Т.Ю. Войтенко
Е.Н. Яковлева

ВВЕДЕНИЕ В АЛГЕБРУ
Задачи и решения

Учебное пособие

ФЛИНТА • НАУКА

ISBN 978-5-9765-2986-1
9 785976 529861

Т.Ю. Войтенко
Е.Н. Яковлева

ВВЕДЕНИЕ В АЛГЕБРУ
Задачи и решения

Учебное пособие

ФЛИНТА • НАУКА

Министерство образования и науки РФ
Федеральное государственное автономное образовательное
учреждение высшего образования
«Сибирский федеральный университет»

Т.Ю. Войтенко
Е.Н. Яковлева

ВВЕДЕНИЕ В АЛГЕБРУ

Задачи и решения

Учебное пособие

Рекомендовано УМО РАЕ по классическому университетскому и техническому образованию в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлениям подготовки: 44.03.05, 44.03.01 — «Педагогическое образование» (Профили подготовки: «Математика и физика», «Информатика», «Информатика и экономика»)

Москва
Издательство «ФЛИНТА»
Издательство «Наука»
2017

УДК 512.5(075.8)
ББК 22.144я73
В65

Войтенко Т.Ю.

В65 Введение в алгебру. Задачи и решения : учеб. пособие / Т.Ю. Войтенко, Е.Н. Яковлева. — М. : ФЛИНТА : Наука, 2017. — 148 с.

ISBN 978-5-9765-2986-1 (ФЛИНТА)
ISBN 978-5-02-039354-7 (Наука)

Учебное пособие по курсу высшей алгебры, изучаемому в первом семестре, охватывает материал следующих разделов: множества и отношения, бинарные алгебраические операции, группы, кольца, поля и комплексные числа. Пособие может быть использовано для первичного ознакомления с изучаемым материалом, для подготовки к практическим занятиям, для закрепления полученных знаний, умений и навыков.

Для студентов различных форм обучения по направлению «Педагогическое образование».

УДК 512.5(075.8)
ББК 22.144я73

ISBN 978-5-9765-2986-1 (ФЛИНТА)
ISBN 978-5-02-039354-7 (Наука)

Содержание

Введение в алгебру
Задачи и решения

Учебное пособие

Книга представляет собой учебное пособие по курсу высшей алгебры, изучаемом в первом семестре, и охватывает материал следующих разделов: множества и отношения, бинарные алгебраические операции, группы, кольца, поля и комплексные числа. Пособие может быть использовано для первичного ознакомления с изучаемым материалом, для подготовки к практическим занятиям, для закрепления полученных знаний, умений и навыков.

Предназначено для студентов различных форм обучения по направлению «Педагогическое образование».

Содержание

Предисловие

Данное учебное пособие содержит материал по теории алгебраических систем, излагаемый, как правило, в первом семестре курса высшей алгебры в педагогических вузах. Материал распределен по следующим разделам: множества и отношения, бинарные алгебраические операции, группы, кольца, поля и комплексные числа.

В начале каждого параграфа кратко сформулированы основные положения соответствующего раздела теории. Далее приведены примеры и задачи с решениями. В заключении параграфа содержатся задачи для самостоятельного решения, которые снабжены указаниями и ответами. Наличие большого числа решенных задач познакомит читателя с приемами и методами решения алгебраических задач.

Пособие подготовлено на основе материалов занятий по алгебре, проводимых авторами в течение многих лет на физико-математическом факультете Лесосибирского педагогического института – филиала Сибирского федерального университета.

При работе над пособием использовалась учебная литература, список которой приведен в конце книги, там же приведен список используемых обозначений и указатель терминов.

Мы искренне благодарны всем преподавателям кафедры алгебры и математической логики Института Математики и фундаментальной информатики СФУ, в общении с которыми сложилось наше представление об алгебре и ее преподавании. Особую благодарность мы хотим выразить профессору В. М. Левчуку за постоянную поддержку и интеллектуальное вдохновение.

Авторы

§ 1. Множества

Множество – одно из основных понятий современной математики. Это понятие принимают за первоначальное и поэтому не определяют через другие. Можно сказать, что множество это совокупность объектов (чисел, точек, функций и т.д.), которая рассматривается как единое целое. Синонимами слова множества являются также слова: семейство, класс.

Произвольные множества в математике обычно обозначают большими латинскими буквами: A, B, C, ...

Об объектах, образующих множество, говорят, что они *принадлежат* этому множеству, или являются его *элементами* (*точками*).

Запись $a \in A$ означает, что объект a есть элемент множества A, или объект a принадлежит множеству A. Если элемент a не принадлежит множеству A, то пишут $a \notin A$. Сам символ $\in$ называют *знаком принадлежности*.

Множество, не содержащее ни одного элемента, называется *пустым множеством* и обозначается через $\emptyset$.

Существует два способа задания множества: непосредственное перечисление всех элементов множества (этот способ пригоден лишь для задания конечного множества), указание характеристического свойства.

Например, если $\mathbb{Z}$ – множество всех целых чисел, то множество $2\mathbb{Z}$ четных целых чисел, т.е. чисел, кратных 2, можно записать как $2\mathbb{Z} = \{z \in \mathbb{Z} \mid z = 2x \text{ для некоторого } x \in \mathbb{Z}\}$.

Говорят, что множество B *включено* в множество A, если каждый элемент множества B является также элементом множества A; обозначается $B \subseteq A$. Другими словами можно сказать, что множество A *содержит* множество B. Сам символ $\subseteq$ называют *знаком включения*. Множество B при этом называют *подмножеством* множества A.

Два множества A и B считают *равными*, если они состоят из одних и тех же элементов; обозначается $A = B$ (если A и B не равны, то пишут соответственно $A \neq B$). Используя отношение включения, определение равенства двух множеств можно записать так

$$A = B \;\Leftrightarrow\; A \subseteq B \;\text{ и }\; B \subseteq A.$$

Различают два вида включения:

1) *строгое включение* $A \subset B$: существует хотя бы один элемент множества B, не принадлежащий множеству A;

2) *нестрогое включение* $A \subseteq B$: не существует ни одного элемента множества B, не принадлежащего множеству A.

Если $A \subset B$, но $A \neq B$ и $A \neq \emptyset$, то A называется *собственным подмножеством* множества B.

Основными операциями над множествами, с помощью которых можно получить из любых двух множеств A и B новые множества, являются:

◇ *объединение*

$$A \cup B = \{x \,|\, x \in A \text{ или } x \in B\};$$

◇ *пересечение*

$$A \cap B = \{x \,|\, x \in A \text{ и } x \in B\};$$

◇ *разность*

$$A \setminus B = \{x \,|\, x \in A \text{ и } x \notin B\}.$$

Если $B \subseteq A$, то разность $A \setminus B$ называется *дополнением множества B до множества A*.

Если все рассматриваемые в ходе какого-либо рассуждения множества являются подмножествами некоторого множества U, то такое множество U называется *универсальным*

множеством. Разность $U \setminus A$ в этом случае называется *дополнением множества* A и обозначается через $\overline{A}$.

Для графического изображения множеств и их свойств часто используются диаграммы Эйлера–Венна. На рис. 1 заштрихованная часть изображает объединение, пересечение и разность множеств A, B.

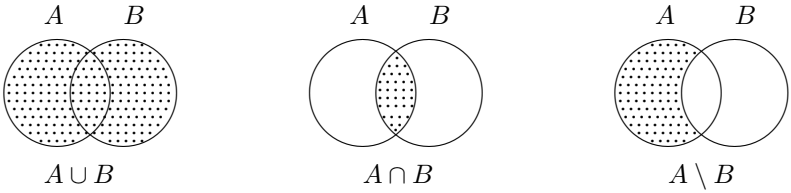


Рис. 1

Примеры решения задач

Задача 1. Доказать, что существует лишь одно множество, не имеющие элементов.

Доказательство. Предположим, что существуют два пустых множества $\emptyset_1$ и $\emptyset_2$, причем $\emptyset_1 \neq \emptyset_2$. Для любого множества A имеем $A \cap \emptyset = \emptyset$. Следовательно, $\emptyset_1 \cap \emptyset_2 = \emptyset_2 = \emptyset_1$. □

Задача 2. Доказать, что $\{\emptyset\} \neq \emptyset$.

Доказательство. Множество $\{\emptyset\}$ состоит из одного элемента $\emptyset$, а пустое множество $\emptyset$ совсем не содержит никаких элементов. □

Задача 3. Существуют ли такие множества A, B и C, что

$$A \cap B \neq \emptyset, \quad A \cap C = \emptyset, \quad (A \cap B) \setminus C = \emptyset?$$

Решение. Так как $A \cap B \neq \emptyset$, то предположим, что элемент $x \in A \cap B$. Тогда $x \in A$ и $A \cap C = \emptyset$, следовательно, $x \notin C$. Отсюда, по определению разности двух множеств, получаем $x \in (A \cap B) \setminus C$ и $(A \cap B) \setminus C \neq \emptyset$, что противоречит условию. Значит, таких множеств A, B и C не существует. □

Задача 4. Доказать, что для любых множеств A, B, C выполняется свойство дистрибутивности объединения относительно пересечения, т.е.

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

Доказательство. Для доказательства этого равенства нам необходимо будет доказать два включения: 1) $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$ и 2) $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.

1) Пусть $x \in A \cup (B \cap C)$. Тогда $x \in A$ или $x \in B \cap C$. Если $x \in A$, то $x \in A \cup B$ и $x \in A \cup C$. Отсюда следует, что $x \in (A \cup B) \cap (A \cup C)$. Если $x \in B \cap C$, то $x \in B$ и $x \in C$, следовательно, $x \in A \cup B$ и $x \in A \cup C$, и значит, $x \in (A \cup B) \cap (A \cup C)$.

Мы доказали, что любого элемента x, из условия $x \in A \cup \cup (B \cap C)$ следует, что $x \in (A \cup B) \cap (A \cup C)$, т.е. мы доказали включение $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.

2) Пусть теперь $x \in (A \cup B) \cap (A \cup C)$. Тогда $x \in A \cup B$ и $x \in A \cup C$. Следовательно, $x \in A$ или $x \in B$ и $x \in A$ или $x \in C$. Откуда получаем, что $x \in A$ или $x \in B \cap C$, и, значит, $x \in A \cup (B \cap C)$.

Таким образом, мы доказали, что любого элемента x, если $x \in (A \cup B) \cap (A \cup C)$, то $x \in A \cup (B \cap C)$, т.е. мы доказали включение $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.

Объединяя включения 1) и 2), имеем $A \cup (B \cap C) = (A \cup \cup B) \cap (A \cup C)$. □

Задача 5. Доказать, что для любых двух множеств A, B

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

Доказательство. Пусть $x \in \overline{A \cup B}$. Тогда $x \notin A \cup B$, и следовательно, $x \notin A$ $x \notin B$. Отсюда следует, что $x \in \overline{A}$ и $x \in \overline{B}$, и, стало быть, $x \in \overline{A} \cap \overline{B}$, т.е. верно включение $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$.

Докажем обратное включение. Пусть $x \in \overline{A} \cap \overline{B}$. Тогда $x \in \overline{A}$ и $x \in \overline{B}$, следовательно, $x \notin A$ и $x \notin B$. Откуда получаем, что $x \notin A \cup B$, и, значит, $x \in \overline{A \cup B}$. Таким образом, имеем включение $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$.

Объединяя два полученных включения, получаем требуемое равенство. □

Упражнения для самостоятельной работы

1.1. Перечислить элементы следующих множеств:

а) $\{x \in \mathbb{N} \mid x < 6\}$;

б) $\{x \in \mathbb{Z} \mid |x| \leq 2\}$;

в) $\{x \in \mathbb{R} \mid x^2 - 3x + 2 = 0\}$;

г) $\{(x, y) \mid x \in \mathbb{Z},\, y \in \mathbb{Z},\, x^2 + y^2 = 1\}$;

д) множество всех чисел от 0 до 30, которые можно представить в виде суммы квадратов двух натуральных чисел.

1.2. Задать множества с помощью характеристического свойства:

а) множество всех нечетных целых чисел;

б) множество всех действительных чисел, модуль которых больше 3;

в) множество всех целых делителей числа 246, по модулю больших 2;

г) множество всех пар рациональных чисел, сумма квадратов которых равна 1;

д) $\{1, 6, 11, 16, 21, 26\}$.

1.3. Равны ли следующие множества:

а) $\{2, 4, 5\}$ и $\{2, 4, 2, 5\}$;

б) $\{1, 2, 5\}$ и $\{\{1\}, \{2\}, \{5\}\}$;

в) $\{1, 3\}$ и $\{\{1, 3\}\}$;

г) $\Big\{x \in \mathbb{Z} \mid x \vdots 4 \text{ и } x \vdots 6\Big\}$ и $\Big\{x \in \mathbb{Z} \mid x \vdots 24\Big\}$;

д) $\big\{x \in \mathbb{R} \bigm| \frac{1}{x-2} < 1\big\}$ и $\{x \in \mathbb{R} \mid x > 3\}$;

е) $\{x \in \mathbb{R} \mid 6 \leq x \leq 5\}$ и $\emptyset$?

1.4. Верны ли следующие включения:

а) $\{x^2 \mid x \in \mathbb{Q}\} \subseteq \{x^4 \mid x \in \mathbb{Q}\}$;

б) $\{4k + 1 \mid k \in \mathbb{Z}\} \subseteq \{2k + 1 \mid k \in \mathbb{Z}\}$;

в) $\{x \in \mathbb{R} \mid x^2 + x + 2 = 0\} \subseteq \emptyset$;

г) $\{(x, y) \in \mathbb{R}^2 \mid x > 0,\, y > 0\} \subseteq \{(x, y) \in \mathbb{R}^2 \mid xy > 0\}$?

1.5. Указать все подмножества множества $\{\{1, 2\}, \{3\}, 1\}$.

1.6. Соединить множества символами $\in$ или $\subseteq$ так, чтобы получилось верное утверждение:

а) 1 и $\mathbb{N}$;

б) $\{1, 2\}$ и $\mathbb{N}$;

в) $\{1, 2\}$ и $\{1, 2, \{1\}, \{2\}\}$;

г) $\{1, 2\}$ и $\{1, 2, \{1, 2\}\}$;

д) $\emptyset$ и $\mathbb{R}$;

е) $\emptyset$ и $\{\emptyset\}$.

1.7. Доказать, что если $A \subseteq B$, $B \subseteq C$ и $C \subseteq A$, то $A = B = C$.

1.8. Найти $A \cup B$, $A \cap B$, $A \setminus B$, $B \setminus A$, $\overline{A}$, $\overline{B}$:

а) $A = \{1, 2, 3\}$, $B = \{2, 3, 4, 5\}$, $U = \{0, 1, \ldots, 9\}$;

б) $A = \{x \mid x$ делится на $2\}$, $B = \{x \mid x$ делится на $3\}$, $U = \mathbb{N}$.

1.9. Изобразите с помощью кругов Эйлера – Венна множеств A, B и C, удовлетворяющих указанному условию:

а) $A \subseteq B$ и $B \subseteq C$;

б) если $A \subseteq A \cap B$;

в) если $A \cup B \subseteq A$;

г) если $A = A \setminus B$.

1.10. Доказать, что $A \cup B = A$ тогда и только тогда, когда $B \subseteq A$.

1.11. Доказать, что если $A \cap B = B$ для любого множества A, то $B = \emptyset$.

1.12. Доказать, что для любых множеств A и B имеет место включение

$$A \cap B \subseteq A \cup B.$$

1.13. Верны ли, следующие утверждения:

а) если $A \cup B = A \cup C$, то $B = C$;

б) если $A \cap B = A \cap C$, то $B = C$;

в) если $A \cup B = A \cup C$ и $A \cap B = A \cap C$, то $B = C$?

1.14. Доказать основные теоретико-множественные тождества и проиллюстрировать их с помощью кругов Элера–Венна:

а) $A \cup A = A$ (идемпотентность объединения);

б) $A \cap A = A$ (идемпотентность пересечения);

в) $A \cup B = B \cup A$ (коммутативность объединения);

г) $A \cap B = B \cap A$ (коммутативность пересечения);

д) $A \cup (B \cup C) = (A \cup B) \cup C$ (ассоциативность объединения);

е) $A \cap (B \cap C) = (A \cap B) \cap C$ (ассоциативность пересечения);

ж) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (дистрибутивность объединения относительно пересечения);

з) $\overline{A \cap B} = \overline{A} \cup \overline{B}$;

и) $A \cup \overline{A} = U$;

к) $A \cap \overline{A} = \emptyset$;

л) $A \cup \emptyset = A$;

м) $A \cap \emptyset = \emptyset$.

1.15. Доказать следующие тождества:

а) $A \cup (A \cap B) = A$;

б) $A \cap (A \cup B) = A$;

в) $A \setminus B = A \cap \overline{B}$;
г) $A \cup (B \setminus C) = (A \cup B) \cap (A \cup \overline{C})$;
д) $(A \setminus B) \cup (A \cap B) = A$;
е) $A \cap B = A \cap (\overline{A} \cup B)$;
ж) $(A \cup B) \cap (A \cup \overline{B}) = (A \cap B) \cup (A \cap \overline{B}) = A$;
з) $(A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$;
и) $(A \setminus B) \cup (\overline{A} \setminus \overline{B}) = (A \cup B) \setminus (A \cap B)$;
к) $(\overline{A} \setminus \overline{B}) \cup (\overline{B} \setminus \overline{A}) = (A \cup B) \setminus (A \cap B)$;
л) $(A \setminus \overline{B}) \cup (\overline{A} \setminus B) = (B \cup \overline{A}) \cap (A \cup \overline{B})$;
м) $A \setminus (A \setminus B) = A \cap B$;
н) $B \cup (A \setminus B) = A \cup B$;
о) $B \cap (A \setminus B) = \emptyset$;
п) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$;
р) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$;
с) $\overline{A \setminus B} = \overline{A} \cup B$;
т) $(A \setminus B) \setminus C = (A \setminus C) \setminus (B \setminus C)$;
у) $A \setminus (B \cup C) = (A \setminus B) \setminus C$.

1.16. Найти множество X, удовлетворяющие следующим условиям:
а) $A \setminus X = A$ и $A \cup X = U$;
б) $A \setminus X = \emptyset$ и $A \cup X = A$.

1.17. Доказать, что:
а) $A \cup B \subseteq C \Leftrightarrow A \subseteq C$ и $B \subseteq C$;
б) $(A \setminus B) \cup B = A \Leftrightarrow B \subseteq A$;
в) $(A \cup B) \setminus B = A \Leftrightarrow A \cap B = \emptyset$;
г) $A \cup B = A \setminus B \Leftrightarrow B = \emptyset$;
д) $A \subseteq B \subseteq C \Leftrightarrow A \cup B = B \cap C$.

1.18. *Симметрической разностью* множеств A и B называется множество $A \dot{-} B = (A \setminus B) \cup (B \setminus A)$. Доказать тождества:
а) $A \dot{-} B = B \dot{-} A$;
б) $A \dot{-} (B \dot{-} C) = (A \dot{-} B) \dot{-} C$;
в) $A \cap (B \dot{-} C) = (A \cap B) \dot{-} (A \cap C)$;

г) $A\dot{-}(A\dot{-}B) = B$;
д) $A\dot{-}\emptyset = A$;
е) $A\dot{-}A = \emptyset$.

1.19. Упростить выражения:
а) $\overline{A \setminus B} \cap (\overline{A} \cup \overline{B})$;
б) $((A \cap \overline{B}) \cup (\overline{B} \cap C)) \cap ((\overline{A} \cap B) \cup B)$;
в) $\overline{\overline{A \setminus B} \cap (\overline{A} \cup \overline{B})}$;
г) $(A \cap B \cap C \cap \overline{D}) \cup (\overline{A} \cap C) \cup (\overline{B} \cap C)) \cup (C \cup D)$.

§ 2. Бинарные отношения

Пусть A и B – произвольные множества. Пару $\langle a, b\rangle$ элементов $a \in A$, $b \in B$, взятых в данном порядке, будем называть *упорядоченной парой*. Упорядоченные пары $\langle a, b\rangle$ и $\langle c, d\rangle$ будем считать *равными* и записывать $\langle a, b\rangle = \langle c, d\rangle$ тогда и только тогда, когда $a = c,\ b = d$.

Прямым (декартовым) произведением двух множеств A и B называется множество всех упорядоченных пар $\langle a, b\rangle$:

$$A \times B = \{\langle a, b\rangle \mid a \in A,\ b \in B\}.$$

Прямым (декартовым) произведением n множеств $A_1, \ldots, A_n$ называется множество всех упорядоченных n-ок $\langle a_1, \ldots, a_n\rangle$:

$$A_1 \times \ldots \times A_n = \{\langle a_1, \ldots, a_n\rangle \mid a_1 \in A_1, \ldots, a_n \in A_n\}.$$

Если $A_1 = \ldots = A_n = A$, то множество $A_1 \times \ldots \times A_n$ называется *прямой n-й степенью множества A* и обозначается через A^n.

Бинарным отношением между элементами множеств A и B называется любое подмножество R множества $A \times B$. Если $A = B$, то отношение называется *бинарным отношением на A*.

Если R – бинарное отношение и $\langle a, b\rangle \in R$, то говорят, что a и b *связаны отношением R*, или что *элемент a находится в отношении R к b*, или что для a и b *выполняется отношение R*. Вместо записи $\langle a, b\rangle \in R$ часто используют более простую aRb (например, $a < b,\ a = b,\ a \perp b$).

Бинарное отношение R на множестве A называется *рефлексивным*, если aRa для любого $a \in A$.

Примерами рефлексивных отношений могут служить отношение параллельности на множестве прямых плоскости,

отношение равенства на каком-либо множестве чисел, отношение делимости на множестве целых чисел.

Бинарное отношение R на множестве A называется *антирефлексивным (иррефлексивным)*, если для любого $a \in A$ условие aRa не выполняется.

Примерами антирефлексивных отношений могут служить отношение перпендикулярности на множестве прямых плоскости, отношение неравенства ($\neq$) на каком-либо множестве чисел.

Бинарное отношение R на множестве A называется *симметричным*, если для любых a, $b \in A$ из условия aRb следует bRa.

Примерами симметричных отношений могут служить отношение параллельности на множестве прямых плоскости, отношение перпендикулярности на множестве прямых плоскости, отношение равенства на каком-либо множестве чисел.

Бинарное отношение R на множестве A называется *антисимметричным*, если для любых a, $b \in A$ из условий aRb, bRa следует $a = b$.

Примерами антисимметричных отношений могут служить отношение $\leq$ на множестве действительных чисел, отношение включения $\subseteq$ на какой-либо совокупности множеств, отношение делимости на множестве натуральных чисел.

Бинарное отношение R на множестве A называется *транзитивным*, если для любых a, b, $c \in A$ из условий aRb, bRc следует aRc.

Примерами транзитивных отношений могут служить отношение отношение параллельности на множестве прямых плоскости, отношение равенства на каком-либо множестве чисел, отношение делимости на множестве целых чисел.

Бинарное отношение R на множестве A называется *отношением эквивалентности*, если оно рефлексивно, симмет-

рично и транзитивно на A. При этом элементы, находящиеся в отношении R, называют *эквивалентными*.

Примерами отношений эквивалентности являются отношение параллельности на множестве прямых плоскости, отношение равенства на каком-либо множестве чисел, отношение подобия на множестве треугольников плоскости.

Если R отношение эквивалентности на множестве A и a произвольный элемент из A, то подмножество

$$[a]_R = \{x \in A \mid xRa\}$$

всех элементов, эквивалентных данному элементу a, называется *классом эквивалентности, порожденном элементом* a.

Совокупность всех классов эквивалентности множества A по отношению R называется *фактормножеством* A *по* R и обозначается через A/R.

Основные свойства классов эквивалентности. Пусть R – отношение эквивалентности на множестве A. Тогда

1) $a \in [a]_R$;
2) $aRb \Leftrightarrow [a]_R = [b]_R$.

Из свойства 1) вытекает, что каждый элемент множества A принадлежит некоторому классу эквивалентности, а из свойства 2) – что два класса эквивалентности либо не пересекаются, либо совпадают.

Бинарное отношение R на множестве A называется *отношением частичного порядка* (или *отношением нестрого порядка*), если оно рефлексивно, транзитивно и антисимметрично. Множество с заданным на нем отношением частичного порядка называют *частично упорядоченным*.

Примерами частичного порядка могут служить отношение включения $\subseteq$ на какой-либо совокупности множеств, от-

ношение $\leq$ на множестве действительных чисел, отношение делимости на множестве натуральных чисел.

Отношение частичного порядка R на множестве A называется *отношением линейного порядка*, если для любых двух различных элементов a и b множества A либо aRb, либо bRa. Множество с заданным на нем отношением линейного порядка называют *линейно упорядоченным*.

Примерами линейного порядка являются отношения «меньше» $<$ и «меньше или равно» $\leq$ на множестве действительных чисел.

Примеры решения задач

Задача 1. Доказать, что операция прямого произведения множеств некоммутативна, т.е.

$$A \times B \neq B \times A.$$

Доказательство. Пусть $A = \{a, b, c\}$, $B = \{a', b'\}$. Тогда

$$A \times B = \{\langle a, a'\rangle, \langle a, b'\rangle, \langle b, a'\rangle, \langle b, b'\rangle, \langle c, a'\rangle, \langle c, b'\rangle\},$$

но

$$B \times A = \{\langle a', a\rangle, \langle a', b\rangle, \langle a', c\rangle, \langle b', a\rangle, \langle b', b\rangle, \langle b', c\rangle\}.$$

Видим, что $A \times B \neq B \times A$.

Равенство $A \times B = B \times A$ возможно тогда и только тогда, когда множества A и B совпадают. $\square$

Задача 2. Изобразить на плоскости с декартовой системой координат следующие множества:

а) $[a, b] \times [c, d]$, где $[a, b]$ и $[c, d]$ – отрезки действительной прямой;

б) $[a, b]^2$.

Решение. По определению

$$[a,\, b] \times [c,\, d] = \{\langle x,\, y\rangle \mid x \in [a,\, b],\ y \in [c,\, d]\}.$$

Каждой паре $\langle x,\, y\rangle$ можно сопоставить точку координатной плоскости, абсцисса которой равна x, а ордината – y. Если $x \in [a,\, b]$, а $y \in [c,\, d]$, то прямому произведению $[a,\, b] \times [c,\, d]$ будет соответствовать множество точек плоскости с координатами из множеств $[a,\, b]$ и $[c,\, d]$. В случае а) это прямоугольник (рис. 2), в случае б) – квадрат. □

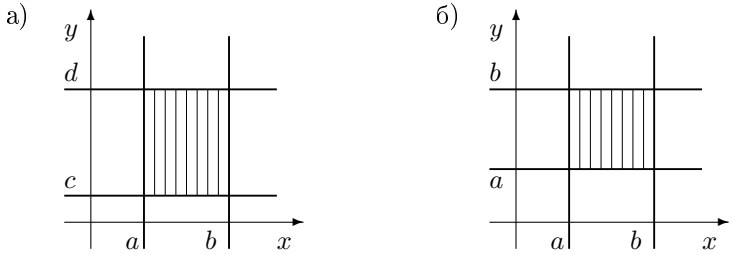


Рис. 2

Задача 3. Доказать, что

$$(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D).$$

При каких A, B, C, D получается равенство?

Доказательство. Пусть $x \in (A \times B) \cup (C \times D)$. Тогда $x = \langle y, z\rangle$ и $y \in A$, $z \in B$ или $y \in C$, $z \in D$. Отсюда следует, что $y \in A \cup C$, $z \in B \cup D$ и $x = \langle y, z\rangle \in (A \cup C) \times (B \cup D)$. Таким образом, мы доказали включение $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$.

Равенство $(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup D)$ возможно тогда и только тогда, когда выполняется хотя бы одно из

четырех условий: 1) $A = C$; 2) $B = D$; 3) $A \subseteq C$ и $B \subseteq D$; 4) $D \subseteq B$ и $C \subseteq A$. Если ни одно из этих условий не выполняется, то можно найти: а) либо упорядоченную пару $\langle y, z\rangle$, такую, что $y \in A \setminus C$, $z \in D \setminus B$; б) либо упорядоченную пару $\langle y', z'\rangle$, такую, что $y' \in C \setminus A$, $z' \in B \setminus D$. В обоих случаях такая пара принадлежит множеству $(A \cup C) \times (B \cup D)$, но не принадлежит множеству $(A \times B) \cup (C \times D)$. □

Задача 4. На множестве целых чисел $\mathbb{Z}$ задано бинарное отношение R: $aRb \Leftrightarrow a \leq b + 1$. Выяснить, какими свойствами (рефлексивность, симметричность, антисимметричность, транзитивность) оно обладает.

Решение. Отношение R будет являться рефлексивным, так как $a \leq a + 1$ для любого $a \in \mathbb{Z}$. Если $a \leq b + 1$, то не всегда $b \leq a + 1$, например, $2 \leq 5 + 1$, но неверно, что $5 \leq 2 + 1$, следовательно, R не симметрично. Отношение R было бы антисимметричным, если из условий $a \leq b + 1$ и $b \leq a + 1$ следовало бы $a = b$, но в нашем случае мы получаем $a - 1 \leq b \leq a + 1$. И, наконец, R не является транзитивным: если $a \leq b + 1$ и $b \leq c + 1$, то $a \leq c + 2$ (вместо $a \leq c + 1$). □

Задача 5. Является ли бинарное отношение R, заданное на множестве $M = \{1, 2, 3\}$, отношением эквивалентности, если:

а) $R = \{\langle 1, 1\rangle, \langle 2, 2\rangle, \langle 1, 2\rangle, \langle 2, 1\rangle, \langle 3, 3\rangle\}$;

б) $R = \{\langle 1, 1\rangle, \langle 2, 2\rangle, \langle 1, 2\rangle\}$?

Решение. Если R это отношение эквивалентности, то оно, по определению, должно быть рефлексивным, симметричным и транзитивным. Отношение R в случае а) является рефлексивным, так как $\langle 1, 1\rangle$, $\langle 2, 2\rangle$ и $\langle 3, 3\rangle$ принадлежат R. Для каждой пары в R существует симметричная ей пара, например, для пары $\langle 1, 2\rangle$ симметричной будет являться пара

$\langle 2, 1\rangle \in R$. Кроме того, R транзитивное отношение, поскольку из условий $\langle a, b\rangle \in R$ и $\langle b, c\rangle \in R$, всегда следует, что и $\langle a, c\rangle \in R$; например, для пар $\langle 2, 1\rangle \in R$ и $\langle 1, 2\rangle \in R$ пара $\langle 2, 2\rangle$ также принадлежит R. Таким образом, можем сделать вывод, что в случае а) R – отношение эквивалентности.

В случае б) отношение R не будет являться отношением эквивалентности, так как оно не рефлексивно: $\langle 3, 3\rangle \notin R$ и не симметрично: для пары $\langle 1, 2\rangle \in R$ симметричная ей пара $\langle 2, 1\rangle$ не принадлежит R. Однако, это отношение будет являться транзитивным. □

Задача 6. Пусть $m \in \mathbb{N}$. Определим на множестве $\mathbb{Z}$ бинарное отношение $\equiv$ следующим образом: $a \equiv b \pmod m \Leftrightarrow a - b$ делится на m (читается: a сравнимо с b по модулю m). Доказать, что такое отношение является отношением эквивалентности. Описать классы эквивалентности.

Доказательство. Действительно, $a - a = 0$ делится на любое натуральное m, т.е. $a \equiv a \pmod m$ (рефлексивность). Если $a - b \vdots m$, то и $b - a \vdots m$, т.е. из условия $a \equiv b \pmod m$ следует, что $b \equiv a \pmod m$ (симметричность). Если $a - b \vdots m$ и $b - c \vdots m$, то $a - c = (a - b) + (b - c) \vdots m$, т.е. из условия $a \equiv b \pmod m$, $b \equiv c \pmod m$ следует, что $a \equiv c \pmod m$ (транзитивность).

Можно заметить, что целые числа a и b сравнимы по модулю m тогда и только тогда, когда при делении на m они имеют одинаковые остатки. Так как отношение сравнимости целых чисел по модулю m является отношением эквивалентности на $\mathbb{Z}$, то все множество $\mathbb{Z}$ разбивается на непересекающиеся классы (множества) чисел, сравнимых по модулю m, т.е. дающих одинаковые остатки при делении на m. Класс всех целых чисел, имеющих при делении на m остаток r, на-

зывают *классом вычетов по модулю* m и обозначают через $\overline{r}$, так что $\overline{r} = \{r + mq \mid q \in \mathbb{Z}\}$.

Фактормножество, получаемое в этом случае, обычно обозначают через $\mathbb{Z}_m$. Так как различные остатки от деления целых чисел на m исчерпываются числами $0, 1, \ldots, m-1$, то число классов вычетов по модулю m равно m, и фактормножество $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$. □

Упражнения для самостоятельной работы

2.1. Перечислить элементы множеств $A \times B$ и $B \times A$:

а) $A = \{1, 2\}$, $B = \{3, 4, 5\}$;

б) $A = \{1, 2\}$, $B = \{1, 2, 3\}$;

в) $A = \{1\}$, $B = \{1, 2, 3\}$;

г) $A = \emptyset$, $B = \{1, 2\}$.

2.2. Пусть $A, B \subseteq C$. Доказать, что справедливо равенство $A \times B = (A \times C) \cap (C \times B)$.

2.3. Пусть A, B, C, D – непустые множества. Доказать, что:

а) $A \subseteq B$ и $C \subseteq D \Leftrightarrow A \times C \subseteq B \times D$;

б) $A = B$ и $C = D \Leftrightarrow A \times C = B \times D$.

2.4. Доказать, что:

а) $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$;

б) $(A \cup B) \times C = (A \times C) \cup (B \times C)$;

в) $A \times (B \cup C) = (A \times B) \cup (A \times C)$;

г) $(A \cap B) \times C = (A \times C) \cap (B \times C)$;

д) $A \times (B \cap C) = (A \times B) \cap (A \times C)$;

е) $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$;

ж) $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$.

2.5. Пусть A, B – непустые множества и $(A \times B) \cup (B \times A) = C \times D$. Доказать, что $A = B = C = D$.

2.6. Для каждого из следующих бинарных отношений, заданных на множестве M, выяснить, какими свойствами (ре-

флексивность, симметричность, антисимметричность, транзитивность) оно обладает:

а) $M = \mathbb{N}$, $aRb \Leftrightarrow a < b$;
б) $M = \mathbb{N}$, $aRb \Leftrightarrow a \leq b$;
в) $M = \mathbb{N}$, $aRb \Leftrightarrow a \neq b$;
г) $M = \mathbb{N}$, $aRb \Leftrightarrow a + b = 1$;
д) $M = \mathbb{N}$, $aRb \Leftrightarrow \text{НОД}(a, b) \neq 1$;
е) $M = \mathbb{N} \times \mathbb{N}$, $\langle a, b\rangle R\langle c, d\rangle \Leftrightarrow ad = bc$;
ж) $M = \mathbb{Z}$, $aRb \Leftrightarrow |a| = |b|$;
з) $M = \mathbb{Z}$, $aRb \Leftrightarrow a^2 + b^2 = 1$;
и) $M = \mathbb{Z}$, $aRb \Leftrightarrow 2a = 3b$;
к) $M = \mathbb{Z}$, $aRb \Leftrightarrow a + b > 5$ и $b < 0$;
л) $M = \mathbb{Z} \times \mathbb{Z}$, $\langle a, b\rangle R\langle c, d\rangle \Leftrightarrow a - b = c - d$ и $a \neq b$;
м) $M = \mathbb{R}$, $aRb \Leftrightarrow ab > 0$;
н) $M = \mathbb{R}$, $aRb \Leftrightarrow a^2 + a = b^2 + b$;
о) $M = \mathbb{R}$, $aRb \Leftrightarrow a - b \in \mathbb{Z}$;
п) $M = \mathbb{R}$, $aRb \Leftrightarrow b = |a|$ или $b = a^2$;
р) $M = P(\mathbb{Z})$ – множество всех подмножеств множества $\mathbb{Z}$, $ARB \Leftrightarrow A \cap B = \emptyset$;
с) $M = P(\mathbb{Z})$, $ARB \Leftrightarrow A \subset B$;
т) $M = P(\mathbb{Z})$, $ARB \Leftrightarrow A \cap B \neq \emptyset$.

2.7. Построить бинарное отношение:

а) рефлексивное и транзитивное, но не симметричное;
б) рефлексивное и симметричное, но не транзитивное;
в) антисимметричное и транзитивное, но не рефлексивное;
г) симметричное и транзитивное, но не рефлексивное.

2.8. Доказать, что симметричное и антисимметричное бинарное отношение R является транзитивным.

2.9. Доказать, что следующие бинарные отношения, заданные на множестве M, являются отношениями эквивалентности:

а) $M = \mathbb{N}$, $aRb \Leftrightarrow |a - b|$ делится на n;

б) $M = \mathbb{Z}$, $aRb \Leftrightarrow (a > 0$ и $b > 0)$ или $(a = b = 0)$ или $(a > 0$ и $b > 0)$;

в) M – множество векторов плоскости, $\vec{a}R\vec{b} \Leftrightarrow \vec{a}$ коллинеарен $\vec{b}$;

г) M – множество правильных n-угольников, $aRb \Leftrightarrow a$ подобен b.

2.10. Доказать, что каждое из следующих отношений, заданных на множестве M, является отношением эквивалентности, и найти классы эквивалентности:

а) $M = \mathbb{N} \times \mathbb{N}$, $\langle a, b\rangle R\langle c, d\rangle \Leftrightarrow a + d = b + c$;

б) $M = \mathbb{R}$, $aRb \Leftrightarrow a^2 = b^2$;

в) $M = \mathbb{R}$, $aRb \Leftrightarrow a - b \in \mathbb{Z}$.

2.11. На множестве $\mathbb{R}$ задано бинарное отношение $aRb \Leftrightarrow a^2+a = b^2+b$. Доказать, что R – отношение эквивалентности. Сколько элементов может содержать класс эквивалентности?

2.12. Доказать, что отношение $\langle a, b\rangle R\langle c, d\rangle \Leftrightarrow a^2+b^2 = c^2+d^2$ является отношением эквивалентности на множестве $\mathbb{R} \times \mathbb{R}$. Найти классы эквивалентности и изобразить их на координатной плоскости.

2.13. Построить минимальное отношение эквивалентности R на множестве $M = \{1, 2, 3, 4, 5\}$ так, чтобы $1R2$, $2R3$.

2.14. Найти все фактормножества множества $\{1, 2, 3\}$.

2.15. Показать, что множество $\{1, 2, 3, 4\}$ имеет 15 различных фактормножеств.

2.16. На множестве A^4, где $A = \{0, 1\}$, заданы бинарные отношения R_1, R_2 так, что для элементов $a = \langle a_1, a_2, a_3, a_4\rangle$, $b = \langle b_1, b_2, b_3, b_4\rangle \in A^4$: $aR_1b \Leftrightarrow a_i \leq b_i$ для некоторого $i = 1, 2, 3, 4$, $aR_2b \Leftrightarrow a_i \leq b_i$ для всех $i = 1, 2, 3, 4$. Выяснить, являются ли они отношениями частичного порядка.

§ 3. Бинарные алгебраические операции

Будем говорить, что на множестве M задана *бинарная алгебраическая операция*, если задано правило (закон) по которому каждой упорядоченной паре $\langle a, b\rangle$ элементов $a, b \in M$ ставится в соответствие однозначно определенный элемент $c \in M$. Другими словами, бинарная алгебраическая операция на M есть отображение множества $M \times M$ во множество M.

Бинарную алгебраическую операцию обычно обозначают каким-либо знаком, чаще всего точкой $\cdot$, пишут $c = a \cdot b$ (как и при умножении чисел, знак $\cdot$ иногда опускают), реже используют символы: $+$, $*$, $\circ$ и др. Запись операции точкой называют *мультипликативной*[1] записью, а запись плюсом – *аддитивной*[2] записью.

Простейшими **примерами** бинарных операций являются сложение и умножение на множествах натуральных чисел $\mathbb{N}$, целых чисел $\mathbb{Z}$, рациональных чисел $\mathbb{Q}$ и действительных чисел $\mathbb{R}$. Вычитание является бинарной операцией на множествах $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и не является таковой на множестве $\mathbb{N}$. На множестве $P(M)$ всех подмножеств множества M объединение и пересечение любых двух подмножеств являются бинарными операциями.

В алгебре кроме бинарных рассматривают также n-арные операции при любом n, являющиеся отображениями множества M^n в M. При $n = 1$ операция называется *унарной*. **Примером** унарной операции может служить операция транспонирования матриц.

На множестве M может быть задана не одна алгебраическая операция. Всякое множество, с заданными на нем алгеб-

[1] От латинского слова multiplicatio – умножение.

[2] От латинского слова additio – сложение.

раическими операциями, называют *алгебраической системой (структурой)*.

Примерами алгебраических систем могут служить: множество целых чисел $\mathbb{Z}$, с заданными на нем операциями сложения и умножения; множество действительных чисел $\mathbb{R}$ с операциями сложения, умножения, вычитания; множество $M_n(\mathbb{R})$ квадратных матриц порядка n с элементами из $\mathbb{R}$ с операциями сложения и умножения матриц.

Все бинарные алгебраические операции можно классифицировать по их свойствам.

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

$$(a * b) * c = a * (b * c); \tag{1}$$

операция $*$ называется *коммутативной*, если для любых $a, b \in M$

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

Например, операции сложения и умножения на числовых множествах $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ассоциативны и коммутативны, тогда как операция умножения матриц на $M_n(\mathbb{R})$ ассоциативна, но не коммутативна, а вычитание на множествах $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ не обладает ни тем ни другим свойством.

Равенство (2) может выполняться для некоторых элементов множества M, даже если операция не коммутативна. Такие элементы называются *перестановочными* (*коммутирующими*).

Элемент $e \in M$ называется *нейтральным* относительно операции $*$, если для любого $a \in M$ выполняются равенства

$$a * e = e * a = a. \tag{3}$$

Например, число 1 является нейтральным элементом множеств $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ относительно умножения, 0 является

нейтральным элементом множеств $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ относительно сложения. Множество $\mathbb{N}$ натуральных чисел относительно сложения и множество $\mathbb{Z}$ целых чисел относительно вычитания нейтральных элементов не имеют.

Пусть e – нейтральный элемент множества M относительно операции $*$. Элемент $b \in M$ называется *симметричным* к элементу $a \in M$, если

$$a * b = b * a = e. \tag{4}$$

Например, относительно сложения целых чисел симметричным к целому числу a является это же число, взятое со знаком минус $-a$, относительно умножения рациональных чисел симметричным к числу a, $a \neq 0$ является число $\dfrac{1}{a}$ (число 0 не имеет симметричного элемента относительно умножения).

Следующие свойства связывают две бинарные операции, заданные на множестве M. Операция $*$ называется *дистрибутивной* относительно операции $\circ$ на множестве M, если для любых элементов $a, b, c \in M$ выполняются равенства

$$a * (b \circ c) = (a * b) \circ (a * c), \quad (b \circ c) * a = (b * a) \circ (c * a). \tag{5}$$

Например, на всех числовых множествах операция умножения дистрибутивна относительно операции сложения, операция пересечения на множестве $P(M)$ дистрибутивна относительно операции объединения, а операция объединения дистрибутивна относительно операции пересечения. Однако операция сложения чисел не дистрибутивна относительно умножения.

Если операцию, заданную на каком-либо множестве, обозначают $+$ и называют суммой, то в этом случае нейтральный элемент называют *нулевым* элементом и обозначают θ

или 0, а элемент, симметричный к элементу a – *противоположным* к a и обозначают $-a$. Если используют мультипликативную запись, то нейтральный элемент называют *единичным* элементом и обозначают e или 1, а элемент симметричный к элементу a – *обратным* к a и обозначают a^{-1}.

Примеры решения задач

Задача 1. Является ли вычитание бинарной операцией на множестве $A = \{-3, -2, -1, 0, 1, 2, 3\}$?

Решение. Вычитание будет задано (определено) на множестве A, если в результате вычитания двух любых чисел из данного множества получается число, также принадлежащие множеству A. Рассмотрим, например, разность чисел -3 и $1 : -3 - 1 = -4 \notin A$. Таким образом, вычитание не будет являться бинарной операцией на множестве A. □

Задача 2. Является ли деление алгебраической операцией на множестве всех рациональных чисел $\mathbb{Q}$?

Решение. Частное от деления двух рациональных чисел будет однозначно определенным рациональным числом, кроме случая, когда делителем является число 0, так как деление на нуль невозможно. Поэтому деление на множестве всех рациональных чисел не является бинарной алгебраической операцией. Однако, если вместо всего множества рациональных чисел $\mathbb{Q}$ мы возьмем множество $\mathbb{Q}^*$ рациональных чисел, отличных от нуля – $\mathbb{Q} \setminus \{0\}$, то на этом множестве деление уже будет являться алгебраической операцией. □

Задача 3. Показать, что умножение $n \times n$ матриц, состоящих из действительных чисел, является бинарной операцией на множестве всех невырожденных матриц (матрица называется *невырожденной*, если ее определитель не равен нулю), а сложение матриц – нет.

Доказательство. Пусть $A = (a_{ij})$ и $B = (b_{ij})$ $(a_{ij}, b_{ij} \in \mathbb{R})$ – произвольные невырожденные матрицы n-ого порядка: $|A| \neq 0$, $|B| \neq 0$. Тогда их произведение $AB = C = (c_{ij})$ $(c_{ij} \in \mathbb{R})$ является однозначно определенной матрицей n-ого порядка. Остается показать, что матрица C является невырожденной матрицей. Для этого воспользуемся одним известным утверждением линейной алгебры, а именно: *определитель произведения двух матриц равен произведению определителей этих матриц*. Откуда следует, что $|C| = |A| \cdot |B|$. Так как $|A| \neq 0$, $|B| \neq 0$, то и $|C| \neq 0$, т.е. матрица C – невырожденная. Таким образом, произведение двух невырожденных матриц n-ого порядка снова есть невырожденная матрица n-ого порядка. Следовательно, по определению бинарной операции, умножение на множестве всех невырожденных матриц является бинарной операцией, а само множество невырожденных матриц с операцией умножения является алгебраической системой.

Теперь покажем, что сложение матриц n-ого порядка не является бинарной операцией на множестве всех невырожденных матриц. Для этого нам достаточно будет привести пример двух таких невырожденных матриц, сумма которых есть матрица с нулевым определителем. Рассмотрим матрицы 2-ого порядка. Пусть, например,

$$A = \begin{pmatrix} 3 & 2 \\ 8 & -1 \end{pmatrix}, \; B = \begin{pmatrix} 5 & -2 \\ 4 & 1 \end{pmatrix}.$$

Обе эти матрицы являются невырожденными, так как $|A| = \begin{vmatrix} 3 & 2 \\ 8 & -1 \end{vmatrix} = 3 \cdot (-1) - 8 \cdot 2 = -19 \neq 0$ и $|B| = \begin{vmatrix} 5 & -2 \\ 4 & 1 \end{vmatrix} = 5 \cdot 1 - 4 \cdot (-2) = 13 \neq 0$.

Однако, сумма этих матриц $A + B = \begin{pmatrix} 3+5 & 2+(-2) \\ 8+4 & -1+1 \end{pmatrix} =$

$= \begin{pmatrix} 8 & 0 \\ 12 & 0 \end{pmatrix}$, как это несложно видеть, является матрицей с нулевым определителем. □

Задача 4. Доказать, что на множестве $\mathbb{R}$ всех действительных чисел бинарная операция, заданная формулой $a \circ b = \dfrac{a+b}{2}$, коммутативна, но не ассоциативна. Будет ли эта операция ассоциативной на множестве, состоящем только из нуля?

Доказательство. Воспользуемся определением коммутативной бинарной операции. Пусть $a, b \in \mathbb{R}$. Тогда в силу коммутативности сложения действительных чисел получаем:

$$a \circ b = \frac{a+b}{2} = \frac{b+a}{2} = b \circ a,$$

и, значит, операция $\circ$ коммутативна на $\mathbb{R}$.

Проверим ассоциативность. Для любых $a, b, c \in \mathbb{R}$ имеем:

$$(a \circ b) \circ c = \frac{a+b}{2} \circ c = \frac{\dfrac{a+b}{2} + c}{2} = \frac{a+b+2c}{4},$$

но

$$a \circ (b \circ c) = a \circ \frac{b+c}{2} = \frac{a + \dfrac{b+c}{2}}{2} = \frac{2a+b+c}{4}.$$

Следовательно, $(a \circ b) \circ c \neq a \circ (b \circ c)$ при $a \neq c$ и данная операция не является ассоциативной на $\mathbb{R}$. На множестве $\{0\}$ операция будет являться ассоциативной, так как здесь $(a \circ b) \circ c = 0 = a \circ (b \circ c)$. □

Задача 5. Доказать, что на множестве M, содержащем не менее двух элементов, бинарная операция, заданная формулой $a \circ b = b$, ассоциативна. Имеет ли множество M нейтральный элемент относительно этой операции?

Доказательство. Проверим условие ассоциативности. Для любых элементов $a, b, c \in M$ будут выполняться равенства:

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

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

и поэтому операция $\circ$ ассоциативна на M.

Предположим, что в M существует нейтральный элемент e, и пусть a – любой другой элемент этого множества. Тогда, по определению нейтрального элемента, $a \circ e = a$, но по условию задачи $a \circ e = e$. Следовательно, $a = e$, и M состоит из одного элемента, что противоречит условию. Значит, наше предположение было не верным и в M нейтрального элемента относительной заданной операции не существует. □

Задача 6. Каким нейтральным элементом обладает множество M матриц вида $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$, где $a \in \mathbb{R}$, относительно матричного умножения. Найти все обратимые элементы этого множества.

Решение. Для произвольной матрицы из рассматриваемого множества будем иметь:

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}.$$

Следовательно, матрица $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M$ будет являться нейтральным (единичным) элементом множества M.

Чтобы произвольная матрица $A \in M$ имела обратную A^{-1}, необходимо и достаточно, чтобы ее определитель был отличен от нуля. Так как $|A| = \begin{vmatrix} 1 & a \\ 0 & 1 \end{vmatrix} = 1 \neq 0$, то A^{-1} существует, и, следовательно, все элементы множества M будут

обратимы. Обратной к матрице A будет являться матрица $A^{-1} = \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix}$. $\square$

Упражнения для самостоятельной работы

3.1. Является ли бинарной алгебраической операцией:

а) сложение на множестве четных чисел;

б) сложение на множестве нечетных чисел;

в) нахождение наибольшего общего делителя на множестве $\mathbb{N}$?

3.2. Является ли деление бинарной алгебраической операцией на множестве: а) $\mathbb{R}$; б) $\mathbb{R}^+$?

3.3. Является ли бинарной алгебраической операцией на множествах $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}^+$ операция $\circ$, выполняемая по правилу:

а) $a \circ b = \min\{a, b\}$;

б) $a \circ b = \max\{a, b\}$;

в) $a \circ b = a^b$.

3.4. Является ли бинарной алгебраической операцией умножение на множестве:

а) диагональных матриц вида $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, где a – произвольное действительное число;

б) нижнетреугольных матриц вида $\begin{pmatrix} a_{11} & 0 & 0 \\ a_{21} & a_{22} & 0 \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$, где a_{ij} – произвольные действительные числа?

3.5. Образуют ли алгебраические системы множества $\mathbb{N}$, $\mathbb{Q}$ относительно операции $\circ$, выполняемой по правилу:

а) $a \circ b = (a+b)^2$;

б) $a \circ b = \dfrac{a+b}{2}$;

в) $a \circ b = \dfrac{a(a+1)+b(b+1)}{2}$.

3.6. Является ли алгебраической системой множество радиус-векторов, исходящих из начала прямоугольной декартовой системы координат и расположенных в первой четверти плоскости, с операцией: а) сложения векторов; б) вычитания векторов?

3.7. Доказать, что декартов квадрат $\mathbb{R}^2$ множества $\mathbb{R}$ с операцией сложения $\langle a, b\rangle + \langle c, d\rangle = \langle a + c,\, b + d\rangle$ является алгебраической системой.

3.8. Пусть $M = \{a+b\sqrt{5} \,|\, a,\, b \in \mathbb{Z}\}$. Образует ли алгебраическую систему множество чисел M относительно операций: а) сложения; б) вычитания; в) умножения?

3.9. Являются ли коммутативными и ассоциативными на множестве $\mathbb{Q}^*$ рациональных чисел, отличных от нуля, операции умножения и деления?

3.10. Какие из следующих операций коммутативны; ассоциативны на множестве $\mathbb{N}$:

а) $a \circ b = a^b$;

б) операция нахождения наибольшего общего делителя;

в) операция нахождения наименьшего общего кратного.

3.11. Докажите, что на множестве $\mathbb{R}^+$ бинарная операция $a \circ b = \sqrt{ab}$ коммутативна, но не ассоциативна.

3.12. Почему действие, выполняемое по правилу $a \circ b = a^2 - b^2$, не является бинарной операцией на множестве $\mathbb{N}$ и является таковой на множестве $\mathbb{Z}$? Выяснить, коммутативна ли операция $\circ$ на $\mathbb{Z}$; является ли она ассоциативной?

3.13. Показать, что действие, задаваемое правилом $a \circ b = a^2 + b^2$, является коммутативной, но не ассоциативной операцией на множестве $\mathbb{R}$.

3.14. Показать, что бинарная операция матричного умножения на множестве матриц вида $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$, где $a \in \mathbb{R}$, коммутативна и ассоциативна.

3.15. Доказать, что множество $\mathbb{R}$ не содержит нейтрального элемента относительно бинарной операции $a \circ b = \dfrac{a+b}{2}$.

3.16. Содержит ли множество чисел $\{m \,|\, m = 2n,\ n \in \mathbb{Z}\}$ нейтральный элемент относительно обычного умножения?

3.17. Доказать, что относительно бинарной операции, выполняемой по правилу $a \circ b = \sqrt{ab}$, множество $\mathbb{R}^+$ не обладает нейтральным элементом.

3.18. Доказать, что множество натуральных чисел $\mathbb{N}$ относительно операции $a \circ b = \min\{a, b\}$ не обладает нейтральным элементом.

3.19. Обладает ли множество чисел вида $a + b\sqrt{2}$, где a и b – произвольные целые числа, нейтральным элементом относительно обычного умножения? Существуют ли обратные элементы к элементам $1 + \sqrt{2}$ и $3 - \sqrt{2}$?

3.20. Найти обратные элементы относительно матричного умножения для следующих матриц: $\begin{pmatrix} -2 & 0 \\ 0 & -2 \end{pmatrix}$, $\begin{pmatrix} \sqrt{2} & 1 \\ 0 & \sqrt{2} \end{pmatrix}$, $\begin{pmatrix} -\dfrac{1}{3} & 0 \\ 1 & \dfrac{1}{3} \end{pmatrix}$.

3.21. Доказать, что во множестве натуральных чисел относительно операции $a \circ b = \max\{a, b\}$ существует нейтральный элемент. Найти все симметризуемые элементы этого множества.

3.22. Существует ли во множестве $P(M)$ всех подмножеств множества M нейтральный элемент относительно операции пересечения подмножеств; объединения подмножеств? Какие элементы из множества $P(M)$ имеют симметричные?

3.23. Для следующих бинарных операций заданных на множестве $\mathbb{R}$, доказать:

а) операция $a \circ b = ab - ba$ дистрибутивна относительно

сложения; умножения;

б) операция $a \circ b = \dfrac{a+b}{2}$ дистрибутивна относительно себя;

в) операция $a * b = \max\{a, b\}$ дистрибутивна относительно операции $a \circ b = \min\{a, b\}$.

3.24. На множестве $\mathbb{R}^2$ определены операции сложения и умножения по правилам: $\langle a,\, b\rangle + \langle c,\, d\rangle = \langle a + c,\, b + d\rangle$, $\langle a,\, b\rangle \cdot \langle c,\, d\rangle = \langle a,\, d\rangle$. Являются ли эти операции коммутативными, ассоциативными, дистрибутивными одна относительно другой?

3.25. Какими свойствами должно обладать сложение и умножение для того, чтобы было справедливо тождество $(a+b)^2 = a^2 + 2ab + b^2$?

§ 4. Группы

Группой называется непустое множество G с заданной на нем бинарной алгебраической операцией $\cdot$ (которую условно будем называть умножением) такой, что выполняются следующие условия (аксиомы группы).

G_0) Если $a, b \in G$, то $a \cdot b \in G$ – *замкнутость множества G относительно операции $\cdot$.*

G_1) Для любых элементов $a, b, c \in G$ выполняется равенство $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ – *ассоциативность операции $\cdot$.*

G_2) Для любого $a \in G$ существует единичный элемент $e \in G$ такой, что выполняются равенства $a \cdot e = e \cdot a = a$ – *существование единичного элемента e.*

G_3) Для любого $a \in G$ существует обратный к нему элемент a^{-1} такой, что $a \cdot a^{-1} = a^{-1} \cdot a = e$ – *существование обратного элемента a^{-1}.*

Определенную таким образом группу обозначают в виде $(G; \cdot)$, или просто G, если ясно, о какой операции идет речь.

Группу $(G; \cdot)$ называют *коммутативной* или *абелевой*[1], если для любых $a, b \in G$ выполняется равенство $a \cdot b = b \cdot a$ – *коммутативность операции $\cdot$.*

При построении общей теории групп обычно используют мультипликативную терминологию, которой мы и будем придерживаться в дальнейшем. Аддитивная терминология применяется, как правило, только к абелевым группам.

Если для алгебраической системы $(G; \cdot)$ выполняется только условие G_0) из определения группы, то такую алгебраическую систему называют *группоидом*. Группоид с ассоциативной операцией, т.е. выполняются условия G_0) и G_1),

[1] Н.Г. Абель – норвежский математик (1802 – 1829).

называют *полугруппой.* Полугруппу, обладающую единичным элементом, принято называть *моноидом.*

Замечания

1) Выражение «на множестве задана операция»уже означает замкнутость этого множества относительно данной операции, и поэтому условие G_0) в определенном смысле является лишним. Однако включение этого условия в определении группы служит полезным напоминанием о необходимости его проверки.

2) Из свойства ассоциативности можно вывести, что произведение произвольного числа (а не только трех) элементов не зависит от расстановки скобок. Пользуясь этим, скобки обычно вообще опускают.

3) Условие G_3) на первый взгляд может показаться некорректным, поскольку мы не уточнили о каком из единичных элементов e идет речь в равенстве $a \cdot a^{-1} = a^{-1} \cdot a = e$. На самом деле, в таком уточнении нет необходимости, так как легко доказывается единственность e и a^{-1} (e – для всей группы, a^{-1} – для данного a) в произвольной группе.

4) В условии G_2) определения группы мы потребовали выполнение равенств $a \cdot e = e \cdot a = a$ для существования единичного элемента e относительно операции умножения $\cdot$, в общем случае не обязательно коммутативной. Если для любых элементов a группоида $(G; \cdot)$ выполняется только равенство $a \cdot e = a$, то элемент e называют *правым единичным элементом* группоида $(G; \cdot)$; если выполняется равенство $e \cdot a = a$, то соответственно – *левым единичным элементом* группоида $(G; \cdot)$. Аналогичной терминологии придерживаются и при выполнении только одного из равенств условия G_3). Можно показать, что в полугруппе $(G; \cdot)$ при одновременном выполнении условий существования правого единичного элемента e и правого обратного элемента a^{-1} элемент e является и ле-

вым единичным элементом, a^{-1} является и левым обратным элементом, а, следовательно, $(G;\cdot)$ в этом случае будет является группой. Это обстоятельство облегчает иногда проверку того, является ли данная полугруппа группой.

Основные свойства группы. Пусть $(G;\cdot)$ – группа. Тогда

1) в группе G существует единственный нейтральный элемент;

2) для каждого элемента в группе G существует единственный симметричный элемент;

3) для любых элементов a, $b \in G$ каждое из уравнений

$$ax = b, \quad ya = b$$

имеет в группе G единственное решение;

4) для любых элементов a, $b \in G$ справедливо равенство

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

5) для любого элемента $a \in G$ выполняется равенство

$$(a^{-1})^{-1} = a.$$

Приведем **примеры** групп.

1. Целые числа $\mathbb{Z}$ относительно операции сложения образуют группу. Нулевым элементом этой группы является число 0, а противоположным к элементу a является число $-a$. Так как операция сложения целых чисел коммутативна, то $(\mathbb{Z};+)$ – абелева группа. Она называется *аддитивной группой целых чисел.*

Относительно операции умножения целые числа группу не образуют, так как не выполнено условие G_3): обратным к целому числу a является число $\dfrac{1}{a}$, но оно не является целым числом при $a \neq 1$.

Кроме $(\mathbb{Z};\ +)$, абелевыми группами по сложению являются также алгебраические системы $(\mathbb{Q};\ +)$, $(\mathbb{R};\ +)$, $(\mathbb{C};\ +)$.

2. Множество $\mathbb{Q}^*$ всех рациональных чисел, отличных от нуля, с операцией умножения есть группа, причем абелева. Единичным элементом этой группы является число 1, а обратным к элементу a является число $\dfrac{1}{a}$. Группу $(\mathbb{Q}^*;\ \cdot)$ называют *мультипликативной группой рациональных чисел.*

Наряду с $(\mathbb{Q}^*;\ \cdot)$ рассматривают также абелевы группы $(\mathbb{R}^*;\ \cdot)$, $(\mathbb{C}^*;\ \cdot)$.

Множества всех рациональных, действительных и комплексных чисел (включая нуль) группами относительно операции умножения не являются, поскольку число 0 обратного не имеет.

3. Множество, состоящее всего из одного числа 1, является абелевой группой по умножению.

4. Множества всех векторов плоскости и пространства, выходящих из начала координат, с операцией сложения образуют абелевы группы.

Может случиться так, что одна группа содержится в другой. Подмножество H группы G называется *подгруппой* группы G, если H является группой относительно операции, определенной в G. Обозначается: $H \leq G$.

На практике, чтобы установить, что непустое подмножество H группы G есть подгруппа этой группы, достаточно проверить два условия:

1) подмножество H замкнуто относительно операции, определенной в G, т.е. если $a,\ b \in H$, то $ab \in H$;

2) подмножество H замкнуто относительно взятия обратного элемента, т.е. если $a \in H$, то $a^{-1} \in H$.

В любой группе G подмножество $\{e\}$, состоящее из одной единицы, является подгруппой, которая называется *единичной подгруппой.* Любая группа также является подгруппой в

самой себе. Подгруппы, отличные от единичной и всей группы, называются *собственными подгруппами*.

Аддитивные группы $(\mathbb{Z};\,+)$ и $(\mathbb{Q};\,+)$ являются **примерами** собственных подгрупп в $(\mathbb{R};\,+)$, причем $(\mathbb{Z};\,+)$ – подгруппа в $(\mathbb{Q};\,+)$. Множество $\{1,\,-1\}$ является подгруппой мультипликативной группы $(\mathbb{R}^*;\,\cdot)$. Другой пример подгруппы в этой группе – множество $\mathbb{R}^+$ всех положительных действительных чисел. В аддитивной группе всех целых чисел $\mathbb{Z}$ множество $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ чисел, делящихся на $n\,(n \in \mathbb{N})$, является подгруппой.

Группу G, состоящую из конечного числа элементов, называют *конечной*, а число элементов в ней называют *порядком* группы и обозначают $|G|$. Группу, содержащую бесконечное число элементов, называют *бесконечной* группой. Так, например, группа из примера 3 – конечная; аддитивная группа целых чисел $(\mathbb{Z};\,+)$ и мультипликативная группа, отличных от нуля рациональных чисел $(\mathbb{Q}^*;\,\cdot)$, представляют собой примеры бесконечных групп.

Заметим, что произвольную группу $(G;\,\cdot)$ можно считать заданной, если известно чему равны попарные произведения элементов этой группы. Если $(G;\,\cdot)$ конечная группа порядка n, то всю информацию о группе можно получить с помощью квадратной таблицы, состоящей из $n+1$ строк и столбцов (включая заглавные). В заглавной строке (слева направо) и в заглавном столбце (сверху вниз) записываются все элементы $g_1,\,g_2,\ldots,g_n$ группы $(G;\,\cdot)$ в одном и том же выбранном порядке. Произведение g_ig_j элементов g_i и g_j группы $(G;\,\cdot)$ будет располагаться на пересечении строки, соответствующей элементу g_i, и столбца, соответствующего элементу g_j.

Таблица 1

	g_1	$\dots$	g_i	$\dots$	g_n
g_1					
$\vdots$					
g_i			g_ig_j		
$\vdots$					
g_n					

Построенную таблицу называют *таблицей умножения* или *таблицей Кэли* [1]. Подчеркнем, что описанная таблица называется таблицей умножения условно, следуя мультипликативной терминологии, в которой любую заданную на множестве операцию мы называем умножением. Таблицу умножения можно построить для любого конечного множества с любой заданной на нем операцией.

Приведем **пример** конечной группы, которая играет очень важную роль в теории групп. Для этого введем понятие подстановки.

Подстановкой n-ой степени конечного непустого множества Ω называют любое взаимно однозначное (биективное) отображение множества Ω на себя.

Для определенности договариваются считать, что элементами множества Ω являются числа $1, 2, \dots, n$, т.е. $\Omega = \{1, 2, \dots, n\}$. Чтобы задать какое-либо отображение множества Ω на себя (иначе, преобразование множества Ω), нужно для каждого числа $i \in \Omega$ указать число $\alpha_i \in \Omega$, в которое i переходит. Поэтому всякую подстановку n-ой степени удобно записывать в следующем виде

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix},$$

[1] А. Кэли – английский математик (1821 – 1895).

помещая под каждым числом i множества Ω соответствующее ему число α_i.

Из n чисел можно создать $n!$ различных подстановок, т.е. общее число всех подстановок n-ой степени равно $n!$ Так, например, подстановок 3-ей степени всего $3! = 1 \cdot 2 \cdot 3 = 6$:

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}.$$

Произведением $\pi_1\pi_2$ *подстановок* π_1 и π_2 считают подстановку, которая получается в результате последовательного выполнения сначала подстановки π_1, а затем подстановки π_2. Например, в результате умножения подстановок

$$\pi_1 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \ \pi_2 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},$$

мы получим подстановку

$$\pi_1\pi_2 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}.$$

Так как подстановка π_1 переводит число 1 в 2, а подстановка π_2 число 2 переводит снова в это же число, то в результате подстановка $\pi_1\pi_2$ переводит число 1 в 2. Аналогично число 2 подстановкой π_1 переводится в число 3, а число 3 подстановкой π_2 – в число 1, значит, окончательно число 2 подстановкой $\pi_1\pi_2$ переводится в число 1.

Несложно показать, что умножение подстановок ассоциативно, т.е. для любых подстановок n-ой степени π_1, π_2 и π_3 верно равенство

$$(\pi_1\pi_2)\pi_3 = \pi_1(\pi_2\pi_3). \tag{1}$$

Действительно, пусть подстановка π_1 переводит α в β, π_2 переводит β в γ, а π_3 переводит γ в δ, где $\alpha, \beta, \gamma, \delta$ – числа из

множества $\{1, 2, \ldots, n\}$. Схематично это можно изобразить следующем образом

$$\pi_1 : \alpha \to \beta, \quad \pi_2 : \beta \to \gamma, \quad \pi_3 : \gamma \to \delta.$$

Тогда, применяя правило умножения подстановок, получаем

$$\pi_1\pi_2 : \alpha \to \gamma, \quad (\pi_1\pi_2)\pi_3 : \alpha \to \delta;$$

$$\pi_2\pi_3 : \beta \to \delta, \quad \pi_1(\pi_2\pi_3) : \alpha \to \delta.$$

Откуда следует равенство (1).

Относительно определенной выше операции умножения множество всех подстановок n-ой степени обладает единичным элементом e, которым является *тождественная* подстановка

$$e = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}.$$

Обратной для подстановки

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix}$$

является подстановка

$$\pi^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ 1 & 2 & \ldots & n \end{pmatrix},$$

так как $\pi\pi^{-1} = \pi^{-1}\pi = e$.

Таким образом, мы доказали, что все подстановки n-ой степени относительно операции умножения подстановок образуют группу. Эта группа является конечной (ее порядок равен $n!$), называется *симметрической группой n-ой степени* и обозначается S_n.

Легко показать, что группа S_n не коммутативна. Выше мы рассмотрели произведение

$$\pi_1\pi_2 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}.$$

Перемножив подстановки π_1 и π_2 в другом порядке, получим

$$\pi_2\pi_1 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}.$$

Следовательно, группа S_n $(n > 2)$ не является коммутативной.

Рассмотрим пример групп, которые наиболее просто устроены. Группу $(G; \cdot)$ будем называть *циклической*, если она состоит из всех целых степеней одного элемента $g \in G$, т.е.

$$G = \{g^n \,|\, n \in \mathbb{Z}\} = \left\{\ldots, g^{-3}, g^{-2}, g^{-1}, g^0 = e, g^1, g^2, g^3, \ldots\right\}.$$

Элемент g при этом называется *образующим* группы, а сама группа обозначается как $G = \langle g\rangle$. Можно также сказать, что циклическая группа G *порождена элементом* g. Если $(G; +)$ аддитивная циклическая группа, то, по определению,

$$G = \{ng \,|\, n \in \mathbb{Z}\},$$

где $ng = \underbrace{g + g + \ldots + g}_{n\text{ раз}}$.

Поскольку в циклической группе $G = \langle g\rangle$ для любых $m, n \in \mathbb{Z}$ выполняются равенства

$$g^m g^n = g^{m+n} = g^{n+m} = g^n g^m,$$

то группа $G = \langle g\rangle$ абелева.

Для произвольной циклической группы $G = \langle g\rangle$ справедливо одно из двух: либо все степени образующего g различны,

либо имеются совпадения степеней образующего, т.е. $g^m = g^n$ при $m \neq n$.

В первом случае говорят, что элемент g имеет *бесконечный порядок*, а порожденную им циклическую группу называют *бесконечной циклической*.

Примером бесконечной циклической группы может служить аддитивная группа целых чисел $(\mathbb{Z}; +)$. Образующим элементом здесь будет являться число 1. Бесконечной циклической группой также будет являться мультипликативная группа всех целых степеней двойки:

$$\langle 2 \rangle = \left\{ \ldots, 2^{-3}, 2^{-2}, 2^{-1}, 2^0 = 1, 2^1, 2^2, 2^3, \ldots \right\}.$$

Во втором случае, при $m > n$ равенство $g^m = g^n$ умножением на g^{-n} можно привести к виду $g^{m-n} = e$, где e – единичный элемент группы. Следовательно, существует положительная степень образующего, равная единичному элементу группы. Наименьшая из таких степеней, называется *порядком* элемента g. Допустим, что порядок g равен n, тогда среди элементов

$$g^0 = e, g^1, g^2, \ldots, g^{n-1} \tag{2}$$

нет равных. Так как иначе, из равенства $g^i = g^j$ при условии $0 \leq j < i < n$ следовало бы, что $g^{i-j} = e$, причем $0 < i-j < n$, т.е. нашлась бы меньшая чем n положительная степень g, равная единичному элементу – противоречие с определением порядка элемента. Кроме того, любая степень g^k элемента g совпадает с одним из элементов (2). Действительно, если представить целое число k в виде $k = nq + r$ (здесь q – неполное частное, а r – остаток от деления k на n, $0 \leq r < n$), то будем иметь:

$$g^k = g^{nq+r} = (g^n)^q g^r = e^q g^r = g^r.$$

Таким образом, элементами (2) исчерпывается вся группа G и мы можем утверждать, что порядок группы, порожденной элементом порядка n, также равен n, т.е. G в этом случае будет являться *циклической группой порядка* n.

Классическим **примером** конечной циклической группы служит *аддитивная группа классов вычетов по модулю* m. Поясним, из каких элементов состоит эта группа.

Пусть m – произвольное натуральное число, называемое в дальнейшем модулем. Два целых числа a и b будем называть *сравнимыми по модулю* m, если при делении на m они имеют одинаковые остатки. Тот факт, что a сравнимо с b по модулю m коротко можно записать в виде соотношения $a \equiv b \,(\mathrm{mod}\, m)$, называемого *сравнением* (см. также задачу 6 § 2).

Из приведенного выше определения следует, что все множество целых чисел $\mathbb{Z}$ разбивается на классы (подмножества) чисел, сравнимых между собой по модулю m, т.е. дающих при делении на m одинаковые остатки. Класс всех целых чисел, имеющих при делении на m одинаковый остаток r, называют *классом вычетов по модулю* m и обозначают как $\overline{r}$, так что

$$\overline{r} = \{r + mq \,|\, q \in \mathbb{Z}\}.$$

Множество всех классов вычетов по модулю m обычно обозначают как $\mathbb{Z}_m$. Так как различные остатки от деления целых чисел на m исчерпываются числами $0, 1, \ldots, m-1$, то число классов вычетов по модулю m равно m, и

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}.$$

На множестве $\mathbb{Z}_m$ определяют операции сложения $(+)$ и умножения $(\cdot)$ по следующим правилам:

$$\begin{aligned} \overline{a} + \overline{b} &= \overline{a+b}; \\ \overline{a} \cdot \overline{b} &= \overline{ab}. \end{aligned} \tag{3}$$

Таким образом, что сложить (перемножить) два класса вычетов $\overline{a}$, $\overline{b}$, нужно сложить (перемножить) их представители, а затем взять класс вычетов, содержащий полученную сумму (произведение). В определении (3) в качестве таких представителей выбраны числа a и b. Несложно доказывается, что определение (3) корректно, т.е. результат сложения (умножения) классов не зависит от выбора представителей.

Покажем, что все классы вычетов по модулю m относительно сложения образуют группу. Прежде всего заметим, что операции сложения и умножения над классами вычетов сводятся к соответствующим операциям над целыми числами, следовательно, обе они ассоциативны и коммутативны. Роль нулевого элемента в $\mathbb{Z}_m$ играет нулевой класс вычетов $\overline{0}$: $\overline{a}+\overline{0}=\overline{a}$ для любого $\overline{a}\in\mathbb{Z}_m$. Кроме того, для любого $\overline{a}$ существует противоположный класс вычетов $-\overline{a}=\overline{-a}$, так как $\overline{a}+\overline{-a}=\overline{a+(-a)}=\overline{0}$. Все эти свойства позволяют нам заключить, что $(\mathbb{Z}_m;+)$ – абелева группа. Эта группа будет являться циклической группой порядка m с образующим $\overline{1}$.

Действительно,

$$\underbrace{\overline{1}+\overline{1}+\ldots+\overline{1}}_{m\text{ раз}}=\overline{m}=\overline{0},$$

и все элементы множества $\mathbb{Z}_m$ кратны $\overline{1}$:

$$0\cdot\overline{1}=\overline{0},\ \ 1\cdot\overline{1}=\overline{1},\ \ 2\cdot\overline{1}=\underbrace{\overline{1}+\overline{1}}_{2\text{ раза}}=\overline{2},\ldots,\underbrace{\overline{1}+\overline{1}+\ldots+\overline{1}}_{m-1\text{ раз}}=\overline{m-1}.$$

Поскольку m произвольное натуральное число, то рассмотренный выше пример говорит о том, что существуют конечные группы любого наперед заданного порядка.

Пусть G и G' – две группы, и пусть существует взаимно однозначное отображение φ элементов группы G на элементы группы G', причем такое, что операции $\cdot$ в группе G

соответствует операция $\circ$ в группе G', т.е. если

$$\varphi(g_1) = g_1', \qquad \varphi(g_2) = g_2',$$

то

$$\varphi(g_1 \cdot g_2) = g_1' \circ g_2'.$$

Тогда отображение φ называют *изоморфизмом* группы G на группу G', а группы, между которыми можно установить изоморфное отображение, называют *изоморфными*.

Тот факт, что группа G изоморфна группе G' часто обозначают как $G \cong G'$.

Изоморфные группы, отличаясь лишь природой элементов из которых они состоят, относительно рассматриваемых операций имеют одинаковые свойства, и поэтому с точки зрения алгебры представляют собой *одну и ту же* группу.

Примером изоморфных групп могут служить группы $(\mathbb{R}^+; \cdot)$ и $(\mathbb{R}; +)$, где $\mathbb{R}^+$ – множество всех положительных действительных чисел. Биективное отображение $\varphi : \mathbb{R}^+ \to \mathbb{R}$, по которому $\varphi(g) = \log g$, и основное свойство логарифмов

$$\log(ab) = \log a + \log b$$

позволяют заключить, что φ – изоморфизм.

Примеры решения задач

Задача 1. Образует ли группу относительно операции умножения множество чисел $G = \{-1, 1\}$? Если да, то является ли она абелевой группой?

Решение. Проверим условие G_0) замкнутости множества $G = \{-1, 1\}$ относительно операции умножения: в результате умножения любых двух чисел из данного множества должно

получится число, также принадлежащие множеству G. Имеем:

$$1 \cdot 1 = 1 \in G,\ 1 \cdot (-1) = -1 \in G,$$

$$(-1) \cdot 1 = -1 \in G,\ (-1) \cdot (-1) = 1 \in G,$$

т.е. условие G_0) выполняется.

Условие G_1) определения группы здесь также выполняется, так как умножение целых чисел обладает свойством ассоциативности. Далее, число 1, очевидно, удовлетворяет условию G_2), и, кроме того, для каждого элемента из множества G существует обратный – условие G_3). Обратными к элементам 1 и -1 являются сами эти элементы, так как $1 \cdot 1 = 1$, $(-1) \cdot (-1) = 1$.

Таким образом, все условия определения группы выполняются, и, следовательно, множество G относительно операции умножения является группой, т.е. $(\{-1, 1\}; \cdot)$ – группа. Так как умножение целых чисел коммутативно, то эта группа абелева. □

Задача 2. Доказать, что множество $\mathbb{Q}^*$ относительно операции $\circ$, выполняемой по правилу $a \circ b = \dfrac{a \cdot b}{2}$, образует группу.

Доказательство. Проверим, определена ли на множестве рациональных чисел без нуля, операция $\circ$, другими словами, проверим условие G_0). Пусть $a, b \in \mathbb{Q}^*$. Тогда произведение $a \cdot b$ двух рациональных ненулевых чисел снова рациональное ненулевое число, и если мы это число разделим на 2, то, по прежнему, не выйдем за пределы множества $\mathbb{Q}^*$. Получаем, что $a \circ b \in \mathbb{Q}^*$ и условие G_0) выполняется.

Докажем, что операция $\circ$ ассоциативна, т.е. равенство $(a \circ b) \circ c = a \circ (b \circ c)$ выполняется для всех $a, b, c \in \mathbb{Q}^*$.

Имеем:

$$(a \circ b) \circ c = \frac{a \cdot b}{2} \circ c = \frac{\frac{a \cdot b}{2} \cdot c}{2} = \frac{a \cdot b \cdot c}{4},$$

$$a \circ (b \circ c) = a \circ \frac{b \cdot c}{2} = \frac{a \cdot \frac{b \cdot c}{2}}{2} = \frac{a \cdot b \cdot c}{4},$$

и требуемое равенство выполняется.

Найдем элемент e такой, что $a \circ e = e \circ a = a$ для любого элемента $a \in \mathbb{Q}^*$:

$$a \circ e = \frac{a \cdot e}{2} = a,$$

$$a \cdot e = 2a,$$

откуда следует, что

$$e = 2,$$

$2 \in \mathbb{Q}^*$. Поскольку операция $\circ$ коммутативна:

$$a \circ b = \frac{a \cdot b}{2} = \frac{b \cdot a}{2} = b \circ a$$

для любых $a, b \in \mathbb{Q}^*$, то нам достаточно было проверить одно из равенств $a \circ e = e \circ a = a$.

Осталось проверит условие G_3): для каждого элемента a из $\mathbb{Q}^*$ должен существовать элемент x также из множества $\mathbb{Q}^*$ такой, что $a \circ x = x \circ a = e$. Решая одно из уравнений:

$$a \circ x = \frac{a \cdot x}{2} = 2,$$

$$x \circ a = \frac{x \cdot a}{2} = 2,$$

получаем

$$x = \frac{4}{a},$$

где $a \neq 0$ – по условию задачи, $\frac{4}{a} \in \mathbb{Q}^*$.

Итак, $(\mathbb{Q}^*; \circ)$ – группа, даже абелева. $\square$

Задача 3. Доказать, что множество M всех невырожденных матриц n-ого порядка с действительными элементами образует группу относительно операции умножения матриц. Является ли эта группа абелевой?

Доказательство. Прежде всего отметим, что на множестве M умножение матриц является бинарной операцией (см. задачу 3 § 3), которая, как известно из теории матриц, ассоциативна. Таким образом, условия G_0) и G_1) определения группы выполняются.

Единичным элементом множества M относительно умножения будет являться *единичная* матрица E, т.е. диагональная матрица вида

$$E = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}.$$

Легко видеть, что матрица E невырожденная. Поскольку определитель любой диагональной матрицы равен произведению элементов главной диагонали, получаем $|E| = 1 \neq 0$. Кроме того, для любой матрицы A из множества M верны равенства: $A \cdot E = E \cdot A = A$.

Наконец, для каждой невырожденной матрицы A существует обратная матрица A^{-1} такая, что $A \cdot A^{-1} = A^{-1} \cdot A = E$, причем матрица A^{-1} также будет являться невырожденной, т. е. $|A^{-1}| \neq 0$. Это следует из теоремы об умножении определителей:

$$|E| = |A \cdot A^{-1}| = |A| \cdot |A^{-1}|$$

и из условия $|A| \neq 0,\ |E| \neq 0$.

Итак, мы доказали, что $(M;\, \cdot)$ – группа. Эта группа не будет являться абелевой, так как умножение матриц не является коммутативной операцией. Это легко показать на примере.

Пусть $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 2 \\ 5 & 1 \end{pmatrix}$. Тогда

$$AB = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 5 & 1 \end{pmatrix} = \begin{pmatrix} 10 & 4 \\ 20 & 10 \end{pmatrix},$$

но

$$BA = \begin{pmatrix} 0 & 2 \\ 5 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 6 & 8 \\ 8 & 14 \end{pmatrix},$$

поэтому $AB \neq BA$. □

Группа всех невырожденных матриц n-ого порядка с действительными элементами относительно умножения носит специальное название: *общая линейная группа степени n над* $\mathbb{R}$ и обозначается $\mathrm{GL}_n(\mathbb{R})$.

Задача 4. Пусть S – множество матриц вида $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$, где a и b – произвольные действительные числа. Найти в полугруппе $(S; \cdot)$ по умножению матриц правые и левые единичные элементы, элементы, обратимые слева или справа относительно этих единичных элементов.

Решение. В полугруппе $(S; \cdot)$ правый единичный элемент $e_r = \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}$, $x, y \in \mathbb{R}$ будем искать, исходя из условия

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} e_r = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}.$$

Перемножив матрицы в левой части равенства, получим:

$$\begin{pmatrix} ax & ay \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix},$$

или, что равносильно,

$$ax = a,\ ay = b.$$

Откуда следует, что

$$x = 1,\ y = \frac{b}{a}.$$

Поскольку, по условию a и b произвольные действительные числа, то в случае, когда $a = 0$ значение y не определено. Это означает, что правого единичного элемента в полугруппе $(S;\ \cdot)$ не существует.

Если $e_l = \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}$ – левый единичный элемент полугруппы $(S;\ \cdot)$, то

$$e_l \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$$

для любой матрицы $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in S$. Решая матричное уравнение

$$\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix},$$

находим:

$$xa = a,\ \ xb = b.$$

Отсюда следует, что

$$x = 1,\ \ y = \lambda,$$

где λ – произвольное действительное число, и, стало быть, $e_l = \begin{pmatrix} 1 & \lambda \\ 0 & 0 \end{pmatrix}$ – левый единичный элемент полугруппы $(S;\ \cdot)$.

Итак, в полугруппе $(S;\ \cdot)$ не существует правого единичного элемента, но существует левый единичный элемент. Если оба единичных элемента существовали и совпадали бы,

то можно было говорить просто о единичном (двустороннем) элементе полугруппы.

Выясним теперь условия, при которых матрица $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ будет обратима слева или справа, т.е. определим при каких $a, b \in \mathbb{R}$ для данной матрицы будут существовать левый или правый обратные элементы относительно единичного элемента $e = \begin{pmatrix} 1 & \lambda \\ 0 & 0 \end{pmatrix}$. Если матрица $\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}$, где $x, y \in \mathbb{R}$, является левым обратным элементом для матрицы $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$, то должно выполняться равенство

$$\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & \lambda \\ 0 & 0 \end{pmatrix}.$$

Откуда получаем

$$x = \frac{1}{a}, \quad x = \frac{\lambda}{b}.$$

Из первого равенства следует условие на a: $a \neq 0$; учитывая второе равенство, можно получить условие на b: $b = \lambda a$. Таким образом, для матрицы $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ при $a \neq 0$, $b = \lambda a$ будет существовать левая обратная матрица относительно нейтрального элемента $e_l = \begin{pmatrix} 1 & \lambda \\ 0 & 0 \end{pmatrix}$.

Для обратимой справа матрицы $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ должно выполняться равенство

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & \lambda \\ 0 & 0 \end{pmatrix}.$$

Выражая из последнего уравнения x и y, находим

$$x = \frac{1}{a}, \quad y = \frac{\lambda}{a}.$$

Ясно, что здесь единственным условием будет ограничение на a: $a \neq 0$. Следовательно, любая матрица $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ при $a \neq 0$ обратима справа. □

Задача 5. Бинарная алгебраическая операция $\cdot$ на множестве G называется *обратимой*, если каждое из уравнений $ax = b$, $ya = b$ для любых a и b из G имеет в G не более одного решения. Доказать, что непустое множество G, на котором определена ассоциативная и обратимая операция, является группой.

Доказательство. Покажем, что если ассоциативная операция обратима, то в G существует единичный элемент e и для каждого элемента a найдется элемент b, который удовлетворяет равенствам: $ab = ba = e$.

Рассмотрим уравнение $gx = g$, где g – произвольный элемент множества G. Так как операция обратима, то это уравнение имеет решение. Обозначим элемент, являющейся решением данного уравнения, через e. Покажем, что e – правый единичный элемент множества G.

Пусть a – произвольный элемент множества G, а g' – является решением уравнения $xg = a$. Тогда для элементов e и g' справедливы равенства: $ge = g$ и $g'g = a$. Отсюда, учитывая ассоциативность операции $\cdot$, получаем:

$$ae = (g'g)e = g'(ge) = g'g = a$$

для любого $a \in G$. Следовательно, e – правый единичный элемент множества G.

Аналогично находится левый единичный элемент e' такой, что $e'a = a$ для любого $a \in G$. Причем элементы e и e' будут совпадать, как это следует из равенств $e'e = e'$ и $e'e = e$. Значит, для всякого $a \in G$ справедливо $ae = ea = a$, и, следовательно, e – единичный элемент.

Пусть опять a – произвольный элемент из G. В силу обратимости операции $\cdot$ уравнение $ax = e$ имеет решение, причем единственное. Обозначив это решение через b, получаем: $ab = e$. Аналогично находится элемент b' левый обратный к элементу a. Равенства

$$b' = b'e = b'(ab) = (b'a)b = eb = b$$

показывают, что элементы b' и b совпадают, и, следовательно, $ab = ba = e$, т.е. b является обратным элементом для элемента a. Итак, мы показали, что каждый элемент из множества G имеет обратный.

Приведенные выше рассуждения позволяют сделать вывод, что множество G является группой. □

Задача 6. Доказать, что непустое подмножество H группы G является подгруппой тогда и только тогда, когда оно обладает следующими свойствами:

1) если a, $b \in H$, то $ab \in H$;

2) если $a \in H$, то $a^{-1} \in H$.

Доказательство. Любая подгруппа, по определению, обладает свойствами 1), 2). Обратно, пусть H обладает этими свойствами. Согласно свойству 1) H замкнуто относительно умножения. Так как операция ассоциативна в G, то она ассоциативна и в H. Если $a \in H$, то из свойств 2) и 1) следует, что $e = aa^{-1} \in H$, и e является единицей в H. Теперь,учитывая свойство 2), получаем, что H – группа. □

Задача 7. Для множества $G = \{\pi_1, \pi_2, \pi_3, \pi_4\}$, состоящего из подстановок $\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$, $\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, $\pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$, $\pi_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$, составить таблицу умножения и с ее помощью убедиться, что $(G; \cdot)$ абелева группа.

Решение. Вычисляя всевозможные попарные произведения подстановок $\pi_1, \pi_2, \pi_3, \pi_4$, составим таблицу умножения элементов множества G.

Таблица 2

	π_1	π_2	π_3	π_4
π_1	π_1	π_2	π_3	π_4
π_2	π_2	π_3	π_4	π_1
π_3	π_3	π_4	π_1	π_2
π_4	π_4	π_1	π_2	π_3

Прежде всего, таблица 2 наглядно показывает, что произведение любых двух подстановок из G снова есть одна из подстановок множества G. Видим также, что первый столбец таблицы совпадает с ее заглавным столбцом, также как и первая строка совпадает с заглавной строкой таблицы. Это означает, что подстановка π_1 является единичным элементом множества G относительно умножения. На пересечении строки, соответствующей π_2, и столбца, соответствующего π_4, равно как и на пресечении строки, соответствующей π_4, и столбца, соответствующего π_2, находится подстановка π_1, следовательно, подстановки π_2 и π_4 будут являться взаимно обратными элементами множества G. Аналогично находим, что подстановка π_3 является обратной к самой себе.

Таким образом, учитывая, что умножение подстановок ассоциативная операция, можно сделать вывод, что $(G; \cdot)$ группа. Коммутативность операции умножения выражается

в симметричности таблицы относительно ее главной диагонали, т.е. диагонали, идущей слева вниз направо. Таблица 2 обладает этим свойством, значит, $(G;\cdot)$ абелева группа. □

Заметим, что в таблице 2 среди элементов каждой строки и каждого столбца любой элемент множества G встречается ровно один раз. Это закономерность совсем не случайна и обязательно должна выполняться, если мы хотим, чтобы таблица умножения задавала именно группу (эта закономерность равносильна требованию обратимости операции умножения – см. задачу 5).

Задача 8. Выяснить, является ли таблица 3 таблицей умножения элементов некоторой группы?

Таблица 3

	b_0	b_1	b_2	b_3
b_0	b_0	b_1	b_2	b_3
b_1	b_1	b_2	b_0	b_2
b_2	b_2	b_0	b_1	b_3
b_3	b_1	b_2	b_3	b_0

Решение. Используя, приведенное выше замечание, совсем несложно заключить, что множество элементов b_0, b_1, b_2, b_3 относительно операции, заданной таблицей 3, группой не является. Так, например, во второй строке этой таблицы элемент b_2 встречается два раза, тогда как элемент b_3 отсутствует вовсе. □

Задача 9. Пусть $M = \{a_0, a_1, a_2, a_3, a_4, a_5\}$ – множество самосовмещений правильного треугольника ABC, где $\{a_0, a_1, a_2\}$ – повороты (вращения) треугольника в его плоскости вокруг центра O против часовой стрелки на углы

$0°, 120°, 240°$ соответственно; $\{a_3, a_4, a_5, \}$ – отражения треугольника ABC относительно его осей симметрии l_1, l_2, l_3 (см. рис. 3). Показать, что множество M относительно операции умножения самосовмещений является группой (напомним, что любое преобразование некоторой фигуры в себя, сохраняющее расстояние между ее точками, называется *самосовмещением* или *симметрией* данной фигуры, а последовательное выполнение любых двух таких преобразований – *произведением* или *композицией* самосовмещений).

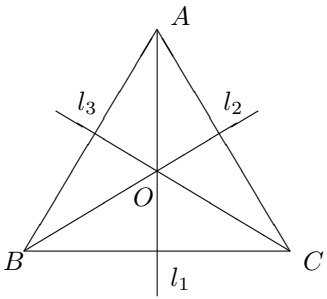


Рис. 3

Решение. Каждое из шести преобразований, переводящих треугольник ABC в себя удобно записать в виде подстановки множества вершин треугольника, где в верхней строке перечислены все вершины треугольника, а нижняя строка показывает, куда каждая вершина переходит. Так что

$$a_0 : \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}, \quad a_1 : \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}, \quad a_2 : \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix},$$

$$a_3 : \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}, \quad a_4 : \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}, \quad a_5 : \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}.$$

Составим таблицу умножения элементов a_0, a_1, a_2, a_3, a_4, a_5, пользуясь правилом умножения подстановок (см. таблицу 4).

Из построенной таблицы видно, что произведение любой пары элементов множества M есть снова элемент этого же множества, следовательно, множество M замкнуто относительно операции умножения. Иначе говоря, последовательное выполнение любых двух самосовмещений из шести равносильно какому-то одному самосовмещению треугольника.

Таблица 4

	a_0	a_1	a_2	a_3	a_4	a_5
a_0	a_0	a_1	a_2	a_3	a_4	a_5
a_1	a_1	a_2	a_0	a_4	a_5	a_3
a_2	a_2	a_0	a_1	a_5	a_3	a_4
a_3	a_3	a_5	a_4	a_0	a_2	a_1
a_4	a_4	a_3	a_5	a_1	a_0	a_2
a_5	a_5	a_4	a_3	a_2	a_1	a_0

Например, последовательное выполнение преобразований a_1 (поворот на 120° относительно точки O) и a_3 (отражение от оси l_1) равносильно преобразованию a_4 (отражение от оси l_2). Единичным элементом множества M будет являться элемент a_0 – поворот на 0° или тождественное преобразование. Равенства $a_1a_2 = a_0$ и $a_2a_1 = a_0$ позволяют заключить, что обратным к элементу a_1 будет являться элемент a_2 и, наоборот, обратным к элементу a_2 – элемент a_1. Обратные к элементам a_3, a_4, a_5 совпадают с самими этими элементами. Все перечисленные выше факты и ассоциативность операции умножения подстановок дают нам право говорить, что $(M; \cdot)$ – группа. Она называется *группой самосовмещений*

правильного треугольника. Так как таблица 4 не симметрична относительно главной диагонали, то группа самосовмещений правильного треугольника не является абелевой.

Из таблицы 4 видно, что повороты a_0, a_1, a_2 правильного треугольника также образуют группу. Эта группа называется *группой поворотов треугольника.* □

Задача 10. Показать, что группа $(G;\cdot)$, которая состоит из подстановок $\pi_1 = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$, $\pi_2 = \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$, $\pi_3 = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$, $\pi_4 = \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}$ (см. задачу 7) является циклической с образующим $\pi_2 = \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$.

Решение. В самом деле,

$$\pi_2^0 = \pi_1 = e, \quad \pi_2^1 = \pi_2,$$

$$\pi_2^2 = \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix} = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix} = \pi_3,$$

$$\pi_2^3 = \pi_3\pi_2 = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix} = \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix} = \pi_4,$$

а, возводя π_2 в четвертую степень, мы снова получим π_1:

$$\pi_2^4 = \pi_4\pi_2 = \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix} = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix} = \pi_1.$$

□

Задача 11. Найти все образующие в группе поворотов треугольника (см. задачу 9).

Решение. Данная группа состоит из трех элементов a_0, a_1, a_2, где a_0 поворот треугольника вокруг его центра на угол $0°$, a_2 – поворот на $120°$, a_3– поворот на $240°$ (напомним, что под умножением поворотов, мы понимаем последовательное их выполнение). Единичный элемент $e = a_0$ не может

быть образующим, так как, возводя a_0 в степень, мы всегда будем получать только a_0. Если a_1 – образующий группы, то должны выполняться условия: 1) $a_1^3 = e$; 2) множество всех меньших степеней a_1 должно совпадать со множеством элементов группы. Имеем:

$$a_1^3 = a_1 \cdot a_1 \cdot a_1 = (\text{поворот на } 360^\circ) = a_0 = e;$$

$$a_1^0 = e, \quad a_1^1 = a_1, \quad a_1^2 = a_1 \cdot a_1 = (\text{поворот на } 240^\circ) = a_2.$$

Следовательно, элемент a_1 является образующим циклической группы поворотов треугольника. Аналогичные равенства будут выполняться, как это несложно проверить, и для элемента a_2. Таким образом, в циклической группе поворотов треугольника два образующих: a_1 и a_2. □

Задача 12. Доказать, что множество квадратных матриц $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $a = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, $b = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $c = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ образует подгруппу в мультипликативной группе всех невырожденных матриц 2-го порядка. Является ли эта подгруппа абелевой? Является ли она циклической? Если группа циклическая, то найти все ее образующие.

Решение. Все данные матрицы имеют определитель, равный 1, поэтому принадлежат группе $\mathrm{GL}_2(\mathbb{R})$ невырожденных матриц 2-го порядка.

Для доказательства того, что данное множество матриц является подгруппой, достаточно проверить, что это множество замкнуто относительно умножения и взятия обратного элемента. Это наглядно видно из таблицы умножения матриц.

Таблица 5

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Так, например, $b^{-1} = c,\ c^{-1} = b$.

Эта подгруппа является циклической. В качестве образующего элемента в ней можно выбрать, например, матрицу b: $b^0 = e,\ b^1 = b,\ b^2 = a,\ b^3 = c$. Кроме того, образующим элементом в этой подгруппе может служить и матрица c: $c^0 = e,\ c^1 = c,\ c^2 = a,\ c^3 = b$.

Любая циклическая группа является абелевой. В нашем случае это подтверждается еще приведенной выше таблицей умножения. □

Задача 13. Докажите, что аддитивная группа $\mathbb{Z}$ всех целых чисел и мультипликативная группа целых степеней числа 2 изоморфны.

Решение. Для доказательства изоморфности двух групп построим между ними изоморфное отображение. Пусть $A = \{x | \, x = 2^k,\ k \in \mathbb{Z}\}$. Рассмотрим отображение

$$\begin{aligned} \varphi : \mathbb{Z} &\to A, \\ k &\to 2^k \end{aligned}$$

для любого k из $\mathbb{Z}$. Докажем, что оно взаимнооднозначно (биективно) и, кроме того, выполняется равенство $\varphi(k_1 + k_2) = \varphi(k_1) \cdot \varphi(k_2)$.

Покажем, что отображение инъективно и сюръективно. Для любых чисел $k_1, k_2 \in \mathbb{Z}$ из равенства $\varphi(k_1) = \varphi(k_2)$ следует $2^{k_1} = 2^{k_2}$, что возможно только в случае $k_1 = k_2$. Это

отображение сюръективно, так как для любого $\varphi(k) = 2^k \in A$ существует прообраз в $\mathbb{Z}$, равный k. Из инъективности и сюръективности отображения следует его биективность.

Кроме того, для любых k_1, $k_2 \in \mathbb{Z}$, в силу свойства степеней с одинаковым основанием, получаем $\varphi(k_1+k_2) = 2^{k_1+k_2} = = 2^{k_1} \cdot 2^{k_2} = \varphi(k_1) \cdot \varphi(k_2)$.

Таким образом, отображение $\varphi : \mathbb{Z} \to A$ является изоморфизмом. Следовательно, группа всех целых чисел изоморфна мультипликативной группе целых степеней числа 2. □

Задача 14. Показать, что все группы, содержащие три элемента (группы третьего порядка), изоморфны между собой.

Решение. Пусть мы имеем множество G из трех элементов e, a, b. Очевидно, что число неизоморфных групп третьего порядка равно числу различных таблиц умножения, которые можно задать для элементов e, a, b. При составлении таблиц следует помнить о том, что каждая таблица должна быть такой, чтобы G относительно соответствующей операции была группой. Построим таблицу с заглавной строкой и заглавным столбцом.

Таблица 6

	e	a	b
e			
a			
b			

В группе обязательно должен быть единичный элемент e. Тогда первая строка и первый столбец должны совпадать с заглавными строкой и столбцом.

Таблица 7

	e	a	b
e	e	a	b
a	a		
b	b		

Осталось заполнить 4 клетки. Если учесть, что в каждой строке и каждом столбце каждый элемент должен встретиться лишь один раз (это следствие обратимости операции в группе), то оставшиеся клетки заполнятся однозначно (см. таблицу 8).

Таким образом, на трех элементах можно лишь одним способом определить операцию так, чтобы множество этих элементов относительно определенной операции было группой. Это и значит, что существует лишь одна группа из трех элементов, иначе говоря, все группы из трех элементов изоморфны.

Таблица 8

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Конкретным примером группы третьего порядка может служить множество подстановок $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$, $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$, $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ относительно операции умножения. □

Упражнения для самостоятельной работы

4.1. Образует ли группу каждое из следующих множеств относительно указанной операции над элементами:

а) четные числа относительно сложения;

б) нечетные целые числа относительно вычитания;

в) целые числа относительно вычитания;

г) целые числа, кратные данному натуральному числу n, относительно сложения;

д) неотрицательные целые числа относительно сложения;

е) положительные рациональные числа относительно умножения;

ж) положительные рациональные числа относительно деления;

з) степени данного действительного числа a, $a \neq 0, \pm 1$, с целыми показателями относительно умножения;

и) числа вида $a + b\sqrt{5}$ относительно сложения, где a и b – произвольные целые числа;

к) все классы вычетов по модулю n относительно сложения;

л) матрицы порядка n с целыми элементами относительно умножения;

м) матрицы порядка n с действительными элементами и определителем, равным 1, относительно умножения;

н) многочлены степени n с действительными коэффициентами от одной переменной относительно сложения;

о) многочлены степени не выше n с действительными коэффициентами от одной переменной относительно сложения;

п) все подмножества множества M относительно операции $\circ$, выполняемой по формуле $A \circ B = (A \cup B) \setminus (A \cap B)$;

р) все действительные числа из полуинтервала $[0, 1)$ с операцией $\circ$, где $a \circ b$ – дробная часть числа $a + b$?

4.2. Является ли группой множество матриц вида $\begin{pmatrix} a & b \\ b & b \end{pmatrix}$, где a и b – произвольные, не равные одновременно нулю действительные числа, относительно операции умножения матриц?

4.3. Образуют ли группу множество матриц вида $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, где a и b – произвольные, не равные одновременно нулю действительные числа, относительно операции: а) сложения матриц; б) умножения матриц?

4.4. Доказать, что множество матриц вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, где a и b – произвольные, не равные одновременно нулю действительные числа, образуют группу относительно операции умножения матриц.

4.5. Выяснить, образует ли группу множество матриц вида $\begin{pmatrix} a & b \\ \lambda b & a \end{pmatrix}$, где a и b – произвольные, не равные одновременно нулю действительные числа, λ – фиксированное действительное число, относительно операции умножения матриц?

4.6. Доказать, что множество матриц вида $\begin{pmatrix} a_{11} & 0 & 0 \\ a_{21} & a_{22} & 0 \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$, где $a_{ij} \in \mathbb{R}$, $a_{ii} \neq 0$ $(i, j = 1, 2, 3)$, является группой относительно операции умножения матриц.

4.7. Образуют ли группу множество положительных действительных чисел с операцией:

а) $a \circ b = a^b$;

б) $a \circ b = a^2 b^2$?

4.8. Доказать, что множество $\mathbb{Z}$ образует группу относительно действия, заданного формулой

$$a \circ b = \begin{cases} a + b, \text{если } a - \text{четное число}, b - \text{любое целое число}, \\ a - b, \text{если } a - \text{нечетное число}, b - \text{любое целое число}. \end{cases}$$

4.9. Пусть G – множество всевозможных троек чисел вида $(a_1, a_2, 1)$ и $(b_1, b_2, -1)$ и пусть на G определена операция $\circ$,

выполняемая по правилу

$$(a_1, a_2, \varepsilon_1) \circ (b_1, b_2, \varepsilon_2) = (a_1 + b_1, a_2 + b_2, \varepsilon_1 \cdot \varepsilon_2).$$

Доказать, что $(G; \circ)$ – группа.

4.10. Доказать основные свойства группы 1) – 5).

4.11. Доказать, что если $a^2 = aa = e$ для любого элемента a мультипликативной группы G, то G абелева группа.

4.12. Показать, что группоид $(\mathbb{R}; \circ)$ не является полугруппой относительно операции, выполняемой по правилу $a \circ b = a^2 + b^2$.

4.13. Доказать, что группоид $(\mathbb{Z}; \circ)$ с операцией $a \circ b = a + b + ab$, является полугруппой. Что служит в $(\mathbb{Z}; \circ)$ нейтральным элементом? Найти в $(\mathbb{Z}; \circ)$ все обратимые элементы.

4.14. На множестве M определена операция $\circ$, выполняемая по правилу $a \circ b = a$. Доказать, что $(M; \circ)$ – полугруппа. Существуют ли в этой полугруппе правые и левые единичные элементы, обратимые элементы? При каких условиях $(M; \circ)$ является группой?

4.15. На множестве M^2, где M – некоторое множество, определена операция $\circ : (a, b) \circ (c, d) = (a, d)$. Является ли M^2 полугруппой относительно этой операции? Существует ли в M^2 нейтральный элемент?

4.16. Определить сколько элементов содержит полугруппа, состоящая из всех степеней матрицы $A = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$? Является ли эта полугруппа группой?

4.17. Элемент $aba^{-1}b^{-1}$ называется *коммутатором элементов* a и b группы G и обозначается через $[a, b]$. Коммутатор равен единице тогда и только тогда, когда элементы a и b перестановочны. Доказать, что коммутатор произвольных элементов группы обладает следующими свойствами:

а) $[a,b]^{-1}=[b,a]$;
б) $[a,b^{-1}]=b^{-1}[b,a]b$;
в) $[ab,c]=a[b,c]a^{-1}[a,c]$.

4.18. Доказать, что множество четных целых чисел является подгруппой аддитивной группы $\mathbb{Z}$ целых чисел. Образует ли множество нечетных чисел подгруппу в группе $\mathbb{Z}$?

4.19. Доказать, что любая подгруппа аддитивной группы $\mathbb{Z}$ состоит из всех чисел, кратных некоторому натуральному числу n.

4.20. Доказать, что во всякой группе:

а) пересечение любого набора подгрупп является подгруппой;

б) объединение двух подгрупп является подгруппой тогда и только тогда, когда одна из подгрупп содержится в другой.

4.21. На множестве $M=\{a,\,b,\,c\}$ бинарная операция задана таблицей 9. Выяснить, обладает ли множество M единичным элементом относительно заданной бинарной операции, является ли заданная операция коммутативной, ассоциативной. Образует ли множество M полугруппу, группу?

Таблица 9

	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

4.22. На множестве $G=\{a_0,\,a_1,\,a_2,\,a_3\}$ операция задана таблицей 10. Доказать, что эта алгебраическая система является абелевой группой.

Таблица 10

	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

4.23. Известны элементы, стоящие в трех вершинах прямоугольника таблицы Кэли некоторой конечной группы (см. таблицу 11). Найти элемент, находящийся в четвертой вершине, если 1 обозначен нейтральный элемент.

Таблица 11

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

4.24. Найдите порядок каждого элемента симметрической группы S_3 третьей степени, а затем выясните, какие циклические подгруппы S_3 они порождают. Сколько всего различных подгрупп имеет группа S_3?

4.25. Какой порядок имеет элемент $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 1 & 6 \end{pmatrix}$ симметрической группы S_6 и какую циклическую подгруппу этой группы он порождает?

4.26. Постройте циклические подгруппы группы S_4, порожденные ее элементами $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ и $b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$, а затем найдите пересечение этих подгрупп. Является ли пересечение $\langle a \rangle \cap \langle b \rangle$ абелевой подгруппой группы S_4?

4.27. Сколько подгрупп имеет группа (см. задачу 12)

$$\left\{e=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, a=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}, b=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}, c=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\right\}?$$

4.28. Найти все подгруппы циклической группы, образующим элементом которой является подстановка $\begin{pmatrix}1&2&3&4&5&6&7&8&9\\ 2&3&4&5&6&7&8&9&1\end{pmatrix}$.

4.29. Описать группы, у которых множество всех ее подгрупп состоит: а) из одной подгруппы; б) из двух подгрупп; в) из трех подгрупп.

4.30. Докажите, что если порядок элемента a группы равен m, то $a^n = e$, тогда и только тогда, когда n делится на m.

4.31. Докажите, что если порядок элемента a группы равен m, то $a^s = a^t$ в том и только в том случае, когда $s - t$ делится на m.

4.32. Докажите, что если порядок элемента a группы равен m, то порядок элемента a^k равен $\dfrac{m}{(m,k)}$, где (m,k) – наибольший общий делитель чисел m и k.

4.33. Выясните, для каких m в симметрической группе S_4 подстановок четвертой степени найдутся элементы порядка m.

4.34. Для каждой из следующих групп составить таблицу умножения ее элементов. Найти взаимно обратные элементы и выяснить коммутативна ли данная группа:

а) группа поворотов квадрата;

б) группа поворотов правильного пятиугольника;

в) группа самосовмещений ромба;

г) группа самосовмещений прямоугольника, не являющегося квадратом;

д) группа самосовмещений квадрата.

4.35. Найти группу поворотов правильного n-угольника.

4.36. Найти порядки всех элементов в группах из упр. 4.34.

4.37. Найдите все подгруппы в группах:

а) $\mathbb{Z}_5$, $\mathbb{Z}_8$, $\mathbb{Z}_{10}$;

б) в группе самосовмещений квадрата.

4.38. Какой вид имеют все подгруппы группы $\mathbb{Z}_n$ классов вычетов целых чисел по модулю n?

4.39. Доказать, что аддитивная группа всех целых чисел $\mathbb{Z}$ и аддитивная группа четных целых чисел $2\mathbb{Z}$ изоморфны.

4.40. Доказать, что аддитивная группа всех действительных чисел $\mathbb{R}$ изоморфна группе матриц вида $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, где $a \in \mathbb{R}$, относительно сложения матриц.

4.41. Доказать, что множество двумерных векторов $(a,\, b)$ и множество матриц вида $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, где $a,\, b \in \mathbb{R}$, являются изоморфными группами относительно операций сложения в этих множествах.

4.42. Пусть в группе $G = \{(a,\, b) \,|\, a,\, b \in \mathbb{R},\, a \neq 0\}$ операция умножения задана по формуле: $(a,\, b)(c,\, d) = (ac,\, ad + b)$. Доказать, что пары вида $(a,\, 0) \in G$ образуют подгруппу H группы G, изоморфную мультипликативной группе ненулевых действительных чисел.

4.43. Выяснить, изоморфна ли группа всех самосовмещений ромба группе всех самосовмещений прямоугольника.

4.44. Найти все (с точностью до изоморфизма) группы порядка: а) 2; б) 3; в) 4; г) 5.

4.45. Доказать, что группа порядка 6 либо коммутативна, либо изоморфна группе S_3.

§ 5. Кольца

Кольцом называется непустое множество R с бинарными алгебраическими операциями сложения $+$ и умножения $\cdot$, удовлетворяющими следующим условиям (аксиомам кольца).

R_1) $(R; +)$ – абелева группа (называется *аддитивной группой кольца*).

R_2) $(R; \cdot)$ – полугруппа (т.е. умножение ассоциативно).

R_3) Для любых элементов a, b, $c \in R$ выполняются равенства $a\cdot(b+c) = a\cdot b+a\cdot c$, $(b+c)\cdot a = b\cdot a+c\cdot a$ – дистрибутивность операции умножения относительно сложения.

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

Замечания

1) Исследуются и неассоциативные кольца. Например, если вместо ассоциативности R_2) умножение удовлетворяет *тождеству Якоби*

$$a(bc) + b(ca) + c(ab) = 0$$

для всех a, b, $c \in R$ и

$$ab = -ba$$

для всех a, $b \in R$, то такое кольцо называется *кольцом Ли.*

2) Когда рассматриваются кольца с единицей, почти всегда исключается случай $0 = 1$.

Сформулируем ряд простейших следствий из определения кольца, хорошо известных для чисел.

Основные свойства кольца. Пусть R – произвольное кольцо. Тогда для любых элементов a, b, $c \in R$ выполняются равенства:

1) $a \cdot 0 = 0 \cdot a = 0$;

2) $(-a) \cdot b = a \cdot (-b) = -(ab)$, $(-a) \cdot (-b) = ab$;

3) $a(b-c) = a \cdot b - a \cdot c$ (разность $a-b$ в кольце R определяется как единственное решение $a + (-b)$ уравнения $b + x = a$ в аддитивной группе $(R; +)$).

Приведем **примеры** колец.

1. Примерами коммутативных колец с единицей являются числовые кольца $(\mathbb{Z}; +, \cdot)$, $(\mathbb{Q}; +, \cdot)$, $(\mathbb{R}; +, \cdot)$.

2. *Кольцо $\mathbb{Z}_m$ классов вычетов по модулю m*, где m – натуральное число. В § 4 определены операции сложения и умножения в этом кольце (формулы (3)) и аддитивная группа.

3. *Кольцо многочленов* $\mathbb{R}[x]$ с действительными коэффициентами. Рассмотрим всевозможные *многочлены*

$$f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n, \quad n \geq 0,$$

относительно *переменной* x с *коэффициентами* $a_0, ..., a_n$ из $\mathbb{R}$; если $a_n \neq 0$, то n называется *степенью* многочлена $f(x)$. Предполагается, что $ax = xa$ для любого $a \in \mathbb{R}$. Если $g(x) = b_0 + b_1 x + \ldots + b_m x^m$, то *сумма* $h(x) = = f(x) + g(x)$ означает многочлен

$$h(x) = (a_0 + b_0) + (a_1 + b_1)x + ... + (a_k + b_k)x^k,$$

где $k = \max(n, m)$ и где коэффициенты a_i или b_i предполагаются равными 0, если индекс i больше, чем степень соответствующего многочлена.

Умножение $f(x)$ и $g(x)$ определяется по правилу:

$$q(x) = f(x)g(x) = a_0b_0 + (a_1b_0 + a_0b_1)x + \cdots = \sum_{i=0}^{n+m} x^i \sum_{j=0}^{i} a_j\, b_{i-j}$$

(отсутствующие коэффициенты также полагаются равными нулю). С левыми частями написанных выражений нужно действовать так как учили в школе: раскрыть скобки и привести подобные.

Из определения сложения (коэффициенты складываются по отдельности при разных степенях) видно, что коммутативность и ассоциативность сложения следует из коммутативности и ассоциативности сложения в $\mathbb{R}$. Противоположный многочлен получается переменой знаков у всех коэффициентов. Поэтому многочлены по сложению образуют группу.

Ассоциативность умножения многочленов следует из ассоциативности умножением в $\mathbb{R}$. Дистрибутивность также легко проверяется по формуле умножения многочленов: подставим в формулу вместо b_j выражение $c_j + d_j$ и затем воспользуемся дистрибутивностью в кольце $\mathbb{R}$:

$$\sum_{j=0}^{i} a_j\, b_{i-j} = \sum_{j=0}^{i} a_j\, (c_{i-j} + d_{i-j}) = \sum_{j=0}^{i} a_j\, c_{i-j} + \sum_{j=0}^{i} a_j\, d_{i-j}.$$

4. *Матричное кольцо* $M_n(\mathbb{R})$ всех квадратных матриц порядка n с действительными элементами является примером некоммутативного кольца ($n \geq 2$) с единицей.

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

6. Любую аддитивную группу R можно превратить в кольцо, если задать на ней нулевое умножение: $a \cdot b = 0$ для любых a, b.

В кольцах с единицей особо выделяют обратимые элементы. Элемент a кольца R называется *обратимым*, если для него в полугруппе $(R;\,\cdot)$ существует обратный элемент a^{-1}, в противном случае a называется *необратимым.* Множество всех обратимых элементов кольца R с единицей образует группу относительно операции умножения. Она называется *мультипликативной группой кольца* и обозначается R^*.

Примером мультипликативной группы кольца может служить группа $\mathbb{Z}^* = \{-1,\,1\}$.

В отличии от числовых колец некоторые нечисловые кольца содержат так называемые делители нуля.

Если R – кольцо, $a,\,b \in R$ и $a \neq 0,\,b \neq 0$, но $ab = 0$, то элемент a называется *левым делителем нуля* в R, а элемент b называется *правым делителем нуля* в R. В коммутативных кольцах, естественно, нет различия между левым и правым делителями нуля.

Коммутативные кольца без делителей нуля называют *областями целостности.*

Примером кольца с делителями нуля может служить кольцо матриц $M_n(\mathbb{R})$. В нем матрицы $A = \begin{pmatrix} a & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & b \end{pmatrix}$ при $a \neq 0,\,b \neq 0$ – делители нуля.

В любом кольце R множество обратимых элементов и множество делителей нуля не пересекаются.

Подмножество S кольца $(R;\,+,\cdot)$ замкнутое относительно операций $+,\cdot$ в R и являющееся кольцом относительно этих операций, называют *подкольцом* кольца R. Подкольцо назы-

вается *собственным*, если оно не совпадает с самим кольцом.

Для того чтобы убедиться, что некоторое непустое подмножество S кольца R является подкольцом, входящие в определение кольца требования ассоциативности, коммутативности и дистрибутивности операций проверять не требуется, поскольку они выполняются для любых элементов из R, а значит, и из S. Поэтому достаточно проверить лишь замкнутость множества S относительно сложения, умножения и взятия противоположного элемента.

Примеры подколец.

1. Кольцо $\mathbb{Z}$ является подкольцом кольца $\mathbb{Q}$.

2. Кольцо $2\mathbb{Z}$ четных целых чисел является подкольцом кольца $\mathbb{Z}$.

3. Множество S всех матриц вида $\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix}$ с произвольными элементами a_i из поля $\mathbb{R}$ является подкольцом кольца $M_n(\mathbb{R})$ всех матриц порядка n над $\mathbb{R}$.

4. Множество L всех матриц вида $\begin{pmatrix} a & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix}_{n\times n}$ с любым a из поля $\mathbb{R}$ является подкольцом кольца $M_n(\mathbb{R})$ и подкольцом кольца S.

Заметим, что подкольцо кольца с единицей может не иметь единицы. Таким является подкольцо из примера 2. С другой стороны, подкольцо L из примера 4 имеет единицу

$E_L = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix}$, которая при $n > 1$ отлична от единицы E самого кольца $M_n(\mathbb{R})$. Подкольцо $\mathbb{Z}$ кольца $\mathbb{Q}$ имеет ту же единицу, что и исходное кольцо.

Примеры решения задач

Задача 1. Доказать, что для любых элементов a, b, c произвольного кольца R выполняются равенства:

1) $a \cdot 0 = 0 \cdot a = 0$;
2) $(-a) \cdot b = a \cdot (-b) = -(ab)$, $(-a) \cdot (-b) = ab$;
3) $a(b - c) = a \cdot b - a \cdot c$.

Доказательство. 1) Так как $0 + 0 = 0$ по определению нулевого элемента кольца, то $a \cdot 0 = a(0 + 0)$, и в силу свойства дистрибутивности имеем:

$$a \cdot 0 = a \cdot 0 + a \cdot 0.$$

Прибавим к обеим частям этого равенства элемент $-(a \cdot 0)$, получим $a \cdot 0 = 0$. Аналогично доказывается и второе равенство $0 \cdot a = 0$.

2) По определению противоположного элемента для элемента $a \cdot b$ в кольце R имеем: $-(a \cdot b)$ есть решение уравнения

$$a \cdot b + x = 0,$$

и оно единственно (см. § 4, основные свойства группы). Поэтому для доказательства равенства $(-a) \cdot b = -(a \cdot b)$ достаточно показать, что этому уравнению удовлетворяет элемент $(-a) \cdot b$. Последний факт устанавливается непосредственной проверкой с использованием свойства 1):

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

Аналогичным образом доказывается и равенство $a \cdot (-b) = -(ab)$.

Воспользовавшись доказанными равенствами, получим:

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

Здесь мы воспользовались также тем, что если $-a$ элемент, противоположный для a, то a – противоположный для $-a$. Этот факт следует непосредственно из определения противоположного элемента.

3) Это свойство доказывает следующая цепочка равенств:

$$a(b-c) = a(b+(-c)) = a \cdot b + a \cdot (-c) = a \cdot b + (-(a \cdot c)) = a \cdot b - a \cdot c.$$

□

Задача 2. Является ли кольцом множество L чисел вида $a + b\sqrt{3}$, где $a, b \in \mathbb{Z}$, относительно обычных операций сложения и умножения?

Решение. Рассмотрим сумму и произведение двух чисел указанного вида:

$$(a + b\sqrt{3}) + (c + d\sqrt{3}) = (a + c) + (b + d)\sqrt{3};$$

$$(a + b\sqrt{3}) \cdot (c + d\sqrt{3}) = (ac + 3bd) + (ad + bc)\sqrt{3}.$$

Мы видим, что числа, полученные в результате выполнения операций, снова принадлежат множеству L, т.е. множество L замкнуто относительно сложения и умножения.

Известно, что на всех числовых множествах обычные операции сложения и умножения являются коммутативными и ассоциативными. Кроме того, умножение дистрибутивно относительно сложения. Значит, и на множестве L сложение и умножение коммутативны, ассоциативны и связаны законом дистрибутивности.

Нейтральным элементом по сложению здесь является число $0 = 0 + 0\sqrt{3} \in L$, по умножению – $1 = 1 + 0\sqrt{3} \in L$.

Противоположным к элементу $a + b\sqrt{3}$ служит элемент $-a + (-b)\sqrt{3} \in L$: $a + b\sqrt{3} + \left(-a + (-b)\sqrt{3}\right) = (a + (-a)) + (b + (-b))\sqrt{3} = 0 + 0\sqrt{3}$.

Все перечисленное выше позволяет сделать вывод, что L, согласно определению, является коммутативным кольцом с единицей. □

Задача 3. Докажите, что если на $\mathbb{Z}$ задана операция формулой

$$a \odot b = -ab,$$

то алгебраическая система $(\mathbb{Z};\, +,\, \odot)$ является коммутативным кольцом с единицей.

Доказательство. Целые числа по сложению образуют абелеву группу, поэтому нам достаточно проверить свойства $\mathbb{Z}$ относительно умножения $\odot$.

Следующие равенства доказывают ассоциативность умножения $\odot$:

$$a \odot (b \odot c) = a \odot (-bc) = -(a \cdot (-bc)) = abc;$$

$$(a \odot b) \odot c = (-ab) \odot c = -((-ab) \cdot c) = abc.$$

Кроме того,

$$a \odot b = -ab = -ba = b \odot a;$$

$$a \odot (b + c) = -(a \cdot (b + c)) = -ab + (-ac) = a \odot b + a \odot c.$$

Откуда следует, что $(\mathbb{Z};\, +,\, \odot)$ – коммутативное кольцо.

Единичный элемент e кольца найдем из условия $a \odot e = a$:

$$-ae = a;$$

$$e = -1.$$

Следовательно, $(\mathbb{Z}; +, \odot)$ – коммутативное кольцо с единицей. $\square$

Упражнения для самостоятельной работы

5.1. Выяснить, образует ли кольцо относительно обычных сложения и умножения:

а) множество $\mathbb{N}$;

б) множество $\mathbb{Z}$;

в) множество $\mathbb{Q}$;

г) множество всех нечетных чисел;

д) множество всех четных чисел;

е) множество неотрицательных целых чисел;

ж) множество чисел вида $a + b\sqrt[3]{5}$, где a, b – целые числа;

з) множество комплексных чисел вида $a + bi$, где a, b – целые числа (множество целых гауссовых чисел);

и) множество чисел вида $a+b\sqrt{3}+c\sqrt{5}$, где a, b, c – целые числа;

к) множество чисел вида $a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15}$, где a, b, c, d – целые числа.

5.2. Выясните, дистрибутивна ли операция $*$ относительно операции $\circ$, если $*$ является операцией возведения в степень на множестве $\mathbb{N}$, а $\circ$ – операцией умножения на том же множестве, т.е. $a * b = a^b$, $a \circ b = a \cdot b$, где a, b – любые элементы из $\mathbb{N}$.

5.3. Проверьте, дистрибутивна ли вторая операция относительно первой:

а) $(\mathbb{N}; +, \otimes)$, где $a \otimes b = (ab)^2$;

б) $(\mathbb{Z}; -, \cdot)$;

в) $(2^M; \oplus, *)$, где $\oplus$ и $*$ – одна из операций: $\cup, \cap, \triangle$ (здесь символ $\triangle$ обозначает симметрическую разность двух множеств, которая определяется формулой $A \triangle B = (A \cup B) \setminus (A \cap B)$).

5.4. Справедливы ли формулы сокращенного умножения для элементов некоммутативных колец?

5.5. Выясните, являются ли кольцами относительно матричного сложения и умножения следующие множества матриц с действительными элементами:

а) множество диагональных матриц порядка $n \geq 2$, т.е. матриц вида

$$\begin{pmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_n \end{pmatrix};$$

б) множество всех матриц вида

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix};$$

в) множество всех матриц вида

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix};$$

г) множество треугольных матриц порядка $n \geq 2$, т.е. матриц вида

$$\begin{pmatrix} a_{11} & 0 & \dots & 0 \\ a_{21} & a_{22} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix};$$

д) множество матриц вида

$$\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix}.$$

5.6. Докажите, что множество M матриц вида $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, где a, b – любые действительные числа, составляет коммутативное кольцо относительно матричного сложения и умножения. Выделите мультипликативную группу этого кольца.

5.7. Какие элементы кольца называются делителями нуля? Выясните, имеет ли кольцо M вещественных матриц вида $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ делители нуля?

5.8. Докажите, что если M – коммутативная группа относительно операции сложения, такая, что $ab = 0$ для любых a, b и нулевого элемента 0 группы M, то алгебраическая система $M = (M; +, \cdot)$ является кольцом.

5.9. На множестве $A = \mathbb{Q}^2$ упорядоченных пар (a, b) рациональных чисел сложение $\oplus$ и умножение $\odot$ определены следующими правилами:

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

Покажите, что $(A; \oplus, \odot)$ является коммутативным кольцом с единицей и с делителями нуля.

5.10. Выясните, является ли система $(\mathbb{Z}; \oplus, \cdot)$ кольцом относительно обычного умножения и операции сложения $\oplus$, выполняемой по правилу:

$$a \oplus b = \begin{cases} a + b, & \text{если } a \text{ – четное число, } b \text{ – любое целое число,} \\ a - b, & \text{если } a \text{ – нечетное число, } b \text{ – любое целое число.} \end{cases}$$

5.11. Покажите, что в определении:

а) кольца аксиома коммутативности сложения выводится из остальных аксиом;

б) кольца без единицы аксиома коммутативности сложения не выводится из остальных аксиом.

5.12. Сколькими способами на множестве из двух элементов можно определить две бинарные операции «сложения» и «умножения» так, чтобы получилось кольцо без единицы?

5.13. Сколькими способами на множестве a, b, c можно определить две бинарные операции «сложения» и «умножения» так, чтобы получилось кольцо без единицы, и роль нуля в нем играл элемент a?

5.14. Докажите, что если элемент a перестановочен с элементами b и c кольца, то a перестановочен с $-b$, ab, b^{-1} (если он существует), $b + c$ и bc.

Примером неассоциативного кольца служит кольцо векторов трехмерного евклидова пространства, в котором операциями служат обычные сложение и векторное произведение.

Хорошо известно, что в этом кольце для любых его элементов выполняются следующие соотношения:

$$a^2 = 0, \tag{1}$$

$$(ab)c + (bc)a + (ca)b = 0 \quad (\textit{тождество Якоби}). \tag{2}$$

Всякое кольцо, удовлетворяющее условиям (1) и (2) называется *лиевым кольцом*.

5.15. Докажите, что:

а) из вышеприведенного условия (1) вытекает *закон антикоммутативности* $ba = -ab$;

б) если R – произвольное ассоциативное кольцо, то, сохраняя аддитивную группу этого кольца, а операцию умножения ab заменяя *операцией коммутирования* $a \circ b = ab - ba$, получим лиево кольцо;

в) всякое лиево ненулевое кольцо является кольцом без единицы.

5.16. Охарактеризуйте все подкольца кольца $(\mathbb{Z}; +, \cdot)$ целых чисел.

5.17. Докажите, что множество L матриц вида $\begin{pmatrix} a & b \\ 5b & a \end{pmatrix}$, $a, b \in \mathbb{Q}$ является подкольцом кольца $M_2(\mathbb{R})$ всех вещественных матриц порядка 2.

5.18. В кольце $M_2(\mathbb{R})$ укажите несколько подмножеств, которые являются его подкольцами.

5.19. Докажите, что подкольцо кольца $M_2(\mathbb{Z})$, содержащее матрицы $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ и $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, совпадает со всем кольцом $M_2(\mathbb{Z})$.

§ 6. Поля

Полем называется непустое множество P с бинарными алгебраическими операциями сложения $+$ и умножения $\cdot$, удовлетворяющими условиям (аксиомам поля):

P_1) $(P; +)$ является абелевой группой.

P_2) $(P^*; \cdot)$ является абелевой группой. (Здесь $P^* = P \setminus \{0\}$, где 0 обозначает нейтральный элемент относительно сложения.)

P_3) Для любых элементов a, b, $c \in P$ выполняется аксиома дистрибутивности: $a \cdot (b + c) = a \cdot b + a \cdot c$.

Другими словами, полем называется коммутативное кольцо с единицей 1, отличной от 0, в котором любой ненулевой элемент обратим.

Так как поля являются кольцами, то они обладают всеми общими свойствами колец. Вместе с тем, для полей могут выполняться и такие свойства, которыми обладают не все кольца.

Основные свойства полей

1) Если P – поле, то уравнение $ax = b$, где $a \neq 0$, имеет единственное решение: $x = a^{-1}b$.

2) В поле нет делителей нуля, т.е.

$$a \cdot b = 0 \Leftrightarrow a = 0 \text{ или } b = 0.$$

Замечание

Обратное утверждение неверно. В кольце $\mathbb{Z}$ целых чисел нет делителей нуля, но оно не является полем.

Аксиомы поля позволяют выполнять арифметические операции аналогично тому, как это делается с числами. Это

неудивительно, так как рациональные, действительные и комплексные числа дают самые простые и самые важные примеры полей. Но этими примерами возможные поля далеко не исчерпываются.

Приведем еще **примеры** полей.

1. Поле классов вычетов $\mathbb{Z}_p$, где p – простое число.

2. В качестве примера нечислового поля построим поле из двух элементов 0, 1, заданными таблицами:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

В этом «самом маленьком» поле 0 является нулем, а 1 – единицей.

3. Произвольное конечное коммутативное кольцо без делителей нуля является полем.

4. Отрицательный пример: кольцо целых чисел $\mathbb{Z}$ не является полем, так как в нем обратимы только ± 1.

В следующем параграфе мы познакомимся еще с одним примером поля.

Для любых элементов a и $b \neq 0$ поля P элемент $a^{-1} \cdot b$ называется *отношением* этих элементов и записывается в виде $\dfrac{a}{b}$. Таким образом, в любом поле выполнимы сложение, умножение, вычитание любых элементов и деление любого элемента на любой ненулевой элемент. Относительно операции деления выполняются все привычные свойства числовых дробей:

1) $\dfrac{a}{b} = \dfrac{c}{d} \Leftrightarrow ad = bc$ (условие равенства дробей);

2) $\dfrac{ac}{bc} = \dfrac{a}{b}$ (основное свойство дроби);

3) $\dfrac{a}{b} \pm \dfrac{c}{d} = \dfrac{ad \pm bc}{bd}$ (правило сложения дробей);
4) $\dfrac{a}{b} \cdot \dfrac{c}{d} = \dfrac{ac}{bd}$ (правило умножения дробей).

Если в кольце единицы может и не быть, то в поле ее наличие гарантировано определением поля. Пусть 1 – единица поля P. Рассмотрим в поле P множество кратных единицы:

$$\begin{aligned} &1 = 1, \\ &2 = 1 + 1, \\ &\ldots\ldots\ldots\ldots \\ &p = \underbrace{1 + 1 + \ldots + 1}_{p \text{ раз}}. \end{aligned}$$

Если для любого натурального числа p сумма p единиц равна 0, то говорят, что поле P имеет *характеристику* p и обозначают $\operatorname{char} P = p$. Если такого числа p не существует, то считается, что характеристика поля P равна 0.

Например, характеристика любого числового поля равна нулю. Поле классов вычетов $\mathbb{Z}_p$ (p – простое число) имеет характеристику, равную p. Характеристика построенного выше поля из двух элементов равна 2.

Если $\operatorname{char} P = p$, то для любого $a \in P$

$$\underbrace{a + a + \ldots + a}_{p \text{ раз}} = 0.$$

Несложно доказать, что характеристика поля, если она положительна, всегда является простым числом.

Замечание

Большинство формул элементарной алгебры справедливы в любом поле, так как при их выводе используются только те свойства операций сложения и умножения, которые входят в число аксиом поля или являются их следствием. Особенность

полей положительной характеристики проявляется только в тех формулах, которые содержат умножение или деление на натуральные числа.

Рассмотрим, например, формулу

$$(a+b)^2 = a^2 + 2ab + b^2.$$

Она справедлива в любом поле, если понимать $2ab$ как $ab + ab$. Однако, в поле характеристики 2 она принимает более простой вид

$$(a+b)^2 = a^2 + b^2.$$

В общем случае в поле характеристики p справедливо тождество

$$(a+b)^p = a^p + b^p.$$

Подмножество F поля P, замкнутое относительно операций, определенных в поле P, и являющееся полем относительно этих операций, называют *подполем* поля P. При этом P называется *расширением* поля F.

Например, поле $\mathbb{Q}$ является подполем поля действительных чисел $\mathbb{R}$, а оно в свою очередь является подполем поля комплексных чисел $\mathbb{C}$.

Числовым полем называется всякое подполе поля комплексных чисел.

Если F – подполе поля P, то единица поля F совпадает с единицей поля P и для элемента $a \neq 0$ из F обратный элемент в F и в P – один и тот же.

Примеры решения задач

Задача 1. Доказать, что для любых элементов a, b поля P:

1) $a \cdot b = 0 \Leftrightarrow a = 0$ или $b = 0$;

2) уравнение $ax = b$, где $a \neq 0$, имеет единственное решение: $x = a^{-1}b$.

Доказательство. 1) Пусть $a \cdot b = 0$. Предположим, что $a \neq 0$, тогда a обратим. Умножим обе части равенства на a^{-1} слева: $a^{-1}(ab) = a^{-1} \cdot 0$. Откуда получим $b = 0$. Обратно, если $a = 0$ или $b = 0$, то по свойствам кольца $a \cdot b = 0$.

2) Непосредственной проверкой можно убедиться, что $x = a^{-1}b$ является решением уравнения $ax = b$. Если x_1, x_2 – два его решения, то $ax_1 = ax_2$, и, умножив обе части последнего равенства на a^{-1}, получим $x_1 = x_2$. □

Задача 2. Образует ли поле относительно операций сложения и умножения матриц множество M матриц вида $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, где a, b – любые действительные числа.

Решение. Пусть A, B – любые матрицы из множества M и $A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ и $B = \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}$. Тогда сумма матриц $A + B = \begin{pmatrix} a+c & 0 \\ 0 & b+d \end{pmatrix}$ и произведение $AB = \begin{pmatrix} ac & 0 \\ 0 & bd \end{pmatrix}$ также принадлежат множеству M. Значит, множество M замкнуто относительно матричного сложения и умножения.

Из теории матриц известно, что на множестве квадратных матриц одного и того же порядка, а значит, и на множестве M, сложение коммутативно, сложение и умножение ассоциативны и умножение дистрибутивно относительно сложения.

Нулевым элементом множества M является матрица $\Theta = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, а противоположным к $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ матрица $\begin{pmatrix} -a & 0 \\ 0 & -b \end{pmatrix}$, снова принадлежащая множеству M.

Кроме того, $BA = \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} \cdot \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} ca & 0 \\ 0 & db \end{pmatrix} = \begin{pmatrix} ac & 0 \\ 0 & bd \end{pmatrix} = AB$, т.е. умножение в M коммутативно. Таким образом, множество матриц M образует коммутативное кольцо.

Выясним, является ли множество M полем. Единичным элементом множества M является единичная матрица $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Для существования обратной для матрицы $A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ необходимо и достаточно, чтобы матрица A была невырожденной. Так как $A \neq \Theta$, то хотя бы одно из чисел a, b отлично от нуля. Определитель матрицы $|A| = ab$ может равняться нулю и в том случае, когда одно из чисел a, b отлично от нуля, т.е. матрица A может быть ненулевой и в то же время вырожденной. Такими являются матрицы вида $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ и $\begin{pmatrix} 0 & 0 \\ 0 & b \end{pmatrix}$, где числа a и b отличны от нуля. В этом случае, когда матрица A имеет такой вид, обратной для нее не существует. Следовательно, множество M полем не является. □

Задача 3. Доказать, что множество M матриц вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, где a и b – любые действительные числа, является полем относительно матричного сложения и умножения. Найти характеристику этого поля.

Доказательство. Рассмотрим сумму и произведение двух матриц $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$ данного множества: $A + B = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix}$, $AB = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}$.

Видим, что $A+B \in M$, $AB \in M$. Как и выше, свойства коммутативности сложения, ассоциативности сложения и умножения и дистрибутивности умножения относительно сложения на множестве матриц одного и того же порядка считаем известными. Нулевым элементом множества M является нулевая матрица Θ, а противоположным к $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ – матрица $\begin{pmatrix} -a & -b \\ b & -a \end{pmatrix}$ из множества M.

Умножение в M коммутативно, так как

$$BA = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \cdot \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} ca-db & cb+da \\ -(da+cb) & ca-db \end{pmatrix} =$$

$$= \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = AB.$$

Единичная матрица E является нейтральным элементом по умножению во множестве M. Вычислим определитель матрицы A: $|A| = a^2+b^2 \neq 0$, т.е. матрица A является невырожденной, а значит, она имеет обратную матрицу A^{-1}. Покажем, что эта матрица также принадлежит множеству M. Имеем:

$$A^{-1} = \frac{1}{a^2+b^2}\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} \dfrac{a}{a^2+b^2} & -\dfrac{b}{a^2+b^2} \\ \dfrac{b}{a^2+b^2} & \dfrac{a}{a^2+b^2} \end{pmatrix} \in M.$$

Из приведенных выше результатов следует, что M – поле.

Найдем характеристику поля M. Единичная матрица $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ – единица поля M. Очевидно, что не существует

натурального числа p такого, что

$$\underbrace{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}+\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}+\ldots+\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}}_{p\text{ раз}}=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}.$$

А это значит, что характеристика поля M равна нулю. □

Упражнения для самостоятельной работы

6.1. Какие из колец в задачах 5.1, 5.5 являются полями?

6.2. Какие из следующих множеств матриц образуют поле относительно матричного сложения и умножения:

а) $\begin{pmatrix}a & b\\ nb & a\end{pmatrix}$, где n – фиксированное целое число, $a,\ b\in\mathbb{Q}$;

б) $\begin{pmatrix}a & b\\ nb & a\end{pmatrix}$, где n – фиксированное целое число, $a,\ b\in\mathbb{R}$;

в) $\begin{pmatrix}a & b\\ nb & a\end{pmatrix}$, $a,\ b\in\mathbb{Z}_p\quad (p=2,\ 3,\ 5,\ 7)$?

6.3. Докажите, что алгебраическая система – множество $\mathbb{Q}$ рациональных чисел с обычной операцией сложения и операцией $\circ$, выполняемой по правилу $a\circ b=\dfrac{a\cdot b}{2}$ для любых элементов из $\mathbb{Q}$, – является полем. Каков единичный элемент этого поля?

6.4. Докажите, что множество матриц $\begin{pmatrix}a & 0\\ 0 & a\end{pmatrix}$, где a – любое рациональное (или действительное) число, является полем относительно матричного сложения и умножения. Будет ли множество матриц данного вида составлять поле, если a – любое целое число?

6.5. Почему кольцо $\{0\}$ не является полем?

6.6. На множестве $M=\{a,\ b\}$ сложение $\oplus$ и умножение

$\odot$ определены следующим образом:

$$a \oplus a = a, \quad a \oplus b = b \oplus a = b, \quad b \oplus b = a,$$
$$a \odot a = b, \quad a \odot b = b \odot a = a, \quad b \odot b = b.$$

Выясните, обладает ли это множество нулем и единицей и являются ли система $(M;\, \oplus,\, \odot)$ полем относительно заданных бинарных операций.

6.7. Докажите, что если B – множестве пар $(a,\, b)$ рациональных чисел и на B две бинарные операции – сложение $\oplus$ и умножение $\odot$ – определены следующими условиями:

$$(a,\, b) \oplus (c,\, d) = (a+c,\, b+d), \quad (a,\, b) \odot (c,\, d) = (ac+2bd,\, ad+bc),$$

то система $(B;\, \oplus,\, \odot)$ является полем, а пары $(0,\, 0)$ и $(1,\, 0)$ соответственно нулем и единицей этого поля.

6.8. В поле матриц вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, где a и b – любые действительные числа, укажите такие его подмножества, которые являются полями.

6.9. Докажите, что множество $\mathbb{Q}[\sqrt{5}]$ чисел вида $a + b\sqrt{5}$, где a, b – любые рациональные числа, является числовым полем.

6.10. Покажите, что числа вида $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ с рациональными a, b, c образуют поле. Найдите в этом поле элемент, обратный числу $1 - \sqrt[3]{2} + 2\sqrt[3]{4}$.

6.11. Докажите, что в поле $M = (M;\, +,\, \cdot)$, где M – множество всех матриц вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ с действительными a и b; $+$, $\cdot$ – обычные матричные операции, существует элемент X такой, что $X^2 = -E$ (E – единичный элемент поля M).

6.12. Докажите, что не существует полей, характеристикой которых была бы единица или какое-либо составное натуральное число.

6.13. Для каких чисел $n = 2, 3, 4, 5, 6, 7$ существует поле из n элементов?

6.14. В поле $\mathbb{Z}_7$ решите уравнения $2x = 3$, $3x = 3$, $3x = 2$, $5x^2 - 2 = 0$. Решите эти же уравнения в полях $\mathbb{Z}_5$ и $\mathbb{Z}_{17}$.

6.15. Решите систему уравнений

$$\begin{cases} x + 2z = 1, \\ y + 2z = 2, \\ 2x + z = 1 \end{cases}$$

в поле вычетов по модулю 5 и модулю 7.

6.16. Докажите, что конечное коммутативное кольцо без делителей нуля, содержащее более одного элемента, является полем.

6.17. Докажите, что кольцо вычетов по модулю m будет полем тогда и только тогда, когда m – простое число.

6.18. Ассоциативное кольцо с единицей, в котором каждый ненулевой элемент обратим, называется *телом*. Иными словами, тело – «некоммутативное поле». Докажите, что кольцо R будет телом тогда и только тогда, когда для любого $a \neq 1$ найдется элемент $b \in R$ такой, что

$$a + b - ab = b + a - ba = 0.$$

§ 7. Комплексные числа

Неразрешимость уравнения

$$x^2 + 1 = 0$$

в поле действительных чисел приводит к необходимости расширить его до большего поля, называемого полем комплексных чисел.

Построим поле комплексных чисел исходя из двух требований: чтобы оно содержало подполе $\mathbb{R}$ и чтобы в нем извлекался корень квадратный из числа -1 (т.е. существовало такое число i, что $i^2 = -1$).

В качестве исходного множества возьмем множество упорядоченных пар действительных чисел

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

Две пары (a, b), (c, d) считаются *равными*, что записывается в виде $(a, b) = (c, d)$, в том и только том случае, когда $a = c,\ b = d$.

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

$$(a, b) + (c, d) = (a + c,\ b + d), \tag{1}$$

$$(a, b) \cdot (c, d) = (ac - bd,\ ad + bc). \tag{2}$$

Множество $\mathbb{C}$ с операциями, определенными равенствами (1), (2), является полем.

Это поле $\mathbb{C}$ называется *полем комплексных чисел*, а его элементы, т.е. пары (a, b) – *комплексными числами.* Заметим, что нулевым элементом поля $\mathbb{C}$ является пара $(0, 0)$, а единицей – пара $(1, 0)$. Противоположным элементом для (a, b) является пара $(-a, -b)$, а обратным для $(a, b) \neq (0, 0)$ –

пара $\left(\dfrac{a}{a^2+b^2}, -\dfrac{b}{a^2+b^2}\right)$ (которую находим из уравнения $(a,b)(x,y)=(1,0)$).

Рассмотрим в $\mathbb{C}$ подмножество M пар вида (a,b), где a – любое число из $\mathbb{R}$:

$$M=\{(a,0)|\, a\in\mathbb{R}\}.$$

Множество M замкнуто относительно операций $+$, $\cdot$ в $\mathbb{C}$, так как:

$$(a,0)+(b,0)=(a+b,0),\quad (a,0)\cdot(b,0)=(a\cdot b,0).$$

Из последних равенств следует не только замкнутость, но и тот факт, что операции над элементами из M производятся точно так же, как и над действительными числами – первыми компонентами пар. Элементы из M лишь обозначениями отличаются от действительных чисел. Поэтому естественно отождествлять пару $(a,0)$ с действительным числом a и включить поле $\mathbb{R}$ в качестве подполя в поле $\mathbb{C}$.

Обозначим

$$(0,1)=i,$$

тогда

$$(0,1)(0,1)=(-1,0)=-1,$$

т.е. $i^2=-1$.

Таким образом, построено поле, которое содержит в себе поле $\mathbb{R}$ и в котором разрешимо уравнение $x^2=-1$, т.е. возможно извлечение квадратного корня из -1. Решениями этого уравнения являются числа i и $-i$.

Для любых a, $b\in\mathbb{R}$ имеем

$$(a,b)=(a,0)+(0,b)=(a,0)+(b,0)(0,1)=a+bi.$$

Представление комплексного числа $z \in \mathbb{C}$ в виде $a + bi$ $(a, b \in \mathbb{R})$ называется его *алгебраической формой*. При этом число a называется *действительной частью* числа z и обозначается $\operatorname{Re} z$, число b называется *мнимой частью* числа z и обозначается $\operatorname{Im} z$. Само число i называется *мнимой единицей*. Комплексные числа вида bi, где $b \in \mathbb{R}$, называются *чисто мнимыми*.

В новых обозначениях равенства (1), (2), определяющие операции $+$, $\cdot$ в $\mathbb{C}$ над комплексными числами, примут вид:

$$(a + bi) + (c + di) = (a + c) + (b + d)i, \tag{3}$$

$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i. \tag{4}$$

Учитывая, что для числа $c + di$ противоположным является число $-c - di$, а обратным при $c + di \neq 0$ – число $\dfrac{c}{c^2 + d^2} - \dfrac{d}{c^2 + d^2}i$, можно в новой форме записать правила вычитания и деления комплексных чисел:

$$(a + bi) - (c + di) = (a - c) + (b - d)i, \tag{5}$$

$$\frac{a + bi}{c + di} = \frac{ac + bd}{c^2 + d^2} - \frac{ad - bc}{c^2 + d^2}i \quad (c + di \neq 0). \tag{6}$$

Всякое комплексное число можно изобразить точкой или вектором на плоскости. А именно, число $z = a + bi$ можно изобразить в прямоугольной системе координат точкой $M(a, b)$ или вектором, выходящим из точки $(0, 0)$ в точку $M(a, b)$ (рис. 4). И наоборот, каждую точку $M(a, b)$ координатной плоскости можно рассматривать как образ комплексного числа $z = a + bi$.

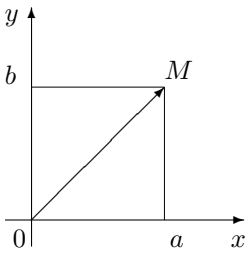


Рис. 4

Плоскость, на которой изображаются комплексные числа, называется *комплексной плоскостью.* Ось абсцисс называется *действительной осью*, так как на ней лежат действительные числа $z = a + 0i$. Ось ординат называется *мнимой осью*, на ней лежат чисто мнимые комплексные числа $z = 0 + bi$.

Иногда удобнее использовать представление комплексных чисел точками, иногда векторами. При векторном представлении сложение комплексных чисел имеет ясную геометрическую интерпретацию. Сложению комплексных чисел соответствует сложение векторов по правилу параллелограмма (рис. 5).

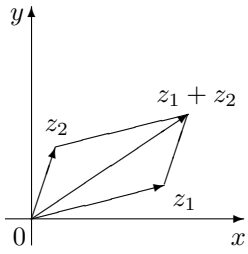


Рис. 5

Два комплексных числа $z = a + bi$ и $\overline{z} = a - bi$, отличающиеся только знаком мнимой части, называются *со-*

пряженными. На комплексной плоскости сопряженным комплексным числам соответствуют точки, симметричные относительно действительной оси (рис. 6).

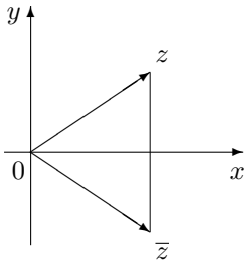


Рис. 6

Очевидно, что $\overline{\overline{z}} = z$. Соотношения

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}, \qquad \overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$$

непосредственно следуют из формул (3) и (4). Частным случаем этих формул являются так же утверждения о сумме и произведении числа z и сопряженного с ним числа $\overline{z}$:

$$z + \overline{z} = 2a, \qquad z \cdot \overline{z} = a^2 + b^2.$$

Вместо декартовых координат на плоскости иногда бывает удобнее использовать полярные (рис. 4). Это приводит к следующим понятиям. Длина вектора $\vec{r}$, изображающего комплексное число z, называется *модулем* этого числа и обозначается $|z|$ или r. Ясно, что

$$|z| = \sqrt{a^2 + b^2}.$$

Величина угла между положительным направлением действительной оси и вектором $\vec{r}$ называется *аргументом* комплексного числа и обозначается $\arg z$ или φ. Аргумент комплексного числа $z = 0$ не определен. Аргумент комплексного

числа $z \neq 0$ – величина многозначная и определяется с точностью до слагаемого $2\pi k$ $(k \in \mathbb{Z})$.

Из соотношений в прямоугольном треугольнике следует:

$$a = r\cos\varphi, \qquad b = r\sin\varphi,$$

откуда

$$z = a + bi = r(\cos\varphi + i\sin\varphi).$$

Такое представление комплексного числа называется его *тригонометрической формой*.

Операции умножения и деления комплексных чисел удобно выполнять в тригонометрической форме.

$$\cos\varphi = \frac{a}{r}, \qquad \sin\varphi = \frac{b}{r}.$$

Пусть

$$z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1), \qquad z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2)$$

– два комплексных числа, заданных в тригонометрической форме. Тогда

$$z_1 z_2 = r_1 r_2(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)), \tag{7}$$

$$\frac{z_1}{z_2} = \frac{r_1}{r_2}(\cos(\varphi_1 - \varphi_2) + i\sin(\varphi_1 - \varphi_2)), \quad (z_2 \neq 0). \tag{8}$$

Из формулы (7) легко получить формулу возведения комплексного числа $z = r(\cos\varphi + i\sin\varphi)$ в степень

$$z^n = r^n(\cos n\varphi + i\sin n\varphi), \tag{9}$$

справедливую для всех $n \in \mathbb{Z}$. Эту формулу называют также *формулой Муавра* [2].

[2] А. Муавр – английский математик (1667 – 1754).

Корень n-ой степени из комплексного числа $z = r(\cos\varphi + i\sin\varphi)$ определяется как комплексное число α, удовлетворяющее условию $\alpha^n = z$. Если положить $\alpha = \rho(\cos\psi + i\sin\psi)$, то по формуле Муавра получаем

$$\alpha^n = \rho^n(\cos n\psi + i\sin n\psi) = r(\cos\varphi + i\sin\varphi).$$

Отсюда имеем:

$$\rho^n = r, \quad n\psi = \varphi + 2\pi k,$$

где k – любое целое число. Следовательно,

$$\rho = \sqrt[n]{r} \quad \text{(арифметическое значение корня)}, \quad \psi = \frac{\varphi + 2\pi k}{n}.$$

Окончательно получаем

$$\alpha_k = \sqrt[n]{z} = \sqrt[n]{r}\left(\cos\frac{\varphi + 2\pi k}{n} + i\sin\frac{\varphi + 2\pi k}{n}\right). \qquad (10)$$

Среди чисел вида (10) имеется ровно n различных комплексных чисел, они получаются при $k = 0, 1, 2, \ldots, n-1$. Они все лежат на окружности радиуса $\sqrt[n]{r}$, образуя вершины правильного n-угольника.

Так как $1 = 1(\cos 0 + i\sin 0)$, $r = 1$, $\varphi = 0$, то формула для корней n-ой степени из 1 принимает вид

$$\varepsilon_k = \sqrt[n]{1} = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, \qquad k = 0, 1, 2, \ldots, n-1. \quad (11)$$

На комплексной плоскости корни n-ой степени из 1 расположены на окружности единичного радиуса и делят ее на n равных частей, одной из точек деления служит число $\varepsilon_0 = 1$ $(k = 0)$ (рис. 7). Все комплексные корни n-ой степени из 1 расположены симметрично относительно действительной оси, т.е. попарно сопряжены. Действительные значения корня n-ой степени из 1 получаются из формулы (11) при $k = 0$, $k = n/2$, если n – четно, и при $k = 0$, если n – нечетно.

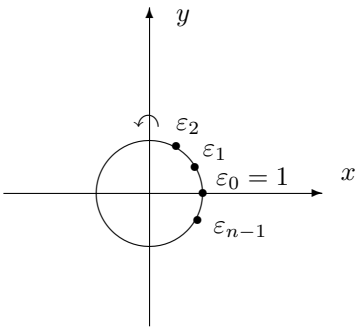


Рис. 7

Примеры решения задач

Задача 1. Выяснить при каких $x, y \in \mathbb{R}$ справедливо равенство

$$3x - 4y - (x - y)i = 3 - 2i.$$

Решение. Так как $z_1 = z_2$ ($z_1 = a_1 + b_1 i,\ z_2 = a_2 + b_2 i$) только если

$$\begin{cases} a_1 = a_2, \\ b_1 = b_2, \end{cases}$$

где $a_1 = 3x - 4y,\ a_2 = 3$ и $b_1 = -(x - y),\ b_2 = -2$, то

$$\begin{cases} 3x - 4y = 3, \\ x - y = 2; \end{cases} \quad \begin{cases} 3(y + 2) - 4y = 3, \\ x = y + 2; \end{cases} \quad \begin{cases} 3y + 6 - 4y = 3, \\ x = y + 2; \end{cases}$$

$$\begin{cases} y = 3, \\ x = y + 2. \end{cases}$$

Откуда следует, что $x = 5,\ y = 3$. □

Задача 2. Выполните действия $\dfrac{2 + i}{3 - i} + \dfrac{3 + i}{2 - i}$.

Решение. Сначала сложим дроби, приведя их к общему знаменателю, а затем выполним деление, домножив числитель и знаменатель дроби на число, сопряженное знаменателю (что позволит освободиться от мнимости в знаменателе):

$$\frac{2+i}{3-i}+\frac{3+i}{2-i}=\frac{(2+i)(2-i)+(3+i)(3-i)}{(3-i)(2-i)}=$$
$$=\frac{4-i^2+9-i^2}{6-5i+i^2}=\frac{13+2}{5(1-i)}=\frac{15}{5(1-i)}\cdot\frac{1+i}{1+i}=\frac{15(1+i)}{5(1-i^2)}=$$
$$=\frac{15}{10}(1+i)=1,5+1,5i. \square$$

Задача 3. Найти значение корня квадратного из числа $a+bi$.

Решение. Пусть $\sqrt{a+bi}=x+yi$, где x и y – неизвестные действительные числа. Возведя обе части этого уравнения в квадрат, получим:

$$a+bi=(x^2-y^2)+2xyi.$$

Последнее уравнение равносильно системе уравнений:

$$\begin{aligned} x^2-y^2&=a,\\ 2xy&=b. \end{aligned}$$

Возведем каждое уравнение в квадрат и сложим полученные уравнения. Получим:

$$(x^2+y^2)^2=a^2+b^2.$$

Отсюда имеем:

$$x^2+y^2=\sqrt{a^2+b^2},$$

где в правой части следует иметь в виду арифметический корень, так как $x^2 + y^2 \geq 0$. Учитывая, кроме того, что $x^2 - y^2 = a$, имеем:

$$x^2 = \frac{a + \sqrt{a^2 + b^2}}{2}; \quad y^2 = \frac{-a + \sqrt{a^2 + b^2}}{2}.$$

Так как $\sqrt{a^2 + b^2} > |a|$, то оба полученные числа – положительны. Извлекая из них квадратные корни, получим действительные значения для x и y:

$$x = \pm\sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}}; \quad y = \pm\sqrt{\frac{-a + \sqrt{a^2 + b^2}}{2}}.$$

Из соотношения $2xy = b$ следует, что при $b > 0$ числа x и y имеют одинаковые знаки, а при $b < 0$ – противоположные. Отсюда имеем формулу:

$$\sqrt{a + bi} = \pm\left(\sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}} \pm i\sqrt{\frac{-a + \sqrt{a^2 + b^2}}{2}}\right).$$

В скобках перед радикалом берется знак $+$, если $b > 0$, и $-$, если $b < 0$. □

Задача 4. Следующие комплексные числа изобразить векторами и записать в тригонометрической форме:

а) $z = -1 + i\sqrt{3}$;

б) $z = -5i$;

в) $z = -3\left(\cos\frac{\pi}{5} - i\sin\frac{\pi}{5}\right)$.

Решение. а) Находим модуль и аргумент комплексного числа $z = -1 + i\sqrt{3}$. Здесь $a = -1$, $b = \sqrt{3}$, $|z| = r =$

$= \sqrt{(-1)^2 + (\sqrt{3})^2} = 2$; $\cos\varphi = \dfrac{-1}{2}$; $\sin\varphi = \dfrac{\sqrt{3}}{2}$. Отсюда $\arg z = \varphi = \dfrac{2\pi}{3}$. Значит, число z в тригонометрической форме имеет вид:

$$-1 + i\sqrt{3} = 2\left(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}\right).$$

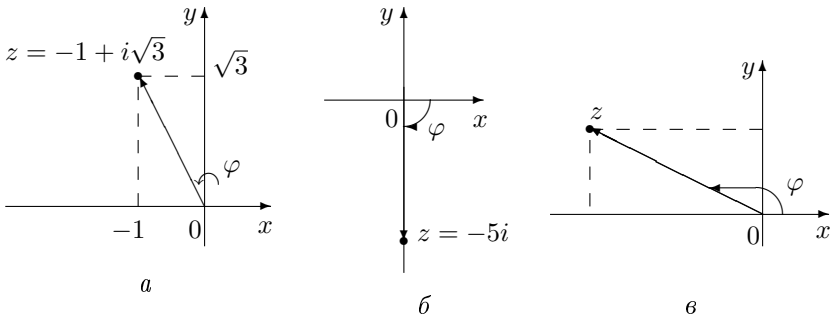
б) Имеем: $r = \sqrt{0 + (-5)^2} = 5$; $\cos\varphi = \dfrac{0}{5} = 0$; $\sin\varphi = \dfrac{-5}{5} = -1$; $\varphi = -\dfrac{\pi}{2}$. Значит,

$$-5i = 5\left(\cos\left(-\frac{\pi}{2}\right) + i\sin\left(-\frac{\pi}{2}\right)\right).$$

в) Запись $z = -3\left(\cos\dfrac{\pi}{5} - i\sin\dfrac{\pi}{5}\right)$ не является тригонометрической формой комплексного числа. Перепишем z в виде $z = 3\left(-\cos\dfrac{\pi}{5} + i\sin\dfrac{\pi}{5}\right)$. Надо найти такой угол φ, что $\cos\varphi = -\cos\dfrac{\pi}{5}$, $\sin\varphi = \sin\dfrac{\pi}{5}$. Таким углом является $\pi - \dfrac{\pi}{5} = \dfrac{4\pi}{5}$, т.е. $\varphi = \dfrac{4\pi}{5}$. Значит,

$$z = 3\left(\cos\frac{4\pi}{5} + i\sin\frac{4\pi}{5}\right).$$

Изображения чисел представлены на рис. 8. □



а *б* *в*

Рис. 8

Задача 5. Изобразить на комплексной плоскости множества точек, удовлетворяющих следующим условиям:

а) $|z| = 2$;

б) $\arg z = \dfrac{\pi}{3}$;

в) $0 \le \operatorname{Im} z < 1,5$;

г) $\operatorname{Re} z > 1$;

д) $\begin{cases} |z| \le 1, \\ \dfrac{\pi}{4} \le \arg z \le \dfrac{3\pi}{4}; \end{cases}$

е) $|z - i| = |z + 2|$.

Решение. а) По формуле модуля комплексного числа будем иметь равенство $\sqrt{x^2 + y^2} = 2$, т. е. $x^2 + y^2 = 4$. Таким образом, множество точек, удовлетворяющих условию $|z| = 2$, представляет собой окружность радиуса 2 с центром в начале координат.

б) Точки z, аргумент которых равен $\dfrac{\pi}{3}$, лежат на луче выходящем из точки $(0, 0)$ под углом $\dfrac{\pi}{3}$ к действительной оси.

в) Данное в условии неравенство можно переписать в виде $0 \le y < 1,5$.

г) Условие $\operatorname{Re} z > 1$ или $x > 1$ определяет множество всех точек, расположенных справа от прямой $x = 1$.

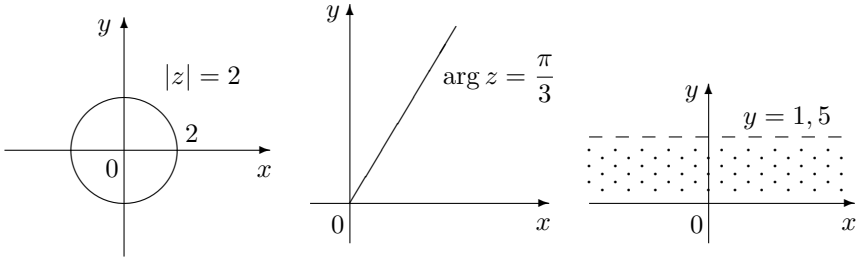
д) Множество точек, расположенных внутри и на границе круга $|z| \leq 1$, заключенных между лучами $\varphi = \dfrac{\pi}{4}$ и $\varphi = \dfrac{3\pi}{4}$ будет удовлетворять условию задачи.

е) Если $z_1 = x_1 + iy_1$ и $z_2 = x_2 + iy_2$ – комплексные числа, то

$$|z_1 - z_2| = \sqrt{(x_1 - x_2)^2 - (y_1 - y_2)^2},$$

т. е. модуль разности двух комплексных чисел равен расстоянию между точками, изображающими эти числа на плоскости. Поэтому равенству из условия задачи $|z - i| = |z - (-2)|$ удовлетворяет множество точек z, равноудаленных от точек $z_1 = i$ и $z_2 = -2$. Это множество точек представляет собой серединный перпендикуляр к отрезку, соединяющему точки $z_1 = i$ и $z_2 = -2$.

Множества точек а) – е) изображены на рис. 9. □



а *б* *в*

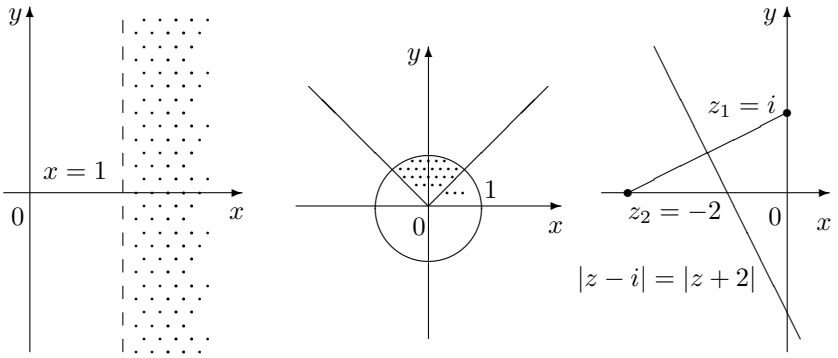


Рис. 9

Задача 6. Выполните действия $(\sqrt{3}-3i)\left(\cos\dfrac{5\pi}{12}-i\sin\dfrac{5\pi}{12}\right)$.

Решение. Представим первый множитель в тригонометрической форме:

$$\sqrt{3}-3i=2\sqrt{3}\left(\cos\frac{5\pi}{3}+i\sin\frac{5\pi}{3}\right).$$

Второй множитель также не представлен в тригонометрической форме, так как перед его мнимой частью стоит знак «−» вместо знака «+». Поэтому представим второй множитель в тригонометрической форме, используя четность косинуса и нечетность синуса: $\cos(-\varphi)=\cos\varphi$, $\sin(-\varphi)=-\sin\varphi$. Тогда можно записать:

$$\cos\frac{5\pi}{12}-i\sin\frac{5\pi}{12}=\cos\left(-\frac{5\pi}{12}\right)+i\sin\left(-\frac{5\pi}{12}\right).$$

Следовательно,

$$(\sqrt{3}-3i)\left(\cos\frac{5\pi}{12}-i\sin\frac{5\pi}{12}\right)=$$
$$=2\sqrt{3}\left(\cos\frac{5\pi}{3}+i\sin\frac{5\pi}{3}\right)\cdot\left(\cos\left(-\frac{5\pi}{12}\right)+i\sin\left(-\frac{5\pi}{12}\right)\right)=$$
$$=2\sqrt{3}\left(\cos\left(\frac{5\pi}{3}-\frac{5\pi}{12}\right)+i\sin\left(\frac{5\pi}{3}-\frac{5\pi}{12}\right)\right)=2\sqrt{3}\times$$
$$\times\left(\cos\frac{5\pi}{4}+i\sin\frac{5\pi}{4}\right)=2\sqrt{3}\left(-\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2}\right)=-\sqrt{6}(1+i).$$

□

Задача 7. Вычислить $(\sqrt{6}-i\sqrt{2})^6$.

Решение. Представим число $\sqrt{6}-i\sqrt{2}$ в тригонометрической форме

$$\sqrt{6}-i\sqrt{2}=2\sqrt{2}\left(\cos\frac{11\pi}{6}+i\sin\frac{11\pi}{6}\right).$$

По формуле Муавра находим

$$(\sqrt{6}-i\sqrt{2})^6=\left[2\sqrt{2}\left(\cos\frac{11\pi}{6}+i\sin\frac{11\pi}{6}\right)\right]^6=$$
$$=(2\sqrt{2})^6\left(\cos\left(6\cdot\frac{11\pi}{6}\right)+i\sin\left(6\cdot\frac{11\pi}{6}\right)\right)=$$
$$=2^9(\cos(-\pi)+i\sin(-\pi))=-2^9=-512.$$

□

Задача 8. Выразить $\cos 3x$ и $\sin 3x$ через $\cos x$ и $\sin x$.

Решение. Комплексное число

$$\alpha = \cos x + i \sin x$$

возведем в 3-ю степень, пользуясь формулой Муавра (9) и биномиальной формулой Ньютона. [3]

Получим с одной стороны,

$$\alpha^3 = (\cos x + i \sin x)^3 = \cos 3x + i \sin 3x;$$

а с другой стороны,

$$\begin{gathered}\alpha^3 = (\cos x + i \sin x)^3 = \\ = \cos^3 x + 3i \cos^2 x \sin x - 3 \cos x \sin^2 x - i \sin^3 x = \\ = (\cos^3 x - 3 \cos x \sin^2 x) + i(3 \cos^2 x \sin x - \sin^3 x).\end{gathered}$$

Так как комплексные числа равны тогда и только тогда, когда равны их действительные и мнимые части, то имеем:

$$\cos 3x = \cos^3 x - 3 \cos x \sin^2 x,$$

$$\sin 3x = 3 \cos^2 x \sin x - \sin^3 x.$$

□

Задача 9. Вычислить все значения корня $\sqrt[4]{-4}$ и изобразить их геометрически.

[3] Формула бинома Ньютона: $(a+b)^n = a^n + C_n^1 a^{n-1} b + \ldots + C_n^k a^{n-k} b^k + \ldots + b^n$. Здесь под a и b подразумеваются произвольные числа, а биномиальные коэффициенты C_n^k вычисляются по формуле $C_n^k = \dfrac{n!}{k!(n-k)!}$, где $n! = 1 \cdot 2 \cdot \ldots \cdot (n-1) \cdot n$. При $n = 2, 3$ получаем известные формулы сокращенного умножения.

Решение. Как известно, корень n-ой степени из ненулевого комплексного числа $z = r(\cos\varphi + i\sin\varphi)$ имеет n различных значений, которые находятся по формуле $\sqrt[n]{r(\cos\varphi + i\sin\varphi)} = \sqrt[n]{r}\left(\cos\dfrac{\varphi+2\pi k}{n} + i\sin\dfrac{\varphi+2\pi k}{n}\right)$, где $\sqrt[n]{r}$ – арифметическое значение корня, а число k пробегает значения $0, 1, 2, \ldots, n-1$. Представим число -4 в тригонометрической форме:

$$-4 = 4(\cos\pi + i\sin\pi).$$

Тогда $\sqrt[4]{4(\cos\pi + i\sin\pi)} = \sqrt[4]{4}\left(\cos\dfrac{\pi+2\pi k}{4} + i\sin\dfrac{\pi+2\pi k}{4}\right)$. Придавая параметру k значения $0, 1, 2, 3$, получим 4 различных значения корня 4-й степени из -4:

$$\alpha_0 = \sqrt{2}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right) = \sqrt{2}\left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) = 1 + i,$$

$$\alpha_1 = \sqrt{2}\left(\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4}\right) = \sqrt{2}\left(-\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) = -1 + i,$$

$$\alpha_2 = \sqrt{2}\left(\cos\frac{5\pi}{4} + i\sin\frac{5\pi}{4}\right) = \sqrt{2}\left(-\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right) = -1 - i,$$

$$\alpha_3 = \sqrt{2}\left(\cos\frac{7\pi}{4} + i\sin\frac{7\pi}{4}\right) = \sqrt{2}\left(\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right) = 1 - i.$$

Найденным корням соответствуют вершины правильного четырехугольника, вписанного в окружность радиуса $\sqrt{2}$ с центром в начале координат (рис. 10). □

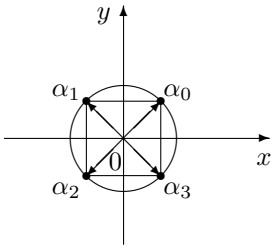


Рис. 10

Задача 10. Пользуясь корнями 3-й степени из 1, вычислить $\sqrt[3]{-8i}$.

Решение. Все значения корня n-й степени из числа z можно получить, умножая одно из них на все значения корня n-й степени из 1. Одно из значений $\sqrt[3]{-8i}$ можно найти непосредственно. Оно равно $2i$, так как $(2i)^3 = -8i$. Найдем теперь по формуле (11) все значения $\sqrt[3]{1}$:

$$\varepsilon_k = \sqrt[3]{1} = \sqrt[3]{\cos 0 + i \sin 0} = \cos \frac{2\pi k}{3} + i \sin \frac{2k}{3} \quad (k = 0, 1, 2);$$

$\varepsilon_0 = 1$, $\varepsilon_1 = -\dfrac{1}{2} + i\dfrac{\sqrt{3}}{2}$, $\varepsilon_2 = -\dfrac{1}{2} - i\dfrac{\sqrt{3}}{2}$. Следовательно, имеем три значения для $\sqrt[3]{-8i}$:

$\alpha_0 = 2i \cdot \varepsilon_0 = 2i$,
$\alpha_1 = 2i \cdot \varepsilon_1 = -\sqrt{3} - i$,
$\alpha_2 = 2i \cdot \varepsilon_2 = \sqrt{3} - i$. □

Упражнения для самостоятельной работы

7.1. Выполнить действия над комплексными числами в алгебраической форме:

а) $(2 + 3i)(3 - 2i)$;
б) $(2 + i)(3 + 7i) - (1 + 2i)(5 + 3i)$;
в) $i^2 + i^3 + i^4 + i^5$;

г) $(2+i)^3+(2-i)^3$;

д) $(1+i)(2+i)+\dfrac{5}{1+2i}$;

е) $\dfrac{(3-5i)(2+3i)}{1+2i}$;

ж) $\dfrac{1+i\sqrt{3}}{1-i\sqrt{3}}-(1-i)^{12}$;

з) $\dfrac{(1+2i)^2-(1-i)^3}{(3+2i)^3-(2+i)^2}$;

и) $\dfrac{(1+i)^n}{(1-i)^{n-2}}$ (n – целое положительное число).

7.2. Вычислить $1-i^5+i^{10}-i^{15}+\ldots+i^{50}$.

7.3. Вычислить i^{77}, i^{98}, i^{-57}, i^n, где n – целое число.

7.4. Доказать равенство $(1+i)^{8n}=2^{4n}$, $n\in\mathbb{Z}$.

7.5. Решить систему уравнений:

а) $\begin{cases} iz_1+(1+i)z_2=2+2i, \\ 2iz_1+(3+2i)z_2=5+3i; \end{cases}$

б) $\begin{cases} (1-i)z_1-3iz_2=-i, \\ 2z_1-(3+3i)z_2=3-i. \end{cases}$

7.6. Найдите $x, y\in\mathbb{R}$, если:

а) $3x-4y-(x-y)i=3-2i$;

б) $5x-2y+(x+y)i=4+5i$;

в) $(2x+yi)+(3y-2xi)=2+i$;

г) $(y^2+1)i+3=(y-2i)y-2y$;

д) $(1+2i)x+(3-5i)y=1-3i$;

е) $2+5ix-3yi=14i+3x-5y$.

7.7. При каких значениях x верно, что $(x-4i)+(2+ix^2)\in\mathbb{R}$?

7.8. Найдите x, если $(1-2ix)^3+11$ – число мнимое.

7.9. Пусть $z=\dfrac{1+ti}{1-ti}$, где $t\in\mathbb{R}$. При каких значениях t

а) $|z|=1$;

б) $z = \dfrac{3-4i}{5}$?

7.10. Найти расстояние между точками:

а) $1-6i$ и $2i$;

б) $1+4i$ и $3-2i$.

7.11. Решить квадратные уравнения:

а) $z^2 = 3-4i$;

б) $z^2 + (5-2i)z + 5(1-i) = 0$;

в) $z^2 + (1-2i)z - 2i = 0$;

г) $z^2 - (1+i)z + 6 + 3i = 0$;

д) $z^2 - 5z + 4 + 10i = 0$.

7.12. Сколько и какие значения имеет произведение $\sqrt{-1}\cdot\sqrt{-4}$?

7.13. Доказать, что $\operatorname{Re} z = \dfrac{z+\overline{z}}{2}$.

7.14. При каких действительных значениях x и y числа $z_1 = x^2 + 4y - yi$ и $z_2 = 4 + y - \dfrac{2}{i} - x^2 i$ будут сопряженными?

7.15. Найти все комплексные числа, каждое из которых сопряжено с самим собой.

7.16. Как связаны между собой два мнимых числа, сумма и произведение которых являются действительными числами?

7.17. Доказать, что если $|z| = 1$, то $\overline{z} = \dfrac{1}{z}$.

7.18. Найти число с наименьшим модулем среди комплексных чисел, удовлетворяющих условию: $|2-2iz| = |z-4|$.

7.19. Найти число с наибольшим модулем среди комплексных чисел z, удовлетворяющих условию $|z+3-4i| = 3$.

7.20. Может ли сумма квадратов двух комплексных чисел быть отрицательна?

7.21. Найти тригонометрическую форму числа:

а) 5; б) i; в) $1+i$; г) $-i$; д) -2; е) $-3i$; ж) $1+i\sqrt{3}$;
з) $-\sqrt{3}+i$; и) $-\sqrt{3}-i$; к) $\sqrt{3}-i$; л) $-1+i\sqrt{3}$;

м) $-1-i\sqrt{3}$; н) $\sin\alpha+i\cos\alpha$; о) $\dfrac{\cos\varphi+i\sin\varphi}{\cos\psi+i\sin\psi}$.

7.22. Найти модуль и аргумент комплексного числа z:

а) $z=\dfrac{1+i}{1-i}+\dfrac{1-i}{1+i}$;

б) $z=\dfrac{(\sqrt{2}+i\sqrt{6})^4}{\left(\sin\dfrac{3\pi}{10}+i\cos\dfrac{7\pi}{10}\right)^2}$.

7.23. Выполнить действия:

а) $\left(\cos\dfrac{\pi}{5}+i\sin\dfrac{\pi}{5}\right)\cdot\left(\cos\dfrac{2\pi}{15}+i\sin\dfrac{2\pi}{15}\right)$;

б) $10\left(\cos\dfrac{3\pi}{4}+i\sin\dfrac{3\pi}{4}\right):\left(5\left(\cos\dfrac{\pi}{4}+i\sin\dfrac{\pi}{4}\right)\right)$;

в) $(1+i)\left(\cos\dfrac{3\pi}{8}+i\sin\dfrac{3\pi}{8}\right)\left(\cos\dfrac{\pi}{8}+i\sin\dfrac{\pi}{8}\right)$;

г) $\dfrac{i}{\cos\dfrac{\pi}{4}+i\sin\dfrac{\pi}{4}}$.

7.24. Как изменится модуль и аргумент комплексного числа z в результате умножения этого числа на:

а) 2;

б) $2i$;

в) $-2i$.

7.25. Где расположены точки $1+2z$, для которых $|z|=1$?

7.26. Изобразить на комплексной плоскости множества точек z, удовлетворяющих следующим условиям:

а) $|z|\le 3$; б) $|z|>3$; в) $|z-3i|<1$; г) $|z+3-2i|>2$;

д) $|\operatorname{Im} z|<2$; е) $|\operatorname{Re} z|\ge\sqrt{2}$; ж) $\begin{cases}\operatorname{Re} z<\operatorname{Im} z,\\ |z|>0,2;\end{cases}$

з) $\arg z=\dfrac{\pi}{2}$; и) $\arg z=310^\circ$; к) $-\dfrac{\pi}{4}<\arg z\le 0$;

л) $|z-3|+|z-2i|=7$; м) $|z-4|-|z-2i|=10$;

н) $\begin{cases} 1 \le z \cdot \overline{z} \le 2, \\ -\sqrt{3} \le \operatorname{Im} z \le 0; \end{cases}$ о) $\begin{cases} |z+i| < 1, \\ |z+1| \ge 1. \end{cases}$

7.27. Изобразить на комплексной плоскости множество всех чисел, для которых $\operatorname{Re}\left(\dfrac{3}{z}\right) \ge \operatorname{Im}\left(\dfrac{1}{z} - 1\right)$.

7.28. Множество точек комплексной плоскости определено следующим условием $|z + 4 - 3i| \le 1$. Какова область изменения выражения $\dfrac{\operatorname{Re} z}{\operatorname{Im} z}$?

7.29. Зная точку z, на комплексной плоскости построить точку:

а) $z' = z - 3$;
б) $z' = iz$;
в) $z' = z + (2 - i)$.

7.30. Вычислить выражения:

а) $(1+i)^{1000}$;
б) $(1+i\sqrt{3})^{150}$;
в) $(\sqrt{3}+i)^{30}$;
г) $(2-\sqrt{3}+i)^{12}$;
д) $\left(\dfrac{1+i\sqrt{3}}{1-i}\right)^{20}$;
е) $\dfrac{(-1+i\sqrt{3})^{15}}{(1-i)^{20}} + \dfrac{(-1-i\sqrt{3})^{15}}{(1+i)^{20}}$.

7.31. Найти $(1 + \sin\varphi + i\cos\varphi)^{16}$.

7.32. Найти z^{12}, если $z + 2\overline{z} = 3 + i$.

7.33. Пользуясь формулой Муавра, выразить $\cos 5x$ и $\sin 5x$ через $\cos x$ и $\sin x$.

7.34. Доказать равенства:

а) $\cos x + \cos 2x + \ldots + \cos nx = \dfrac{\sin\frac{nx}{2}\cos\frac{(n+1)x}{2}}{\sin\frac{x}{2}}$

$(x \ne 2k\pi,\ k \in \mathbb{Z})$;

б) $\sin x + \sin 2x + \ldots + \sin nx = \dfrac{\sin\frac{nx}{2}\sin\frac{(n+1)x}{2}}{\sin\frac{x}{2}}$

$(x \neq 2k\pi,\ k \in \mathbb{Z})$.

7.35. Вычислить:

а) $\sqrt[3]{1}$; б) $\sqrt[3]{i}$; в) $\sqrt[6]{i}$; г) $\sqrt[6]{64}$; д) $\sqrt[6]{-27}$; е) $\sqrt[3]{8i}$;

ж) $\sqrt[10]{512(1-i\sqrt{3})}$; з) $\sqrt[8]{2\sqrt{2}(1-i)}$; и) $\sqrt[4]{-\dfrac{18}{1+i\sqrt{3}}}$;

к) $\sqrt[4]{\dfrac{7-2i}{1+i\sqrt{2}}+\dfrac{4+14i}{\sqrt{2}+2i}-(8-2i)}$;

л) $\sqrt[3]{\dfrac{1-5i}{1+i}-5\dfrac{1+2i}{2-i}+2}$.

7.36. Решить уравнения на множестве комплексных чисел:

а) $z^4 - z^3 + 2z^2 - z + 1 = 0$;

б) $z^8 - 17z^4 + 16 = 0$;

в) $|\overline{z}| - 2z = 2i - 1$.

7.37. Найти все действительные значения параметра a, при которых система $\begin{cases} 2i(z+\overline{z})^2 = z - \overline{z}, \\ |z - a\cdot i| = \dfrac{a^3}{10^2} \end{cases}$ имеет только три решения.

7.38. Число $x_1 = \left(\sin\dfrac{5\pi}{8} + i\cos\dfrac{5\pi}{8}\right)^4$ является корнем уравнения

$$x^3 + (a-2)x^2 + a^2x - 2a^2 - 1 = 0, \quad a \in \mathbb{R}.$$

Найдите остальные корни уравнения.

7.39. Найти корни из единицы степеней 2, 3, 4, 6, 8, 12.

7.40. Найти произведение всех корней степени n из единицы.

7.41. Пусть $\varepsilon_k = \cos\dfrac{2\pi k}{n} + i\sin\dfrac{2\pi k}{n}$ $(0 \leq k < n)$. Доказать, что:

а) $\varepsilon_k = {\varepsilon_1}^k \quad (0 \le k < n)$;

б) $\varepsilon_k \varepsilon_l = \begin{cases} \varepsilon_{k+l}, \text{ если } k+l < n, \\ \varepsilon_{k+l-n}, \text{ если } k+l \ge n, \end{cases} \quad (0 \le k < n,\ 0 \le l < n)$;

в) множество U_n корней степени n из единицы является циклической группой порядка n относительно умножения.

7.42. Корень n-ой степени из 1 называется *первообразным* (*примитивным*), если он не является корнем из 1 никакой меньшей степени. Таковыми будут, например, $\varepsilon_1 = \cos\dfrac{2\pi}{n} + i\sin\dfrac{2\pi}{n}$, ε_{n-1}. Доказать, что следующие утверждения равносильны:

а) ε является первообразным корнем из единицы степени n;

б) порядок ε в группе U_n равен n;

в) ε является порождающим элементом группы U_n.

7.43. Доказать, что если ε является первообразным корнем степени n из единицы, то $\overline{\varepsilon}$ также является первообразным корнем степени n из единицы.

История развития некоторых математических понятий

Ассоциативность Основные законы сложения и умножения были введены как законы при попытках развить новые исчисления – «символическую алгебру» и теорию комплексных и гиперкомплексных чисел. К XIX веку переместительный и сочетательный законы сложения включались в систему аксиом. Названия законов появились позднее, чем были сформулированы сами законы. Термин *ассоциативный* произведен от латинского слова *associare* (ассоциировать, сочетать); он был введен У. Гамильтоном в 1943 г.

Би Латинская приставка, означающая удвоение, входит во многие математические термины.

Группа Термин *groupe* впервые употребил Э. Галуа (1830 г.). Работы Галуа немногочислены, написано сжато, почему и оставались не понятыми современниками. Многие его идеи были заново открыты через много лет после его ранней смерти. Самая первая попытка сформулировать определение абстрактной группы содержится в статье А. Кэли (1854 г.). Понятие группы было поставлено в центр геометрических исследований работами Ф. Клейна и С. Ли. Первое исследование бесконечных групп восходит к Жордану (1870 г.). Несколько лет спустя изучение их было продолжено в различных направлениях Ли, который и создал эту новую ветвь математики (работы 1888 – 1893 гг.). Аксиоматика теории групп в основном была завершена к 30-м годам XX века.

Математические открытия Галуа положили начало новому направлению – теории абстрактных алгебраических структур. Можно смело сказать, что идеи Галуа совершенно преобразили облик всей современной математики. П. С. Александров писал: «Я думаю, что ...понятия числа, множества, функции и группы являются теми четырьмя краеугольными камнями, на которых зиждется все здание современной математики и к которым сводится всякое другое математическое понятие».

Дистрибутивность Латинское слово *distribution* означает разделение. В ходе доказательств правил действий с натуральными числами были выделены основные законы сложения и умножения. Названия законов *дистрибутивный*, *коммутативный* ввел французский артиллерийский офицер и преподаватель Ф. Сервуа в 1815 г.

Кольцо Понятие кольца было введено Р. Дедекиндом в 1879 г. Термин *Ring* предложил в своей работе Д. Гильберт (1897 г.).

Множество К понятию числовых множеств и множеств функций подводили работы многих математиков XX века. Г. Кантор занимался рассмотрением множеств потому, что этого требовали некоторые задачи математического анализа. Примерно в 1879 г. Кантор увидел, что рождается самостоятельное учение – о множествах. Все, что было известно к тому времени о множествах, он опубликовал в ряде статей. Кантор начал изучать множества произвольной природы, развил методы, свойственные современной теории множеств, и поставил ее на строго научную основу. При этом по мере развития теории понятие «множества» претерпело значительные изменения. Интуитивное понимание привело к па-

радоксам теории множеств, полученными разными авторами к 1900 г. Математики разнились во взглядах на новую теорию. В 1904-1908 гг. немецкий математик Э. Цермело сформулировал первую систему аксиом теории множеств. Тем самым был найден выход из кризиса и направление дальнейшего развития теории. Кантор употреблял вначале термин *Inbegriff* (совокупность), а затем – *Mannigfaltigkeit* (многообразие), и наконец – *Menge* – множество. В настоящее время сохранилось его обозначение множества $M = \{m\}$, которое он ввел в 1895 г.

Подстановка Подстановки привлекли внимание математиков во второй половине XVIII в. Многие теоремы о них сформулировал итальянский математик и врач П. Руффини. Его результаты упорядочил и дополнил О. Коши. В статьях 1812–1815 гг. Коши ввел термин *Substitutions* и представил подстановку современным образом. Он ввел определение произведения подстановок, заметил, что оно ассоциативно, но не коммутативно.

Поле Концепции поля появились в работах Л. Кронекера и Р. Дедекинда. Кронекер ввел понятие области рациональности, начало работы над этими вопросами относится к 1853 г. Дедекинд ввел понятие поля *Körper* в лекциях 1857–1858 гг. Работы Кронекера и Дедекинда почти не получили немедленного развития и продолжения, только через 30 лет стала очевидной важность их основополагающих результатов.

Сравнение Термин *сравнимы* (*congruence*) в том смысле, в котором он потом появится у Гаусса, впервые употребил Гольдбах (1742 г.). Понятие в неявном виде встречалась у многих математиков, однако только Гаусс точно

определил его и систематически развил теорию. *Равноостаточные члены* или *числа, сравнимые по модулю* – термины, введеные Гауссом. Он же ввел знак сравнения $\equiv$. Гаусс рассматривал также сравнения высших порядков и системы сравнений. Полное исследование систем линейных сравнений было завершено в конце XIX в.

Транзитивность Этот математический термин образован от латинского слова *transeo* (перехожу).

Формула Муавра Впервые в несколько измененном виде формулу получил английский математик Муавр в 1707 г. Говорят, что на многие вопросы Ньютон отвечал: «Спросите у Муавра, он это знает лучше меня». Независимо от Муавра формулу открыл итальянский ученый – граф Джулио Фаньяно де Фаньяни (1738 г.). В современном виде формулу представил Эйлер во «Введении в анализ».

Числа комплексные Термин *комплексное число* впервые ввел в употребление Карно (1803 г.). Буквальное значение выражения – «сложное, составное число». Позднее термин был повторен Гауссом («Теория биквадратных вычетов», 1828 г.); Гаусс употреблял его систематически, чтобы исключить *мнимое* число. Именно такой термин «составное число» употреблялся в русской литературе до конца XIX в.

Считается, что впервые комплексные числа стали употреблять итальянские математики Кардано (1545 г.) и Бомбелли (1572 г.); Кардано называл их «чисто отрицательными». Однако, в неявном виде эти числа можно найти и в более ранних работах. С другой стороны, еще долго после работ Кардано и Бомбелли даже вы-

дающиеся математики не имели отчетливого понятия о комплексных числах. Лейбниц писал (1702 г.): «Мнимые числа – это прекрасное и чудесное убежище божественного духа, почти сочетание бытия с небытием». Бомбелли в своей «Алгебре» (написана ок.1560 г., издана в 1572 г.) дал первое формальное обоснование действий над комплексными числами.

У Декарта (1637 г.) впервые противопоставлены действительные и мнимые корни уравнения (real – imaginaire). Первой буквой этого термина Декарта – «radices imaginaire» – и обозначена «мнимая единица». Эйлер повторно использовал это обозначение в 1777 г., обозначение стало общепринятым благодаря Гауссу.

В ясной и систематической форме геометрическое изображение комплексных чисел (в виде направленных отрезков) и действий над ними находят в работах датского геодезиста, картографа и землемера Каспара Весселя (1799 г.) и французкого математика Жана Аргана (1806 г.). Всеобщую известность геометрическое представление комплексных чисел получило, начиная с 1831 г., когда появилась статья Гаусса, содержащая и геометрическую интерпретацию комплексных чисел.

И. Бернулли, Лейбниц, Коутс, Муавр обращались с мнимыми числами как с действительными. В попытках обосновать действия с комплексными числами, четко сформулировать требования, предъявляемые к «числам», Гамильтон пришел к законам алгебраических операций: ассоциативному, коммутативному, дистрибутивному.

Термин *модуль* для величины $\sqrt{a^2+b^2}$ ввел Арган в 1814 г., затем его употреблял Коши. Вейерштрасс ввел

название *абсолютная величина* и обозначение $|z|$ в 1841 г. Употреблялись также обозначения $mod.z$, $abs.z$ и др. Название *аргумент* для угла φ комплексного числа употребил впервые Коши (1847 г.), угол φ называли также «амплитудой», «аномалией», «азимутом», «аркусом» комплексной переменной. Названия *сопряженные числа* для $a + bi$, $a - bi$ ввел Коши (1821 г.).

В тригонометрической форме числа были представлены Эйлером и Д'Аламбером (Известно, что Виет сумел решить уравнение 45-ой степени, представив неизвестную в форме, эквивалентной тригонометрической, в 1593 – 1600 гг.). Коши записывал комплексное число в виде $re^{\rho\sqrt{-1}}$ в 1827 г.

Ответы, решения, указания

§1. 1.1. г) $\{(1,1), (-1,1), (1,-1), (-1,-1)\}$; д) например, 0, 1, 2, 4, 5 – всего 16 чисел. **1.2.** в) $\{x \in \mathbb{Z} \mid 246$ делится на x и $|x| > 2\}$; д) $\{1 + 5k \mid k \in \mathbb{Z},\ 0 \leq k \leq 5\}$. **1.3.** Равные множества только в а). **1.4.** Верные включения: б), в), г). **1.6.** а) $1 \in \mathbb{N}$; б) $\{1, 2\} \subseteq \mathbb{N}$; в) $\{1, 2\} \subseteq \{1, 2, \{1\}, \{2\}\}$; г) $\{1, 2\} \in \{1, 2, \{1, 2\}\}$; д) $\emptyset \subseteq \mathbb{R}$; е) $\emptyset \in \{\emptyset\}$. **1.8.** а) $A \cup B = \{1, 2, 3, 4, 5\}$; $A \cap B = \{2, 3\}$; $A \setminus B = \{1\}$; $B \setminus A = \{4, 5\}$; $\overline{A} = \{0, 4, 5, \ldots, 9\}$; $\overline{B} = \{0, 1, 6, 7, 8, 9\}$. **1.12.** Верно а). **1.14.** г) 1. Пусть $x \in A \cup (B \setminus C)$. Тогда $x \in A$ или $x \in B \setminus C$. Если $x \in A$, то $x \in A \cup B$ и $x \in A \cup \overline{C}$, следовательно, $x \in (A \cup B) \cap (A \cup \overline{C})$. Если $x \in B \setminus C$, то $x \in B$ и $x \notin C$. Отсюда следует, что $x \in A \cup B$ и $x \in A \cup \overline{C}$. Итак, $A \cup (B \setminus C) \subseteq (A \cup B) \cap (A \cup \overline{C})$. 2. Пусть $x \in (A \cup B) \cap (A \cup \overline{C})$. Тогда $x \in A \cup B$ и $x \in A \cup \overline{C}$. Отсюда следует, что $x \in A$ или $x \in B$ и $x \in \overline{C}$, т.е. $x \in A$ или $x \in B \setminus C$. Таким образом, $x \in A \cup (B \setminus C)$. Итак, доказано включение $(A \cup B) \cap (A \cup \overline{C}) \subseteq A \cup (B \setminus C)$. Объединяя 1 и 2 получаем равенство $A \cup (B \setminus C) = (A \cup B) \cap (A \cup \overline{C})$. **1.15.** а) $X = \overline{A}$; б) $X = A$. **1.16.** б) $\Rightarrow$ Пусть $(A \setminus B) \cup B = A$ и $x \in B$. Тогда $x \in (A \setminus B) \cup B$, и значит, $x \in A$. $\Leftarrow$ Пусть $B \subseteq A$. Тогда, учитывая равенство $A \setminus B = A \cap \overline{B}$, получаем: $(A \setminus B) \cup B = (A \cap \overline{B}) \cup B = (A \cup B) \cap (\overline{B} \cup B) = (A \cup B) \cap U = A \cup B = A$. **1.17.** в) 1. Пусть $x \in A \cap (B \dot{-} C)$. Тогда $x \in A$ и $x \in B \dot{-} C = (B \setminus C) \cup (C \setminus B)$. Если $x \in B$, то $x \notin C$, значит, $x \in A \cap B$, но $x \notin A \cap C$, т.е. $x \in (A \cap B) \dot{-} (A \cap C)$. Если $x \in C$, то $x \notin B$, значит, $x \in A \cap C$, но $x \notin A \cap B$. Таким образом, и в этом случае $x \in (A \cap B) \dot{-} (A \cap C)$. Итак, доказа-

но, что $A \cap (B \dot{-} C) \subseteq (A \cap B) \dot{-} (A \cap C)$. 2. Пусть $x \in (A \cap B) \dot{-} (A \cap C) = ((A \cap B) \setminus (A \cap C)) \cup ((A \cap C) \setminus (A \cap B))$. Если $x \in A \cap B$ и $x \notin A \cap C$, то $x \in A$, $x \in B$, $x \notin C$. Следовательно, $x \in A$ и $x \in B \setminus C$, а значит, $x \in A$ и $x \in (B \setminus C) \cup (C \setminus B)$, т.е. $x \in A \cap (B \dot{-} C)$. Если $x \in A \cap C$ и $x \notin A \cap B$, то $x \in A$, $x \in C$, $x \notin B$. Значит, $x \in A \cap (B \dot{-} C)$. Итак, $(A \cap B) \dot{-} (A \cap C) \subseteq A \cap (B \dot{-} C)$. Объединяя 1 и 2 получаем требуемое равенство. **1.18.** а) $\overline{A}$; б) $\emptyset$; в) A; г) C.

§2. 2.1. г) $A \times B = B \times A = \emptyset$. **2.2.** Пусть $x = \langle y, z \rangle \in A \times B$. Так как $A \subseteq C$, то $x = \langle y, z \rangle \in C \times B$, а так как $B \subseteq C$, то $x = \langle y, z \rangle \in A \times C$. Следовательно, $x \in (A \times C) \cap (C \times B)$, и поэтому $A \times B \subseteq (A \times C) \cap (C \times B)$. Пусть теперь $x = \langle y, z \rangle \in (A \times C) \cap (C \times B)$. Тогда $x = \langle y, z \rangle \in A \times C$ и $x = \langle y, z \rangle \in C \times B$. Следовательно, $y \in A$, $z \in C$ и $y \in C$, $z \in B$. Откуда получаем: $y \in A \cap C = A$, $z \in C \cap B = B$, и значит, $x = \langle y, z \rangle \in A \times B$. Доказали включение $(A \times C) \cap (C \times B) \subseteq A \times B$. Итак, $A \times B = (A \times C) \cap (C \times B)$. **2.4.** б) Пусть $x \in (A \cup B) \times C$. Тогда $x = \langle y, z \rangle$, где $y \in A \cup B$, $z \in C$. Отсюда $y \in A$ или $y \in B$. Значит, $x = \langle y, z \rangle \in A \times C$ или $x = \langle y, z \rangle \in B \times C$, следовательно, $x \in (A \times C) \cup (B \times C)$. Таким образом, мы доказали включение $(A \cup B) \times C \subseteq (A \times C) \cup (B \times C)$. Пусть теперь $x \in (A \times C) \cup (B \times C)$. Тогда $x \in A \times C$ или $x \in B \times C$. Это означает, что $x = \langle y, z \rangle$ и в первом случае $y \in A$, $z \in C$, а во втором случае $y \in B$, $z \in C$. Значит, $y \in A \cup B$, а $x = \langle y, z \rangle \in (A \cup B) \times C$. Итак, мы доказали включение $(A \times C) \cup (B \times C) \subseteq (A \cup B) \times C$, а вместе с ним и требуемое равенство. **2.5.** Пусть $a \in A$, $b \in B$. Тогда $\langle a, b \rangle \in A \times B$, а значит, $\langle a, b \rangle \in (A \times B) \cup (B \cup A) = C \times D$, т.е. $a \in C$, $b \in D$. С другой стороны, $\langle b, a \rangle \in B \times A$, а значит, $\langle b, a \rangle \in (A \times B) \cup (B \times A) = C \times D$, т.е.

$b \in C$, $a \in D$. Тогда, так как $a \in C$ и $a \in D$, то $\langle a, a\rangle \in C \times D = (A \times B) \cup (B \times A)$. Это означает, что $\langle a, a\rangle \in A \times B$ или $\langle a, a\rangle \in B \times A$, в любом случае получаем, что $a \in B$. Аналогично, $\langle b, b\rangle \in C \times D$, а значит, $b \in A$. Итак, доказано равенство $A = B$. Тогда $A \times B = C \times D$, и по задаче 1 $A = C$, $B = D$. **2.6.** в) Не рефлексивно, симметрично, не антисимметрично, транзитивно; д) рефлексивно, симметрично, не антисимметрично, не транзитивно; з) не рефлексивно, симметрично, не антисимметрично, не транзитивно; и) не рефлексивно, не симметрично, антисимметрично, не транзитивно; л) рефлексивно; симметрично, не антисимметрично, транзитивно; о) рефлексивно, симметрично, не антисимметрично, транзитивно; с) не рефлексивно, не симметрично, антисимметрично, транзитивно. **2.7.** а) Например, на множестве $\mathbb{R}$ $aRb \Leftrightarrow a \leq b$; б) на множестве $\mathbb{R}$ $aRb \Leftrightarrow |a - b| \leq 1$; в) на множестве $\mathbb{N}$ $aRb \Leftrightarrow a < b$; г) на множестве $\mathbb{R}$ $aRb \Leftrightarrow a, b > 0$. **2.10.** Класс эквивалентности образуют: а) все упорядоченные пары, у которых одна и та же разность между первой и второй компонентами; б) все числа равные между собой по абсолютной величине; в) все числа с одинаковыми дробными частями. **2.11.** Класс эквивалентности может состоят из одного элемента, в случае, когда $a = b$ или из двух, когда $a = -(b + 1)$. **2.13.** $R = \{\langle 1, 2\rangle, \langle 2, 3\rangle, \langle 2, 1\rangle, \langle 3, 2\rangle, \langle 1, 1\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle\}$. **2.14.** Фактормножества: $\{[1] = [2] = [3] = \{1, 2, 3\}\}$, $\{[1] = [2] = \{1, 2\}, [3]\}$, $\{[1] = [3] = \{1, 3\}, [2]\}$, $\{[2] = [3] = \{2, 3\}, [1]\}$, $\{[1] = \{1\}, [2] = \{2\}, [3] = \{3\}\}$. **2.16.** R_1 не является, R_2 является.

§3. 3.1. а), в) Является; б) не является. **3.2.** а) Не является; б) является. **3.4.** а), б) Является. **3.5.** а), в) Об-

разуют и $\mathbb{N}$, и $\mathbb{Q}$; б) образует только $\mathbb{Q}$. **3.6.** а) Является; б) не является. **3.8.** Образует. **3.9.** Деление не коммутативно и не ассоциативно. **3.10.** б), в) Операции и коммутативны, и ассоциативны. **3.16.** Не содержит. **3.18.** Условие существования нейтрального элемента множества $\mathbb{N}$ относительно операции $\circ$ равносильно существованию максимального натурального числа. **3.19.** Нейтральный элемент – число $1 = 1 + 0\sqrt{2}$. $(1+\sqrt{2})^{-1} = -1 + \sqrt{2}$. Обратного элемента для числа $3 - \sqrt{2}$ не существует, так как $(3-\sqrt{2})^{-1} = \dfrac{1}{3-\sqrt{2}} = \dfrac{3+\sqrt{2}}{(3-\sqrt{2})(3+\sqrt{2})} = \dfrac{3+\sqrt{2}}{7} = \dfrac{3}{7} + \dfrac{1}{7}\sqrt{2}$ и полученное число не принадлежит рассматриваемому множеству. **3.20.** $\begin{pmatrix} -2 & 0 \\ 0 & -2 \end{pmatrix}^{-1} = \begin{pmatrix} -1/2 & 0 \\ 0 & -1/2 \end{pmatrix}$, $\begin{pmatrix} \sqrt{2} & 1 \\ 0 & \sqrt{2} \end{pmatrix}^{-1} = \begin{pmatrix} 1/\sqrt{2} & -1/2 \\ 0 & 1/\sqrt{2} \end{pmatrix}$, $\begin{pmatrix} -1/3 & 0 \\ 1 & 1/3 \end{pmatrix}^{-1} = \begin{pmatrix} -3 & 0 \\ 9 & 3 \end{pmatrix}$. **3.21.** Нейтральный элемент 1; единственный симметризуемый элемент 1. **3.22.** Относительно операции объединения нейтральным элементом является пустое множество, а относительно операции пересечения – само множество $P(M)$; только пустое множество имеет симметричный элемент относительно объединения, а относительно пересечения – только множество $P(M)$. **3.24.** Сложение коммутативно и ассоциативно; умножение ассоциативно, но не коммутативно; сложение дистрибутивно относительно умножения.

§4. 4.1. а), г), е), з), и), к), м), о), п), р) Образует; б), в), д), ж), л), н) не образует. **4.2.** Найдем произведе-

ние матриц из данного множества: $\begin{pmatrix} a & b \\ b & b \end{pmatrix}\begin{pmatrix} c & d \\ d & d \end{pmatrix} = \begin{pmatrix} ac+bd & ad+bd \\ bc+bd & 2bd \end{pmatrix}$. Отсюда слудует, что полученное произведение не всегда принадлежит рассматриваемому множеству. Значит, это множество не является группой относительно умножения. **4.3.** а) Не образует; б) не образуют. **4.5.** Образует при $\lambda < 0$. **4.7.** а) Не образует; б) не образуют. **4.8.** Рассматриваемое на $\mathbb{Z}$ действие сводится к сложению или вычитанию целых чисел, а поскольку как сложение, так и вычитание элементов из $\mathbb{Z}$ дает в результате элемент из $\mathbb{Z}$, то на множестве $\mathbb{Z}$ рассматриваемое действие является бинарной операцией. Для проверки ассоциативности заданной операции, необходимо рассмотреть все возможные случаи: если a, b – четные числа, c – любое число из $\mathbb{Z}$; a – четное число, b – нечетное, а c – любое число из $\mathbb{Z}$; a – нечетное число, b – четное, а c – любое число из $\mathbb{Z}$; a, b – нечетные числа, c – любое число из $\mathbb{Z}$. Нейтральным элементом в $\mathbb{Z}$ будет являться 0. Для любого элемента $a \in \mathbb{Z}$ в $\mathbb{Z}$ существует обратный элемент: для четного a обратным будет противоположное число $-a$, так как $a \circ (-a) = a + (-a) = 0$; для нечетного a обратным будет само число a, так как $a \circ a = a - a = 0$. **4.11.** Рассмотреть произведение $(ab)^2 = ab \cdot ab = e$. **4.12.** Операция $\circ$ не ассоциативна. **4.13.** Нейтральным элементом относительно операции $\circ$ является 0. Обратимы все элементы, отличные от -1. **4.14.** Любой элемент a множества M является правым единичным элементом, а левый единичный элемент существует лишь в случае, когда M состоит из одного элемента; любой элемент множества M обратим слева относительно правого единичного эле-

мента, а справа обратим только сам правый единичный элемент при условии, что M состоит из одного элемента. **4.15.** Является; единичный элемент не существует, если M^2 состоит более чем из одной пары элементов. **4.16.** Полугруппа содержит три элемента; группой не является. **4.20.** б) Если $A \cup B$ – подгруппа, $x \in A \setminus B$, $y \in B \setminus A$, рассмотреть xy. **4.21.** Единичным элементом является b; операция коммутативна и ассоциативна; $(M; \cdot)$ – полугруппа, но не группа. **4.23.** Из таблицы Кэли следует: а) $x_m x_k = a$; б) $x_t x_k = 1$; в) $x_t x_p = b$. В группе для любого элемента существует обратный. Домножим равенство а) справа на x_k^{-1}: $x_m = a x_k^{-1}$. Равенство с) домножим слева на x_t^{-1} : $x_p = x_t^{-1} b$. Таким образом, $x_m x_p = a x_k^{-1} x_t^{-1} b$. Из равенства б) находим: $x_t = x_k^{-1}$. Окончательно получаем $x_m x_p = a x_t x_t^{-1} b = ab$. **4.24.** Элемент $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ имеет порядок 1, элементы $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ и $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ – порядок 3, остальные элементы имеют порядок 2. Группа S_3 имеет 6 различных подгрупп, включая $\{e\}$ и S_3. Все подгруппы, кроме S_3, являются циклическими. **4.25.** Порядок элемента a равен 5. $\langle a \rangle = \left\{ a^0 = e,\ a^1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 1 & 6 \end{pmatrix},\ a^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 1 & 2 & 6 \end{pmatrix},\ a^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 1 & 2 & 3 & 6 \end{pmatrix},\ a^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 2 & 3 & 4 & 6 \end{pmatrix} \right\}$ – искомая подгруппа. **4.26.** $\langle a \rangle = \left\{ a^0 = e,\ a^1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix},\ a^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix},\ a^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \right\}$, $\langle b \rangle = \left\{ b^0 = e,\ b^1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix},\ b^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = a^2,\ b^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = a \right\}$, пересечение $\langle a \rangle \cap \langle b \rangle = \{e,\ a,\ a^2\}$ является циклической подгруппой. **4.27.** Данная группа – циклическая с образующим элементом b. Она имеет три подгруппы, вклю-

чая саму группу и $\{e\}$. **4.28.** Так как порядок элемента a равен 9, то искомые подгруппы будут: 1) сама группа $\langle a\rangle = \{e, a, a^2, ..., a^8\}$; 2) $\{e, a^3, a^6\}$; 3) $\{e\}$. **4.29.** а) Группа содержит лишь единичный элемент; б) циклическая группа простого порядка p; в) циклическая группа порядка p^2, где p – простое. **4.30.** Если $n \vdots m$, то $n = mq$, и $a^n = a^{mq} = (a^m)^q = e^q = e$. Обратно, пусть $a^n = e$. Разделив n на m с остатком, получим: $n = mq + r,\ 0 \le r < m$. Отсюда и из условия $a^n = e$ следует, что $a^r = e$, и $r = 0$ по определению порядка элемента. Значит, n делится на m. **4.33.** $m = 1, 2, 3, 4$. **4.34.** в) Коммутативная группа самосовмещений ромба состоит из элементов g_0, g_1, g_2, g_3, где g_0, g_1 – повороты ромба вокруг его центра на углы 0°, 180°; g_2, g_3 – отражения ромба относительно его диагоналей. При этом $g_1g_2 = g_3,\ g_1g_3 = g_2,\ g_2g_3 = g_1$; г) таблица умножения имеет вид:

	g_0	g_1	g_2	g_3
g_0	g_0	g_1	g_2	g_3
g_1	g_1	g_0	g_3	g_2
g_2	g_2	g_3	g_0	g_1
g_3	g_3	g_2	g_2	g_0

где g_0 и g_1 – повороты прямоугольника вокруг его центра на углы 0° и 180°, g_2 и g_3 – отражения прямоугольника относительно осей симметрии; д) $\{a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7\}$, где a_0, a_1, a_2, a_3 – повороты вокруг центра квадрата на углы $0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$; a_4, a_5, a_6, a_7 – отражения относительно осей симметрии квадрата (двух диагоналей и двух прямых, соеди-

няющих серидины противоположных сторон). Таблица умножения имеет вид:

	a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7
a_0	a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7
a_1	a_1	a_2	a_3	a_0	a_7	a_6	a_4	a_5
a_2	a_2	a_3	a_0	a_1	a_5	a_4	a_7	a_6
a_3	a_3	a_0	a_1	a_2	a_6	a_7	a_5	a_4
a_4	a_4	a_6	a_5	a_7	a_0	a_2	a_1	a_3
a_5	a_5	a_7	a_4	a_6	a_2	a_0	a_3	a_1
a_6	a_6	a_5	a_7	a_4	a_3	a_1	a_0	a_2
a_7	a_7	a_4	a_6	a_5	a_1	a_3	a_4	a_0

4.35. Группа состоит из n элементов: поворотов вокруг центра многоугольника на углы 0, α, 2α, 3α, $\ldots$, $(n-1)\alpha$, где $\alpha = \dfrac{2\pi}{n}$ радиан. **4.36.** в) Порядок единичного элемента g_0 равен 1, остальные элементы имеют порядок 2; д) порядок единичного элемента a_0 равен 1, элементы a_1 и a_3 (повороты на $\dfrac{\pi}{2}$, $\dfrac{3\pi}{2}$ соответственно) имеют порядок 4, остальные элементы этой группы имеют порядок 2. **4.37.** а) Группа $\mathbb{Z}_5$ имеет подгруппы: $\{\overline{0}\}$, $\mathbb{Z}_5$; группа $\mathbb{Z}_8$ имеет подгруппы: $\{\overline{0}\}$, $\{\overline{0}, \overline{4}\}$, $\{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$, $\mathbb{Z}_8$; группа $\mathbb{Z}_{10}$ имеет подгруппы: $\{\overline{0}\}$, $\{\overline{0}, \overline{5}\}$, $\{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}\}$, $\mathbb{Z}_{10}$; б) группа имеет подгруппы: $\{a_0, a_1, a_2, a_3\}$ (группа поворотов), $\{a_0, a_2\}$ (подгруппа, порожденная центральной симметрией a_2), $\{a_0, a_4\}$, $\{a_0, a_5\}$, $\{a_0, a_6\}$, $\{a_0, a_7\}$ (подгруппы, порожденные отражениями), а также две тривиальные подгруппы: $\{a_0\}$ и саму группу. **4.38.** Все подгруппы имеют вид: $\{\overline{0}, \overline{d}, 2\overline{d}, 3\overline{d}, \ldots, (k-1)\overline{d}\}$, где

d – любой делитель числа n, причем $n = kd$. **4.42.** Множество H является подгруппой группы G, так как H замкнуто относительно умножения и для любого элемента $(a, 0) \in H$ существует обратный элемент $(a, 0)^{-1} = (a^{-1}, 0) \in H$. Отображение $\varphi : H \to \mathbb{R}^*$, определенное правилом $\varphi((a, 0)) = a$, является изоморфизмом. **4.43.** Группы изоморфны, см. упр. 4.34 в) и г). **4.44.** а) Одна группа – циклическая группа 2-го порядка с элементами e, a и таблицей:

	e	a
e	e	a
a	a	e

б) Одна группа – циклическая группа 3-го порядка с элементами e, a, b и таблицей:

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Примером такой группы является подгруппа группы S_3, состоящая из элементов: $\left\{e = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right\}$. в) Две группы: 1) циклическая группа четвертого порядка с элементами e, a, b, c и таблицей:

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Примером такой группы является подгруппа группы S_4, состоящая из подстановок: $\left\{e = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}\right\}$;
2) четверная группа с элементами e, a, b, c и таблицей:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

В представлении подстановками элементы этой группы можно записать: $\left\{e = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}\right\}$.
г) Одна группа – циклическая группа 5-го порядка с элементами e, a, b, c, d и таблицей:

	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

Примером такой группы может служить группа поворотов правильного пятиугольника: поворотов вокруг центра пятиугольника на углы 0°, 72°, 144°, 216°, 288°.
4.45. Если в группе для любого элемента x выполняется $x^2 = e$, то см. упр. 4.11; в противном случае найти неперестановочные элементы x и y, для которых $x^2 = y^3 = e$.

§5. 5.1. б), в), д), з), к) Образует; а), г), е), ж), и) не образует. **5.2.** Нет. **5.3.** а) Нет; б) да. **5.4.** Нет. **5.5.** Да, все кольца.

5.7. Имеет, например: $\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0&0\\0&1\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$. **5.9.** Свойства коммутативности и ассоциативности сложения и умножения в $\mathbb{Q}^2$ вытекают из свойств соответствующих операций в поле рациональных чисел $\mathbb{Q}$, кроме того, умножение дистрибутивно относительно сложения. Нейтральным элементом по сложению в $\mathbb{Q}^2$ является пара $(0;0)$, а по умножению – $(1;1)$. Противоположным к элементу $(a;b)$ является элемент $(-a;-b)\in\mathbb{Q}^2$. Делителями нуля в $\mathbb{Q}^2$ служат пары $(a;0)$ и $(0;b)$, $a\neq 0$, $b\neq 0$. **5.10.** Не является: операция $\oplus$ не коммутативна. **5.11.** а) Имеем равенства $0=(x+y)+(-(x+y))$ и $0=(x+y)+(-(y+x))$, где $-(y+x)=(-1)(y+x)=-y+(-x)$. Откуда $-(x+y)=-(y+x)$ и $x+y=y+x$. б) Пусть R – некоммутативная группа. Назовем операцию в R «сложением» в кольце, а «произведение» любых двух элементов из R положим равным нейтральному элементу группы – «нулю». Получим некоммутативное кольцо. **5.12.** 4. **5.13.** 2. **5.15.** а) $0=(a+b)^2=a^2+ab+ba+b^2=ab+ba$. **5.16.** Все подкольца имеют тот же вид, что и подгруппы аддитивной группы $\mathbb{Z}$, т.е. $H_0, H_1, H_2, \ldots$, где $H_0=\{0\}$, а $H_n=\{nk|k\in\mathbb{Z}\}$. **5.18.** В задаче 5.17 вместо 5 можно взять другое число.

§6. 6.1. В задаче 5.1: в) поле, в задаче 5.5: б) поле. **6.2.** а) Если $\sqrt{n}\notin\mathbb{Q}$. б) Если $n<0$. в) $n=2$ при $p=3$; $n=2,3$ при $p=5$; $n=3,5,6$ при $p=7$. **6.3.** Единичным элементом является число 2. **6.5.** По определению поле должно содержат более одного элемента. **6.6.** Поле. Нулем является a, единицей – b. **6.8.** Например, множество матриц указанного вида, где $a,b\in\mathbb{Q}$, или множество матриц в которых $b=0$. **6.10.** Обратным элементом к

числу $1-\sqrt[3]{2}+2\sqrt[3]{4}$ является $\frac{1}{43}\left(5+9\sqrt[3]{2}-\sqrt[3]{4}\right)$. **6.12.** Единица не может являться характеристикой поля, так как условие $1e=e=0$ противоречит определению поля. Допустим, что характеристика p поля P – составное число. Тогда $p=ab$, где $1<a<p$, $1<b<p$, и $pe=(ab)e=(ae)(be)=0$. Отсюда, учитывая, что в поле нет делителей нуля, получаем: $ae=0$ или $be=0$. Но то и другое противоречит минимальности числа p. Следовательно, p – простое число. **6.13.** Мультипликативная группа поля из четырех элементов имеет порядок 3, и для построения такого поля достаточно иметь матрицу 2-го порядка над полем $\mathbb{Z}_2$, для чего достаточно, чтобы она удовлетворяла уравнению $A^2+A+E=\Theta$, т.е. $\operatorname{tr}A=\det A=1$ (здесь через trA обозначена сумма элементов главной диагонали матрицы, называемая следом матрицы). Такая матрица $\begin{pmatrix}0&1\\1&1\end{pmatrix}$, и поле состоит элементов Θ, E, A, $A+E$; при $n=6$ рассмотреть порядки элементов в аддитивной группе. **6.14.** В поле $\mathbb{Z}_5$ уравнение $2x=3$ имеет решение $x=4$, уравнение $3x=3$ имеет решение $x=1$, $3x=2$ имеет решение $x=4$, уравнение $5x^2=2$ решений не имеет. В поле $\mathbb{Z}_7$ уравнение $2x=3$ имеет решение $x=5$, $3x=3$ имеет решение $x=1$, $3x=2$ имеет решение $x=3$, уравнение $5x^2=2$ решений не имеет. В поле $\mathbb{Z}_{17}$ уравнение $2x=3$ имеет решение $x=10$, $3x=3$ имеет решение $x=1$, $3x=2$ имеет решение $x=12$, уравнение $5x^2=2$ решений не имеет. **6.15.** Над полем $\mathbb{Z}_5$ система имеет единственное решение $(2,3,2)$, над полем $\mathbb{Z}_7$ система имеет единственное решение $(5,6,5)$. **6.16.** Пусть $R=\{r_0=0,r_1=1,...,r_{n-1}\}$ – кольцо из n элементов без делителей нуля. Для любого $r_k\neq 0$ $(1\leq k\leq n-1)$

все произведения $r_k r_1, ..., r_k r_{n-1}$ различны, поскольку r_k не является делителем нуля. Следовательно, найдется i для которого $r_k r_i = 1$, т.е. $r_i = r_k^{-1}$. **6.18.** $b = a(a-1)^{-1}$ и откуда следуют требуемые равенства. Обратно, из равенства $(1-a)+c = (1-a)c = c(1-a)$ для любого $c \in R$ следует $1-a+c = c-ac$, откуда $a(1-c) = (1-c)a = 1$.

§7. 7.1. а) $12+5i$, б) $4i$, в) 0, г) 4, д) $2+i$, е) $\frac{19}{5} - \frac{43}{5}i$, ж) $\frac{127}{2} + \frac{\sqrt{3}}{2}i$, з) $\frac{44}{318} - \frac{\sqrt{5}}{318}i$, и) $2i^{n-1}$. **7.2.** $-i$. **7.3.** $i^n = 1$ при $n = 4k$, $i^n = i$ при $n = 4k+1$, $i^n = -1$ при $n = 4k+2$, $i^n = -i$ при $n = 4k+3$, где k – целое число; $i^{77} = i$; $i^{98} = -1$; $i^{-57} = -i$. **7.5.** а) $z_1 = 2, z_2 = 1-i$, б) $\emptyset$. **7.6.** а) $(5;3)$, б) $(2;3)$, в) $\left(-\frac{1}{8}; \frac{3}{4}\right)$, г) $y = -1$, д) $\left(-\frac{4}{11}; \frac{5}{11}\right)$, е) $(4;2)$. **7.7.** $x_1 = 2, x_2 = -2$. **7.8.** $x_1 = 1, x_2 = -1$. **7.9.** а) при любых $t \in \mathbb{R}$, б) при $t = -\frac{1}{2}$. **7.10.** а) $\sqrt{65}$, б) $2\sqrt{10}$. **7.11.** а) $z_1 = 2-i, z_2 = -2+i$, б) $z_1 = -2+i, z_2 = -3+i$, в) $z_1 = 2i, z_2 = -1$, г) $z_1 = 1+2i, z_2 = 3i$, д) $z_1 = 5-2i, z_2 = 2i$. **7.14.** $(1;1), (-1;1)$. **7.15.** Множество $\mathbb{R}$. **7.16.** Сопряжены. **7.19.** $z = -4,8 + 6,4i$. **7.20.** Да. **7.21.** а) $5(\cos 0 + i \sin 0)$, б) $\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}$, в) $\sqrt{2}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right)$, г) $\cos\left(-\frac{\pi}{2}\right) + i\sin\left(-\frac{\pi}{2}\right)$, д) $2(\cos\pi + i\sin\pi)$, е) $3\left(\cos\left(-\frac{\pi}{2}\right) + i\sin\left(-\frac{\pi}{2}\right)\right)$, ж) $2\left(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}\right)$, з) $2\left(\cos\frac{5\pi}{6} + i\sin\frac{5\pi}{6}\right)$, и) $2\left(\cos\left(-\frac{5\pi}{6}\right) + i\sin\left(-\frac{5\pi}{6}\right)\right)$, к) $2\left(\cos\left(-\frac{\pi}{6}\right) + i\sin\left(-\frac{\pi}{6}\right)\right)$, л) $2\left(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}\right)$, м) $2\left(\cos\left(-\frac{2\pi}{3}\right) + i\sin\left(-\frac{2\pi}{3}\right)\right)$, н) $\cos\left(\frac{\pi}{2} - \alpha\right) +$

$i\sin\left(\frac{\pi}{2}-\alpha\right)$, о) $\cos(\varphi-\psi)+i\sin(\varphi-\psi)$. **7.22.** а) 0; аргумент не определен, б) 64; $-\frac{4}{15}\pi$. **7.23.** а) $\frac{1}{2}+\frac{\sqrt{3}}{2}i$, б) $2i$, в) $-1+i$, г) $\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i$. **7.26.** а) Замкнутый круг радиуса 3 с центром в начале координат. б) Множество точек, находящихся вне круга радиуса 3 с центром в начале координат. в) Открытый круг радиуса 1 с центром в точке $3i$. г) Множество точек, находящихся вне круга радиуса 2 с центром в точке $-3+2i$. д) Внутренность полосы, заключенной между прямыми $y=\pm 2$. е) Множество всех точек, расположенных справа от прямой $x=\sqrt{2}$ и слева от прямой $x=-\sqrt{2}$, включая эти прямые. ж) Пересечение двух областей: множество точек, находящихся вне круга радиуса 0,2 с центром в начале координат и полуплоскости $x<y$, без прямой $y=x$. з) Луч, исходящий из начала координат под углом $\frac{\pi}{2}$; и) луч, исходящий из начала координат под углом $310°$. к) Внутренность угла, образованного положительной вещественной полуосью и лучом, выходящим из начала координат под углом $-\frac{\pi}{4}$ к этой полуоси, не включая этот луч. л) Эллипс с фокусами в точках 3 и $2i$. м) Гипербола с фокусами в точках 4 и $2i$. н) Часть кольца, образованного окружностями, включая и границы, радиусов 1 и 2 с центром в начале координат, ограниченная прямыми $y=-\sqrt{3}$, $y=0$, включая эти прямые. о) Пересечение двух областей: внутренность круга с радиусом 1 и центром в точке $-i$ и множество точек, находящихся вне круга радиуса 1 с центром в точке -1, включая границу. **7.27.** Если $z=x+yi$, то $\operatorname{Re}\left(\frac{3}{z}\right)=\frac{3x}{x^2+y^2}$, а $\operatorname{Im}\left(\frac{1}{z}-1\right)=-\frac{y}{x^2+y^2}$.

Следовательно, заданное условие принимает вид: $\frac{3x}{x^2+y^2} \geq \frac{-y}{x^2+y^2}$. Откуда искомое множество – полуплоскость $y \geq -3x$ с исключенной точкой 0. **7.28.** Пусть $z = x + yi$, тогда $\operatorname{Re} z = x, \operatorname{Im} z = y$, $\frac{\operatorname{Re} z}{\operatorname{Im} z} = \frac{x}{y} = k$ и $|z + 4 - 3i| = \sqrt{(x+4)^2 + (y-3)^2} \leq 1$. Следовательно, получаем систему $\begin{cases} (x+4)^2 + (y-3)^2 \leq 1, \\ y = \frac{1}{k}x. \end{cases}$

Тогда диапазон изменения величины $\frac{1}{k}$ ограничен угловыми коэффициентами прямых – касательных к окружности $(x + 4)^2 + (y - 3)^2 = 1$, проведенных из точки 0: $-\operatorname{tg}\left(\operatorname{arctg}\frac{3}{4} - \arcsin\frac{1}{5}\right) \leq \frac{1}{k} \leq -\operatorname{tg}\left(\arcsin\frac{1}{5} - \operatorname{arctg}\frac{3}{4}\right)$. Найдем числовые выражения для границ диапазона: $\operatorname{tg}\left(\arcsin\frac{1}{5}\right) = \frac{1}{\sqrt{24}}$, $\operatorname{tg}\left(\operatorname{arctg}\frac{3}{4} - \arcsin\frac{1}{5}\right) = \frac{4}{6+\sqrt{6}}$. Аналогично можно получить, $\operatorname{tg}\left(\arcsin\frac{1}{5} + \operatorname{arctg}\frac{3}{4}\right) = \frac{4}{6-\sqrt{6}}$. Итак, $-\frac{4}{6+\sqrt{6}} \leq \frac{1}{k} \leq -\frac{4}{6-\sqrt{6}}$, значит, $-\frac{6-\sqrt{6}}{4} \geq k \geq -\frac{6+\sqrt{6}}{4}$. Таким образом, областью изменения выражения $\frac{\operatorname{Re} z}{\operatorname{Im} z}$ является интервал $\left[-\frac{6+\sqrt{6}}{4}; -\frac{6-\sqrt{6}}{4}\right]$. **7.29.** а) Сдвинуть вектор z на

вектор $\overline{a}(-3;0)$. б) Повернуть радиус-вектор точки z на угол $\frac{\pi}{2}$ против часовой стрелки. в) Перенести радиус-вектор точки z на вектор $\overline{a}(2;-1)$. **7.30.** а) 2^{500}, б) 2^{150}, в) -2^{30}, г) $(2+\sqrt{3})^{12}$, д) $2^{15}i$, е) -64. **7.31.** $2^{16}\cdot\cos^{16}\left(\dfrac{\pi-2\varphi}{4}\right)(\cos 8\varphi - i\sin 8\varphi)$. **7.32.** $z^{12}=-64$. **8.33.** $\sin 5x = 5\cos^4 x\sin x - 10\cos^2 x\sin^3 x + \sin^5 x, \cos 5x = \cos^5 x - 10\cos^3 x\sin^2 x + 5\cos x\sin^4 x$. **7.35.** а) $1,\ -\dfrac{1}{2}\pm i\dfrac{\sqrt{3}}{2}$, б) $\dfrac{\sqrt{3}}{2}+\dfrac{1}{2}i,\ -\dfrac{\sqrt{3}}{2}+\dfrac{1}{2}i,\ -i$,

в) $\cos\dfrac{(4k+1)\pi}{12}+i\sin\dfrac{(4k+1)\pi}{12}\qquad(0\le k\le 5)$,

г) $2\sqrt{1}$, д) $\pm\dfrac{\sqrt{3}}{2}(\sqrt{3}+i),\ \pm i\sqrt{3},\ \pm\dfrac{\sqrt{3}}{2}(\sqrt{3}-i)$,

е) $\sqrt{3}+i,\ -\sqrt{3}+i,\ -2i$,

ж) $2\left(\cos\dfrac{(6k-1)\pi}{30}+i\sin\dfrac{(6k-1)\pi}{30}\right)\quad(0\le k\le 9)$,

з) $\sqrt[4]{2}\left(\cos\dfrac{(8k-1)\pi}{32}+i\sin\dfrac{(8k-1)\pi}{32}\right)\quad(0\le k\le 7)$,

и) $\pm\left(\dfrac{3}{2}+i\dfrac{\sqrt{3}}{2}\right),\ \pm\left(\dfrac{\sqrt{3}}{2}-i\dfrac{3}{2}\right)$, к) $\pm\dfrac{\sqrt{2}}{2}\pm i\dfrac{\sqrt{2}}{2}$,

л) $2i,\ -\sqrt{3}-i,\ \sqrt{3}-i$. **7.36.** а) $z_{1,2}=\pm i,\quad z_{3,4}=\dfrac{1\pm\sqrt{3}i}{2}$,

б) $z_{1,2}=\pm 1,\quad z_{3,4}=\pm i,\quad z_{5,6}=\pm 2,\quad z_{7,8}=\pm 2i$,

в) $z=\dfrac{4}{3}-i$. **7.37.** $a=10$. **7.38.** Преобразуем выражение x_1: $\left(\sin\dfrac{5\pi}{8}+i\cos\dfrac{5\pi}{8}\right)^4 = \left(\sin\left(\dfrac{\pi}{2}+\dfrac{\pi}{8}\right)+i\cos\left(\dfrac{\pi}{2}+\dfrac{\pi}{8}\right)\right)^4 = \left(\cos\dfrac{\pi}{8}-i\sin\dfrac{\pi}{8}\right)^4 =$

$= \left(\cos\left(\pi - \frac{7\pi}{8}\right) - i\sin\left(\pi - \frac{7\pi}{8}\right)\right)^4 =$
$\left(-\cos\frac{7\pi}{8} - i\sin\frac{7\pi}{8}\right)^4 = \left(\cos\frac{7\pi}{8} + i\sin\frac{7\pi}{8}\right)^4 =$
$\cos\left(4\cdot\frac{7\pi}{8}\right) + i\sin\left(4\cdot\frac{7\pi}{8}\right) = \cos\frac{7\pi}{2} + i\sin\frac{7\pi}{2} = 0 - i =$
$-i$. Итак, $x_1 = -i$. Поскольку x_1 – корень уравнения, мы имеем ${x_1}^3 + (a-2){x_1}^2 + a^2x_1 - 2a^2 - 1 = 0$; $(-i)^3 + (a-2)(-i)^2 + a^2(-i) - 2a^2 - 1 = 0$; $i-(a-2)-a^2i-2a^2-1=0$; $-(2a^2+a-2+1)+(1-a^2)i=0$, что возможно только, если $\begin{cases} 2a^2+a-1=0, \\ 1-a^2=0, \end{cases}$ т.е. только при $a=-1$. При $a=-1$ уравнение примет вид $x^3-3x^2+x-3 = x^2(x-3)+(x-3) = (x^2+1)(x-3) = 0$. Значит, $x_2 = i$, $x_3 = 3$. Итак, $\{-i, i, 3\}$ – множество всех корней уравнения. **7.39.** $\{\pm1\}$, $\left\{1, \frac{1}{2} \pm i\frac{\sqrt{3}}{2}\right\}$, $\{\pm1, \pm i\}$, $\left\{\pm1, \pm\frac{1}{2}(1+i\sqrt{3}), \pm\frac{1}{2}(1-i\sqrt{3})\right\}$, $\left\{\pm1, \pm i, \pm\frac{\sqrt{2}}{2}(1+i), \pm\frac{\sqrt{2}}{2}(1-i)\right\}$, $\left\{\pm i, \pm\frac{1}{2}(1+i\sqrt{3}), \pm\frac{1}{2}(\sqrt{3}+i), \pm\frac{1}{2}(\sqrt{3}-i)\right\}$. **7.40.** $(-1)^{n-1}$; все сомножители, отличные от 1 и -1, разбить на пары взаимно обратных. **7.43.** ε и $\overline{\varepsilon}$ имеют одинаковые порядки.

Список литературы

[1] Александрова Н. В. *История математических терминов, понятий, обозначений.* – М.: URSS, 2008.

[2] Бутузов В. Ф., Крутицкая И. Д., Шишкин А. А. *Линейная алгебра в вопросах и задачах.* – М.: Физматлит, 2003.

[3] Варпаховский Ф. Л., Солодовников А. С., Стеллецкий И.В. *Алгебра. Группы, кольца, поля. Векторные и евклидовы пространства. Линейные отображения.* – М.: Просвещение, 1978.

[4] Винберг Э. Б. *Курс алгебы.* – М.: Факториал, 2002.

[5] Глухов М. М. *Алгебра и аналитическая геометрия.* – М.: Гелиос АРВ, 2005.

[6] Глухов М. М., Елизаров В. П., Нечаев А. А. *Алгебра.* – М.: Гелиос АРВ, 2003.

[7] Глухов М. М., Солодовников А. С. *Задачник-практикум по курсу высшей алгебры.* – М.: Просвещение, 1965.

[8] Дураков Б. К. *Краткий курс высшей алгебы.* – М.: ФИЗМАТЛИТ, 2006.

[9] Ермолаеева Н. Н., Козынченко В. А., Курбатова Г. И. *Практические занятия по алгебре. Элементы теории множеств, теории чисел, комбинаторики. Алгебраиченские структуры.* – СПб.: Лань, 2014.

[10] Журавлев Ю. И., Флеров Ю. А., Вялый М. Н. *Дискретный анализ. Основы высшей алгебры.* – М.: МЗ Пресс, 2007.

[11] Крылов П. А., Туганбаев А. А., Чехлов А. Р. *Задачи по теории колец, модулей и полей.* – М.: Факториал Пресс, 2007.

[12] Крючков Н. И., Крючкова В. В. *Сборник заданий по алгебре.* – М.: Академия, 2007.

[13] Кострикин А. И. *Введение в алгебру. Ч. I. Основы алгебры.* – М.: Физматлит, 2001.

[14] Кострикин А. И. (ред.) *Сборник задач по алгебре* – М.: Физматлит, 2001.

[15] Куликов Л. Я. *Алгебра и теория чисел.* – М.: Высшая школа, 1979.

[16] Куликов Л. Я., Москаленко А. И., Фомин А. А. *Сборник задач по алгебре и теории чисел.* – М.: Просвещение, 1993.

[17] Курош А. Г. *Курс высшей алгебры.* – СПб.: Лань, 2007.

[18] Лавров И. А., Максимова Л. Л. *Задачи по теории множеств, математической логике и теории алгоритмов.* – М.: Физматлит, 2004

[19] Ларин С. В. *Группы, кольца и поля.* – Красноярск: Краснояр.гос.пед.ун-т им. В.П. Астафьева, 2010.

[20] Лунгу К. Н., Письменный Д. Т., Федин С. Н., Шевченко Ю. А. *Сборник задач по высшей математике.* – М.: АЙРИС-пресс, 2001.

[21] Михалев А. А., Михалев А. В. *Начала алгебры, часть I.* – М.: Интернет-Университет Информационных Технологий, 2009.

[22] Нечаев В. А. *Задачник-практикум по алгебре.* – М.: Просвещение, 1983.

[23] Окунев Л. Я. *Высшая алгебра.* – СПб.: Лань, 2009.

[24] Проскуряков И. В. *Сборник задач по линейной алгебре.* – М.: Лаборатория Базовых Знаний, 2001.

[25] Тимофеева И. Л., Сергеева И. Е., Лукьянова Е. В. *Вводный курс математики.* – М.: Академия, 2011.

[26] Фаддеев Д. К. *Лекции по алгебре.* – М.: Наука, 1984.

[27] Фаддеев Д. К., Соминский И. С. *Сборник задач по высшей алгебре.* – М.: Наука, 1977.

[28] Чехлов А. Р. *Упражнения по основам теории групп.* – Томск: Томский государственный университет, 2004.

[29] Шахмейстер А. Х. *Комплексные числа.* – М.: МЦНМО, 2011.

Указатель обозначений

Указатель терминов