q=73$.

ЛИТЕРАТУРА

1. *Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А.* Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы. 2-е изд., доп. – М.: КомКнига, 2012. – 356 с.

2. *Глухов М.М., Елизаров В.П., Нечаев А.А.* Алгебра: учебник. – СПб.: Изд-во «Лань», 2015. – 608 с.

3. *Лидл Р., Нидеррайтер Г.* Конечные поля: в 2 т. – М.: Мир, 1988.

4. *Лидл Р., Пильц Г.* Прикладная абстрактная алгебра: учеб. пособие. – Екатеринбург: Изд-во Урал. ун-та, 1996.

5. *Садовничий В., Носов В., Ященко В.* Криптография как один из источников развития математики // Научные и методологические проблемы информационной безопасности / под. ред. В.П. Шерстюка. МЦНМО, 2004. – С. 11–18.

Учебные пособия издательства НГПУ

6. *Тропин М.П.* Теория чисел: курс лекций для студентов математического факультета. – Новосибирск: Изд-во НГПУ, 2006.

7. *Кузьмичёв А.И., Тропин М.П.* Теория чисел: задачник-практикум для студентов 3-го курса математического факультета. – Новосибирск: Изд-во НГПУ, 2009.

8. *Тропин М. П.* Алгебра: теория делимости: курс лекций для студентов 2-го курса ИФМИЭО. – Новосибирск: Изд-во НГПУ, 2011.

9. *Тропин М. П.* Алгебра: теория делимости: практикум для студентов 2-го курса ИФМИЭО. – Новосибирск: Изд-во НГПУ, 2011.

10. *Тропин М. П., Урман А. А.* Алгебра: многочлены, алгебраические числа, элементы теории кодирования: курс лекций для студентов 2-го курса математического факультета. – Новосибирск: Изд-во НГПУ, 2008.

11. *Тропин М. П., Урман А. А.* Алгебра: многочлены, алгебраические числа, элементы теории кодирования: задачник-практикум для студентов 2-го курса математического факультета. – Новосибирск: Изд-во НГПУ, 2008.

Учебные пособия по теории кодирования и криптографии

12. *Берлекэмп Э.* Алгебраическая теория кодирования. – М.: Мир, 1971.

13. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. – М.: Мир, 1986.

14. *Гашков С.Б., Применко Э.Ф., Черепнёв М.А.* Криптографические методы защиты информации. – М.: Издательский центр «Академия», 2010.

15. *Герман О.Н., Нестеренко Ю.В.* Теоретико-числовые методы в криптографии: учебник для студ. учреждений высш. проф. образования. – М.: Издательский центр «Академия», 2012. – 272 с.

16. *Глухов М.М., Круглов И.А., Пичкур А.Б., Черёмушкин А.В.* Введение в теоретико-числовые методы криптографии. – СПб.: Лань, 2011. – 400 с.

17. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки. – М.: Мир, 1976.

18. *Применко Э.*А. Алгебраические основы криптографии. – М.: Книжный дом «ЛИБРОКОМ», 2013. – 288 с.

19. *Ростовцев А.Г.* Алгебраические основы криптографии. – СПб.: НПО «Мир и семья»; ООО «Интерлайн», 2000. – 354 с.

20. *Рябко Б.Я., Фионов А.Н.* Криптографические методы защиты информации. – М.: Горячая линия-Телеком, 2012.

21. *Сидельников В.М.* Теория кодирования. – М.: ФИЗМАТЛИТ, 2008. – 324 с.

22. *Соловьёва Ф.И.* Введение в теорию кодирования: учеб. пособие. 2-е изд. – Новосибирск: Редакц.-изд. центр НГУ, 2011. – 124 с.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

СОДЕРЖАНИЕ

Михаил Петрович ТРОПИН

ОСНОВЫ ПРИКЛАДНОЙ АЛГЕБРЫ

Учебное пособие

Издание второе, стереотипное

Редакция
естественнонаучной литературы

ЛР № 065466 от 21.10.97
Гигиенический сертификат 78.01.10.953.П.1028
от 14.04.2016 г., выдан ЦГСЭН в СПб

Издательство «ЛАНЬ»
lan@lanbook.ru; www.lanbook.com;
196105, Санкт-Петербург, пр. Юрия Гагарина, д. 1, лит. А.
Тел.: (812) 412-92-72, 336-25-09.
Бесплатный звонок по России: 8-800-700-40-71

ГДЕ КУПИТЬ

ДЛЯ ОРГАНИЗАЦИЙ:

Для того, чтобы заказать необходимые Вам книги, достаточно обратиться в любую из торговых компаний Издательского Дома «ЛАНЬ»:

по России и зарубежью
«ЛАНЬ-ТРЕЙД». 196105, Санкт-Петербург, пр. Ю. Гагарина, д. 1, лит. А.
тел.: (812) 412-85-78, 412-14-45, 412-85-82; тел./факс: (812) 412-54-93
e-mail: trade@lanbook.ru; ICQ: 446-869-967

www.lanbook.com
пункт меню **«Где купить»**
раздел **«Прайс-листы, каталоги»**

в Москве и в Московской области
«ЛАНЬ-ПРЕСС». 109387, Москва, ул. Летняя, д. 6
тел.: (499) 722-72-30, (495) 647-40-77; e-mail: lanpress@lanbook.ru

в Краснодаре и в Краснодарском крае
«ЛАНЬ-ЮГ». 350901, Краснодар, ул. Жлобы, д. 1/1
тел.: (861) 274-10-35; e-mail: lankrd98@mail.ru

ДЛЯ РОЗНИЧНЫХ ПОКУПАТЕЛЕЙ:

интернет-магазин
Издательство «Лань»: http://www.lanbook.com

магазин электронных книг
Global F5: http://globalf5.com/

Подписано в печать 29.03.20.
Бумага офсетная. Гарнитура Школьная. Формат 60×90 $^{1}/_{16}$.
Печать офсетная. Усл. п. л. 18,00. Тираж 30 экз.

Заказ № 322-20.

Отпечатано в полном соответствии
с качеством предоставленного оригинал-макета
в АО «Т8 Издательские Технологии».
109316, г. Москва, Волгоградский пр., д. 42, к. 5.