Н. Н. ЕРМОЛАЕВА,
В. А. КОЗЫНЧЕНКО,
Г. И. КУРБАТОВА

ПРАКТИЧЕСКИЕ ЗАНЯТИЯ ПО АЛГЕБРЕ

ЭЛЕМЕНТЫ ТЕОРИИ МНОЖЕСТВ, ТЕОРИИ ЧИСЕЛ, КОМБИНАТОРИКИ. АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ

Под редакцией Г. И. Курбатовой

ДОПУЩЕНО
УМО вузов РФ по образованию в области прикладных математики и физики в качестве учебного пособия для студентов, обучающихся по направлению подготовки «Прикладные математика и физика», а также для студентов, обучающихся по другим направлениям и специальностям в области естественных и математических наук, техники и технологии

ЛАНЬ®
САНКТ-ПЕТЕРБУРГ · МОСКВА · КРАСНОДАР
2014

ББК 22.1я73
Е 74

Ермолаева Н. Н., Козынченко В. А., Курбатова Г. И.
Е 74 Практические занятия по алгебре. Элементы теории множеств, теории чисел, комбинаторики. Алгебраические структуры: Учебное пособие / Под ред. Г. И. Курбатовой. — СПб.: Издательство «Лань», 2014. — 112 с. — (Учебники для вузов. Специальная литература).

ISBN 978-5-8114-1657-8

Книга охватывает материал первых лекций курса алгебры. В пособии рассмотрены задачи из элементарной теории множеств и отображений, простейшие задачи по алгебраическим структурам, задачи по элементарной теории чисел, комбинаторные задачи.

Настоящее учебное пособие является первым в запланированной серии, состоящей из четырех частей и охватывающей весь обязательный практический материал по курсу алгебры для обучающихся по образовательным программам подготовки бакалавров университетов и технических вузов по направлениям «Прикладные математика и физика», «Прикладные математика и информатика» и «Фундаментальная информатика и информационные технологии».

ББК 22.1я73

Рецензенты:
А. Ю. УТЕШЕВ — доктор физико-математических наук, профессор Санкт-Петербургского государственного университета;
В. Ф. ЗАЙЦЕВ — доктор физико-математических наук, профессор кафедры математического анализа РГПУ им. А. И. Герцена.

Обложка
Е. А. ВЛАСОВА

ПРЕДИСЛОВИЕ

В учебный процесс в последнее время добавляются новые дисциплины, это приводит к сокращению основных курсов и неизбежно сказывается на качестве их изложения. Недостаток времени, отведенного на практические занятия по алгебре, вынуждает преподавателей ряд важных и интересных задач либо оставлять для самостоятельного решения (что по силам не всем студентам), либо исключать из рассмотрения. Курс алгебры читается в первые семестры обучения. Как показывает опыт, некоторым студентам для усвоения потока новой информации не хватает практики обращения с новыми понятиями. Те несколько задач, которые преподаватель успевает рассмотреть в отведенные программой часы, оказываются явно недостаточными. Авторы надеются, что данное учебное пособие частично исправит эту ситуацию и поможет студентам как в усвоении основных положений теории, так и в овладении методами решения задач. Мы включили также некоторые интересные задачи, освещающие важные нюансы теории, которые не рассматриваются на лекциях ввиду ограниченности отведенных часов.

Настоящее учебное пособие является *первым* в запланированной серии, состоящей из четырех частей и охватывающей весь обязательный практический материал по курсу алгебры для бакалавриата университетов по специальностям «Прикладные математика и физика», «Прикладные математика и информатика» и «Информационные технологии».

Пособие охватывает материал первых 4 лекций курса алгебры. В § 1 рассмотрены задачи из элементарной теории множеств и отображений, в § 2 — простейшие задачи по алгебра-

ическим структурам, в § 3 — задачи по элементарной теории чисел, в § 4 — комбинаторные задачи.

В следующей, *второй части* серии, рассмотрены задачи по комплексным числам и многочленам, в *третьей части* — задачи по матрицам, системам линейных уравнений и определителям, в *четвертой, заключительной части*, рассмотрены задачи линейной алгебры.

На весь курс алгебры программой предусмотрено порядка 37 лекций, поэтому и курс, и практические занятия содержат *только необходимый минимум*, утвержденный государственным образовательным стандартом по указанным специальностям.

В начале каждого параграфа кратко (без доказательств) сформулированы основные положения соответствующего раздела теории, далее следуют формулировки рассматриваемых задач и отдельный большой раздел, посвященный их решению. Задачи для самостоятельного решения снабжены указаниями и ответами.

Последовательность задач и их содержание согласованы с курсом алгебры, который более 15 лет читается одним из авторов на факультете прикладной математики–процессов управления Санкт-Петербургского государственного университета.

В учебном пособии содержится *около 140 задач, и практически все они снабжены подробными решениями*. Это познакомит читателей с приемами и методами решения определенного круга задач алгебры и будет хорошей стартовой площадкой для решения более сложных задач. Уместно напомнить, что польза от готового решения возможна только в том случае, если перед обращением к нему предприняты попытки самостоятельного решения. Поэтому авторы настоятельно рекомендуют читателям обращаться к разделу «Решения и ответы» только после упорной самостоятельной работы. Наличие подробных решений большинства задач окажет помощь в самоконтроле и в выработке навыков решения задач. Кроме того, оно будет весьма полезно для лиц, самостоятельно

изучающих алгебру. Задачи 1, 3 и 4 параграфов представляют интерес для учителей и учащихся старших классов физико-математических школ и лицеев. Электронный вариант учебного пособия может быть использован при дистанционной форме обучения.

При работе над пособием авторы пользовались монографиями, учебниками и задачниками, список которых приведен в конце книги, там же для удобства читателей приведен список используемых обозначений и сокращений.

Наш приятный долг — поблагодарить профессоров Н. В. Егорова и Д. А. Овсянникова, которые явились инициаторами этой работы. Мы признательны Ю. В. Волкову и нашим рецензентам — профессорам А. Ю. Утешеву и В. Ф. Зайцеву — за внимательное прочтение рукописи, плодотворное обсуждение ряда вопросов и полезные замечания.

Авторы

§ 1. ЭЛЕМЕНТЫ ТЕОРИИ МНОЖЕСТВ. ОТОБРАЖЕНИЯ

Множество — совокупность различимых объектов. Это фундаментальное понятие математики. Множество задается либо перечислением его элементов, либо указанием правила, определяющего принадлежность элементов к этому множеству. Элементы множества *должны быть различимы*, порядок перечисления элементов не существенен.

Пример. ▷ Множество натуральных чисел $\mathbf{N}$ можно задать следующим образом: $\mathbf{N} = \{x \in \mathbf{Z} \mid x > 0\}$, где $\mathbf{Z}$ — множество целых чисел. Множество B целых чисел, дающих при делении на натуральное число m $(m > 3)$ остаток 3: $B = \{3 + qm | \, q \in \mathbf{Z}\}$. ◁

Пустое множество $\varnothing$ — множество, не содержащее ни одного элемента.

Множество B является **подмножеством** (п/м) множества A, если B состоит из некоторой совокупности элементов из A $(B \subset A)$. Каждое множество имеет два тривиальных п/м, это — оно само и пустое множество, все другие п/м называются *нетривиальными*.

Операции с множествами и их свойства

Равенство. Множества A и B равны, если состоят из одних и тех же элементов. Для доказательства равенства двух множеств надо доказать два включения:

$$A = B \quad \leftrightarrow \quad A \subset B \quad \text{и} \quad B \subset A.$$

Объединение (дизъюнкция) $A \cup B$ множеств A и B состоит из элементов, которые принадлежат хотя бы одному из множеств: A или B.

Пересечение (конъюнкция) $A \cap B$ множеств A и B состоит из элементов, которые принадлежат обоим множествам A и B.

Разность $A \setminus B$ состоит из элементов множества A, не принадлежащих множеству B.

Универсальное множество U — всеобъемлющее множество в рассматриваемом круге задач. (Например, $U = \mathbf{Z}$ для задач о целых числах.)

Дополнение $\overline{A}$ множества A (до универсального множества) $\overline{A} = U \setminus A$ есть множество элементов из U, не принадлежащих A.

Например, для множества четных чисел $\mathbf{Z}_1$, являющегося подмножеством множества $\mathbf{Z}$ целых чисел, дополнением $\overline{\mathbf{Z}}_1$ служит множество $\mathbf{Z}_2$ нечетных чисел:

$$\overline{\mathbf{Z}}_1 = \mathbf{Z} \setminus \mathbf{Z}_1 = \mathbf{Z}_2.$$

Здесь роль универсального множества играет множество $\mathbf{Z}$.

Пусть A — подмножество множества B. Дополнением $\overline{A}$ множества A до множества B называется множество элементов из B, не принадлежащих множеству A:

$$\overline{A} = B \setminus A.$$

Основные свойства операций со множествами

1. $A \cup A = A, \quad A \cap A = A$ (*рефлексивность*).

2. $A \cup B = B \cup A, \quad A \cap B = B \cap A$ (*коммутативность*).

3. $A \cup (B \cup C) = (A \cup B) \cup C$ (*ассоциативность*).

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

4. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (*дистрибутивность*).

5. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (*дистрибутивность*).

6. $A \setminus B = A \cap \overline{B}$ (это равенство позволяет переходить от разности множеств к их пересечению).

7. Свойства универсального множества: $A \cup U = U$, $A \cap U = A$.

8. Свойства пустого множества: $A \cup \varnothing = A, \quad A \cap \varnothing = \varnothing$.

9. Свойства дополнения: $\overline{\overline{A}} = A, \quad A \cup \overline{A} = U, \quad A \cap \overline{A} = \varnothing$.

10. $A \cap B = \varnothing \leftrightarrow A \setminus B = A$.

11. $A \subset B \leftrightarrow A \setminus B = \varnothing$.

12. $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

13. $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

14. $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.

15. $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

Декартово произведение множеств

Множество $\{(a, b) |\ a \in A,\ b \in B\}$ упорядоченных пар называется **декартовым произведением** множеств A и B и обозначается $A \times B$. Декартово произведение множеств в общем случае не коммутативно, поэтому в каждой паре важен порядок. Операция декартового произведения множеств дистрибутивна относительно операций объединения и пересечения множеств:

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

Операция $\times$ обобщается на n множеств, что позволяет ввести понятие степени множества: $A^n = A \times A \times \ldots \times A$.

Разбиение множества. Говорят, что подмножества B, C множества A образуют **разбиение** A, если они удовлетворяют двум требованиям: 1) $B \cap C = \varnothing$; 2) $B \cup C = A$.

17. Понятие разбиения обобщается на n подмножеств. Подмножества $A_1, \ldots, A_n$ образуют разбиение A, если

1) $A_i \cap A_j = \varnothing$ при $i \neq j$, $i, j = 1, \ldots, n$;

2) $A_1 \cup \ldots \cup A_n = A$.

18. Множества $A \setminus B$ и $A \cap B$ образуют разбиение множества A.

Множество называется **конечным**, если его элементы можно занумеровать натуральными числами от 1 до n. Пустое множество $\varnothing$ полагается конечным.

Мощность конечного множества равна количеству его элементов. Мощность множества A обозначается $\operatorname{Card} A$ или $|A|$; $|\varnothing| = 0$. Для двух непересекающихся конечных множеств очевидно равенство

$$A \cap B = \varnothing \to |A \cup B| = |A| + |B|.$$

Аналогичное равенство имеет место и для n конечных попарно непересекающихся множеств.

19. Для любых конечных множеств A и B имеет место равенство

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

Мощность декартового произведения *конечных* множеств A и B равна $|A \times B| = |A||B|$.

Отношения эквивалентности

20. Бинарным отношением ω на множествах A и B называется любое подмножество ω их декартова произведения $\omega \subset A \times B$.

Элементы $x \in A$ и $y \in B$ находятся в отношении ω, если $(x, y) \in \omega$, это обозначается также $x\omega y$, при этом говорится, что x находится в отношении ω к y. Бинарным отношением на множестве A называется подмножество D его декартового произведения: $D \subset A \times A$. Важным классом бинарных отношений являются отношения эквивалентности.

Бинарное отношение $\sim$ на множестве A называется **отношением эквивалентности**, если оно *рефлексивно*, *симметрично* и *транзитивно*, а именно:

1) $x \sim x$ для $\forall\, x \in A$ (*рефлексивность*);

2) $x \sim y \to y \sim x$ для $\forall\, x, y \in A$ (*симметричность*);

3) $x \sim y$ и $y \sim z \to x \sim z$ для $\forall\, x, y, z \in A$ (*транзитивность*).

Пример. Отношение равенства является отношением эквивалентности на любом множестве.

Пусть на множестве A задано отношение эквивалентности $\omega \subset A \times A$. **Классом эквивалентности** K_x называется множество всех $y \in A$, для которых $(x, y) \in \omega$. Каждый элемент $x \in A$ задает класс эквивалентности $K_x = \{y \in A \mid y \sim x\}$.

Свойства классов эквивалентности

21. Все элементы в одном классе эквивалентны между собой.

22. Класс эквивалентности K_a содержит элемент a.

23. Классы эквивалентности целиком покрывают множество A, т. е. их объединение равно A.

24. Два класса эквивалентности на множестве A либо совпадают, либо не пересекаются.

25. Классы эквивалентности образуют разбиение множества A.

26. $K_a = K_b \leftrightarrow a \sim b$.

27. Задание любого разбиения $A_1, \ldots, A_s$ множества A задает на нем отношение эквивалентности. **Фактормножеством** множества A по отношению эквивалентности $(\sim)$ называется множество, обозначаемое $A/_\sim$, элементами которого являются классы эквивалентности, а именно:

$A/_\sim = \{K_{x_1}, \ldots, K_{x_n}\}$.

Отображения

Пусть X, Y — некоторые множества. Правило f, по которому *каждому* элементу $a \in X$ ставится в соответствие *один и только один* элемент $f(a) \in Y$, называется **отображением** и обозначается $\boxed{f : X \to Y.}$

Тождественное отображение $\mathrm{Id}_X : X \to X$ любому элементу ставит в соответствие сам же этот элемент $\mathrm{Id}_X(x) = x$.

Образом элемента $x \in X$ при отображении $f : X \to Y$ называется элемент $y \in Y$, в который это отображение переводит x, т. е. $y = f(x) \in Y$. Для $\forall\, x \in X$ образ $f(x) \in Y$ *существует и единственен*. Пусть $A \subset X$, подмножество $f(A) \subset Y$ есть *образ подмножества* A при отображении $f : X \to Y$:

$$f(A) = \{y \in Y \mid \exists\, x \in A,\ f(x) = y\}.$$

Подмножество $f(X) \subset Y$ называется **образом отображения** $f : X \to Y$ и обозначается $\mathrm{Im}\, f$

$$\mathrm{Im}\, f \stackrel{d}{=} f(X) \subset Y.$$

28. Отображение $f : X \to Y$ называется **инъективным**, если оно не «склеивает», т. е. если для $\forall\, x_1, x_2 \in X$

$$\boxed{x_1 \neq x_2} \to \boxed{f(x_1) \neq f(x_2).}$$

29. Отображение $f : X \to Y$ называется **сюръективным**, если множество Y не содержит элементов, в которые ничего «не перешло», т. е. если $\boxed{\operatorname{Im} f = Y.}$

30. Отображение $f : X \to Y$ называется **биективным** (или *взаимно однозначным*), если оно инъективно и сюръективно одновременно.

Прообразом $f^{-1}(y)$ элемента $y \in Y$ при отображении $f : X \to Y$ называется подмножество множества X, состоящее из элементов, перешедших при этом отображении в элемент y.

Определения инъективных, сюръективных и биективных отображений можно дать в терминах прообразов элементов, а именно:

31. Отображение $f : X \to Y$ *инъективно*, если прообраз любого элемента $y \in Y$ содержит *не более одного элемента*.

32. Отображение $f : X \to Y$ *сюръективно*, если прообраз любого элемента $y \in Y$ содержит *не менее одного элемента*.

33. Отображение $f : X \to Y$ *биективно*, если прообраз любого элемента $y \in Y$ *состоит из одного элемента*.

Равенство двух отображений $f_1 : X_1 \to Y_1$ и $f_2 : X_2 \to Y_2$ означает, что совпадают множества $X_1 = X_2 = X$ и $Y_1 = Y_2 = Y$, кроме того, для $\forall x \in X$ выполняется равенство $f_1(x) = f_2(x)$.

Композиция отображений. Пусть заданы два отображения $f : X \to Y$ и $g : Y \to Z$. Отображение, определенное следующим образом: $h : X \to Z \quad h = g \circ f \to \forall x \in X \; h(x) = (g \circ f)(x) = g(f(x))$, называется **композицией** отображений $f : X \to Y$ и $g : Y \to Z$.

Свойства композиции отображений

Композиция отображений *ассоциативна* и в общем случае *не коммутативна*.

34. Композиция инъекций является инъекцией.

35. Композиция сюръекций является сюръекцией.

36. Композиция биекций является биекцией.

Обратное отображение. Отображение $g : Y \to X$ называется **левым обратным** к отображению $f : X \to Y$, если $g \circ f = \mathrm{Id}_X$, т. е. $\forall\, x \in X \quad g(f(x)) = x$. Отображение $g : Y \to X$ называется **правым обратным** к отображению $f : X \to Y$, если $f \circ g = \mathrm{Id}_Y$, т. е. $\forall\, y \in Y \quad f(g(y)) = y$.

37. Для существования **левого обратного** отображения к отображению $f : X \to Y$ необходимо и достаточно, чтобы отображение $f : X \to Y$ было **инъекцией**.

38. Для существования **правого обратного** отображения к отображению $f : X \to Y$ необходимо и достаточно, чтобы отображение $f : X \to Y$ было **сюръекцией**.

Отображение $f^{-1} : Y \to X$ называется **обратным** к отображению $f : X \to Y$, если оно одновременно и левое, и правое обратное.

39. Для существования **обратного** отображения $f^{-1} : Y \to X$ к отображению $f : X \to Y$ необходимо и достаточно, чтобы отображение $f : X \to Y$ было **биекцией**.

Замечание. Принято использовать одинаковое обозначение f^{-1} для двух разных вещей:
для обратного отображения $f^{-1} : Y \to X$ и для прообраза $f^{-1}(y)$ элемента y, прообраз является подмножеством множества X в отображении $f : X \to Y$.

40. Обратное отображение единственно.

41. Если $f^{-1} : Y \to X$ является обратным отображением к $f : X \to Y$, то $f : X \to Y$ — биекция и является обратным к $f^{-1} : Y \to X$.

42. Обратное отображение биективно.

43. Пусть $h : X \to Y$ и $f : Y \to Z$ — биективные отображения, для которых определена их композиция, тогда $(f \circ h)^{-1} = h^{-1} \circ f^{-1}$.

44. Прообразы элементов $y \in Y$ при отображении $f : X \to \to Y$ образуют разбиение множества X.

45. Множества A и B называются *равномощными*, если $\exists$ хотя бы одно биективное отображение $f : A \to B$.

46. *Счетным* называется бесконечное множество, равномощное множеству натуральных чисел.

47. Множество $\mathbf{R}$ действительных чисел *несчетно*.

Мощность множества $\mathbf{R}$ называется *мощностью континуума*, про множество X, равномощное множеству $\mathbf{R}$, говорят, что оно имеет мощность континуума.

ЗАДАЧИ К § 1

1.1. Доказать: $(A \cup B) \setminus A = B \setminus A$.

1.2. Доказать: $A \subset B \leftrightarrow \overline{A} \cup B = U$.

1.3. Доказать, что $A \times B \subset A \times C$, если $B \subset C$.

1.4. Пусть $A \subset B$ и D произвольные множества. Доказать справедливость включения: $A \cap D \subset B \cap D$.

1.5. Доказать, что $A \subset (B \cap D)$, если $A \subset B$ и $A \subset D$.

1.6. Доказать свойство 15 операций над множествами, а именно $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$.

1.7. Является ли операция разности множеств «$\setminus$» ассоциативной, т. е. выполняется ли равенство $A \setminus (B \setminus C) = (A \setminus B) \setminus C$?

1.8. Доказать: $C \times (A \cap B) = (C \times A) \cap (C \times B)$.

1.9. Доказать, что $(B \setminus A) \cup A = B$, если $A \subset B$.

1.10. Доказать: $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$.

1.11. Пусть A, B, C — подмножества некоторого множества D. Доказать, что $(A \cap B) \subset C \leftrightarrow A \subset (\overline{B} \cup C)$.

1.12. Доказать тождество $A \triangle B = (A \cup B) \setminus (A \cap B)$, где $\triangle$ — симметрическая разность, определяемая равенством $A \triangle B = (A \setminus B) \cup (B \setminus A)$.

1.13. Доказать: $A \setminus B = A \triangle (A \cap B)$.

1.14. Доказать, что операция симметрической разности $\triangle$ множеств является коммутативной.

1.15. Доказать дистрибутивность операции $\cap$ относительно операции $\triangle$, т. е. доказать равенства:

1) $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$;

2) $(A \triangle B) \cap C = (A \cap C) \triangle (B \cap C)$.

1.16. Доказать, что операция симметрической разности $\triangle$ множеств является ассоциативной.

1.17. Доказать справедливость включения

$$(A \setminus B) \subset ((A \setminus D) \cup (D \setminus B)).$$

1.18. Определить множества $A \cup B$, $A \cap B$, $A \setminus B$, $B \setminus A$, если $A = \{x \in \mathbf{R} \,|\, (x-4)(x+2) \leq 0\}$, $B = \{x \in \mathbf{R} \,|\, x^2 - 9 \leq \leq 0\}$.

1.19. На множестве ненулевых вещественных чисел $\mathbf{R} \setminus \{0\}$ задано бинарное отношение: $xy > 0$. Является ли оно рефлексивным, симметричным, транзитивным?

1.20. Доказать, что если подмножества E и F множества A удовлетворяют соотношениям $E \cup F = A$, $E \cap F \neq \varnothing$, то каждое из них является дополнением другого до A.

1.21. На множестве ненулевых вещественных чисел $\mathbf{R}\setminus\{0\}$ заданы два бинарных отношения:

$$1)\ x - y \in \mathbf{Z}; \qquad 2)\ x/y \in \mathbf{Z}.$$

Для каждого из них выяснить, является ли оно рефлексивным, симметричным, транзитивным.

1.22. Для следующих отображений выяснить, существует ли к ним левое обратное, правое обратное или обратное отображение, если возможно, привести пример:

а) $f : \mathbf{R} \to \hat{R},\ \hat{R} = \{x \in \mathbf{R} \,|\, x \geq 0\},\ f(x) = |x|$;

б) $f : \mathbf{N} \to \mathbf{N},\ \ f(x) = kx,\ k \in \mathbf{N},\ k \neq 1$;

в) $f : R_+ \to R_+,\ R_+ = \{x \in \mathbf{R} \,|\, x > 0\},\ a \in R_+\ \ f(x) = \dfrac{a}{x}$.

1.23. Для следующих отображений выяснить, какое обратное отображение существует и, если возможно, привести пример:

$$f : X \to Y \quad f(x) = x^2,$$

а) $X = \mathbf{N},\ \ Y = \mathbf{N}$; б) $X = \mathbf{Z},\ \ Y = \mathbf{N} \cup \{0\}$;

в) $X = \mathbf{R},\ Y = \hat{R},\ \hat{R} = \{x \in \mathbf{R} \,|\, x \geq 0\}$;

г) $X = \mathbf{N},\ Y = f(\mathbf{N})$.

1.24. Является ли отображением $f : \mathbf{R} \times \mathbf{R} \to \mathbf{R}$, $\forall\ (a,\, b) \in \mathbf{R} \times \mathbf{R}\ \ f(a, b) = a/b$?

1.25. Пусть $f : X \to Y$ — отображение и $A \subset B \subset X$. Доказать: $f(A) \subset f(B)$.

1.26. Для отображения $f : X \to Y$, $A \subset X$, $A \neq \varnothing$ доказать, что

$$\boxed{y \in f(A)} \leftrightarrow \boxed{f^{-1}(y) \cap A \neq \varnothing.}$$

Здесь $f^{-1}(y)$ — прообраз элемента y.

1.27. Доказать, что образ объединения множеств для любого отображения равен объединению образов, т. е.

$$f(A \cup B) = f(A) \cup f(B).$$

1.28. Пусть $f : X \to Y$, $g : Y \to Z$, $h : Z \to Q$ — биективные отображения, для которых определена их композиция. Доказать: $(f \circ g \circ h)^{-1} = h^{-1} \circ g^{-1} \circ f^{-1}$.

1.29. Пусть $f_1 : X_1 \to X_2$ и $f_2 : X_2 \to X_3$, $\ldots$, $f_n : X_n \to \to X_{n+1}$ — биективные отображения, для которых определена их композиция.

Доказать $(f_1 \circ \ldots \circ f_n)^{-1} = f_n^{-1} \circ f_{n-1}^{-1} \circ \ldots \circ f_1^{-1}$.

1.30. Найти образ элемента $a \in X$ для отображения $\psi : X \to X$, $\psi = (g \circ \varphi)^{-1} \circ (\varphi^{-1} \circ g^{-1})^{-1}$, если $g : X \to \to X$ и $\varphi : X \to X$ — биективные отображения.

1.31. Доказать, что множество $\mathbf{N}^2 = \mathbf{N} \times \mathbf{N}$ является счетным.

1.32. Доказать: если множество X — конечно, то для биективности отображения $f : X \to X$ достаточно, чтобы оно было либо инъекцией, либо сюръекцией.

1.33. Доказать, что если $f : V \to W$ — биективное отображение и $A \subset W$, $B \subset W$, то справедливы равенства:

а) $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$;

б) $f^{-1}(A \setminus B) = f^{-1}(A) \setminus f^{-1}(B)$;

в) $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.

РЕШЕНИЯ И ОТВЕТЫ К ЗАДАЧАМ §1

1.1. Доказать: $(A \cup B) \setminus A = B \setminus A$.

Доказательство. Преобразуем левую часть, перейдя от разности множеств к их пересечению. Свойства операций с множествами позволяют записать:

$$(A \cup B) \setminus A \overset{6}{=} (A \cup B) \cap \overline{A} \overset{5}{=}$$
$$\overset{5}{=} \underbrace{(A \cap \overline{A})}_{\varnothing} \cup (B \cap \overline{A}) \overset{8}{=} B \cap \overline{A} \overset{6}{=} B \setminus A.$$

Число над знаком равенства здесь и далее показывает номер свойства, в силу которого проведено преобразование.

1.2. Доказать: $A \subset B \leftrightarrow \overline{A} \cup B = U$.

Доказательство. $A \subset B \overset{11}{\leftrightarrow} A \setminus B = \varnothing \leftrightarrow \overline{A \setminus B} = U \overset{6}{\leftrightarrow}$
$\overset{6}{\leftrightarrow} \overline{A \cap \overline{B}} = U \overset{13}{\leftrightarrow} \overline{A} \cup \overline{\overline{B}} = U \overset{9}{\leftrightarrow} \overline{A} \cup B = U.$

1.3. Доказать, что $A \times B \subset A \times C$, если $B \subset C$.

Доказательство. Если $B \subset C$, то $\forall\, b \in B \longrightarrow b \in C$. $(*)$
$\forall x \in A \times B \longrightarrow x = (a, b) \quad a \in A$ и $b \in B \overset{*}{\longrightarrow}$
$x = (a, b) \quad a \in A$ и $b \in C \longrightarrow x \in A \times C$.

1.6. Доказать свойство 15, а именно $X \setminus (A \cup B) = (X \setminus A) \cap$
$\cap (X \setminus B)$.

Доказательство. Покажем, что левая и правая части равны.

Преобразуем левую часть:

$$X \setminus (A \cup B) \overset{6}{=} X \cap (\overline{A \cup B}) \overset{12}{=} X \cap (\overline{A} \cap \overline{B}) \overset{3}{=} X \cap \overline{A} \cap \overline{B}.$$

Преобразуем правую часть:

$$X \setminus A \overset{6}{=} X \cap \overline{A} \quad \text{и} \quad X \setminus B \overset{6}{=} X \cap \overline{B} \longrightarrow$$
$$\longrightarrow (X \setminus A) \cap (X \setminus B) \overset{6}{=} (X \cap \overline{A}) \cap (X \cap \overline{B}) \overset{3,\,2}{=}$$
$$\overset{3,\,2}{=} (\underbrace{X \cap X}_{X}) \cap \overline{A} \cap \overline{B} = X \cap \overline{A} \cap \overline{B}.$$

1.7. Является ли операция разности множеств «$\setminus$» ассоциативной, т. е. выполняется ли равенство $A \setminus (B \setminus C) = (A \setminus B) \setminus C$?

Решение. Докажем, что операция разности множеств не является ассоциативной. Для этого достаточно привести пример множеств A, B, C, для которых равенство $A \setminus (B \setminus C) = (A \setminus B) \setminus C$ не выполняется. Пусть $A \neq \varnothing$ и пусть $A \subset B \subset C$. В этом случае по свойству 11 операций со множествами выполняются равенства $B \setminus C = \varnothing$ и $A \setminus B = \varnothing$, которые позволяют найти левую и правую части исследуемого равенства в следующем виде:

$$\text{левая часть} = A \setminus (B \setminus C) = A \setminus \varnothing = A \cap U = A,$$

$$\text{правая часть} = (A \setminus B) \setminus C = \varnothing \setminus C = \varnothing \cap \overline{C} = \varnothing.$$

Несовпадение левой и правой частей доказывает отсутствие ассоциативности операции разности множеств.

1.8. Доказать: $C \times (A \cap B) = (C \times A) \cap (C \times B)$.

Доказательство. Найдем левую и правую части.
Левая часть:

$C \times (A \cap B) = \{(x, y) |\ x \in C \text{ и } y \in (A \cap B)\}$.

Правая часть:

$$C \times A = \{(x, y) \mid x \in C \text{ и } y \in A\}.$$

$$C \times B = \{(x, y) \mid x \in C \text{ и } y \in B\}.$$

$$(C \times A) \cap (C \times B) = \{(x,y) \,|\, (x,y) \in (C \times A) \text{ и } (x,y) \in (C \times B)\} =$$

$$= \{(x,y) |\ (x \in C \text{ и } y \in A) \text{ и } (x \in C \text{ и } y \in B)\} =$$

$$= \{(x,y) |\ x \in C \text{ и } \underbrace{(y \in A \text{ и } y \in B)}_{y \in A \cap B}\} =$$

$$= \{(x,y) |\ x \in C \text{ и } y \in (A \cap B)\}.$$

Левая и правая части равны $\to$ операция $(\times)$ дистрибутивна относительно операции пересечения множеств.

1.9. Доказать, что $(B \setminus A) \cup A = B$, если $A \subset B$.

Доказательство. Это очевидно из диаграмм Эйлера–Венна, но можно доказать и пользуясь свойствами операций с множествами.

$$(B \setminus A) \cup A \overset{6}{=} (B \cap \overline{A}) \cup A \overset{4}{=} (B \cup A) \cap (\underbrace{\overline{A} \cup A}_{U}) \overset{7}{=} B \cup A = B.$$

1.10. Доказать: $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$.

Доказательство.

$A \setminus (B \setminus C) \overset{6}{=} A \cap \overline{(B \setminus C)} \overset{6}{=} A \cap \overline{(B \cap \overline{C})} \overset{13}{=} A \cap \left(\overline{B} \cup \overline{\overline{C}}\right) \overset{5,9}{=}$
$\overset{5,9}{=} \left(A \cap \overline{B}\right) \cup (A \cap C) \overset{6}{=} (A \setminus B) \cup (A \cap C)$.

1.11. Пусть A, B, C — подмножества некоторого множества D. Доказать, что $A \cap B \subset C \leftrightarrow A \subset \overline{B} \cup C$.

Доказательство. $A \cap B \subset C \overset{11}{\leftrightarrow} (A \cap B) \setminus C = \varnothing \overset{6,3}{\leftrightarrow}$

$$\overset{6,3}{\leftrightarrow} A \cap B \cap \overline{C} = \varnothing. \qquad (*)$$

$A \subset \overline{B} \cup C \overset{11}{\leftrightarrow} A \setminus (\overline{B} \cup C) = \varnothing \overset{6,12}{\leftrightarrow} A \cap (\overline{\overline{B}} \cap \overline{C}) \overset{3,9}{=}$

$$\overset{3,9}{=} A \cap B \cap \overline{C} = \varnothing. \qquad (**)$$

Из $(*)$, $(**)$ следует: $A \cap B \subset C \leftrightarrow A \subset \overline{B} \cup C$.

1.12. Доказать тождество $A \triangle B = (A \cup B) \setminus (A \cap B)$, где $\triangle$ — симметрическая разность, определяемая равенством $A \triangle B = (A \setminus B) \cup (B \setminus A)$.

Доказательство. $(A \setminus B) \cup (B \setminus A) \overset{6}{=} \big(A \cap \overline{B}\big) \cup \big(B \cap \overline{A}\big) \overset{4}{=}$

$$\overset{4}{=} \big(\big(A \cap \overline{B}\big) \cup B\big) \cap \big(\big(A \cap \overline{B}\big) \cup \overline{A}\big) \overset{4}{=}$$

$$\overset{4}{=} \big((B \cup A) \cap \underbrace{\big(B \cup \overline{B}\big)}_{U} \big) \cap \big(\underbrace{\big(\overline{A} \cup A\big)}_{U} \cap \big(\overline{A} \cup \overline{B}\big) \big) \overset{7}{=}$$

$$\overset{7}{=} (B \cup A) \cap (\overline{A} \cup \overline{B}) \overset{13}{=} (B \cup A) \cap (\overline{A \cap B}) \overset{6}{=} (B \cup A) \setminus (A \cap B).$$

1.15. Доказать дистрибутивность операции $\cap$ относительно операции $\triangle$ со множествами:

1) $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$;

2) $(A \triangle B) \cap C = (A \cap C) \triangle (B \cap C)$.

Доказательство. Докажем равенство 1. Найдем левую и правую части.

Левая часть:

$$A \cap ((B \setminus C) \cup (C \setminus B)) = A \cap \big((B \cap \overline{C}) \cup (C \cap \overline{B})\big) =$$
$$= \big(A \cap B \cap \overline{C}\big) \cup \big(A \cap C \cap \overline{B}\big).$$

Правая часть:

$$(A \cap B) \triangle (A \cap C) = \underbrace{((A \cap B) \setminus (A \cap C))}_{1.1} \cup \underbrace{((A \cap C) \setminus (A \cap B))}_{1.2}.$$

$1.1 = A \cap B \cap (\overline{A} \cup \overline{C}) = B \cap A \cap (\overline{A} \cup \overline{C}) = B \cap ((A \cap \overline{A}) \cup$
$\cup (A \cap \overline{C})) = B \cap A \cap \overline{C}$.

$1.2 = A \cap C \cap (\overline{A} \cup \overline{B}) = C \cap A \cap (\overline{A} \cup \overline{B}) = C \cap ((A \cap \overline{A}) \cup$
$\cup (A \cap \overline{B})) = C \cap A \cap \overline{B}$.

Правая часть равна $(B \cap A \cap \overline{C}) \cup (C \cap A \cap \overline{B}) \longrightarrow$ левая часть равна правой части.

Равенство 2 доказать самостоятельно.

1.16. Доказательство ассоциативности операции симметрической разности предоставляется читателям.

1.17. Доказать справедливость включения

$$(A \setminus B) \subset ((A \setminus D) \cup (D \setminus B)).$$

Доказательство. Надо доказать

$$\forall\, x \in (A \setminus B) \longrightarrow x \in (A \setminus D) \cup (D \setminus B).$$

Относительно множества D возможны две ситуации:

$$x \in D, \qquad x \notin D.$$

Докажем справедливость включения для $x \in D$.

$\forall\, x \in (A \setminus B) \longrightarrow x \in A$ и $x \notin B \longrightarrow$ (т. к. $x \in D$) $\longrightarrow$
$\longrightarrow x \in (D \setminus B) \longrightarrow x \in (A \setminus D) \cup (D \setminus B)$.

Докажем справедливость включения для $x \notin D$.

$\forall\, x \in (A \setminus B) \longrightarrow x \in A$ и $x \notin B \longrightarrow$ (т.к. $x \notin D$) $\longrightarrow$
$\longrightarrow x \in (A \setminus D) \longrightarrow x \in (A \setminus D) \cup (D \setminus B)$.

1.18. Определить множества $A \cup B$, $A \cap B$, $A \setminus B$, $B \setminus A$, если $A = \{x \in \mathbf{R} \,|\, (x-4)(x+2) \leq 0\}$, $B = \{x \in \mathbf{R} \,|\, x^2 - 9 \leq \leq 0\}$.

Ответ: $A \cup B = \{x \in [-3, 4]\}$, $A \cap B = \{x \in [-2, 3]\}$, $A \setminus B = \{x \in (3, 4]\}$, $B \setminus A = \{x \in [-3, -2)\}$.

1.19. На множестве ненулевых вещественных чисел $\mathbf{R}\setminus\{0\}$ задано бинарное отношение $xy > 0$. Является ли оно рефлексивным, симметричным, транзитивным?

Решение. Бинарное отношение $xy > 0$ является рефлексивным, т. к. для любого $x \in \mathbf{R} \setminus \{0\}$ выполняется $xx > 0$.

Оно симметрично, т. к. для $\forall\, x,\, y \in \mathbf{R} \setminus \{0\}$ выполняется: $xy > 0 \longrightarrow yx > 0$.

Докажем транзитивность:

из неравенства $xy > 0$ следует:

либо $x > 0$ и $y > 0$, либо $x < 0$ и $y < 0$;

из неравенства $yz > 0$ следует:

либо $y > 0$ и $z > 0$, либо $y < 0$ и $z < 0$.
Таким образом,

$$x > 0 \longrightarrow y > 0 \longrightarrow z > 0 \longrightarrow xz > 0;$$
$$x < 0 \longrightarrow y < 0 \longrightarrow z < 0 \longrightarrow xz > 0.$$

Следовательно, отношение $xy > 0$ транзитивно.

1.21. На множестве ненулевых вещественных чисел $\mathbf{R}\backslash\{0\}$ заданы два бинарных отношения:

$$1)\ x - y \in \mathbf{Z}; \qquad 2)\ x/y \in \mathbf{Z}.$$

Для каждого из них выяснить, является ли оно рефлексивным, симметричным, транзитивным?

Ответ: Отношение 1) рефлексивно, симметрично и транзитивно; 2) рефлексивно, транзитивно, но не симметрично.

1.22. Для следующих отображений выяснить, существует ли к ним левое обратное, правое обратное или обратное отображение, если возможно, привести пример:

а) $f : \mathbf{R} \to \hat{R},\ \hat{R} = \{x \in \mathbf{R} |\, x \geq 0\},\ f(x) = |x|$;

б) $f : \mathbf{N} \to \mathbf{N},\ \ f(x) = kx,\ k \in \mathbf{N},\ k \neq 1$;

в) $f : R_+ \to R_+,\ R_+ = \{x \in \mathbf{R} |\, x > 0\},\ a \in R_+\ \ f(x) = \dfrac{a}{x}$.

Решение. а) Это отображение не инъективно, т. к. $\forall\, x \in \mathbf{R}$ $f(x) = f(-x)$. Но оно сюръективно, т. к. для $\forall\, y \in \hat{R}$ $\exists\, x \in \mathbf{R}$ $y = |x|$. По свойству 38 существует правое обратное отображение, которое можно задать, например, следующим образом: $g : \hat{R} \to \mathbf{R}$

$$\forall\, y \in \hat{R}\ \ g(y) = y.$$

Покажем, что оно — правое обратное отображение.
$\forall\, y \in \hat{R}\ \ f \circ g(y) = f\,(g(y)) = f(y) = |y| = y$, т. е. $f \circ g = \mathrm{Id}_{\hat{R}}$.
Правое обратное отображение *не единственно*. Например, отображение $h : \hat{R} \to \mathbf{R}$

$$\forall\, y \in \hat{R}\ \ h(y) = -y$$

также является правым обратным, т. к.

$$\forall\, y \in \hat{R} \quad f(h(y)) = f(-y) = |-y| = y \to f \circ h = \mathrm{Id}_{\hat{R}}.$$

б) Это отображение инъективное, т. к. для любых $x_1,\ x_2 \in$ $\in \mathbf{N}$, $x_1 \neq x_2$ при $k \neq 1$ следует: $f(x_1) = kx_1 \neq kx_2 = f(x_2)$. Оно не сюръективное, т. к. в элементы не кратные k ничего не переходит. По свойству 37, существует левое обратное отображение, например: $g : \mathbf{N} \to \mathbf{N}$

$$g(n) = \begin{cases} \dfrac{n}{k}, & \text{для } n \in \mathrm{Im} f, \\ n_*, & \text{для } n \notin \mathrm{Im} f, \end{cases}$$

где n_* — любое натуральное число. Проверим, что это отображение является левым обратным.

$\forall\, n \in \mathbf{N} \quad g(f(n)) = g(kn) = \frac{kn}{k} = n \quad \longrightarrow g \circ f = \mathrm{Id}_{\mathbf{N}}.$

в) Отображение $g : R_+ \to R_+ \ \ g(x) = \dfrac{a}{x}$ является обратным к $f : R_+ \to R_+ \ \ f(x) = \dfrac{a}{x}$. Действительно:

$$\forall x \in R_+ \quad g(f(x)) = g\left(\frac{a}{x}\right) = \frac{ax}{a} = x \longrightarrow g \circ f = \mathrm{Id}_{R^+}.$$

$$\forall x \in R_+ \quad f(g(x)) = f\left(\frac{a}{x}\right) = \frac{ax}{a} = x \longrightarrow f \circ g = \mathrm{Id}_{R^+}.$$

По свойству 41 из существования обратного отображения следует, что прямое отображение является биекцией, а из свойства 40 следует, что обратное отображение единственно.

1.23. Для следующих отображений выяснить, какое обратное отображение существует и, если возможно, привести пример:

$$f : X \to Y \quad f(x) = x^2,$$

а) $X = \mathbf{N},\ Y = \mathbf{N}$; б) $X = \mathbf{Z},\ Y = \mathbf{N} \cup \{0\}$;

в) $X = \mathbf{R},\ Y = \hat{R},\ \hat{R} = \{x \in \mathbf{R} |\ x \geq 0\}$; г) $X = \mathbf{N},\ Y = f(\mathbf{N})$.

Ответ:

а) инъекция $\longrightarrow$ существует левое обратное отображение; пример левого обратного отображения $g : \mathbf{N} \to \mathbf{N}$

$$g(n) = \begin{cases} \sqrt{n}, & \text{если } n \in \mathrm{Im} f, \\ n_*, & \text{если } n \notin \mathrm{Im} f, \end{cases}$$

где n_* — любое натуральное число;

б) ни сюръекция, ни инъекция $\longrightarrow$ никакого обратного отображения не существует;

в) сюръекция $\longrightarrow$ существует правое обратное отображение; пример правого обратного отображения $g : \hat{R} \to \mathbf{R}$ $g = \sqrt{x}$, $\forall\, x \in \hat{R}$;

г) биекция $\longrightarrow$ существует обратное отображение, оно равно $g : f(\mathbf{N}) \to \mathbf{N}$ $\forall n \in f(\mathbf{N})$ $g(n) = \sqrt{n}$.

1.24. Является ли отображением $f : \mathbf{R} \times \mathbf{R} \to \mathbf{R}$, $\forall\ (a,\, b) \in \mathbf{R} \times \mathbf{R}$ $f(a, b) = a/b$?

Ответ: нет, т. к. для $(a, 0) \in \mathbf{R} \times \mathbf{R}$ $f(a, 0) = \dfrac{a}{0} \notin \mathbf{R}$.

1.25. Пусть $f : X \to Y$ — отображение и $A \subset B \subset X$. Доказать: $f(A) \subset f(B)$.

Доказательство.

$\forall y \in f(A) \leftrightarrow \exists x \in A,\ f(x) = y \overset{\text{т. к. } A \subset B}{\longrightarrow} \exists x \in B,$ $f(x) = y \leftrightarrow y \in f(B)$. Таким образом,

$$\forall y \in f(A) \to y \in f(B) \ \to \ f(A) \subset f(B).$$

1.26. Для отображения $f : X \to Y,\ A \subset X,\ A \neq \varnothing$ доказать, что

$$\boxed{y \in f(A)} \leftrightarrow \boxed{f^{-1}(y) \cap A \neq \varnothing.}$$

Здесь $f^{-1}(y)$ — прообраз элемента y.

Доказательство. $y \in f(A) \leftrightarrow \exists\, x \in A,\ y = f(x) \longleftrightarrow$ $\longleftrightarrow \exists\, x \in f^{-1}(y) \cap A \longleftrightarrow f^{-1}(y) \cap A \neq \varnothing$.

1.27. Доказать, что образ объединения множеств для любого отображения равен объединению образов, т. е.

$$f(A \cup B) = f(A) \cup f(B).$$

Доказательство. Воспользуемся результатами предыдущей задачи:

$$\forall y \; y \in f(A \cup B) \leftrightarrow f^{-1}(y) \cap (A \cup B) \neq \varnothing.$$

Пользуясь дистрибутивностью $\cap$ относительно $\cup$, запишем

$\big(\big(f^{-1}(y) \cap A\big) \cup \big(f^{-1}(y) \cap B\big)\big) \neq \varnothing \leftrightarrow f^{-1}(y) \cap A \neq \varnothing$ или

$f^{-1}(y) \cap B \neq \varnothing \leftrightarrow y \in f(A)$ или $y \in f(B) \leftrightarrow y \in f(A) \cup f(B)$.

Замечание. *Образ пересечения множеств в общем случае не равен пересечению образов*, а является его подмножеством т. е. $f(A \cap B) \subset f(A) \cap f(B)$.

1.28. Пусть $f : X \to Y$, $g : Y \to Z$, $h : Z \to Q$ — биективные отображения, для которых определена их композиция. Доказать: $(f \circ g \circ h)^{-1} = h^{-1} \circ g^{-1} \circ f^{-1}$.

Доказательство. $(f \circ g \circ h)^{-1} = ((f \circ g) \circ h)^{-1} = h^{-1} \circ (f \circ g)^{-1} = h^{-1} \circ g^{-1} \circ f^{-1}$.

1.30. Найти образ элемента $a \in X$ для отображения $\psi : X \to X$, $\psi = (g \circ \varphi)^{-1} \circ (\varphi^{-1} \circ g^{-1})^{-1}$, если $g : X \to X$ и $\varphi : X \to X$ — обратимые отображения.

Решение. $\psi = \varphi^{-1} \circ g^{-1} \circ (g^{-1})^{-1} \circ (\varphi^{-1})^{-1} =$

$$= \varphi^{-1} \circ \underbrace{g^{-1} \circ g}_{\mathrm{Id}} \circ \varphi = \mathrm{Id}_X \longrightarrow \psi(a) = \mathrm{Id}_X(a) = a.$$

1.31. Доказать, что множество $\mathbf{N}^2 = \mathbf{N} \times \mathbf{N}$ является счетным.

Доказательство. Множество $\mathbf{N}^2 = \{(a, b) |\; a \in \mathbf{N}, b \in \mathbf{N}\}$ является счетным, если оно равномощно множеству натуральных чисел $\mathbf{N}$ (п. 46).

Для доказательства равномощности (п. 45) найдем взаимно однозначное соответствие между множествами $\mathbf{N}$ и $\mathbf{N}^2$. Для этого построим бесконечную таблицу вида

$$\begin{array}{cccc} (1,1) & (1,2) & (1,3) & \dots \\ (2,1) & (2,2) & (2,3) & \dots \\ (3,1) & (3,2) & (3,3) & \dots \\ \dots & \dots & \dots & \dots \end{array}$$

Развернем эту таблицу в последовательность, например, проходя по очереди диагонали, начиная с левого верхнего угла, т. е. $(1,1)$, $(2,1)$, $(1,2)$, $(3,1)$, $(2,2)$, $(1,3)$, $\dots$

Пронумеруем полученную последовательность. Эта нумерация и есть искомое взаимно однозначное соответствие между множествами $\mathbf{N}$ и $\mathbf{N}^2$. Следовательно, множество $\mathbf{N}^2$ — счетно. Аналогично можно показать, что множество $\mathbf{N}^k$ счетно.

1.32. Доказать: если множество X — конечно, то для биективности отображения $f : X \to X$ достаточно, чтобы оно было либо инъекцией, либо сюръекцией.

Доказательство. Воспользуемся следующими фактами:
1) в данной задаче образы и прообразы элементов принадлежат одному и тому же множесту X;
2) прообразы элементов не пересекаются (это следует из свойств 17 и 44);
3) для конечных непересекающихся множеств $A_1, ..., A_n$ верно равенство $|A_1 \cup ... \cup A_n| = |A_1| + ... + |A_n|$;
4) при инъекции прообраз любого элемента y_k содержит не более одного элемента (31), т. е. $|f^{-1}(y_k)| \leq 1$, а при сюръекции — не менее одного (32), т. е. $|f^{-1}(y_k)| \geq 1$.
Пусть мощность множества X равна $|X| = n$.
Как известно (44), прообразы элементов $y \in Y$ при отображении $f : X \to Y$ образуют разбиение множества X. Это

позволяет записать

$$X = \underbrace{f^{-1}(x_1) \cup \cdots \cup f^{-1}(x_n)}_{\text{всего } n \text{ слагаемых}}.$$

Так как прообразы не пересекаются, то из 3) следует:

$$|X| = |f^{-1}(x_1)| + ... + |f^{-1}(x_n)|. \qquad (*)$$

Рассмотрим случай инъекции. В равенстве $(*)$ n слагаемых, и величина каждого слагаемого меньше или равна единице. Чтобы равенство выполнялось, необходимо, чтобы каждое слагаемое равнялось единице, при этом условии отображение будет биекцией.

Рассмотрим случай сюръекции. В равенстве $(*)$ n слагаемых, и для сюръекции величина каждого больше или равна единице. Чтобы равенство выполнялось, необходимо, чтобы каждое слагаемое равнялось единице, т. е. и в этом случае отображение биективно.

1.33. Доказать, что если $f : V \to W$ — биективное отображение и $A \subset W$, $B \subset W$, то справедливы равенства:

а) $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$;

б) $f^{-1}(A \setminus B) = f^{-1}(A) \setminus f^{-1}(B)$;

в) $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.

Доказательство. а) Для доказательства равенства двух множеств надо доказать два включения:

1) $f^{-1}(A \cap B) \subset (f^{-1}(A) \cap f^{-1}(B))$,

2) $(f^{-1}(A) \cap f^{-1}(B)) \subset f^{-1}(A \cap B)$.

Докажем включения 1) и 2).

Для $\forall\, x \in f^{-1}(A \cap B) \Leftrightarrow \forall\, x\, f(x) \in (A \cap B) \Leftrightarrow \forall\, x \quad f(x) \in$ $\in A$ и $f(x) \in B \Leftrightarrow \forall\, x \quad x \in f^{-1}(A)$ и $x \in f^{-1}(B) \Leftrightarrow \forall\, x \quad x \in$ $\in (f^{-1}(A) \cap f^{-1}(B))$.

Включения 1) и 2) доказаны.

б) Как и в пункте а), докажем два включения:

1) $f^{-1}(A \setminus B) \subset (f^{-1}(A) \setminus f^{-1}(B))$,

2) $(f^{-1}(A) \setminus f^{-1}(B)) \subset f^{-1}(A \setminus B)$.

Для $\forall\, x \in f^{-1}(A \setminus B) \Leftrightarrow$

$f(x) \in (A \setminus B) \Leftrightarrow f(x) \in A$ и $f(x) \notin B \Leftrightarrow x \in f^{-1}(A)$ и

$x \notin f^{-1}(B) \Leftrightarrow \forall\, x \quad x \in (f^{-1}(A) \setminus f^{-1}(B))$.

Включения 1) и 2) доказаны, следовательно, множества $f^{-1}(A \setminus B)$ и $f^{-1}(A) \setminus f^{-1}(B)$ равны.

Равенство в) доказывается по аналогичной схеме.

§ 2. АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ

Группы

Простейшей алгебраической структурой является **полугруппа** — множество с заданной на нем бинарной ассоциативной операцией. Полугруппа, операция в которой коммутативна, называется коммутативной, или *абелевой*. Элемент e полугруппы W называется **нейтральным, или единицей**, если для любого $a \in W$ выполняется: $ae = ea = a$.

Можно доказать, что в полугруппе нейтральный элемент, если он есть, — единственен. Полугруппа с нейтральным элементом называется **моноидом**. Элемент a^{-1} моноида называется **обратным** к a, а сам элемент a называется обратимым, если $aa^{-1} = a^{-1}a = e$. Можно доказать, что для обратимого элемента моноида **обратный к нему элемент единственен.** Моноид, каждый элемент которого обратим, называется **группой**.

Повторим условия, которым должна удовлетворять операция на множестве W, чтобы эта алгебраическая структура являлась группой:

1) операция не должна выводить из множества W, т. е.
$\forall\ a,\ b \in W \quad ab \in W$;

2) операция должна быть ассоциативной, т. е.
$\forall\ a,\ b,\ c \in W \quad (ab)c = a(bc)$;

3) должен существовать нейтральный элемент, т. е.
такой элемент e, $\quad e \in W$, что для $\forall\ a \in W \quad ae = ea = a$;

4) должен существовать обратный элемент для каждого элемента из множества W, т. е. $\forall\ a \in W \quad \exists \quad a^{-1} \in W$ такой, что $aa^{-1} = a^{-1}a = e$.

Если, кроме того, операция коммутативна, группа называется *абелевой*.

Замечание. Далее, в задаче 2.21, доказано, что аксиомы 1)–4) являются избыточными, а именно, допустимо следующее определение группы с более слабыми требованиями: множество с бинарной и ассоциативной операцией является группой, если в нем существует левый нейтральный элемент и для каждого элемента существует левый обратный элемент.

Можно доказать, что в группе:

1. Нейтральный элемент единственен.

2. Обратный элемент к каждому элементу единственен.

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

Таблица Кэли. Если множество W состоит из конечного числа элементов, бинарная операция может быть задана перечислением результата ее выполнения. Это принято записывать в виде *таблицы Кэли*. Например, нетрудно убедиться в том, что множество $W = \{a, b\}$ с операцией, заданной таблицей Кэли

	a	b
a	a	b
b	b	b

,

является коммутативным моноидом, нейтральный элемент которого равен a (см. задачу 2.1).

4. Степень элемента. Для натурального n и элемента a полугруппы степень a^n определяется как произведение n экземпляров a: $a^n = aa\ldots a$. Если в полугруппе есть нейтральный элемент, полагают $a^0 \stackrel{\text{d}}{=} e$; если a имеет обратный

элемент a^{-1}, принимается $a^{-n} = (a^{-1})^n$, где a^{-1} — обратный для a. Перебор всевозможных случаев показывает, что

4′. $a^n a^m = a^{n+m}$.

Число элементов группы G (если оно конечно) называется **порядком** группы G и обозначается $|G|$. Группа G при этом называется *конечной*. Если множество G бесконечно, группа называется *бесконечной*.

Подмножество W' множества W называется **подгруппой** группы W, если его элементы образуют группу относительно групповой операции в W. У каждой группы есть две *несобственных* подгруппы — это она сама и подгруппа, состоящая из одного нейтрального элемента. Остальные подгруппы, если они существуют, называются *собственными*.

5. Необходимыми и достаточными условиями того, что подмножество W' есть подгруппа, являются:

1) операция не выводит из этого подмножества W', т. е. для любых a, $b \in W' \longrightarrow ab \in W'$;

2) обратный элемент принадлежит подмножеству W', т. е. для любого $a \in W' \longrightarrow a^{-1} \in W'$.

Морфизмы групп

6. Отображение $f : B \to W$ из группы B в группу W называется **гомоморфным**, или просто *морфизмом*, если для любых b_1, $b_2 \in B$ $f(b_1 b_2) = f(b_1) f(b_2)$, *мономорфизмом*, или вложением, если это отображение к тому же инъективно, и **изоморфизмом**, если оно биективно. Гомоморфизм группы в себя называется **эндоморфизмом**, изоморфизм группы в себя — **автоморфизмом**.

В левой части равенства $f(b_1 b_2) = f(b_1) f(b_2)$ множители b_1 и b_2 связывает операция группы B, а множители $f(b_1)$ и $f(b_2)$ в правой части связаны операцией группы W.

Пусть $f : B \to W$ — гомоморфизм из группы B в группу W. **Ядром** $\mathrm{Ker} f$ гомоморфизма называется прообраз ней-

трального элемента группы W; **образом** $\mathrm{Im}\, f$ гомоморфизма называется образ отображения $f : B \to W$, а именно

7. $\mathrm{Ker} f = \{x \in B \mid\ f(x) = e_W\}; \mathrm{Im}\, f = \{y \in W \mid\ \exists x \in \in B,\ f(x) = y\}$.

Свойства гомоморфизма групп

8. Гомоморфизм $f : B \to W$ переводит нейтральный элемент e_B группы B в нейтральный элемент e_W группы W.

9. Гомоморфизм $f : B \to W$ переводит обратный элемент в обратный: $\forall\, x \in B\ f(x^{-1}) = f^{-1}(x)$.

10. Ядро $\mathrm{Ker} f$ гомоморфизма $f : B \to W$ является подгруппой группы B.

11. Образ $\mathrm{Im}\, f$ гомоморфизма $f : B \to W$ является подгруппой группы W.

Мультипликативная и аддитивная формы

Наряду с мультипликативной формой записи операции, когда ее результат называется *произведением* и обозначается ab или $a * b$, используется также аддитивная форма записи, когда результат операции называется *суммой* и обозначается $a + b$. В этом случае нейтральный элемент называют *нулем* и обозначают 0; вместо обратного элемента a^{-1} говорят о *противоположном* элементе и обозначают его $-a$; аналогом *степени* элемента является его *кратное*, обозначаемое na; обратная операция называется вычитанием.

Кольца и поля

Пусть на множестве W заданы две бинарные операции, одну из которых условно называют сложением, другую — умножением. **Умножение дистрибутивно относительно сложения**, если для любых $a, b, c \in W$ выполняются следующие равенства:

12. $a(b+c)=ab+ac, \qquad (a+b)c=ac+bc.$
Это обычные правила раскрытия скобок.

Кольцом (ассоциативным) называется множество W, для элементов которого определены операции сложения и умножения, причем, по сложению это абелева группа, по умножению — полугруппа, и умножение дистрибутивно относительно сложения.

Различные требования к умножению выделяют различные классы колец, например, кольцо с единицей и коммутативное кольцо.

Свойства операций в кольце

Обозначим K — кольцо. Пользуясь определениями операций сложения, умножения и дистрибутивностью умножения относительно сложения в кольце, а также определениями 0 (нейтрального элемента по сложению) и 1 (нейтрального элемента по умножению), можно доказать следующие свойства операций в кольце:

1) $\forall\ a \in K \quad a0=0a=0;$

2) $\forall\ a,b \in K \quad (-a)b=a(-b)=-(ab);$

3) $\forall\ a,b \in K \quad (-a)(-b)=ab;$

4) если K — кольцо с 1, то $\forall\ a \in K \quad (-1)a=a(-1)=-a;$

5) $\forall\ a,b,c \in K \quad a(b-c)=ab-ac; \quad (a-b)c=ac-bc.$

13. Если для ненулевых элементов $a \neq 0$, $b \neq 0$ кольца W выполняется равенство $ab=0$, то a называется левым, а b — правым делителем нуля в кольце W. (В коммутативном кольце говорят просто о делителе нуля.)

Сам 0 в кольце, состоящем более чем из одного элемента, является *тривиальным делителем нуля*. Любой другой делитель нуля называется *нетривиальным*.

14. Можно доказать, что обратимые элементы кольца с единицей не могут быть делителями нуля.

Кольцо, не содержащее нетривиальных делителей нуля, называется *кольцом без делителей нуля*. Коммутативное кольцо с 1, не равной 0, и без делителей нуля называют **целостным** кольцом.

15. Кольцо, все не нулевые элементы которого обратимы, называется **телом**, а коммутативное тело — **полем**.

По аналогии с понятием подгруппы вводится понятие **подкольца** — такого подмножества кольца, элементы которого сами образуют кольцо относительно тех же операций, что и объемлющее кольцо. Для того чтобы подмножество W' было подкольцом кольца W, необходимо и достаточно, чтобы вместе с любыми двумя элементами оно содержало их сумму, разность и произведение. Понятия подтела и подполя определяются аналогично.

16. Гомоморфизмом кольца B в кольцо W называется отображение $f : B \to W$, переводящее сумму в сумму, а произведение — в произведение:

$$f(b_1 + b_2) = f(b_1) + f(b_2) \text{ и } f(b_1 b_2) = f(b_1) f(b_2).$$

Гомоморфизм колец является гомоморфизмом их аддитивных групп. Если гомоморфизм колец биективен, то он является **изоморфизмом колец**. Изоморфизм кольца в себя называется **автоморфизмом**.

ЗАДАЧИ К § 2

2.1. На множестве $G = \{a, b\}$ операция задана таблицей Кэли. Является ли эта алгебраическая структура группой?

1)

	b	a
b	b	a
a	a	b

;

2)

	a	b
a	b	a
b	a	a

;

3)

	a	b
a	a	a
b	b	b

.

2.2. Какой алгебраической структурой является множество всех подмножеств некоторого множества X ($X \neq \varnothing$) с операцией

а) объединения подмножеств;

б) пересечения подмножеств?

2.3. На множестве $G = \{a_0, a_1, a_2, a_3\}$ операция задана следующей таблицей Кэли:

	a_0	a_1	a_2	a_3
a_0	a_0	a_1	a_2	a_3
a_1	a_1	a_0	a_3	a_2
a_2	a_2	a_3	a_0	a_1
a_3	a_3	a_2	a_1	a_0

.

Доказать, что эта алгебраическая структура является абелевой группой.

2.4. Ассоциативна ли операция $*$ на $\mathbf{R}$, заданная правилом $\forall\, x,\, y \in \mathbf{R} \quad x * y = x^2 + y$?

2.5. Доказать, что для произвольного отличного от нуля вещественного числа a множество $G = \{a^n |\ n \in \mathbf{Z}\}$ является абелевой группой по умножению.

2.6. Выяснить, образуют ли группу относительно операции **сложения**

1) множество вещественных чисел $\mathbf{R}$;
2) множество неотрицательных вещественных чисел;
3) множество рациональных чисел $\mathbf{Q}$;
4) множество целых чисел $\mathbf{Z}$;
5) множество четных чисел;
6) множество нечетных чисел;
7) множество, состоящее из одного числа 0.

2.7. Образуют ли группу относительно операции **умножения**
1) множество вещественных чисел $\mathbf{R}$;
2) множество положительных вещественных чисел;
3) множество рациональных чисел $\mathbf{Q}$;
4) множество натуральных чисел $\mathbf{N}$?

2.8. В таблице Кэли некоторой конечной группы выделен прямоугольник и известны элементы, стоящие в трех его вершинах (1 обозначен нейтральный элемент). Найти элемент, находящийся в четвертой вершине.

1)

	...	x_k	...	x_p
...	...	...	...	...
x_m	...	a	...	?
...	...	...	...	...
x_t	...	1	...	b

;

2)

	...	x_k	...	x_p
...	...	...	...	...
x_m	...	1	...	b
...	...	...	...	...
x_t	...	a	...	?

.

2.9. Пусть для любого элемента a группы G выполняется равенство $a^2 = e$, где e — нейтральный элемент. Доказать, что группа является абелевой.

2.10. Какой алгебраической структурой является множество натуральных чисел с заданной операцией $\forall\ a, b \in \mathbf{N}$ $a * b = a^b$?

2.11. Какой алгебраической структурой является по сложению множество $M = \{m\,n |\ n \in \mathbf{Z}\}$, где m — некоторое целое число?

2.12. По какой алгебраической операции $(+, -, \cdot, :)$ множество $\{-1, 1\}$ является группой?

2.13. Какие из следующих алгебраических структур являются группами?

а) $(\{1\}, \cdot)$; б) $(\{1\}, +)$.

2.14. Образует ли множество векторов трехмерного пространства над полем действительных чисел группу относительно операции векторного умножения?

2.15. Пусть G — мультипликативная группа, $a, b \in G$. Доказать: если a коммутирует с b, то a^{-1} коммутирует с b^{-1}.

2.16. Пусть для элементов x, y моноида элементы xy и yx обратимы. Доказать, что элементы x и y тоже обратимы.

2.17. Пусть $(G,\ \circ)$ — группа, $a \in G$. На множестве G определена другая операция $*$: $\forall\, x,\, y \in G\ \ x * y = x \circ a \circ y$.
Доказать, что $(G,\ *)$ — группа.

2.18. Пусть $(G, \circ)$ — группа. На множестве G определена другая операцию $*$: $\forall\, a, b \in\ G\ \ a * b = b \circ a$.
Доказать, что $(G, *)$ — группа.

2.19. Пусть G — множество всех вещественных чисел, отличных от (-1). Доказать, что G — группа относительно операции

$$\forall\ a, b \in G\ \ a * b = ab + a + b.$$

2.20. Пусть H — подгруппа группы G. Доказать, что если множество $(G\backslash H) \cup \{e\}$ — подгруппа группы G, то либо $H = \{e\}$, либо $H = G$, здесь e — нейтральный элемент группы G.

2.21. Доказать, что из существования в полугруппе G левого нейтрального элемента $e_{\text{л}}$ такого, что

$$\exists\, e_{\text{л}} \in G \quad \forall\, a \in G \quad e_{\text{л}} a = a, \tag{1}$$

и существования для каждого элемента полугруппы левого обратного элемента $a_{\text{л}}^{-1}$ такого, что

$$\forall\, a \in G \quad \exists\, a_{\text{л}}^{-1} \in G \quad a_{\text{л}}^{-1} a = e_{\text{л}}, \tag{2}$$

следует, что полугруппа G является **группой**, т. е. левый нейтральный элемент одновременно является и правым нейтральным элементом, а левый обратный элемент для каждого элемента является одновременно и правым обратным.

2.22. На множестве $G = \{(a, b) \mid a, b \in \mathbf{R}, a \neq 0\}$ задана операция умножения $(a, b)(c, d) = (ac, ad + b)$.

Доказать, что такая алгебраическая структура является группой.

2.23. Для каждого из следующих множеств отображений выяснить, образует ли оно группу относительно композиции отображений. В случае положительного ответа указать, будет ли группа абелевой:

1) все отображения множества первых n натуральных чисел на себя;

2) все инъективные отображения множества первых n натуральных чисел на себя;

3) все сюръективные отображения множества первых n натуральных чисел на себя;

4) все биективные отображения множества первых n натуральных чисел на себя.

2.24. Пусть в группе $G = \{(a,b) \mid a,b \in \mathbf{R}, a \neq 0\}$ операция умножения задана следующим образом: $(a,b)(c,d) = (ac, ad+b)$. Доказать, что пары $(a,0) \in G$ образуют подгруппу H группы G изоморфную мультипликативной группе ненулевых действительных чисел.

2.25. Пусть G — группа. Доказать, что для заданного $g \in G$ отображение $f : G \to G$, определенное правилом: для $\forall\, x \in G \quad f(x) = gxg^{-1}$, есть автоморфизм.

2.26. Пусть G — группа. Доказать, что для заданного $g \in G$ отображение $f : G \to G$, определенное правилом: для $\forall\, x \in G \quad f(x) = g^{-1}xg$, есть автоморфизм.

2.27. Пусть G — группа. Доказать, что отображение $\psi : G \to G\ \forall\, a \in G \quad \psi(a) = e$ (e — нейтральный элемент в G), есть эндоморфизм. Найти ядро $\operatorname{Ker}\psi$.

2.28. Доказать, что гомоморфный образ абелевой группы является абелевой группой.

2.29. Доказать изоморфность группы вещественных чисел по сложению группе R_+ положительных вещественных чисел по умножению.

2.30. Доказать, что группа $\mathbf{Z}$ целых чисел по сложению и группа $Z_{\text{ч}}$ четных целых чисел по сложению изоморфны.

2.31. Выяснить, какие из следующих множеств являются кольцами (но не полями) и какие — полями относительно указанных операций:

1) целые числа по сложению и умножению;

2) четные числа по сложению и умножению;

3) целые числа, кратные данному целому k $(k \neq 0)$, по сложению и умножению;

4) вещественные числа по сложению и умножению.

2.32. Доказать, что кольцо с единицей, содержащее не менее двух элементов, не может иметь единицу, равную нейтральному элементу по сложению.

2.33. Доказать, что в поле не может быть делителей нуля.

2.34. Найти правые и левые делители нуля в кольце $\mathbf{R}\times\mathbf{R}$ с заданными операциями:

а) сложения $(a,b)+(c,d)=(a+c,b+d)$ и умножения $(a,b)(c,d)=(ac,bd)$;

б) сложения $(a,b)+(c,d)=(a+c,b+d)$ и умножения $(a,b)(c,d)=(ad,bd)$.

2.35. Доказать, что в кольце с единицей коммутативность сложения следует из остальных аксиом кольца.

2.36. Пусть X — некоторое не пустое множество и 2^X — множество всех его подмножеств. Доказать, что 2^X — кольцо относительно операций

$(+)$ — симметрической разности подмножеств,

$(\cdot)$ — пересечения подмножеств.

Доказать, что это кольцо коммутативно и обладает единицей.

2.37. Доказать, что существует поле, состоящее из двух элементов.

2.38. Доказать, что множество S_n всех биективных отображений из конечного множества $V(|V|=n)$ в себя является группой по композиции отображений (эта группа называется симметрической группой). Найти ее порядок.

2.39. Доказать, что если на элементах коммутативной аддитивной группы $(K,+)$ задать операцию умножения следующим образом: $\forall\ a,b\in K\quad a*b=0$, то структура $(K,+,*)$ будет кольцом.

2.40. Доказать, что для группы G отображение

$$f:G\to G,\ \forall\ a\in G\quad f(a)=a^{-1}$$

является автоморфизмом тогда и только тогда, когда группа G абелева.

2.41. Кольцо с 1 называется *булевым*, если каждый его элемент a является *идемпотентным*, т. е. удовлетворяет условию $a^2 = a$. Доказать:

1) для любого элемента a булева кольца справедливо равенство $a + a = 0$;

2) булево кольцо коммутативно.

2.42. Доказать, что если все элементы коммутативного кольца имеют общий делитель, то в этом кольце есть 1. (Определение общего делителя приведено в § 3.)

РЕШЕНИЯ И ОТВЕТЫ К ЗАДАЧАМ § 2

2.1. На множестве $G = \{a, b\}$ операция задана таблицей Кэли. Является ли эта алгебраическая структура группой?

1)

	b	a
b	b	a
a	a	b

.

Решение. 1) Из таблицы Кэли видно, что операция не выводит из множества G, т. е. является бинарной. Выясним, является ли операция ассоциативной. В общем случае для n элементов доказательство ассоциативности операции требует проверки n^3 равенств. В данной задаче надо доказать следующие 8 равенств:

1. $a(aa) = (aa)a$.
2. $a(ab) = (aa)b$.
3. $a(ba) = (ab)a$.
4. $a(bb) = (ab)b$.
5. $b(aa) = (ba)a$.
6. $b(ab) = (ba)b$.
7. $b(ba) = (bb)a$.

8. $b(bb) = (bb)b$.

Докажем, например, четвертое равенство. Из таблицы Кэли следует: $a \underbrace{(bb)}_{b} = ab = a$; $\underbrace{(ab)}_{a} b = ab = a$.

Аналогично доказываются остальные равенства.

Из таблицы Кэли следует, что b является нейтральным элементом, т. к. $ab = ba = a$, $bb = b$.

Далее, из таблицы Кэли следует: $aa = b$ и $bb = b$. Отсюда, в силу единственности обратного элемента, находим: $a^{-1} = a$, $b^{-1} = b$.

Таблица Кэли симметрична, следовательно, операция коммутативна. Таким образом, рассматриваемая алгебраическая структура является абелевой группой.

2)

	a	b
a	b	a
b	a	a

.

Для таблицы 2) операция является бинарной, но не ассоциативной, например, не выполняется равенство

$$a(bb) = (ab)b,$$

в котором левая часть равна b, а правая часть равна a.

Поэтому эта структура не является даже полугруппой.

3)

	a	b
a	a	a
b	b	b

.

Для таблицы 3) операция является бинарной и ассоциативной, в чем можно убедиться, проверив выполнение равенств, аналогичных равенствам 1–8, приведенным выше. Однако здесь ни a, ни b не подходят на роль нейтрального элемента. Действительно, для a не выполняются равенства $ba = ab = b$, поскольку, как следует из таблицы Кэли, $ab = a$. А для b не выполняются равенства $ab = ba = a$, так как $ba = b$. Следовательно, эта алгебраическая структура является полугруппой, причем некоммутативной.

2.2. Какой алгебраической структурой является множество всех подмножеств некоторого множества X ($X \neq \varnothing$) с операцией

а) объединения подмножеств;

б) пересечения подмножеств?

Решение. а) Операция $\cup$ является бинарной, ассоциативной и коммутативной (свойства 1, 2 операций со множествами).
Нейтральным элементом является пустое множество $\varnothing$ в силу свойства 8 операций со множествами.
Обратного элемента нет $\rightarrow$ множество всех подмножеств некоторого множества с заданной операцией $\cup$ является коммутативным моноидом.

б) Аналогично доказывается, что множество всех подмножеств некоторого множества X с операцией $\cap$ является коммутативным моноидом, нейтральным элементом является множество X.

2.4. Ассоциативна ли операция $*$ на $\mathbf{R}$, определенная правилом $\forall\, x,\, y \in \mathbf{R}\ \ x * y = x^2 + y$?

Решение.
$(x * y) * z = (x^2 + y) * z = (x^2 + y)^2 + z$;
$x * (y * z) = x^2 + (y * z) = x^2 + y^2 + z$.
Операция $*$ не ассоциативна.

2.5. Доказать, что для произвольного отличного от нуля вещественного числа a множество $G = \{a^n |\ n \in \mathbf{Z}\}$ является абелевой группой по умножению.

Доказательство. Операция умножения на множестве G является бинарной, т. к. $\forall\, i, j \in \mathbf{Z}\ a^i a^j = a^{i+j} (4), i + j \in \in \mathbf{Z} \longrightarrow a^{i+j} \in G$.
Ассоциативность операции следует из свойств степени (4'): $\forall\, a^i,\, a^j,\, a^k \in G \longrightarrow (a^i a^j) a^k = a^{i+j+k} = a^i (a^j a^k)$.
$a^0 = 1$ нейтральный элемент $\in G (4)$.

Для любого $a^n \in G$ обратным является $a^{-n} \in G$, т. к. по свойству степени (4') $a^n a^{-n} = a^{-n} a^n = a^0 = 1$.

$\forall\, a^k, a^n \in G \quad a^n a^k = a^k a^n$, т. к. $a^n a^k = a^{n+k} = a^{k+n} = a^k a^n$.

Таким образом, доказано, что множество G по умножению является абелевой группой.

2.6. Выяснить, образуют ли группу относительно операции сложения

1) множество вещественных чисел $\mathbf{R}$;
2) множество неотрицательных вещественных чисел;
3) множество рациональных чисел $\mathbf{Q}$;
4) множество целых чисел $\mathbf{Z}$;
5) множество четных чисел;
6) множество нечетных чисел;
7) множество из одного числа 0.

Ответ: 1) да; 2) нет; 3) да; 4) да; 5) да; 6) нет; 7) да.
Рассмотрим, например, 5). Операция сложения на множестве $Z_{\text{ч}}$ четных чисел является бинарной, т. к. сумма двух четных чисел является четным числом, т. е. $\forall\ 2n,\ 2m \in Z_{\text{ч}}$ выполняется:

$2n + 2m = 2(n + m) \in Z_{\text{ч}}$.

Операция является ассоциативной в силу ассоциативности операции сложения целых чисел.
Нейтральным элементом по сложению является $0 \in Z_{\text{ч}}$.
Для любого $2n \in Z_{\text{ч}}$ противоположным является $-2n \in Z_{\text{ч}}$.

Таким образом, доказано, что множество четных чисел по сложению образует группу.

2.7. Образуют ли группу относительно операции умножения

1) множество вещественных чисел $\mathbf{R}$;
2) множество положительных вещественных чисел;
3) множество рациональных чисел $\mathbf{Q}$;
4) множество натуральных чисел $\mathbf{N}$?

Ответ: 1) нет; 2) да; 3) нет; 4) нет.

2.8. В таблице Кэли некоторой конечной группы выделен прямоугольник и известны элементы, стоящие в трех его вершинах (1 обозначен нейтральный элемент). Найти элемент в четвертой вершине.

1)

	...	x_k	...	x_p
...	...	...	...	...
x_m	...	a	...	?
...	...	...	...	...
x_t	...	1	...	b

.

Решение. 1) Найдем элемент $x_m x_p$. Из таблицы Кэли следует:

а) $x_m x_k = a$;

б) $x_t x_k = 1$;

с) $x_t x_p = b$.

В группе для любого элемента существует обратный. Домножим равенство а) справа на x_k^{-1}.

$$x_m \underbrace{x_k x_k^{-1}}_{1} = a x_k^{-1} \Longrightarrow \quad x_m = a x_k^{-1}.$$

Равенство с) домножим слева на x_t^{-1}.

$$\underbrace{x_t^{-1} x_t}_{1} x_p = x_t^{-1} b \quad \Longrightarrow \quad x_p = x_t^{-1} b.$$

Таким образом, $x_m x_p = a x_k^{-1} x_t^{-1} b$.

Докажем, что $x_k^{-1} = x_t$. Домножим равенство б) справа на x_k^{-1}.

$$x_t \underbrace{x_k x_k^{-1}}_{1} = x_k^{-1} \quad \longrightarrow x_t = x_k^{-1}.$$

Окончательно находим $x_m x_p = a x_t x_t^{-1} b = ab$.

2) Решить самостоятельно.

Ответ: ab.

2.9. Пусть для любого элемента a группы G выполняется равенство $a^2 = e$, где e — нейтральный элемент. Доказать, что группа является абелевой.

Доказательство. Условие задачи позволяет для любого элемента a записать $a^2 = aa = e \to a^{-1}aa = a^{-1} \to a = a^{-1}$. Таким образом, в заданной группе любой элемент равен обратному к нему элементу. Для элемента ab отсюда следует: $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$, т. е. $\forall\ a,\ b \in G\ ab = ba \longrightarrow$ группа абелева.

2.10. Какой алгебраической структурой является множество натуральных чисел с заданной операцией $\forall\ a, b \in \mathbf{N}$ $a * b = a^b$?

Ответ: операция бинарна и не ассоциативна, структура даже не полугруппа.

2.11. Какой алгебраической структурой является по сложению множество $M = \{m\,n|\ n \in \mathbf{Z}\}$, где m — некоторое целое число?

Решение. Если $m = 0$, то $M = \{0\}$. Это множество является группой по сложению.

Пусть $m \neq 0$. Операция бинарна, т. к. $\forall\ x,\ y \in M\ \ x = mn_1$, $y = mn_2 \longrightarrow x + y = m(n_1 + n_2),\ (n_1 + n_2) \in \mathbf{Z} \longrightarrow x + y \in M$.

Операция ассоциативна, т. к.

$\forall\ x,\ y,\ z \in M\ \ (x+y)+z = m(n_1+n_2)+mn_3 = m(n_1+n_2+n_3)$;

$x + (y + z) = mn_1 + m(n_2 + n_3) = m(n_1 + n_2 + n_3)$.

Операция коммутативна, т. к.

$\forall\ x,\ y \in M\ \ x + y = mn_1 + mn_2 = m(n_1 + n_2) = m(n_2 + n_1) =$

$= mn_2 + mn_1 = y + x$.

Нейтральным элементом по сложению является 0

$$m0 = 0 \to 0 \in M.$$

Противоположным элементу mn является элемент $m(-n) \in$ $\in M$, т. к. $mn + m(-n) = 0$. Таким образом, множество M,

состоящее из целых чисел, кратных заданному $m \in \mathbf{Z}$, является абелевой группой по сложению.

2.12. По какой алгебраической операции $(+, -, \cdot, :)$ множество $\{-1, 1\}$ является группой?

Ответ: по умножению и по делению множество $\{-1, 1\}$ является абелевой группой с нейтральным элементом 1 и обратными элементами $(1)^{-1} = 1$, $(-1)^{-1} = -1$.

2.13. Какие из следующих алгебраических структур являются группами?

а) $(\{1\}, \cdot)$; б) $(\{1\}, +)$.

Ответ: только а).

2.14. Образует ли множество векторов трехмерного пространства над полем действительных чисел группу относительно операции векторного умножения?

Ответ: нет, т. к. нет ассоциативности.

2.15. Пусть G — мультипликативная группа, $a, b \in G$. Доказать: если a коммутирует с b, то a^{-1} коммутирует с b^{-1}.

Указание: воспользоваться равенством (п. 3) $(ab)^{-1} = b^{-1}a^{-1}$ и тем, что в группе из равенства $x = y$ следует: $x^{-1} = y^{-1}$.

2.16. Пусть для элементов x, y моноида элементы xy и yx обратимы. Доказать, что элементы x и y тоже обратимы.

Доказательство. Из обратимости элементов xy и yx следуют равенства:

$$xy(xy)^{-1} = e, \quad (xy)^{-1}xy = e, \tag{a}$$

$$yx(yx)^{-1} = e, \quad (yx)^{-1}yx = e, \tag{b}$$

где e — нейтральный элемент.

Из первого равенства в (a) следует, что если элемент x обратим, то x^{-1} должен быть равен $x^{-1} = y(xy)^{-1}$ (в силу единственности обратного элемента в моноиде и равенства $x^{-1}x = e$).
Докажем, что элемент $y(xy)^{-1}$ является обратным к элементу x. Для этого, кроме равенства $x(y(xy)^{-1}) = e$, должно выполняться равенство

$$y(xy)^{-1}x = e. \qquad \text{(c)}$$

Докажем (c). Преобразуем левую часть первого равенства (b), вставив множитель $(xy)^{-1}xy = e$ и воспользовавшись ассоциативностью операции в моноиде

$$yx(yx)^{-1} = e \to y(\underbrace{(xy)^{-1}xy}_{e})x(yx)^{-1} = e \to$$
$$\to y(xy)^{-1}x(\underbrace{yx(yx)^{-1}}_{e}) = e \to y(xy)^{-1}x = e,$$

таким образом, равенство (c) доказано, и элемент $y(xy)^{-1}$ является обратным к элементу x, т. е. x — обратим.

Предлагается самостоятельно доказать, что элемент $x(yx)^{-1}$ является обратным к элементу y и, следовательно, y — обратим.

2.17. Пусть $(G,\ \circ)$ — группа, $a \in G$. На множестве G определена другая операция $*$ следующим образом: $\forall\, x,\, y \in \in G\ \ x * y = x \circ a \circ y$. Доказать, что $(G,\ *)$ — группа.

Доказательство. 1. Операция $*$ бинарна, т. к.
$\forall\, x,\, y \in G\ \ x * y \in G$, т. к. $x \circ a \circ y \in G$.

2. Операция $*$ ассоциативна, т. к.
$(x * y) * z = (x \circ a \circ y) * z = (x \circ a \circ y) \circ a \circ z = x \circ a \circ y \circ a \circ z.$
$x * (y * z) = x \circ a \circ (y * z) = x \circ a \circ (y \circ a \circ z) = x \circ a \circ y \circ a \circ z.$

3. Докажем, что нейтральным элементом $\widetilde{e}$ по операции $*$ является $\tilde{e} = a^{-1}$. Обозначим e — нейтральный элемент в группе $(G,\ \circ)$.

$$\forall\, x \in G \quad x * a^{-1} = x \underbrace{\circ a \circ a^{-1}}_{e} = x, \quad a^{-1} * x = \underbrace{a^{-1} \circ a}_{e} \circ x = x.$$

4. Найдем обратный элемент $x^{\ominus 1}$ для x относительно операции $*$. Он должен удовлетворять равенствам

$$x * x^{\ominus 1} = x^{\ominus 1} * x = \tilde{e} = a^{-1}.$$

Первое равенство $x * x^{\ominus 1} = a^{-1}$ эквивалентно равенству $x \circ a \circ x^{\ominus 1} = a^{-1}$, домножим его слева на элемент $(x \circ a)^{-1}$, обратный к $(x \circ a)$ относительно операции $\circ$.

$$\underbrace{(x \circ a)^{-1} \circ x \circ a}_{e} \circ x^{\ominus 1} = (x \circ a)^{-1} \circ a^{-1} \longrightarrow$$

$$\longrightarrow x^{\ominus 1} = a^{-1} \circ x^{-1} \circ a^{-1}.$$

Докажем, что найденный $x^{\ominus 1}$ удовлетворяет равенству $x^{\ominus 1} * x = a^{-1}$. Действительно, имеем:

$$x^{\ominus 1} * x = x^{\ominus 1} \circ a \circ x = a^{-1} \circ x^{-1} \circ \underbrace{a^{-1} \circ a}_{e} \circ x = a^{-1}.$$

Таким образом, для $\forall\, x \in G$ обратный элемент $x^{\ominus 1}$ существует и равен $x^{\ominus 1} = a^{-1} \circ x^{-1} \circ a^{-1}$.

Из 1–4 следует, что алгебраическая структура $(G, *)$ — группа.

2.19. Пусть G — множество всех вещественных чисел, отличных от -1. Доказать, что G — группа относительно операции

$a * b = ab + a + b$.

Доказательство. 1. Покажем, что операция $*$ бинарна.

$\forall\, a, b \in G\ a*b = ab+a+b = a(b+1)+b+1-1 = (a+1)(b+1)-1 = c.$

$c \neq -1$, т. к. $a \neq -1$ и $b \neq -1$. Следовательно, $c \in G$, т. е. доказали, что

$$\forall\, a, b \in G \ \to a * b \in G.$$

2. Ассоциативность операции $*$ проверяется непосредственно.

$$(a*b)*c=(ab+a+b)*c=abc+ac+bc+ab+a+b+c.$$
$$a*(b*c)=a*(bc+b+c)=abc+ab+ac+a+bc+b+c=$$
$$=abc+ac+bc+ab+a+b+c.$$

3. Докажем, что нейтральным элементом относительно операции $*$ является $0\in G$.
$\forall\, a\in G\quad a*0=a\,0+a+0=a,$
$0*a=0\,a+0+a=a.$

4. Найдем обратный элемент a^{-1} для a относительно операции $*$. Он должен удовлетворять равенствам

$\forall\, a\in G\quad a*a^{-1}=a^{-1}*a=0.$
$a*a^{-1}=aa^{-1}+a+a^{-1}=0\longrightarrow a^{-1}=-a(a+1)^{-1}.$
$a^{-1}*a=-a(a+1)^{-1}\,a-a(a+1)^{-1}+a=(-a^2-a+a^2+a)(a+$
$+1)^{-1}=0.$

Здесь использованы равенство $a=a(a+1)(a+1)^{-1}$ и одинаковая запись обратного элемента по операции $*$ и по операции умножения ненулевых вещественных чисел. Таким образом, для $\forall\, a\in G$ обратный элемент a^{-1} существует и равен $a^{-1}=-a(a+1)^{-1}$.

Из 1–4 следует, что алгебраическая структура $(G,*)$ является группой.

2.20. Пусть H — подгруппа группы G. Доказать, что если множество $(G\backslash H)\cup\{e\}$ — подгруппа группы G, то либо $H=\{e\}$, либо $H=G$, здесь e — нейтральный элемент группы G.

Решение. Простой пример демонстрирует, что это так. Пусть $\mathbf{Z}$ — множество целых чисел (группа по сложению), $Z_{\text{ч}}$ — множество четных чисел (подгруппа группы $\mathbf{Z}$).

Множество $(\mathbf{Z}\setminus Z_{\text{ч}})\cup\{0\}=Z_{\text{неч}}\cup\{0\}$ — множество, не являющееся группой по сложению, т. к. операция сложения выводит из него. Докажем утверждение в общем случае.

Пусть H — собственная подгруппа группы G, т. е. H отлична от $\{e\}$ и от G. Докажем, что в этом случае множество $(G\backslash H) \cup \{e\}$ не является подгруппой. Найдем такие два элемента множества $(G\backslash H) \cup \{e\}$, произведение которых не принадлежит этому множеству, этого достаточно для доказательства того, что $(G\backslash H) \cup \{e\}$ не является подгуппой (п. 5).

Замечание $(*)$. $\triangleright$ Докажем вспомогательное утверждение, а именно, что

$$\forall\, a \in G \setminus H, \quad \forall\, h \in H \longrightarrow ah \in G \setminus H.$$

Убедимся в том, что ah не входит в подгруппу H. Предположим противное, пусть $ah \in H$. Домножим ah справа на h^{-1} : $ahh^{-1} = a$. В левой части здесь стоит произведение элементов из подгруппы H, следовательно, $ahh^{-1} \in H$, но это противоречит тому, что $a \in G \setminus H$. Полученное противоречие доказывает, что $ah \in G \setminus H$. $\triangleleft$

Заметим, что для $\forall\, a \in G \setminus H \longrightarrow\ a^{-1} \in G \setminus H$, т. к. если предположить противное $(a^{-1} \in H)$, то приходим к условию $a \in H$, (т. к. H — подгруппа), что противоречит тому, что $a \in G \setminus H$.

Пусть $h \in H$, $h \neq e$ и $a \in G \setminus H$. Рассмотрим элементы ha и a^{-1}. Оба они по доказанному в замечании $(*)$ принадлежат $G \setminus H$: $ha \in G \setminus H$, $a^{-1} \in G \setminus H$. Легко видеть, что произведение этих элементов не принадлежит $(G\backslash H) \cup \{e\}$:

$$haa^{-1} = h \in H \longrightarrow\ haa^{-1} \notin (G\backslash H) \cup \{e\},$$

следовательно, $(G\backslash H) \cup \{e\}$ не является собственной подгруппой.

2.21. Доказать, что из существования в полугруппе G левого нейтрального элемента $e_{\text{л}}$ такого, что

$$\forall\, a \in G \quad e_{\text{л}} a = a, \tag{1}$$

и существования для каждого элемента полугруппы левого обратного элемента $a_{\text{л}}^{-1}$ такого, что

$$\forall\, a \in G \quad \exists\, a_{\text{л}}^{-1} \in G \quad a_{\text{л}}^{-1} a = e_{\text{л}}, \tag{2}$$

следует, что полугруппа G является **группой**, т. е. левый нейтральный элемент одновременно является и правым нейтральным элементом, а левый обратный элемент для каждого элемента является одновременно и правым обратным.

Доказательство. Докажем, что для любого элемента полугруппы левый обратный к нему элемент является в этом случае и правым обратным, а именно

$$\forall\ a \in G \quad a_{\text{Л}}^{-1}a = e_{\text{Л}} \quad \to \quad aa_{\text{Л}}^{-1} = e_{\text{Л}}. \tag{3}$$

Обозначим левый обратный элемент к $a_{\text{Л}}^{-1}$ через x, по условию он существует, т. к. левый обратный существует к любому элементу полугруппы

$$xa_{\text{Л}}^{-1} = e_{\text{Л}}. \tag{4}$$

Учтем, что из определения левой единицы (т. е. левого нейтрального элемента) следует равенство:

$$a_{\text{Л}}^{-1} = e_{\text{Л}}a_{\text{Л}}^{-1}.$$

Подставим это представление для $a_{\text{Л}}^{-1}$ в (4): $xe_{\text{Л}}a_{\text{Л}}^{-1} = e_{\text{Л}}$ и выразим $e_{\text{Л}}$ в левой части получившегося равенства в соответствии с (2) и далее воспользуемся ассоциативностью умножения в полугруппе, в результате придем к равенствам

$$\begin{aligned} xa_{\text{Л}}^{-1}aa_{\text{Л}}^{-1} = e_{\text{Л}} \quad \to \quad (xa_{\text{Л}}^{-1})aa_{\text{Л}}^{-1} = e_{\text{Л}} \quad \to \\ \to \quad e_{\text{Л}}aa_{\text{Л}}^{-1} = e_{\text{Л}} \quad \to \quad aa_{\text{Л}}^{-1} = e_{\text{Л}}. \end{aligned}$$

Равенство (3) доказано.

Докажем, что левый нейтральный элемент $e_{\text{Л}}$ (1) является одновременно и правым нейтральным, т. е. является нейтральным элементом по умножению. Докажем, что

$$\forall\ a \in G \quad e_{\text{Л}}a = a \quad \to ae_{\text{Л}} = a. \tag{5}$$

Воспользуемся ассоциативностью умножения, равенствами (3) и преобразуем выражение $ae_{\text{Л}}$ следующим образом:

$$ae_{\text{Л}} = a(a_{\text{Л}}^{-1}a) = (aa_{\text{Л}}^{-1})a = e_{\text{Л}}a = a,$$

таким образом, равенство (5) доказано.

2.22. На множестве $G = \{(a,b) \mid a,b \in \mathbf{R}, a \neq 0\}$ задана операция умножения $(a,b)(c,d) = (ac, ad+b)$. Доказать, что такая алгебраическая структура является группой.

Доказательство. 1. Убедимся в том, что операция бинарна. Для любых двух элементов множества G имеем:

$$(a,b)(c,d) = (ac, ad+b) \in G, \text{ т. к.}$$

$ac \in \mathbf{R}$, $ad+b \in \mathbf{R}$, $a \neq 0$, $c \neq 0 \longrightarrow ac \neq 0$, т. е. операция бинарная.

2. Покажем, что операция ассоциативна.

$$((a,b)(c,d))\,(f,g) = (ac, ad+b)(f,g) = (acf, acg+ad+b),$$

$$(a,b)\,((c,d)(f,g)) = (a,b)(cf, cg+d) = (acf, acg+ad+b).$$

Таким образом, для любых трех элементов из G выполняется равенство

$$((a,b)(c,d))\,(f,g) = (a,b)\,((c,d)(f,g))\,,$$

т. е. операция ассоциативна.

3. Нейтральный элемент (e_1, e_2), если он существует, должен удовлетворять равенствам

$$\forall\,(a,b) \in G \quad (e_1,e_2)(a,b) = (a,b) \text{ и } (a,b)(e_1,e_2) = (a,b),$$

соответственно должны выполняться равенства:

$$\begin{cases} e_1 a = a, \\ e_1 b + e_2 = b \end{cases}$$

и

$$\begin{cases} a e_1 = a, \\ a e_2 + b = b. \end{cases}$$

Их выполнение возможно при $e_1 = 1, e_2 = 0$. Следовательно, нейтральный элемент существует и равен $(1,0)$.

4. Найдем обратный элемент $(a,b)^{-1}$ к элементу (a,b), если он существует. Обратный элемент должен удовлетворять равенствам

$$\forall\ (a,b)\in G\quad (a,b)^{-1}(a,b)=(a,b)(a,b)^{-1}=(1,0).$$

Обозначим $(a^*,b^*)=(a,b)^{-1}$. Из равенств $(a^*,b^*)(a,b)=$ $=(a,b)(a^*,b^*)=(1,0)$ следует:

$$\left\{\begin{array}{ll} a^*a=1, & \to\\ a^*b+b^*=0, & \end{array}\right.$$

$$\to\left\{\begin{array}{l} a^*=a^{-1},\\ a^{-1}b+b^*=0. \end{array}\right.$$

Отсюда находим, что $a^*=a^{-1},\quad b^*=-a^{-1}b$. Таким образом, для любого $(a,b)\in G$ найден обратный элемент, равный $(a^{-1},-a^{-1}b)$.

Из 1–4 следует, что рассматриваемая алгебраическая структура является группой.

2.23. Для каждого из следующих множеств отображений выяснить, образует ли оно группу относительно композиции отображений. В случае положительного ответа указать, будет ли группа абелевой:

1) все отображения множества первых n натуральных чисел на себя;

2) все инъективные отображения множества первых n натуральных чисел на себя;

3) все сюръективные отображения множества первых n натуральных чисел на себя;

4) все биективные отображения множества первых n натуральных чисел на себя.

Решение. Обозначим $\hat{N}$ — множество первых n натуральных чисел, $|\hat{N}|=n$.

Пусть W — множество всевозможных отображений из $\hat{N}$ в $\hat{N}$, т. е. $W=\{f_1,\ f_2,\dots,f_m\},\quad f_i:\hat{N}\to\hat{N},\quad i=1,2,\dots,m$.

Количество всевозможных отображений из конечного множества $\hat{N}$ в себя, как следует из решенной далее задачи 4.13 § 4, равно n^n, т. е. $|W| = n^n$.

Выясним, для каких отображений множество W по композиции отображений является группой. Композиция любых отображений $f_1, f_2 \in W$ является отображением из W, т. е. операция бинарна. Операция ассоциативна, т. к. композиция отображений (если она определена) ассоциативна. В данном случае определена композиция любых отображений из W. Нейтральным элементом, очевидно, является тождественное отображение $\mathrm{Id} \in W$, т. к. $\forall\ f \in W\ f \circ \mathrm{Id} = \mathrm{Id} \circ f = f$. Таким образом, для отображения 1) структура $(W, \circ)$ является моноидом.

Для группы необходимо существование для каждого элемента обратного, т. е. для любого отображения $f : \hat{N} \to \hat{N}$ необходимо существование обратного отображения $f^{-1} : \hat{N} \to \hat{N}$. Как известно (п. 39 § 1), для этого необходима биективность отображения f. В задаче 1.32 § 1 доказано, что для биективности отображения из конечного множества в себя достаточно, чтобы отображение было либо инъекцией, либо сюръекцией. Таким образом, во 2), 3) и 4) вариантах речь идет о биективных отображениях. Пусть W_1 — множество биективных отображений из $\hat{N}$ в $\hat{N}$. Композиция биекций является биекцией (п. 36 § 1), следовательно, операция композиции отображений не выводит из множества W_1, т. е. является бинарной. Композиция биекций, как и композиция любых отображений, ассоциативна. Нейтральный элемент, т. е. тождественное отображение $\mathrm{Id} : \hat{N} \to \hat{N}$, есть биективное отображение, т. е. $\mathrm{Id} \in W_1$. Поэтому структуры 2)–4) будут моноидами, каждый элемент которых обратим, т. е. будут группами, причем некоммутативными, поскольку коммутативности операции композиции отображений в общем случае нет.

Количество всевозможных биективных отображений из конечного множества $\hat{N}$ в себя, как следует из решенной далее

задачи 4.14 § 4, равно $n!$, т. е. порядок каждой из групп 2)–4) равен $n!$.

Замечание. Если в качестве $\hat{N}$ взять произвольное конечное множество мощности n, то получим так называемую *симметрическую группу* S_n, элементами которой являются биекции $f : \hat{N} \to \hat{N}$, $|\hat{N}| = n$, $S_n = \{f_1 \dots, f_m\}$, $|S_n| = n!$. Симметрическая группа является стартовой площадкой, с которой начинаются всевозможные применения теории групп.

2.24. Пусть в группе $G = \{(a, b) \mid a, b \in \mathbf{R}, a \neq 0\}$ операция умножения задана следующим образом: $(a, b)(c, d) = (ac, ad + b)$. Доказать, что пары $(a, 0) \in G$ образуют подгруппу H группы G, изоморфную мультипликативной группе ненулевых действительных чисел.

Доказательство. Множество H является подгруппой группы G, т. к. (п. 5)

а) $\forall\ (a, 0), (c, 0) \in H \longrightarrow (a, 0)(c, 0) = (ac, 0) \in H$, т. е. операция не выводит из множества H.

б) Как следует из решения задачи 2.22, обратный элемент к элементу $(a, b) \in G$ равен $(a, b)^{-1} = (a^{-1}, -a^{-1}b)$. Таким образом, $\forall\ (a, 0) \in H \longrightarrow$ обратный элемент существует и равен $(a, 0)^{-1} = (a^{-1}, 0) \in H$.

Докажем, что подгруппа H изоморфна группе $(\underbrace{R \setminus \{0\}}_{R^*}, \cdot)$. Для этого достаточно построить изоморфное отображение из H в R^*.

Докажем, что отображение $\psi : H \to R^*$, определенное правилом $\forall\, (a, 0) \in H \quad \psi((a, 0)) \overset{d}{=} a \quad (a \in R^*)$, является изоморфизмом, т. е. гомоморфно и биективно.

Оно гомоморфно, т. к. для любых $(a, 0),\ (b, 0) \in H$

$$\psi((a, 0)(b, 0)) = \psi((ab, 0)) = ab = \psi((a, 0))\psi((b, 0)).$$

То, что отображение ψ биективное, следует из существования обратного отображения (п. 39 § 1). Убедимся в том, что оно

существует.

$$\psi^{-1} : R^* \to H,\ \forall x \in R^*\ \ \psi^{-1}(x) = (x, 0).$$

$$\forall x \in R^*\ \ \psi\psi^{-1}(x) = \psi(\psi^{-1}(x)) = \psi(x, 0) = x =$$

$$= \mathrm{Id}_{R^*}(x) \longrightarrow \psi\,\psi^{-1} = \mathrm{Id}_{R^*};$$

$$\forall (a, 0) \in H\ \ \psi^{-1}\psi(a, 0) = \psi^{-1}(\psi(a, 0)) = \psi^{-1}(a) =$$

$$= (a, 0) = \mathrm{Id}_H(a, 0) \longrightarrow \psi^{-1}\psi = \mathrm{Id}_H.$$

Построенное изоморфное отображение доказывает изоморфность этих групп.

2.25. Пусть G — группа. Доказать, что для заданного $g \in$ $\in G$ отображение $f : G \to G$, определенное правилом $\forall\ x \in$ $\in G\ \ f(x) = gxg^{-1}$, есть автоморфизм.

Доказательство. Докажем, что отображение $f : G \to G$ — изоморфно, т. е. биективно и гомоморфно.

1. *Биективность*. Покажем, что отображение инъективно. Для любых $x_1, x_2 \in G$ из равенства $f(x_1) = f(x_2) \to$ $\to\ gx_1g^{-1} = gx_2g^{-1} \to x_1 = x_2$. В соответствием с п. 28 § 1, такое отображение инъективно.

Покажем, что отображение сюръективно, т. е. что для $\forall\, h \in G$ существует $x \in G$ такой, что $h = f(x)$.

Найдем этот x: $h = f(x) = gxg^{-1} \to x = g^{-1}hg$. Для $\forall\ h$ такой элемент $g^{-1}hg$ существует и принадлежит G.

Из инъективности и сюръективности отображения следует его биективность.

2. Докажем, что $f : G \to G$ — *гомоморфизм*.

Для любых $a, b \in G\ \ f(ab) = gabg^{-1} = gag^{-1}gbg^{-1} =$ $= f(a)f(b)$.

Из 1–2 следует, что отображение $f : G \to G$ является автоморфизмом.

2.27. Пусть G — группа. Доказать, что отображение $\psi : G \to G\ \forall a \in G\ \ \psi(a) = e$ (e — нейтральный элемент в G), есть эндоморфизм. Найти ядро $\mathrm{Ker}\,\psi$.

Ответ. $\operatorname{Ker}\psi = G$.

2.28. Доказать, что гомоморфный образ абелевой группы является абелевой группой.

Доказательство. Дано: G — абелева группа, $f : G \to H$ — гомоморфное отображение. Надо доказать, что $f(G)$ является абелевой группой, т. е. доказать, что для $\forall\, u, v \in f(G)$ выполняется равенство $uv = vu$. То, что $f(G)$ является группой, следует из того, что образ $\operatorname{Im} f$ любого гомоморфизма $f : G \to$ $\to H$ $(\operatorname{Im} f = f(G))$ является подгруппой группы H (п. 11). Докажем коммутативность.

$\forall\, u, v \in f(G) \longrightarrow \exists\, x, y \in G$ такие, что $u = f(x)$, $v =$ $= f(y) \longrightarrow uv = f(x)f(y) =$ т. к. гомоморфизм $= f(xy) =$ т. к. группа G абелева $= f(yx) = f(y)f(x) = uv$.

2.29. Доказать изоморфность группы вещественных чисел по сложению группе положительных R_+ вещественных чисел по умножению.

Доказательство. Для доказательства изоморфности двух групп достаточно построить изоморфное отображение одной группы на другую (п. 12).

Рассмотрим отображение $f : R \to R_+ \;\; \forall\, x \in R \;\; f(x) = e^x$.

Докажем, что оно биективно и гомоморфно, т. е. является изоморфизмом.

Для доказательства биективности достаточно построить обратное отображение $f^{-1} : R_+ \to R$, $f^{-1}f = \operatorname{Id}_R$, $ff^{-1} =$ $= \operatorname{Id}_{R_+}$ (п. 39 § 1).

Здесь и далее для облегчения записи опустим знак композиции. Нетрудно проверить, что обратным является отображение, заданное правилом

$$\forall\, y \in R_+ \;\; f^{-1}(y) = \ln y.$$

Действительно, имеют место равенства:

$$\forall y \in R_+ \quad ff^{-1}(y) = f(\ln y) = e^{\ln\, y} = \\ = y = \mathrm{Id}_{R_+}(y) \to ff^{-1} = \mathrm{Id}_{R_+};$$

$$\forall x \in R \quad f^{-1}f(x) = f^{-1}(e^x) = \ln e^x = \\ = x = \mathrm{Id}_R(x) \to f^{-1}f = \mathrm{Id}_R.$$

Докажем, что $f : R \to R_+$ — гомоморфизм.

$$\forall x, y \in R \quad f(x+y) = e^{x+y} = e^x e^y = f(x)f(y).$$

Итак, отображение $f : R \to R_+$ является изоморфизмом, отсюда следует изоморфность группы вещественных чисел по сложению группе положительных вещественных чисел по умножению.

2.30. Доказать, что группа $\mathbf{Z}$ целых чисел по сложению и группа $Z_{\text{ч}}$ четных целых чисел по сложению изоморфны.

Доказательство. Для доказательства изоморфности двух групп построим между ними изоморфное отображение (п. 12).

Рассмотрим отображение $\varphi : \mathbf{Z} \to Z_{\text{ч}}$ $\forall x \in \mathbf{Z}$ $\varphi(x) = 2x$. Докажем, что оно биективно и гомоморфно, т. е. является изоморфизмом.

Для доказательства *биективности* достаточно построить обратное отображение (п. 41 § 1). Нетрудно проверить, что обратным является отображение $\varphi^{-1} : Z_{\text{ч}} \to \mathbf{Z}$, заданное правилом $\forall y \in Z_{\text{ч}} \quad \varphi^{-1}(y) = \dfrac{y}{2}$.

Действительно, имеют место равенства:

$\forall y \in Z_{\text{ч}} \quad \varphi\varphi^{-1}(y) = \varphi\left(\dfrac{y}{2}\right) = 2\dfrac{y}{2} = y = \mathrm{Id}_{Z_{\text{ч}}}(y) \to \varphi\varphi^{-1} = \mathrm{Id}_{Z_{\text{ч}}}$;

$\forall x \in \mathbf{Z} \quad \varphi^{-1}\varphi(x) = \varphi^{-1}(2x) = \dfrac{2x}{2} = x = \mathrm{Id}_{\mathbf{Z}}(x) \to \varphi^{-1}\varphi = \mathrm{Id}_{\mathbf{Z}}$.

Докажем, что $\varphi : \mathbf{Z} \to Z_{\text{ч}}$ является *гомоморфизмом*.

$$\forall x, y \in \mathbf{Z} \quad \varphi(x+y) = 2(x+y) = 2x + 2y = \varphi(x) + \varphi(y).$$

Таким образом, $\varphi : \mathbf{Z} \to Z_{\text{ч}}$ является изоморфизмом, следовательно, группа целых чисел по сложению изоморфна группе четных целых чисел по сложению.

2.31 Выяснить, какие из следующих множеств являются кольцами (но не полями) и какие полями относительно указанных операций:

1) целые числа по сложению и умножению;

2) четные числа по сложению и умножению;

3) целые числа, кратные данному целому числу k $(k \neq 0)$ по сложению и умножению;

4) вещественные числа по сложению и умножению.

Решение. В качестве примера рассмотрим решение 2), т. е. докажем, что четные числа по сложению и умножению образуют кольцо. В задаче 2.6 5) доказано, что структура $(Z_{\text{ч}}, +)$ является абелевой группой. По умножению множество четных чисел является коммутативной полугруппой, т. к. произведение четных чисел является четным числом, т. е. операция умножения на множестве четных чисел бинарна. Умножение четных чисел (как и других целых чисел) ассоциативно, коммутативно и, кроме того, умножение дистрибутивно относительно сложения для четных чисел. Во множестве $Z_{\text{ч}}$ нет нейтрального элемента по умножению, т. к. $1 \notin Z_{\text{ч}}$, следовательно, $(Z, +, \cdot)$ только кольцо, но никогда не поле. Остальные задачи решить самостоятельно.

Ответ: 1)–3) — кольца, но не поля, 4) — поле.

2.33. Доказать, что в поле не может быть делителей нуля.

Доказательство. По определению (п. 15), поле — коммутативное кольцо, все ненулевые элементы которого обратимы. Из п. 14 следует, что обратимые элементы кольца не могут быть делителями нуля $\longrightarrow$ поле не может содержать делителей нуля.

2.34. Найти правые и левые делители нуля в кольце $\mathbf{R}\times\mathbf{R}$ с заданными операциями

а) сложения $(a,b)+(c,d)=(a+c,b+d)$ и
умножения $(a,b)(c,d)=(ac,bd)$;

б) сложения $(a,b)+(c,d)=(a+c,b+d)$ и
умножения $(a,b)(c,d)=(ad,bd)$.

Решение. а) Легко проверяется, что заданная операция умножения является коммутативной, т. к. $ac=ca$, $bd=db$ для любых вещественных a,b,c,d. Поэтому далее речь идет о делителе нуля в коммутативном кольце.

Пара $(x,y)\neq(0,0)$ является нетривиальным делителем нуля в коммутативном кольце, если существует пара $(\xi,\eta)\neq$ $\neq(0,0)$ такая, что $(x,y)(\xi,\eta)=(0,0)$ (п. 13). По определению операции умножения имеем: $(x,y)(\xi,\eta)=(x\xi,y\eta)$. Убедимся в том, что пары, в которых $x=0$, $y\neq0$ и $\xi\neq0$, $\eta=0$, являются нетривиальными делителями нуля. Действительно: $(0,y)(\xi,0)=(0,0)$.

б) Решить самостоятельно.

2.35. Доказать, что в кольце K с единицей e коммутативность сложения следует из остальных аксиом кольца.

Доказательство. Докажем, что сложение коммутативно, т. е. что для $\forall\ a,\ b\in K$ $a+b=b+a$. Раскроем скобки в выражении $(a+b)(e+e)$, пользуясь дистрибутивностью умножения относительно сложения. Сделаем это двумя способами:

1. $(a+b)(e+e)=(a+b)e+(a+b)e=ae+be+ae+be=$ $=a+b+a+b$.

2. $(a+b)(e+e)=a(e+e)+b(e+e)=ae+ae+be+be=$ $=a+a+b+b$.

В результате пришли к равенству $a+b+a+b=a+a+b+b$, из которого следует условие коммутативности $b+a=a+b$ операции сложения.

2.36. Пусть X — некоторое не пустое множество и 2^X — множество всех его подмножеств. Доказать, что 2^X — кольцо относительно операций

$(+)$ — симметрической разности подмножеств,

$(\cdot)$ — пересечения подмножеств.

Доказать, что это кольцо коммутативно и обладает единицей.

Указание: воспользоваться задачами 1.14–1.16 § 1 и показать, что нейтральным элементом по сложению является пустое множество $\oslash$, а по умножению — само множество X.

2.37. Доказать, что существует поле, состоящее из двух элементов.

Указание: рассмотреть множество, состоящее из двух элементов, один из которых является нейтральным элементом по сложению, т. е. нулем, а другой — нейтральным элементом по умножению, т. е. единицей.

2.40. Доказать, что отображение $f : G \to G$, $\forall\ a \in G\quad f(a) = a^{-1}$ является автоморфизмом группы G тогда и только тогда, когда группа G абелева.

Доказательство. Пусть G — абелева группа. Докажем, что заданное отображение изоморфно, тогда, по определению автоморфизма (п. 6), оно будет автоморфизмом группы G. Отображение изоморфно, если оно гомоморфно и биективно. Для доказательства гомоморфности воспользуемся свойством групп (п. 3) $(xy)^{-1} = y^{-1}x^{-1}$, с учетом которого для заданного отображения можно записать

$$\forall\, a, b \in G\quad f(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = f(a)f(b).\ (*)$$

Здесь равенство $b^{-1}a^{-1} = a^{-1}b^{-1}$ следует из заданной коммутативности группы G. Из (*) следует, что рассматриваемое отображение гомоморфно.

Докажем биективность. В соответствии с п. 39 § 1 для доказательства биективности отображения $f : G \to G$

достаточно построить обратное к нему отображение. Рассмотрим в качестве обратного отображение:

$$f^{-1} : G \to G \quad \forall\, a \in G \quad f^{-1}(a) = a^{-1}.$$

В том, что оно является обратным, нетрудно убедиться, если учесть свойство групп (п. 3) $\forall\, a \in G \quad (a^{-1})^{-1} = a$. Доказанные гомоморфность и биективность свидетельствуют о том, что рассматриваемое отображение является автоморфизмом.

Пусть отображение $f : G \to G,\ \forall\, a \in G \quad f(a) = a^{-1}$ является автоморфизмом. Докажем, что группа G в этом случае является абелевой.

$\forall\, a, b \in G \quad f(ab) = f(a)f(b) \to (ab)^{-1} = a^{-1}b^{-1}$.

С учетом свойства групп (п. 3) должно выполняться равенство

$\forall\, a, b \in G \quad (ba)^{-1} = a^{-1}b^{-1}$.

Следовательно, имеет место равенство $\forall\ a, b \in G \quad (ba)^{-1} = (ab)^{-1}$. В группе для любых элементов $x,\ y$ из равенства $x^{-1} = y^{-1}$ следует равенство: $x = y$ (для доказательства этого достаточно домножить обе части равенства $x^{-1} = y^{-1}$ слева на x и справа на y), таким образом, из равенства $(ba)^{-1} = (ab)^{-1}$ следует равенство $ba = ab$, доказывающее коммутативность группы G.

2.41. Кольцо с 1 называется *булевым*, если каждый его элемент a является *идемпотентным*, т. е. удовлетворяет условию $a^2 = a$. Доказать:

1) для любого элемента a булева кольца справедливо равенство $a + a = 0$;

2) булево кольцо коммутативно.

Доказательство. 1) Докажем, что для любого элемента a булева кольца K справедливо равенство $a + a = 0$.

Элемент $a+a\ \in K \longrightarrow (a+a)^2 = a+a \longrightarrow aa+aa+aa+aa = a + a \longrightarrow a + a + a + a = a + a \longrightarrow a + a = 0$.

В частности, в булевом кольце любой элемент равен своему противоположному: $a = -a$. $(*)$

2) Докажем коммутативность булева кольца K.

$$\forall\ a, b \in K \to (a+b) \in K \to$$
$$\to (a+b)^2 = a+b \longrightarrow \underbrace{aa}_{a} + ab + ba + \underbrace{bb}_{b} = a+b \longrightarrow$$
$$\longrightarrow ab + ba = 0 \longrightarrow ab = -ba \longrightarrow ab = ba,$$
$$\text{т. к. } (*) \quad -ba = ba.$$

2.42. Доказать, что если все элементы коммутативного кольца имеют общий делитель, то в этом кольце есть 1. (Определение общего делителя приведено в § 3.)

Доказательство. Тот факт, что элемент a коммутативного кольца $\mathcal{K}$ имеет делитель d означает, что существует элемент c кольца такой, что

$$a = cd = dc, \quad d, c \in \mathcal{K}.$$

По условию задачи *все* элементы кольца имеют общий делитель, следовательно, и сам d имеет делителем этот общий делитель d, т. е.

$$d = ed = de, \quad e \in \mathcal{K}. \tag{1}$$

Из равенства (1) следует, что для d элемент e является нейтральным, т. е. единицей. Докажем, что e является единицей для любого элемента кольца, т. е. что для $\forall\ x \in \mathcal{K}$ выполняются равенства $xe = ex = x$. Воспользуемся тем, что все элементы имеют d делителем, и запишем

$$\forall\ x \in \mathcal{K} \quad x = c_x d = dc_x, \quad c_x \in \mathcal{K}. \tag{2}$$

Равенства (1), (2), ассоциативность и коммутативность умножения в кольце позволяют записать следующие равенства, доказывающие, что e является единицей данного кольца:

$$\forall\ x \in \mathcal{K} \quad x \overset{2}{=} c_x d \overset{1}{=} c_x de; \quad x \overset{2}{=} dc_x \overset{1}{=} edc_x \overset{2}{=} ec_x d \to$$
$$\to \quad (c_x d)e = e(c_x d) = x \quad \to \quad xe = ex = x.$$

§ 3. ЭЛЕМЕНТАРНАЯ ТЕОРИЯ ЧИСЕЛ

Множество целых чисел $\mathbf{Z}$ с операциями сложения и умножения чисел является *целостным коммутативным кольцом с единицей*. Приведем основные сведения из теории делимости в кольце целых чисел. Целое число a делится на целое число b ($a \vdots b$), если существует целое c такое, что $a = bc$.

Свойства отношения делимости в кольце $\mathbf{Z}$

1. $a \vdots a$ (рефлексивность).

2. $a \vdots b$ и $b \vdots c \to a \vdots c$ (транзитивность).

3. $\forall a \ \in \mathbf{Z} \quad 0 \vdots a$.

4. $\forall a \in \mathbf{Z}$ имеет делители ± 1, $\pm a$.

5. $a \vdots b$ и $c \vdots b \to \forall q, s \in \mathbf{Z} \quad qa \pm sc \vdots b$.

6. $a \vdots b \to \forall k \in \mathbf{Z} \quad ak \vdots b$.

7. $a \vdots b$ и $b \vdots a \to a = \pm b$.

8. $a \vdots b$ и $a \neq 0 \to |a| \geq |b|$.

9. $a \vdots b$ и $|b| > |a| \to a = 0$.

10. $a \vdots b \longleftrightarrow a \vdots |b|$.

11. $a \vdots d$ и $b \vdots c \to ab \vdots dc$.

12. 1 делится *только* на ± 1; если для положительных целых $a, b \quad ab = 1$, то $a = 1$ и $b = 1$.

Целой частью числа $x \in \mathbf{R}$, обозначаемой $\lfloor x \rfloor$, называется наибольшее целое, не превосходящее x: $\lfloor x \rfloor \in \mathbf{Z}$, $\lfloor x \rfloor \le x < \lfloor x \rfloor + 1$. *Пример:* $\lfloor -2,5 \rfloor = -3$, $\lfloor 2,5 \rfloor = 2$.

13. *Деление с остатком в кольце целых чисел.* Для $\forall\, a, b \in \mathbf{Z}$, $b \neq 0$ существуют и единственны числа $q, r \in \mathbf{Z}$ такие, что:

$$\boxed{a = bq + r, \quad 0 \le r < |b|.}$$

q называется неполным частным, r — остатком; если остаток равен нулю, q называется частным.

Наибольшим общим делителем целых чисел $a, b \in \mathbf{Z}$, не равных нулю одновременно, называется наибольшее натуральное число, являющееся делителем a и b. Наибольший общий делитель a и b обозначается далее (a, b).

Наименьшим общим кратным целых чисел $a, b \in \mathbf{Z}$, не равных нулю одновременно, называется наименьшее натуральное число, кратное a и b, наименьшее общее кратное a и b обозначается $[a, b]$.

Взаимно простыми называются числа $a, b \in \mathbf{Z}$, для которых $(a, b) = 1$.

Перечислим основные **свойства наибольшего общего делителя и взаимно простых чисел**.

14. $(a, b) = a \leftrightarrow b \vdots a$.

15. $(a, 0) = |a|$, если $a \neq 0$.

16. $a, b \in \mathbf{N}$, $a = bq + r$, $r, q \in \mathbf{Z}$, $0 \le r < b \to (a, b) = (b, r)$.

Алгоритм Эвклида

Пусть $a, b \in \mathbf{N}$. Не умаляя общности, положим $a > b$. Если $a \vdots b$, то по свойству 14 наибольшего общего делителя $(a, b) = b$. Пусть $a \not\vdots b$. Разделим a на b с остатком, затем разделим

b на остаток и продолжим процесс деления, пока не получим нулевой остаток:

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

Цепочка делений обрывается, т. к. количество положительных целых чисел r_i, величина которых убывает, *конечно*.

17. Наибольший общий делитель a, b равен последнему ненулевому остатку в алгоритме Эвклида.

Нетрудно доказать, что $(a, b) = (|a|, |b|)$. Из единственности неполного частного и остатка при делении с остатком в $\mathbf{Z}$ и из алгоритма Эвклида следует, что н.о.д. двух целых чисел, из которых хотя бы одно отлично от нуля, существует и единственен. Пример отыскания н.о.д. по алгоритму Эвклида рассмотрен в решении задачи 3.4 г).

18. $(am, bm) = m(a, b)$ для $\forall\, m \in \mathbf{N}$.

19. Линейное представление $d = (a, b)$. Существуют и не единственны числа $x, y \in \mathbf{Z}$ такие, что $ax + by = d$. В частности, эти числа $x, y \in \mathbf{Z}$ могут быть найдены из алгоритма Эвклида.

20. $(a, b) = 1 \leftrightarrow \exists\, u, v \in \mathbf{Z} \qquad au + bv = 1.$

21. $(a, b) = d \leftrightarrow \left(\dfrac{a}{d}, \dfrac{b}{d}\right) = 1.$

22. $(a, b) = 1 \rightarrow \forall\, c \in \mathbf{Z} \qquad (ac, b) = (c, b).$

23. $\begin{array}{l} (a_1, b) = 1, \\ (a_2, b) = 1 \end{array} \rightarrow (a_1 a_2, b) = 1.$

Это свойство обобщается на числа $a_1, a_2, \ldots, a_k$, взаимно простые с b: $(a_1 a_2 \ldots a_k, b) = 1$.

24. $(a, b) = 1 \to (a^n, b^m) = 1, \quad m, n \in \mathbf{N}$.

25. $(a, c) = 1$ и $ab \vdots c \to b \vdots c$.

Число $a \in \mathbf{N}$, $a > 1$ называется **простым**, если все натуральные делители a исчерпываются 1 и a.

26. Любое натуральное число, большее 1, имеет делитель, являющийся простым числом.

27. *Множество простых чисел бесконечно* (теорема Эвклида).

28. Любое натуральное число a либо взаимно просто с простым числом p, либо делится на p.

29. Если произведение нескольких натуральных чисел делится на простое число p, то по крайней мере одно из них делится на p.

Каноническое представление целых чисел

Любое натуральное число $a > 1$ можно представить в виде произведения простых чисел $a = p_1 p_2 \ldots p_k$, и это представление единственно с точностью до порядка следования простых сомножителей.

30. Любое натуральное число a имеет единственное каноническое представление

$$a = p_1^{\alpha_1} \ldots p_k^{\alpha_k}, \qquad \alpha_i \in \mathbf{N},$$

$p_1, \ldots, p_k$ — различные простые числа.

31. Канонические представления любых целых чисел $a, b \in \mathbf{Z}$ можно выразить через одни и те же простые множители, если допустить нулевые показатели и считать $p_i^0 = 1$:

$$a = \pm p_1^{\alpha_1} \ldots p_k^{\alpha_k}, \quad b = \pm p_1^{\beta_1} \ldots p_k^{\beta_k}.$$

Единственности такого представления нет.

32. Натуральное число q является делителем натурального числа a тогда и только тогда, когда в каноническое представление числа q входят только простые множители, содержащиеся в каноническом представлении числа a, степени которых не превышают соответствующих степеней в разложении числа a.

Пусть натуральные числа a и b имеют канонические представления $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, $b = p_1^{\beta_1} \dots p_k^{\beta_k}$, $p_1, \dots, p_k$ — простые числа; $\alpha_1, \dots, \alpha_k$, $\beta_1, \dots, \beta_k$ — целые неотрицательные числа. Тогда для наибольшего общего делителя (a, b) и для наименьшего общего кратного $[a, b]$ имеют место представления

$$\boxed{d = (a, b) = p_1^{\delta_1} \dots p_k^{\delta_k}, \qquad \delta_i = \min(\alpha_i, \beta_i),}$$

$$\boxed{m = [a, b] = p_1^{\gamma_1} \dots p_k^{\gamma_k}, \qquad \gamma_i = \max(\alpha_i, \beta_i),}$$

и выполняется равенство

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

Чтобы найти $[a, b]$, не раскладывая числа a и b на простые множители, достаточно найти (a, b) по алгоритму Эвклида и воспользоваться этим равенством.

ЗАДАЧИ К § 3

3.1. Доказать тождества:

а) $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \dots + b^{n-1})$ для любых $n \in \mathbf{N}$;

б) $a^n + b^n = (a + b)(a^{n-1} - a^{n-2}b + \dots + b^{n-1})$ только для нечетных $n \in \mathbf{N}$;

в) $a^n - b^n = (a + b)(a^{n-1} - a^{n-2}b + \dots - b^{n-1})$ только для четных $n \in \mathbf{N}$.

В правых частях этих тождеств выражение во вторых скобках содержит n слагаемых, причем в последних двух тождествах знаки слагаемых чередуются, например:

$$a^7 + b^7 = (a + b)(a^6 - a^5b + a^4b^2 - a^3b^3 + a^2b^4 - ab^5 + b^6);$$

$$a^8 - b^8 = (a+b)(a^7 - a^6b + a^5b^2 - a^4b^3 + a^3b^4 - a^2b^5 + ab^6 - b^7).$$

3.2. Дано: $a \vdots b$, $a \vdots c$, $(b, c) = 1$. Доказать: $a \vdots bc$.

3.3. Пусть $(a, b, c, d, n, m \in \mathbf{N})$. Доказать:

а) $a \vdots b \to a^n \vdots b^n$;

б) $a^n \vdots (a - b) \to b^n \vdots (a - b)$;

в) $(3^{26} + 2^{13}) \vdots 11$;

г) $(3^{11} + 2^{22}) \vdots 7$;

д) $(ab + cd) \vdots (a + c) \to (ad + bc) \vdots (a + c)$;

е) $(n^3 + 5n) \vdots 6 \ \forall n \in \mathbf{N}$;

ж) $(11m + 7n) \vdots 13 \to (m + 3n) \vdots 13$;

з) $(n^5 - n) \vdots 30$.

3.4. Найти, пользуясь алгоритмом Эвклида, наибольший общий делитель и его линейное представление для целых чисел a и b:

а) $a = 493,\ b = 221$;

б) $a = 117,\ b = 92$;

в) $a = 391,\ b = 253$;

г) $a = 843,\ b = 321$.

3.5. Доказать, что решение уравнения $ax+by = c$ $(a, b, c \in \in \mathbf{Z})$ в целых числах возможно тогда и только тогда, когда $c \vdots (a, b)$.

3.6. Доказать, что k делится на $(a, a+k)$.

3.7. Доказать, что при $(a,b)=1$ выполняется:

а) $(a+b, a)=1$;

б) $(a+b, ab)=1$.

3.8. Дано, что уравнение $x^n+a_1x^{n-1}+\ldots+a_n=0$ $(n\in\mathbf{N}$, $a_1,\ldots,a_n\in\mathbf{Z})$ имеет рациональный корень x_*. Доказать: x_* — целое число.

3.9. Доказать: $\left(\frac{a^m-1}{a-1}, a-1\right)=(a-1, m)$, $a, m\in\mathbf{N}$, $a>1$.

3.10. Доказать, что число натуральных делителей числа n $(n\in\mathbf{N})$ не превосходит $2\sqrt{n}$. Оценить величину n, если n имеет 10^5 делителей.

3.11. Доказать, что существует бесконечно много простых чисел вида:

а) $3q+2$;

б) $4q+3$;

в) $6q+5$, $q\in\mathbf{Z}$.

3.12. Доказать, что при $n>2$ произведение всех простых чисел, не превосходящих n, больше n.

3.13. Доказать: $p_{n+1}<p_1p_2\ldots p_n$; $p_1, p_2, \ldots, p_{n+1}$ — первые простые числа.

3.14. Доказать: $p_{n+1}<2^{2^n}$ при $n\in\mathbf{N}$; $p_1, p_2, \ldots, p_{n+1}$ — первые простые числа.

3.15. Доказать, что между числами n и $n!$ есть, по крайней мере, одно простое число $(n\in\mathbf{N}$, $n>2)$.

3.16. Дано: $a \in \mathbf{N}$, $a \neq 1$, a — наименьшее из чисел взаимно простых с каждым из чисел $1, 2, \ldots, n$. Доказать: a — простое число.

3.17. Доказать, что $n^4 + 4$ — составное число ($n \in \mathbf{N}$, $n > 1$).

3.18. Доказать, что среди 1000 следующих друг за другом чисел натурального ряда может не оказаться ни одного простого числа.

3.19. Дано: $(a^n - 1)$ — простое число. Доказать: $a = 2$ и n — простое. (Простые числа вида $(2^p - 1)$ называются числами Мерсенна.)

3.20. Дано: $(a^n + 1)$ — простое число. Доказать: $n = 2^k$, $k \in \mathbf{N}$. (Простые числа вида $(2^{2^k} + 1)$ называются числами Ферма.)

3.21. Обозначим, как принято выше, $[a, b]$ — наименьшее общее кратное чисел a и b.

а) Найти $[a, b]$ для целых a, b задачи 3.4.

б) Доказать: $(a + b, [a, b]) = (a, b)$.

3.22. Доказать, что целое положительное число a является квадратом некоторого целого числа c тогда и только тогда, когда степень каждого простого множителя в каноническом разложении числа a четная. Обобщить этот результат, а именно доказать, что целое число a является n-й степенью целого числа c тогда и только тогда, когда степень каждого простого множителя в каноническом разложении числа a кратна n.

3.23. Дано: $(a, b) = 1$ и $ab = c^2$. Доказать: $\exists\ m, n \in \mathbf{N}$ такие, что $a = m^2$, $b = n^2$ $(a, b, c \in \mathbf{N})$.

3.24. Доказать: $a^n \vdots b^n \to a \vdots b$ $(a, b, n \in \mathbf{N})$.

3.25. Дано: $(n, m) = 1$, $x^n = y^m$ $(x, y, n, m \in \mathbf{N})$. Доказать: $\exists\, t \in \mathbf{N}$ такое, что $x = t^m$, $y = t^n$.

3.26. Доказать, что квадрат любого простого числа p $(p > 3)$ при делении на 24 дает остаток 1.

3.27. Доказать, что остаток от деления простого числа p на 30 есть либо 1, либо простое число.

3.28. Дано: числа p, $2p + 1$ простые и $p > 3$. Доказать: число $4p + 1$ является составным.

3.29. Обозначим $\lfloor \alpha \rfloor$ — целую часть вещественного числа α. Доказать: $\lfloor \alpha + \beta \rfloor \geq \lfloor \alpha \rfloor + \lfloor \beta \rfloor$, $\alpha, \beta \in \mathbf{R}$.

3.30. Доказать, что показатель γ, с которым простое число p входит в каноническое разложение числа $k!$, равен

$$\gamma = \left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{p^2} \right\rfloor + \ldots + \left\lfloor \frac{k}{p^s} \right\rfloor, \quad p^{s+1} > k \geq p^s.$$

3.31. Чему равно число нулей, которыми оканчивается число 100!?

3.32. Доказать, что произведение $(n + 1)(n + 2) \ldots (n + k)$ подряд идущих k чисел натурального ряда делится на $k!$.

3.33. Доказать, не прибегая к соображениям комбинаторики, что число сочетаний

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

является целым $(0 \leq k \leq n,\ (k, n \in \mathbf{N}),\ 0! = 1)$.

3.34. Доказать, что число

$$S = \frac{1}{2} + \ldots + \frac{1}{n}, \quad n > 1$$

не является целым $(n \in \mathbf{N})$.

РЕШЕНИЯ И ОТВЕТЫ К ЗАДАЧАМ § 3

3.1. Доказать тождества:

а) $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \ldots + b^{n-1})$ для любых $n \in \mathbf{N}$;

б) $a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + \ldots + b^{n-1})$ только для нечетных $n \in \mathbf{N}$;

в) $a^n - b^n = (a+b)(a^{n-1} - a^{n-2}b + \ldots - b^{n-1})$ только для четных $n \in \mathbf{N}$.

Доказательство. Все эти тождества проверяются непосредственно.

3.2. Дано: $a \vdots b$, $a \vdots c$, $(b, c) = 1$. Доказать: $a \vdots bc$.

Доказательство. Домножим линейное разложение $bu + cv = 1$ на число a и учтем, что $abu \vdots bc$ и $acv \vdots bc$, т. к. $a \vdots c \to ab \vdots bc \to abu \vdots bc$ и $a \vdots b \to ac \vdots bc \to acv \vdots bc$.

3.3. Пусть $(a, b, c, d, n, m \in \mathbf{N})$. Доказать:

а) $a \vdots b \to a^n \vdots b^n$.

Доказательство. $a \vdots b \to a = qb \to a^n = q^n b^n \to a^n \vdots b^n$.

б) $a^n \vdots (a-b) \to b^n \vdots (a-b)$.

Доказательство. $a^n - (a^n - b^n) = b^n$. Оба слагаемых в левой части делятся на $(a-b)$, относительно первого слагаемого это дано, для второго — следует из задачи 3.1 а). По свойству 5 отношения делимости их разность, т. е. b^n, тоже делится на $(a-b)$.

в) $(3^{26} + 2^{13}) \vdots 11$.

Доказательство. Достаточно воспользоваться тождеством задачи 3.1 б) и учесть $3^2 + 2 = 11$.

г) $(3^{11} + 2^{22}) \vdots 7$. Доказывается аналогично в).

д) $(ab + cd) \vdots (a + c) \to (ad + bc) \vdots (a + c)$.

Доказательство. $((ab+cd)+(ad+bc)) = b(a+c)+d(a+c) = (b+d)(a+c) \to \vdots\,(a+c)$. Далее достаточно воспользоваться свойством 5 отношения делимости.

Задачи е) и з) доказываются методом математической индукции. Рассмотрим, например, доказательство

з) $(n^5 - n) \vdots 30$.

Для $n = 2 \to 2^5 - 2 = 30 \to (2^5 - 2) \vdots 30$. Допустим $(n^5 - n) \vdots 30$. Докажем, что $(n+1)^5 - (n+1) \vdots 30$. Воспользуемся биномом Ньютона (§ 4), перегруппируем слагаемые и запишем

$$(n+1)^5 - (n+1) = (n^5 - n) + 5(n^4 + 2n^3 + 2n^2 + n).$$

Первое слагаемое в правой части этого равенства делится на 30 в силу индукционного предположения. Чтобы доказать, что на 30 делится второе слагаемое, достаточно доказать, что оно делится на 5 (что очевидно) и на 6. Поскольку числа 5 и 6 взаимно просты, отсюда будет следовать, что второе слагаемое делится на 30 (задача 3.2). Воспользуемся очевидным разложением $(n^4+2n^3+2n^2+n) = n(n+1)(n^2+n+1)$, из которого непосредственно следует, что второе слагаемое делится на 2, т. к. для любого натурального n одно из чисел n или $n+1$ является четным. Докажем, что $n(n+1)(n^2+n+1)$ делится на 3. Число n при делении на 3 может иметь остаток либо 0, либо 1, либо 2. Если остаток 0, на 3 делится n, если остаток 1, т. е. $n = 3q+1$, на 3 делится (n^2+n+1); если остаток 2, на 3 делится $(n+1)$. Таким образом, при любом n величина $n(n+1)(n^2+n+1)$ делится на 3. Числа 2, 3 взаимно просты, следовательно, $n(n+1)(n^2+n+1)$ должно делиться на их произведение, т. е. на 6.

ж) $(11m + 7n) \vdots 13 \to (m + 3n) \vdots 13$.

Доказательство. Воспользуемся равенством

$$(11m + 7n) + 2(m + 3n) = 13(m + n),$$

из которого в соответствии со свойством 5 отношения делимости следует, что $2(m+3n)$ делится на 13, поскольку и правая часть, и первое слагаемое левой части делятся на 13. Из условия $2(m+3n) \vdots 13$ в соответствии с п. 25 следует, что $(m+3n) \vdots 13$, т. к., очевидно, $(2,13)=1$.

3.4. Найти, пользуясь алгоритмом Эвклида, наибольший общий делитель и его линейное представление для целых чисел a и b:

а) $a=493,\ b=221$;

б) $a=117,\ b=92$;

в) $a=391,\ b=253$;

г) $a=843,\ b=321$.

Рассмотрим, например, *решение задачи г)*. Выполним, следуя алгоритму Эвклида, последовательные деления с остатком; (a,b) равен последнему ненулевому остатку (п. 17).

1) $843 = 321 \cdot 2 + 201$,
2) $321 = 201 \cdot 1 + 120$,
3) $201 = 120 \cdot 1 + 81$,
4) $120 = 81 \cdot 1 + 39$,
5) $81 = 39 \cdot 2 + \boxed{3}$,
6) $39 = 3 \cdot 13$.

843	321
642	2
321	201
201	1
201	120
120	1
120	81
81	1
81	39
78	2
39	3
39	13
0	

$$a=843, \quad b=321,$$
$$d=(a,b)=3.$$

Чтобы найти линейное представление d, т. е. целые u, v, такие что

$$d=au+bv,$$

выразим остатки, идя снизу вверх в равенствах 5)–1):

$$\begin{aligned} 3 = d &= 81 - 2 \cdot 39 \quad (5),\\ 39 &= 120 - 81 \quad (4),\\ 81 &= 201 - 120 \quad (3),\\ 120 &= b - 201 \quad (2),\\ 201 &= a - 2b \quad (1). \end{aligned}$$

Из (4), (3) $\rightarrow$

$$39 = b - 201 - 201 + b - 201 = 2b - 3 \cdot 201 = 2b - 3(a - 2b).$$

Из (3), (2), (1) $\rightarrow$

$$81 = a - 2b - b + a - 2b = 2a - 5b.$$

Из (5) $\rightarrow$

$$d = 2a - 5b - 2(2b - 3(a - 2b)) = 8a - 21b;$$

$$3 = d = 8 \cdot 843 - 21 \cdot 321 \rightarrow \ u = 8, \quad v = -21.$$

Задачи а)–в) решить самостоятельно.

Ответ: а) $d = 17$; б) $d = 1$; в) $d = 23$.

3.5. Доказать, что решение уравнения $ax+by = c$ $(a, b, c \in \in \mathbf{Z})$ в целых числах возможно тогда и только тогда, когда $c \vdots (a, b)$.

Доказательство. Пусть $(a, b) = d \rightarrow c = ax + by = dq_1x + + dq_2y$ $(q_1, q_2 \in \mathbf{Z}) \rightarrow c \vdots d$; пусть $c \vdots d \rightarrow c = qd$ $(q \in \mathbf{Z})$, для d существует линейное представление $d = au + bv$ $(u, v \in \mathbf{Z}) \rightarrow \rightarrow c = q(au + bv) = ax + by$ $(x, y \in \mathbf{Z})$.

3.6. Доказать, что k делится на $(a, a + k)$.

Указание: $k = (a+k)-a$, далее воспользоваться свойством 5 отношения делимости.

3.7. Доказать, что при $(a, b) = 1$ выполняется:
а) $(a + b, a) = 1$;

б) $(a+b, ab) = 1$.

Доказательство.

а) Числа взаимно просты тогда и только тогда, когда их канонические разложения не содержат одинаковых простых множителей в степенях, отличных от нуля. Пусть $a+b$ и a не взаимно просты, т. е. пусть они имеют общий простой множитель p. Тогда $b = (a+b) - a = pq$ $(q \in \mathbf{Z})$, т. е. a и b имеют общий простой множитель p, следовательно, a и b не взаимно просты. Полученное противоречие доказывает задачу.

б) Аналогично задаче а) доказывается, что $(a+b, b) = 1$ при $(a, b) = 1$. Из условий $(a+b, a) = 1$ и $(a+b, b) = 1$ в соответствии с п. 23 следует: $(a+b, ab) = 1$.

3.8. Дано, что уравнение $x^n + a_1 x^{n-1} + \ldots + a_n = 0$ $(n \in \mathbf{N},\ a_1, \ldots, a_n \in \mathbf{Z})$ имеет рациональный корень x_*. Доказать: x_* — целое число.

Доказательство.

$x_* = \frac{a}{b}$; a, b — взаимно простые числа. Подставим $x_* = \frac{a}{b}$ в уравнение и домножим все члены на b^n, полученное равенство позволяет написать

$$a^n = bc, \quad c \in \mathbf{Z}. \tag{1}$$

Из взаимной простоты a, b и свойства 24 следует:

$$(a, b) = 1 \to (a^n, b) = 1. \tag{2}$$

Из (1), (2) $\to b = 1$, т. е. $x_* = a \in \mathbf{Z}$.

3.9. Доказать: $\left(\frac{a^m-1}{a-1}, a-1\right) = (a-1, m)$, $a, m \in \mathbf{N}$, $a > 1$.

Доказательство.

Пусть $d = \left(\frac{a^m-1}{a-1}, a-1\right) \to a-1 \vdots d$. Докажем, что d — общий делитель $a-1, m$. Для доказательства того, что $m \vdots d$,

воспользуемся тождеством

$$\frac{a^m-1}{a-1} = 1 + a + \ldots + a^{m-1} = \\ = (a^{m-1}-1) + (a^{m-2}-1) + \ldots + (a-1) + m. \quad (3)$$

Чтобы доказать, что d — наибольший общий делитель чисел $a-1$ и m, предположим противное. Пусть $\exists\ \delta > d$ и δ — общий делитель $a-1, m$; из (3) $\to \frac{a^m-1}{a-1} : \delta \to \delta$ — общий делитель $\frac{a^m-1}{a-1}, a-1$ и $\delta > d$, что противоречит определению d. Это противоречие доказывает, что d — наибольший общий делитель $a-1$ и m, т. е. $d = \left(\frac{a^m-1}{a-1}, a-1\right) = (a-1, m)$.

3.10. Доказать, что число натуральных делителей числа n $(n \in \mathbf{N})$ не превосходит $2\sqrt{n}$. Оценить величину n, если n имеет 10^5 делителей.

Доказательство. Пусть $a_1, \ldots, a_m$ — делители числа n, число которых равно m. Они разбиваются на пары $n = a_1 a_m$, $n = a_2 a_{m-1}, \ldots$ В каждой паре один из сомножителей $\le \sqrt{n}$, следовательно, s (число различных пар) удовлетворяет неравенству $s \le \sqrt{n} \to m = 2s \le 2\sqrt{n}$. При $m = 10^5$ из неравенства $2\sqrt{n} \ge 10^5 \to n \ge 25 \cdot 10^8$.

3.11. Доказать, что существует бесконечно много простых чисел вида:

а) $3q + 2$;

б) $4q + 3$;

в) $6q + 5$, $q \in \mathbf{Z}$.

Рассмотрим доказательство утверждения а). Остаток при делении отличного от 3 простого числа p на 3 равен либо 1, либо 2, следовательно, либо $p = 3q + 1$, либо $p = 3\tilde{q} + 2 = 3\hat{q} - 1$, $q, \tilde{q}, \hat{q} \in \mathbf{Z}$. Непосредственно проверяется, что при перемножении чисел вида $3q + 1$ не может получиться число вида $3q - 1$.

Докажем 3.11. а) от противного. Пусть таких чисел конечное число и $p_1, p_2, \ldots, p_k$ — все простые числа вида $3q-1$. Рассмотрим $Q = 3p_1p_2 \ldots p_k - 1$. Каждое натуральное число имеет делителем простое число, т. е. $\exists\ p_*$ — простое и $Q \vdots p_*$. Простое число p_* не может совпадать ни с одним из $p_1, \ldots, p_k$, т. к. в этом случае получили бы разложение 1 на множители, отличные от 1, что невозможно. С другой стороны, все простые числа, входящие в каноническое разложение Q, не могут иметь вид $3q+1$, т. к. число Q имеет вид $3q-1$, следовательно, среди простых делителей Q должен быть хотя бы один, имеющий вид $3q-1$ и не совпадающий ни с одним из $p_1, \ldots, p_k$. Противоречие доказывает бесконечность множества простых чисел вида $3q-1$.

Задачи б), в) доказываются по аналогичной схеме.

3.12. Доказать, что при $n > 2$ произведение всех простых чисел, не превосходящих n, больше n.

Доказательство.

Пусть $p_1, \ldots, p_k$ — все простые числа, не превосходящие n. Рассмотрим $Q = p_1 \ldots p_k - 1$. Существует простой делитель p_* числа Q, и он не может совпадать ни с одним из $p_1, \ldots, p_k$ (см. задачу 3.11), следовательно, $p_* > n$, $Q \geq p_* > n \to$ $\to Q > n \to p_1 \ldots p_k > n$.

3.13. Доказать: $p_{n+1} < p_1p_2 \ldots p_n$; $p_1, p_2, \ldots, p_{n+1}$ — первые простые числа.

Доказательство.

$Q = p_1p_2 \ldots p_n - 1$; $\exists$ простое p_* такое, что $Q \vdots p_* \to$ (см. задачу 3.12) $\to p_{n+1} \leq p_* \leq Q \to p_{n+1} < p_1 \ldots p_n$.

3.14. Доказать: $p_{n+1} < 2^{2^n}$ при $n \in \mathbf{N}$; $p_1, p_2, \ldots, p_{n+1}$ — первые простые числа.

Доказательство. Докажем методом математической индукции. База: при $n = 2$ $p_3 < 2^{2^2}$, т. к. $(5 < 16)$.

Индукционное предположение: для любого простого числа p_k $(k < n+1)$ $p_k < 2^{2^{k-1}}$. Индукционный переход: из задачи 3.13 $\to$ $p_{n+1} < p_1 p_2 \dots p_n < 2^{(1+2+2^2+\dots+2^{n-1})} \to p_{n+1} < \frac{2^{2^n}}{2} \to$ $\to p_{n+1} < 2^{2^n}$.

3.15. Доказать, что между числами n и $n!$ есть, по крайней мере, одно простое число ($n \in \mathbf{N}$, $n > 2$).

Доказательство. Рассмотрим число $Q = p_1 \dots p_k - 1$, где $p_1, \dots, p_k$ — первые простые числа, не превосходящие n. В решении задачи 3.12 доказано, что существует простой делитель p_* числа Q, удовлетворяющий неравенству $n < p_* \le Q$. С другой стороны, очевидно неравенство $Q = p_1 \dots p_k - 1 < n!$, т. к. $n!$ можно представить $n! = p_1 \dots p_k q$, где q — произведение всех составных чисел от 1 до n; в результате приходим к неравенству

$$n < p_* \le Q < n!,$$

из которого следует доказываемое утверждение.

3.16. Дано: $a \in \mathbf{N}$, $a \ne 1$, a — наименьшее из чисел взаимно простых с каждым из чисел $1, 2, \dots, n$. Доказать: a — простое число.

Доказательство. Дано:

$$(a, 1) = (a, 2) = \dots = (a, n) = 1. \qquad (*)$$

Из равенств $(*)$ следует $a > n$ и для $\forall\, k \le n$ $a \not\vdots k$. Допустим, что число a составное, т. е. $a = bc$, $b < a$, $c < a$.

Тогда для $\forall\, k \le n$ $bc \not\vdots k$, следовательно,

$$\forall\, k \le n \qquad b \not\vdots k \text{ и } \quad c \not\vdots k. \qquad (**)$$

Все делители числа $m \le n$ находятся среди чисел $1, 2, \dots, m$. Поэтому из $(**)$ следует, что число b и число c взаимно простые с каждым из чисел $1, 2, \dots, n$. Поскольку $b < a$, $c < a$, приходим к противоречию с тем, что a — наименьшее из чисел с указанным свойством. Следовательно, предположение, что a составное, неверно, т. е. a — простое число.

3.17. Доказать, что $n^4 + 4$ — составное число ($n \in \mathbf{N}$, $n > 1$).

Доказательство. Разложим $n^4 + 4$ на множители.

Пусть $n = m+1$, $n^4+4 = (m+1)^4+4 = m^4+4m^3+6m^2+$ $+4m+1+4 =$ (представим $1+4 = 6-1$) $= (m^4-1)+(4m^3+$ $+4m)+(6m^2+6) = (m^2+1)((m^2-1)+4m+6) \Rightarrow n^4+4 =$ $= ((n-1)^2+1)((n-1)^2+4(n-1)+5)$.

3.18. Доказать, что среди 1000 следующих друг за другом чисел натурального ряда может не оказаться ни одного простого числа.

Доказательство.

Среди чисел вида $n!+2, n!+3, \ldots, n!+n$ нет ни одного простого числа. Поэтому для решения задачи достаточно положить $n = 1000$. Тогда в последовательности $n!+2, n!+$ $+3, \ldots, n!+1001$, содержащей 1000 следующих друг за другом чисел натурального ряда, нет ни одного простого числа.

3.19. Дано: $(a^n - 1)$ — простое число. Доказать: $a = 2$ и n — простое. (Простые числа вида $(2^p - 1)$ называются числами Мерсенна.)

Доказательство.

Из тождества 3.1 а) следует, что a^n-1 не может быть простым ни при $a \neq 2$, ни при $n = ms$, т. к.

$a^n - 1 = (a-1)(\ldots)$ $\qquad$ $2^{ms} - 1 = (2^m - 1)(\ldots)$.

3.20. Дано: $(a^n + 1)$ — простое число. Доказать: $n = 2^k$, $k \in \mathbf{N}$. (Простые числа вида $(2^{2^k} + 1)$ называются числами Ферма.)

Доказательство.

Для нечетных n выполняется тождество 3.1 б): $a^n + 1 =$ $= (a+1)(\ldots)$. Следовательно, при простом $a^n + 1$ число n должно быть четным: $a^{2m} + 1 = (a^2)^m + 1$. По тем же

причинам m должно быть четным и т. д. $\to n = 2m$, $m = 2s$, $s = 2t \ldots \to n = 2^k$.

3.21. Обозначим, как принято выше, $[a, b]$ — наименьшее общее кратное чисел a и b.

а) Найти $[a, b]$ для целых a, b задачи 3.4.

б) Доказать: $(a + b, [a, b]) = (a, b)$.

Докажем пункт б).
$d = (a, b) \to \left(\frac{a}{d}, \frac{b}{d}\right) = 1$. Из формулы $[a, b] = \frac{ab}{(a,b)} \to$

$$\to (a + b, [a, b]) = \left(a + b, \frac{ab}{d}\right) = \\ = \left(d\left(\frac{a}{d} + \frac{b}{d}\right), d\left(\frac{a}{d} \cdot \frac{b}{d}\right)\right) = d(\tilde{a} + \tilde{b}, \tilde{a}\tilde{b}),$$

где

$$\tilde{a} = \left(\frac{a}{d}\right),\ \tilde{b} = \left(\frac{b}{d}\right) \text{ и } (\tilde{a}, \tilde{b}) = 1.$$

Из задачи 3.7 б) следует, что $(\tilde{a} + \tilde{b}, \tilde{a}\tilde{b}) = 1$ при $(\tilde{a}, \tilde{b}) = 1$. Таким образом, $(a + b, [a, b]) = d$.

3.22. Доказать, что целое положительное число a является квадратом некоторого целого числа c тогда и только тогда, когда степень каждого простого множителя в каноническом разложении числа a четная. Обобщить этот результат, а именно доказать, что целое число a является n-й степенью целого числа c тогда и только тогда, когда степень каждого простого множителя в каноническом разложении числа a кратна n.

Доказательство. Пусть $a = c^2$; из канонического разложения c находим: $c = p_1^{\alpha_1} \ldots p_k^{\alpha_k} \to a = p_1^{2\alpha_1} \ldots p_k^{2\alpha_k}$. Пусть $a = p_1^{2\alpha_1} \ldots p_k^{2\alpha_k} \to a = (p_1^{\alpha_1} \ldots p_k^{\alpha_k})^2$. Аналогично доказывается для $a = c^n$.

3.23. Дано: $(a, b) = 1$ и $ab = c^2$. Доказать: $\exists\ m, n \in \mathbf{N}$ такие, что $a = m^2$, $b = n^2$ $(a, b, c \in \mathbf{N})$.

Доказательство.
Канонические разложения взаимно простых чисел не содержат одинаковых простых множителей в ненулевых степенях, т. е. $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, $b = q_1^{\beta_1} \dots q_s^{\beta_s}$, $ab = p_1^{\alpha_1} \dots q_s^{\beta_s}$, $p_i \neq q_j$, $i = 1, \dots, k$, $j = 1, \dots, s$. Из задачи 3.23 $\to \alpha_1 = 2\tilde{\alpha}_1, \dots, \beta_s = 2\tilde{\beta}_s \to a = (p_1^{\tilde{\alpha}_1} \dots p_k^{\tilde{\alpha}_k})^2$, $b = (q_1^{\tilde{\beta}_1} \dots q_s^{\tilde{\beta}_s})^2$.

3.24. Доказать: $a^n \vdots b^n \to a \vdots b$ $(a, b, n \in \mathbf{N})$.

Доказательство.
Представим a в каноническом виде: $a = p_1^{\alpha_1} \dots p_k^{\alpha_k} \to a^n = p_1^{n\alpha_1} \dots p_k^{n\alpha_k}$; $a^n \vdots b^n \to b^n = p_1^{\delta_1} \dots p_k^{\delta_k}$, $\delta_i \leq n\alpha_i$. Из обобщения задачи 3.23 $\to \delta_i = n\mu_i$. Приходим к неравенству $n\mu_i \leq n\alpha_i \to \mu_i \leq \alpha_i \to a \vdots b$.

3.25. Дано: $(n, m) = 1$, $x^n = y^m$ $(x, y, n, m \in \mathbf{N})$. Доказать: $\exists\, t \in \mathbf{N}$ такое, что $x = t^m$, $y = t^n$.

Доказательство.
Пусть $x = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, $y = q_1^{\gamma_1} \dots q_s^{\gamma_s}$. Из равенства $x^n = y^m$ следует, что в канонические разложения x и y входят одни и те же простые числа, т. е. с учетом обобщения задачи 3.23 имеем: $x^n = p_1^{n\alpha_1} \dots p_k^{n\alpha_k}$, $y^m = p_1^{m\beta_1} \dots p_k^{m\beta_k}$.

$x^n = y^m \to n\alpha_i = m\beta_i$, $i = 1, \dots, k \to n\alpha_i \vdots m \to \alpha_i \vdots m$,

т. к.

$$(m, n) = 1 \to \alpha_i = ms_i,\ s_i \in \mathbf{N} \to \beta_i = ns_i \to$$
$$\to x = p_1^{\alpha_1} \dots p_k^{\alpha_k} = p_1^{ms_1} \dots p_k^{ms_k} = (p_1^{s_1} \dots p_k^{s_k})^m;$$
$$y = p_1^{\beta_1} \dots p_k^{\beta_k} = p_1^{ns_1} \dots p_k^{ns_k} = (p_1^{s_1} \dots p_k^{s_k})^n.$$

Следовательно, $t = p_1^{s_1} \dots p_k^{s_k}$.

3.26. Доказать, что квадрат любого простого числа p $(p > 3)$ при делении на 24 дает остаток 1.

Доказательство.
Любое простое число p можно представить либо в виде $6m+1$, либо в виде $6\tilde{m}+5 = 6\hat{m}-1$ $(m, \tilde{m}, \hat{m} \in \mathbf{Z})$ (*но не любое такое число простое*), т. к. остатки 0, 2, 3, 4 при делении числа

p на 6 невозможны в силу простоты p. Пусть $p = 6m + 1$, $p^2 = 12m(3m+1)+1$. Одно из чисел m, $3m+1$ четно $\to p^2 = = 12\cdot 2\cdot q+1$. Аналогично рассматривается случай $p = 6m-1$.

3.28. Дано: числа p, $2p + 1$ простые и $p > 3$. Доказать: число $4p + 1$ является составным.

Докажем от противного. Пусть $4p + 1$ — простое; при делении на 3 простого числа остаток может быть либо 1, либо $2 \to 4p + 1 = 3k + 1$, либо $4p + 1 = 3k - 1$, $k \in \mathbf{Z} \ \to 4p = 3k$, либо $2(2p + 1) = 3k$. Оба равенства невозможны, т. к. $4p \not\vdots 3$ и $2(2p+1) \not\vdots 3$ в силу заданной простоты p и $2p+1$. Следовательно, $4p + 1$ — составное.

3.30. Доказать, что показатель γ, с которым простое число p входит в каноническое разложение числа $k!$, равен

$$\gamma = \left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{p^2} \right\rfloor + \ldots + \left\lfloor \frac{k}{p^s} \right\rfloor, \qquad p^{s+1} > k \geq p^s.$$

Доказательство основано на подсчете количества множителей числа $n! = 2 \cdot 3 \cdot 4 \ldots (n-1) \cdot n$, которые делятся на заданное p. Докажем, что среди подряд идущих чисел $1, 2, \ldots, n$ количество чисел, делящихся на p, равно $\left\lfloor \frac{n}{p} \right\rfloor$. Целая часть $\lfloor \alpha \rfloor$ числа α определяется неравенствами

$$\lfloor \alpha \rfloor \leq \alpha < \lfloor \alpha \rfloor + 1. \qquad (*)$$

Выпишем ряд чисел, не превосходящих n и кратных p $(p \leq n)$: $p, 2p, \ldots, sp \leq n$. Число s определено неравенством $sp \leq n < (s+1)p$, из которого после деления на p и сопоставления с неравенством $(*)$ следует: $s = \left\lfloor \frac{n}{p} \right\rfloor$. Из доказанного заключаем, что $\left\lfloor \frac{n}{p} \right\rfloor$ множителей числа $n!$ делятся на p, среди них могут быть и такие, которые делятся на p^2, p^3 и т. д.; $\left\lfloor \frac{n}{p^2} \right\rfloor$ множителей числа $n!$ делятся на p^2. Найдем число A_1 множителей в $n!$, которые делятся на p и при этом не делятся

на p^2:

$$A_1 = \left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor .$$

Аналогично находится A_2 — число множителей в $n!$, которые делятся на p^2 и не делятся на p^3:

$$A_2 = \left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor , \quad \text{и т. д.}$$

Найдем суммарный показатель γ, с которым простое число p входит в $n!$:

$$n! = qp^{A_1}(p^2)^{A_2}(p^3)^{A_3}\ldots , \qquad q \not\vdots p.$$

$$\to n! = qp^{\gamma}, \qquad \gamma = A_1 + 2A_2 + 3A_3 + \ldots =$$

$$= \left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor + 2\left\lfloor \frac{n}{p^2} \right\rfloor - 2\left\lfloor \frac{n}{p^3} \right\rfloor + 3\left\lfloor \frac{n}{p^3} \right\rfloor - 3\left\lfloor \frac{n}{p^4} \right\rfloor + \ldots =$$

$$= \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots + \left\lfloor \frac{n}{p^s} \right\rfloor , \qquad p^s \le n.$$

Этот ряд обрывается, т. к. $\left\lfloor \frac{n}{p^{s+1}} \right\rfloor = 0$ при $p^{s+1} > n$.

Следствие: $n! = p_1^{\alpha_1}\ldots p_s^{\alpha_s}$, $p_s \le n$, $\alpha_i = \left\lfloor \frac{n}{p_i} \right\rfloor + \left\lfloor \frac{n}{p_i^2} \right\rfloor + \ldots$

3.31. Чему равно число нулей, которыми оканчивается число 100!?

Указание: найти количество сомножителей числа $10{=}2{\cdot}5$ в разложении 100!, воспользовавшись результатом предыдущей задачи.

Ответ: 100! оканчивается 24 нулями.

3.32. Доказать, что произведение $(n+1)(n+2)\ldots(n+k)$ подряд идущих k чисел натурального ряда делится на $k!$.

Доказательство.
Представим $Q = (n+1)(n+2)\dots(n+k)$ в виде $Q = \frac{(n+k)!}{n!}$. Чтобы доказать, что $Q \vdots k!$, достаточно показать, что показатель β каждого простого числа p в каноническом разложении Q не меньше показателя λ, с которым p входит в каноническое разложение $k!$. Докажем неравенство $\beta \geq \lambda$, используя результат задачи 3.30.

Простое число p входит в каноническое разложение $(n+k)!$ с показателем α, равным

$$\alpha = \left\lfloor \frac{n+k}{p} \right\rfloor + \left\lfloor \frac{n+k}{p^2} \right\rfloor + \dots$$

Простое число p входит в каноническое разложение $n!$ с показателем ξ, равным

$$\xi = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \dots$$

Простое число p входит в каноническое разложение $\frac{(n+k)!}{n!}$ с показателем β, равным $(\alpha - \xi)$, т. е.

$$\beta = \left\lfloor \frac{n+k}{p} \right\rfloor - \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n+k}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor + \dots$$

Простое число p входит в каноническое разложение $k!$ с показателем λ, равным

$$\lambda = \left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{p^2} \right\rfloor + \dots$$

Доказываемое неравенство $\beta \geq \lambda$ или $\beta - \lambda \geq 0$ следует из этих представлений для β и λ, если учесть результат задачи 3.29.

3.33. Доказать, не прибегая к соображениям комбинаторики, что число сочетаний $C_n^k = \frac{n!}{k!(n-k)!}$ является целым $(0 \leq k \leq n,\ (k, n \in \mathbf{N}),\ 0! = 1)$.

Указание: воспользоваться тождеством
$n! = n(n-1)\dots(n-(k-1))(n-k)!$ и результатом задачи 3.32.

3.34. Доказать, что число $S = \frac{1}{2} + \dots + \frac{1}{n}$, $n > 1$ не является целым ($n \in \mathbf{N}$).

Доказательство. Пусть k — наибольшее целое, удовлетворяющее условию $2^k \leq n$; пусть P — произведение всех нечетных чисел, не превосходящих n. Число $2^{k-1}PS$ не является целым. Действительно, оно представляется суммой, в которой все слагаемые, кроме $\frac{2^{k-1}P}{2^k}$, являются целыми числами. Из того, что $2^{k-1}PS$ не целое, следует, что не целым является число S, так как $2^{k-1}P$ — целое число.

§ 4. ЭЛЕМЕНТЫ КОМБИНАТОРИКИ

Комбинаторика — теория конечных множеств. В основе комбинаторных расчетов лежит

правило умножения: *последовательность k действий, первое из которых выполняется n_1 способами, второе — n_2 способами и т. д., выполняется $n_1 \cdot n_2 \cdot \ldots \cdot n_k$ способами.*

Выборка — набор элементов, взятых из множества A. Каждый элемент из A может входить в данную выборку не более одного раза, т. е. либо войти, либо не войти, но не может повторяться в выборке. Одна выборка может отличаться от другой выборки из множества A

1) самими элементами;
2) только расположением элементов;
3) и элементами, и их расположением.

Перестановкой n элементов множества A, состоящего из n элементов, называется выборка, включающая все n элементов, отличающаяся от другой перестановки *только расположением* элементов.

Сочетанием из n элементов по k элементов называется выборка из n элементов множества A, содержащая k элементов $(0 \leq k \leq n)$, отличающаяся от другого сочетания из n по k *только самими элементами* (порядок расположения выбранных k элементов не важен).

Размещением из n элементов по k элементов называется выборка из n элементов множества A, содержащая k элементов $(0 \leq k \leq n)$, отличающаяся от другого размещения из n по k *либо самими элементами, либо их расположением*.

Количество P_n различных перестановок n элементов равно $P_n = n!$; количество A_n^k различных размещений из n элементов по k элементов в каждом размещении $(0 \le k \le n)$ равно

$$A_n^k = \frac{n!}{(n-k)!} = n(n-1)\dots(n-(k-1));$$

количество C_n^k различных сочетаний из n элементов по k элементов в каждом сочетании $(0 \le k \le n)$ равно

$$C_n^k = \frac{A_n^k}{P_n} = \frac{n!}{k!(n-k)!}.$$

Простейшие свойства числа сочетаний C_n^k

1. $C_n^0 = C_n^n = 1$.
2. $C_n^k = C_n^{n-k}$.
3. $C_n^{k+1} + C_n^k = C_{n+1}^{k+1}$.

Бином Ньютона

Для вещественных a, b и натурального n имеет место равенство, называемое **биномом Ньютона**,

$$(a+b)^n = C_n^0 a^n b^0 + C_n^1 a^{n-1} b^1 + \dots$$
$$\dots + C_n^n a^0 b^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k.$$

Для небольших величин n вычисление биномиальных коэффициентов удобно проводить с помощью следующей схемы, называемой треугольником Паскаля.

Треугольник Паскаля

Рассмотрим треугольную таблицу чисел:

						1								$n=0$
					1		1							$n=1$
				1		2		1						$n=2$
			1		3		3		1					$n=3$
		1		4		6		4		1				$n=4$
	1		5		10		10		5		1			$n=5$
1		6		15		20		15		6		1		$n=6$
↑		↑		↑		↑		↑		↑		↑		
$k=0$		1		2		3		4		5		6		

Каждая следующая строка этого треугольника расширена по сравнению с предыдущей строкой на одну позицию влево и на одну позицию вправо. Она всегда начинается и заканчивается числом 1, в ней под всеми числами предыдущей строки стоят пробелы, на каждом другом месте (кроме первого и последнего) стоит число, равное сумме двух ближайших чисел из предыдущей строки. Если строки этого треугольника нумеровать сверху вниз, начиная с 0, и в каждой строке столбцы, содержащие цифры, нумеровать слева направо, начиная с 0, то число, стоящее в k-м столбце n-й строки, будет равно C_n^k

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

Это доказывается индукцией с использованием свойства 3 числа сочетаний, которое позволяет записать $C_{n+1}^k = C_n^k + C_n^{k-1}$. Рассмотренная треугольная таблица чисел называется *треугольником Паскаля*. В n-й строке треугольника Паскаля стоят биномиальные коэффициенты разложения $(a+b)^n$.

ЗАДАЧИ К § 4

4.1. Доказать тождество:

$$C_n^0 + C_n^2 + \ldots + C_n^n = 2^{n-1}, \quad \text{если } n \text{ — четное.}$$

4.2. Доказать, что для нечетного n сумма биномиальных коэффициентов, стоящих на четных местах, равна сумме биномиальных коэффициентов, стоящих на нечетных местах.

4.3. Доказать тождества:

1) $A_{n-1}^m = A_n^m - mA_{n-1}^{m-1}$;

2) $kC_n^k = nC_{n-1}^{k-1}$;

3) $C_n^k = \dfrac{(k+1)}{(n+1)}\, C_{n+1}^{k+1}$;

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

4.4. Доказать тождество

$$C_n^k C_m^0 + C_n^{k-1} C_m^1 + \ldots + C_n^0 C_m^k = C_{m+n}^k.$$

4.5. Доказать, что сумма квадратов биномиальных коэффициентов равна C_{2n}^n:

$$(C_n^0)^2 + (C_n^1)^2 + \ldots + (C_n^n)^2 = C_{2n}^n.$$

4.6. Доказать: $P_1 + 2P_2 + \ldots + nP_n = (n+1)! - 1$.

4.7. Доказать: $C_n^1 + 2C_n^2 + \ldots + nC_n^n = n2^{n-1}$.

4.8. Доказать:

$$C_n^0 + \frac{1}{2}\, C_n^1 + \ldots + \frac{1}{n+1}\, C_n^n = \frac{2^{n+1} - 1}{n+1}\,.$$

4.9. В разложении $\left(\sqrt[3]{3} + \sqrt{2}\right)^5$ найти слагаемые, не содержащие иррациональности.

4.10. Найти коэффициент при x^7 в многочлене

$$f(x) = (1+x)^7 + (1+x)^8 + (1+x)^9 + (1+x)^{10},$$

не раскрывая скобок.

4.11. Найти наибольшее слагаемое в разложении по биному Ньютона

$$\left(\frac{9}{10}+\frac{1}{10}\right)^{50}.$$

4.12. Найти наибольшее слагаемое в разложении по биному Ньютона

$$\left(\frac{1}{2}+\frac{1}{2}\right)^{100}.$$

4.13. Сколько существует различных отображений $f : A \to B$, если $|A| = m$, $|B| = n$?

4.14. Сколько существует различных инъективных отображений $f : A \to B$ и различных биективных отображений $f : A \to A$, если $|A| = m$, $|B| = n$?

4.15. Пусть в азбуке Морзе любая буква состоит из 5 символов, а каждый символ может быть либо точкой, либо тире. Сколько различных букв можно составить?

4.16. Сколько различных натуральных делителей имеет число

$$m = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k} \ ?$$

(p_i — простые числа, α_i — натуральные числа, $i = 1, \ldots, k$.)

4.17. У студента 10 друзей. Каждый день он приглашает некоторых из них в гости. Сколько дней он может делать это так, чтобы компания ни разу не повторилась?

4.18. Сколькими способами можно упорядочить множество $\{1, 2, \ldots, 2n\}$ так, чтобы каждое четное число имело четный номер?

4.19. В группе учится 2 студентки и 8 студентов. В команду должно входить 4 человека, среди которых должна быть хотя бы одна студентка. Сколько таких различных команд можно составить?

4.20. Сколько различных четырехзначных чисел можно составить из цифр $0, 1, 2, 3$, если цифры в записи числа не могут повторяться?

4.21. Сколько существует пятизначных чисел, которые читаются одинаково слева направо и справа налево?

4.22. Сколько существует пятизначных четных чисел?

4.23. Сколько существует перестановок из n элементов, в которых два выделенных элемента не стоят рядом?

4.24. В ящике находится m белых шаров и n черных. Сколькими способами можно выбрать r шаров, из которых белых будет k штук? (Шары каждого цвета различны между собой, например, пронумерованы.)

4.25. В колоде 36 карт, из них 4 туза. Сколькими способами можно сдать 6 карт так, чтобы среди них было 2 туза?

4.26. Сколько различных четырехзначных чисел можно составить из цифр $0, 1, 2, 3, 4, 5, 6, 7$ так, чтобы в записи каждого числа содержалась цифра 1, при условии, что цифры в записи числа не могут повторяться?

4.27. Сколько различных четырехзначных чисел можно составить из цифр $0, 1, 2, 3, 4, 5, 6, 7$ так, чтобы в записи каждого числа содержалась одна цифра 1?

4.28. Сколькими способами можно расставить n книг на двух полках, считая, что порядок расположения книг существенен?

4.29. Домашняя библиотека состоит из 7 книг. Сколько существует способов их прочтения, если имеет значение последовательность прочтения?

4.30. Сколько существует пятизначных чисел, у которых две цифры совпадают, а остальные различны?

РЕШЕНИЯ И ОТВЕТЫ К ЗАДАЧАМ § 4

4.1. Доказать тождество

$$C_n^0 + C_n^2 + \ldots + C_n^n = 2^{n-1}, \quad \text{если } n \text{ — четное.}$$

Доказательство. Запишем бином Ньютона для $a = 1$, $b = 1$ и для $a = 1$, $b = -1$, затем сложим полученные равенства:

$$2^n = C_n^0 + C_n^1 + \ldots + C_n^{n-1} + C_n^n,$$
$$0 = C_n^0 - C_n^1 + \ldots - C_n^{n-1} + C_n^n.$$

4.2. Доказать, что для нечетного n сумма биномиальных коэффициентов, стоящих на четных местах, равна сумме биномиальных коэффициентов, стоящих на нечетных местах.

Доказательство. Запишем бином Ньютона для $a = 1$, $b = -1$ при нечетном n:

$$0 = C_n^0 - C_n^1 + C_n^2 - C_n^3 + \ldots + C_n^{n-1} - C_n^n.$$

Из этого равенства следует:

$$C_n^1 + C_n^3 + \ldots + C_n^n = C_n^0 + C_n^2 + \ldots + C_n^{n-1},$$

т. е. сумма биномиальных коэффициентов, стоящих на нечетных местах, равна сумме биномиальных коэффициентов, стоящих на четных местах.

4.3. Доказать тождества:

1) $A_{n-1}^m = A_n^m - mA_{n-1}^{m-1}$;

2) $kC_n^k = nC_{n-1}^{k-1}$;

3) $C_n^k = \dfrac{(k+1)}{(n+1)} C_{n+1}^{k+1}$;

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

Доказательство. Тождества 1)–3) проверяются непосредственно, 4) следует из бинома Ньютона при $a = 1$, $b = -1$.

4.4. Доказать:

$$C_n^k C_m^0 + C_n^{k-1} C_m^1 + \ldots + C_n^0 C_m^k = C_{m+n}^k. \qquad (*)$$

Доказательство. Воспользуемся равенством $(1+x)^m(1+x)^n = (1+x)^{n+m}$. Разложим по биному Ньютона скобки в левой и правой частях, приравняем коэффициенты при одинаковых степенях x. Искомая сумма $C_n^k C_m^0 + C_n^{k-1} C_m^1 + \ldots + C_n^0 C_m^k$ является коэффициентом при x^k в левой части, соответствующий коэффициент в правой части равен C_{m+n}^k, что доказывает $(*)$.

4.5. Доказать, что сумма квадратов биномиальных коэффициентов равна C_{2n}^n:

$$(C_n^0)^2 + (C_n^1)^2 + \ldots + (C_n^n)^2 = C_{2n}^n.$$

Указание: воспользоваться равенством $(*)$ задачи 4.4, положить $m = k = n$ и учесть свойство биномиальных коэффициентов $C_n^k = C_n^{n-k}$.

4.6. Доказать: $P_1 + 2P_2 + \ldots + nP_n = (n+1)! - 1$.

Доказательство. Прибавим и отнимем в левой части доказываемого тождества сумму $(P_1 + P_2 + \ldots + P_n)$, сгруппируем слагаемые и учтем очевидное тождество $P_k + kP_k = P_{k+1}$:

$$\underbrace{P_1 + P_1}_{P_2} + \underbrace{P_2 + 2P_2}_{P_3} + \ldots + \underbrace{P_n + nP_n}_{P_{n+1}} - P_1 - P_2 - \ldots - P_n =$$

$$= P_{n+1} - P_1 = (n+1)! - 1.$$

4.7. Доказать: $C_n^1 + 2C_n^2 + \ldots + nC_n^n = n2^{n-1}$.

Доказательство.
Тождество 2) задачи 4.3 позволяет записать

$$1C_n^1 = nC_{n-1}^0, \quad 2C_n^2 = nC_{n-1}^1,$$

$$3C_n^3 = nC_{n-1}^2, \ldots, nC_n^n = nC_{n-1}^{n-1},$$

складывая эти равенства, находим

$$C_n^1 + 2C_n^2 + \ldots + nC_n^n = \\ = n(C_{n-1}^0 + C_{n-1}^1 + \ldots + C_{n-1}^{n-1}) = n2^{n-1}.$$

4.8. Доказать: $C_n^0 + \frac{1}{2}C_n^1 + \ldots + \frac{1}{n+1}C_n^n = \frac{2^{n+1}-1}{n+1}$.

Указание: воспользоваться тождеством 3) задачи 4.3.

4.9. В разложении $\left(\sqrt[3]{3} + \sqrt{2}\right)^5$ найти слагаемые, не содержащие иррациональности.

Решение. В разложении k-е слагаемое имеет вид

$$C_5^k 3^{\frac{5-k}{3}} 2^{\frac{k}{2}}.$$

Это выражение рациональное, если $\frac{5-k}{3}$, $\frac{k}{2}$ — целые числа. Нетрудно убедиться в том, что из всех возможных $k = 0, \ldots, 5$ этому условию удовлетворяет только $k = 2$, следовательно, искомое слагаемое равно $C_5^2 \cdot 3 \cdot 2 = 60$.

4.10. Найти коэффициент при x^7 в многочлене

$$f(x) = (1+x)^7 + (1+x)^8 + (1+x)^9 + (1+x)^{10},$$

не раскрывая скобок.

Решение. Добавим к многочлену $f(x)$ многочлен $g(x)$, равный

$$g(x) = 1 + (1+x) + (1+x)^2 + \ldots + (1+x)^6.$$

Очевидно, коэффициенты при x^7 в многочленах $f(x)$ и $f(x) + g(x)$ совпадают. По формуле суммы геометрической прогрессии многочлен $f(x) + g(x)$ можно представить в виде

$$g(x) + f(x) = \frac{(1+x)^{10} - 1}{(1+x) - 1} = \\ = \frac{C_{10}^1 x + \ldots + C_{10}^8 x^8 + \ldots + C_{10}^{10} x^{10}}{x}.$$

Коэффициент при x^7 в многочлене $g(x)+f(x)$ равен: $C_{10}^8 = 45$.

4.11. Найти наибольшее слагаемое в разложении по биному Ньютона

$$\left(\frac{9}{10}+\frac{1}{10}\right)^{50}.$$

Решение. Обозначим $\alpha = \frac{9}{10}$, $\beta = \frac{1}{10}$, разложим $(\alpha+\beta)^{50}$ по биному Ньютона и найдем отношение $(k+1)$-го слагаемого к k-му:

$$\frac{C_{50}^k \alpha^{(50-k)}\beta^k}{C_{50}^{k-1}\alpha^{50-(k-1)}\beta^{(k-1)}} = \frac{(50-(k-1))\beta}{k\alpha} = \frac{51-k}{9k}.$$

Величина слагаемых растет, пока это отношение больше единицы, и убывает, если она меньше единицы. Таким образом, при $k \le 5$ величина слагаемых растет, при $k > 5$ — убывает. Наибольшую величину имеет слагаемое при $k = 5$, оно равно $C_{50}^5 \alpha^{45}\beta^5$.

4.12. Найти наибольшее слагаемое в разложении по биному Ньютона

$$\left(\frac{1}{2}+\frac{1}{2}\right)^{100}.$$

Ответ: $C_{100}^{50}\left(\frac{1}{2}\right)^{100}$.

4.13. Сколько существует различных отображений $f : A \to B$, если $|A| = m$, $|B| = n$?

Решение. Рассмотрим последовательность m действий, первое из которых состоит в отображении первого элемента множества A на множество B, его можно выполнить n способами; второе действие состоит в отображении второго элемента множества A, это действие также можно выполнить n способами, т. к. не требуется инъективности отображений; и т. д. По правилу умножения последовательность этих m действий может быть выполнена $\underbrace{n \cdot n \cdot \ldots \cdot n}_{m} = n^m$ способами,

т. е. существует $N = n^m$ различных отображений из множества A на множество B.

4.14. Сколько существует различных инъективных отображений $f : A \to B$ и различных биективных отображений $f : A \to A$, если $|A| = m$, $|B| = n$?

Решение. Из определений отображения и его инъективности следует, что для существования инъективных отображений в этой задаче должно выполняться неравенство $n \geq m$. Первый элемент множества A можно отобразить n способами. Второй элемент — $(n-1)$ способами, т. к. один элемент множества B «занят», а инъективное отображение не может «склеивать», и т. д. Общее число N различных инъективных отображений по правилу умножения равно

$$N = n(n-1)\dots(n-(m-1)) = A_n^m.$$

Отсюда следует, что число биективных отображений $f : A \to \to A$ из конечного множества A $(|A| = m)$ в себя равно $m \cdot (m-1) \cdot \ldots \cdot 2 \cdot 1 = m! = P_m$.

4.15. Пусть в азбуке Морзе любая буква состоит из 5 символов, а каждый символ может быть либо точкой, либо тире. Сколько различных букв можно образовать?

Решение. Надо сосчитать число вариантов заполнения пяти ячеек при том, что каждая ячейка может быть заполнена двумя способами. По правилу умножения это число равно $2^5 = 32$.

4.16. Сколько различных натуральных делителей имеет число $m = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$? (p_i — простые числа, α_i — натуральные числа, $i = 1, \dots, k$.)

Решение. Как известно (п. 32 § 3), натуральное число d является делителем натурального числа $m = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ тогда и только тогда, когда оно имеет вид $d = p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k}$, $0 \leq \leq \beta_i \leq \alpha_i$.

Число делителей, являющихся степенью p_1, равно (α_1+1),..., число делителей, являющихся степенью p_i, равно (α_i+1). По правилу умножения число различных натуральных делителей числа m равно произведению $(\alpha_1+1)(\alpha_2+1)\cdot\ldots\cdot(\alpha_k+1)$.

4.17. У студента 10 друзей. Каждый день он приглашает некоторых из них в гости. Сколько дней он может делать это так, чтобы компания ни разу не повторилась?

Решение. Число различных компаний, состоящих из k друзей ($0 \le k \le 10$), равно числу сочетаний C_{10}^k. Следовательно, общее число различных компаний равно

$$C_{10}^0 + C_{10}^1 + \ldots + C_{10}^{10} = 2^{10} = 1024,$$

т. е. в течении 1024 дней студент может приглашать друзей в гости так, чтобы компания ни разу не повторилась.

4.18. Сколькими способами можно упорядочить множество $\{1, 2, \ldots, 2n\}$ так, чтобы каждое четное число имело четный номер?

Решение. В этой последовательности всего n четных чисел и столько же четных номеров, следовательно, четные числа можно расставить на четных местах $n!$ способами. Оставшиеся n нечетных чисел на оставшихся n местах с нечетными номерами можно также расставить $n!$ способами. По правилу умножения общее число способов упорядочить множество $\{1, 2, \ldots, 2n\}$ так, чтобы каждое четное число имело четный номер, равно их произведению, т. е. $(n!)^2$.

4.19. В группе учатся 2 студентки и 8 студентов. В команду должно входить 4 человека, среди которых должна быть хотя бы одна студентка. Сколько различных таких команд можно составить?

Решение. Найдем количество различных команд с одной студенткой. С первой студенткой возможно C_8^3 команд и

столько же со второй студенткой, т. е. всего $2C_8^3$. Количество различных команд, в которые входят обе студентки, равно C_8^2. Общее количество команд из 4 человек, среди которых есть хотя бы одна студентка, равно $2 \cdot C_8^3 + C_8^2 = 140$.

4.20. Сколько различных четырехзначных чисел можно составить из цифр $0, 1, 2, 3$, если цифры в записи числа не могут повторяться?

Решение. Первое место четырехзначного числа можно заполнить тремя способами с учетом того, что число не может начинаться с нуля. На второе место можно поставить любую из четырех цифр, кроме той, что стоит на первом месте. На третье место можно поставить любую из четырех цифр, кроме тех, что стоят на первом и втором местах, на четвертое место можно поставить одну единственную оставшуюся цифру. Таким образом, существует N различных четырехзначных чисел $N = 3 \cdot 3 \cdot 2 \cdot 1 = 18$.

4.21. Сколько существует пятизначных чисел, которые читаются одинаково слева направо и справа налево?

Ответ: 900.

4.22. Сколько существует пятизначных четных чисел?

Ответ: 45000.

4.23. Сколько существует перестановок из n элементов, в которых два выделенных элемента не стоят рядом?

Решение. Сначала найдем число перестановок из n элементов, в которых выделенные элементы a, b стоят рядом. Расположим их ab. Существует $(n-1)!$ перестановок, в которых a, b стоят рядом в такой последовательности. Столько же перестановок, в которых они стоят рядом в последовательности ba. Всего существует $n!$ различных перестановок из n элементов,

следовательно, число искомых перестановок равно

$$n! - 2(n-1)!\,.$$

4.24. В ящике находится m белых шаров и n черных. Сколькими способами можно выбрать r шаров, из которых белых будет k штук? (Шары каждого цвета различны между собой, например, пронумерованы.)

Решение. k белых шаров из m белых шаров можно выбрать C_m^k способами. Оставшиеся $(r-k)$ черных шаров из n черных шаров можно выбрать $C_n^{(r-k)}$ способами. Каждому способу выбора k белых шаров соответствует $C_n^{(r-k)}$ способов выбора черных. По правилу умножения общее число различных требуемых выборок равно произведению $C_m^k \cdot C_n^{(r-k)}$.

4.25. В колоде 36 карт, из них 4 туза. Сколькими способами можно сдать 6 карт так, чтобы среди них было 2 туза?

Указание: воспользоваться схемой решения предыдущей задачи.

Ответ: $C_4^2 \cdot C_{32}^4$.

4.26. Сколько различных четырехзначных чисел можно составить из цифр $0, 1, 2, 3, 4, 5, 6, 7$ так, чтобы в записи каждого числа содержалась цифра 1, при условии, что цифры в записи числа не могут повторяться?

Решение. Существует $7 \cdot 6 \cdot 5$ вариантов четырехзначных чисел, у которых цифра 1 стоит на первом месте и которые удовлетворяют требованиям задачи. Существует $6 \cdot 6 \cdot 5$ вариантов четырехзначных чисел, у которых цифра 1 стоит на 2 месте. (Здесь и далее учтено, что цифра 0 не может стоять на первом месте, поэтому из восьми заданных цифр только 6 могут быть расположены на первом месте с учетом того, что цифра 1 стоит на втором месте и она не может повторяться.) Существует $6 \cdot 6 \cdot 5$ вариантов записи четырехзначных чисел,

удовлетворяющих требованиям задачи, у которых цифра 1 стоит на третьем месте, и столько же вариантов, когда цифра 1 стоит на четвертом месте. Общее количество различных четырехзначных чисел, удовлетворяющих требованиям задачи, равно

$$7 \cdot 6 \cdot 5 + 3 \cdot (6 \cdot 6 \cdot 5) = 750.$$

4.27. Сколько различных четырехзначных чисел можно составить из цифр $0, 1, 2, 3, 4, 5, 6, 7$ так, чтобы в записи каждого числа содержалась одна цифра 1?

Решение. Эта задача отличается от рассмотренной выше задачи 4.26 только тем, что цифры, кроме 1, могут в записи числа повторяться. Рассуждая аналогично приведенному выше решению, находим

$$7 \cdot 7 \cdot 7 + 3 \cdot (6 \cdot 7 \cdot 7) = 1225.$$

4.28. Сколькими способами можно расставить n книг на двух полках, считая, что порядок расположения книг существенен?

Решение. Первый вариант расстановки книг: ноль книг на первой полке и n книг — на второй. n книг на второй полке можно расставить $n!$ способами. Таким образом, первый вариант реализуется $n!$ способами.

Второй вариант расстановки книг: одна книга на первой полке и $n-1$ книга — на второй. Одну книгу можно выбрать из n книг A_n^1 способами. Оставшиеся $n-1$ книг на второй полке можно расставить $(n-1)!$ способами. Таким образом, второй вариант реализуется $A_n^1(n-1)!$ способами.

k-ый вариант: k книг на первой полке и $n-k$ книги — на второй. k книги, с учетом порядка их расположения, можно выбрать из n книг A_n^k способами. Оставшиеся $n-k$ книг на второй полке можно расставить $(n-k)!$ способами. Таким образом, k-ый вариант реализуется $A_n^k(n-k)!$ способами.

В последнем, $n+1$ варианте, все n книг будут стоять на первой полке, его можно осуществить $n!$ способами.

Таким образом, общее число S способов расстановки n книг на двух полках равно

$$S = A_n^0(n-0)! + A_n^1(n-1)! + \ldots + A_n^k(n-k)! + \ldots + A_n^n(n-n)!.$$

С учетом очевидного равенства

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

находим: $S = (n+1)!$.

Ответ: общее число способов расстановки n книг на двух полках равно $(n+1)!$.

4.29. Домашняя библиотека состоит из 7 книг. Сколько существует способов их прочтения, если имеет значение последовательность прочтения?

Решение. Существует A_7^k способов прочесть k книг из заданных 7, считая, что последовательность прочтения существенна. Здесь k принимает значения от 0 до 7. Следовательно, суммарное количество S способов прочтения 7 книг равно

$$S = A_7^0 + A_7^1 + \ldots + A_7^7 = 13700.$$

Ответ: существует 13700 способов прочтения 7 книг, если имеет значение последовательность прочтения.

4.30. Сколько существует пятизначных чисел, у которых две цифры совпадают, а остальные различны?

Решение. Существует 4 варианта, в которых у пятизначных чисел совпадающая цифра стоит на 1 месте. Есть 9 способов заполнить первое место и, одновременно, совпадающее с ним место, т. к. число не может начинаться цифрой 0. Оставшиеся три места можно заполнить 9, 8 и 7 способами соответственно, с учетом того, что цифры не могут повторяться.

Суммарное число n_1 пятизначных чисел, у которых совпадающая цифра стоит на 1 месте, по правилу умножения равно

$$n_1 = 4 \cdot (9 \cdot 9 \cdot 8 \cdot 7).$$

Существует 3 варианта, в которых у пятизначных чисел совпадающая цифра стоит на 2 месте (вариант ее совпадения с первой цифрой учтен в n_1). Суммарное число n_2 таких пятизначных чисел по правилу умножения равно

$$n_2 = 3 \cdot (9 \cdot 9 \cdot 8 \cdot 7).$$

Существует 2 варианта, в которых у пятизначных чисел совпадающая цифра стоит на 3 месте (варианты ее совпадения с первой и второй цифрами учтены в n_1 и n_2). Суммарное число n_3 таких пятизначных чисел по правилу умножения равно

$$n_3 = 2 \cdot (9 \cdot 9 \cdot 8 \cdot 7).$$

Существует один вариант, в котором у пятизначных чисел совпадающая цифра стоит на 4 и 5 местах. Количество таких чисел равно

$$n_4 = 1 \cdot (9 \cdot 9 \cdot 8 \cdot 7).$$

Таким образом, общее число n пятизначных чисел, у которых две цифры совпадают, а остальные различны, равно

$$n = (4 + 3 + 2 + 1) \cdot (9 \cdot 9 \cdot 8 \cdot 7) = 45360.$$

Ответ: существует 45360 пятизначных чисел, у которых две цифры совпадают, а остальные различны.

ОСНОВНАЯ ЛИТЕРАТУРА

1. *Виноградов И. М.* Основы теории чисел. М., 1949. 180 с.
2. *Кострикин А. И.* Введение в алгебру. М., 1994. 320 с.
3. *Фаддеев Д. К.* Лекции по алгебре. М., 1984. 416 с.
4. *Кострикин А. И.* Сборник задач по алгебре. М., 2001. 464 с.
5. *Фаддеев Д. К., Соминский И. С.* Сборник задач по высшей алгебре. М., 1977. 288 с.
6. *Проскуряков И. В.* Сборник задач по линейной алгебре. М., 2000. 384 с.

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

1. *Бухштаб А. А.* Теория чисел. М., 1966. 385 с.
2. *Галочкин А. И., Нестеренко Ю. В., Шидловский А. Б.* Введение в теорию чисел. М., 1984. 147 с.
3. *Шмидт Р. А.* Алгебра. Часть I. СПб., 2008. 360 с.
4. *Утешев А. Ю., Черкасов Т. М., Шапошников А. А.* Цифры и шифры. СПб., 2001. 130 с.
5. *Курбатова Г. И.* Начала теории чисел. Лекции и практика решения задач. СПб., 2005. 93 с.

6. *Утешев А. Ю.* Высшая алгебра. Раздел I. СПб., 2006. 184 с.
7. *Гашков С. Б., Чубариков В. Н.* Арифметика. Алгоритмы. Сложность вычислений. М., 2000. 320 с.
8. *Дыбкова Е. В., Жуков И. Б., Семёнов А. А., Шмидт Р. А.* Задачи по алгебре. Основы теории групп. СПб., 1996. 32 с.
9. *Генералов А. И., Дыбкова Е. В., Жуков И. Б. и др.* Задачи по алгебре. Основы теории колец. СПб., 1998. 48 с.

ОБОЗНАЧЕНИЯ

$f \stackrel{d}{=} g$	—	f по определению равно g;
$p \to q$	—	из p следует q;
$p \Leftrightarrow q$ или $p \leftrightarrow q$	—	из p следует q и из q следует p;
$\exists$	—	существует;
$\mathbf{N}$	—	множество натуральных чисел;
$\mathbf{Z}$	—	множество целых чисел;
$\mathbf{R}$	—	множество вещественных чисел;
R_+	—	множество положительных вещественных чисел;
$\mathbf{Q}$	—	множество рациональных чисел;
$Z_{\text{ч}}$	—	множество четных чисел;
$\oslash$	—	пустое множество;
$B \subset A$	—	множество B содержится в множестве A;
$A \cup B$	—	объединение множеств A и B;
$A \cap B$	—	пересечение множеств A и B;
$A \setminus B$	—	разность множеств A и B;
U	—	универсальное множество;
$\overline{A}$	—	дополнение множества A до универсального множества;
$A \times B$	—	декартовое произведение множеств A и B;
$A \triangle B$	—	симметрическая разность множеств A и B;
Card A или $\lvert A \rvert$	—	мощность множества A;

$A/_\sim$	—	фактормножество множества A по отношению эквивалентности $(\sim)$;
$f : X \to Y$	—	отображение из множества X на множество Y;
$\mathrm{Id}_X : X \to X$	—	тождественное отображение на множестве X;
$\mathrm{Im}\, f$	—	образ отображения $f : X \to Y$;
$f^{-1} : Y \to X$	—	обратное отображение к отображению $f : X \to Y$;
$f^{-1}(y)$	—	прообраз элемента y;
$(G,\ +)$	—	алгебраическая структура;
$\mathrm{Ker} f$	—	ядро гомоморфизма $f : B \to W$ из группы B в группу W;
2^X	—	множество всех подмножеств множества X;
S_n	—	симметрическая группа;
$\lfloor x \rfloor$	—	целая часть числа $x \in \mathbf{R}$;
$a \vdots b$	—	целое число a делится на целое число b;
$a \nvdots b$	—	целое число a не делится на целое число b;
н.о.д. a и b или (a, b)	—	наибольший общий делитель чисел $a, b \in \mathbf{Z}$;
$[a, b]$	—	наименьшее общее кратное чисел $a, b \in \mathbf{Z}$;
P_n	—	количество различных перестановок n элементов;
A_n^k	—	количество различных размещений из n элементов по k элементов;
C_n^k	—	количество различных сочетаний из n элементов по k элементов.

ОГЛАВЛЕНИЕ

Надежда Николаевна ЕРМОЛАЕВА,
Владимир Александрович КОЗЫНЧЕНКО,
Галина Ибрагимовна КУРБАТОВА

ПРАКТИЧЕСКИЕ ЗАНЯТИЯ ПО АЛГЕБРЕ
ЭЛЕМЕНТЫ ТЕОРИИ МНОЖЕСТВ, ТЕОРИИ ЧИСЕЛ, КОМБИНАТОРИКИ. АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ

Под редакцией Г. И. Курбатовой

Учебное пособие

Верстка *А. Г. Сандомирская*
Выпускающие *Н. В. Черезова, Т. С. Симонова*

ЛР № 065466 от 21.10.97
Гигиенический сертификат 78.01.07.953.П.007216.04.10
от 21.04.2010 г., выдан ЦГСЭН в СПб

Издательство «ЛАНЬ»
lan@lanbook.ru; www.lanbook.com
192029, Санкт-Петербург, Общественный пер., 5.
Тел./факс: (812) 412-29-35, 412-05-97, 412-92-72.
Бесплатный звонок по России: 8-800-700-40-71

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». 192029, Санкт-Петербург, ул. Крупской, 13
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.lanpbl.spb.ru/price.htm

в Москве и в Московской области
«ЛАНЬ-ПРЕСС». 109263, Москва, 7-я ул. Текстильщиков, д. 6/19
тел.: (499) 178-65-85; 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-магазины:
Издательство «Лань»: http://www.lanbook.com
«Сова»: http://www.symplex.ru; «Ozon.ru»: http://www.ozon.ru
«Библион»: http://www.biblion.ru

Подписано в печать 18.02.14.
Бумага офсетная. Гарнитура Школьная. Формат 84×108 $^{1}/_{32}$.
Печать офсетная. Усл. п. л. 5,88. Тираж 1000 экз.

Заказ № .

Отпечатано в полном соответствии
с качеством предоставленных материалов
в ОАО «ИПК “Чувашия”».
428019, г. Чебоксары, пр. И. Яковлева, д. 13.
Тел.: (8352) 56-00-23