А. В. Овчинников

ЛЕКЦИИ ПО АЛГЕБРЕ

Часть 1

МОСКВА

2026

Оглавление

ГЛАВА 1

Вводные замечания

ИНТЕЛЛЕКТУАЛЬНОЕ *содержание* математических концепций и теорий теснейшим образом связано с *формой* их представления. Хорошо продуманные обозначения позволяют не только отражать свойства изучаемых объектов, но также помогают избежать ошибок и переносить часть исследования на технический уровень, а в некоторых случаях даже подсказывают путь решения задачи. На раннем этапе развития науки математические утверждения формулировались словесно; это часто приводило к неоднозначным трактовкам и громоздким рассуждениям. Позднее в математический обиход вошли буквенные обозначения и специальные символы, привычные сегодня, и математика обрела собственный язык с чётко определённым смыслом выражений и строгой «грамматикой».

1. Математическая символика

А. Математический алфавит.

1.1. Для записи математических выражений используются, прежде всего, арабские цифры

$$0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9$$

и буквы русского, латинского и греческого алфавитов в различных шрифтовых начертаниях: прямом, наклонном (курсивном), готическом, каллиграфическом, ажурном. Эти символы приведены в таблицах 1 и 2.

1.2. Часто буквы снабжают верхними и/или нижними индексами и различными диакритическими знаками:

$$A_i,\ B_{jk},\ C^{\alpha}_{\beta},\ \dot{a},\ \widetilde{A},\ \widehat{B},\ \overrightarrow{AB}.$$

Кроме того, широко используются многочисленные специальные знаки и скобки:

$$=\ +\ -\ \times\ >\ <\ \geqslant\ \leqslant\ \subset\ \cap\ \cup\ \int\ \oint\quad (\,)\quad [\,]\quad \{\,\}\quad \langle\,\rangle.$$

Таблица 1. Латинский алфавит: обычное начертание (столбец 1), курсивное начертание (столбец 2), жирный шрифт (столбец 3), жирный курсив (столбец 4), готический шрифт (столбец 5), каллиграфический шрифт (столбец 6), рукописный шрифт (столбец 7), ажурный шрифт (столбец 8).

1	2	3	4	5	6	7	8	Название
A a	$A\ a$	**A a**	$\boldsymbol{A\ a}$	$\mathfrak{A}\ \mathfrak{a}$	$\mathcal{A}$	$\mathscr{A}$	$\mathbb{A}$	а
B b	$B\ b$	**B b**	$\boldsymbol{B\ b}$	$\mathfrak{B}\ \mathfrak{b}$	$\mathcal{B}$	$\mathscr{B}$	$\mathbb{B}$	бэ
C c	$C\ c$	**C c**	$\boldsymbol{C\ c}$	$\mathfrak{C}\ \mathfrak{c}$	$\mathcal{C}$	$\mathscr{C}$	$\mathbb{C}$	цэ
D d	$D\ d$	**D d**	$\boldsymbol{D\ d}$	$\mathfrak{D}\ \mathfrak{d}$	$\mathcal{D}$	$\mathscr{D}$	$\mathbb{D}$	дэ
E e	$E\ e$	**E e**	$\boldsymbol{E\ e}$	$\mathfrak{E}\ \mathfrak{e}$	$\mathcal{E}$	$\mathscr{E}$	$\mathbb{E}$	е, э
F f	$F\ f$	**F f**	$\boldsymbol{F\ f}$	$\mathfrak{F}\ \mathfrak{f}$	$\mathcal{F}$	$\mathscr{F}$	$\mathbb{F}$	эф
G g	$G\ g$	**G g**	$\boldsymbol{G\ g}$	$\mathfrak{G}\ \mathfrak{g}$	$\mathcal{G}$	$\mathscr{G}$	$\mathbb{G}$	же, гэ
H h	$H\ h$	**H h**	$\boldsymbol{H\ h}$	$\mathfrak{H}\ \mathfrak{h}$	$\mathcal{H}$	$\mathscr{H}$	$\mathbb{H}$	аш, ха
I i	$I\ i$	**I i**	$\boldsymbol{I\ i}$	$\mathfrak{I}\ \mathfrak{i}$	$\mathcal{I}$	$\mathscr{I}$	$\mathbb{I}$	и
J j	$J\ j$	**J j**	$\boldsymbol{J\ j}$	$\mathfrak{J}\ \mathfrak{j}$	$\mathcal{J}$	$\mathscr{J}$	$\mathbb{J}$	жи, йот
K k	$K\ k$	**K k**	$\boldsymbol{K\ k}$	$\mathfrak{K}\ \mathfrak{k}$	$\mathcal{K}$	$\mathscr{K}$	$\mathbb{K}$	ка
L l	$L\ l$	**L l**	$\boldsymbol{L\ l}$	$\mathfrak{L}\ \mathfrak{l}$	$\mathcal{L}$	$\mathscr{L}$	$\mathbb{L}$	эль
M m	$M\ m$	**M m**	$\boldsymbol{M\ m}$	$\mathfrak{M}\ \mathfrak{m}$	$\mathcal{M}$	$\mathscr{M}$	$\mathbb{M}$	эм
N n	$N\ n$	**N n**	$\boldsymbol{N\ n}$	$\mathfrak{N}\ \mathfrak{n}$	$\mathcal{N}$	$\mathscr{N}$	$\mathbb{N}$	эн
O o	$O\ o$	**O o**	$\boldsymbol{O\ o}$	$\mathfrak{O}\ \mathfrak{o}$	$\mathcal{O}$	$\mathscr{O}$	$\mathbb{O}$	о
P p	$P\ p$	**P p**	$\boldsymbol{P\ p}$	$\mathfrak{P}\ \mathfrak{p}$	$\mathcal{P}$	$\mathscr{P}$	$\mathbb{P}$	пэ
Q q	$Q\ q$	**Q q**	$\boldsymbol{Q\ q}$	$\mathfrak{Q}\ \mathfrak{q}$	$\mathcal{Q}$	$\mathscr{Q}$	$\mathbb{Q}$	ку
R r	$R\ r$	**R r**	$\boldsymbol{R\ r}$	$\mathfrak{R}\ \mathfrak{r}$	$\mathcal{R}$	$\mathscr{R}$	$\mathbb{R}$	эр
S s	$S\ s$	**S s**	$\boldsymbol{S\ s}$	$\mathfrak{S}\ \mathfrak{s}$	$\mathcal{S}$	$\mathscr{S}$	$\mathbb{S}$	эс
T t	$T\ t$	**T t**	$\boldsymbol{T\ t}$	$\mathfrak{T}\ \mathfrak{t}$	$\mathcal{T}$	$\mathscr{T}$	$\mathbb{T}$	тэ
U u	$U\ u$	**U u**	$\boldsymbol{U\ u}$	$\mathfrak{U}\ \mathfrak{u}$	$\mathcal{U}$	$\mathscr{U}$	$\mathbb{U}$	у
V v	$V\ v$	**V v**	$\boldsymbol{V\ v}$	$\mathfrak{V}\ \mathfrak{v}$	$\mathcal{V}$	$\mathscr{V}$	$\mathbb{V}$	вэ
W w	$W\ w$	**W w**	$\boldsymbol{W\ w}$	$\mathfrak{W}\ \mathfrak{w}$	$\mathcal{W}$	$\mathscr{W}$	$\mathbb{W}$	дубль-вэ
X x	$X\ x$	**X x**	$\boldsymbol{X\ x}$	$\mathfrak{X}\ \mathfrak{x}$	$\mathcal{X}$	$\mathscr{X}$	$\mathbb{X}$	икс
Y y	$Y\ y$	**Y y**	$\boldsymbol{Y\ y}$	$\mathfrak{Y}\ \mathfrak{y}$	$\mathcal{Y}$	$\mathscr{Y}$	$\mathbb{Y}$	игрек
Z z	$Z\ z$	**Z z**	$\boldsymbol{Z\ z}$	$\mathfrak{Z}\ \mathfrak{z}$	$\mathcal{Z}$	$\mathscr{Z}$	$\mathbb{Z}$	зэт

Таблица 2. Греческий алфавит

A α	альфа	I ι	йота	P ρ ϱ	ро
B β	бета	K κ $\varkappa$	каппа	Σ σ ς	сигма
Γ γ	гамма	Λ λ	лямбда	T τ	тау
Δ δ	дельта	M μ	мю (ми)	Υ υ	ипсилон
E ε ϵ	эпсилон	N ν	ню (ни)	Φ φ ϕ	фи
Z ζ	дзета	Ξ ξ	кси	X χ	хи
H η	эта	O o	омикрон	Ψ ψ	пси
Θ θ ϑ	тэта	Π π ϖ	пи	Ω ω	омега

1.3. Многие символы раз и навсегда зарезервированы для часто встречающихся объектов; например, буквы ажурного шрифта $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$ традиционно используются для обозначения множеств натуральных, целых, рациональных, вещественных и комплексных чисел соответственно.

Б. Переменные.

1.4. Под *переменной* в математике понимается символ (обычно буква или буква с индексами), служащий для обозначения произвольного объекта из некоторой фиксированной совокупности объектов, называемой *областью возможных значений* рассматриваемой переменной. Часто область возможных значений переменной явно не указывается, но из контекста ясно, какова эта область.

1.5. Если переменная употребляется таким образом, что допускается подстановка вместо неё любых объектов из области её возможных значений, то переменная называется *свободной*.

1.6. Однако в математике встречается и другое употребление переменных, при котором не предполагается и не допускается подстановка конкретных объектов вместо переменной. Например, в выражении

$$\int_0^1 x^3\,dx,$$

где x — вещественная числовая переменная, нельзя подставлять вместо x какие-либо конкретные числа: например, запись

$$\int_0^1 5^3\,d5$$

бессмысленна. В таких случаях, т.е. когда по смыслу выражения, содержащего переменную, подстановка конкретных объектов вместо переменной недопустима, эта переменная называется *связанной*. В сущности, связанная переменная не является переменной; её было естественно считать переменной на некотором (раннем) этапе образования рассматриваемого выражения из более простых выражений.

1.7. Связанную переменную можно произвольным образом переименовать (т.е. обозначить другой буквой), при этом смысл выражения не изменится; так,

$$\int_0^1 x^3\,dx = \int_0^1 y^3\,dy = \int_0^1 \xi^3\,d\xi = \frac{1}{4}.$$

1.8. В одном выражении могут встречаться одновременно и свободные, и связанные переменные; например, в выражении

$$\int_0^1 (xy)^3\,dx$$

переменная x является связанной, а y — свободной. Различение свободных и связанных вхождений переменной в выражение важно для правильного понимания смысла выражения.

В. Знак равенства. Символ $=$ используется в математике в разных смыслах.

1.9. Чаще всего символ $=$ употребляется в смысле, описываемом словами «два имени одного и того же объекта». Например, выражение $2 \cdot 6 = 3 \cdot 4$ означает, что $2 \cdot 6$ и $3 \cdot 4$ — два имени одного и того же числа (одно и то же число). Этот смысл символа $=$ будем считать его главным смыслом.

1.10. В другом смысле символ $=$ используется в уравнениях; например, когда рассматривается уравнение $x + 2 = 4$, то вовсе не утверждается, что $x + 2$ и 4 — два имени одного и того же, но требуется найти такие x, что значения выражений $x+2$ и 4 совпадают.

1.11. Для указания тождественного равенства двух выражений (т.е. их совпадения для всех значений переменных из области возможных значений) вместо символа $=$ часто используется символ $\equiv$; например, $(x + y)^2 \equiv x^2 + 2xy + y^2$ для всех вещественных чисел x

и y; $\dfrac{x^2-1}{x-1} \equiv x+1$ для всех вещественных $x \neq 1$ (здесь требуется указание о том, для каких значений переменной имеет место тождественное равенство).

1.12. В *определениях* символ $=$ имеет смысл знака присваивания имени вновь определяемому понятию, например, $n! = 1 \cdot 2 \cdot \ldots \cdot n$ при $n \geqslant 1$: здесь слева от знака $=$ стоит имя $n!$, которым обозначается произведение всех последовательных натуральных чисел от 1 до n включительно (*факториал* натурального числа n). В случаях, когда символ $=$ используется в указанном смысле, часто употребляются символы $\overset{\text{def}}{=\!=}$ и $:=$ («равенство по определению»); так, в рассмотренном примере лучше записать $n! \overset{\text{def}}{=\!=} 1 \cdot 2 \cdot \ldots \cdot n$ или $n! := 1 \cdot 2 \cdot \ldots \cdot n$.

1.13. Упомянем ещё одно широко распространённое обозначение. Тот факт, что целочисленная переменная j принимает значения в множестве $\{m, m+1, \ldots, m+n\}$, состоящем из последовательных целых чисел, записывается тремя равносильными способами:

$$j \in \{m, m{+}1, \ldots, m{+}n\}; \quad j = m, m{+}1, \ldots, m{+}n; \quad j = \overline{m, m+n}.$$

2. Логические операции

А. Логика высказываний.

1.14. *Высказывание* — это предложение, про которое разумно говорить, что оно истинно или ложно. Фразы «Есть ли жизнь на Марсе?» и «Добро пожаловать!» не являются высказываниями (как и любые вопросительные или восклицательные предложения). Определение «треугольник *называется* равносторонним, если все его стороны равны между собой» — *не* высказывание (как и вообще любое *определение*), но фраза «если все стороны треугольника равны, то он *является* равносторонним» — истинное (в силу только что приведённого определения) высказывание. Фразы «$2 + 2 = 4$» и «$5 > 7$» — высказывания (первое — истинное, второе — ложное), а $2 + 3$ — не высказывание.

Итак, *логическое высказывание* — это повествовательное предложение, которое формализует некоторое выражение мысли и представляет собой утверждение, которому можно поставить в соответствие одно из двух логических значений: ложь (0) или истина (1). Для обозначения высказываний будем использовать прописные латинские буквы.

1.15. Из высказываний можно образовывать новые высказывания при помощи основных *логических операций*, которые удобно определять с помощью таблиц истинности.

1.16. Определение. *Отрицание* — логическая операция, в результате которой из данного высказывания A получается новое высказывание $\neg A$ («не-A», «неверно, что A», «A не имеет места») по следующему правилу:

A	$\neg A$
0	1
1	0

(1.1)

В классической логике справедлив *закон исключенного третьего*, утверждающий, что из двух высказываний A и $\neg A$ одно и только одно обязательно является истинным.

1.17. Определение. *Конъюнкция* — логическая операция, которая заключается в соединении двух высказываний A и B в новое высказывание $A \wedge B$ («A и B») по следующему правилу:

A	B	$A \wedge B$
0	0	0
0	1	0
1	0	0
1	1	1

(1.2)

Из таблицы истинности видно, что высказывание $A \wedge B$ истинно только в том случае, когда оба высказывания A и B истинны. Например, высказывание «$2 < 3$ и 4 — чётное число» истинно, а высказывания «$2 < 3$ и 5 — чётное число», «$2 > 3$ и 5 — чётное число» ложны.

1.18. Определение. *Дизъюнкция* — логическая операция, которая заключается в соединении двух высказываний A и B в новое высказывание $A \vee B$ («A или B») по следующему правилу:

A	B	$A \vee B$
0	0	0
0	1	1
1	0	1
1	1	1

(1.3)

Из таблицы истинности видно, что высказывание $A \vee B$ ложно только в том случае, когда оба высказывания A и B ложны. Например,

высказывание «$2 > 3$ или 5 — чётное число» ложно, а высказывания «$2 < 3$ или 5 — чётное число», «$2 < 3$ или 4 — чётное число» истинны.

1.19. Определение. *Импликация* — логическая операция, которая заключается в соединении двух высказываний A и B в новое высказывание $A \Rightarrow B$ («если A, то B») по следующему правилу:

A	B	$A \Rightarrow B$
0	0	1
0	1	1
1	0	0
1	1	1

(1.4)

Высказывание A называется *посылкой* (или *антецедентом*) высказывания $A \Rightarrow B$, высказывание B — его *заключением* (*консеквентом*).

1.20. В обыденной речи утверждение «если A, то B», как правило, предполагает наличие причинной связи между тем, что утверждается в высказывании A, и тем, что утверждается в высказывании B, и его истинность зависит от смысла этих высказываний. В логике учитывается лишь истинность или ложность высказываний, но не их смысл и тем более причинная связь.

Импликация двух высказываний ложна лишь в одном случае — когда посылка истинна, а заключение ложно. Импликация с ложной посылкой по определению истинна; например высказывания «если $2^2 = 5$, то $3^2 = 9$», «если $2^2 = 5$, то $3^2 = 10$» оба истинны. Такое определение на первый взгляд кажется не вполне естественным, однако математическая практика показывает, что оно удобно. В повседневной речи импликации с ложными посылками не употребляются, а в математическом языке принятое определение часто значительно сокращает речь, позволяя не оговаривать специально особые случаи рассуждений.

О высказываниях вида «если A, то B» с ложной посылкой A говорят, что они *истинны тривиальным образом*, т.е. истинны не в силу внутренней содержательной связи между высказываниями A и B, а вследствие соглашения о трактовке логического союза «если..., то...».

1.21. Приведем пример использования импликации с ложной посылкой в математике, приводящий к сокращению речи. Известен приём решения алгебраических иррациональных уравнений с квадратными корнями, основанный на возведении обеих частей уравнения в квадрат. При использовании этого приема могут появляться «посторонние корни», но «потеряться» корни не могут. Это означает, что *любой корень уравнения*

$$f(x) = g(x) \tag{1.5}$$

является также и корнем уравнения

$$[f(x)]^2 = [g(x)]^2. \tag{1.6}$$

Это высказывание мы считаем верным несмотря на то, что исходное уравнение может вообще не иметь корней. Если высказывание

> «любой корень уравнения (1.5) является также корнем уравнения (1.6)»

представить в форме

> «если число a является корнем уравнения (1.5), то оно является также корнем уравнения (1.6)»,

то становится ясным, что наша уверенность в истинности этого высказывания (независимо от того, имеет ли уравнение (1.5) корни) основана на бессознательном применении соглашения об истинности импликации с ложной посылкой. Если бы мы хотели сформулировать утверждение об уравнениях (1.5), (1.6) без учета этого соглашения, то пришлось бы формулировать так:

> «если уравнение (1.5) имеет корни, то любой корень уравнения (1.5) является также корнем уравнения (1.6)».

Очевидно, что принятое соглашение сокращает речь.

1.22. Определение. *Эквивалентность* — логическая операция, которая заключается в соединении двух высказываний A и B в новое высказывание $A \Leftrightarrow B$ («A тогда и только тогда, когда B», «A эквивалентно B») по следующему правилу:

A	B	$A \Leftrightarrow B$
0	0	1
0	1	0
1	0	0
1	1	1

(1.7)

Из таблицы истинности видно, что высказывание $A \Leftrightarrow B$ истинно в том и только том случае, когда высказывания A и B оба истинны или оба ложны.

1.23. Предложение. *Справедливы следующие соотношения, в которых знак равенства означает совпадение логических значений («ложь» 0 или «истина» 1) левой и правой частей*:

(1) *коммутативность*:

$$A \vee B = B \vee A, \quad A \wedge B = B \wedge A;$$

(2) *ассоциативность*:

$$(A \vee B) \vee C = A \vee (B \vee C),$$
$$(A \wedge B) \wedge C = A \wedge (B \wedge C);$$

(3) *дистрибутивность*:

$$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C),$$
$$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C);$$

(4) *закон исключённого третьего*:

$$A \vee \neg A = 1, \quad A \wedge \neg A = 0;$$

(5) *закон двойного отрицания*:

$$\neg\neg A = A;$$

(6) *законы де Моргана*:

$$\neg(A \wedge B) = \neg A \vee \neg B, \quad \neg(A \vee B) = \neg A \wedge \neg B;$$

(7) *закон контрапозиции*:

$$(A \Rightarrow B) = (\neg B \Rightarrow \neg A).$$

Доказательство. Каждое из приведенных соотношений может быть легко доказано при помощи таблиц истинности. Докажем, например, закон контрапозиции:

A	B	$A \Rightarrow B$	$\neg A$	$\neg B$	$\neg B \Rightarrow \neg A$
0	0	1	1	1	1
0	1	1	1	0	1
1	0	0	0	1	0
1	1	1	0	0	1

(здесь использованы таблицы истинности (1.1) и (1.4)). Сравнивая истинностные значения высказываний $A \Rightarrow B$ и $\neg B \Rightarrow \neg A$, видим, что они совпадают при любых истинностных значениях высказываний A и B. □

Б. Логика предикатов.

1.24. *Предикат* — это выражение, содержащее одну (одноместный предикат) или несколько переменных (s-местный предикат, если число переменных равно s), которое превращается в высказывание, если вместо этих переменных подставить объекты из области возможных значений.

Предикат может быть не определён при некоторых значениях входящих в него переменных; например, одноместный предикат $\sqrt{x} > 2$ с числовой переменной x, являющийся истинным при $x > 4$ и ложным при $0 \leqslant x \leqslant 4$, не определен при $x < 0$. В таких случаях, т.е. когда при некоторых значениях переменных рассматриваемый предикат не определён, он считается ложным при этих значениях переменных.

С помощью логических операций $\neg$, $\wedge$, $\vee$, $\Rightarrow$ из данных предикатов можно строить более сложные предикаты.

1.25. *Кванторы* — это логические операции, которые из предиката $P(x)$ строят высказывание, дающее количественную характеристику области истинности предиката $P(x)$. Наиболее употребительны *квантор общности* $\forall$ и *квантор существования* $\exists$.

1.26. Определение. Пусть P — одноместный предикат, X — область возможных значений переменной x. Обозначим через

$$(\forall x \in X)P(x) \tag{1.8}$$

следующее высказывание: «*для любого* значения $x \in X$ высказывание, полученное подстановкой этого значения в предикат P вместо переменной, истинно» или, короче, «*для любого* $x \in X$ высказывание $P(x)$ истинно». (Разумеется, полученное высказывание (1.8) может оказаться как истинным, так и ложным; см. пример 1.29 ниже.) Символ $\forall$ называется *квантором общности*, выражение $(\forall x \in X)$ — *квантором общности по переменной* x, а переход от предиката P к высказыванию (1.8) — *применением* к предикату P *квантора общности* по переменной x («*навешиванием* квантора на предикат»). Вместо $(\forall x \in X)P(x)$ часто пишут $\forall x \in X : P(x)$.

1.27. Определение. Пусть P — одноместный предикат, X — область возможных значений переменной x. Обозначим через

$$(\exists x \in X)P(x) \tag{1.9}$$

следующее высказывание: «*существует* такое значение $x \in X$, что высказывание, полученное подстановкой этого значения в предикат P вместо переменной, истинно» или, короче, «*существует* такое $x \in X$, что высказывание $P(x)$ истинно». Символ $\exists$ называется *квантором существования*, выражение $(\exists x \in X)$ — *квантором существования по переменной* x, а переход от предиката P к высказыванию (1.9) — *применением* к предикату P *квантора существования* по переменной x. Вместо $(\exists x \in X)P(x)$ часто пишут $\exists x \in X : P(x)$.

1.28. Кванторы $\forall$ и $\exists$ называют *взаимно двойственными*.

1.29. Пример. $(\forall x \in \mathbb{R})(x^2 \geqslant 0)$ и $(\exists x \in \mathbb{R})(|x| \leqslant 0)$ — истинные высказывания; $(\forall x \in \mathbb{R})(x^2 > 0)$ и $(\exists x \in \mathbb{R})(|x| < 0)$ — ложные высказывания.

1.30. В выражениях (1.8), (1.9) буква x является *связанной переменной*; от x эти выражения не зависят. Таким образом, *применение квантора связывает переменную*.

1.31. Часто используется более вольная система обозначений. Так, в большинстве случаев опускаются скобки вокруг выражений $(\forall x \in X)$ и $(\exists x \in X)$. Указание области X возможных значений переменной также может быть задано не в виде $x \in X$, а в виде

выражения иного типа, например, $\forall x > 0$. В ряде случаев указание области X вообще опускается; так, в случае, когда из контекста ясно, что x — вещественная числовая переменная, вместо $\forall x \in \mathbb{R}$ допустимо написать просто $\forall x$.

1.32. Предложение. *Справедливы следующие аналоги законов де Моргана*:

$$\neg(\forall x \in X)P(x) \quad = \quad (\exists x \in X)\neg P(x), \tag{1.10}$$

$$\neg(\exists x \in X)P(x) \quad = \quad (\forall x \in X)\neg P(x), \tag{1.11}$$

Доказательство. Докажем соотношение (1.10); для этого требуется установить истинность двух импликаций «левая часть $\Rightarrow$ правая часть» и «правая часть $\Rightarrow$ левая часть».

1. Пусть высказывание $\neg(\forall x)P(x)$ истинно, т.е., по определению отрицания, $(\forall x)P(x)$ ложно. Следовательно, не для любого значения переменной x высказывание $P(x)$ истинно. Значит, существует такое значение переменной x, для которого $P(x)$ ложно. Обозначим одно из таких значений через a. Итак, $a \in X$ и высказывание $P(a)$ ложно, так что $\neg P(a)$ истинно. Значит, существует такое x, что $\neg P(x)$ истинно, т.е. $(\exists x)\neg P(x)$.

2. Пусть теперь высказывание $(\exists x)\neg P(x)$ истинно. Тогда, по определению квантора существования, найдется такое значение переменной x, что $\neg P(x)$ истинно. Обозначим одно из таких значений через a. Итак, $a \in X$ и $\neg P(a)$ истинно, т.е. $P(a)$ ложно. Но тогда, по определению квантора общности, ложно и $(\forall x)P(x)$, т.е. $\neg(\forall x)P(x)$ истинно.

Соотношение (1.11) доказывается аналогично. □

1.33. Правило, выражаемое соотношениями (1.10), (1.11), можно сформулировать следующим образом: *чтобы получить отрицание высказывания, начинающегося с квантора, нужно этот квантор заменить на двойственный* (т.е. квантор общности на квантор существования и наоборот) *и перенести знак отрицания за квантор.*

1.34. Если P — двухместный предикат, то его можно превратить в высказывание, применяя кванторы по каждой переменной. В результате можно получить следующие восемь высказываний:

$$(\forall y)(\forall x)P(x,y), \qquad (\exists y)(\forall x)P(x,y),$$
$$(\forall x)(\forall y)P(x,y), \qquad (\exists x)(\forall y)P(x,y),$$
$$(\forall y)(\exists x)P(x,y), \qquad (\exists y)(\exists x)P(x,y),$$
$$(\forall x)(\exists y)P(x,y), \qquad (\exists x)(\exists y)P(x,y),$$

Возникает вопрос: можно ли переставлять кванторы в этих выражениях?

Легко видеть, что

$$(\forall x)(\forall y)P(x,y) \quad = \quad (\forall y)(\forall x)P(x,y),$$
$$(\exists x)(\exists y)P(x,y) \quad = \quad (\exists y)(\exists x)P(x,y);$$

иными словами, *одноименные кванторы можно переставлять*. «Разноименные» же кванторы переставлять нельзя. Например, высказывание $(\forall y)(\exists x)(x > y)$ («для любого числа y существует большее число x») истинно, однако высказывание $(\exists x)(\forall y)(x > y)$ («существует число x, большее любого другого числа y») ложно.

1.35. При написании высказывания, имеющего вид предиката с применёнными к нему кванторами общности, эти кванторы общности (стоящие впереди) разрешается опускать. Так, истинное высказывание

$$(\forall x)(\forall y)\ (x+y)^2 = x^2 + 2xy + y^2 \tag{1.12}$$

можно написать короче:

$$(x+y)^2 = x^2 + 2xy + y^2;$$

эта запись по форме является двухместным предикатом, а по смыслу — высказыванием (1.12).

3. Математические утверждения

А. Аксиоматический метод.

1.36. Аксиоматический метод — это способ построения научной теории, при котором некоторые её положения (называемые *аксиомами*) принимаются без доказательства (входящие в аксиомы понятия являются неопределяемыми), а остальные выводятся из аксиом по заранее оговоренным логическим законам и правилам. Положения, доказываемые на основе аксиом, называются *теоремами*. Одним из исторически первых примеров применения аксиоматического метода является изложение геометрии в «Началах» Евклида (III в. до н. э.).

1.37. Процесс построения теории по аксиоматическому методу состоит из следующих шагов.

I. Формулировка *основных* (неопределяемых) *понятий*, составляющих фундамент теории: это *объекты* изучения и *отношения* между ними (например, в геометрии основными понятиями являются точка и прямая, а одним из основных отношений — отношение инцидентности, выражаемое словами «точка лежит на прямой»). Все остальные понятия и отношения определяются через эти базовые.

II. Формулировка *аксиом* — принимаемых без доказательства утверждений, которые выражают фундаментальные принципы теории.

III. Вывод *теорем*: из аксиом по правилам логики выводятся все остальные утверждения теории. Доказательство представляет собой последовательность формул, каждая из которых либо является аксиомой, либо получается из предыдущих утверждений (формул) согласно правилам вывода.

Совокупность основных понятий, исходных аксиом и выведенных на их основе теорем образует *аксиоматическую теорию*.

1.38. Различают неформальные и формальные аксиоматические теории. В неформальных теориях рассуждения ведутся на содержательном уровне, а правила вывода соответствуют «житейской» логике. В античности под аксиомами понимали положения, которые, будучи совершенно очевидными и интуитивно ясными для всех, не нуждаются в доказательстве. Подобное понимание аксиом преобладало вплоть до XIX в. вплоть до построения неевклидовых геометрий.

1.39. После появления работ Н. И. Лобачевского[1] и Я. Бойяи[2], показавших, что в основание геометрии могут быть положены разные системы аксиом, аксиомы стали трактоваться как положения, которые при данном дедуктивном построении теории принимаются за исходные независимо от того, насколько они просты и интуитивно очевидны. При таком подходе аксиомы перестают носить характер абсолютных истин, а становятся зависимыми от того, какая теория строится на их основе.

1.40. В конце XIX — начале XX века Д. Гильберт[3] и его последователи провозгласили программу формализации математики. Аксиомы из предложений содержательной теории превращаются в наборы формул, из которых по формально определённым правилам вывода выводятся другие формулы теории, которая становится,

[1]Николай Иванович Лобачевский (1792—1856) — выдающийся русский математик, один из создателей неевклидовой геометрии, ректор Казанского университета.

[2]Янош Бойяи (János Bolyai; 1802—1860) — венгерский математик, один из первооткрывателей неевклидовой геометрии.

[3]Давид Гильберт (David Hilbert; 1862—1943) — выдающийся немецкий математик.

таким образом, исчислением формул. В формальных теориях процесс умозаключений строго формализован: задаётся язык (синтаксис), выбираются аксиомы (которые делятся на логические — универсальные, и собственные — конкретной теории) и правила вывода. При радикальной формализации из теории «изгоняются» интуитивные и наглядные представления, которые, однако остаются обильным источником эвристических идей.

1.41. К аксиоматической системе обычно предъявляют требования *непротиворечивости* (в теории нельзя одновременно вывести и утверждение, и его отрицание), *полноты* (для любой формулы либо она сама, либо её отрицание доказуемы) и *независимости* (ни одна из аксиом не может быть выведена из других).

1.42. Как показал К. Гёдель[1], достаточно богатые теории (например, арифметика натуральных чисел) не допускают полной аксиоматизации. Это ставит предел возможностям полной формализации научного знания.

Б. Теоремы и доказательства.

1.43. В математике *доказательством* называется цепочка логических умозаключений, показывающая, что при некотором наборе аксиом и правил рассуждений верно некоторое утверждение. Доказанные утверждения называют *теоремами*; если ни утверждение, ни его отрицание ещё не доказаны, то такое утверждение называют *гипотезой*. В математических текстах теоремами обычно именуют только достаточно важные утверждения; менее важные и технически несложные утверждения-теоремы обычно называют леммами, предложениями, следствиями и прочими подобными терминами.

1.44. Основные виды формулировок теорем следующие:

(1) *категорические*: A есть B (пример: «сумма углов треугольника равна 180°»);
(2) *импликативные*: $A \Rightarrow B$ (пример: «если число делится на 10, то его последняя цифра — нуль»); высказывание A называют *условием* (*посылкой*) теоремы, B — *заключением* (*следствием*);
(3) *разделительные* (*классификационные*): S есть или A, или B, или C.

1.45. Следствие B импликативной теоремы «$A \Rightarrow B$» называется условием, *необходимым* для истинности посылки A. (Без выполнения B утверждение A не может быть истинным.) Теорема, выражающая необходимое условие, называется *свойством*.

[1] Курт Фридрих Гёдель (нем. Kurt Friedrich Gödel; 1906—1978) — австрийский логик и математик.

1.46. Посылка A теоремы «$A \Rightarrow B$» называется условием, *достаточным* для выполнения следствия B. (Если A истинно, то утверждение B заведомо верно.) Теорема, выражающая достаточное условие, называется *признаком*.

1.47. Пример. Для того чтобы число делилось на 2, необходимо, чтобы последняя цифра в его десятичной записи не была семеркой:

$$\text{число делится на 2} \quad \Longrightarrow \quad \underbrace{\text{последняя цифра не 7.}}_{\text{необходимое условие делимости на 2}}$$

Это условие не является достаточным: число 13 не заканчивается на 7, но на 2 не делится. Таким образом, необходимые условия содержат «лишние случаи». Утверждение «*если число делится на* 2*, то его последняя цифра не* 7» — свойство (одно из свойств) чётных чисел.

1.48. Пример. Для того чтобы число делилось на 2, достаточно, чтобы его последняя цифра была нулём:

$$\underbrace{\text{последняя цифра 0}}_{\text{достаточное условие делимости на 2}} \quad \Longrightarrow \quad \text{число делится на 2.}$$

Это условие не является необходимым: число 14 делится на 2, но его последняя цифра не 0. Таким образом, достаточные условия содержат «не все случаи». Утверждение «*если последняя цифра числа — нуль, то число делится на* 2» является признаком (одним из признаков) делимости на 2.

1.49. Достаточные условия стараются сделать возможно более широкими, т.е. охватывающими возможно большее число случаев, в которых интересующий нас факт все ещё имеет место, а необходимые условия — возможно более узкими, т.е. охватывающими возможно меньше лишних случаев, в которых изучаемый факт уже не имеет места.

1.50. Теорема, выражающая одновременно необходимое и достаточное условие, называется *критерием*: $A \Leftrightarrow B$. Критерии часто формулируются с помощью речевого оборота «*тогда и только тогда*».

1.51. Пример. Следующее утверждение может служить примером критерия: «*для того чтобы число делилось на* 3*, необходимо и достаточно, чтобы сумма его цифр делилась на* 3». В другой формулировке: «*число делится на* 3 *тогда и только тогда, когда сумма его цифр делится на* 3».

1.52. Рассмотрим следующие четыре импликативные теоремы, образованные из высказываний A и B:

$$A \Rightarrow B, \tag{1.13}$$

$$B \Rightarrow A, \tag{1.14}$$

$$\neg A \Rightarrow \neg B, \tag{1.15}$$

$$\neg B \Rightarrow \neg A. \tag{1.16}$$

Теоремы (1.13) и (1.14) (и соответственно, теоремы (1.15) и (1.16)) называются *взаимно обратными* теоремами: теорема (1.14) — это теорема, обратная теореме (1.13) и наоборот. Теоремы (1.13) и (1.15) (и соответственно, теоремы (1.14) и (1.16)) называются *взаимно противоположными теоремами*. Теорему (1.16) называют *контрапозицией* исходной теоремы (1.13).

1.53. Как показывает следующая таблица истинности, взаимно обратные теоремы (1.13) и (1.14) логически почти не зависят друг от друга: истинность одной из них не влечёт ни истинности, ни ложности другой, однако эти теоремы не могут быть одновременно ложными:

A	B	$A \Rightarrow B$	$B \Rightarrow A$
0	0	1	1
0	1	1	0
1	0	0	1
1	1	1	1

Взаимно противоположные теоремы (1.13) и (1.15) связаны аналогично (убедитесь в этом самостоятельно).

1.54. Если для некоторой теоремы $A \Rightarrow B$ верна и обратная теорема $B \Rightarrow A$, то они могут быть объединены в критерий $A \Leftrightarrow B$.

1.55. Пример. Исходная теорема: «*если в треугольнике один из углов прямой, то два других угла — острые*», — истинное утверждение. Обратная теорема: «*если два угла в треугольнике острые, то третий угол — прямой*», — ложное утверждение. Теорема Пифагора и обратная к ней теорема могут быть объединены в критерий: «*для того чтобы треугольник был прямоугольным, необходимо и достаточно, чтобы для его сторон a, b, c выполнялось соотношение $a^2 + b^2 = c^2$*».

1.56. В силу закона *контрапозиции*

$$(\neg B \Rightarrow \neg A) \quad == \quad (A \Rightarrow B)$$

теорема, противоположная к обратной, равносильна исходной. Этот прием может быть использован для доказательства в случае, когда теорема, противоположная к обратной, доказывается проще, чем исходная теорема. Этот приём часто называют «доказательством от противного».

4. Упражнения и задачи

1.1. Укажите, какие из следующих выражений являются высказываниями, и определите их истинностные значения:

(а) азот — газ;
(б) я учусь в университете;
(в) снег белый;
(г) белый снег;
(д) $x > 0$;
(е) $(x + y)^2$;
(ж) $(x + y)^2 = x^2 + y^2$;
(з) $(x + y)^2 = x^2 + 2xy + y^2$.

1.2. Является ли высказыванием следующее предложение: «*Это предложение ложно.*»?

1.3. Расчлените следующие сложные высказывания на простые и запишите с помощью логической символики:

(а) сегодняшний день солнечный и тёплый;
(б) сегодняшний день солнечный, но не тёплый;
(в) данный четырёхугольник — квадрат или ромб;
(г) Петя и Вася решили задачу;
(д) автором этой книги является Иванов или Петров;
(е) это ни необходимо, ни желательно.

1.4. Пусть A и B — два данных высказывания. С помощью операций $\neg$ и $\wedge$ постройте из A и B такое сложное высказывание C, что

(а) C истинно тогда и только тогда, когда A и B оба истинны;
(б) C истинно тогда и только тогда, когда A истинно, а B ложно;
(в) C истинно тогда и только тогда, когда A и B оба ложны;
(г) C ложно тогда и только тогда, когда A и B оба истинны.

1.5. Из простых высказываний A, B, C постройте составное высказывание, которое было бы истинно тогда и только тогда, когда истинна только одна (безразлично какая) из компонент.

1.6. Какие из следующих импликаций истинны:

(а) если $2 \cdot 2 = 4$, то $2 < 3$;
(б) если $2 \cdot 2 = 4$, то $2 > 3$;
(в) если $2 \cdot 2 = 5$, то $2 < 3$;
(г) если $2 \cdot 2 = 5$, то $2 > 3$;
(д) если сегодня понедельник, то завтра вторник;
(е) если сегодня понедельник, то завтра суббота.

1.7. Пусть A и B — два данных высказывания. С помощью операций $\neg$ и $\Rightarrow$ постройте из A и B такое сложное высказывание C, что

(а) C ложно тогда и только тогда, когда A и B оба истинны;
(б) C ложно тогда и только тогда, когда A истинно, а B ложно;
(в) C ложно тогда и только тогда, когда A ложно, а B истинно;
(г) C истинно тогда и только тогда, когда A ложно, а B истинно.

1.8. Запишите с помощью логической символики следующие высказывания и установите их истинностные значения:

(а) для того чтобы треугольник был равносторонним, необходимо, чтобы его углы были равны;
(б) для того чтобы треугольник был равносторонним, достаточно, чтобы его углы были равны;
(в) для того чтобы число делилось на три, необходимо, чтобы оно делилось на шесть;
(г) для того чтобы число делилось на три, достаточно, чтобы оно делилось на шесть.

1.9 (р)**.** Запишите с помощью логической символики следующие высказывания и определите их истинностные значения:

(а) для того чтобы произведение чисел обращалось в нуль, необходимо и достаточно, чтобы один из сомножителей был равен нулю;
(б) сумма чисел делится на 3 тогда и только тогда, когда все слагаемые делятся на 3;
(в) если четырехугольник является квадратом, то все углы его прямые, и обратно.

Исправьте ложные высказывания так, чтобы получились истинные высказывания.

1.9. (а) Введём обозначения A_k = «$x_k = 0$», где $k = 1, \ldots, N$, N — число сомножителей, B = «$\prod\limits_{k=1}^{N} x_k = 0$». Тогда истинное высказывание (а) записывается в виде $B \Leftrightarrow (A_1 \vee A_2 \vee \cdots \vee A_N)$ или $B \Leftrightarrow \bigvee\limits_{k=1}^{N} A_k$.

(б) Введём обозначения C_k = «число x_k делится на 3», где $k = 1, \ldots, N$, N — число слагаемых, D = «$\sum\limits_{k=1}^{N} x_k$ делится на 3». Тогда ложное высказывание (б) записывается в виде $(C_1 \wedge C_2 \wedge \cdots \wedge C_N) \Leftrightarrow D$ или $\bigwedge\limits_{k=1}^{N} C_k \Leftrightarrow D$. Высказывание $\bigwedge\limits_{k=1}^{N} C_k \Rightarrow D$ истинно.

(в) Введём обозначения E =«данный четырёхугольник является квадратом», F =«все углы данного четырехугольника прямые». Тогда ложное высказывание (в) записывается в виде $E \Leftrightarrow F$. Высказывание $E \Rightarrow F$ истинно.

1.10 (р)**.** Дано высказывание: «Если четырёхугольник является прямоугольником, то вокруг него можно описать окружность». Запишите его в виде импликации $A \Rightarrow B$. Постройте высказывания $B \Rightarrow A$, $\neg A \Rightarrow \neg B$, $\neg B \Rightarrow \neg A$. Какие из них истинны?

1.10. Введём следующие высказывания:

A = «данный четырёхугольник является прямоугольником»,

B = «вокруг данного четырёхугольника можно описать окружность».

Тогда $A \Rightarrow B$ — истинное высказывание. Высказывание $B \Rightarrow A$ («если вокруг четырёхугольника можно описать окружность, то он является прямоугольником») ложно (например, окружность можно описать вокруг трапеции).

Высказывание $\neg A \Rightarrow \neg B$ («если четырёхугольник не является прямоугольником, то вокруг него нельзя описать окружность») ложно (см. предыдущий пример).

Высказывание $\neg B \Rightarrow \neg A$ («если вокруг четырёхугольника нельзя описать окружность, то он не является прямоугольником») истинно, поскольку получено из исходного истинного высказывания $A \Rightarrow B$ с помощью контрапозиции.

1.11 (р)**.** Докажите, что высказывание $A \Rightarrow (B \Rightarrow A)$ является истинным независимо от того, истинно или ложно высказывание A.

1.11. Построим таблицу истинности для высказывания $A \Rightarrow (B \Rightarrow A)$:

A	B	$B \Rightarrow A$	$A \Rightarrow (B \Rightarrow A)$
0	0	1	1
0	1	0	1
1	0	1	1
1	1	1	1

Последний столбец показывает, что высказывание $A \Rightarrow (B \Rightarrow A)$ истинно при любых A и B.

1.12 (р)**.** Докажите с помощью таблиц истинности закон поглощения $A \vee (A \wedge B) = A$.

1.12. Доказательство сводится к заполнению таблицы истинности

A	B	$A \wedge B$	$A \vee (A \wedge B)$
0	0	0	0
0	1	0	0
1	0	0	1
1	1	1	1

(здесь использованы таблицы истинности для операций конъюнкции и дизъюнкции). Сравнивая истинностные значения высказываний A и $A \vee (A \wedge B)$, видим, что они совпадают при любых истинностных значениях высказываний A и B.

1.13 (р)**.** Докажите с помощью таблиц истинности закон двойного отрицания и закон исключённого третьего.

1.13.

$\neg\neg A = A$

A	$\neg A$	$\neg\neg A$
0	1	0
1	0	1

$A \vee \neg A = 1$

A	$\neg A$	$A \vee \neg A$
0	1	1
1	0	1

$A \wedge \neg A = 0$

A	$\neg A$	$A \wedge \neg A$
0	1	0
1	0	0

1.14 (р)**.** Докажите с помощью таблиц истинности законы де Моргана $\neg(A \wedge B) = \neg A \vee \neg B$, $\neg(A \vee B) = \neg A \wedge \neg B$.

1.14.

Для $\neg(A \wedge B) = \neg A \vee \neg B$:

A	B	$A \wedge B$	$\neg(A \wedge B)$	$\neg A$	$\neg B$	$\neg A \vee \neg B$
0	0	0	1	1	1	1
0	1	0	1	1	0	1
1	0	0	1	0	1	1
1	1	1	0	0	0	0

Для $\neg(A \vee B) = \neg A \wedge \neg B$:

A	B	$A \vee B$	$\neg(A \vee B)$	$\neg A$	$\neg B$	$\neg A \wedge \neg B$
0	0	0	1	1	1	1
0	1	1	0	1	0	0
1	0	1	0	0	1	0
1	1	1	0	0	0	0

1.15 (р)**.** Докажите с помощью таблиц истинности соотношения $\neg(A \Rightarrow B) = (A \wedge \neg B)$, $(A \vee B) = (\neg A \Rightarrow B)$.

1.15.

Для $\neg(A \Rightarrow B) = (A \wedge \neg B)$:

A	B	$A \Rightarrow B$	$\neg(A \Rightarrow B)$	$\neg B$	$A \wedge \neg B$
0	0	1	0	1	0
0	1	1	0	0	0
1	0	0	1	1	1
1	1	1	0	0	0

Для $(A \vee B) = (\neg A \Rightarrow B)$:

A	B	$A \vee B$	$\neg A$	$\neg A \Rightarrow B$
0	0	0	1	0
0	1	1	1	1
1	0	1	0	1
1	1	1	0	1

1.16. Переформулируйте следующие утверждения, не используя слов «необходимо» и «достаточно» (на смысл утверждений внимание не обращайте):

(а) для того, чтобы дифференцируемая функция имела экстремум в некоторой точке, необходимо, чтобы её производная в этой точке обращалась в нуль;

(б) для того, чтобы функция была непрерывной в некоторой точке, достаточно, чтобы она была дифференцируемой в этой точке;

(в) для того, чтобы числовой ряд сходился, необходимо, чтобы его общий член стремился к нулю;

(г) для того, чтобы ограниченная числовая последовательность имела предел, достаточно, чтобы она была монотонной.

1.17. Для каждого из утверждений задачи 1.16 сформулируйте эквивалентное утверждение, заменив слово «необходимо» на слово «достаточно» и наоборот.

1.18. Для каждого из утверждений задачи 1.16 сформулируйте его контрапозицию тремя способами: с использованием слова «необходимо», с использованием «достаточно» и без использования этих слов.

ГЛАВА 2

Множества, соответствия, отображения

МНОЖЕСТВО — фундаментальное понятие математики, появляющееся во всех её областях. Никакого определения понятию множества не даётся; мы считаем это понятие первичным. С элементами теории множеств читатель встречался в школьном курсе математики. В этой главе, помимо множеств, обсуждаются важнейшие для математики понятия соответствий, отношений и отображений.

1. Множества и операции над ними

А. Наивная теория множеств.

2.1. Общепризнано, что создателем теории множеств является Г. Кантор[1]. Он определил множество как «единое имя для совокупности всех объектов, обладающих данным свойством», а сами эти объекты назвал элементами множества. Теория, созданная Кантором, в настоящее время называется *наивной теорией множеств*.

2.2. Первичные понятия теории множеств — *множество* и отношение «*быть элементом*», называемое *отношением принадлежности* (*инцидентности*). Если высказывание «*множество A является элементом множества B*» истинно, пишем $A \in B$, а если ложно — то $A \notin B$ (или $\neg(A \in B)$).

2.3. С современной точки зрения в стандартной теории множеств *абсолютно все объекты* суть множества: никаких иных объектов, кроме множеств, в теории множеств не рассматривают. Однако отношение инцидентности позволяет считать, что одни множества являются элементами других, и с этой точки зрения следует чётко различать множества и элементы, из которых состоят множества. Например, число 2 и множество $\{2\}$ — разные объекты; так, о множестве $\{2\}$ нельзя задать вопрос, чётное оно или нечётное: множество не может быть чётным или нечётным, но может быть

[1]Георг Кантор (Georg Cantor; 1845—1918) — немецкий математик.

конечным или бесконечным, одно- или многоэлементным, пустым или непустым (см. ниже п. 2.18) и т. п. Наоборот, о числе 2 нельзя спрашивать, одноэлементное оно или непустое и т. п. Итак, у объектов 2 и $\{2\}$ разные *атрибуты*: 2 — чётное простое положительное число, $\{2\}$ — непустое одноэлементное конечное множество. Очевидно, всегда $a \in \{a\}$. Очевидно также, что $b \in \{a\} \;\Leftrightarrow\; b = a$.

2.4. Пусть $P(x)$ — какой либо одноместный предикат. В наивной теории множеств считается, что предикат $P(x)$ позволяет выделить все объекты, обладающие свойством $P(x)$, т.е. что *существует множество всех объектов x, обладающих свойством $P(x)$*; это множество обозначается $\{x \mid P(x)\}$ или $\{x : P(x)\}$. Такое правило образования множеств интуитивно приемлемо и выглядит достаточно естественным; его называют *наивной схемой аксиом выделения* (не аксиомой, а именно *схемой аксиом*, т.е. группой однородных аксиом: каждому предикату $P(x)$ соответствует своя аксиома выделения). Однако применение этого правила может приводить к различным парадоксам, самым известным среди которых является парадокс Рассела[1].

2.5. ***Парадокс Рассела.*** Пусть $K = \{x : x \notin x\}$. Тогда

$$K \in K \;\Leftrightarrow\; K \notin K.$$

Парадокс Расселла имеет множество неформальных формулировок (парадокс лжеца, парадокс брадобрея и др.)

Б. Аксиоматика Цермело—Френкеля.

2.6. Чтобы избежать парадоксов, подобных парадоксу Рассела, необходимо аксиоматизировать теорию множеств и называть множествами только те совокупности объектов, существование которых гарантируется имеющимися аксиомами. Одной из наиболее употребительных систем аксиом теории множеств является система Цермело[2]—Френкеля[3] (сокращённо ZF). Система аксиом ZF в полном объёме нам не понадобится; перечислим лишь те понятия и основанные на них конструкции, которые будут использоваться в дальнейшем; заинтересованный читатель найдёт подробности в Приложении **??**.

2.7. ***Аксиома существования:*** множества существуют.

[1] Бертран Рассел (Bertrand Russell; 1872–1970) — британский философ, логик, математик и общественный деятель.

[2] Эрнст Це́рмело (Ernst Zermelo; 1871—1953) — немецкий математик.

[3] Абрахам Галеви (Адольф) Френкель (нем. Abraham Halevi (Adolf) Fraenkel; 1891—1965) — израильский математик.

2.8. ***Аксиома объёмности (экстенсиональности):*** Два множества равны тогда и только тогда, когда они имеют одни и те же элементы. Равенство множеств обозначается символом «=».

2.9. Если каждый элемент множества A является элементом множества B, то множество A называется подмножеством множества B; этот факт записывается в виде $A \subseteq B$. Очевидно, $A = B$ равносильно $A \subseteq B \wedge B \subseteq A$. Вместо $A \subseteq B$ часто пишут $A \subset B$.

2.10. ***Аксиома пары*** является простейшей аксиомой, позволяющей строить новые множества из уже имеющихся: если даны множества A и B, то можно получить множество C, содержащее в точности A и B, причём такое C единственно в силу аксиомы объёмности: $C = \{A, B\}$. Множество C называется *неупорядоченной парой*, состоящей из (элементов) A и B. Очевидно, $\{A, B\} = \{B, A\}$. Если $A = B$, вместо $\{A, A\}$ пишут $\{A\}$; множество $\{A\}$ содержит единственный элемент A и называется *синглетоном*.

2.11. Множество

$$(A, B) \stackrel{\text{def}}{=\!=} \big\{\{A\}, \{A, B\}\big\}$$

называется *упорядоченной парой*, состоящей из элементов A и B.

2.12. Предложение. *Упорядоченные пары* (A_1, B_1) *и* (A_2, B_2) *равны тогда и только тогда, когда* $A_1 = A_2$ *и* $B_1 = B_2$:

$$(A_1, B_1) = (A_2, B_2) \;\Leftrightarrow\; (A_1 = A_2) \wedge (B_1 = B_2).$$

Доказательство. Импликация $\Leftarrow$ очевидна. Докажем импликацию $\Rightarrow$. Пусть $(A_1, B_1) = (A_2, B_2)$, т.е.

$$\big\{\{A_1\}, \{A_1, B_1\}\big\} = \big\{\{A_2\}, \{A_2, B_2\}\big\}. \tag{2.1}$$

1. Предположим, что $A_1 \neq B_1$; тогда множество $\{A_1, B_1\}$ состоит из двух элементов. Так как оно является элементом множества в левой части равенства (2.1), то оно является элементом множества в правой, так что либо $\{A_1, B_1\} = \{A_2, B_2\}$, либо $\{A_1, B_1\} = \{A_2\}$; второе невозможно, ибо двухэлементное множество не может быть равно одноэлементному. Итак, $\{A_1, B_1\} = \{A_2, B_2\}$. Далее, одноэлементное множество $\{A_1\}$ является элементом множества в левой части равенства (2.1), поэтому оно является элементом множества в правой части и следовательно равно $\{A_2\}$ (поскольку не может быть равным двухэлементному множеству $\{A_2, B_2\}$). Отсюда $A_1 = A_2$ и $B_1 = B_2$.

2. Аналогично рассматривается ситуация, когда $A_2 \neq B_2$.

3. Осталось рассмотреть случай $A_1 = B_1$. Левая часть (2.1) равна

$$\big\{\{A_1\}, \{A_1, B_1\}\big\} = \big\{\{A_1\}, \{A_1, A_1\}\big\} = \big\{\{A_1\}, \{A_1\}\big\} = \big\{\{A_1\}\big\},$$

т.е. представляет собой множество с единственным элементом $\{A_1\}$. Но тогда и правая часть должны быть одноэлементным множеством, т.е. $\{A_2\} = \{A_2, B_2\}$, что возможно лишь при $A_2 = B_2$; следовательно правая часть (2.1) равна $\big\{\{A_2\}\big\}$. Получаем, что $A_1 = A_2$, так что все четыре элемента A_1, A_2, B_1, B_2 совпадают. □

2.13. Можно определить упорядоченные тройки, четвёрки и т. д.:

$$(A, B, C) \stackrel{\text{def}}{=\!=} \big((A, B), C\big), \quad (A, B, C, D) \stackrel{\text{def}}{=\!=} \big((A, B, C), D\big), \quad \ldots.$$

2.14. ***Схема аксиом выделения.*** Как уже было сказано выше, схемы аксиом — это группы однородных аксиом. Пусть $P(x)$ — некоторый одноместный предикат. В любом множестве A можно выделить (под)множество B всех элементов $x \in A$, для которых предикат $P(x)$ является истинным:

$$B \stackrel{\text{def}}{=\!=} \{x \mid x \in A \wedge P(x)\}.$$

Ввиду аксиомы объёмности такое множество B единственно; будем обозначать его $\{x \in A \mid P(x)\}$ или $\{x \in A : P(x)\}$. Предикат $P(x)$ называется *характеристическим свойством* элементов множества B. Каждому предикату $P(x)$ соответствует своя аксиома выделения.

2.15. Частным случаем конструкции, описанной в аксиоме выделения, является запись вида $\{a; b; c; \ldots\}$, обозначающая множество, элементы которого перечислены внутри фигурных скобок.

2.16. *Пересечение* $A \cap B$ множеств A и B определяется как множество, состоящее из элементов, которые принадлежат одновременно множествам A и B:

$$A \cap B \stackrel{\text{def}}{=\!=} \big\{x \mid x \in A \wedge x \in B\big\}.$$

2.17. *Разность* $A \setminus B$ множеств A и B определяется как множество, состоящее из элементов, которые принадлежат множеству A, но не принадлежат множеству B:

$$A \setminus B \stackrel{\text{def}}{=\!=} \big\{x \mid x \in A \wedge x \notin B\big\}.$$

2.18. Из определения разности множеств следует, что для любого множества A множество $A \setminus A$ не содержит ни одного элемента; в силу аксиом объёмности такое множество единственно. Оно называется *пустым множеством* и обозначается $\varnothing$.

2.19. Поскольку импликация с ложной посылкой истинна (см. определение 1.19 и п. 1.20), для любого x и любого A верна импликация

$$x \in \varnothing \quad \Longrightarrow \quad x \in A,$$

так что $\varnothing \subset A$ для любого множества A, в том числе и пустого: $\varnothing \subset \varnothing$. При этом $\varnothing \cap \varnothing = \varnothing$.

2.20. *Объединение* $A \cup B$ множеств A и B — это множество, состоящее из всех элементов множества A и всех элементов множества B:

$$A \cup B \stackrel{\text{def}}{=\!=} \{x \mid x \in A \vee x \in y\}.$$

Если множества A и B не пересекаются, т.е. $A \cap B = \varnothing$, то вместо $A \cup B$ иногда пишут $A \sqcup B$ и называют это множество *дизъюнктным объединением*.

2.21. Понятие объединения множеств вместе с аксиомой пары позволяет определить неупорядоченные тройки, четвёрки и т. д.:

$$\{X_1, X_2, X_3\} \stackrel{\text{def}}{=\!=} \{X_1, X_2\} \cup \{X_3\},$$
$$\{X_1, X_2, X_3, X_4\} \stackrel{\text{def}}{=\!=} \{X_1, X_2, X_3\} \cup \{X_4\}, \quad \ldots.$$

2.22. ***Аксиома степени (аксиома булеана)*** позволяет образовать множество $\mathcal{P}(A)$, элементами которого являются все *подмножества* данного множества, называемое *множеством-степенью* или *булеаном*[1] множества A. Другие обозначения булеана: 2^A, $\exp A$.

2.23. *Декартовым произведением* (или *прямым произведением*) множеств A и B называется множество $A \times B$, элементами которого являются упорядоченные пары (a, b), где $a \in A$, $b \in B$:

$$A \times B \stackrel{\text{def}}{=\!=} \big\{(a, b) \mid a \in A \wedge b \in B\big\}.$$

Декартово произведение нескольких (конечного числа) множеств будет введено в п. 2.98 (см. с. 55).

2.24. *Диагональю* Δ_A множества A называется следующее подмножества декартова квадрата $A \times A \equiv A^2$:

$$\Delta_A = \{(a, a) \mid a \in A\} \subset A \times A.$$

[1] Джордж Буль (George Boole; 1815—1864) — английский математик и логик.

B. Операции над множествами и их свойства.

2.25. Замечание. (а) Множество считается заданным только в том случае, если перечислены все его элементы либо указан способ построения любого элемента этого множества: при помощи аксиомы выделения (характеристического свойства) или теоретико-множественных операций. Поэтому, например, некорректно говорить о прямой как о множестве точек, как это обычно делается в школьных курсах геометрии. Высказывания «прямая — неопределяемое понятие» и «прямая — это множество точек» взаимно противоречивы.

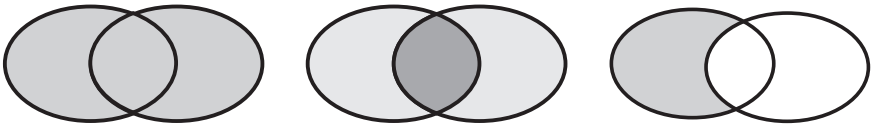
(б) Из определения равенства множеств вытекает, что порядок элементов при записи множеств несуществен; например, $\{a, b, c\}$ и $\{c, b, a\}$ — одно и то же множество. Мы считаем, что в множестве элементы расположены «в беспорядке», так что говорить о первом, втором и т. д. элементе данного множества бессмысленно (по крайней мере до тех пор, пока элементы множества не перенумерованы, что, кстати говоря, не всегда возможно; обратите внимание, что понятием «нумерация элементов множества» мы не обладаем!).

(в) Для того чтобы понятие «число элементов множества» было вполне определённым, нужно — при нашем понимании равенства множеств — условиться, что в множестве не бывает одинаковых (неразличимых) элементов. Таким образом, например, запись $\{a, a, b\}$ считается некорректной и должна быть заменена на $\{a, b\}$.

(г) Следует чётко различать знаки $\in$ и $\subset$ и обозначаемые ими понятия. Например, для множества $A = \{\{a, b\}, \{c, d, e\}\}$ запись $\{a, b\} \in A$ верна, а запись $\{a, b\} \subset A$ неверна, ибо в A нет ни элемента a, ни элемента b. Для множества $B = \{a, b, \{a, b\}\}$, состоящего из трёх элементов a, b и $\{a, b\}$, обе записи $\{a, b\} \in B$ и $\{a, b\} \subset B$ осмысленны, но смысл их различен.

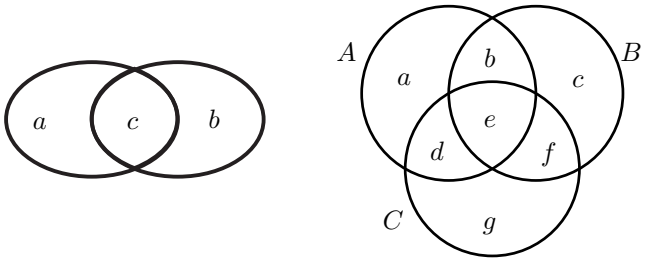
2.26. Определение. В ситуации, когда все множества, участвующие в некотором рассуждении, являются подмножествами некоторого множества U, называемого *универсальным множеством* (*универсумом*), удобно рассматривать дополнение *дополнением* A' множества A, т.е. разность $U \setminus A$. Дополнение множества A обозначается также $\overline{A}$, $\complement A$.

2.27. Для наглядного изображения множеств и отношений между ними часто используются диаграммы, называемые *диаграммами Эйлера* (диаграммами Эйлера—Венна). На рис. 2.1 с помощью диаграмм Эйлера проиллюстрированы понятия объединения, пересечения и разности множеств.



(а) объединение (б) пересечение (в) разность

Рис. 2.1. Диаграммы Эйлера



(а) (б)

Рис. 2.2. Множества в общем положении

2.28. Будем говорить, что два множества A и B *находятся в общем положении*, если существуют такие элементы a, b, c, что $a \in A$, $a \notin B$, $b \in B$, $b \notin A$, $c \in A$, $c \in B$. Два множества в общем положении изображены на рис. 2.2, где символ a, например, обозначает список всех элементов, содержащихся в множестве A, но не содержащихся в множестве B и т. д.

Понятие трёх множеств в общем положении вводится аналогично; опираясь на диаграмму Эйлера, изображённую на рис. 2.2, сформулируйте определение самостоятельно.

2.29. Предложение. *Операции над множествами обладают следующими свойствами*:

(1) *коммутативность*:

$$A \cap B = B \cap A, \quad A \cup B = B \cup A;$$

(2) *ассоциативность*:

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

(3) *взаимная дистрибутивность*:

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

(4) $A \setminus B = A \cap B'$;

(5) $\varnothing' = U$; $U' = \varnothing$;
(6) *законы де Моргана*:

$$(A \cap B)' = A' \cup B', \quad (A \cup B)' = A' \cap B'. \tag{2.2}$$

Доказательство. Докажем равенство $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$. Пусть $x \in (A \cup B) \cap C$; это означает, что x входит в C и по крайней мере в одно из множеств A или B. Но тогда x принадлежит хотя бы одному из множеств $A \cap C$ или $B \cap C$, т.е. входит в правую часть доказываемого равенства. Обратно, пусть $x \in (A \cap C) \cup (B \cap C)$, т.е. $x \in A \cap C$ или $x \in B \cap C$. Следовательно, $x \in C$ и, кроме того, x входит в A или в B, т.е. $X \in A \cup B$, так что $x \in (A \cup B) \cap C$. Равенство доказано.

Приведённое рассуждение удобно записать с помощью логических символов, введённых в лекции 1. При проведении выкладок мы пользуемся правилами преобразования логических выражений, сформулированными в теореме 1.23:

$$\begin{aligned} x \in (A \cup B) \cap C \;&\Leftrightarrow\; \big(x \in A \cup B\big) \;\wedge\; \big(x \in C\big) \;\Leftrightarrow \\ &\Leftrightarrow\; \big(x \in A \;\vee\; x \in B\big) \;\wedge\; \big(x \in C\big) \;\Leftrightarrow \\ &\Leftrightarrow\; \big(x \in A \;\wedge\; x \in C\big) \;\vee\; \big(x \in B \;\wedge\; x \in C\big) \;\Leftrightarrow \\ &\Leftrightarrow\; \big(x \in A \cap C\big) \cup \big(x \in B \cap C\big) \;\Leftrightarrow \\ &\Leftrightarrow\; x \in (A \cap C) \cup (B \cap C). \end{aligned}$$

Удобно воспользоваться также техникой диаграмм Эйлера. Рассмотрим три множества A, B, C в общем положении (см. рис. 2.2):

$$A = \{a, b, d, e\}, \quad B = \{b, c, e, f\}, \quad C = \{d, e, f, g\}.$$

Имеем:

$$A \cup B = \{a, b, c, d, e, f\}, \quad (A \cup B) \cap C = \{d, e, f\},$$
$$A \cap C = \{d, e\}, \quad B \cap C = \{e, f\}, (A \cap C) \cup (B \cap C) = \{d, e, f\},$$

что и требовалось доказать. □

Г. Индуктивные множества и натуральные числа. Для любого множества a его *последователем* назовём множество $S(a) \stackrel{\text{def}}{=\!=} a \cup \{a\}$.

2.30. Множество A называется *индуктивным*, если выполнены следующие условия:

(i) $\varnothing \in A$;
(ii) если $a \in A$, то $a \cup \{a\} \in A$.

Аксиома бесконечности, входящая в состав системы Цермело—Френкеля, постулирует существование индуктивных множеств.

2.31. Наименьшим индуктивным множеством является множество $\mathbb{N}_0$, состоящее из следующих элементов:

$$0 \stackrel{\text{def}}{=\!=} \varnothing,$$

$$1 \stackrel{\text{def}}{=\!=} S(0) = 0 \cup \{0\} = \varnothing \cup \{\varnothing\} = \{\varnothing\} = \{0\},$$

$$2 \stackrel{\text{def}}{=\!=} S(1) = 1 \cup \{1\} = \bigl\{\varnothing, \{\varnothing\}\bigr\} = \{0, 1\},$$

$$3 \stackrel{\text{def}}{=\!=} S(2) = 2 \cup \{2\} = \Bigl\{\varnothing, \{\varnothing\}, \bigl\{\varnothing, \{\varnothing\}\bigr\}\Bigr\} = \{0, 1, 2\} \quad \text{и т. д.}$$

Множество $\mathbb{N}_0$ называется *множеством натуральных чисел*. Этот подход к натуральным числам называется определением Фреге[1]—Рассела; он весьма близок к аксиоматике Пеано (см. ниже п. 2.35).

2.32. Существуют два подхода к определению натуральных чисел; один основан на использовании чисел для обозначения количества предметов (нет предметов, один предмет, два предмета и т. д.), а другой — для нумерации предметов (первый, второй, третий, ...). В первом случае натуральный ряд начинается с нуля и обозначается $\mathbb{N}_0$, а во втором — с единицы и обозначается $\mathbb{N}$. Различие между этими двумя подходами по большей части терминологическое и на структуру теории натуральных чисел не влияет.

2.33. Теорема (принцип индукции)**.** *Пусть множество A удовлетворяет следующим условиям*:

(i) $0 \in A$;

(ii) *для любого $n \in \mathbb{N}$ из предположения $n \in A$ следует $S(n) \in A$.*

Тогда $\mathbb{N}_0 \subseteq A$.

Доказательство. Очевидно, множество $\mathbb{N}_0 \cap A$ индуктивно; поэтому $\mathbb{N}_0 \subseteq \mathbb{N}_0 \cap A$, откуда $\mathbb{N}_0 \subseteq A$. □

Если в качестве множества A выступает

$$A = \{n \in \mathbb{N}_0 \mid P(n)\},$$

где $P(n)$ — некоторый одноместный предикат, то теорему 2.33 можно переформулировать следующим образом.

2.34. Теорема (метод математической индукции)**.** *Пусть $P(n)$ — некоторый одноместный предикат, зависящий от натурального параметра n. Если высказывание $P(0)$ истинно* (база индукции)

[1] Фридрих Людвиг Готлоб Фреге (Friedrich Ludwig Gottlob Frege; 1848–1925) — немецкий логик, математик и философ.

и доказано, что для любого $n \in \mathbb{N}_0$ *из истинности высказывания* $P(n)$ *вытекает истинность высказывания* $P(n')$*, где* $n' = S(n)$ *— натуральное число, следующее за* n (шаг индукции)*, то предикат* $P(n)$ *является тождественно истинным на множестве натуральных чисел*:

$$P(0) \ \wedge \ \Big(\forall n\colon \ P(n) \Rightarrow P(n')\Big) \quad \Rightarrow \quad \Big(\forall n\colon \ P(n)\Big).$$

2.35. Задолго до появления аксиоматики Цермело—Френкеля, в 1889 г., Дж. Пеано[1] предложил аксиоматику натуральных чисел, весьма похожую на подход Фреге—Рассела. Приведём соответствующие аксиомы.

2.36. Определение. Множество $\mathbb{N}_0$ будем называть *натуральным рядом*, (а его элементы — *натуральными числами*), если на нём задано отображение[2] $S : \mathbb{N}_0 \to \mathbb{N}_0$, ставящее в соответствие каждому элементу $x \in \mathbb{N}_0$ элемент $x' = S(x) \in \mathbb{N}_0$, называемый *следующим* за x (*отображение следования*) и удовлетворяющее следующим аксиомам:

$\mathbb{N}$**1:** нуль является натуральным числом: $0 \in \mathbb{N}_0$;
$\mathbb{N}$**2:** нуль не следует ни за каким натуральным числом:

$$\forall x \in \mathbb{N}_0\colon \ S(x) \neq 0;$$

$\mathbb{N}$**3:** если натуральное число z следует как за числом x, так и за числом y, то $x = y$:

$$(S(x) = z \ \wedge \ S(y) = z) \quad \Rightarrow \quad (x = y);$$

$\mathbb{N}$**4:** *аксиома индукции*: пусть A — подмножество натурального ряда, содержащее нуль и обладающее следующим свойством: если $x \in A$, то $S(x) \in A$; тогда A совпадает с натуральным рядом:

$$(0 \in A) \ \wedge \ (\forall x \in A\colon \ S(x) \in A) \quad \Rightarrow \quad (A = \mathbb{N}_0).$$

2.37. Арифметические операции над натуральными обсуждаются в разделе **??**.

---

[1] Джузеппе Пеано (Giuseppe Peano; 1858—1932) — итальянский математик.

[2] Понятие отображения вводится ниже в разделе 3, однако в настоящий момент достаточно школьного представления об отображении как о правиле, которое каждому элементу некоторого множества ставит в соответствие единственный элемент другого множества.

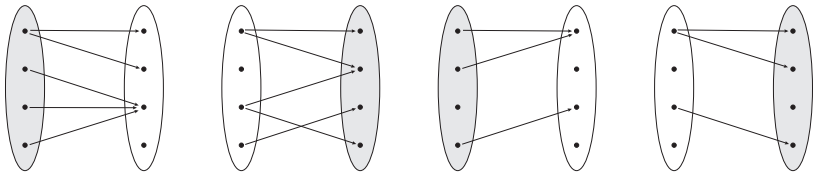


Рис. 2.3. Типы соответствий (к определению 2.41): (а) всюду определённое; (б) сюръективное; (в) функциональное; (г) инъективное

2. Соответствия и отношения

А. Соответствия.

2.38. Определение. *Соответствием* R, заданным на множествах A и B, называется любое подмножество R декартова произведения $A \times B$ этих множеств. Если $(a, b) \in R$, то говорят, что элементы $a \in A$ и $b \in B$ находятся в рассматриваемом соответствии R. Вместо записи $(a, b) \in R$ обычно используют *инфиксную* запись (т.е. запись, при которой знак соответствия ставится между элементами): $a\ R\ b$.

2.39. Для соответствия $R \subset A \times B$ введём следующие термины:

(а) *область отправления* — множество A;
(б) *область прибытия* — множество B;
(в) *область определения* $\operatorname{dom} R$ — множество всех *первых* элементов пар из R:

$$\operatorname{dom} R = \{a \mid \exists b : (a, b) \in R\};$$

(г) *область значений* $\operatorname{im} R$ — множество всех *вторых* элементов пар из R:

$$\operatorname{im} R = \{b \mid \exists a : (a, b) \in R\}.$$

2.40. В случае конечных множеств A и B соответствие $R \subset A \times B$ удобно иллюстрировать с помощью графика: элементы множеств A и B изображаются точками; точки $a \in A$ и $b \in B$ соединяются стрелкой, если $a\ R\ b$ (см. рис. 2.3).

2.41. Определение. Соответствие $R \subset A \times B$ называется

(а) *всюду определённым*, если область определения совпадает с областью отправления: $\operatorname{dom} R = A$; на графике из каждой точки области отправления исходит хотя бы одна стрелка (см. рис. 2.3(а));

(б) *сюръективным*, если область значений совпадает с областью прибытия: $\operatorname{im} R = B$; на графике в каждую точку области прибытия приходит хотя бы одна стрелка (см. рис. 2.3(б));

(в) *функциональным*, если в нём нет пар с одинаковыми первыми и различными вторыми компонентами, т.е.

$$\forall (a_1, b_1), (a_2, b_2) \in R \quad b_1 \neq b_2 \;\Rightarrow\; a_1 \neq a_2$$

или, по контрапозиции,

$$\forall (a_1, b_1), (a_2, b_2) \in R \quad a_1 = a_2 \;\Rightarrow\; b_1 = b_2;$$

на графике из каждой точки области отправления исходит не более одной стрелки (см. рис. 2.3(в)), т.е. запрещены ситуации вида $\bullet \rightrightarrows$;

(г) *инъективным*, если в нём нет пар с различными первыми и одинаковыми вторыми компонентами, т.е.

$$\forall (a_1, b_1), (a_2, b_2) \in R \quad a_1 \neq a_2 \;\Rightarrow\; b_1 \neq b_2$$

или, по контрапозиции,

$$\forall (a_1, b_1), (a_2, b_2) \in R \quad b_1 = b_2 \;\Rightarrow\; a_1 = a_2;$$

на графике в каждую точку области прибытия приходит не более одной стрелки (см. рис. 2.3(г)), т.е. запрещены ситуации вида $\rightrightarrows \bullet$;

(д) *взаимно однозначным соответствием*, или *биективным соответствием*, или *биекцией* между множествами A и B, если оно всюду определено, функционально, сюръективно и инъективно.

2.42. Неформально биекция между множествами A и B может быть описана следующим образом: *каждому* элементу множества A (определённость всюду) поставлен в соответствие *один* элемент множества B (функциональность), причём *разным* элементам множества A соответствуют *разные* элементы множества B (инъективность) и *каждый* элемент множества B соответствует *хотя бы* одному элементу множества A (сюръективность).

Б. Отношения.

2.43. Соответствия $R \subset A \times A$ (у которых область отправления совпадает с областью прибытия) называют *отношениями* на множестве A. Отношения позволяют «сравнивать» элементы множества между собой. Читателю хорошо знакомы следующие примеры отношений на множестве вещественных чисел: $=$, $>$, $\leqslant$.

2.44. Диагональ Δ_A множества A (см. определение **??**, с. **??**) определяет отношение, называемое *тождественным* и обозначаемое обычно $\equiv$.

2.45. Определение. Отношение R на множестве A называется *рефлексивным*, если

$$\forall a \in A : a \; R \; a.$$

Если это условие не выполнено ни для одного элемента множества A, то отношение R называется *антирефлексивным*:

$$\forall a \in A : \neg(a \; R \; a).$$

Если условие рефлексивности выполнено не для всех элементов множества A, то отношение R называется *иррефлексивным*:

$$\exists a \in A : \neg(a \; R \; a)$$

Очевидно, любое антирефлексивное отношение является иррефлексивным, но обратное утверждение неверно.

2.46. Пример. Рассмотрим следующие отношения:

(i) отношение равенства вещественных чисел $=$;
(ii) отношение неравенства вещественных чисел $\neq$;
(iii) отношение «меньше» вещественных чисел $<$;
(iv) отношение «меньше или равно» вещественных чисел $\leqslant$;
(v) отношение делимости натуральных чисел $\vdots$ (пишем $a \vdots b$, если $a \in \mathbb{N}$ делится на $b \in \mathbb{N}$);
(vi) отношение $\eqslantless$ вещественных чисел, определённое правилом $a \eqslantless b \overset{\text{def}}{\Leftrightarrow} a = |b|$;
(vii) отношение строгого включения множеств $\subset$;
(viii) отношение нестрогого включения множеств $\subseteq$;
(ix) отношение параллельности прямых (плоскостей) $\parallel$;
(x) отношение коллинеарности прямых (компланарности плоскостей) $|||$, отличающееся от отношения параллельности тем, что совпадающие прямые (плоскости), не будучи параллельными, являются коллинеарными (компланарными);
(xi) отношение подобия геометрических фигур $\sim$;
(xii) отношение родства «быть родителем»;
(xiii) отношение родства «быть сиблингом»[1].

[1] Сиблинги — термин, обозначающий детей, имеющих хотя бы одного общего родителя, и позволяющий избежать необходимости уточнять пол братьев и сестёр индивида.

Рефлексивные	$=$, $\leqslant$, $\vdots$, $\subseteq$, $\sim$, $\|\|\|$
Антирефлексивные	$\neq$, $<$, $\subset$, $\parallel$, «быть родителем», «быть сиблингом»
Иррефлексивное	$\fallingdotseq$

2.47. Определение. Отношение R на множестве A называется *симметричным*, если из того факта, что элемент a находится в отношении R к элементу b, следует, что элемент b находится в отношении R к элементу a:

$$\forall a, b \in A : (a\ R\ b) \Longrightarrow (b\ R\ a).$$

Отношение R на множестве A называется *асимметричным*, если

$$\forall a, b \in A : (a\ R\ b) \Longrightarrow \neg(b\ R\ a);$$

иными словами, невозможно одновременное выполнение соотношений $(a\ R\ b)$ и $(b\ R\ a)$. Отношение R на множестве A называется *антисимметричным*, если из $a\ R\ b$ и $b\ R\ a$ следует, что $a = b$:

$$\forall a, b \in A : (a\ R\ b) \wedge (b\ R\ a) \Longrightarrow (a = b).$$

2.48. Пример. Для отношений, рассмотренных в примере 2.46, имеем:

	Являются	Не являются
Симметричные	$=$, $\neq$, $\parallel$, $\|\|\|$, $\sim$, «быть сиблингом»	$<$, $\leqslant$, «быть родителем»
Асимметричные	$<$, «быть родителем»	$\leqslant$, $\subseteq$
Антисимметричные	$=$, $\leqslant$, $\subseteq$, $\vdots$, $\fallingdotseq$	$<$, $\neq$

2.49. Замечание. Сравнивая определения симметричных, асимметричных и антисимметричных отношений, можно убедиться в следующем:

(1) непустое отношение не может быть одновременно симметричным и асимметричным;
(2) однако термины «симметричное отношение» и «асимметричное отношение» не являются антонимами; например, отношение $\leqslant$ не является симметричным, но и не является асимметричным;
(3) отношение может быть одновременно симметричным и антисимметричным; примером может служить отношение $=$;
(4) любое антисимметричное отношение не является асимметричным, так что термины «асимметричное отношение» и «антисимметричное отношение» не являются синонимами;

(5) термины «симметричное отношение» и «антисимметричное отношение» не являются антонимами; например, отношение $<$ не является симметричным, но и не является антисимметричным;
(6) свойства антирефлексивности и антисимметричности несовместны.

2.50. Определение. Отношение R на множестве A называется *транзитивным*, если

$$\forall a, b, c \in A : (a\ R\ b) \wedge (b\ R\ c) \Longrightarrow (a\ R\ c).$$

Отношение, не обладающее свойством транзитивности, называется *интранзитивным*.

2.51. Пример. Отношения $=$, $<$, $\leqslant$, $\subset$, $\subseteq$, $\sim$, $|||$ являются транзитивными, отношения $\neq$, $\|$, «быть родителем», «быть сиблингом»[1] — не являются.

B. Отношения порядка.

2.52. Определение. Отношение $R \subset A \times A$ называется *отношением* (*нестрогого*) *частичного порядка*, если оно рефлексивно, транзитивно и антисимметрично. Типичное обозначение: $\preccurlyeq$. Множество с заданным на нем отношением частичного порядка называется *частично упорядоченным* (аббревиатура ч.у.м.).

2.53. Определение. Два элемента a, b частично упорядоченного множества A с отношением частичного порядка $\preccurlyeq$ называются *сравнимыми*, если $a \preccurlyeq b$ или $b \preccurlyeq a$. Обратите внимание, что в определении 2.52 не требуется, чтобы любые два элемента множества были сравнимы. Если в ч.у.м. A любые два элемента сравнимы, то порядок называется *линейным*, а множество — *линейно упорядоченным*.

2.54. Пример. 1. Множество вещественных чисел (а также любое его подмножество) с отношением $\leqslant$ является линейно упорядоченным.
2. Введём на множестве $\mathbb{R}^2$ отношение частичного порядка $\preccurlyeq$, полагая

$$(a_1, b_1) \preccurlyeq (a_2, b_2) \quad \stackrel{\text{def}}{=\!=} \quad (a_1 \leqslant b_1) \wedge (a_2 \leqslant b_2).$$

[1] Действительно, если X — сын $A(\male)$ и $B(\female)$, Y — сын $B(\female)$ и $C(\male)$, Z — сын $C(\male)$ и $D(\female)$, то X и Y — братья (общий отец $C(\male)$), Y и Z — братья (общая мать $D(\female)$), но X и Z братьями не являются, так как общих родителей не имеют.

(Самостоятельно проверьте, что это отношение действительно является частичным порядком.) Это порядок не является линейным: пары $(1,0)$ и $(0,1)$ несравнимы.

3. На множестве числовых функций с вещественными аргументами и значениями можно ввести частичный порядок, считая, что

$$f \preccurlyeq g \quad \stackrel{\text{def}}{=\!=} \quad \forall x \in \mathbb{R}\ f(x) \leqslant g(x).$$

Этот порядок не является линейным (приведите пример несравнимых функций).

4. На множестве натуральных чисел определим отношение $\preccurlyeq$ правилом

$$a \preccurlyeq b \quad \stackrel{\text{def}}{=\!=} \quad b \vdots a$$

(по поводу обозначения $\vdots$ см. пример 2.46, с. 39).

5. Пусть A — произвольное множество. Отношение включения $\subseteq$ на множестве $\mathcal{P}(A)$ всех его подмножеств является частичным порядком.
6. На множестве букв русского алфавита определен традиционный *алфавитный порядок* а $\preccurlyeq$ б $\preccurlyeq$ в $\preccurlyeq \cdots \preccurlyeq$ я. Этот порядок, очевидно, линеен.
7. На множестве слов[1], составленных из букв русского алфавита, определен так называемый *лексикографический порядок*:
   (i) если слово x является началом слова y, то $x \preccurlyeq y$ (например, кот $\preccurlyeq$ котёл);
   (ii) если ни одно из слов не является началом другого, сравниваем первые (слева) различные буквы этих слов; то слово, где эта буква меньше в алфавитном порядке, является меньшим в смысле лексикографического порядка (например, стол $\preccurlyeq$ стул).

   Лексикографический порядок линеен (этот факт облегчает составление словарей).

2.55. Определение. Отношение $R \subset A \times A$ называется *отношением строгого частичного порядка*, если оно антирефлексивно и транзитивно. Типичное обозначение: $\prec$.

Примером отношения строгого порядка является отношение $<$ на множестве вещественных чисел.

Г. Отношение эквивалентности.

[1]Термин «слово» обозначает произвольную конечную последовательность букв алфавита, возможно, семантически бессмысленную.

2.56. Определение. Отношение $R \subset A \times A$ называется *отношением эквивалентности*, если оно рефлексивно, симметрично и транзитивно:

(i) *рефлексивность*: для любого $a \in A$ имеем $a \mathrel{R} a$;
(ii) *симметричность*: для любых $a, b \in A$ из $a \mathrel{R} b$ следует $b \mathrel{R} a$;
(iii) *транзитивность*: для любых $a, b, c \in A$ из $a \mathrel{R} b$ и $b \mathrel{R} c$ следует $a \mathrel{R} c$.

Вместо $a \mathrel{R} b$ используют следующие типичные инфиксные обозначения: $a \sim b$, $a \simeq b$, $a \cong b$, $a \approx b$.

2.57. Пример. 1. Как следует из примеров 2.46 и 2.48, отношениями эквивалентности являются отношения равенства чисел $=$, подобия геометрических фигур $\sim$, коллинеарности прямых (компланарности плоскостей) $|||$.
2. Тождественное отношение $\equiv$ на множестве A является *наименьшим* отношением эквивалентности на A в том смысле, что для любого другого отношения эквивалентности R на A имеем $\Delta_A \subseteq R$.

2.58. Определение. Пусть $\sim$ — отношение эквивалентности на множестве A. Для каждого элемента $a \in A$ его *классом эквивалентности относительно отношения* $\sim$ называется множество

$$[a] \stackrel{\text{def}}{=\!=} \{x \in A \mid x \sim a\}.$$

Например, если на множестве всех треугольников введено отношение подобия и $\triangle ABC$ — равносторонний, то классом эквивалентности $[\triangle ABC]$ является множество всех равносторонних треугольников.

2.59. Теорема.

1. *Если множество A представлено в виде объединения непересекающихся подмножеств, $A = \bigsqcup\limits_{\alpha \in \mathfrak{A}} A_\alpha$, то отношение «лежать в одном подмножестве» является отношением эквивалентности.*
2. *Любое отношение эквивалентности $\sim$ порождает разбиение множества A на непересекающиеся классы эквивалентности своих элементов:*

$$A = \bigsqcup [a].$$

Доказательство. Утверждение 1 очевидно. Для доказательства утверждения 2 рассмотрим произвольное отношение эквивалентности $\sim$ на множестве A и построим для него соответствующее

разбиение множества A в объединение непересекающихся подмножеств. Возьмём для каждого элемента $a \in A$ его класс эквивалентности. Докажем, что для двух различных $a_1, a_2 \in A$ классы $[a_1]$ и $[a_2]$ либо не пересекаются, либо совпадают. Предположим, что пересечение классов $[a_1]$ и $[a_2]$ непусто, т.е. $\exists c \in [a_1] \cap [a_2]$. Тогда $c \sim a_1$ и $c \sim a_2$, откуда $a_1 \sim c$ (симметричность) и $a_1 \sim a_2$ (транзитивность), т.е. $a_1 \in [a_2]$. Аналогично получаем, что $a_2 \in [a_1]$. Итак, $[a_1] \subset [a_2]$ и $[a_2] \subset [a_1]$, поэтому (см. п. **??**) $[a_1] = [a_2]$: пересекающиеся классы полностью совпадают. В силу рефлексивности каждый элемент $a \in A$ принадлежит задаваемому им классу, $a \in [a]$, т.е. действительно все множество A разбито на непересекающиеся классы: $A = \bigsqcup [a]$. □

2.60. Определение. Рассмотрим отношение эквивалентности $\sim$ на множестве A. Множество

$$A/\sim \stackrel{\text{def}}{=\!=} \{[a] \mid a \in A\},$$

состоящее из всех классов эквивалентности $[a]$ относительно $\sim$, называется *фактор-множеством* множества A по отношению $\sim$.

2.61. Каждый класс эквивалентности $[x]$ определяется любым своим элементом; составить представление об устройстве класса можно, взяв из него какой-либо любой элемент, называемый *представителем* этого класса.

2.62. Пример. Рассмотрим множество A всех студентов некоторого учебного заведения, на котором введено отношение эквивалентности

$$(a \sim b) \stackrel{\text{def}}{=\!=} (\text{«студенты } a \text{ и } b \text{ учатся в одной группе»})$$

(проверьте выполнение свойств (i)–(iii) определения 2.56 самостоятельно). Классами эквивалентности являются в этом случае студенческие группы, а фактор-множеством — множество групп.

2.63. Пример. В математическом анализе рассматривается следующее отношение эквивалентности на множестве функций:

$$f(x) \sim g(x) \text{ при } x \to x_0, \quad \text{если } \lim_{x \to x_0} \frac{f(x)}{g(x)} = 1.$$

Это отношение позволяет значительно упростить вычисление пределов.

3. Отображения

Понятие отображения играет в математике центральную роль. Термины «отображение», «функция», «функционал», «оператор», «преобразование» являются синонимами; их употребление определяется сложившейся в разных разделах математики традицией.

A. Основные термины.

2.64. Определение. Пусть f — соответствие, заданное на множествах X и Y (т.е. подмножество декартова произведения $X \times Y$), *определённое всюду* на множестве X (см. определение 2.41) и обладающее свойством *функциональности*: в нём нет пар с одинаковыми первыми и разными вторыми компонентами, т.е.

$$\forall (x_1, y_1), (x_2, y_2) \in f \quad y_1 \neq y_2 \implies x_1 \neq x_2.$$

Соответствие f называется *отображением*, определённым ***на*** множестве X и принимающим значения ***в*** множестве Y.[1]

2.65. Это определение уточняет знакомое читателю из школьного курса представление о функции как о правиле, которое *каждому* элементу одного множества (области определения) ставит в соответствие *единственный* элемент другого множества (области значений). В школе читатель имел дело в основном с *числовыми* функциями (область определения и множество значений — числовые множества, т.е. подмножества $\mathbb{R}$); в курсах высшей математики нам придётся иметь дело с отображениями множеств другой природы.

2.66. С понятием отображения связаны следующие термины и обозначения:

(a) если $(x, y) \in f$, то говорят, что y — *значение* отображения f на элементе x (в точке x), или y — *образ элемента* x при отображении f, и используют записи $y = f(x)$, $f\colon x \mapsto y$ и $x \overset{f}{\longmapsto} y$; говорят также, что отображение f переводит (преобразует, превращает; функция f отображает) элемент x в элемент y;[2]

[1] Предлоги «на» и «в» в этом определении употребляются не произвольно, а играют самостоятельную роль, имеют терминологическое значение; см. определение 2.68 ниже.

[2] Символ $f(x)$ обозначает *значение отображения на элементе* x; отображением является именно f, а не $f(x)$! Выражение «функция $y = f(x)$» не вполне корректно: оно *задаёт* функцию, но *не является* ею. Однако во многих разделах математики часто обозначают через $f(x)$ как саму функцию, так и выражение, её задающее. Такое соглашение является в большинстве случаев удобным и вполне оправданным.

(б) *образ множества* $C \subset X$ при отображении f — это множество
$$f(C) = \{f(c) \mid c \in C\} = \{y \in Y \mid \exists c \in C : (c, y) \in f\};$$
(в) X — *область определения* отображения f; используются обозначения $\operatorname{dom} f$ и $D(f)$;
(г) Y — *область прибытия* отображения f; говорят, что отображение f принимает значения ***в*** множестве Y;
(д) $\operatorname{im} f \stackrel{\text{def}}{=\!=} \{y \in Y \mid \exists x : y = f(x)\} \subset Y$ — *область значений* отображения f; говорят, что отображение f принимает значения ***на*** множестве $\operatorname{im} f$; используется также обозначение $R(f)$;
(е) записи $f\colon X \to Y$, $X \xrightarrow{f} Y$ означают, что f — отображение с областью определения X и областью прибытия Y;
(ж) взаимно однозначное (биективное) отображение $f\colon X \to X$ часто называют (особенно в геометрии) *преобразованием* множества X;
(з) *прообраз элемента* $y \in Y$ — это множество
$$f^{-1}(y) \stackrel{\text{def}}{=\!=} \{x \in X \mid f(x) = y\};$$
символ $f^{-1}(y)$ не следует ассоциировать с обратным отображением, которое может и не существовать (см. ниже п. **??**);
(и) *прообраз подмножества* $B \subset Y$ — это множество
$$f^{-1}(B) \stackrel{\text{def}}{=\!=} \{x \in X \mid f(x) \in B\} = \bigcup_{y \in B} f^{-1}(y).$$
Очевидно, если $y \in Y \setminus \operatorname{im} f$, то $f^{-1}(y)$ не существует или, эквивалентно, $f^{-1}(\{y\}) = \varnothing$.

2.67. Два отображения f и g называются *равными*, если их соответствующие области совпадают: $X \xrightarrow{f} Y$, $X \xrightarrow{g} Y$, причём $f(x) = g(x)$ для любого $x \in X$.

2.68. Определение (ср. определение 2.41)**.** Отображение $f\colon X \to Y$ называется
(а) *сюръективным* (сюръекцией, или отображением «на»), если $\operatorname{im} f = Y$;
(б) *инъективным* (инъекцией), если из неравенства $x_1 \neq x_2$ вытекает $f(x_1) \neq f(x_2)$ или, по контрапозиции, из $f(x_1) = f(x_2)$ следует $x_1 = x_2$;
(в) *биективным* (взаимно однозначным, биекцией), если оно одновременно сюръективно и инъективно.

2.69. Пример. Пусть $\mathbb{R}_{\geqslant 0} \stackrel{\text{def}}{=\!=} \{x \in \mathbb{R} \mid x \geqslant 0\}$ — множество всех неотрицательных вещественных чисел. Три отображения

$f\colon \mathbb{R} \to \mathbb{R}$, $g\colon \mathbb{R} \to \mathbb{R}_{\geqslant 0}$, $h\colon \mathbb{R}_{\geqslant 0} \to \mathbb{R}_{\geqslant 0}$, определённые одним и тем же правилом $x \mapsto x^2$, все различны:

(1) f не является ни сюръективным ($\operatorname{im} f = \mathbb{R}_{\geqslant 0}$), ни инъективным (числа x и $-x$ имеют один и тот же образ);
(2) g сюръективно, но не является инъективным;
(3) h биективно.

2.70. Определение. В дальнейшем будут использоваться следующие отображения.

1. Отображение $\mathrm{id}_X\colon X \to X$, определённое правилом $\mathrm{id}_X\colon x \mapsto x$, называется *тождественным*. Очевидно, оно биективно.
2. Пусть $c \in X$. Отображение $X \to X$, определённое правилом $x \mapsto c$, называется *постоянным отображением*, или *константой*, и обозначается тем же символом, что и элемент c, т.е. $c\colon X \to X$, $c\colon x \mapsto c$.
3. Пусть $X \subseteq Y$. Отображение $\iota\colon X \to Y$, определённое на X правилом $\iota\colon x \mapsto x$, ставит каждому элементу $x \in X$ тот же самый элемент, но уже в множестве Y. Это отображение называется *вложением множества* X в множество Y и часто обозначается $\iota\colon X \hookrightarrow Y$.

2.71. Определение. Пусть $X \subset \tilde{X}$. Отображение $f\colon X \to Y$ называется *сужением* (или *ограничением*) отображения $g\colon \tilde{X} \to Y$ на подмножество X, если $f(x) = g(x)$ для всех $x \in X$; обозначение $f = g|_X$. В свою очередь, отображение $g\colon \tilde{X} \to Y$ называется *продолжением* отображения $f\colon X \to Y$ на множество $\tilde{X}$.

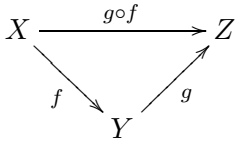
2.72. Пример. Отображение вложения $f\colon X \hookrightarrow Y$ является сужением тождественного отображения $\mathrm{id}_Y\colon Y \to Y$ на подмножество X: $f = \mathrm{id}_Y|_X$.

Б. Композиция отображений.

2.73. Определение. *Композицией* (или *суперпозицией*) отображений $f\colon X \to Y$ и $g\colon Y \to Z$ называется отображение $g \circ f\colon X \to Z$, определённое условием

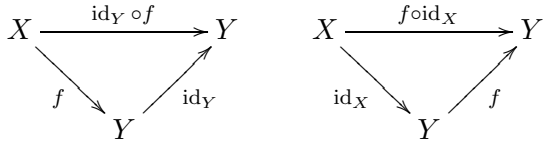
$$(\forall x \in X)\ (g \circ f)(x) = g\big(f(x)\big)$$

(правее пишется то отображение, которое применяется первым). То же самое наглядно изображается при помощи диаграммы



Про эту диаграмму говорят, что она *коммутативна*, т.е. результат перехода от X к Z не зависит от того, сделаем мы это непосредственно при помощи $g \circ f$ или воспользуемся промежуточным множеством Y.

2.74. Замечание. Из диаграмм



очевидно, что для любого отображения $f\colon X \to Y$

$$\mathrm{id}_Y \circ f = f \circ \mathrm{id}_X = f.$$

2.75. Замечание. Композиция отображений, вообще говоря, не коммутативна, т.е. $g \circ f \neq f \circ g$, хотя бы по той причине, что для $X \xrightarrow{f} Y$ и $Y \xrightarrow{g} Z$ отображение $X \xrightarrow{g\circ f} Z$ определено, а $f \circ g$ — не определено, если $Z \neq X$. Но даже в случае преобразований $f, g\colon X \to X$, когда обе композиции $g \circ f$ и $f \circ g$ определены, коммутативность может не иметь места, как показывают примеры числовых функций $f\colon x \mapsto x^2$ и $g\colon x \mapsto \sin x$:

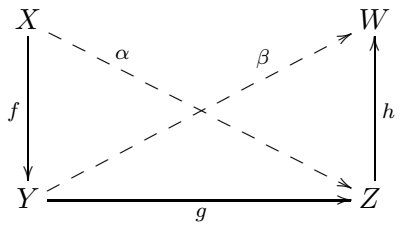
$$(g \circ f)(x) = g(f(x)) = \sin(x^2), \quad (f \circ g)(x) = f(g(x)) = (\sin x)^2.$$

2.76. Предложение. *Композиция отображений ассоциативна, т.е. для отображений $f\colon X \to Y$, $g\colon y \to Z$, $h\colon Z \to W$ имеет место соотношение*

$$(h \circ g) \circ f = h \circ (g \circ f),$$

что позволяет не ставить скобки и писать $h \circ g \circ f$.

Доказательство. Все необходимые рассуждения легко восстанавливаются по диаграмме



где $\alpha = g \circ f$, $\beta = h \circ g$. В соответствии с определением равенства отображений нужно сравнить значения отображений $h \circ (g \circ f)$ и

$h \circ (g \circ f)$ на элементе $x \in X$. Согласно определению композиции отображений имеем

$$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))) = \\ = (h \circ g)(f(x)) = ((h \circ g) \circ f)(x). \quad \square$$

$\square$

B. Обратное отображение.

2.77. Определение. Пусть $f\colon X \to Y$ и $g\colon Y \to X$ — отображения. Если

$$g \circ f = \mathrm{id}_X,$$

то отображение g называется *левым обратным* для f, а f — *правым обратным* для g.

2.78. Предложение. *Если для отображений $f\colon X \to Y$ и $g\colon Y \to X$ выполняется соотношение $g \circ f = \mathrm{id}_X$, то f инъективно, а g сюръективно.*

Доказательство. Пусть $x_1, x_2 \in X$ и $f(x_1) = f(x_2)$. Тогда

$$x_1 = \mathrm{id}_X(x_1) = (g \circ f)(x_1) = g(f(x_1)) = \\ = g(f(x_2)) = (g \circ f)(x_2) = \mathrm{id}_X(x_2) = x_2,$$

т.е. f инъективно. Далее, если x — произвольный элемент из X, то

$$x = \mathrm{id}_X(x) = (g \circ f)(x) = g(f(x)),$$

т.е. каждый элемент $x \in X$ является образом некоторого элемента (а именно, $f(x)$) под действием отображения g, т.е. g — сюръективно. $\square$

2.79. Определение. Пусть $f\colon X \to Y$ и $g\colon Y \to X$ — отображения. Если

$$g \circ f = \mathrm{id}_X \quad \text{и} \quad f \circ g = \mathrm{id}_Y, \tag{2.3}$$

то отображение g называется *двусторонним обратным* (или просто *обратным*) к отображению f и обозначается f^{-1}. Таким образом,

$$f(x) = y \quad \Leftrightarrow \quad f^{-1}(y) = x.$$

Отображения f и f^{-1} называют *взаимно обратными*.

2.80. Замечание. Обратное отображение обозначается тем же символом f^{-1}, что и операция взятия прообраза; следует избегать смешения этих понятий: прообраз элемента (или множества) существует даже в том случае, когда отображение не имеет обратного.

2.81. Теорема. *Если для отображения существует (двустороннее) обратное, то оно единственно.*

Доказательство. Предположим, что для отображения $f\colon X \to Y$ существуют два обратных отображения $g\colon Y \to X$ и $g'\colon Y \to X$, т.е.

$$g \circ f = \mathrm{id}_X, \quad f \circ g = \mathrm{id}_Y,$$
$$g' \circ f = \mathrm{id}_X, \quad f \circ g' = \mathrm{id}_Y .$$

Имеем:

$$g' = \mathrm{id}_X \circ g' = (g \circ f) \circ g' = g \circ (f \circ g') = g \circ \mathrm{id}_Y = g. \qquad \square$$

2.82. Теорема. *Отображение $f\colon X \to Y$ имеет обратное тогда и только тогда, когда оно биективно.*

Доказательство. Необходимость. Пусть отображение $f\colon X \to Y$ имеет обратное $g = f^{-1}$; тогда из равенств (2.3) и предложения 2.78 вытекает как инъективность, так и сюръективность отображения f.

Достаточность. Предположим, что f биективно. Тогда для любого $y \in Y$ существует единственный элемент $x \in X$, для которого $f(x) = y$. Положив $g(y) = x$, мы определим отображение $g\colon Y \to X$, обладающее свойствами (2.3). Значит, $f^{-1} = g$. $\square$

2.83. Пример. Положим $X = \mathbb{R}_{\geqslant 0}$, $Y = \mathbb{R}$ и рассмотрим функции

$$f\colon \mathbb{R}_{\geqslant 0} \to \mathbb{R},\ x \mapsto \sqrt{x}, \qquad g\colon \mathbb{R} \to \mathbb{R}_{\geqslant 0},\ x \mapsto x^2.$$

Так как

$$(g \circ f)(x) = g(f(x)) = g(\sqrt{x}) = (\sqrt{x})^2 = x \ \Leftrightarrow\ (g \circ f) = \mathrm{id}_X,$$

функция f является *правой обратной* для g и инъективна (для $x_1 \neq x_2$ имеем $\sqrt{x_1} \neq \sqrt{x_2}$), а функция g является *левой обратной* для f и сюръективна ($\operatorname{Im} g = X = \mathbb{R}_{\geqslant 0}$). Функции f и g взаимно обратными *не являются*.

Для биективных функций

$$F\colon \mathbb{R}_{\geqslant 0} \to \mathbb{R}_{\geqslant 0}, \quad x \mapsto \sqrt{x},$$
$$G\colon \mathbb{R}_{\geqslant 0} \to \mathbb{R}_{\geqslant 0}, \quad x \mapsto x^2,$$

имеем

$$(G \circ F)(x) = G(F(x)) = G(\sqrt{x}) = (\sqrt{x})^2 = x \ \Leftrightarrow\ G \circ F = \mathrm{id}\,|_X,$$
$$(F \circ G)(x) = F(G(x)) = F(x^2) = \sqrt{x^2} = x \quad \Leftrightarrow\ F \circ G = \mathrm{id}\,|_X,$$

так что функции F и G являются *взаимно обратными*.

2.84. Пример. Отображение $\sin\colon \mathbb{R} \to [-1;1]$ не имеет обратного, поскольку не является биективным (оно не инъективно), однако его сужение

$$\sin\big|_{[-\pi/2;\pi/2]}\colon \left[-\frac{\pi}{2};\frac{\pi}{2}\right] \to [-1;1],$$

будучи взаимно однозначным, имеет обратное отображение

$$\arcsin\colon [-1;1] \to \left[-\frac{\pi}{2};\frac{\pi}{2}\right].$$

2.85. Предложение.

(i) *Если отображение $f\colon X \to Y$ биективно, то $f^{-1}\colon Y \to X$ также биективно, причём*

$$(f^{-1})^{-1} = f. \tag{2.4}$$

(ii) *Если $f\colon X \to Y$, $h\colon Y \to Z$ — биективные отображения, то их композиция $h \circ f\colon X \to Z$ также биективна, причём*

$$(h \circ f)^{-1} = f^{-1} \circ h^{-1}. \tag{2.5}$$

Доказательство. (i) По теореме 2.82 биективность f влечет существование f^{-1}, что в силу той же теоремы эквивалентно биективности f^{-1}. Симметричность условий (2.3), записанных в виде

$$f^{-1} \circ f = \mathrm{id}_X, \quad f \circ f^{-1} = \mathrm{id}_Y,$$

даёт равенство (2.4).

(ii) Согласно условию и теореме 2.82 существуют отображения $f^{-1}\colon Y \to X$, $h^{-1}\colon Z \to Y$ и их композиция $f^{-1} \circ h^{-1}\colon Z \to X$. Равенства

$$\begin{aligned}\big(f^{-1} \circ h^{-1}\big) \circ \big(h \circ f\big) &= f^{-1} \circ \big(h^{-1} \circ (h \circ f)\big) = \\ &= f^{-1} \circ \big(\underbrace{(h^{-1} \circ h)}_{=\mathrm{id}_Y} \circ f\big) = f^{-1} \circ (\mathrm{id}_Y \circ f) = f^{-1} \circ f = \mathrm{id}_X,\end{aligned}$$

$$\begin{aligned}\big(h \circ f\big) \circ \big(f^{-1} \circ h^{-1}\big) &= \big((h \circ f) \circ f^{-1}\big) \circ h^{-1} = \\ &= \big(h \circ \underbrace{(f \circ f^{-1})}_{=\mathrm{id}_Y}\big) \circ h^{-1} = (h \circ \mathrm{id}_Y) \circ h^{-1} = \mathrm{id}_Z\end{aligned}$$

показывают, что $f^{-1} \circ h^{-1}$ — обратное отображение к $h \circ f$. □

Г. Факторизация отображений. В теореме 2.59 было установлено взаимно однозначное соответствие между отношениями эквивалентности на множестве и разбиениями этого множества в объединение непересекающихся классов.

2.86. Определение. Пусть X — множество, $\sim$ — отношение эквивалентности на X, $X/\!\sim$ — соответствующее фактор-множество (см. определение 2.60). Отображение

$$\pi\colon X \to X/\!\sim, \quad x \mapsto [x] \tag{2.6}$$

которое каждому элементу x множества X ставит в соответствие его класс эквивалентности $[x]$, называется *канонической проекцией* множества X на фактор-множество $X/\!\sim$. Очевидно, каноническая проекция (2.6) является сюръективным отображением.

2.87. Теорема. *Пусть $f\colon X \to Y$ — отображение. Бинарное отношение $\underset{f}{\sim}$ на X, определённое правилом*

$$\forall x_1, x_2 \in X\colon \quad x_1 \underset{f}{\sim} x_2 \;\Leftrightarrow\; f(x_1) = f(x_2),$$

является отношением эквивалентности. Каждый класс эквивалентности $[x]$ является прообразом любого своего представителя $x \in X$ относительно отображения f:

$$[x] = \bigl\{x' \in X \mid f(x') = f(x)\bigr\} = f^{-1}\bigl(\{x\}\bigr).$$

Доказательство. Рефлексивность: $f(x) = f(x)$.
Симметричность: $f(x_1) = f(x_2) \Rightarrow f(x_2) = f(x_1)$.
Транзитивность: $f(x_1) = f(x_2) \wedge f(x_2) = f(x_3) \Rightarrow f(x_1) = f(x_3)$. $\square$

2.88. Определение. Отображение $f\colon X \to Y$ индуцирует отображение $\bar{f}\colon X/\underset{f}{\sim} \to Y$, определённое правилом

$$\bar{f}([x]) = f(x) \tag{2.7}$$

и называемое *фактор-отображением*.

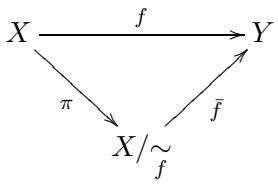
2.89. Замечание. Отображение $\bar{f}\colon X/\underset{f}{\sim} \to Y$, индуцированное отображением $f\colon X \to Y$, определено корректно, т.е. не зависит от выбора представителя x класса $[x]$, так как

$$[x] = [x'] \;\Leftrightarrow\; f(x) = f(x').$$

2.90. Теорема. *Отображение f может быть представлено в виде композиции*

$$f = \bar{f} \circ \pi$$

сюръективной канонической проекции $\pi\colon X \to X/\underset{f}{\sim}$ *и инъективного фактор-отображения* $\bar{f}$:



Отображение $\bar{f}$*, делающее диаграмму коммутативной, единственно.*

Доказательство. Соотношение (2.7) может быть переписано в виде

$$(\bar{f} \circ \pi)(x) = f(x) \;\Leftrightarrow\; f = \bar{f} \circ \pi.$$

Отображение π сюръективно (см. определение 2.6). Инъективность $\bar{f}$ вытекает из того, что

$$\bar{f}([x_1]) = \bar{f}([x_2]) \;\Leftrightarrow\; f(x_1) = f(x_2) \;\Leftrightarrow\; [x_1] = [x_2].$$

Пусть $f'\colon X/\underset{f}{\sim} \to Y$ — еще одно отображение, для которого $f = f' \circ \pi$. Тогда

$$f'([x]) = f'(\pi(x)) = (f' \circ \pi)(x) = f(x) = \bar{f}([x]),$$

так что $f' = \bar{f}$. □

2.91. Пример (см. рис. 2.4)**.** Рассмотрим на евклидовой плоскости E функцию $f\colon E \to \mathbb{R}_{\geqslant 0}$, которая каждой точке $M \in E$ ставит в соответствие расстояние от этой точки до некоторой фиксированной точки O: $f(M) = |OM|$. Классы эквивалентности относительно отношения эквивалентности $\overset{f}{\sim}$, порождённого этой функцией, — это концентрические окружности с центром в точке O (а также сама точка O); фактор-множество $E/\overset{f}{\sim}$ состоит из этих окружностей. Отображение $\varphi\colon E/\overset{f}{\sim} \to \mathbb{R}_{\geqslant 0}$ ставит в соответствие каждой окружности её радиус (точке O соответствует число 0).

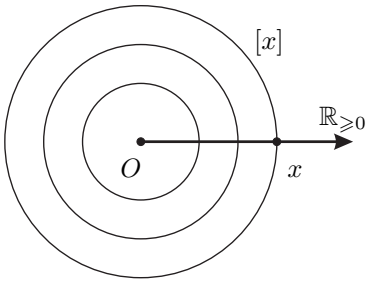


Рис. 2.4.

Д. Семейства элементов множества.

2.92. Определение. *n-Членным семейством* (*упорядоченным набором*, *конечной последовательностью*) элементов множества X будем называть отображение

$$f\colon \{1, 2, \ldots, n\} \to X, \quad k \mapsto x_k,$$

которое каждому натуральному числу $k \in \{1, 2, \ldots, n\}$ ставит в соответствие некоторый элемент $x_k \overset{\text{def}}{=\!=} f(k)$ множества X, называемый *k-м членом семейства*. Всё семейство обозначается при этом $(x_1, x_2, \ldots, x_n)$.

2.93. Определение. Множество всех n-членных семейств элементов множества X называется n-й *декартовой степенью* множества X и обозначается X^n:

$$X^n \overset{\text{def}}{=\!=} \Big\{ (x_1, \ldots, x_n) \;\Big|\; x_k \in X,\ k = 1, \ldots, n \Big\}.$$

2.94. Если $\{j_1, j_2, \ldots, j_s\} \subset \{1, 2, \ldots, n\}$, то сужение отображения f

$$f\big|_{\{j_1, j_2, \ldots, j_s\}}\colon \{j_1, j_2, \ldots, j_s\} \to X$$

определяет *подсемейство* $(x_{j_1}, x_{j_2}, \ldots, x_{j_s})$ семейства $(x_1, x_2, \ldots, x_n)$.

2.95. Определение. Отображение

$$g\colon \mathbb{N} \to X, \quad k \mapsto x_k, \tag{2.8}$$

которое каждому натуральному числу $k \in \mathbb{N}$ ставит в соответствие некоторый элемент x_k множества X, называется (бесконечной) *последовательностью* элементов множества X.

2.96. Определение. Если M — бесконечное подмножество множества $\mathbb{N}$ натуральных чисел, $M = \{m_1, m_2, \dots\}$, то сужение отображения (2.8)

$$g\big|_M\colon M \to X, \quad m_k \mapsto x_{m_k}$$

называется *подпоследовательностью* рассмотренной последовательности.

2.97. Аналогично определению 2.92 семейства элементов множества X можно сформулировать определения семейства, состоящего из элементов различных множеств, и декартова произведения различных множеств.

2.98. Определение. Пусть $X_1, \dots, X_n$ — множества. *Семейством* (упорядоченным набором) $(x_1, \dots, x_n)$, где $x_k \in X_k$, $k \in \{1, \dots, n\}$, будем называть отображение

$$f\colon \{1, 2, \dots, n\} \to X_1 \cup X_2 \cup \dots \cup X_n, \quad k \mapsto x_k \in X_k,$$

которое каждому натуральному числу $k \in \{1, 2, \dots, n\}$ ставит в соответствие некоторый элемент $x_k \stackrel{\text{def}}{=\!=} f(k) \in X_k$ множества X_k, называемый k-м членом семейства. Множество всех семейств $(x_1, \dots, x_n)$ называется *декартовым произведением* множеств $X_1, \dots, X_n$ и обозначается $X_1 \times \dots \times X_n$.

2.99. Существование отображения, фигурирующего в определении 2.98, интуитивно очевидно; в случае, когда набор множеств $X_1, \dots, X_n$ конечен, этот факт может быть доказан исходя из аксиом теории множеств и не требует постулирования в качестве отдельной аксиомы. Ситуация меняется, если рассматривается бесконечный набор множеств. Пусть $\mathfrak{A}$ — какое-либо множество (назовём его множеством индексов) и X_α — какие-либо множества, «занумерованные» индексами $\alpha \in \mathfrak{A}$. В этом случае факт существования отображения f из определения 2.98 должен быть постулирован отдельно, поскольку он не вытекает из остальных аксиом, т.е. является независимым утверждением. Соответствующее утверждение называется аксиомой выбора.

2.100. ***Аксиома выбора.*** Для любого набора непустых множеств $\{X_\alpha \mid \alpha \in \mathfrak{A}\}$ найдется (хотя бы одно) отображение $f\colon \mathfrak{A} \to \bigcup\limits_{\alpha\in\mathfrak{A}}$,

удовлетворяющее условию

$$\forall \alpha \in \mathfrak{A} : f(\alpha) \in X_\alpha.$$

2.101. Аксиома выбора была сформулирована и опубликована Э. Цермело в 1904 г. Из аксиомы выбора следуют некоторые парадоксальные утверждения, вызывающие интуитивный протест, например, парадокс Банаха—Тарского; подобные парадоксы служат доводами против принятия аксиомы выбора.

2.102. ***Парадокс Банаха—Тарского.*** Пусть B и B' — два шара разных радиусов в трёхмерном евклидовом пространстве. Шар B можно представить в виде объединения конечного числа попарно непересекающихся множеств $B = X_1 \cup \cdots \cup X_n$, а шар B' — в виде объединения конечного числа попарно непересекающихся множеств $B' = X'_1 \cup \cdots \cup X'_n$ таким образом, что множество X_1 переводится некоторым движением пространства в X'_1, X_2 переводится некоторым движением пространства в $X'_2, \ldots, X_n$ переводится некоторым движением пространства в X'_n. Иными словами, шар B можно разрезать на конечное число частей, из которых можно сложить B'.

4. Мощность множества

A. Мощности конечных множеств.

2.103. Определение. *Мощностью* конечного множества A называется натуральное число, равное количеству элементов этого множества, и обозначаемое $|A|$, $\operatorname{card} A$, $\#A$ (мы используем первое из этих обозначений). Конечное множество A мощности n для краткости будем называть *n-множеством*.

2.104. Предложение. *Мощность декартова произведения конечных множеств A и B равна произведению мощностей этих множеств*:

$$|A \times B| = |A| \cdot |B|.$$

Доказательство. Рассмотрим множества $A = \{a_1, \ldots, a_m\}$, $B = \{b_1, \ldots, b_n\}$. Предложение 2.104 становится очевидным, если элементы множества $A \times B$ записать в таблицу вида

	b_1	b_2	$\ldots$	b_n
a_1	(a_1, b_1)	(a_1, b_2)	$\ldots$	(a_1, b_n)
a_2	(a_2, b_1)	(a_2, b_2)	$\ldots$	(a_2, b_n)
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$
a_m	(a_m, b_1)	(a_m, b_2)	$\ldots$	(a_m, b_n)

□

2.105. Для декартова произведения нескольких множеств результат аналогичен:

$$\bigl|X_1 \times \cdots \times X_s\bigr| = \bigl|X_1\bigr| \cdot \ldots \cdot \bigl|X_s\bigr|.$$

2.106. Предложение. *Пусть A — конечное множество, $|A| = n$. Мощность булеана $\mathcal{P}(A)$ множества A (т.е. количество всех различных подмножеств множества A) равна 2^n.*

Доказательство. Найдем число подмножеств множества $A = \{1, 2, \ldots, n\}$. Закодируем каждое подмножество $X \subset A$ конечной n-членной последовательностью Y, состоящей из нулей и единиц, поставив в соответствие подмножеству X последовательность Y, на i-м месте которой стоит единица тогда и только тогда, когда $i \in X$. Например, при $n = 3$ имеем

X	$\{\varnothing\}$	$\{1\}$	$\{2\}$	$\{3\}$	$\{1,2\}$	$\{1,3\}$	$\{2,3\}$	$\{1,2,3\}$
Y	000	100	010	001	110	101	011	111

Очевидно, построенное отображение $f\colon X \mapsto Y$ взаимно однозначно. Но каждая упорядоченная последовательность длины n, состоящая из нулей и единиц, является элементом декартовой степени $\{0,1\}^n$ двухэлементного множества $\{0,1\}$, так что $|\{0,1\}^n| = |\{0,1\}|^n = 2^n$. Таким образом, если A — конечное множество, то множество всех его подмножеств состоит из $2^{|A|}$ элементов; этот факт объясняет, почему множество $\mathcal{P}(A)$ всех подмножеств множества A обозначается также символом 2^A (даже в случае, когда A — бесконечное множество). □

2.107. Предложение. *Мощность объединения двух конечных множеств может быть найдена при помощи следующих формул:*

(а) *если множества A и B не пересекаются, то*

$$|A \sqcup B| = |A| + |B|;$$

(б) *если множества A и B пересекаются, то*

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

Доказательство. Формула для непересекающихся множеств очевидна; более того, легко видеть (и доказать методом математической индукции), что для нескольких непересекающихся множеств справедлива формула

$$\left|\bigsqcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i|.$$

Для двух пересекающихся множеств в сумме $|A| + |B|$ элементы пересечения $A \cap B$ учтены дважды, и чтобы компенсировать это, нужно вычесть $|A \cap B|$ в правой части формулы. Более формальное рассуждение:

$$A \cup B = \big(A \setminus B\big) \sqcup \big(B \setminus A\big) \sqcup \big(A \cap B\big).$$

Обозначив $|A \cap B| = q$, $|A| = a$, $|B| = b$, находим $|A \setminus B| = a - q$, $|B \setminus A| = b - q$, так что

$$|A \cup B| = |A \setminus B| + |B \setminus A| + |A \cap B| = (a-q)+(b-q)+q = a+b-q. \quad \square$$

Формула для мощности объединения может быть обобщена на случай произвольного конечного числа множеств.

2.108. Определение. Пусть X — произвольное множество, $A \subset X$ — его подмножество. *Индикатором* (индикаторной функцией) подмножества A называется функция $\chi[A] : X \to \{0, 1\}$, определённая формулой

$$\chi[A](x) = \begin{cases} 1, & x \in A, \\ 0, & x \notin A. \end{cases}$$

2.109. Предложение. *Индикаторная функция $\chi[A] : X \to X$ множества $A \subset X$ обладает следующими свойствами*:

(а) $\chi[A'] = 1 - \chi[A]$, *где A' — дополнение подмножества A в множестве X*;

(б) $\chi[A \cap B] = \chi[A] \cdot \chi[B]$; *для нескольких множеств $A_1, \ldots, A_n$*

$$\chi\left[\bigcap_{k=1}^{n} A_k\right] = \prod_{k=1}^{n} \chi[A_k];$$

(в) $|A| = \sum\limits_{x \in X} \chi[A](x)$.

Доказательство.

(а) $\big\{x \in A \;\Leftrightarrow\; \chi[A](x) = 1\big\} \;\Leftrightarrow\; \big\{x \notin A' \;\Leftrightarrow\; \chi[A'](x) = 0\big\}$;

(б) $\chi[A \cap B](x) = 1 \;\Leftrightarrow$

$$\Leftrightarrow\; \big\{x \in A \Leftrightarrow \chi[A](x) = 1\big\} \wedge \big\{x \in B \Leftrightarrow \chi[B](x) = 1\big\}.$$

В случае нескольких множеств доказательство производится индукцией с использованием равенства

$$A_1 \cap \cdots \cap A_{k-1} \cap A_k = (A_1 \cap \cdots \cap A_{k-1}) \cap A_k;$$

(см. предложение 2.29). Утверждение (в) очевидно. $\square$

2.110. Теорема (формула включений-исключений)**.** *Если* A_i, $i = 1, \ldots, n$, *— конечные множества, то*

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_i |A_i| - \sum_{i<j} |A_i \cap A_j| + \\ + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n-1} |A_1 \cap A_2 \cap \ldots \cap A_n|.$$

Доказательство. В частном случае двух множеств имеем

$$\chi[A \cup B] = 1 - \chi[A' \cap B'] = 1 - \big(1 - \chi[A]\big)\big(1 - \chi[B]\big) = \\ = \chi[A] + \chi[B] - \chi[A]\chi[B]$$

(ср. с приведённым выше доказательством). В общем случае, поскольку

$$\bigcup_{i=1}^{n} A_i = \left(\bigcap_{i=1}^{n} A_i'\right)',$$

имеем

$$\chi\left[\bigcup_{i=1}^{n} A_i\right] = 1 - \chi\left[\bigcap_{i=1}^{n} A_i'\right] = 1 - \prod_{i=1}^{n}\Big(1 - \chi\big[A_i\big]\Big) = \\ = \sum_i \chi\big[A_i\big] - \sum_{i<j} \chi\big[A_i \cap A_j\big] + \sum_{i<j<k} \chi\big[A_i \cap A_j \cap A_k\big] - \cdots + \\ + (-1)^{n-1} \chi\big[A_1 \cap A_2 \cap \ldots \cap A_n\big],$$

откуда и вытекает требуемая формула. □

Б. Равномощные множества.

2.111. Определение. Два множества A и B называются *равномощными*, если между этими множествами существует взаимно однозначное соответствие (биекция) $f\colon A \to B$. Факт равномощности множеств A и B обозначается $|A| = |B|$, $\operatorname{card} A = \operatorname{card} B$ или $A \sim B$.

2.112. Очевидно, два конечных множества A и B равномощны тогда и только тогда, когда они состоят из одинакового числа элементов.

2.113. Предложение. *Отношение равномощности множеств обладает всеми свойствами отношения эквивалентности: оно рефлексивно, симметрично и транзитивно.*

2.114. Мы сознательно избегаем говорить, что отношение равномощности *является* отношением эквивалентности, чтобы не пришлось указывать, на каком множестве задано это отношение; как показывает парадокс Расселла (см. п. 2.5, с. 28), о «множестве всех множеств» говорить нельзя, а конкретизировать класс всех множеств, которые допустимо рассматривать, в рамках наивной теории множеств невозможно.

Доказательство. Рефлексивность: каждое множество равномощно самому себе, поскольку в качестве взаимно однозначного отображения, о котором идёт речь в определении 2.111, можно взять тождественное отображение $\mathrm{id}_A : A \to A$. *Симметричность* вытекает из того, что каждая биекция обратима, а *транзитивность* — из того факта, что композиция биекций также биективна (см. утверждения **??** и **??** теоремы **??**, с. **??**). □

В. Бесконечные множества.

2.115. Определение. Множество A называется *бесконечным*, если в нём существует собственное подмножество $B \subset A$ (т.е. $B \neq A$), равномощное множеству A. Множество, не являющееся бесконечным, называется *конечным*.

2.116. В рамках аксиоматики Цермело—Френкеля существование бесконечных множеств гарантируется аксиомой бесконечности (см. п. **??**, с. **??**).

2.117. Простейший пример бесконечного множества — множество натуральных чисел $\mathbb{N} = \{1, 2, 3, \dots\}$, равномощное, например, своему собственному подмножеству $2\mathbb{N} = \{2, 4, 6, \dots\}$, состоящему из чётных чисел. Биекция $f\colon \mathbb{N} \to 2\mathbb{N}$ задаётся формулой $n \mapsto 2n$, а обратное отображение $f^{-1}\colon 2\mathbb{N} \to \mathbb{N}$ — формулой $m \mapsto m/2$.

Г. Счётные множества.

2.118. Поскольку известно, что мощности конечных множеств могут быть различными, возникает вопрос, существуют ли бесконечные множества, не являющиеся равномощными.

2.119. Определение. Множество называется *счётным*, если оно равномощно множеству $\mathbb{N}$ натуральных чисел. Неформально говоря, множество счётно, если его элементы можно перенумеровать, т.е. представить множество в виде бесконечной последовательности $\{x_1, x_2, \dots\}$ (см. определение 2.95, с. 55).

2.120. Теорема (свойства счётных множеств)**.**

1. *Любое подмножество счётного множества конечно или счётно.*
2. *Любое бесконечное множество содержит счётное подмножество* (в этом смысле счётные множества являются «наименьшими» бесконечными множествами).
3. *Объединение конечного или счётного числа конечных или счётных множеств является конечным или счётным множеством.*
4. *Прямое произведение конечного числа счётных множеств счётно.*

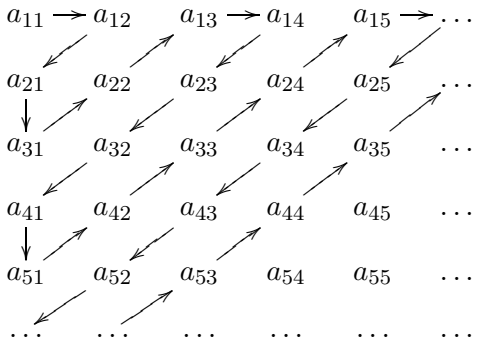
Доказательство. 1. Пусть множество B является подмножеством счётного множества $A = \{a_1, a_2, \dots\}$. Удалим из последовательности $a_1, a_2, \dots$ те элементы, которые не принадлежат B, сохраняя порядок оставшихся элементов. Тогда оставшиеся элементы образуют либо конечную последовательность (и тогда B конечно), либо бесконечную (и тогда B счётно).

2. Пусть A — произвольное бесконечное множество. Выберем какой-либо элемент b_1. Так как множество A бесконечно, то множество $A \setminus \{b_1\}$ также бесконечно; из него выберем элемент b_2 и отметим, что множество $A \setminus \{b_1, b_2\}$ бесконечно. Продолжая процесс, построим бесконечную последовательность $b_1, b_2, \dots$; построение не прервется ни на каком шаге, поскольку A бесконечно. Множество $B = \{b_1, b_2, \dots\}$ и является искомым счётным подмножеством.

3. Пусть имеется счётное число счётных множеств

$$A_1 = \{a_{11}, a_{12}, \dots\}, \quad A_2 = \{a_{21}, a_{22}, \dots\}, \quad \dots.$$

Расположив элементы каждого из них слева направо в последовательность и записав последовательности одну под другой, получим бесконечную таблицу



элементы которой можно записать в виде последовательности

$$a_{11},\ a_{12},\ a_{21},\ a_{31},\ a_{22},\ a_{13},\ a_{14},\ a_{23},\ a_{32},\ a_{41},\ \dots.$$

Если множества A_i не пересекались, то искомое представление для их объединения получено, если пересекались — в построенной последовательности нужно удалить повторения, оставив только один из повторяющихся элементов. Если множеств конечное число или какие-либо из множеств конечны, то в описанной конструкции части членов не будет, и останется либо конечное, либо счётное множество.

4. Пусть $A = \{a_1, a_2, \dots\}$ — счётное множество; докажем по индукции, что A^n счётно. База индукции: $A^1 = A$ — счётное множество. Переход от $n = 1$ к $n = 2$: множество $A^2 = A \times A$ разбивается на счётное число непересекающихся счётных множеств $\{a_1\} \times A$, $\{a_2\} \times A$, … (элементами i-го множества являются пары, первый член которых равен a_i), поэтому A^2 — счётное множество. Аналогично выполняется индукционный переход в общем случае: если известно, что A^n счётно, то $A^{n+1} = A \times A^n$ разбивается на счётное число непересекающихся счётных множеств $\{a_1\} \times A^n$, $\{a_2\} \times A^n$ и т. д. и потому также счётно. □

2.121. Примеры.

1. Множество $\mathbb{Z}$ целых чисел счётно, так как его элементы можно расположить в последовательность $0, 1, -1, 2, -2, \dots$.
2. Множество $\mathbb{Q}$ рациональных чисел счётно. Рациональные числа представляются несократимыми дробями с целыми числителем и знаменателем. Множество дробей с данным знаменателем счётно, поэтому $\mathbb{Q}$ представимо в виде объединения счётного числа счётных множеств.
3. Множества $\mathbb{N}^k$, $\mathbb{Z}^k$, $\mathbb{Q}^k$, состоящие из всех конечных последовательностей натуральных, целых или рациональных чисел соответственно, счётны.
4. Число называется *алгебраическим*, если оно является корнем ненулевого многочлена с целыми коэффициентами. Множество алгебраических чисел счётно, поскольку многочлен задаётся конечной последовательностью своих коэффициентов (целых чисел), а каждый многочлен имеет конечное число корней.

2.122. Предложение. *Если множество A бесконечно, а множество B конечно или счётно, то $A \cup B \sim A$.*

Доказательство. Без ограничения общности можно считать, что $B \cap A = \varnothing$, т.е. рассматривать дизъюнктное объединение $A \sqcup B$ (в противном случае вместо B рассмотрим множество $B \setminus A$, которое конечно либо счётно; ясно, что $A \cup B = A \sqcup (B \setminus A)$). Выделим в A счётное подмножество P и положим $Q = A \setminus P$; тогда $A = P \sqcup Q$.

Нужно доказать, что

$$A \sqcup B = P \sqcup Q \sqcup B \sim P \sqcup Q = A.$$

Поскольку $P \sqcup B$ и P оба счётны, между ними существует биекция $f\colon P \sqcup B \to P$. Рассмотрим отображение

$$g\colon P \sqcup Q \sqcup B \to P \sqcup Q, \quad x \mapsto \begin{cases} f(x) \in P, & \text{если } x \in P \sqcup B, \\ x \in Q, & \text{если } x \in Q. \end{cases}$$

Очевидно, это отображение биективно. □

Д. Несчётные множества.

2.123. Предложение. *Множество*[1] $2^{\mathbb{N}}$*, элементами которого являются бесконечные последовательности, состоящие из нулей и единиц, не является счётным.*

Доказательство. Предположим, что множество $2^{\mathbb{N}}$ счётно; тогда все последовательности нулей и единиц можно перенумеровать: $\alpha_1, \alpha_2, \ldots$. Составим бесконечную таблицу, строками которой являются наши последовательности:

$$\begin{aligned} \alpha_1 &= \underline{\alpha_{11}}\ \alpha_{12}\ \alpha_{13}\ \ldots \\ \alpha_2 &= \alpha_{21}\ \underline{\alpha_{22}}\ \alpha_{23}\ \ldots \\ \alpha_3 &= \alpha_{31}\ \alpha_{32}\ \underline{\alpha_{33}}\ \ldots \\ &\vdots \end{aligned}$$

(через α_{ij} обозначен j-й член i-й последовательности). Рассмотрим теперь последовательность, образованную стоящими на диагонали членами α_{11}, α_{22}, …; её i-й член равен α_{ii} и совпадает с i-м членом i-й последовательности. Заменив все члены этой последовательности на противоположные (т.е. нули на единицы и наоборот), получим последовательность β, у которой $\beta_i = 1 - \alpha_{ii}$, так что последовательность β отличается от любой из последовательностей α_i (в позиции i) и потому отсутствует в таблице. Но мы предположили, что таблица включает в себя все последовательности; полученное противоречие доказывает наше утверждение. □

[1] Обозначение этого множества объясняется следующим образом. Символом Y^X принято обозначать множество всех отображений $f\colon X \to Y$. Согласно этой нотации $\{0,1\}^{\mathbb{N}}$ — это множество отображений $f\colon \mathbb{N} \to \{0,1\}$, ставящих в соответствие каждому натуральному числу нуль или единицу, т.е. бесконечных последовательностей, состоящих из нулей и единиц. Для упрощения записи вместо $\{0,1\}^{\mathbb{N}}$ пишем $2^{\mathbb{N}}$ (число 2 — это мощность множества $\{0,1\}$).

2.124. Предложение. *Числовой отрезок* $[0,1]$*, множество* $2^{\mathbb{N}}$ *и множество* $\mathcal{P}(\mathbb{N})$ *всех подмножеств натурального ряда равномощны и несчётны*:

$$[0,1] \sim 2^{\mathbb{N}} \sim \mathcal{P}(\mathbb{N}).$$

Доказательство. Докажем, что $[0,1] \sim 2^{\mathbb{N}}$. Каждое число $x \in [0,1]$ записывается в виде последовательности нулей и единиц, построенной следующим образом: первый элемент равен 0 или 1 в зависимости от того, попадает ли число x в левую или правую половину отрезка; чтобы определить следующий знак, нужно выбранную половину снова поделить пополам и посмотреть, куда попадёт x и т. д. Обратное соответствие устроено так: последовательности $x_0x_1x_2\ldots$ соответствует число, являющееся суммой бесконечной геометрической прогрессии

$$\frac{x_0}{2} + \frac{x_1}{2^2} + \frac{x_2}{2^3} + \ldots.$$

Описанное соответствие пока не является биективным: двоично-рациональные числа, т.е. дроби вида $m/2^n$, имеют два представления. Например, числу $3/8$ отвечают последовательности $011000\ldots$ и $010111\ldots$. Соответствие станет взаимно однозначным, если отбросить все последовательности «с единицей в периоде», кроме последовательности $1111\ldots$, изображающей единицу. Но таких последовательностей счётное число, поэтому на мощность это не повлияет. Итак, $[0,1] \sim 2^{\mathbb{N}}$.

Докажем, что $2^{\mathbb{N}} \sim \mathcal{P}(\mathbb{N})$. Поставим в соответствие каждой последовательности из $2^{\mathbb{N}}$ (т.е. каждому отображению $f\colon \mathbb{N} \to \{0,1\}$) множество номеров мест, на которых стоят единицы. Например, последовательности, состоящей из одних нулей, соответствует пустое множество, последовательности, состоящей из одних единиц — весь натуральный ряд, а последовательности $101010\ldots$ — множество нечётных чисел. Полученное соответствие является взаимно однозначным. □

2.125. Несчётное множество вещественных чисел не может совпадать со счётным множеством алгебраических чисел; следовательно, существует вещественное число, не являющееся алгебраическим (т.е. не являющееся корнем никакого ненулевого многочлена с целыми коэффициентами). Такие числа называются *трансцендентными*. Отметим, что широко используемые в математике числа π и e являются трансцендентными.

Е. Теорема Кантора и сравнение мощностей.

2.126. Теорема (теорема Кантора)**.** *Никакое множество X не равномощно множеству $\mathcal{P}(X) \equiv 2^X$ всех своих подмножеств.*

Доказательство. Предположим обратное, т.е. пусть $f\colon X \to 2^X$ — биекция. Рассмотрим множество

$$Z = \{x \in X \mid x \notin f(x)\} \subset X,$$

т.е. множество тех элементов $x \in X$, которые не принадлежат соответствующему им подмножеству. Докажем, что подмножеству Z не соответствует ни один элемент множества X. Если это не так, т.е. существует такой $z \in X$, что $Z = f(z)$, то $z \in Z \;\Leftrightarrow\; z \notin f(z)$ по построению множества Z и $z \notin f(z) \;\Leftrightarrow\; z \notin Z$ по предположению $f(z) = Z$. Полученное противоречие показывает, что Z не соответствует ни одному элементу множества X, т.е. отображение f не биективно. □

Ж. Сравнение мощностей. Определение равномощности уточняет интуитивную идею о множествах «одинакового размера». Дадим формальное определение ситуации, когда одно множество «больше» другого.

2.127. Определение. Будем говорить, что мощность множества A не больше мощности множества B (обозначение $A \preccurlyeq B$), если A равномощно некоторому подмножеству множества B (возможно, самому B).[1]

2.128. Теорема (теорема Кантора—Бернштейна[2])**.** *Если множество A равномощно некоторому подмножеству множества B, а B равномощно некоторому подмножеству множества A, то множества A и B равномощны.*

Заинтересованный читатель может найти доказательство этой теоремы в специальной литературе, посвящённой теории множеств.

2.129. Теорема Кантора—Бернштейна значительно упрощает доказательства равномощности. Например, для доказательства равномощности куба и шара в пространстве достаточно заметить, что из куба можно вырезать маленький шар (гомотетичный, а следовательно, равномощный большому), а из шара — маленький кубик.

2.130. Вернёмся к вопросу о сравнении мощностей. Для данных множеств A и B теоретически имеются четыре возможности:

[1] Мы сознательно отказываемся от записи $|A| \leqslant |B|$, чтобы избежать ненужной аллюзии со сравнением чисел.

[2] Феликс Бернштейн (Felix Bernstein; 1878–1956) — немецкий математик.

(i) A равномощно некоторой части B, а B равномощно некоторой части A; в этом случае множества равномощны;
(ii) A равномощно некоторой части B, но B не равномощно никакой части A; в этом случае говорят, что A *имеет меньшую мощность, чем* B;
(iii) B равномощно некоторой части A, но A не равномощно никакой части B; в этом случае говорят, что A *имеет большую мощность, чем* B;
(iv) ни A не равномощно никакой части B, ни B не равномощно никакой части A. Этот случай на самом деле невозможен, но доказательство этого факта выходит за рамки данной книги.

3. Континуум-гипотеза.

2.131. Мощность счётного множества обозначается символом[1] $\aleph_0$. Мощность континуума $\mathfrak{c}$ — это мощность множества вещественных чисел $\mathbb{R}$ (а также мощность равномощных ему множеств, например, $2^{\mathbb{N}}$). В силу того, что $\mathbb{R} \sim 2^{\mathbb{N}}$, мощность континуума обозначают также $2^{\aleph_0}$.

2.132. Возникает естественный вопрос: каков смысл индекса 0 в $\aleph_0$? Что такое, например, $\aleph_1$? Обычно $\aleph_1$ обозначает наименьшую несчётную мощность (можно доказать, что таковая существует). *Континуум-гипотеза* утверждает, что $\mathfrak{c} = \aleph_1$.

2.133. Континуум-гипотеза была высказана Г. Кантором в начале 80-х гг. XIX в. Многочисленные попытки самого Кантора и многих математиков конца XIX — начала XX вв. доказать континуум-гипотезу оказались безуспешными. Сложившаяся ситуация привела многих математиков к убеждению, что континуум-гипотеза не может быть решена традиционными средствами теории множеств. Это убеждение было подтверждено методами математической логики и аксиоматической теории множеств. В 1936 г. К. Гёдель доказал, что континуум-гипотеза не может быть опровергнута в рамках аксиоматической теории Цермело—Френкеля, а в 1963 г. П. Коэн[2] доказал, что и отрицание континуум-гипотезы совместно с этой теорией, так что континуум-гипотезу невозможно доказать с помощью обычных методов теории множеств. Полученные результаты свидетельствуют о том, что на современном этапе развития теории

[1] $\aleph$ — первая буква еврейского алфавита; читается «а́леф».

[2] Пол Джозеф Коэн (Paul Joseph Cohen; 1934–2007) — американский математик.

множеств возможны различные подходы к основаниям этой науки, существенно различным образом отвечающие на естественные проблемы, возникающие в теории множеств.

5. Упражнения и задачи

2.1. Пусть $f\colon X \to Y$ — отображение, A и B — подмножества множества X. Докажите следующие соотношения:
(а) $(A \subset B) \Rightarrow (f(A) \subset f(B)) \not\Rightarrow (A \subset B)$;
(б) $(A \neq \varnothing) \Rightarrow (f(A) \neq \varnothing)$;
(в) $f(A \cap B) \subset f(A) \cap f(B)$;
(г) $f(A \cup B) = f(A) \cup f(B)$.

2.2. Пусть $f\colon X \to Y$ — отображение, A' и B' — подмножества множества Y. Докажите следующие соотношения:
(а) $(A' \subset B') \Rightarrow (f^{-1}(A') \subset f^{-1}(B'))$;
(б) $f^{-1}(A' \cap B') \subset f^{-1}(A') \cap f^{-1}(B')$;
(в) $f^{-1}(A' \cup B') = f^{-1}(A') \cup f^{-1}(B')$.

2.3. Докажите, что отображение $f\colon X \to Y$ сюръективно в том и только том случае, если

$$\forall B' \subset Y: \quad f(f^{-1}(B')) = B'.$$

2.4. Докажите, что отображение $f\colon X \to Y$ биективно в том и только том случае, если для

$$\forall A \subset X,\ \forall B' \subset Y: \quad \big(f^{-1}(f(A)) = A\big) \wedge \big(f(f^{-1}(B') = B')\big).$$

2.5. Докажите, что следующие утверждения относительно отображения $f\colon X \to Y$ эквивалентны:
(а) f инъективно;
(б) $\forall A \subset X\colon f^{-1}(f(A)) = A$;
(в) $\forall A \subset X, \forall B \subset X\colon f(A \cap B) = f(A) \cap f(B)$;
(г) $f(A) \cap f(B) = \varnothing \ \Leftrightarrow\ A \cap B = \varnothing$;
(д) если $X \supset A \supset B$, то $f(A \setminus B) = f(A) \setminus f(B)$.

2.6. (а) Докажите, что для любого отображения $f\colon X \to Y$ отображение $F\colon X \to X \times Y$, заданное правилом $x \overset{F}{\longmapsto} (x, f(x))$, является инъективным.
(б) Частица движется равномерно по окружности Y. Пусть X — ось времени и $x \overset{F}{\longmapsto} y$ — соответствие между моментом времени x и положением $y = f(x) \in Y$ частицы. Изобразите график функции $f\colon X \to Y$ в декартовом произведении $X \times Y$.

ГЛАВА 3

Алгебраические системы

КАЖДОЕ множество может быть снабжено некоторыми отношениями и операциями; например, на множестве вещественных чисел имеется отношение строгого порядка $<$, отношение равенства $=$, операции сложения $+$ и умножения $\cdot$ чисел и т. д. Множества с введёнными на них дополнительными математическими структурами называют *алгебраическими системами*. В этой главе кратко представлены простейшие и в то же время наиболее важные типы алгебраических систем.

1. Операции на множестве

Под *операцией* на множестве понимается отображение, которое одному или нескольким элементам множества (аргументам, или операндам) ставит в соответствие другой элемент (значение).

3.1. Определение. n-арная операция на множестве X — это отображение прямого произведения n экземпляров множества X в само множество X, т.е. $G^n \to G$. По определению, 0-арная (нуль-арная) операция — это просто выделенный элемент множества. Чаще всего рассматриваются 1-арные (унарные) и 2-арные (бинарные) операции.

Каждая операция обладает определёнными свойствами, характеризующими её и определяющими взаимоотношения этой операции с другими отображениями рассматриваемого множества.

A. Унарные операции.

3.2. Определение. *Унарная операция* на множестве X — это отображение $f\colon X \to X$. Для обозначения унарной операции часто используется *префиксная* форма записи, при которой знак операции ставится перед элементом, к которому она применяется.

3.3. Определение. Унарная операция $f\colon X \to X$ на множестве X называется *инволютивной* (*инволюцией*), если $f\bigl(f(x)\bigr) = x$ для

любого $x \in X$. Иными словами, инволюция является отображением, которое обратно самому себе: $f = f^{-1}$. Часто дополнительно предполагают, что инволюция не является тождественным отображением.

3.4. Пример. Примерами унарных операций могут служить операция изменения знака числа $x \mapsto (-x)$, комплексное сопряжение $z \mapsto \bar{z}$, переход от множества к его дополнению $X \mapsto \complement X$, логическое отрицание высказывания $A \mapsto \neg A$, преобразование подобия в геометрии и т. п. Все приведённые примеры, кроме последнего, представляют инволютивные унарные операции.

3.5. Предложение. *Любая инволюция f на множестве X является биективным отображением.*

Доказательство. 1. Докажем инъективность. Пусть $f(x_1) = f(x_2)$; тогда $f\big(f(x_1)\big) = f\big(f(x_2)\big)$, т.е. $x_1 = x_2$.

2. Докажем сюръективность. Требуется для любого $y \in X$ найти такой $x \in X$, что $y = f(x)$. Поскольку $f(y) = f\big(f(x)\big) = x$, элемент $x = f(y)$ является искомым. □

3.6. Предложение. *Композиция двух инволюций f и g на множестве X является инволюцией тогда и только тогда, когда они коммутируют*: $f \circ g = g \circ f$.

Доказательство. Если $f \circ g$ — инволюция, т.е. $(f \circ g)^{-1} = f \circ g$, то

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

Наоборот, если инволюции f и g коммутируют, $f \circ g = g \circ f$, то

$$(f \circ g)^{-}1 = g^{-1} \circ f^{-1} = g \circ f = f \circ g. \qquad \square$$

Б. Бинарные операции.

3.7. Определение. *Бинарной операцией* f на множестве X называется отображение $f\colon X \times X \to X$, которое ставит в соответствие упорядоченной паре $(x, y) \in X \times X$ некоторый элемент $z = f(x, y)$ множества X. Для обозначения бинарной операции вместо записи $f(x, y)$ используется, как правило, *инфиксная* запись с помощью специальных знаков операций; при такой форме записи знак операции ставится *между* элементами, к которым применяется эта операция, например, $x + y$ для сложения чисел или $x \cdot y$ для умножения.

3.8. Определение. Бинарная операция $*\colon X \times X \to X$ на множестве X называется *коммутативной*, если

$$\forall x, y \in X : \quad x * y = y * x.$$

3.9. Примеры.

1. Сложение и умножение вещественных чисел коммутативны:
$$a + b = b + a, \quad a \cdot b = b \cdot a.$$
2. Логические операции конъюнкция и дизъюнкция на множестве высказываний коммутативны:
$$A \wedge B \equiv B \wedge A, \quad A \vee B \equiv B \vee A.$$
3. Объединение и пересечение множеств коммутативны:
$$A \cup B = B \cup A, \quad A \cap B = B \cap A.$$
4. Вычитание, деление и возведение в степень вещественных чисел коммутативными не являются:
$$a - b \neq b - a, \quad \frac{a}{b} \neq \frac{b}{a}, \quad a^b \neq b^a.$$

3.10. Определение. Бинарная операция $*\colon X \times X \to X$ на множестве X называется *ассоциативной*, если

$$\forall x, y, z \in X : \quad (x * y) * z = x * (y * z).$$

3.11. Примеры.

1. Сложение и умножение вещественных чисел ассоциативны:
$$(a + b) + c = a + (b + c), \quad (a \cdot b) \cdot c = a \cdot (b \cdot c).$$
2. Логические операции конъюнкция и дизъюнкция на множестве высказываний ассоциативны:
$$(A \wedge B) \wedge C \equiv A \wedge (B \wedge C), \quad (A \vee B) \vee C \equiv A \vee (B \vee C).$$
3. Объединение и пересечение множеств ассоциативны:
$$(A \cup B) \cup C = A \cup (B \cup C), \quad (A \cap B) \cap C = A \cap (B \cap C).$$
4. Операция композиции отображений ассоциативна (см. теорему 2.76, с. 48):
$$(h \circ g) \circ f = h \circ (g \circ f)$$
для любых отображений $f\colon X \to Y$, $g\colon y \to Z$, $h\colon Z \to W$.
5. Вычитание вещественных чисел не обладает свойством ассоциативности: $(a - b) - c \neq a - (b - c)$.

3.12. Ассоциативность и коммутативность бинарной операции — независимые свойства. Примеры операций, одновременно ассоциативных и коммутативных, читателю хорошо известны. Операция $*$ на $\mathbb{Z}$, заданная правилом $n*m \stackrel{\text{def}}{=\!=} -n-m$, очевидно, коммутативна, но ассоциативной не является:

$$(n*m)*l = (-n-m)*l = -(-n-m)-l = n+m-l,$$
$$n*(m*l) = -n-(m*l) = -n-(-m-l) = -n+m+l.$$

Примером ассоциативной, но не коммутативной операции может служить композиция отображений.

3.13. Пусть X — множество с заданной на нём бинарной операцией $*$, которую будем для определённости называть умножением и для краткости опускать знак операции, т.е. писать xy вместо $x*y$. Можно различными способами составлять различные произведения, состоящие из n сомножителей, не меняя их порядка:

(i) при $n=2$ такое произведение лишь одно: x_1x_2;
(ii) при $n=3$ имеется два произведения: $(x_1x_2)x_3$ и $x_1(x_2x_3)$;
(iii) при $n=4$ таких произведений уже пять: $((x_1x_2)x_3)x_4$, $(x_1(x_2x_3))x_4$, $x_1((x_2x_3)x_4)$, $x_1(x_2(x_3x_4))$, $(x_1x_2)(x_3x_4)$.

Докажем, что в случае ассоциативной операции все эти произведения совпадают.

3.14. Предложение. *Если бинарная операция на множестве X ассоциативна, то результат её применения к n элементам множества не зависит от расстановки скобок.*

Доказательство. При $n=1$ и $n=2$ доказывать нечего, при $n=3$ утверждение теоремы представляет собой определение ассоциативности. Применим индукцию по n. Предположим, что утверждение доказано для числа перемножаемых элементов $<n$ и докажем его для n сомножителей, т.е. проверим, что

$$(x_1\dots x_k)(x_{k+1}\dots x_n) = (x_1\dots x_l)(x_{l+1}\dots x_n) \tag{3.1}$$

для любых k и l, $1 \leqslant k,l \leqslant n-1$. В последнем равенстве мы выписали лишь внешние пары скобок, поскольку по предположению индукции расстановка внутренних скобок несущественна. Назовём расстановку скобок

$$\Big(\dots\big((x_1x_2)x_3\big)\dots x_{k-1}\Big)x_k$$

левонормированной. Если $k = n-1$, то в силу индуктивного предположения произведение n сомножителей приводится к левонормированному виду:

$$(x_1 \dots x_{n-1})x_n = \Big(\dots \big((x_1x_2)x_3\big) \dots x_{n-1}\Big)x_n.$$

В случае $k < n-1$ ввиду ассоциативности имеем

$$\begin{aligned}(x_1 \dots x_k)(x_{k+1} \dots x_n) &= (x_1 \dots x_k)\big((x_{k+1} \dots x_{n-1})x_n\big) = \\ &= \Big((x_1 \dots x_k)(x_{k+1} \dots x_{n-1})\Big)x_n = \\ &= \Big(\dots \Big(\Big(\dots (x_1x_2) \dots x_k\Big)x_{k+1}\Big) \dots x_{n-1}\Big)x_n,\end{aligned}$$

т.е. снова получили левонормированную расстановку скобок. К такому же виду приводится правая часть равенства (3.1). □

3.15. В случае ассоциативной операции $\cdot$ (иногда для краткости знак операции опускаем) благодаря предложению 3.14 можно рассматривать выражения вида $a_1a_2 \dots a_n$ без скобок и при помощи индукции распространять на них свойства, доказанные для меньшего числа операндов. Например, свойство ассоциативности теоретико-множественных операций $\cap$ и $\cup$ (см. предложение 2.29, с. 33) позволяет рассматривать выражения

$$\bigcap_{k=1}^{n} A_k \stackrel{\text{def}}{=\!=} A_1 \cap A_2 \cap \dots \cap A_n, \quad \bigcup_{k=1}^{n} A_k \stackrel{\text{def}}{=\!=} A_1 \cup A_2 \cup \dots \cup A_n.$$

Законы де Моргана могут быть обобщены на случай любого конечного числа множеств $A_1, \dots, A_n$:

$$\left(\bigcap_{k=1}^{n} A_k\right)' = \bigcup_{k=1}^{n} A'_k, \quad \left(\bigcup_{k=1}^{n} A_k\right)' = \bigcap_{k=1}^{n} A'_k.$$

3.16. Определение. Пусть $\circ$ и $*$ — две бинарные операции, заданные на множестве X. Операция $*$ называется *дистрибутивной* относительно операции $\circ$, если

$$\forall x, y, z \in X \quad (x \circ y) * z = (x * z) \circ (y * z), \quad z * (x \circ y) = (z * x) \circ (z * y).$$

3.17. В случае некоммутативной операции нужно различать дистрибутивность справа (первое из приведённых соотношений) и слева (второе соотношение); если же операция коммутативна, то понятия дистрибутивности слева и справа совпадают.

3.18. Примеры.

1. Умножение вещественных чисел дистрибутивно относительно сложения:
$$(a+b)c = ac + bc, \quad c(a+b) = ca + cb.$$
Здесь опущены некоторые скобки, что возможно благодаря соглашению о приоритете операций: сначала выполняются все умножения, а затем сложения.
2. Логические операции конъюнкция и дизъюнкция взаимно дистрибутивны:
$$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C),$$
$$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C).$$
3. Операции объединения и пересечения множеств взаимно дистрибутивны:
$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C),$$
$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C).$$
4. Сложение вещественных чисел не является дистрибутивным относительно умножения: $(a \cdot b) + c \neq (a + c) \cdot (b + c)$.

B. Нейтральные и обратимые элементы.

3.19. Определение. Пусть $*$ — бинарная операция на множестве X. Элемент $e \in X$ называется *нейтральным* относительно операции $*$, если
$$\forall x \in X \quad e * x = x * e = x.$$

3.20. В случае некоммутативной операции $*$ различают левый нейтральный элемент e_l, определяемый соотношением $e_l * x = x$, и правый нейтральный элемент e_r, определяемый соотношением $x * e_r = x$ для каждого $x \in X$. В нашем курсе рассматриваются только двусторонние (т.е. являющиеся одновременно левыми и правыми) нейтральные элементы.

3.21. Примеры.
1. Нуль 0 является нейтральным элементом относительно сложения чисел, а единица 1 — нейтральным элементом относительно умножения чисел.
2. Ложное высказывание 0 является нейтральным элементом относительно дизъюнкции, а истинное высказывание 1 — нейтральным элементом относительно конъюнкции:
$$A \vee 0 = A, \quad A \wedge 1 = A.$$

3. Пустое множество является нейтральным элементом относительно операции объединения множеств, а универсальное множество (см. п. 2.26, с. 32) — нейтральным элементом относительно операции пересечения:

$$A \cup \varnothing = A, \quad A \cap U = A.$$

3.22. Предложение. *Если двусторонний нейтральный элемент относительно бинарной операции $*$ существует, то он единствен.*

Доказательство. Пусть e и e' — двусторонние нейтральные элементы относительно операции $*$, то есть для любого элемента x

$$e * x = x * e = x, \quad e' * x = x * e' = x.$$

Полагая в первом из этих равенств $x = e'$, а во втором — $x = e$, получим

$$e * e' = e' * e = e', \quad e' * e = e * e' = e.$$

Так как левые части этих равенств равны, то равны и правые: $e' = e$. □

3.23. Определение. Пусть $*$ — бинарная операция на множестве X, обладающая двусторонним нейтральным элементом e. Элемент x' называется *обратным* к элементу $x \in X$ относительно операции $*$, если $x' * x = e = x * x'$. В этом случае элемент x называется *обратимым*, а элементы x и x' — *взаимно обратными*.

3.24. В случае некоммутативной операции различают левый x_l и правый x_r обратные элементы, определяемые соответственно соотношениями $x_l * x = e$ и $x * x_r = e$. В нашем курсе рассматриваются только двусторонние обратные элементы.

3.25. Очевидно, нейтральный элемент e является обратным самому себе.

3.26. Примеры.

1. Относительно сложения вещественных чисел обратным к числу $x \in \mathbb{R}$ является противоположное число $-x$.
2. Относительно умножения вещественных чисел обратным к ненулевому числу $x \in \mathbb{R}$ является число $1/x$; число нуль не имеет обратного относительно умножения.

3.27. Предложение. *Пусть $*$ — ассоциативная операция, x и y — произвольные обратимые элементы, x' и y' — их обратные.*

1. *Обратный элемент x' единствен.*
2. *Элемент $x * y$ обратим; его обратным является $y' * x'$.*
3. *Элемент, обратный к x', также обратим, причём $(x')' = x$.*

Доказательство. 1. Пусть u и v — два элемента, обратных к x относительно операции $*$, т.е.

$$x * u = e = u * x, \quad x * v = e = v * x.$$

В силу ассоциативности операции $*$ имеем

$$u = u * e = u * (x * v) = (u * x) * v = e * v = v.$$

2. В силу ассоциативности $*$ имеем

$$(x*y)*(y'*x') = \big((x*y)*y'\big)*x' = \big(x*(y*y')\big)*x' = (x*e)*x' = x*x' = e.$$

Аналогично доказывается, что $(y' * x') * (x * y) = e$.

3. Пользуясь предыдущим фактом, получаем

$$(x')' * x' = (x * x')' = e' = e. \qquad \square$$

3.28. Предложение. *Пусть $*$ — ассоциативная бинарная операция на множестве X, обладающая нейтральным элементом e. Тогда для любого обратимого элемента $a \in X$ каждое из уравнений $a * x = b$ и $x * a = b$ имеет единственное решение, причём*

$$a * x = b \quad \Rightarrow \quad x = a' * b,$$
$$x * a = b \quad \Rightarrow \quad x = b * a',$$

где a' — элемент, обратный к a.

Доказательство. Имеем

$$a * x = b \;\Rightarrow\; a' * (a * x) = a' * b \;\Rightarrow\; (a' * a) * x = a' * b \;\Rightarrow$$
$$\Rightarrow\; e * x = a' * b \quad \Rightarrow \quad x = a' * b.$$

Единственность решения следует из однозначности выражающей его формулы. Для уравнения $x * a = b$ доказательство аналогично. $\square$

Г. Подмножество, замкнутое относительно бинарной операции.

3.29. Пусть $*$ — бинарная операция на множестве X. Подмножество $Y \subset X$ называется *замкнутым* относительно операции $*$, если

$$\forall x, y \in Y \quad x * y \in Y.$$

3.30. Примеры.

1. Подмножество в $\mathbb{Z}$, состоящее из всех чётных чисел, замкнуто относительно операций сложения и умножения целых чисел.
2. Подмножество в $\mathbb{Z}$, состоящее из всех нечётных чисел, замкнуто относительно операции умножения целых чисел, но не замкнуто относительно операции сложения.

Д. Бинарная операция, согласованная с отношением эквивалентности. Пусть на множестве X заданы одновременно бинарная операция $*$ и отношение эквивалентности $\sim$. Напомним, что отношение эквивалентности определяет разбиение множества X на непересекающиеся классы эквивалентных элементов, а множество полученных классов называется фактор-множеством множества X по отношению $\sim$ и обозначается $X/\sim$ (см. теорему 2.59, с. 43).

3.31. Определение. Бинарная операция $*$ и отношение $\sim$ на множестве X называются *согласованными*, если

$$\forall x, x', y, y' \in X \quad (x \sim x') \wedge (y \sim y') \;\Rightarrow\; x * y \sim x' * y'.$$

В этом случае на фактор-множестве $X/\sim$ можно определить бинарную операцию, которую будем обозначать тем же символом $*$, по правилу

$$[x] * [y] = [x * y].$$

Для того чтобы найти результат применения операции $*$ к классам $[x]$ и $[y]$, нужно в каждом из них взять по произвольному представителю, например, $x \in [x]$ и $y \in [y]$, найти $x * y$ и объявить результатом класс $[x * y]$, содержащий результат вычисления. Тот факт, что полученный класс не зависит от выбора представителей, обеспечивается согласованностью операции $*$ и отношения эквивалентности $\sim$.

3.32. Все свойства операции $*$ на множестве X, имеющие характер тождеств, например, коммутативность, ассоциативность, наличие нейтрального элемента и обратного элемента, наследуются операцией на фактор-множестве. Например, если операция на X — сложение, обладающее нейтральным элементом — нулём 0, то класс эквивалентности $[0]$ является нейтральным элементом (нулём) в $X/\sim$; если $(-x)$ — элемент, противоположный элементу $x \in X$, то класс $[-x]$ является элементом фактор-множества $X/\sim$, противоположным элементу $[x]$.

Е. Внешние бинарные операции.

3.33. *Внешняя бинарная операция* на паре множеств A и B, принимающая значения в множестве C, — это отображение

$$F : A \times B \to C, \quad (a, b) \mapsto c = F(a, b).$$

Для внешних бинарных операций также часто используется инфиксная форма записи: вместо $F(a, b)$ записывают нечто вроде $a * b$ или $b \circ a$. В таком контексте бинарные операции вида $A \times A \to A$ называют *внутренними*.

3.34. Поскольку операнды внешней бинарной операции разнородны (т.е. принадлежат разным множествам), вопрос о коммутативности бессмыслен, а запись операции в виде $a * b$ или $b \circ a$ определяется сложившейся традицией или соображениями удобства. Так, для операции умножения вектора на число допустимы оба варианта: записи $\alpha\boldsymbol{a} = \boldsymbol{a}\alpha$.

3.35. Если на множествах A и/или B введены внутренние бинарные операции, то правомерен вопрос об их взаимоотношениях с внешними операциями. Так, операция умножения числа и вектора обладает свойством $(\alpha\beta)\boldsymbol{x} = \alpha(\beta\boldsymbol{x})$, напоминающим закон ассоциативности; впрочем, сходство исчезает, если явно указать знаки операций: если $\cdot$ — операция умножения вещественных чисел (внутренняя), $*$ — операция умножения числа на вектор внешняя, то приведённое равенство принимает вид $(\alpha \cdot \beta) * \boldsymbol{x} = \alpha * (\beta * \boldsymbol{x})$, в левой и правой частях которого наборы операций разные. По этой причине использовать термин «ассоциативность» в этой ситуации не вполне корректно.

2. Группы

А. Основные определения и примеры.

3.36. Определение. Непустое множество G с заданной на нём бинарной операцией $*\colon G \times G \to G$ называется *группой*, если выполняются следующие свойства:

Г1: операция $*$ ассоциативна, т.е.

$$\forall a, b, c \in G: \quad a * (b * c) = (a * b) * c;$$

Г2: операция $*$ обладает *нейтральным элементом*:

$$\exists e \in G\ \forall a \in G: \quad a * e = e * a = a;$$

Г3: каждый элемент множества G обратим:

$$\forall a \in G\ \exists b \in G: \quad a * b = b * a = e;$$

обратный элемент для a обозначается a^{-1}.

Требования **Г1**–**Г3** называются *аксиомами группы*.

3.37. Группа G, содержащая конечное число элементов, называется *конечной*, и в этом случае число её элементов называется *порядком* и обозначается $|G|$. В противном случае группа называется *бесконечной*.

3.38. Для конечной группы можно построить «таблицу умножения»:

	e	x_1	$\cdots$	x_j	$\cdots$	x_n
e	e	x_1		x_j		x_n
x_1	x_1	$x_1 * x_1$		$x_1 * x_j$		$x_1 * x_n$
$\vdots$						
x_i	x_i	$x_i * x_1$		$x_i * x_j$		$x_i * x_n$
$\vdots$						
x_n	x_n	$x_n * x_1$		$x_n * x_j$		$x_n * x_n$

Левый сомножитель произведения берётся из заголовочного столбца, а правый — из заголовочной строки этой таблицы, называемой *таблицей Кэли*.

3.39. Группа называется *абелевой*, если операция в ней коммутативна. Иными словами, в абелевой группе в дополнение к аксиомам **Г1**–**Г3** выполняется следующая аксиома:

Г4: операция $*$ коммутативна, т.е.

$$\forall a, b \in G: \quad a * b = b * a.$$

В этом случае операцию обычно называют *сложением* и обозначают символом $+$; такая форма записи групповой операции называется *аддитивной*. Нейтральный элемент абелевой группы называют *нулём* и обозначают 0, а элемент, обратный к $a \in G$, называют *противоположным* и обозначают $-a$. Символом $a - b$ обозначают такой элемент $c \in G$, что $a = b + c$; при заданных $a, b \in G$ этот элемент единствен (см. предложение 3.28). Таблица Кэли абелевой группы симметрична относительно главной диагонали.

3.40. Для неабелевых групп используется альтернативный способ записи, *мультипликативный*; в этом случае операцию называют *умножением* и обозначают символом $\cdot$, который в ряде случаев вовсе опускают, записывая ab вместо $a \cdot b$ или $a * b$. Элемент, обратный к a, обозначают a^{-1}.

3.41. В дальнейшем при разработке общих теоретических вопросов будем пользоваться мультипликативной формой записи, обозначать операцию в группе символом $\cdot$ и называть умножением, а нейтральный элемент обозначать символом e и называть единицей. Запись $(G, \cdot, e)$ означает, что G — группа с умножением $\cdot$ и единицей e.

3.42. Предложение. *Для любой группы $(G, \cdot, e)$ справедливы следующие утверждения*:

(i) *единица e группы единственна*;
(ii) *для каждого элемента $a \in G$ его обратный a^{-1} единствен*;
(iii) *для любых элементов $a, b, c \in G$ из равенств $ac = bc$ и $ca = cb$ вытекает равенство $a = b$ (законы сокращения справа и слева)*;
(iv) *для любых $a, b \in G$ элемент $ab \in G$ обратим*; *его обратным является $b^{-1}a^{-1}$*;
(v) *элемент, обратный к a^{-1}, обратим, причём $(a^{-1})^{-1} = a$.*

Доказательство. Приведённые утверждения являются частными случаями предложений 3.22 и 3.27. □

3.43. Примеры.

1. Множество, состоящее из единственного элемента e и снабжённое операцией $*$, действующей по правилу $e * e = e$, является группой; элемент e является единицей.
2. Множество $\{1, -1\}$ является абелевой группой относительно операции умножения.
3. Множество вещественных чисел с операцией сложения $(\mathbb{R}, +)$ является абелевой группой и называется *аддитивной группой* $\mathbb{R}$. Нейтральным элементом является нуль, а обратным к числу $a \in \mathbb{R}$ — противоположное число $-a \in \mathbb{R}$. Аналогично определяются аддитивные группы $\mathbb{Q}$, $\mathbb{C}$.
4. Множество ненулевых вещественных чисел с операцией умножения $(\mathbb{R} \setminus \{0\}, \cdot)$ является абелевой группой и называется *мультипликативной группой* $\mathbb{R}^*$. Нейтральным элементом является единица, а обратным к числу $a \in \mathbb{R}^*$ — число $a^{-1} \in \mathbb{R}^*$. Аналогично определяются мультипликативные группы чисел $\mathbb{Q}^*$, $\mathbb{C}^*$.
5. Множество *всех* рациональных (вещественных, комплексных) чисел не образует группу относительно умножения, поскольку элемент 0 не имеет обратного относительно этой операции.
6. Множество целых чисел с операцией сложения $(\mathbb{Z}, +)$ — абелева группа. Нейтральным элементом является нуль, а обратным (противоположным, см. п. 3.39) к числу $a \in \mathbb{Z}$ — число $-a \in \mathbb{Z}$. Обратите внимание, что множество целых чисел не является группой относительно операции умножения несмотря на ассоциативность этой операции и наличие нейтрального элемента (единицы), поскольку обратимыми элементами относительно операции умножения являются лишь ± 1.

Читателю рекомендуется привести аналогичные примеры групп и не-групп самостоятельно. Многочисленные примеры будут появляться в дальнейшем изложении.

Б. Альтернативные определения.

3.44. В определении группы можно заменить аксиомы **Г2** (существование двустороннего нейтрального элемента) и **Г3** (существование двустороннего обратного элемента) на аксиомы существования *левого* (или правого) нейтрального элемента и *левого* (или правого) обратного элемента:

Г3′: $\exists e \in G\ \forall x \in G$: $e * x = x$,
Г4′: $\forall x \in G\ \exists y \in G$: $y * x = e$,

Заинтересованному читателю предлагается доказать это утверждение самостоятельно (см. задачу 3.2).

3.45. С формальной точки зрения в группе имеется не одна, а *три* операции: бинарная групповая операция $*$, унарная операция взятия обратного элемента и нуль-арная операция — нейтральный элемент группы. В некоторых случаях такой подход бывает полезен, однако мы его использовать не будем.

3.46. Обозначим через $a/b = ab^{-1}$ операцию *правого деления*. Три операции, входящие в определение группы из п. 3.45, выражаются через операцию / следующим образом:

$$e = a/a, \quad a^{-1} = (a/a)/a, \quad a * b = a/\big((b/b)/b\big).$$

Кроме того, нетрудно проверить соотношения $a = a/(a/a)$ и $(a/a)/(b/c) = c/b$.

3.47. Можно показать, что группу можно определить как множество G с одной бинарной операцией $G \times G \to G$, $(a, b) \mapsto a/b$, удовлетворяющей следующим двум аксиомам:

(i) для любых $a, b, c \in G$ выполняется равенство $(a/c)/(b/c) = a/b$;
(ii) для любых $a, b \in G$ уравнение $a/x = b$ разрешимо.

В. Подгруппы.

3.48. Определение. Непустое подмножество $H \subset G$ группы G называется *подгруппой* в G, если оно замкнуто относительно умножения в группе G и взятия обратного элемента, т.е. если выполняются следующие условия:

(i) $ab \in H$ для всех $a, b \in H$,
(ii) $a^{-1} \in H$ для любого $a \in H$.

Тот факт, что H является подгруппой в G, обозначается $H \leqslant G$ (или $H < G$, если $H \leqslant G$ и $H \neq G$), в то время как символ $\subset$ используется для обозначения подмножеств, не являющихся подгруппами.

3.49. Поскольку $aa^{-1} = e$, отсюда следует, что $e \in H$. Очевидно, $\{e\}$ и G являются подгруппами группы G; эти подгруппы называют *тривиальными*. Очевидно, любая подгруппа H группы G сама является группой относительно той же операции.

3.50. Предложение. *Подмножество H группы G является подгруппой тогда и только тогда, когда $e \in H$ и для любых $a, b \in H$ выполнено $ab^{-1} \in H$.*

Доказательство. Достаточность почти очевидна: если $H < G$, то в силу требований (i) и (ii) определения 3.48 для всех $a, b \in H$ имеем $ab^{-1} \in H$.

Необходимость. Пусть для любых $a, b \in H$ выполнено условие $ab^{-1} \in H$. Выбрав пару элементов $e, a \in H$, убеждаемся, что $ea^{-1} = a^{-1} \in H$. Поскольку $(b^{-1})^{-1} = b$, то $ab = a(b^{-1})^{-1} \in H$. □

3.51. Предложение. *Если $H_1 < G$ и $H_2 < G$, то $H_1 \cap H_2 < G$ (пересечение подгрупп является подгруппой).*

Доказательство. Так как $e \in H_1$ и $e \in H_2$, то $e \in H_1 \cap H_2$. Далее, рассмотрим произвольные элементы $a, b \in H_1 \cap H_2$:

$$a, b \in H_1 \cap H_2 \Rightarrow \left\{\begin{matrix} a, b \in H_1 \\ a, b \in H_2 \end{matrix}\right\} \Rightarrow \left\{\begin{matrix} ab^{-1} \in H_1 \\ ab^{-1} \in H_2 \end{matrix}\right\} \Rightarrow ab^{-1} \in H_1 \cap H_2,$$

так что согласно предложению 3.50 получаем $H_1 \cap H_2 < G$. □

3.52. Примеры.

1. Группа $(\mathbb{R}_+, \cdot)$ положительных вещественных чисел с операцией умножения является подгруппой мультипликативной группы $\mathbb{R}^*$.
2. Множество $2\mathbb{Z}$ чётных целых чисел образует подгруппу группы $\mathbb{Z}$ из примера 3.43.6. Множество нечётных целых чисел подгруппой не является (почему?).
3. В аддитивной группе $\mathbb{R}$ имеется цепочка подгрупп $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.
4. В мультипликативной группе $\mathbb{R}^*$ имеется цепочка подгрупп $\{\pm 1\} \subset \mathbb{Q}^* \subset \mathbb{R}^*$.

3. Кольца и поля

A. Основные определения и примеры колец.

3.53. Определение. *Кольцом* называется непустое множество R с двумя заданными на нём бинарными операциями, называемыми *сложением* и *умножением* (знаки операций $+$ и $\cdot$ соответственно; $\cdot$ обычно опускается) и обладающими следующими свойствами:

K1: относительно сложения $+$ множество R образует абелеву группу, называемую *аддитивной группой кольца*; нейтральный элемент этой группы называется *нулём* и обозначается 0;

K2: умножение $\cdot$ дистрибутивно относительно сложения: для любых $a, b, c \in R$ имеют место соотношения

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

Требования **K1** и **K2** называются *аксиомами кольца*. Если, кроме того, операция умножения коммутативна (ассоциативна), то кольцо называется *коммутативным* (*ассоциативным*); отметим, что некоммутативные и неассоциативные кольца встречаются весьма часто. Если операция умножения обладает нейтральным элементом, то он называется *единицей* кольца, а само кольцо — *кольцом с единицей*, или *унитальным кольцом*; в этом случае дополнительно предполагают, что $0 \neq 1$.

3.54. Элемент a унитального кольца называется *обратимым*, если для него существует (двусторонний) обратный (относительно операции умножения) элемент a': $a\cdot a' = a'\cdot a = 1$.

3.55. Возможна ситуация, при которой произведение ненулевых элементов a, b кольца́ равно нулю: $ab = 0$; такие ко́льца называют *кольцами с делителями нуля*. Если же из равенства $ab = 0$ следует, что либо $a = 0$, либо $b = 0$, то говорят, что кольцо не имеет делителей нуля.

3.56. В кольце без делителей нуля возможно сокращение: если $ac = bc$ и $c \neq 0$, то $a = b$. Действительно, если $ac = bc$, то $(a-b)c = 0$ и, поскольку $c \neq 0$, заключаем, что $a-b = 0$, т.е. $a = b$. Аналогично, если $ca = cb$ и $c \neq 0$, то $a = b$.

3.57. Определение. *Целостным кольцом*,, или *областью целостности* называется коммутативное ассоциативное унитальное кольцо без делителей нуля, т.е. кольцо, в котором из $ab = 0$ вытекает $(a = 0) \vee (b = 0)$.

3.58. Определение. Непустое подмножество $S \subset R$ кольца R называется *подкольцом* в R, если оно

(i) является подгруппой аддитивной группы кольца;
(ii) замкнуто относительно операции умножения.

В этом случае кольцо R называют *расширением* кольца S.

3.59. Очевидно, любое подкольцо само является кольцом относительно тех же операций, причём оно наследует такие свойства, как коммутативность и ассоциативность.

3.60. Примеры.

1. Множество $\mathbb{Z}$ целых чисел с операциями сложения и умножения является целостным кольцом $(\mathbb{Z}, +, \cdot)$ (оно коммутативно, ассоциативно, обладает единицей и не имеет делителей нуля). В этом кольце обратимыми являются только элементы 1 и -1.

2. Множество $2\mathbb{Z}$ чётных целых чисел с операциями сложения и умножения является коммутативным ассоциативным кольцом без единицы $(2\mathbb{Z}, +, \cdot)$. Кольцо $2\mathbb{Z}$ является подкольцом кольца целых чисел $\mathbb{Z}$.
3. Цепочка подгрупп аддитивной группы $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ (см. пример 3.52.3) является одновременно и цепочкой подколец, каждое из которых является целостным.
4. Множество всех числовых функций $f\colon \mathbb{R} \to \mathbb{R}$ является коммутативным ассоциативным унитальным кольцом относительно обычных операций сложения и умножения функций. Это кольцо не является целостным, т.е. обладает делителями нуля; например, произведение функций
$$f(x) = \begin{cases} 0, & x < 0, \\ 1, & x \geqslant 0, \end{cases} \qquad g(x) = \begin{cases} 1, & x < 0, \\ 0, & x \geqslant 0 \end{cases}$$
есть функция, тождественно равная нулю. В рассматриваемом кольце имеются как обртимые, так и необратимые элементы.
5. Множество многочленов от переменной x с вещественными коэффициентами является целостным кольцом относительно операций сложения и умножения многочленов; это кольцо обозначается $\mathbb{R}[x]$. Обратимыми элементами кольца $\mathbb{R}[x]$ являются многочлены нулевой степени, т.е. отличные от нуля константы.
6. На множестве $\mathbb{R} \times \mathbb{R}$ введём операции
$$(a, b) + (a', b') \stackrel{\text{def}}{=\!=} (a + a', b + b'),$$
$$(a, b) \cdot (a', b') \stackrel{\text{def}}{=\!=} (aa', bb').$$
Легко проверить, что относительно этих операций множество $\mathbb{R} \times \mathbb{R}$ является коммутативным ассоциативным кольцом с единицей $(1, 1)$, обладающее делителями нуля:
$$(x, 0) \cdot (0, y) = (0, 0).$$

Б. Поля.

3.61. Определение. *Полем* называется коммутативное ассоциативное унитальное кольцо, в котором любой ненулевой элемент обратим.

3.62. В любом поле
$$ab = 0 \quad \Rightarrow \quad (a = 0) \vee (b = 0).$$
Действительно, если $a \neq 0$, то, умножив обе части равенства $ab = 0$ на a^{-1}, получим $b = 0$. Таким образом, любое поле является целостным кольцом.

3.63. Примеры.

1. Множества рациональных чисел $\mathbb{Q}$ и вещественных чисел $\mathbb{R}$ являются примерами полей, хорошо знакомых читателю из школьного курса. Эти поля называются *числовыми полями*.
2. Кольцо $\mathbb{Z}$ целых чисел полем не является, поскольку в нём обратимы только элементы ± 1.
3. Менее тривиальным примером числового поля является множество $\mathbb{Q}[\sqrt{2}] \stackrel{\text{def}}{=\!=} \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ (проверьте самостоятельно).

3.64. Определение. Подмножество $\mathbb{L} \subset \mathbb{K}$ поля $\mathbb{K}$ называется *подполем* в $\mathbb{K}$, если оно замкнуто относительно операций сложения, вычитания (т.е. операции, обратной к сложению), умножения и деления (т.е. операции, обратной к умножению); очевидно, $\mathbb{L}$ при этом само является полем. Поле $\mathbb{K}$ при этом называется *расширением* поля $\mathbb{L}$. Например, поле вещественных чисел $\mathbb{R}$ является расширением поля рациональных чисел $\mathbb{Q}$.

B. Поле отношений целостного кольца.

3.65. Пусть R — целостное кольцо. Определим на множестве $R \times R$ отношение эквивалентности $\simeq$ по правилу

$$(a, b) \simeq (a', b') \;\Leftrightarrow\; ab' = a'b \tag{3.2}$$

(докажите самостоятельно, что это отношение действительно является отношением эквивалентности; см. задачу 3.3). Из определения (3.2) следует, что $(a, b) \simeq (ac, bc)$ для любого $c \neq 0$. Условимся записывать класс эквивалентности, содержащий пару (a, b), как «дробь» a/b или $\frac{a}{b}$ (это символ, не подразумевающий фактического деления).

3.66. Определим на $R \times R$ сложение и умножение по правилам

$$(a, b) + (a', b') = (ab' + a'b,\ bb'), \quad (a, b) \cdot (a', b') = (aa',\ bb'). \tag{3.3}$$

Эти операции согласованы с отношением эквивалентности (3.2) (см. задачу 3.4), поэтому в силу определения 3.31 они индуцируют операции на фактор-множестве $R \times R/\simeq$, которые запишем в привычном виде:

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}, \quad \frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}. \tag{3.4}$$

Нетрудно проверить (см. задачу 3.5), что фактор-множество $R \times R/\simeq$ с указанными операциями представляет собой поле, называемое полем отношений (или полем дробей) целостного кольца R и обозначается $\operatorname{Frac} R$ или $\operatorname{Quot} R$.

3.67. Пример. Поле рациональных чисел является полем отношений кольца целых чисел: $\mathbb{Q} = \operatorname{Frac}\mathbb{Z}$.

4. Гомоморфизмы и изоморфизмы

3.68. Определение. Рассмотрим две алгебраические системы с одинаковым количеством попарно однотипных операций: множество X с унарными операциями $r, s, \ldots$ и бинарными операциями $\circ, *, \ldots$ и множество Y с унарными операциями $\rho, \sigma, \ldots$ и бинарными операциями $\bullet, \star, \ldots$. Отображение $f : X \to Y$ называется *гомоморфизмом* этих алгебраических систем, если для любых $x, x_1, x_2 \in X$ имеем

$$f(rx) = \rho f(x), \quad f(sx) = \sigma f(x), \quad \ldots,$$
$$f(x_1 \circ x_2) = f(x_1) \bullet f(x_2), \quad f(x_1 * x_2) = f(x_1) \star f(x_2), \quad \ldots.$$

3.69. Определение. Взаимно однозначный гомоморфизм называется *изоморфизмом*. Алгебраические системы, между которыми существует изоморфизм, называют *изоморфными*.

3.70. Не исключается ситуация, когда $X = Y$, т.е. возможно рассматривать отображение $f : X \to X$ алгебраической системы в себя. Если $r, s, \ldots$ — унарные операции на множестве X, $\circ, *, \ldots$ — бинарные операции, то отображение f называется *гомоморфизмом*, если для любых $x, x_1, x_2 \in X$ имеем

$$f(rx) = rf(x), \quad f(sx) = sf(x), \quad \ldots,$$
$$f(x_1 \circ x_2) = f(x_1) \circ f(x_2), \quad f(x_1 * x_2) = f(x_1) * f(x_2), \quad \ldots.$$

Гомоморфизмы алгебраической системы в себя называются *эндоморфизмами*, а изоморфизмы — *автоморфизмами*. Очевидно, для любой алгебраической системы X тождественное отображение $\mathrm{id}_X : X \to X$ является автоморфизмом.

3.71. Отношение изоморфности алгебраических систем обладает всеми свойствами отношения эквивалентности: оно рефлексивно, симметрично и транзитивно (см. замечание 2.114, с. 60).

3.72. В алгебре мы интересуемся только теми свойствами алгебраических систем, которые выражаются в терминах операций, заданных на этих системах. Две изоморфные алгебраические системы являются «одинаково устроенными» в том смысле, что любое утверждение, сформулированное только в терминах операций, справедливо в одной из этих систем тогда и только тогда, когда оно справедливо в другой. Поэтому безразлично, какую из изоморфных друг другу алгебраических систем изучать: все они являются

различными реализациями (моделями) одного и того же абстрактного объекта. Однако различные модели одной и той же алгебраической системы могут обладать специфическими свойствами, облегчающими их исследование; например, при изучении модели геометрического происхождения можно использовать геометрические методы и т. п.

5. Упражнения и задачи

3.1 (р)**.** Пусть $*$ — ассоциативная операция на множестве X, обладающая нейтральным элементом e. Докажите, что если x — обратимый элемент, удовлетворяющий условию $x * x = x$, то $x = e$.

3.2 (р)**.** Докажите утверждение из п. 3.44. Приведите пример, который показывает, что из существования *левого* нейтрального элемента и *правого* обратного элемента *не следует* выполнение аксиом группы.

3.3. Пусть R — целостное кольцо. Докажите, что отношение на множестве $R \times R$, заданное формулой (3.2), является отношением эквивалентности.

3.4. Пусть R — целостное кольцо. Докажите, что операции на множестве $R \times R$, заданные формулами (3.3), согласованы с отношением эквивалентности (3.2).

3.5. Докажите, что множество $R \times R/\simeq$, где отношение эквивалентности $\simeq$ задано формулой (3.2), снабжённое операциями (3.4), является полем.

ГЛАВА 4

Числовые системы

1. Натуральные числа

А. Операции над натуральными числами. Понятие натурального числа, базирующееся на теоретико-множественном подходе, было введено в разделе Г. Арифметические операции на множестве $\mathbb{N}_0$ натуральных чисел и отношение сравнения определяются следующим образом.

4.1. Определение. *Сложение* на множестве $\mathbb{N}_0$ — это бинарная операция $(x, y) \mapsto x + y$ на $\mathbb{N}_0$, удовлетворяющая следующим аксиомам:

A1. $\forall x \in \mathbb{N}_0$: $x + 0 = x$;
A2. $\forall x, y \in \mathbb{N}_0$: $x + S(y) = S(x + y)$.

4.2. Согласно определению 4.1 имеем

$$
\begin{aligned}
&x + 0 = x,\\
&x + 1 = x + S(0) = S(x + 0) = S(x),\\
&x + 2 = x + S(1) = S(x + 1) = S(S(x)),\\
&x + 3 = x + S(2) = S(x + 2) = S(S(S(x))), \quad \ldots .
\end{aligned}
$$

4.3. Определение. *Умножение* на множестве $\mathbb{N}_0$ — это бинарная операция $(x, y) \mapsto x \cdot y$ на bN_0, удовлетворяющая следующим аксиомам:

M1. $\forall x \in \mathbb{N}_0$: $x \cdot 0 = 0$;
M2. $\forall x, y \in \mathbb{N}_0$: $x \cdot S(y) = x \cdot y + x$.

4.4. Согласно определению 4.3 имеем

$$
\begin{aligned}
&x \cdot 0 = 0,\\
&x \cdot 1 = x \cdot S(0) = x \cdot 0 + x = 0 + x = x,\\
&x \cdot 2 = x \cdot S(1) = x \cdot 1 + x = x + x,\\
&x \cdot 3 = x \cdot S(2) = x \cdot 2 + x = x + x + x, \quad \ldots .
\end{aligned}
$$

4.5. Можно доказать, что такие операции обладают привычными свойствами, известными из школьного курса, например, свойствами коммутативности, ассоциативности, дистрибутивности умножения относительно сложения (попытайтесь это сделать; см. задачи **??**–**??**).

Б. Сравнение натуральных чисел.

4.6. Для двух натуральных чисел x и y выполняется одно и только одно из следующих соотношений:

(i) $x = y$;
(ii) $x = y + z$, где $x \in \mathbb{N}_0$, $z \neq 0$;
(iii) $y = x + z$, где $x \in \mathbb{N}_0$, $z \neq 0$.

В первом случае говорят, что x *больше* y и пишут $x > y$ или что y *меньше* x и пишут $y < x$. Если $x > y$ или $x = y$, то пишут $x \geqslant y$ или $y \leqslant x$.

4.7. Предложение. *Любое непустое подмножество $A \subset \mathbb{N}_0$ содержит наименьшее число, т.е. меньшее всех других чисел данного множества.*

Доказательство. Предположим, что существует непустое $A \subset \mathbb{N}_0$, в котором нет наименьшего элемента. Рассмотрим предикат

$P(n)$: ни одно натуральное число $k \leqslant n$ не принадлежит A.

Докажем истинность этого предиката методом математической индукции.

База индукции: $n = 0$. Если $0 \in A$, то 0 — наименьший элемент в A, что противоречит предположению индукции. Следовательно, высказывание $P(0)$ истинно.

Шаг индукции. Предположим, что высказывание $P(n)$ истинно, т.е. для любого $k \leqslant n$ имеем $k \notin A$. Если $n + 1 \in A$, то $n + 1$ — наименьший элемент в A, так как все меньшие натуральные числа не принадлежат множеству A; это противоречит предположению. Следовательно, $n + 1 \notin A$, т.е. высказывание $P(n + 1)$ истинно. Итак, $P(n)$ истинно для всех $n \in \mathbb{N}_0$, так что $A = \varnothing$. □

В. Делимость натуральных чисел. Основная теорема арифметики.

4.8. Говорят, что натуральное число a *делится* на натуральное число d (делитель, divisor), если существует такое натуральное число q (частное, quotient), что $a = qd$; для обозначения этого факта используются записи $a \vdots d$ («a делится на d») и $d \mid a$ («d делит (является делителем) a»). Таким образом, операция деления, обратная

к операции умножения, определяется как результат решения уравнения $b \cdot x = a$. Она выполнима не всегда; например, уравнение $2x = 3$ натуральных решений не имеет. Однако всегда возможно так называемое *деление с остатком*, описанное ниже в разделе B.

4.9. Определение. Натуральное число $p \geqslant 2$ называется *простым*, если его нельзя представить в виде $p = ab$, где $a \geqslant 2$, $b \geqslant 2$. Иными словами, натуральное число p является простым, если оно имеет ровно два натуральных делителя 1 и p. Натуральное число $p \geqslant 2$, не являющееся простым, называется *составным*. Числа 0 и 1 не относят ни к простым, ни к составным.

4.10. Теорема (теорема Евклида)**.** *Множество простых чисел бесконечно.*

Доказательство. Предположим, что множество простых чисел конечно и состоит из элементов $2 = p_1 < p_2 < \cdots < p_n$. Тогда число $P = p_1 \dots p_n + 1 > p_n$ не является простым и, следовательно, должно делиться хотя бы на одно из чисел $p_1, \dots, p_n$, например, на p_k, где $1 \leqslant k \leqslant n$. Поскольку $p_1 \dots p_n$ делится на p_k, то и число 1 должно делиться на p_k, что невозможно, поскольку $1 < p_k$. □

4.11. Теорема. *В множестве натуральных чисел существуют сколь угодно длинные интервалы, не содержащие ни одного простого числа.*

Доказательство. Возьмём произвольное натуральное число n и рассмотрим натуральные числа

$$(n+1)! + 2, \quad (n+1)! + 3, \quad \dots, \quad (n+1)! + n + 1;$$

все эти числа составные. Получили n идущих подряд составных чисел. □

4.12. Теорема (основная теорема арифметики)**.** *Любое натуральное число $n > 1$ можно представить в виде произведения простых сомножителей, причём это разложение единственно с точностью до порядка сомножителей.* (*Мы не исключаем случай, когда разложение состоит только из одного множителя.*)

Доказательство. Существование. Используем индукцию. Очевидно, для (простого) числа 2 утверждение верно. Предположим, что оно справедливо для всех чисел $< n$, и докажем его для числа n. Если n — простое, то доказывать нечего. В противном случае $n = ab$, где $1 < a < n$, $1 < b < n$. Каждое из чисел a, b либо простое, либо (в силу индуктивного предположения) может быть разложено в произведение простых. Подставляя их разложения в формулу

$n = ab$, получаем разложение исходного числа n на простые сомножители.

Единственность. Для доказательства единственности потребуется следующий факт, который будет доказан позже (см. предложение 4.37): *если простое число p делит произведение $a_1 \dots a_n$, то оно делит хотя бы один из сомножителей $a_1, \dots, a_n$.*

Предположим, что число n имеет два разных разложения на простые сомножители:

$$n = p_1 \cdot p_2 \cdot p_3 \cdots p_k = q_1 \cdot q_2 \cdot q_3 \cdots q_l. \tag{4.1}$$

Нужно доказать, что $k = l$ и $p_j = q_j$ после подходящей перенумерации множителей. Используем индукцию по числу сомножителей. При $k = 1$ единственность очевидна. Если $k > 1$, то $p_1 \mid q_1 q_2 \dots q_l$ и, следовательно, существует такой номер i, что $p_1 \mid q_i$ и поэтому $p_1 = q_i$; можно считать, что $i = 1$ и $p_1 = q_1$. Сокращая равенство (4.1) на p_1, получим

$$p_2 \cdot p_3 \cdots p_k = q_2 \cdot q_3 \cdots q_l.$$

По предположению индукции отсюда следует, что $k = l$ и $p_j = q_j$, $j = 2, \dots, l$, после подходящей перенумерации. □

4.13. Определение. *Наибольшим общим делителем* двух натуральных чисел a и b называется их общий делитель, делящийся на всех их общие делители. Обозначение НОД(a, b) или $\gcd(a, b)$ (greatest common divisor).

4.14. *Наименьшим общим кратным* двух натуральных чисел a и b называется их общее кратное, делящее все их общие кратные. Обозначение НОК(a, b) или $\operatorname{lcm}(a, b)$ (least common multiple).

4.15. Понятия НОД и НОК очевидным образом обобщаются на произвольное количество чисел.

4.16. Определения 4.13 и 4.14 отличаются от школьных, согласно которым НОД(a, b) — это *максимальный* из общих делителей чисел a и b, а НОК(a, b) — минимальное из общих кратных. Школьные определения невозможно обобщить на кольца, в которых отсутствует отношение порядка, поэтому мы от них отказываемся в пользу определений 4.13 и 4.14, допускающих подобные обобщения. Однако при таком существование НОД и НОК не является очевидным; для НОД доказательство приведено ниже в теореме 4.33.

4.17. Если известны разложения натуральных чисел a и b в произведения простых сомножителей:

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

то

$$\text{НОД}(a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdots p_k^{\min(\alpha_k,\beta_k)}, \tag{4.2}$$

$$\text{НОК}(a,b) = p_1^{\max(\alpha_1,\beta_1)} \cdots p_k^{\max(\alpha_k,\beta_k)}. \tag{4.3}$$

Отсюда вытекает, что

$$\text{НОД}(a,b) \cdot \text{НОК}(a,b) = ab.$$

4.18. Операции НОД и НОК на множестве $\mathbb{N}$ являются ассоциативными: для любых $a, b, c \in \mathbb{N}$ имеем

$$\text{НОД}\big(a, \text{НОД}(b,c)\big) = \text{НОД}\big(\text{НОД}(a,b), c\big) = \text{НОД}(a,b,c),$$
$$\text{НОК}\big(a, \text{НОК}(b,c)\big) = \text{НОК}\big(\text{НОК}(a,b), c\big) = \text{НОК}(a,b,c);$$

это вытекает из (4.2) и ассоциативности минимума и максимума:

$$\min\big(a, \min(b,c)\big) = \min\big(\min(a,b), c\big) = \min(a,b,c),$$
$$\max\big(a, \max(b,c)\big) = \max\big(\max(a,b), c\big) = \max(a,b,c).$$

2. Целые числа

А. Формальное определение.

4.19. Если $a, b \in \mathbb{N}_0$ и $a \geqslant b$, то уравнение $b + x = a$ относительно неизвестной x имеет единственное решение, которое обозначается $x = a - b$; таким образом, на множестве $\mathbb{N}_0$ возникает операция вычитания, обратная к операции сложения. Эта операция определена не для всех пар натуральных чисел.

4.20. Рассмотрим на множестве $\mathbb{N}_0 \times \mathbb{N}_0$ упорядоченных пар натуральных чисел отношение, определённое следующим образом:

$$(a,b) \simeq (x,y) \quad \Leftrightarrow \quad a + y = b + x. \tag{4.4}$$

Легко проверить, что это отношение является отношением эквивалентности:

(а) рефлексивность: $(a,b) \simeq (a,b)$, поскольку $a + b = b + a$;
(б) симметричность: если $(a,b) \simeq (x,y)$, т.е. $a + y = b + x$, то $x + b = y + a$, так что $(x,y) \simeq (a,b)$;
(в) транзитивность: если $(a,b) \simeq (x,y)$ и $(x,y) \simeq (p,q)$, то

$$\left.\begin{matrix} a + y = b + x, \\ x + q = y + p \end{matrix}\right\} \Leftrightarrow\ a + y + x + q = b + x + y + p \ \Leftrightarrow$$
$$\Leftrightarrow\ a + q = b + p \ \Leftrightarrow\ (a,b) \simeq (p,q).$$

4.21. Таким образом, множество упорядоченных пар натуральных чисел $\mathbb{N}_0 \times \mathbb{N}_0$ разбивается в дизъюнктное объединение классов эквивалентности. Фактор-множество $\mathbb{N}_0 \times \mathbb{N}_0/\simeq$ называется *множеством целых чисел* $\mathbb{Z}$, а его элементы — *целыми числами*.

4.22. Если $a \geqslant b$, то класс эквивалентности $\big[(a,b)\big]$ содержит элемент $(a-b,0)$:

$$(a,b) \simeq (a-b,0) \;\Leftrightarrow\; a+0 = b+(a-b).$$

Произведём отождествление $a-b \equiv (a,b)$, т.е. рассмотрим множество $\mathbb{N}_0$ как подмножество множества $\mathbb{Z}$:

$$\iota : \mathbb{N}_0 \hookrightarrow \mathbb{Z}, \quad \iota(n) = \big[(n,0)\big].$$

где ι — отображение вложения (см. определение 2.70, с. 47).

4.23. Если $a < b$, то класс $\big[(a,b)\big]$ называют *отрицательным целым числом*, противоположным к натуральному числу $n = b-a = \iota^{-1}\big(\big[(b,a)\big]\big)$, и обозначают $-n$:

$$\big[(a,b)\big] = -\big[(b,a)\big].$$

4.24. На множестве $\mathbb{N}_0 \times \mathbb{N}_0$ определим операцию сложения $+$ следующим образом:

$$(a,b)+(p,q) \stackrel{\text{def}}{=\!=} (a+p, b+q).$$

Проверим, что эта операция согласована с введённым отношением эквивалентности $\simeq$ (см. определение 3.31, с. 76), т.е.

$$\text{если } (a',b') \simeq (a,b) \text{ и } (p',q') \simeq (p,q),$$
$$\text{то } (a',b')+(p',q') \simeq (a,b)+(p,q).$$

Итак, пусть $(a',b') \simeq (a,b)$ и $(p',q') \simeq (p,q)$, т.е.

$$a'+b = b'+a, \quad p'+q = q'+p. \tag{4.5}$$

Поскольку

$$(a,b)+(p,q) = (a+p,\ b+q), \quad (a',b')+(p',q') = (a'+p',\ b'+q'),$$

требуется проверить равенство

$$a+p+b'+q' = b+q+a'+p',$$

которое, очевидно, верно в силу (4.5).

4.25. Итак, на фактор-множестве $\mathbb{Z} = \mathbb{N}_0 \times \mathbb{N}_0/\simeq$ корректно определена операция сложения:

$$\big[(a,b)\big] + \big[(p,q)\big] \stackrel{\text{def}}{=\!=} \big[(a+p,b+q)\big],$$

являющаяся, очевидно, коммутативной и ассоциативной, т.е. для любых $m, n, l \in \mathbb{Z}$ выполняются соотношения

$$m + n = n + m, \quad (m + n) + l = m + (n + l).$$

4.26. Сумма чисел $-n$ и n равна нулю:

$$-n + n = \big[(b, a)\big] + \big[(a, b)\big] = \big[(b + a, a + b)\big] = \big[(0, 0)\big].$$

4.27. *Модулем* целого числа n называется натуральное число

$$|n| = \begin{cases} n, & n \geqslant 0; \\ -n, & n < 0. \end{cases}$$

Б. Умножение и деление целых чисел.

4.28. Операция умножения $\cdot$ на множестве $\mathbb{Z}$ определяется следующим образом:

$$\big[(a, b)\big] \cdot \big[(p, q)\big] \stackrel{\text{def}}{=\!=} \big[(ap + bq,\ aq + bp)\big]. \tag{4.6}$$

Проверьте, что эта операция определена корректно (ср. п. 4.24; см. задачу **??**), обладает свойствами коммутативности и ассоциативности и даёт тот же результат, что и операция, известная из школьного курса.

4.29. Наличие в множестве $\mathbb{Z}$ целых чисел операций сложения и умножения превращает это множество в коммутативное ассоциативное унитальное кольцо без делителей нуля.

4.30. Целое число $-1 \equiv [(0, 1)]$ — «минус единица» — обладает свойством $-1 \cdot n = -n$, где $n \in \mathbb{N}_0$. Действительно, если $n = [(a, b)]$, где $a \geqslant b$, то

$$-1 \cdot n = [(0, 1)] \cdot [(a, b)] = [(b, a)] = -n.$$

Таким образом, любое отличное от нуля целое число можно представить в виде εn, где $n \in \mathbb{N}$, а $\varepsilon = \pm 1$.

4.31. Делимость целых чисел определяется точно так же, как для натуральных чисел, см. п. 4.8. Хотя отношение делимости определено на множестве целых чисел, его достаточно рассматривать лишь на множестве натуральных чисел (см. п. 4.30), что мы и будем зачастую делать в дальнейшем, оставляя читателю работу по распространению обсуждаемых фактов на все целые числа. Очевидно, любой натуральный делитель натурального числа m не превосходит m.

В. Деление с остатком.

4.32. Теорема. *Для любых целых чисел a и d $(d \neq 0)$ существуют такие целое q и натуральное r, что выполняется равенство*

$$a = qd + r, \quad \text{где } 0 \leqslant r < |d|.$$

Числа q и r (остаток, remainder) *определены единственным образом.*

Доказательство. Случай 1: $d > 0$. В множестве

$$\{nd \mid n \in \mathbb{Z}\} = \{\ldots,\ -2d,\ -d,\ 0,\ d,\ 2d,\ \ldots\}$$

всех целых чисел, кратных d, найдётся наибольшее число, не превосходящее a; обозначим его qd, т.е.

$$qd \leqslant a < (q+1)d.$$

Вычтем qd из всех частей этого двойного неравенства:

$$0 \leqslant a - qd < d.$$

Введя обозначение $r = a - qd$, получаем

$$a = qd + r, \quad 0 \leqslant r < d.$$

Случай 2: $d < 0$. Положим $d' = -d > 0$. Согласно доказанному, для положительного делителя d' существуют такие q' и r, что

$$a = q'd' + r, \quad 0 \leqslant r < d'.$$

Положив $q = -q'$, получим

$$a = qd + r, \quad 0 \leqslant r < d' = -d = |d|.$$

Докажем *единственность*. Предположим, что

$$a = q_1 d + r_1 = q_2 d + r_2, \quad 0 \leqslant r_1 < |d|, \quad 0 \leqslant r_2 < |d|.$$

Отсюда

$$(q_1 - q_2)d = r_2 - r_1. \tag{4.7}$$

Складывая неравенства $-|d| < -r_1 \leqslant 0$ и $0 \leqslant r_2 < |d|$, получаем, что $-|d| < r_2 - r_1 < |d|$, т.е. $|r_2 - r_1| < d$. Левая часть (4.7) является целым числом, кратным d, поэтому равенство в (4.7) возможно только если обе части равны нулю. Итак, $r_1 = r_2$, откуда следует, что $q_1 = q_2$. □

Г. Алгоритм Евклида.

4.33. Теорема. *Для любых двух целых чисел a и b существует их наибольший общий делитель d, причём он может быть представлен в виде*

$$d = au + bv, \tag{4.8}$$

где u и v — некоторые целые числа. Формула (4.8) *называется* соотношением Безу.[1]

Доказательство. Если $b = 0$, то $d = a = a\cdot 1 + b\cdot 0$. Если a делится на b, то $d = b = a\cdot 0 + b\cdot 1$. В противном случае разделим с остатком a на b, затем b на полученный остаток, затем первый остаток на второй остаток и т. д. Поскольку остатки убывают, на некотором шаге деление выполнится без остатка. Получаем следующую цепочку равенств:

$$\begin{aligned}
a &= q_1 b + r_1, && 0 \leqslant r_1 < |b|,\\
b &= q_2 r_1 + r_2, && 0 \leqslant r_2 < r_1,\\
r_1 &= q_3 r_2 + r_3, && 0 \leqslant r_3 < r_2,\\
&\ldots\ldots\ldots\ldots && \ldots\ldots\ldots\\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1}, && 0 \leqslant r_{n-1} < r_{n-2},\\
r_{n-2} &= q_n r_{n-1} + r_n, && 0 \leqslant r_n < r_{n-1},\\
r_{n-1} &= q_{n+1} r_n.
\end{aligned}$$

Двигаясь по этой цепочке равенств снизу вверх, последовательно получаем

$$\begin{aligned}
r_{n-1} &= q_{n+1} r_n && \Rightarrow \quad r_n \mid r_{n-1},\\
r_{n-2} &= q_n r_{n-1} + r_n = && \\
&= q_n\bigl(q_{n+1} r_n\bigr) + r_n = && \\
&= \bigl(q_n q_{n+1} + 1\bigr)\cdot r_n && \Rightarrow \quad r_n \mid r_{n-2},\\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1} = (\ldots) r_n && \Rightarrow \quad r_{n-3} \mid r_n,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots && \ldots\ldots\ldots\\
b &= (\ldots) r_n && \Rightarrow \quad r_n \mid b,\\
q &= (\ldots) r_n && \Rightarrow \quad r_n \mid a;
\end{aligned}$$

[1] Этьен Безу (Étienne Bézout; 1730–1783) — французский математик.

таким образом, r_n — общий делитель чисел a и b. Двигаясь по той же цепочке равенств сверху вниз, находим

$$\begin{aligned} r_1 &= a - bq_1 = au_1 + bv_1, \\ r_2 &= b - q_2 r_1 = b - q_2(au_1 + bv_1) = au_2 + bv_2, \\ &\dots\dots\dots\dots\dots\dots \\ r_n &= \dots = au_n + bv_n, \end{aligned}$$

где u_i, v_i $(i = 1, \dots, n)$ — некоторые целые числа, в частности,

$$\begin{aligned} u_1 &= 1, & v_1 &= -q_1, \\ u_2 &= -aq_2, & v_2 &= q_1 q_2 + 1, \quad \dots. \end{aligned}$$

Таким образом, r_n можно представить в виде $r_n = au + bv$. Отсюда следует, что r_n делится на любой общий делитель чисел a и b, т.е. в соответствии с определением 4.13 является наибольшим общим делителем. □

4.34. Процесс нахождения наибольшего общего делителя, использованный в доказательстве теоремы 4.33, называется *алгоритмом Евклида*: его описание содержится в «Началах» Евклида (III в до н. э.), однако Евклид не является первооткрывателем: упоминание алгоритма содержится в «Топике» Аристотеля (IV в. до н. э.).

4.35. Целые числа a и b называются *взаимно простыми*, если НОД$(a, b) = 1$. В соответствии с теоремой 4.33 для взаимно простых целых чисел a и b существуют такие целые числа u и v, что $au + bv = 1$. Это равенство является не только необходимым, но и достаточным условием взаимной простоты.

4.36. Предложение. *Если для целых чисел a и b существуют такие целые числа u и v, что $au + bv = 1$, то числа a и b взаимно просты.*

Доказательство. Если НОД$(a, b) = d$, то $a = \alpha d$, $b = \beta d$, так что

$$1 = au + bv = \alpha du + \beta dv = (\alpha u + \beta v)d$$

и поэтому $1 \vdots d \Rightarrow d = 1$. □

4.37. Предложение. *Если простое целое число p делит произведение $a_1 \dots a_n$, то оно делит хотя бы один из сомножителей $a_1, \dots, a_n$.*

Доказательство. Используем индукцию по числу сомножителей n. Пусть $n = 2$ и $p \mid a_1 a_2$, т.е. $a_1 a_2 = pk$. Предположим, что p не

делит a_1; тогда НОД$(p, a_1) = 1$ и, следовательно, существуют такие $u, v \in \mathbb{Z}$, что $pu + a_1 v = 1$. Умножая это равенство на a_2, получим

$$\begin{aligned} pua_2 + a_1 a_2 v = a_2 \quad &\Rightarrow \quad pua_2 + pkv = a_2 \quad \Rightarrow \\ &\Rightarrow \quad p(ua_2 + kv) = a_2 \quad \Rightarrow \quad p \mid a_2. \end{aligned}$$

Если $n > 2$, то запишем $a_1 a_2 \dots a_n = a_1(a_2 \dots a_n)$. Согласно доказанному $p \mid a_1$ или $p \mid (a_2 \dots a_n)$; во втором случае по предположению индукции $p \mid a_i$, где i — один из индексов $2, \dots, n$. □

3. Комплексные числа

Как было отмечено в примере 3.67, поле рациональных чисел $\mathbb{Q}$ является полем отношений кольца целых чисел. Поле вещественных (действительных) чисел $\mathbb{R}$ изучается в курсе математического анализа. В этом разделе обсудим некоторые вопросы, связанные с построением поля комплексных чисел $\mathbb{C}$.

A. Определение поля $\mathbb{C}$.

4.38. Построим расширение поля вещественных чисел $\mathbb{R}$, в котором становится возможным извлечение квадратного корня из отрицательного числа. Для этого введём «число» i, называемое *мнимой единицей* и обладающее свойством $i^2 = -1$; тогда, например,

$$x^2 + 1 = 0 \quad \Leftrightarrow \quad x = \pm i.$$

Рассмотрим множество, элементами которого являются объекты вида $x + iy$, где x и y — вещественные числа, а арифметические операции осуществляются так же, как операции над многочленами, с учётом соотношения $i^2 = -1$. Такие объекты называются *комплексными числами*. Вещественные числа x и y называются соответственно *вещественной* и *мнимой* частями комплексного числа $z = x + iy$ и обозначаются

$$x = \operatorname{Re} z, \quad y = \operatorname{Im} z.$$

Комплексные числа с нулевой вещественной частью $(0 + iy)$ называются *чисто мнимыми*.

4.39. Операции над комплексными числами $x+iy \in \mathbb{C}$ и $u+iv \in \mathbb{C}$ вводятся следующим образом:

$$(x + iy) \pm (u + iv) = (x \pm u) + i(y \pm v) \in \mathbb{C}, \tag{4.9}$$

$$\begin{aligned} (x + iy) \cdot (u + iv) &= xu + xiv + iyu + iyiv = \\ &= (xu - yv) + i(xv + yu) \in \mathbb{C}, \end{aligned} \tag{4.10}$$

$$\frac{x+iy}{u+iv} = \frac{(x+iy)(u-iv)}{(u+iv)(u-iv)} = \frac{(xu+yv)+i(yu-xv)}{u^2+v^2} = \\ = \frac{xu+yv}{u^2+v^2} + i\frac{yu-xv}{u^2+v^2} \in \mathbb{C}. \tag{4.11}$$

Б. Существование поля $\mathbb{C}$.

4.40. Существование комплексных чисел можно доказать, построив *модель* поля $\mathbb{C}$. На множестве $\mathbb{R}\times\mathbb{R}$ всех упорядоченных пар $z=(x,y)$ вещественных чисел введём операции сложения и умножения формулами, подсказанными соотношениями (4.10) и (4.9):

$$(x,y)\pm(u,v) \stackrel{\text{def}}{=\!=} (x\pm u,\ y\pm v), \tag{4.12}$$

$$(x,y)\cdot(u,v) \stackrel{\text{def}}{=\!=} (xu-yv,\ xv+yu). \tag{4.13}$$

Нетрудно проверить, что эти операции обладают следующими свойствами.

4.41. Теорема (свойства арифметических операций над комплексными числами)**.** *Для любых $z_1,z_2,z_3\in\mathbb{C}$ выполняются следующие соотношения*:

(i) *коммутативность сложения*: $z_1+z_2=z_2+z_1$;
(ii) *ассоциативность сложения*: $(z_1+z_2)+z_3=z_1+(z_2+z_3)$;
(iii) *коммутативность умножения*: $z_1z_2=z_2z_1$;
(iv) *ассоциативность умножения*: $(z_1z_2)z_3=z_1(z_2z_3)$;
(v) *дистрибутивность*: $z_1(z_2+z_3)=z_1z_2+z_1z_3$.

4.42. Имеем очевидные соотношения

$$(x,y)+(0,0)=(x,y),\quad (x,y)\cdot(1,0)=(x,y),$$
$$(x,0)+(u,0)=(x+u,0),\quad (x,0)\cdot(u,0)=(xu,0).$$

Это позволяет отождествить пару вида $(x,0)$ с вещественным числом x; в частности, $(0,0)=0$ и $(1,0)=1$. Таким образом, поле $\mathbb{R}$ вещественных чисел вкладывается в поле $\mathbb{C}$ комплексных чисел как подполе.

4.43. Непосредственная проверка доказывает справедливость формулы

$$(x,y)^{-1} = \left(\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2}\right). \tag{4.14}$$

Введём обозначение $i \stackrel{\text{def}}{=\!=} (0,1)$; тогда

$$i^2=-1,\quad (0,y)=(0,1)\cdot(y,0)=iy,\quad (x,y)=(x,0)+(0,y)=x+iy.$$

Итак, мы построили модель поля комплексных чисел, состоящую из упорядоченных пар вещественных чисел с заданными операциями (4.12) и (4.13), что доказывает существование поля $\mathbb{C}$. Запись комплексного числа (x, y) в виде $x + iy$ называется *алгебраической формой записи*.

4.44. Теорема (основная теорема алгебры)**.** *Множество комплексных чисел $\mathbb{C}$ является алгебраически замкнутым числовым полем. Иными словами, любой многочлен с комплексными коэффициентами имеет по крайней мере один комплексный корень.*

Для доказательства этой теоремы недостаточно одних лишь алгебраических методов, требуются ещё и средства математического анализа. Короткое доказательство будет приведено в курсе теории функции комплексной переменной.

B. Матричная модель поля комплексных чисел.

4.45. Рассмотрим (2×2)-матрицу

$$\mathbb{J} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Легко проверить, что $\mathbb{J}^2 = -\mathbb{1}$; это соотношение похоже на свойство мнимой единицы $i^2 = -1$. Убедимся, что множество вещественных (2×2)-матриц вида

$$Z = \begin{pmatrix} x & -y \\ y & x \end{pmatrix} = x\mathbb{1} + y\mathbb{J} \tag{4.15}$$

является моделью поля комплексных чисел, т.е. каждому комплексному числу $z = x + iy$ можно взаимно однозначно поставить в соответствие матрицу $Z = x\mathbb{1} + y\mathbb{J}$, причём арифметическим операциям над комплексными числами будут соответствовать операции над матрицами. Факт соответствия комплексного числа $z = x + iy$ и матрицы $Z = x\mathbb{1} + y\mathbb{J}$ будем записывать в виде $z \leftrightarrow Z$.

4.46. Для матриц $x\mathbb{1} + y\mathbb{J}$ и $u\mathbb{1} + v\mathbb{J}$ имеем

$$(x\mathbb{1} + y\mathbb{J}) \pm (u\mathbb{1} + v\mathbb{J}) = (x \pm u)\mathbb{1} + (y \pm v)\mathbb{J},$$
$$(x\mathbb{1} + y\mathbb{J}) \cdot (u\mathbb{1} + v\mathbb{J}) = (xu - yv)\mathbb{1} + (xv + yu)\mathbb{J},$$

что по форме совпадает с правилами (4.12) и (4.13) (см. с. 98) сложения и умножения комплексных чисел. Таким образом, если $z_1 \leftrightarrow Z_1$ и $z_2 \leftrightarrow Z_2$, то $z_1 \pm z_2 \leftrightarrow Z_1 \pm Z_2$ и $z_1 z_2 \leftrightarrow Z_1 Z_2$. Кроме того, поскольку единичная матрица коммутирует с любой матрицей того же порядка, ясно, что умножение матриц вида (4.15) коммутативно.

4.47. Поскольку матрица $\mathbb{J}$ кососимметрична, т.е. $\mathbb{J}^T = -\mathbb{J}$, транспонирование матрицы (4.15) приводит к сопряжённому комплексному числу:

$$(x\mathbb{1} + y\mathbb{J})^T = x\mathbb{1}^T + y\mathbb{J}^T = x\mathbb{1} - y\mathbb{J}.$$

Таким образом, если $z \leftrightarrow Z$, то $\bar{z} \leftrightarrow Z^T$.

4.48. Модулю комплексного числа $z = x + iy$ соответствует определитель матрицы $Z = x\mathbb{1} + y\mathbb{J}$; этот факт мы запишем в виде $|z| \leftrightarrow \det Z$.

4.49. Матрица, обратная к (4.15), равна

$$Z^{-1} = \frac{1}{x^2+y^2}\begin{pmatrix} x & y \\ -y & x \end{pmatrix} = \frac{x}{x^2+y^2}\mathbb{1} + \frac{-y}{x^2+y^2}\mathbb{J},$$

что также совпадает по форме с (4.14), т.е. если $z \leftrightarrow Z$, то $z^{-1} \leftrightarrow Z^{-1}$.

4.50. Тригонометрическая форма записи комплексного числа приводит к следующему матричному представлению:

$$z = r(\cos\varphi + i\sin\varphi) \;\leftrightarrow\; Z = r\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}.$$

Геометрический смысл полученной матрицы выяснится в дальнейшем (см. **??**).

Таким образом, мы построили реализацию комплексных чисел в виде вещественных (2×2)-матриц. Построенное взаимно однозначное соответствие между полем $\mathbb{C}$ и множеством матриц вида (4.15) (которое, разумеется, тоже является полем) является *изоморфизмом* (см. определение 3.69, с. 85).

4. Кольца вычетов и поля вычетов

A. Определение колец вычетов.

4.51. Два целых числа x и y называются *сравнимыми по модулю* m, где $m \in \mathbb{N}$, если разность $x - y$ делится на m; обозначение $x \equiv y \pmod m$. Очевидно, $x \equiv y \pmod m$ тогда и только тогда, когда числа x и y при делении на m дают одинаковый остаток.

4.52. Предложение. *Отношение* $\equiv \pmod m$ *сравнимости по модулю является отношением эквивалентности.*

Доказательство. Рефлексивность: $x \equiv x \pmod m$, поскольку $x - x = 0$ делится на m.

Симметричность: $x \equiv y \pmod m$ означает, что $x - y$ делится на m, а потому и $y - x = -(x - y)$ делится на m, т.е. $y \equiv x \pmod m$.

Транзитивность: соотношения $x \equiv y \pmod m$ и $y \equiv z \pmod m$ означают, что числа $x - y$ и $y - z$ делятся на m; но тогда и число $x - z = (x - y) + (y - z)$ также делится на m, т.е. $x \equiv z \pmod m$. □

4.53. Так как при делении целых чисел на m возможные остатки суть $0,\ 1,\ \ldots,\ m-1$ (всего имеется m различных остатков), существует ровно m классов эквивалентности по отношению $\equiv \pmod m$; они называются *классами вычетов* по модулю m. Соответствующее фактор-множество состоит из m элементов (классов вычетов) и обозначается $\mathbb{Z}_m$ или $\mathbb{Z}/m\mathbb{Z}$:

$$\begin{aligned}
[0]_m &= \{x \in \mathbb{Z} \mid x \equiv 0 \pmod m\} = \{0 + mk,\ k \in \mathbb{Z}\},\\
[1]_m &= \{x \in \mathbb{Z} \mid x \equiv 1 \pmod m\} = \{1 + mk,\ k \in \mathbb{Z}\}, \quad \ldots,\\
[m-1]_m &= \{x \in \mathbb{Z} \mid x \equiv m-1 \pmod m\} = \{(m-1) + mk,\ k \in \mathbb{Z}\}.
\end{aligned}$$

(Если модуль сравнения m зафиксирован и в процессе рассуждений не меняется, то для краткости будем писать $[x]$ вместо $[x]_m$.)

4.54. Отметим, что каждый класс эквивалентности может быть обозначен многими разными способами. Например, классы эквивалентности по модулю 2 суть

$$\begin{aligned}
[0]_2 = [2]_2 = [4]_2 = [-2]_2 = [-4]_2 = \ldots,\\
[1]_2 = [3]_2 = [5]_2 = [-1]_2 = [-3]_2 = \ldots,
\end{aligned}$$

а по модулю 3 —

$$\begin{aligned}
[0]_3 = [3]_3 = [6]_3 = [-3]_3 = [-6]_3 = \ldots,\\
[1]_3 = [4]_3 = [7]_3 = [-2]_3 = [-5]_3 = \ldots,\\
[2]_3 = [5]_3 = [8]_3 = [-1]_3 = [-4]_3 = \ldots.
\end{aligned}$$

4.55. Любая совокупность чисел, взятых по одному из каждого класса вычетов, называется *полной системой вычетов* по модулю m. Например, полными системами вычетов по модулю m являются

$$0,\ 1,\ \ldots,\ m-1 \qquad \text{и} \qquad 1,\ 2,\ \ldots,\ m.$$

В случае нечётного модуля, $m = 2k + 1$, одной из возможных полных систем вычетов является

$$-k,\ -k+1,\ \ldots,\ -2,\ -1,\ 0,\ 1,\ 2,\ \ldots,\ k-1,\ k.$$

4.56. Проверим, что введённое отношение эквивалентности согласовано с операциями сложения и умножения на $\mathbb{Z}$. Пусть

$$a \equiv a' \pmod m \quad \Leftrightarrow \quad a - a' = m\alpha \quad \Leftrightarrow \quad a' = a + m\alpha, \quad \alpha \in \mathbb{Z},$$
$$b \equiv b' \pmod m \quad \Leftrightarrow \quad b - b' = m\beta \quad \Leftrightarrow \quad b' = b + m\beta, \quad \beta \in \mathbb{Z}.$$

Складывая последние равенства, получим

$$a' + b' = (a + b) + m(\alpha + \beta) \quad \Leftrightarrow \quad a + b \equiv a' + b' \pmod m.$$

Для умножения проверка аналогична:

$$a'b' = \big(a + m\alpha\big)\big(b + m\beta\big) = ab + m\underbrace{\big(a\beta + b\alpha + m\alpha\beta\big)}_{\in\mathbb{Z}} \equiv ab \pmod m.$$

4.57. Таким образом, на множестве классов эквивалентности $\mathbb{Z}_m$ можно определить операции сложения и умножения элементов:

$$[a] + [b] \stackrel{a+b}{=\!=}, \quad [a] \cdot [b] \stackrel{a\cdot b}{=\!=}, \tag{4.16}$$

после чего оно становится кольцом, называемым *кольцом вычетов* по модулю m.

4.58. ***Кольцо*** $\mathbb{Z}_2$**.** Кольцо вычетов по модулю 2 состоит из двух элементов — [0] и [1], первый из которых представляет собой класс всех чисел, делящихся на 2 без остатка, т.е. из чётных чисел, а второй класс [1] состоит из нечётных чисел. Операции сложения и умножения соответствуют естественным представлениям о сумме и произведении чётных и нечётных чисел, например, сумма двух нечётных чисел есть чётное число ($[1] + [1] = [0]$) и т. д. Таблицы сложения и умножения в кольце $\mathbb{Z}_2$ имеют следующий вид:

$+$	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

,

$\cdot$	[0]	[1]
[0]	[0]	[0]
[1]	[0]	[1]

. (4.17)

Таблица умножения показывает, что ненулевой элемент [1] кольца $\mathbb{Z}_2$ обратим, $[1]^{-1} = [1]$, так что кольцо $\mathbb{Z}_2$ является полем. Это простейший пример конечного поля.

4.59. ***Кольцо*** $\mathbb{Z}_3$**.** Кольцо вычетов по модулю 3 имеет следующие таблицы сложения и умножения:

$+$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

,

$\cdot$	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

. (4.18)

Здесь также ненулевые элементы обратимы:

$$[1]^{-1} = [1], \quad [2]^{-1} = [2],$$

поэтому $\mathbb{Z}_3$ — поле.

4.60. ***Кольцо*** $\mathbb{Z}_4$**.** В кольце вычетов по модулю 4 таблицы сложения и умножения следующие:

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

,

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

. (4.19)

В кольце $\mathbb{Z}_4$ имеются делители нуля: $[2]\cdot[2] = [0]$. Это кольцо полем не является.

Б. Поля вычетов.

4.61. Предложение. *Кольцо вычетов $\mathbb{Z}_m$ является полем тогда и только тогда, когда m — простое число.*

Доказательство. Предположим, что число m — составное, т.е. $m = kl$, где $1 < k, l < m$. Тогда оба класса $[k]_m$ и $[l]_m$ ненулевые, но

$$[k]_m \cdot [l]_m = [kl]_m = [m]_m = [0]_m,$$

т.е. в кольце $\mathbb{Z}_m$ имеются делители нуля, и потому оно не является полем.

Теперь предположим, что число m простое. Пусть $[a]_m \neq [0]_m$, т.е. число a не делится на m. Попытаемся найти обратный элемент для $[a]_m$ подбором, умножая $[a]_m$ по очереди на все элементы кольца. Получим элементы

$$[0]_m,\ [a]_m,\ [2a]_m,\ \ldots,\ [(m-1)a]_m. \tag{4.20}$$

Докажем, что все эти элементы различны. Действительно, если $[ka]_m = [la]_m$, где $0 \leqslant k < l \leqslant m-1$, то $[(l-k)a]_m = 0$, т.е. число $(l-k)a$ делится на m, что невозможно, поскольку ни $l-k$, ни a не делятся на m. Таким образом, в последовательности элементов (4.20) встречаются все элементы кольца $\mathbb{Z}_m$, в том числе $[1]_m$, что означает обратимость элемента $[a]_m$. □

B. Характеристика поля.

4.62. В полях вычетов мы встречаемся с новым явлением, не имевшим места в числовых полях $\mathbb{Q}$ и $\mathbb{R}$: в поле $\mathbb{Z}_p$ (p — простое число) имеет место равенство

$$\underbrace{1+1+\cdots+1}_{p \text{ слагаемых}} = 0.$$

4.63. Определение. Пусть $\mathbb{K}$ — произвольное поле. Наименьшее натуральное число p, для которого в поле $\mathbb{K}$ выполняется равенство

$$\underbrace{1+1+\cdots+1}_{p \text{ слагаемых}} = 0, \tag{4.21}$$

называется *характеристикой* этого поля и обозначается $\operatorname{char}\mathbb{K}$; если такого p не существует, то по определению полагаем $\operatorname{char}\mathbb{K} = 0$.

4.64. Таким образом, поля вычетов $\mathbb{Z}_p$ (p — простое число) имеют характеристику p, а для числовых полей $\operatorname{char}\mathbb{Q} = \operatorname{char}\mathbb{R} = 0$.

4.65. Если $\operatorname{char}\mathbb{K} = p$, то для любого $a \in \mathbb{K}$ имеем

$$\underbrace{a+a+\cdots+a}_{p \text{ слагаемых}} = a \cdot \underbrace{(1+1+\cdots+1)}_{p \text{ слагаемых}} = 0.$$

4.66. В произвольном поле $\mathbb{K}$ определим умножение на натуральное число k как умножение на элемент $\underbrace{1+1+\cdots+1}_{k \text{ слагаемых}}$. Тогда деление на k можно понимать как деление на этот элемент. В случае, когда k делится на характеристику поля, указанный элемент равен нулю и деление невозможно. Например, в поле $\mathbb{Z}_2$ невозможно деление на $2 \overset{1}{=\!=}_2 +[1]_2 = [0]_2$.

4.67. Предложение. *Если характеристика поля не равна нулю, то она является простым числом.*

Доказательство. Пусть $\operatorname{char}\mathbb{K} = p = kl$, где $1 < k, l < n$. Тогда

$$\underbrace{1+1+\cdots+1}_{p \text{ слагаемых}} = \underbrace{(1+1+\cdots+1)}_{k \text{ слагаемых}} \cdot \underbrace{(1+1+\cdots+1)}_{l \text{ слагаемых}} = 0,$$

так что

$$\text{либо } \underbrace{1+1+\cdots+1}_{k \text{ слагаемых}} = 0, \quad \text{либо } \underbrace{1+1+\cdots+1}_{l \text{ слагаемых}} = 0,$$

что противоречит определению характеристики. □

5. Циклические группы

A. Определения.

4.68. В произвольной группе G можно определить степени элемента $a \in G$ с целыми показателями:

$$a^n \stackrel{\text{def}}{=\!=} \begin{cases} \underbrace{a \cdot a \cdot \ldots \cdot a}_{n}, & \text{если } n > 0, \\ e, & \text{если } n = 0, \\ \underbrace{a^{-1}a^{-1} \cdots a^{-1}}_{n}, & \text{если } n < 0. \end{cases}$$

Элементарно доказываются соотношения $a^m x^n = a^{m+n}$ для любых $m, n \in \mathbb{Z}$ и $(a^n)^{-1} = a^{-n}$.

4.69. Предложение. *Все степени произвольного элемента a группы G образуют подгруппу в G, которая называется* циклической подгруппой*, порождённой элементом a. Циклическая подгруппа абелева.*

Доказательство. Поскольку $a^0 = e$ и $a^m a^n = a^{m+n}$, остаётся сослаться на предложение 3.50. □

4.70. Определение. Группа G называется *циклической*, если она порождается одним элементом в том смысле, что существует такой элемент $a \in G$, что любой элемент $b \in G$ может быть представлен в виде $b = a^n$, где $x \in \mathbb{Z}$. Обозначение $G = \langle a \rangle$.

4.71. Возможны два принципиально различных случая: либо все степени элемента a различны, либо нет. В первом случае циклическая группа $G = \langle a \rangle$ бесконечна и изоморфна аддитивной группе $(\mathbb{Z}, +)$; изоморфизм задаётся формулой

$$f : \mathbb{Z} \to G, \quad n \mapsto a^n.$$

4.72. Может оказаться, что $a^k = a^l$, где $k > l$; тогда $a^{k-l} = e$. Наименьшее из натуральных чисел m, для которых $a^m = e$, называется *порядком* элемента a и обозначается $\operatorname{ord} a$. В этом случае циклическую подгруппу, порождённую элементом a, обозначают $\langle a \mid a^m = e \rangle$, что, впрочем, часто сокращают до $\langle a \rangle$, если порядок $\operatorname{ord} x$ ясен из контекста.

4.73. Предложение. *Пусть* $\operatorname{ord} a = m$.

(i) $a^k = e$ *тогда и только тогда, когда* k *делится на* m.
(ii) $a^k = a^l$ *тогда и только тогда, когда* $k - l$ *делится на* m.

(iii) *Подгруппа* $\langle a\rangle$ *содержит* m *элементов*: $\bigl|\langle a\rangle\bigr| = \operatorname{ord} a$, *т.е. порядок циклической подгруппы равен порядку порождающего её элемента.*[1]

(iv) $\operatorname{ord} a^k = \dfrac{m}{\mathit{НОД}(m,k)}$.

(v) *Элемент* a^k *циклической группы* $G = \langle a\rangle$ *порядка* m *является порождающим тогда и только тогда, когда* $\mathit{НОД}(m,k) = 1$.

Доказательство. (i). Выполним деление с остатком числа k на число m: $k = qm + r$, где $0 \leqslant r < m$. По определению $\operatorname{ord} a$ имеем

$$e = a^k = (a^m)^q \cdot a^r = a^r \;\Leftrightarrow\; r = 0.$$

(ii). Согласно только что доказанному

$$a^k = a^l \;\Leftrightarrow\; a^{k-l} = e \;\Leftrightarrow\; k - l \text{ делится на } m.$$

(iii). Действительно, $\langle a\rangle = \{e, a, a^2, \ldots, a^{m-1}\}$.

(iv). Пусть $\text{НОД}(m,k) = d$; тогда $m = m_1 d$ и $k = k_1 d$, так что m_1 и k_1 взаимно просты: $\text{НОД}(m_1, k_1) = 1$. Выясним, для каких натуральных p выполняется соотношение $(a^k)^p = e$. Имеем:

$$(a^k)^p = e \;\Leftrightarrow\; kp \text{ делится на } m \;\Leftrightarrow$$
$$\Leftrightarrow\; k_1 p \text{ делится на } m_1 \;\Leftrightarrow\; p \text{ делится на } m_1.$$

Следовательно, наименьшее натуральное p, для которого $(a^k)^p = e$, равно $m_1 = m/d$, т.е. $\operatorname{ord} a^k = m/\,\text{НОД}(m,k)$.

Утверждение (v) непосредственно вытекает из (iv). □

Б. Примеры циклических групп.

4.74. ***Аддитивная группа*** $(\mathbb{Z}, +)$ является бесконечной циклической группой, $\mathbb{Z} = \langle 1\rangle$.

4.75. ***Аддитивная группа*** $(\mathbb{Z}_m, +)$ ***кольца вычетов по модулю*** m является конечной циклической группой, $\mathbb{Z}_m = \langle [1]\rangle$.

4.76. ***Мультипликативная группа*** C_m ***корней степени*** m ***из единицы*** состоит из комплексных чисел

$$z_k = \exp\frac{2\pi i k}{m} = \cos\frac{2\pi k}{m} + i\sin\frac{2\pi k}{m}, \quad k = 0, 1, \ldots, m-1.$$

Ясно, что $z_k = z_1^k$. Следовательно, $C_m = \langle z_1\rangle$.

[1] Обратите внимание, что здесь слово «порядок» используется в двух различных смыслах (ср. определения 3.37 и 4.72).

Порождающие элементы группы C_m называются *первообразными корнями* m-й степени из единицы. Это корни $z_k = \exp(2\pi ik/m)$, где НОД$(m,k) = 1$. Например, первообразные корни 12-й степени из 1 — это z_1, z_5, z_7, z_{11}.

Поскольку корни m-й степени из 1 изображаются на комплексной плоскости вершинами правильного m-угольника, то C_m является группой вращений, совмещающих этот m-угольник с собой; операцией в этой группе является композиция (последовательное выполнение) вращений. Кроме того, очевидно, что эта же группа состоит из преобразований, совмещающих правильную m-угольную пирамиду с самой собой: все такие преобразования — это повороты пирамиды на углы $2\pi k/m$, $k = 0, 1, \ldots, m-1$, вокруг её оси (высоты).

B. Строение циклических групп и их подгрупп.

4.77. Теорема. *Любая бесконечная циклическая группа изоморфна группе $\mathbb{Z}$. Любая конечная циклическая группа порядка m изоморфна аддитивной группе $\mathbb{Z}_m$.*

Доказательство. Первое утверждение было доказано в п. 4.71. Пусть $G = \langle a\rangle$ — конечная циклическая группа порядка m. Рассмотрим отображение

$$f : \mathbb{Z}_m \to G, \quad [k] \mapsto a^k, \quad k \in \mathbb{Z}.$$

Так как

$$[k] = [l] \;\Leftrightarrow\; k \equiv l \pmod m \;\Leftrightarrow\; a^k = a^l,$$

то отображение f корректно определено и взаимно однозначно. Свойство $f(k+l) = f(k)f(l)$ вытекает из формулы $a^{k+l} = a^k a^l$. Таким образом, f — изоморфизм. □

4.78. Предложение. *Любая подгруппа циклической группы сама является циклической.*

Доказательство. Пусть $G = \langle a\rangle$ — циклическая группа и S — её подгруппа, отличная от e. Ясно, что если $a^{-k} \in S$, $k \in \mathbb{N}$, то $a^k \in S$. Пусть m — наименьшее из натуральных чисел, для которых $a^m \in S$. Докажем, что $S = \langle a^m\rangle$.

Пусть $a^k \in S$. Разделим k на m с остатком: $k = qm + r$, $0 \leqslant r < m$. Тогда

$$a^k = (a^m)^q\, a^r \;\Rightarrow\; a^r = a^k (a^m)^{-q} \in S,$$

откуда в силу определения числа m следует, что $r = 0$, так что $a^k = (a^m)^q$. □

ГЛАВА 5

Векторные пространства

ВЕКТОР в современной математике — также одно из фундаментальных понятий, но, в отличие от понятия матрицы, возникло оно относительно недавно. В элементарной геометрии вектор — это направленный отрезок. Интуитивно вектор понимается как объект, имеющий величину и направление. Естественным образом векторам ставятся в соответствие параллельные переносы, что объясняет сам термин (лат. vector — несущий). Интерпретация вектора как параллельного переноса позволяет ввести операции сложения векторов и умножения векторов на числа, что открывает возможность применять алгебраические методы при решении геометрических задач. Векторы широко используются и в физике: они представляют величины, имеющие помимо численного значения ещё и направление (силы, скорости и т. п.). Если в пространстве задана система координат, то вектор однозначно задаётся набором своих координат. Поэтому упорядоченные наборы чисел тоже называют векторами.

Первые понятия исчисления векторов возникли в рамках геометрической модели комплексных чисел К. Ф. Гаусса. Позже [1] и Г. Грассман[2] разработали алгебраические операции над векторами и некоторые операции векторного анализа. Впоследствии этот формализм использовал Дж. К. Ма́ксвелл[3] в своих трудах по электромагнетизму, тем самым обратив внимание учёных на новое исчисление. Современный вид придал векторному анализу О. Хевисайд[4].

---

[1]Уильям Роуэн Га́мильтон (William Rowan Hamilton; 1805–1865) — ирландский математик и физик.

[2]Герман Гюнтер Грассман (Hermann Günther Grassmann; 1809–1877) — немецкий физик, математик и филолог.

[3]Джеймс Клерк Максвелл (James Clerk Maxwell; 1831–1879) — британский (шотландец по происхождению) физик и математик.

[4]Оливер Хевисайд (Oliver Heaviside; 1850–1925) — английский учёный-самоучка, инженер, математик и физик.

Широкое применение теории векторов объясняется тем, что векторные представления адекватно передают суть многих геометрических и физических понятий и закономерностей. Кроме того, векторные формулы не зависят от выбора той или иной системы координат, т.е. имеют инвариантный характер и отражают сущность явления «в чистом виде». Наконец, в векторных выкладках соединяются наиболее привлекательные черты алгебраического и геометрического методов исследования, благодаря чему векторные формулы отличаются краткостью и наглядностью.

Если принять вектор за основное понятие и зафиксировать в аксиомах свойства операций над векторами, доказанные в рамках элементарной геометрии как теоремы, то получится фундаментальное понятие векторного пространства. В рамках этого абстрактного определения векторами оказываются очень многие математические объекты: функции, матрицы и т. п. Изучением общих алгебраических свойств таких объектов занимается специальный раздел математики — *линейная алгебра*.

1. Определение векторного пространства

A. Определение и примеры.

5.1. Свойства линейных операций над матрицами и над направленными отрезками выглядят совершенно одинаково; это наводит на мысль, что матрицы и векторы являются просто различными реализациями одного и того же абстрактного объекта, а именно, множества с двумя заданными на нём операциями, обладающими идентичными свойствами.

5.2. Определение. *Векторное пространство над полем* $\mathbb{K}$ — это непустое множество $\mathcal{V}$, элементы которого называются *векторами* и обозначаются строчными латинскими буквами жирного начертания: $\boldsymbol{x}, \boldsymbol{y}, \ldots$, на котором заданы две операции:

(a) внутренняя бинарная операция

$$+ : \mathcal{V} \times \mathcal{V} \to \mathbb{K}, \quad (\boldsymbol{x}, \boldsymbol{y}) \mapsto \boldsymbol{x} + \boldsymbol{y},$$

называемая сложением векторов, и

(b) внешняя бинарная операция

$$\bullet : \mathbb{K} \times \mathcal{V} \to \mathcal{V}, \quad (\alpha, \boldsymbol{x}) \mapsto \alpha \cdot \boldsymbol{x} \equiv \alpha\boldsymbol{x},$$

называемая умножением вектора на число,

обладающие следующими свойствами:

ВП1: *коммутативность сложения*:

$$\forall \boldsymbol{x}, \boldsymbol{y} \in \mathcal{V} \quad \boldsymbol{x} + \boldsymbol{y} = \boldsymbol{y} + \boldsymbol{x};$$

ВП2: *ассоциативность сложения*:

$$\forall \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in \mathcal{V} \quad (\boldsymbol{x} + \boldsymbol{y}) + \boldsymbol{z} = \boldsymbol{x} + (\boldsymbol{y} + \boldsymbol{z});$$

ВП3: *существование нулевого вектора*:

$$\exists \mathbf{0} \in \mathcal{V}\ \forall \boldsymbol{x} \in \mathcal{V} \quad \mathbf{0} + \boldsymbol{x} = \boldsymbol{x};$$

ВП4: *существование противоположного вектора*:

$$\forall \boldsymbol{x} \in \mathcal{V}\ \exists -\boldsymbol{x} \in \mathcal{V} \quad \boldsymbol{x} + (-\boldsymbol{x}) = \mathbf{0};$$

ВП5: *свойство единицы*:

$$\forall \boldsymbol{x} \in \mathcal{V} \quad 1 \cdot \boldsymbol{x} = \boldsymbol{x};$$

ВП6: *«ассоциативность»*[1] *умножения на число*:

$$\forall \boldsymbol{x} \in \mathcal{V},\ \forall \alpha, \beta \in \mathbb{R}:\ \big(\alpha \cdot \beta\big) \cdot \boldsymbol{x} = \alpha \cdot \big(\beta \cdot \boldsymbol{x}\big);$$

ВП7: *дистрибутивность относительно сложения векторов*:

$$\forall \boldsymbol{x}, \boldsymbol{y} \in \mathcal{V},\ \forall \alpha \in \mathbb{R}:\ \alpha\big(\boldsymbol{x} + \boldsymbol{y}\big) = \alpha\boldsymbol{x} + \alpha\boldsymbol{y};$$

ВП8: *дистрибутивность относительно сложения чисел*[2]:

$$\forall \boldsymbol{x} \in \mathcal{V},\ \forall \alpha, \beta \in \mathbb{R}:\ \big(\alpha + \beta\big)\boldsymbol{x} = \alpha\boldsymbol{x} + \beta\boldsymbol{x}.$$

Запись $\mathcal{V}(\mathbb{K})$ означает, что $\mathcal{V}$ — векторное пространство над полем $\mathbb{K}$.

5.3. Аксиомы **ВП1**–**ВП4** означают, что векторное пространство является абелевой группой относительно операции сложения векторов.

5.4. ***Нулевое векторное пространство.*** Простейшее векторное пространство состоит из единственного нулевого вектора; будем обозначать его $\{\mathbf{0}\}$.

5.5. ***Пространства направленных отрезков.*** Направленные отрезки позволяют построить несколько различных векторных пространств над полем вещественных чисел: можно рассматривать векторы (направленные отрезки) на прямой (соответствующее векторное пространство будем обозначать $\mathbb{V}_1$), на плоскости ($\mathbb{V}_2$), в пространстве ($\mathbb{V}_3$).

---

[1] См. п. 3.35, с. 77. Обратите внимание, что знак $\cdot$ имеет разный смысл в разных частях этой формулы: в скобках в левой части $\cdot$ обозначает умножение чисел, а во всех остальных случаях — умножение вектора на число.

[2] Здесь также знак $+$ в левой части равенства обозначает сложение чисел, а в правой части — сложение векторов.

5.6. ***Пространство матриц*** $\mathbb{K}^{m\times n}$**.** Множество $\mathbb{K}^{m\times n}$ матриц фиксированного размера (m строк и n столбцов) с элементами из поля $\mathbb{K}$ и обычными линейными операциями является векторным пространством.

5.7. ***Арифметическое пространство*** $\mathbb{K}^n$**.** Частный случай пространства матриц — пространство $\mathbb{K}^n$, элементами которого являются матрицы, состоящие из единственного столбца $(x_1,\dots,x_n)^T$. Аналогичное пространство, элементами которого являются матрицы-строки, обозначаются $\mathbb{K}^{*n}$.

5.8. ***Функциональные векторные пространства.*** Пусть $\mathcal{X}$ — произвольное множество, $\mathcal{F}(\mathcal{X})$ — множество всех функций $f:\mathcal{X}\to\mathbb{R}$, определённых на $\mathcal{X}$ и принимающих значения в $\mathbb{R}$. Определим сумму $f+g$ двух функций f и g и произведение αf функции f на число α «поточечно», т.е. соотношениями

$$\forall x\in\mathcal{X}:\quad (f+g)(x)=f(x)+g(x),\quad (\alpha f)(x)=\alpha\cdot f(x).$$

Аксиомы **ВП1**–**ВП8** проверяются без труда. Таким образом, здесь «векторами» являются функции.

5.9. ***Пространства многочленов.*** В частности, можно рассматривать векторное пространство $\mathbb{K}[t]$, элементами которого являются многочлены от переменной t, а линейные операции заданы, как в примере 5.8. Кроме того, множества $\mathbb{K}[t]_n$ многочленов степени *не выше* n также являются векторными пространствами.[1]

5.10. Рассмотрим пространство, векторами которого являются положительные вещественные числа; положительное вещественное число x, рассматриваемое как вектор нашего пространства, будем обозначать $\boldsymbol{x}$. Сложение векторов $\boldsymbol{x}$ и $\boldsymbol{y}$ (будем обозначать его знаком $\boxplus$) определим как умножение соответствующих положительных чисел:

$$\boldsymbol{x}\boxplus\boldsymbol{y}\stackrel{\text{def}}{=\!=}x\cdot y,$$

а умножение вектора $\boldsymbol{x}$ на число α (обозначаем его знаком $\boxdot$) — как возведение положительного числа x в степень α:

$$\alpha\boxdot\boldsymbol{x}\stackrel{\text{def}}{=\!=}x^{\alpha}.$$

Читателю предлагается проверить выполнение аксиом **ВП1**–**ВП8** самостоятельно. Этот пример показывает, что операции сложения векторов и умножения вектора на число в абстрактном векторном пространстве могут совершенно не соответствовать интуитивному

[1] Объясните, почему множество многочленов степени, *равной* n, *не* является векторным пространством.

представлению об этих операциях, инспирированному их названиями.

Б. Простейшие следствия аксиом векторного пространства.

5.11. Предложение.

(i) *Нулевой вектор* $\mathbf{0} \in \mathcal{V}$ *единствен.*
(ii) *Для любого вектора* $\boldsymbol{x} \in \mathcal{V}$ *противоположный вектор* $-\boldsymbol{x}$ *единствен.*
(iii) *Для любых двух векторов* $\boldsymbol{a}, \boldsymbol{b} \in \mathcal{V}$ *уравнение* $\boldsymbol{a}+\boldsymbol{x} = \boldsymbol{b}$ *имеет единственное решение* $\boldsymbol{x} = \boldsymbol{b} + (-\boldsymbol{a})$, *что кратко записывается в виде* $\boldsymbol{x} = \boldsymbol{b} - \boldsymbol{a}$.
(iv) *Для любого вектора* $\boldsymbol{x} \in \mathcal{V}$ *имеем* $0 \cdot \boldsymbol{x} = \mathbf{0}$.
(v) *Для любого вектора* $\boldsymbol{x} \in \mathcal{V}$ *его противоположный* $-\boldsymbol{x}$ *выражается формулой* $-\boldsymbol{x} = (-1) \cdot \boldsymbol{x}$.
(vi) *Для любого вектора* $\boldsymbol{x} \in \mathcal{V}$ *и любого числа* $\alpha \in \mathbb{K}$ *имеют место соотношения* $-(\alpha \cdot \boldsymbol{x}) = (-\alpha) \cdot \boldsymbol{x} = \alpha \cdot (-\boldsymbol{x})$.
(vii) *Для любого числа* $\alpha \in \mathbb{K}$ *имеем* $\alpha \cdot \mathbf{0} = \mathbf{0}$.

Доказательство. Утверждения (i)–(iii) являются переформулировками предложений 3.22, 3.27 и 3.28 для векторных пространств.

(iv). Из цепочки равенств

$$\boldsymbol{x} + 0 \cdot \boldsymbol{x} \overset{\text{ВП5}}{=\!=} 1 \cdot \boldsymbol{x} + 0 \cdot \boldsymbol{x} \overset{\text{ВП8}}{=\!=} (1+0) \cdot \boldsymbol{x} = 1 \cdot \boldsymbol{x} \overset{\text{ВП5}}{=\!=} \boldsymbol{x}$$

следует, что $0 \cdot \boldsymbol{x} = \mathbf{0}$.

(v). Аналогично предыдущему, имеем

$$(-1) \cdot \boldsymbol{x} + \boldsymbol{x} \overset{\text{ВП5}}{=\!=} (-1) \cdot \boldsymbol{x} + 1 \cdot \boldsymbol{x} \overset{\text{ВП8}}{=\!=} (-1+1) \cdot \boldsymbol{x} = 0 \cdot \boldsymbol{x} \overset{\text{п. 4}}{=\!=} \mathbf{0},$$

т.е. $(-1) \cdot \boldsymbol{x}$ — вектор, противоположный $\boldsymbol{x}$.

(vi). Имеем

$$-(\alpha\boldsymbol{x}) \overset{\text{п. 5}}{=\!=} (-1) \cdot (\alpha\boldsymbol{x}) \overset{\text{ВП6}}{=\!=} (-1 \cdot \alpha) \cdot \boldsymbol{x} = (-\alpha) \cdot \boldsymbol{x},$$

$$-(\alpha\boldsymbol{x}) \overset{\text{п. 5}}{=\!=} (-1) \cdot (\alpha\boldsymbol{x}) \overset{\text{ВП6}}{=\!=} (-1 \cdot \alpha) \cdot \boldsymbol{x} =$$

$$= \big(\alpha \cdot (-1)\big) \cdot \boldsymbol{x} \overset{\text{ВП6}}{=\!=} \alpha \cdot \big((-1) \cdot \boldsymbol{x}\big) \overset{\text{п. 5}}{=\!=} \alpha \cdot (-\boldsymbol{x}).$$

(vii). Имеем

$$\alpha \cdot \boldsymbol{x} + \alpha \cdot \mathbf{0} \overset{\text{ВП7}}{=\!=} \alpha \cdot (\boldsymbol{x} + \mathbf{0}) \overset{\text{ВП3}}{=\!=} \alpha \cdot \boldsymbol{x} \quad \Rightarrow \quad \alpha \cdot \mathbf{0} = \mathbf{0}. \qquad \square$$

2. Подпространства и линейные оболочки

А. Линейные комбинации.

5.12. Определение. Пусть дано семейство векторов $\boldsymbol{x}_1$, $\boldsymbol{x}_2$, …, $\boldsymbol{x}_r \in \mathcal{V}(\mathbb{K})$ и семейство чисел α_1, α_2, …, $\alpha_r \in \mathbb{K}$. *Линейной комбинацией* векторов $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_r$ с коэффициентами $\alpha_1, \alpha_2, \ldots, \alpha_r$ называется вектор

$$\alpha_1\boldsymbol{x}_1 + \alpha_2\boldsymbol{x}_2 + \cdots + \alpha_r\boldsymbol{x}_r \equiv \sum_{k=1}^{r} \alpha_k\boldsymbol{x}_k; \tag{5.1}$$

про этот вектор будем говорить, что он *линейно выражается* через векторы $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_r$.

5.13. Операция сложения векторов является *бинарной*, т.е. позволяет говорить лишь о сумме *двух* векторов. Однако определение 5.12 линейной комбинации корректно благодаря ассоциативности операции сложения векторов (см. п. 3.13 и предложение 3.14, с. 71).

5.14. Линейная комбинация называется *тривиальной*, если все её коэффициенты равны нулю:

$$\alpha_1 = \alpha_2 = \cdots = \alpha_r = 0.$$

Ясно, что тривиальная линейная комбинация произвольных векторов равна нулевому вектору.

5.15. Мы не будем рассматривать линейные комбинации бесконечных последовательностей векторов. Для того чтобы можно было говорить о бесконечных линейных комбинациях, нужно сначала определить понятие суммы бесконечного числа слагаемых; эти вопросы выходят за рамки линейной алгебры и рассматриваются в курсе функционального анализа.

Б. Линейные оболочки.

5.16. Определение. *Линейной оболочкой* векторов $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r$ называется множество всех линейных комбинаций этих векторов:

$$L(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r) \stackrel{\text{def}}{=\!=} \Big\{ \alpha_1\boldsymbol{x}_1 + \cdots + \alpha_r\boldsymbol{x}_r \;\Big|\; \alpha_1, \ldots, \alpha_r \in \mathbb{K} \Big\}.$$

Например, линейная оболочка двух не параллельных направленных отрезков $\boldsymbol{a}$ и $\boldsymbol{b}$ состоит из всех направленных отрезков, лежащих в одной плоскости с $\boldsymbol{a}$ и $\boldsymbol{b}$ (или параллельных этой плоскости).

5.17. Предложение (транзитивность линейной комбинации)**.** *Пусть векторы* $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_p$ *принадлежат линейной оболочке векторов* $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_q$*. Тогда*

$$L(\boldsymbol{y}_1, \ldots, \boldsymbol{y}_p) \subset L(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_q).$$

Иными словами, если вектор $\boldsymbol{x}$ *линейно выражается через векторы* $\boldsymbol{y}_1, \ldots \boldsymbol{y}_p$*, каждый из которых, в свою очередь, линейно выражается через векторы* $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_q$*, то* $\boldsymbol{x}$ *линейно выражается через* $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_q$*.*

Доказательство. Убедимся, что любой вектор $\boldsymbol{x}$, лежащий в линейной оболочке $L(\boldsymbol{y}_1, \ldots, \boldsymbol{y}_p)$, лежит также и в $L(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_q)$. Итак, пусть $\boldsymbol{x} \in L(\boldsymbol{y}_1, \ldots, \boldsymbol{y}_p)$, т.е.

$$\boldsymbol{x} = \beta_1 \boldsymbol{y}_1 + \cdots + \beta_p \boldsymbol{y}_p.$$

Поскольку $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_p \in L(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_q)$, имеем

$$\boldsymbol{y}_1 = \alpha_{11}\boldsymbol{x}_1 + \cdots + \alpha_{1q}\boldsymbol{x}_q, \quad \ldots, \quad \boldsymbol{y}_p = \alpha_{p1}\boldsymbol{x}_1 + \cdots + \alpha_{pq}\boldsymbol{x}_q.$$

Таким образом,

$$\begin{aligned}\boldsymbol{x} &= \beta_1 \boldsymbol{y}_1 + \cdots + \beta_p \boldsymbol{y}_p = \\ &= \beta_1\big(\alpha_{11}\boldsymbol{x}_1 + \cdots + \alpha_{1q}\boldsymbol{x}_q\big) + \cdots + \beta_p\big(\alpha_{p1}\boldsymbol{x}_1 + \cdots + \alpha_{pq}\boldsymbol{x}_q\big) = \\ &= \big(\beta_1\alpha_{11} + \cdots + \beta_p\alpha_{p1}\big)\boldsymbol{x}_1 + \cdots + \big(\beta_1\alpha_{1q} + \cdots + \beta_p\alpha_{pq}\big)\boldsymbol{x}_q,\end{aligned}$$

а это означает, что $\boldsymbol{x} \in L(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_q)$, т.е.

$$L(\boldsymbol{y}_1, \ldots, \boldsymbol{y}_p) \subset L(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_q). \qquad \square$$

B. Подпространства.

5.18. Подпространства векторного пространства — это подмножества, замкнутые относительно операции сложения векторов и умножения на произвольные числа. Точное определение таково.

5.19. Определение. Подмножество $\mathcal{P}$ векторного пространства $\mathcal{V}$ называется *подпространством*, если для любых векторов $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{P}$ их произвольная линейная комбинация $\alpha\boldsymbol{x} + \beta\boldsymbol{y}$ также принадлежит этому множеству:

$$\forall \boldsymbol{x}, \boldsymbol{y} \in \mathcal{P},\ \forall \alpha, \beta \in \mathbb{K} \quad \alpha\boldsymbol{x} + \beta\boldsymbol{y} \in \mathcal{P}.$$

Запись $\mathcal{P} \Subset \mathcal{V}$ означает, что $\mathcal{P}$ является подпространством в $\mathcal{V}$; запись $A \subset \mathcal{V}$ означает, что A является подмножеством в $\mathcal{V}$ (не обязательно подпространством).

5.20. Очевидно, само пространство $\mathcal{V}$ и множество $\{\mathbf{0}\}$, состоящее из одного нулевого вектора, являются подпространствами; они называются *тривиальными* подпространствами.

5.21. Каждое подпространство $\mathcal{P}$ произвольного векторного пространства $\mathcal{V}$ само является векторным пространством.

5.22. Примеры.

1. Для пространств направленных отрезков имеем $\mathbb{V}_1 \Subset \mathbb{V}_2 \Subset \mathbb{V}_3$.
2. Подмножество в $\mathbb{K}^n$, состоящее из всех столбцов, первый элемент которых равен нулю, образует подпространство в $\mathbb{K}^n$. Подмножество же, состоящее из столбцов, первый элемент которых равен 1, подпространством не является.
3. Подмножество в $\mathbb{K}^n$, состоящее из всех решений однородной линейной системы $AX = O$, является подпространством в $\mathbb{K}^n$ в силу принципа суперпозиции для однородных систем.
4. Подмножество $C(\mathcal{X})$, состоящее из функций, непрерывных на открытом числовом множестве $\mathcal{X} \subset \mathbb{R}$, является подпространством в векторном пространстве $\mathcal{F}(\mathcal{X})$ всех функций, определённых на $\mathcal{X}$: $C(\mathcal{X}) \Subset \mathcal{F}(\mathcal{X})$. Аналогично, подмножество $C^1(\mathcal{X})$, состоящее из функций, имеющих непрерывную производную в любой точке $x \in \mathcal{X}$, является подпространством в $C(\mathcal{X})$: $C^1(\mathcal{X}) \Subset C(\mathcal{X}) \Subset \mathcal{F}(\mathcal{X})$.
5. Векторное пространство $\mathbb{R}[t]$, состоящее из всех многочленов от переменной t, является подпространством векторного пространства $\mathcal{F}(\mathbb{R})$ всех функций, определённых на всей вещественной оси: $\mathbb{R}[t] \Subset \mathcal{F}(\mathbb{R})$.
6. Векторное пространство $\mathbb{K}[t]_n$, состоящее из всех многочленов степени не выше n от переменной t, является подпространством векторного пространства $\mathbb{K}[t]_m$, где $m > n$; таким образом,

$$\mathbb{K} = \mathbb{K}[t]_0 \Subset \mathbb{K}[t]_1 \Subset \mathbb{K}[t]_2 \Subset \cdots \Subset \mathbb{K}[t].$$

5.23. Теорема. *Линейная оболочка $L(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r)$ произвольных векторов $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r$ векторного пространства $\mathcal{V}$ является подпространством в $\mathcal{V}$.*

Доказательство. Рассмотрим произвольные векторы $\boldsymbol{y}$ и $\boldsymbol{z}$ из указанной линейной оболочки; эти векторы линейно выражаются следующим образом:

$$\boldsymbol{y} = \sum_{k=1}^{r} \alpha_k \boldsymbol{x}_k, \quad \boldsymbol{z} = \sum_{k=1}^{r} \beta_k \boldsymbol{x}_k,$$

где α_k, β_k — некоторые числа. Рассмотрим произвольную линейную комбинацию векторов $\boldsymbol{y}$ и $\boldsymbol{z}$ и убедимся, что она также лежит в

линейной оболочке $L(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r)$:

$$\alpha\boldsymbol{y} + \beta\boldsymbol{z} = \alpha\left(\sum_{k=1}^{r} \alpha_k \boldsymbol{x}_k\right) + \beta\left(\sum_{k=1}^{r} \beta_k \boldsymbol{x}_k\right) = \sum_{k=1}^{r} (\alpha\alpha_k + \beta\beta_k)\boldsymbol{x}_k. \quad \square$$

Г. Способы задания подпространств в $\mathbb{K}^n$.

5.24. Фактически существуют всего два способа задать подпространство в $\mathbb{K}^n$:

(i) либо как линейную оболочку некоторого семейства столбцов (теорема 5.23),

(ii) либо как множество решений некоторой однородной системы линейных уравнений.

5.25. Чтобы перейти от задания подпространства способом (i) к заданию способом (ii), нужно составить однородную систему уравнений, имеющую заданное множество решений.

5.26. Чтобы перейти от задания подпространства способом (ii) к заданию способом (i), требуется решить заданную систему однородных уравнений.

Д. Пересечение и сумма подпространств.

5.27. Предложение. *Пересечение $\mathcal{P} \cap \mathcal{Q}$ двух подпространств $\mathcal{P}$ и $\mathcal{Q}$ произвольного векторного пространства $\mathcal{V}$ само является подпространством в $\mathcal{V}$.*

Доказательство. Для произвольных векторов $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{P} \cap \mathcal{Q}$ и произвольных чисел $\alpha, \beta \in \mathbb{K}$ имеем:

$$\begin{aligned} \boldsymbol{x}, \boldsymbol{y} \in \mathcal{P} \cap \mathcal{Q} &\Rightarrow (\boldsymbol{x}, \boldsymbol{y} \in \mathcal{P}) \wedge (\boldsymbol{x}, \boldsymbol{y} \in \mathcal{Q}) \Rightarrow \\ &\Rightarrow (\alpha\boldsymbol{x} + \beta\boldsymbol{y} \in \mathcal{P}) \wedge (\alpha\boldsymbol{x} + \beta\boldsymbol{y} \in \mathcal{Q}) \Rightarrow \alpha\boldsymbol{x} + \beta\boldsymbol{y} \in \mathcal{P} \cap \mathcal{Q}. \quad \square \end{aligned}$$

5.28. Объединение подпространств, вообще говоря, подпространством не является. Действительно, пусть

$$\mathcal{P} = L\left(\begin{pmatrix}1\\0\end{pmatrix}\right), \quad \mathcal{Q} = L\left(\begin{pmatrix}0\\1\end{pmatrix}\right), \quad \mathcal{P} \cup \mathcal{Q} = \left\{\begin{pmatrix}\alpha\\0\end{pmatrix}, \begin{pmatrix}0\\\beta\end{pmatrix} \;\middle|\; \alpha, \beta \in \mathbb{K}\right\}.$$

Сумма векторов $(1;0)^T$ и $(0;1)^T$, принадлежащих множеству $\mathcal{P} \cup \mathcal{Q}$, равна $(1;1)^T$ и не принадлежит $\mathcal{P} \cup \mathcal{Q}$.

5.29. Определение. Пусть $\mathcal{P}$, $\mathcal{Q}$ — подпространства векторного пространства $\mathcal{V}$. *Суммой* $\mathcal{P}+\mathcal{Q}$ подпространств $\mathcal{P}$ и $\mathcal{Q}$ называется множество

$$\mathcal{P}+\mathcal{Q} \stackrel{\text{def}}{=\!=} \Big\{ \boldsymbol{x}+\boldsymbol{y} \;\Big|\; \boldsymbol{x}\in\mathcal{P},\ \boldsymbol{y}\in\mathcal{Q} \Big\}.$$

5.30. Предложение. *Сумма $\mathcal{P}+\mathcal{Q}$ подпространств $\mathcal{P}$, $\mathcal{Q}$ векторного пространства $\mathcal{V}$ является подпространством в $\mathcal{V}$.*

Доказательство. Для любых векторов $\boldsymbol{u},\boldsymbol{v} \in \mathcal{P}+\mathcal{Q}$ имеем $\boldsymbol{u}=\boldsymbol{x}_1+\boldsymbol{y}_1$ и $\boldsymbol{v}=\boldsymbol{x}_2+\boldsymbol{y}_2$, где $\boldsymbol{x}_1,\boldsymbol{x}_2\in\mathcal{P}$, $\boldsymbol{y}_1,\boldsymbol{y}_2\in\mathcal{Q}$. Для любых чисел $\alpha,\beta\in\mathbb{K}$ имеем

$$\begin{aligned}\alpha\boldsymbol{u}+\beta\boldsymbol{v} &= \alpha(\boldsymbol{x}_1+\boldsymbol{y}_1)+\beta(\boldsymbol{x}_2+\boldsymbol{y}_2) = \\ &= \underbrace{(\alpha\boldsymbol{x}_1+\beta\boldsymbol{x}_2)}_{\in\mathcal{P}} + \underbrace{(\alpha\boldsymbol{y}_1+\beta\boldsymbol{y}_2)}_{\in\mathcal{Q}} \in \mathcal{P}+\mathcal{Q}.\end{aligned}$$ □

3. Линейная зависимость и независимость

A. Линейно зависимые и линейно независимые семейства векторов.

5.31. Определение. Семейство векторов $\boldsymbol{x}_1,\dots,\boldsymbol{x}_r$ называется *линейно зависимым*, если существует нетривиальная линейная комбинация этих векторов, равная нулевому вектору.

Семейство векторов $\boldsymbol{x}_1,\dots,\boldsymbol{x}_r$ называется *линейно независимым*, если равенство линейной комбинации этих векторов нулевому вектору возможно лишь в том случае, если эта линейная комбинация тривиальна.

5.32. Подчеркнём, что понятие линейной зависимости или независимости относится не к отдельным векторам, а к их *семействам* (упорядоченным наборам). Заметим, однако, что свойство семейства векторов быть линейно зависимым или линейно независимым не зависит от нумерации векторов в нём. Допуская некоторую вольность формулировок, часто говорят не о «линейно зависимых (независимых) семействах векторов», а о «линейно зависимых (независимых) векторах».

5.33. Примеры.

1. В векторном пространстве $\{\mathbf{0}\}$ нет линейно независимых семейств: любое семейство векторов этого пространства (состоящее, разумеется, лишь из нулевых векторов) линейно зависимо.

2. Если в векторном пространстве $\mathcal{V}$ имеется ненулевой вектор $\boldsymbol{x}$, то одноэлементное семейство $(\boldsymbol{x})$ линейно независимо, а двухэлементное семейство $(\boldsymbol{x}, -\boldsymbol{x})$ линейно зависимо.
3. На прямой $\mathbb{V}_1$ любой ненулевой направленный отрезок образует линейно независимое семейство, а любые два направленных отрезка линейно зависимы.
4. На плоскости $\mathbb{V}_2$ любые два ненулевых непараллельных направленных отрезка линейно независимы, а любые три направленных отрезка линейно зависимы.
5. В пространстве $\mathbb{V}_3$ любые три ненулевых направленных отрезка, не параллельных одной плоскости, линейно независимы, а любые четыре направленных отрезка линейно зависимы.
6. В пространстве $\mathbb{K}[t]$ всех многочленов с коэффициентами из поля $\mathbb{K}$ многочлены 1, t, t^2, $\ldots$, t^n линейно независимы при любом $n \in \mathbb{N}$.

5.34. Ясно, что множество векторов, состоящее из единственного элемента, линейно независимо тогда и только тогда, когда оно состоит из ненулевого вектора. Действительно, если $\boldsymbol{a} \neq \boldsymbol{0}$, то равенство $\alpha\boldsymbol{a} = \boldsymbol{0}$ возможно лишь при $\alpha = 0$. Линейно зависимое семейство двух векторов называется *коллинеарным*, а трёх — *компланарным*; про сами векторы, образующие такие семейства, также говорят, что они коллинеарны (соответственно, компланарны).

5.35. Векторы $\boldsymbol{a}$ и $\boldsymbol{b}$ коллинеарны тогда и только тогда, когда один из них линейно выражается через другой, т.е. эти векторы пропорциональны и, следовательно, — в наглядных геометрических терминах — параллельны одной и той же прямой.

Компланарность векторов $\boldsymbol{a}$, $\boldsymbol{b}$ и $\boldsymbol{c}$ означает, что один из них может быть линейно выражен через два других, например, $\boldsymbol{c} = \alpha\boldsymbol{a} + \beta\boldsymbol{b}$; с наглядно-геометрической точки зрения это означает, что вектор $\boldsymbol{c}$ лежит в одной плоскости с векторами $\boldsymbol{a}$ и $\boldsymbol{b}$.

Б. Свойства линейно зависимых и линейно независимых семейств векторов.

5.36. Теорема.

1. *Любое семейство с повторениями*[1] *линейно зависимо.*
2. *Если в семействе векторов* $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r$ *имеется нулевой вектор* $\boldsymbol{0}$*, то это семейство линейно зависимо.*
3. *Семейство векторов* $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r$ *линейно зависимо тогда и только тогда, когда хотя бы один из этих векторов можно представить в виде линейной комбинации остальных.*

[1] Это означает, что среди членов семейства имеются одинаковые.

4. *Если в семействе векторов* $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r, \boldsymbol{x}_{r+1}, \ldots, \boldsymbol{x}_s$ *имеется линейно зависимое подсемейство* $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r$*, то и всё семейство также линейно зависимо.*
5. *Любое подсемейство линейно независимого семейства векторов является линейно независимым.*
6. *Если семейство векторов* $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r$ *линейно независимо, а семейство векторов* $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r, \boldsymbol{x}$ *линейно зависимо, то* $\boldsymbol{x}$ *является линейной комбинацией векторов* $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r$*.*
7. *Если семейство векторов* $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r$ *линейно независимо, а вектор* $\boldsymbol{x}$ *нельзя через них выразить, то семейство векторов* $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r, \boldsymbol{x}$ *также линейно независимо.*

Доказательство. 1. Пусть, например, в семействе векторов $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r$ первый и второй векторы совпадают, $\boldsymbol{x}_1 = \boldsymbol{x}_2$. Тогда нетривиальная линейная комбинация

$$1 \cdot \boldsymbol{x}_1 + (-1) \cdot \boldsymbol{x}_2 + 0 \cdot \boldsymbol{x}_3 + \cdots + 0 \cdot \boldsymbol{x}_r$$

равна нулевому вектору.

2. Пусть в семействе векторов $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r$ один вектор нулевой, например, $\boldsymbol{x}_r = \boldsymbol{0}$. Нетривиальная линейная комбинация

$$0 \cdot \boldsymbol{x}_1 + 0 \cdot \boldsymbol{x}_2 + \cdots + 1 \cdot \boldsymbol{x}_r$$

равна, очевидно, нулевому вектору.

3. Пусть семейство векторов $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r$ линейно зависимо; тогда существует их нетривиальная линейная комбинация, равная нулевому вектору:

$$\alpha_1 \boldsymbol{x}_1 + \cdots + \alpha_r \boldsymbol{x}_r = \boldsymbol{0}.$$

Среди коэффициентов этой линейной комбинации имеются ненулевые; для определённости будем считать, что $\alpha_r \neq 0$; тогда

$$\boldsymbol{x}_r = -\frac{\alpha_1}{\alpha_r}\boldsymbol{x}_1 - \cdots - \frac{\alpha_{r-1}}{\alpha_r}\boldsymbol{x}_{r-1},$$

что и требовалось. Обратно, если

$$\boldsymbol{x}_r = \beta_1 \boldsymbol{x}_1 + \cdots + \beta_{r-1}\boldsymbol{x}_{r-1},$$

то

$$(-1)\boldsymbol{x}_r + \beta_1 \boldsymbol{x}_1 + \cdots + \beta_{r-1}\boldsymbol{x}_{r-1} = \boldsymbol{0};$$

это нетривиальная линейная комбинация, равная нулевому вектору, т.е. семейство $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r$ линейно зависимо.

4. Если подсемейство $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r$ линейно зависимо, то существует линейная комбинация

$$\alpha_1 \boldsymbol{x}_1 + \cdots + \alpha_r \boldsymbol{x}_r = \boldsymbol{0},$$

в которой имеется хотя бы один ненулевой коэффициент. Если теперь к этой линейной комбинации добавить тривиальную линейную комбинацию векторов $\boldsymbol{x}_{r+1}, \ldots, \boldsymbol{x}_s$, то получится нетривиальная линейная комбинация

$$\overbrace{\underbrace{\alpha_1\boldsymbol{x}_1 + \cdots + \alpha_r\boldsymbol{x}_r}_{\text{нетрив. л.к.}} + \underbrace{0\cdot\boldsymbol{x}_{r+1} + \ldots 0\cdot\boldsymbol{x}_s}_{\text{трив. л.к.}}}^{\text{нетрив. л.к.}} = \mathbf{0},$$

что и требовалось.

Утверждение 5 непосредственно следует из предыдущего по контрапозиции.

6. Поскольку семейство векторов $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r, \boldsymbol{x}$ линейно зависимо, выполняется соотношение

$$\alpha_1\boldsymbol{x}_1 + \cdots + \alpha_r\boldsymbol{x}_r + \alpha\boldsymbol{x} = \mathbf{0}. \tag{5.2}$$

Докажем, что $\alpha \neq 0$. Действительно, в противном случае получим

$$\alpha_1\boldsymbol{x}_1 + \cdots + \alpha_r\boldsymbol{x}_r = \mathbf{0}$$

и, следовательно, $\alpha_1 = \cdots = \alpha_r = 0$ в силу линейной независимости семейства векторов $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r$. Значит, равенство (5.2) выполняется лишь при нулевых значениях всех коэффициентов, что противоречит линейной зависимости семейства векторов $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r, \boldsymbol{x}$. Итак, в (5.2) имеем $\alpha \neq 0$, откуда

$$\boldsymbol{x} = -\frac{\alpha_1}{\alpha}\boldsymbol{x}_1 - \cdots - \frac{\alpha_r}{\alpha}\boldsymbol{x}_r.$$

Утверждение 7 непосредственно следует из предыдущего по контрапозиции. □

Следующий факт о линейной зависимости векторов менее очевиден.

5.37. Теорема. *Если векторы $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_s$ принадлежат линейной оболочке $L(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r)$ и $s > r$, то они линейно зависимы.*

Доказательство. Каждый из векторов $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_s$ можно представить в виде линейной комбинации векторов $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r$:

$$\begin{aligned}
\boldsymbol{y}_1 &= a_1^1\boldsymbol{x}_1 + a_1^2\boldsymbol{x}_2 + \cdots + a_1^r\boldsymbol{x}_r,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\boldsymbol{y}_s &= a_s^1\boldsymbol{x}_1 + a_s^2\boldsymbol{x}_2 + \cdots + a_s^r\boldsymbol{x}_r,
\end{aligned}$$

где a_j^i — некоторые числа. Введя в рассмотрение матрицы[1]

$$\underset{1\times s}{\boldsymbol{Y}} = \big\|\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_s\big\|, \qquad \underset{r\times s}{A} = \begin{pmatrix} a_1^1 & a_2^1 & \ldots & a_s^1 \\ a_1^2 & a_2^2 & \ldots & a_s^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^r & a_2^r & \ldots & a_s^r \end{pmatrix},$$

$$\underset{1\times r}{\boldsymbol{X}} = \big\|\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_r\big\|,$$

мы можем записать эти равенства в виде одного матричного соотношения

$$\boldsymbol{Y} = \boldsymbol{X}A. \tag{5.3}$$

Рассмотрим следующую систему r однородных линейных уравнений с s неизвестными:

$$\begin{cases} a_1^1 z^1 + a_2^1 z^2 + \cdots + a_s^1 z^s = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_1^r z^1 + a_2^r z^2 + \cdots + a_s^r z^s = 0 \end{cases} \quad \Leftrightarrow \quad AZ = O, \quad \text{где } Z = \begin{pmatrix} z^1 \\ z^2 \\ \vdots \\ z^s \end{pmatrix}.$$

Поскольку по условию $s > r$, т.е. количество неизвестных превышает количество уравнений, согласно предложению **??** (см. с. **??**) эта однородная система имеет нетривиальное решение $Z_0 = (z_0^1, z_0^2, \ldots, z_0^s)^T$. Составим линейную комбинацию векторов $Y_1, \ldots, Y_s$ с коэффициентами $z_0^1, z_0^2, \ldots, z_0^s$:

$$z_0^1 Y_1 + z_0^2 Y_2 + \cdots + z_0^s Y_s \equiv \boldsymbol{Y} Z_0.$$

В силу (5.3) имеем

$$\boldsymbol{Y}Z_0 = (\boldsymbol{X}A)Z_0 = \boldsymbol{X}(AZ_0) = \boldsymbol{X}O = \boldsymbol{0},$$

что и доказывает линейную зависимость векторов $Y_1, \ldots, Y_s$. □

Контрапозицией теоремы 5.37 является следующая теорема.

5.38. Теорема. *Если векторы $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_s$, принадлежащие линейной оболочке $L(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r)$, линейно независимы, то $s \leqslant r$.*

Доказательство. Теорема 5.38 допускает прямое доказательство, не опирающееся на теорию линейных систем.

Применим метод математической индукции по числу r. При $r = 1$ утверждение очевидно: если векторы $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_s$ принадлежат линейной оболочке $L(\boldsymbol{x}_1)$, то они пропорциональны вектору $\boldsymbol{x}_1$, а следовательно и между собой, и потому линейно независимое семейство могут образовывать только если их не более одного, т.е. $s = 1$.

[1] Обратите внимание, что коэффициенты разложения вектора $\boldsymbol{y}_1$ располагаются в первом столбце, а не в первой строке матрицы A (для остальных векторов аналогично).

Предположим, что утверждение теоремы верно для $r-1$ векторов $\boldsymbol{x}_1,\dots,\boldsymbol{x}_{r-1}$, и докажем его справедливость для случая r векторов. Итак, пусть в линейной оболочке $L(\boldsymbol{x}_1,\dots,\boldsymbol{x}_r)$ имеются линейно независимые векторы

$$\boldsymbol{y}_1=a_1^1\boldsymbol{x}_1+\dots+a_1^r\boldsymbol{x}_r,\quad\dots,\quad\boldsymbol{y}_s=a_s^1\boldsymbol{x}_1+\dots+a_s^r\boldsymbol{x}_r. \tag{5.4}$$

Требуется доказать, что $s\leqslant r$.

Если все коэффициенты при $\boldsymbol{x}_r$ равны нулю, то утверждение доказано, поскольку в этом случае, по предположению индукции, имеем $s\leqslant r-1$, так что подавно $s\leqslant r$.

Предположим, что хотя бы один из коэффициентов при $\boldsymbol{x}_r$ отличен от нуля, например, a_s^r. Выразим из последнего равенства (5.4) вектор $\boldsymbol{x}_r$:

$$\boldsymbol{x}_r=\frac{1}{a_s^r}\boldsymbol{y}_s-\frac{a_s^1}{a_s^r}\boldsymbol{x}_1-\dots-\frac{a_s^{r-1}}{a_s^r}\boldsymbol{x}_{r-1}.$$

Подставляя полученное выражение в каждое из предыдущих равенств (5.4), приводя подобные слагаемые и обозначая образующиеся коэффициенты буквой b с индексами, получаем следующие равенства:

$$\boldsymbol{y}_1-\frac{a_1^r}{a_s^r}\boldsymbol{y}_s=b_1^1\boldsymbol{x}_1+\dots+b_1^{r-1}\boldsymbol{x}_{r-1},\quad\dots,\quad\boldsymbol{y}_{s-1}-\frac{a_{s-1}^r}{a_s^r}\boldsymbol{y}_s=b_{s-1}^1\boldsymbol{x}_1+\dots+b_{s-1}^{r-1}\boldsymbol{x}_{r-1}.$$

Эти равенства означают, что векторы

$$\boldsymbol{y}_1'=\boldsymbol{y}_1-\frac{a_1^r}{a_s^r}\boldsymbol{y}_s,\quad\dots,\quad\boldsymbol{y}_{s-1}'=\boldsymbol{y}_{s-1}-\frac{a_{s-1}^r}{a_s^r}\boldsymbol{y}_s$$

принадлежат линейной оболочке $L(\boldsymbol{x}_1,\dots,\boldsymbol{x}_{r-1})$. Если мы установим, что они линейно независимы, отсюда по предположению индукции будет следовать, что $s-1\leqslant r-1$, т.е. $s\leqslant r$.

Докажем линейную независимость векторов $\boldsymbol{y}_1',\dots,\boldsymbol{y}_{s-1}'$. Рассмотрим равенство

$$\lambda^1\boldsymbol{y}_1'+\dots+\lambda^{s-1}\boldsymbol{y}_{s-1}'=\boldsymbol{0},$$

т.е.

$$\lambda^1\left(\boldsymbol{y}_1-\frac{a_1^r}{a_s^r}\boldsymbol{y}_s\right)+\dots+\lambda^{s-1}\left(\boldsymbol{y}_{s-1}-\frac{a_{s-1}^r}{a_s^r}\boldsymbol{y}_s\right)=\boldsymbol{0}.$$

Раскрывая скобки, получим

$$\lambda^1\boldsymbol{y}_1+\dots+\lambda^{s-1}\boldsymbol{y}_{s-1}-\left(\lambda^1\frac{a_1^r}{a_s^r}+\dots+\lambda^{s-1}\frac{a_{s-1}^r}{a_s^r}\right)\boldsymbol{y}_s=\boldsymbol{0}.$$

В силу линейной независимости векторов $\boldsymbol{y}_1,\dots,\boldsymbol{y}_s$ все коэффициенты в этом равенстве равны нулю; в частности, $\lambda^1=\dots=\lambda^{s-1}=0$, так что векторы $\boldsymbol{y}_1',\dots,\boldsymbol{y}_{s-1}'$ линейно независимы. □

4. Размерность и базис векторного пространства

A. Размерность векторного пространства.

5.39. Определение. Если для любого $n\in\mathbb{N}$ в векторном пространстве $\mathcal{V}$ найдётся линейно независимое семейство, состоящее из n векторов, то пространство $\mathcal{V}$ называется *бесконечномерным*.

5.40. Пример 5.33.6 показывает, что пространство $\mathbb{K}[t]$ бесконечномерно.

5.41. С использованием кванторов определение 5.39 записывается следующим образом: векторное пространство $\mathcal{V}$ называется бесконечномерным, если

$$\forall n \in \mathbb{N}\ \exists k,\ k > n,\ \exists \boldsymbol{x}_1, \ldots, \boldsymbol{x}_k \text{ — линейно независимые.}$$

Сформулируем отрицание этого определения (см. п. 1.33, с. 16):

$$\exists n \in \mathbb{N}\ \forall k,\ k > n,\ \forall \boldsymbol{x}_1, \ldots, \boldsymbol{x}_k \text{ — линейно зависимые.} \qquad (5.5)$$

5.42. Определение. Векторное пространство $\mathcal{V}$ называется *конечномерным*, а именно, *n-мерным*, если

(i) в $\mathcal{V}$ существует линейно независимое семейство, состоящее из n векторов;
(ii) любое семейство в $\mathcal{V}$, состоящее более чем из n векторов, линейно зависимо.

Число n называется *размерностью*[1] пространства $\mathcal{V}$ и обозначается $\dim \mathcal{V}$.

5.43. Пример 5.33.1 означает, что $\dim\{\mathbf{0}\} = 0$. Примеры 5.33.3–5 показывают, что $\dim \mathbb{V}_1 = 1$, $\dim \mathbb{V}_2 = 2$ и $\dim \mathbb{V}_3 = 3$.

5.44. Нас в первую очередь интересуют именно конечномерные векторные пространства. Немногочисленные примеры бесконечномерных пространств всегда будут специально оговариваться.

Б. Базис и координаты вектора. Пусть $\mathcal{V}$ — конечномерное векторное пространство.

5.45. Определение. *Базисом* векторного пространства $\mathcal{V}$ называется семейство $\boldsymbol{E} = \big(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\big)$ элементов этого пространства, обладающее следующими свойствами:

(i) *линейная независимость*;
(ii) *полнота*: любой вектор пространства $\mathcal{V}$ может быть выражен через $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$.

5.46. Подчеркнём, что базис — это не множество, а именно семейство, т.е. *упорядоченный набор векторов*. Переставив местами векторы некоторого базиса, мы снова получим базис, но другой.

5.47. Предложение. *Все базисы конечномерного векторного пространства $\mathcal{V}$ состоят из одинакового числа векторов. Это число равно размерности* $\dim \mathcal{V}$ *векторного пространства $\mathcal{V}$.*

[1] Обратите внимание, что это наименьшее из чисел, обладающих свойством (5.5).

Доказательство. Рассмотрим в векторном пространстве $\mathcal{V}$ два различных базиса $\boldsymbol{E} = \{\boldsymbol{e}_1, \dots, \boldsymbol{e}_n\}$ и $\boldsymbol{F} = \{\boldsymbol{f}_1, \dots, \boldsymbol{f}_m\}$. Поскольку $\boldsymbol{f}_1, \dots, \boldsymbol{f}_m \in L(\boldsymbol{e}_1, \dots, \boldsymbol{e}_n)$, согласно теореме 5.38 имеем $m \leqslant n$. Аналогично получаем $n \leqslant m$, откуда $n = m$.

Поскольку в $\mathcal{V}$ имеются линейно независимые семейства, состоящие из n векторов (например, базисы), а любое семейство, состоящее из $n+1$ векторов, линейно зависимо по теореме 5.37, число n и является размерностью этого пространства согласно определению 5.42. □

5.48. Ясно, что если $\{\boldsymbol{e}_1, \dots, \boldsymbol{e}_n\}$ — базис в векторном пространстве $\mathcal{V}$, то $\mathcal{V} = L(\boldsymbol{e}_1, \dots, \boldsymbol{e}_n)$.

5.49. Определение. Пусть $\boldsymbol{E} = \{\boldsymbol{e}_1, \dots, \boldsymbol{e}_n\}$ — произвольный базис n-мерного векторного пространства $\mathcal{V}$. Тогда для любого вектора $\boldsymbol{x} \in \mathcal{V}$ существуют такие числа $x^1, \dots, x^n$, что

$$\boldsymbol{x} = x^1\boldsymbol{e}_1 + \dots + x^n\boldsymbol{e}_n \equiv \sum_{k=1}^{n} x^k\boldsymbol{e}_k. \tag{5.6}$$

Числа $x^1, \dots, x^n$ называются *координатами* вектора $\boldsymbol{x}$ в базисе $\boldsymbol{E}$, а формула (5.6) — *разложением вектора* $\boldsymbol{x}$ по базису $\boldsymbol{E}$.

5.50. Пусть $\boldsymbol{E} = \{\boldsymbol{e}_1, \dots, \boldsymbol{e}_n\}$ — матрица-строка из базисных векторов, а $X = \{x^1, \dots, x^n\}^T$ — столбец координат вектора $\boldsymbol{x}$ в этом базисе (обратите внимание, что нумерация векторов базиса (нижние индексы) и координат вектора (верхние индексы) согласована с правилом нумерации элементов матриц). Тогда формула (5.6) может быть записана в векторном виде:

$$\boldsymbol{x} = \boldsymbol{E}X. \tag{5.7}$$

5.51. Предложение. *Разложение вектора по базису единственно, т.е. набор координат векторов в данном базисе определен однозначно.*

Доказательство. Предположим, что в базисе $\{\boldsymbol{e}_1, \dots, \boldsymbol{e}_n\}$ вектор $\boldsymbol{x}$ имеет два различных набора координат:

$$\boldsymbol{x} = x^1\boldsymbol{e}_1 + \dots + x^n\boldsymbol{e}_n = y^1\boldsymbol{e}_1 + \dots + y^n\boldsymbol{e}_n.$$

Вычитая второе разложение из первого, получим

$$\boldsymbol{0} = (x^1 - y^1)\boldsymbol{e}_1 + \dots + (x^n - y^n)\boldsymbol{e}_n.$$

Так как векторы базиса линейно независимы, то это равенство возможно лишь при нулевых коэффициентах, т.е.

$$x^1 = y^1, \quad \dots, \quad x^n = y^n.$$ □

5.52. Пусть $\boldsymbol{x}$ и $\boldsymbol{y}$ — два вектора, а $x^1, \dots, x^n$ и $y^1, \dots, y^n$ — их координаты в некотором базисе $\boldsymbol{E} = \big(\boldsymbol{e}_1, \dots, \boldsymbol{e}_n\big)$. Тогда

$$\boldsymbol{x} = x^1\boldsymbol{e}_1 + \dots + x^n\boldsymbol{e}_n, \quad \boldsymbol{y} = y^1\boldsymbol{e}_1 + \dots + y^n\boldsymbol{e}_n.$$

Поэтому

$$\boldsymbol{x} + \boldsymbol{y} = x^1\boldsymbol{e}_1 + \dots + x^n\boldsymbol{e}_n + y^1\boldsymbol{e}_1 + \dots + y^n\boldsymbol{e}_n = \\ = (x^1 + y^1)\boldsymbol{e}_1 + \dots + (x^n + y^n)\boldsymbol{e}_n,$$

т.е. *при сложении векторов их координаты складываются.* Аналогично,

$$\alpha\boldsymbol{x} = \alpha(x^1\boldsymbol{e}_1 + \dots + x^n\boldsymbol{e}_n) = (\alpha x^1)\boldsymbol{e}_1 + \dots + (\alpha x^n)\boldsymbol{e}_n,$$

т.е. *при умножении вектора на число его координаты умножаются на это число.*

В. Правило суммирования Эйнштейна. Векторы базиса нумеруются нижними индексами, а координаты вектора верхними именно для того, чтобы для записи сумм однотипных слагаемых вида (5.6) можно было использовать компактные матричные обозначения типа (5.7). Легко видеть, что выбранный способ нумерации полностью согласуется с правилом нумерации элементов матриц: верхний индекс нумерует строку, а нижний — столбец.

5.53. В алгебре используется и другой способ записи сумм вида (5.6), предложенный А. Эйнштейном и состоящий в следующем. Пусть имеется выражение (одночлен), представляющее собой произведение некоторых величин, снабжённых верхними и нижними индексами. Если некоторый индекс встречается в этом выражении дважды, причём один раз сверху и один раз снизу, то это выражение обозначает *сумму* одночленов, в которой повторяющийся индекс принимает некоторый (заранее оговорённый) диапазон значений, хотя знак суммирования $\sum$ отсутствует.

5.54. Так, выражение $a_k b^k$ означает сумму $a_1 b^1 + a_2 b^2 + \dots + a_n b^n$ (должно быть ясно из контекста или оговорено в явном виде, что индекс суммирования k пробегает значения от 1 до n). Выражение для элементов произведения матриц

$$\{AB\}_j^k = \sum_{l=1}^{s} a_l^k\, b_j^l$$

также можно записать в обозначениях Эйнштейна:

$$\{AB\}_j^k = a_l^k\, b_j^l, \quad l = 1, \dots, s.$$

Выражение $a_k b^k c^k$ *не* обозначает сумму, поскольку индекс суммирования встречается в нём не дважды, а трижды. Однако в выражениях вида $(a_k + b_k)c^k$, напоминающих по форме свойство дистрибутивности умножения относительно сложения, предполагается суммирование:

$$\begin{aligned}(a_k + b_k)c^k &= (a_1 + b_1)c^1 + (a_2 + b_2)c^2 + \cdots + (a_n + b_n)c^n = \\ &= a_1c^1 + a_2c^2 + \cdots + a_nc^n + b_1c^1 + b_2c^2 + \cdots + b_nc^n = \\ &= a_kc^k + b_kc^k.\end{aligned}$$

Читатель быстро привыкнет к этим обозначениям и оценит их компактность и удобство; сомнительные и трудные случаи мы всегда будем особо оговаривать.

5.55. Напомним (см. формулу **??**, с. **??**), что *символ Кронекера* — это обозначение для элементов единичной матрицы:

$$\delta_k^j = \begin{cases} 1, & \text{если } \ j = k, \\ 0, & \text{если } \ j \neq k. \end{cases}$$

Часто встречаются суммы вида $a_j\delta_k^j$, $b^k\delta_k^j$ и т. п. В развёрнутом виде первая из этих сумм имеет вид

$$a_1\delta_k^1 + a_2\delta_k^2 + \cdots + a_k\delta_k^k + \cdots + a_n\delta_k^n.$$

Из n слагаемых в этой сумме отлично от нуля лишь одно, а именно k-е, поэтому вся сумма равна a_k. Таким образом,

$$a_j\delta_k^j = a_k,$$

т.е. *суммирование с символом Кронекера сводится просто к замене индекса.*

Г. Важные теоремы о размерности и базисах.

5.56. Теорема (теорема о монотонности размерности)**.**

1. *Пусть* $\mathcal{P}$ *и* $\mathcal{Q}$ *— два подпространства в* $\mathcal{V}$*, причём* $\mathcal{Q} \subset \mathcal{P}$*. Тогда* $\dim \mathcal{Q} \leqslant \dim \mathcal{P}$*.*
2. *Пусть* $\mathcal{P}$ *и* $\mathcal{Q}$ *— два подпространства в* $\mathcal{V}$*, причём* $\mathcal{Q} \subset \mathcal{P}$ *и* $\dim \mathcal{P} = \dim \mathcal{Q}$*. Тогда* $\mathcal{P} = \mathcal{Q}$*.*

Доказательство. 1. Пусть $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_r$ — базис в $\mathcal{P}$, т.е. $\dim \mathcal{P} = r$, а $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_s$ — базис в $\mathcal{Q}$, т.е. $\dim \mathcal{Q} = s$. По теореме 5.38 имеем $s \leqslant r$, что и требовалось.

2. Пусть $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_s$ — базис в $\mathcal{Q}$, т.е. $\dim \mathcal{Q} = s$. Предположим, что $\mathcal{Q} \subset \mathcal{P}$, но $\mathcal{Q} \neq \mathcal{P}$. Тогда существует такой вектор $\boldsymbol{z} \in \mathcal{P}$,

что $\boldsymbol{z} \notin \mathcal{Q}$. Поскольку $\boldsymbol{z}$ не может быть представлен в виде линейной комбинации векторов $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_s$, делаем вывод, что семейство $\boldsymbol{z}, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_s$ линейно независимо (см. утверждение 7 теоремы 5.36, с. 118). Таким образом, $\mathcal{P}$ содержит не менее $s+1$ линейно независимых векторов, т.е. $\dim \mathcal{P} \geqslant s+1$. Получили противоречие с условием $\dim \mathcal{P} = \dim \mathcal{Q}$. □

5.57. Теорема (теорема о пополнении базиса)**.** *Пусть $\mathcal{P}$ — подпространство в векторном пространстве $\mathcal{V}$, причём $\dim \mathcal{P} = p < \dim \mathcal{V} = n$, $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_p$ — базис в $\mathcal{P}$. Тогда найдутся такие векторы $\boldsymbol{e}_{p+1}, \ldots, \boldsymbol{e}_n \in \mathcal{V} \setminus \mathcal{P}$, что семейство векторов*

$$\boldsymbol{e}_1,\ \ldots,\ \boldsymbol{e}_p,\ \boldsymbol{e}_{p+1},\ \ldots,\ \boldsymbol{e}_n$$

является базисом в $\mathcal{V}$.

Доказательство. Так как $p < n$, то найдётся такой вектор $\boldsymbol{e}_{p+1} \in \mathcal{V}$, что векторы $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_p, \boldsymbol{e}_{p+1}$ линейно независимы; при этом $\boldsymbol{e}_{p+1} \notin \mathcal{P}$, так как в противном случае получили бы $\dim \mathcal{P} > p$.

Если $p+1 = n$, пополнение базиса завершено. Если $p+1 < n$, продолжаем процесс. Процесс завершается через конечное число шагов, поскольку пространство $\mathcal{V}$ конечномерно. □

5.58. Теорема (формула Грассмана)**.** *Если $\mathcal{P}$ и $\mathcal{Q}$ — подпространства векторного пространства $\mathcal{V}$, то*

$$\dim(\mathcal{P} + \mathcal{Q}) = \dim \mathcal{P} + \dim \mathcal{Q} - \dim(\mathcal{P} \cap \mathcal{Q}). \tag{5.8}$$

Доказательство. Пусть $\dim \mathcal{P} = p$, $\dim \mathcal{Q} = q$, $\dim(\mathcal{P} \cap \mathcal{Q}) = r$. Рассмотрим в $\mathcal{P} \cap \mathcal{Q}$ произвольный базис $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_r$. Используя процедуру пополнения базиса, достроим это семейство векторов до базиса

$$\boldsymbol{e}_1,\ \ldots,\ \boldsymbol{e}_r,\ \boldsymbol{f}_1,\ \ldots,\ \boldsymbol{f}_{p-r} \tag{5.9}$$

подпространства $\mathcal{P} \ni \mathcal{P} \cap \mathcal{Q}$. Аналогично построим базис

$$\boldsymbol{e}_1,\ \ldots,\ \boldsymbol{e}_r,\ \boldsymbol{g}_1,\ \ldots,\ \boldsymbol{g}_{q-r} \tag{5.10}$$

подпространства $\mathcal{Q} \ni \mathcal{P} \cap \mathcal{Q}$. Теорема 5.58 будет доказана, если мы покажем, что $p+q-r$ векторов

$$\boldsymbol{e}_1,\ \ldots,\ \boldsymbol{e}_r,\quad \boldsymbol{f}_1,\ \ldots,\ \boldsymbol{f}_{p-r},\quad \boldsymbol{g}_1,\ \ldots,\ \boldsymbol{g}_{q-r} \tag{5.11}$$

образуют базис подпространства $\mathcal{P} + \mathcal{Q}$.

Сначала докажем линейную независимость семейства (5.11). Пусть

$$\alpha_1\boldsymbol{e}_1 + \cdots + \alpha_r\boldsymbol{e}_r + \beta_1\boldsymbol{f}_1 + \cdots + \beta_{p-r}\boldsymbol{f}_{p-r} + \gamma_1\boldsymbol{g}_1 + \cdots + \gamma_{q-r}\boldsymbol{g}_{q-r} = \boldsymbol{0}.$$

Для краткости положим

$$\boldsymbol{e} = \alpha_1\boldsymbol{e}_1 + \cdots + \alpha_r\boldsymbol{e}_r,$$

$$\boldsymbol{f} = \beta_1 \boldsymbol{f}_1 + \cdots + \beta_{p-r} \boldsymbol{f}_{p-r},$$
$$\boldsymbol{g} = \gamma_1 \boldsymbol{g}_1 + \cdots + \gamma_{q-r} \boldsymbol{g}_{q-r}.$$

Векторы $\boldsymbol{e} \in \mathcal{P} \cap \mathcal{Q}$, $\boldsymbol{f} \in \mathcal{P}$ и $\boldsymbol{g} \in \mathcal{Q}$ удовлетворяют соотношению $\boldsymbol{e} + \boldsymbol{f} + \boldsymbol{g} = \boldsymbol{0}$. Имеем

$$\boldsymbol{e} + \boldsymbol{f} \in \mathcal{P} \quad \Rightarrow \quad \boldsymbol{g} = -\boldsymbol{e} - \boldsymbol{f} \in \mathcal{P} \quad \Rightarrow \quad \boldsymbol{g} \in \mathcal{P} \cap \mathcal{Q},$$

т.е. вектор $\boldsymbol{g}$ линейно выражается через $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_r$. Однако он также линейно выражается через $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_{q-r}$. Поскольку два различных разложения по базису (5.10) существовать не могут, видим, что оба разложения имеют нулевые коэффициенты. Поэтому $\gamma_1 = \cdots = \gamma_{q-r} = 0$, т.е. $\boldsymbol{g} = \boldsymbol{0}$.

Но тогда $\boldsymbol{e} + \boldsymbol{f} = \boldsymbol{0}$; поскольку (5.9) — базис, находим

$$\alpha_1 = \cdots = \alpha_r = \beta_1 = \cdots = \beta_{p-r},$$

т.е. векторы (5.11) линейно независимы.

Для доказательства полноты семейства (5.11) нужно убедиться, что любой вектор $\boldsymbol{u}$ из $\mathcal{P} + \mathcal{Q}$ можно разложить в линейную комбинацию векторов (5.11). Имеем $\boldsymbol{u} = \boldsymbol{x} + \boldsymbol{y}$, где $\boldsymbol{x} \in \mathcal{P}$ и $\boldsymbol{y} \in \mathcal{Q}$. Сложив разложение вектора $\boldsymbol{x}$ по базису (5.9) с разложением вектора $\boldsymbol{y}$ по базису (5.10), получим представление вектора $\boldsymbol{u}$ в виде линейной комбинации векторов (5.11). □

Д. Примеры.

5.59. Нулевое векторное пространство $\{\boldsymbol{0}\}$ не имеет базиса.

5.60. В качестве базиса пространства $\mathbb{V}_1$ может быть взят произвольный ненулевой вектор из $\mathbb{V}_1$. Аналогично, базисами в $\mathbb{V}_2$ и $\mathbb{V}_3$ могут служить произвольные упорядоченные пары (тройки) неколлинеарных (некомпланарных) векторов.

5.61. ***Базис арифметического пространства*** $\mathbb{K}^n$**.** Легко проверить, что векторы (столбцы)

$$\boldsymbol{e}_1 = \big(1, 0, \ldots, 0\big)^T, \quad \ldots, \quad \boldsymbol{e}_n = \big(0, 0, \ldots, 1\big)^T \tag{5.12}$$

линейно независимы[1], а любой другой столбец является их линейной комбинацией:

$$\boldsymbol{x} = \big(x^1,\ x^2, \ldots, x^n\big)^T = x^1 \boldsymbol{e}_1 + x^2 \boldsymbol{e}_2 + \cdots + x^n \boldsymbol{e}_n.$$

[1]Действительно, равенство линейной комбинации этих столбцов с коэффициентами $\alpha_1, \ldots, \alpha_n$

$$\alpha_1 \boldsymbol{e}_1 + \cdots + \alpha_n \boldsymbol{e}_n \equiv \big(\alpha_1, \ldots, \alpha_n\big)^T$$

нулевому столбцу возможно лишь в случае, когда $\alpha_1 = \cdots = \alpha_n = 0$.

Поэтому столбцы (5.12) образуют базис в $\mathbb{K}^n$, называемый *стандартным*, а $\dim \mathbb{K}^n = n$.

Отметим, что компоненты (элементы) столбца $\big(x^1, \dots, x^n\big)^T$ являются координатами этого столбца в стандартном базисе пространства $\mathbb{K}$; в другом базисе координаты будут другие. Таким образом, нужно различать термины «компоненты столбца» и «координаты столбца»: первый термин имеет инвариантный (т.е. не зависящий от выбора базиса) смысл, а второй привязан к базису.

5.62. ***Фундаментальное семейство решений*** $X_1, \dots, X_s$ однородной линейной системы $AX = O$ является базисом в множестве всех её решений, которое, напомним (см. пример 5.22.3), представляет собой подпространство пространства столбцов.

5.63. ***Пространство комплексных столбцов*** $\mathbb{C}^n$ ***над полем*** $\mathbb{R}$**.** Множество $\mathbb{C}^n$ можно рассматривать как векторное пространство над полем вещественных чисел; это означает, что компонентами столбцов являются комплексные числа, но коэффициентами при образовании линейных комбинаций (в том числе и координатами векторов) могут служить лишь вещественные числа. Будем обозначать это векторное пространство $\mathbb{C}^n(\mathbb{R})$. Стандартный базис этого пространства состоит из векторов

$$\begin{aligned} \boldsymbol{e}_1 &= \big(1, 0, \dots, 0\big)^T, \qquad \dots, \qquad \boldsymbol{e}_n = \big(0, 0, \dots, 1\big)^T, \\ \boldsymbol{e}_{n+1} &= \big(i, 0, \dots, 0\big)^T, \qquad \dots, \qquad \boldsymbol{e}_{2n} = \big(0, 0, \dots, i\big)^T. \end{aligned}$$

Действительно, любой вектор-столбец с комплексными компонентами может быть представлен в виде следующей вещественной линейной комбинации столбцов $\boldsymbol{e}_1, \dots, \boldsymbol{e}_{2n}$:

$$\begin{pmatrix} x^1 + iy^1 \\ x^2 + iy^2 \\ \vdots \\ x^n + iy^n \end{pmatrix} = x^1\boldsymbol{e}_1 + \dots + x^n\boldsymbol{e}_n + y^1\boldsymbol{e}_{n+1} + \dots + y^n\boldsymbol{e}_{2n}.$$

Отсюда вытекает, что $\dim \mathbb{C}^n(\mathbb{R}) = 2n$.

5.64. ***Базис пространства многочленов*** $\mathbb{K}[t]_n$**.** Докажем, что в пространстве $\mathbb{K}[t]_n$ многочленов степени не выше n многочлены

$$\boldsymbol{e}_0 = 1, \quad \boldsymbol{e}_1 = t, \quad \boldsymbol{e}_2 = t^2, \quad \dots, \quad \boldsymbol{e}_n = t^n \tag{5.13}$$

линейно независимы. Действительно, приравняем нулю их линейную комбинацию:

$$\alpha_0 + \alpha_1 t + \alpha_2 t^2 + \dots + \alpha_n t^n = 0.$$

Предположив, что хотя бы один коэффициент α_k отличен от нуля, получаем уравнение относительно t степени не выше n, которое имеет лишь конечное число корней т.е. указанное равенство не может выполняться тождественно для всех t.

Далее, поскольку произвольный многочлен

$$x(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n$$

можно представить в виде

$$x(t) = a_0 \boldsymbol{e}_0 + a_1 \boldsymbol{e}_1 + a_2 \boldsymbol{e}_2 + \cdots + a_n \boldsymbol{e}_n,$$

видим, что векторы (многочлены) (5.13) образуют базис в векторном пространстве $\mathbb{K}[t]_n$ и $\dim \mathbb{K}[t]_n = n + 1$; этот базис назовём *стандартным*.

5. Изоморфизм

5.65. Определение. Рассмотрим два векторных пространства над одним и тем же числовым полем $\mathbb{K}$: пространство $\mathcal{V}$ с операциями $\oplus$, $\odot$ и нулевым вектором $\mathbf{0}_{\mathcal{V}}$ и пространство $\mathcal{W}$ с операциями $\boxplus$, $\boxdot$ и нулевым вектором $\mathbf{0}_{\mathcal{W}}$. Взаимно однозначное отображение $g\colon \mathcal{V} \to \mathcal{W}$ называется *изоморфизмом векторных пространств* (см. п. 3.69), если оно обладает следующим свойством (свойством линейности):

$$\forall \boldsymbol{x}, \boldsymbol{y} \in \mathcal{V},\ \forall \alpha, \beta \in \mathbb{K}: \quad g(\alpha \odot \boldsymbol{x} \oplus \beta \odot \boldsymbol{y}) = \alpha \boxdot g(\boldsymbol{x}) \boxplus \beta \boxdot g(\boldsymbol{y});$$

в упрощённых обозначениях (когда операции в пространствах $\mathcal{V}$ и $\mathcal{W}$ обозначаются одними и теми же символами)

$$\forall \boldsymbol{x}, \boldsymbol{y} \in \mathcal{V},\ \forall \alpha, \beta \in \mathbb{K}: \quad g(\alpha \boldsymbol{x} + \beta \boldsymbol{y}) = \alpha g(\boldsymbol{x}) + \beta g(\boldsymbol{y}).$$

Два векторных пространства $\mathcal{V}$ и $\mathcal{W}$, для которых существует хотя бы один изоморфизм $g\colon \mathcal{V} \to \mathcal{W}$, называются *изоморфными* (обозначение $\mathcal{V} \approx \mathcal{W}$).

5.66. В аксиоматической теории векторных пространств мы интересуемся только теми их свойствами, которые выражаются в терминах операций сложения векторов и умножения векторов на числа. У изоморфных пространств такие свойства одинаковы, поэтому в рамках аксиоматической теории изоморфные пространства неразличимы (хотя конкретные реализации изоморфных пространств могут быть совершенно различными). Таким образом, утверждения, справедливые для какого-либо векторного пространства, имеют место и во всех изоморфных ему пространств. На этом обстоятельстве и основан метод координат, лежащий в основе аналитической геометрии.

5.67. Координаты $x^1, \dots, x^n$ вектора $\boldsymbol{x} \in \mathcal{V}$ в (заранее зафиксированном) базисе $\boldsymbol{E} = \big(\boldsymbol{e}_1, \dots, \boldsymbol{e}_n\big)$ составляют упорядоченную последовательность $(x^1, \dots, x^n)$ чисел, т.е. элемент арифметического пространства $\mathbb{K}^n$ (напомним, что элементами пространства $\mathbb{K}^n$ мы договорились считать столбцы). Поэтому формула

$$g(\boldsymbol{x}) = \big(x^1, \dots, x^n\big)^T \tag{5.14}$$

определяет взаимно однозначное отображение $g\colon \mathcal{V} \to \mathbb{K}^n$. Установленные выше (см. п. 5.52) свойства координат означают, что это отображение является изоморфизмом.

5.68. Определение. Изоморфизм, заданный формулой (5.14), называется *координатным изоморфизмом*, определяемым базисом $\big(\boldsymbol{e}_1, \dots, \boldsymbol{e}_n\big)$.

Из факта существования координатных изоморфизмов вытекает следующее утверждение.

5.69. Теорема.

1. *Каждое n-мерное векторное пространство $\mathcal{V}$ над числовым полем $\mathbb{K}$ изоморфно пространству $\mathbb{K}^n$.*
2. *Все векторные пространства над одним и тем же числовым полем, имеющие одинаковую размерность, изоморфны между собой.*

5.70. Легко проверить, что отношение изоморфности векторных пространств является *отношением эквивалентности* (см. с. 43). Таким образом, класс всех векторных пространств над одним и тем же числовым полем разбивается на непересекающиеся классы эквивалентности, каждый из которых характеризуется натуральным числом — размерностью.

Различных векторных пространств одной размерности существует необозримо много, но классов изоморфных пространств имеется лишь счётное множество, причём для каждого $n \in \mathbb{N}_0$ имеется единственный класс, состоящий из всех n-мерных пространств.

5.71. Изоморфизм $g\colon \mathcal{V} \to \mathcal{W}$ векторных пространств можно задать следующим образом. Зафиксируем базис $\boldsymbol{E} = \big(\boldsymbol{e}_1, \dots, \boldsymbol{e}_n\big)$ пространства $\mathcal{V}$ и базис $\boldsymbol{F} = \big(\boldsymbol{f}_1, \dots, \boldsymbol{f}_n\big)$ пространства $\mathcal{W}$ и рассмотрим линейное отображение $g\colon \mathcal{V} \to \mathcal{W}$, заданное на базисных векторах формулой $g(\boldsymbol{e}_k) = \boldsymbol{f}_k$, $k = 1, \dots, n$. Ясно, что это линейное отображение взаимно однозначно, т.е. является изоморфизмом, переводящим вектор $\boldsymbol{x} \in \mathcal{V}$ в вектор $\boldsymbol{y} \in \mathcal{W}$, имеющий в базисе $\boldsymbol{F}$ те же координаты, что и вектор $\boldsymbol{x}$ в базисе $\boldsymbol{E}$. Поэтому говорят, что изоморфизм g устанавливается *по равенству координат.*

6. Упражнения и задачи

5.1. Выясните, является ли линейным подпространством в $\mathbb{K}^n$ данное множество векторов, и если является, то найдите его размерность и укажите какой-либо базис:

(1) множество векторов, все компоненты которых равны между собой;
(2) множество векторов, первая компонента которых равна 0;
(3) множество векторов, сумма компонент которых равна 0;
(4) множество векторов, сумма компонент которых равна 1.

5.1. **(1)** $\dim = 1$; базис состоит из единственного столбца $(1, 1, \dots, 1)^T$; **(2)** $\dim = n - 1$; базис $\boldsymbol{e}_1 = (0, 1, 0, \dots, 0)^T$, $\boldsymbol{e}_2 = (0, 0, 1, \dots, 0)^T$, $\dots$, $\boldsymbol{e}_{n-1} = (0, 0, 0, \dots, 1)^T$; **(3)** $\dim = n - 1$; базис $\boldsymbol{e}_1 = (1, 0, \dots, 0, -1)^T$, $\boldsymbol{e}_2 = (0, 1, \dots, 0, -1)^T$, $\dots$, $\boldsymbol{e}_{n-1} = (0, 0, \dots, 1, -1)^T$. **(4)** не является.

5.2. Выясните, является ли линейным подпространством в $\mathbb{K}^{n\times n}$ данное множество квадратных матриц, и если является, то найдите его размерность и укажите какой-либо базис:

(1) множество матриц с нулевой первой строкой;
(2) множество диагональных матриц;
(3) множество верхнетреугольных матриц;
(4) множество симметричных матриц;
(5) множество кососимметричных матриц.

5.2. **(1)** $\dim = n(n-1)$, базис E_{21}, E_{22}, $\dots$, E_{2n}, $\dots$, E_{nn}, где E_{jk} — матричные единицы (см. решение задачи **??**, с. **??**); **(2)** $\dim = n$, базис $E_{11}, \dots, E_{nn}$; **(3)** $\dim = n(n+1)/2$, базис E_{11}, $\dots$, E_{1n}, E_{22}, $\dots$, E_{2n}, $\dots$, E_{nn}; **(4)** $\dim = n(n+1)/2$, базис E_{11}, $\dots$, E_{nn}, $E_{12} + E_{21}$, $E_{13} + E_{31}$, $\dots$, $E_{n,n-1} + E_{n-1,n}$; **(5)** $\dim = n(n-1)/2$, базис $E_{12} - E_{21}$, $E_{13} - E_{31}$, $\dots$, $E_{n,n-1} - E_{n-1,n}$. Обратите внимание, что подпространства из примеров (3) и (4) изоморфны.

5.3. Докажите, что для любых трёх векторов $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$ произвольного векторного пространства и любых трёх чисел α, β, γ векторы $\alpha\boldsymbol{a} - \beta\boldsymbol{b}$, $\gamma\boldsymbol{b} - \alpha\boldsymbol{c}$, $\beta\boldsymbol{c} - \gamma\boldsymbol{a}$ линейно зависимы.

5.4. Докажите, что семейство многочленов $\boldsymbol{x}_0 = 1$, $\boldsymbol{x}_1 = t$, $\dots$, $\boldsymbol{x}_n = t^n$, $x \in \mathbb{R}$, линейно независимо.

5.4. Предположим, что существует нетривиальная линейная комбинация

$$\alpha_0\boldsymbol{x}_0 + \alpha_1\boldsymbol{x}_1 + \dots + \alpha_n\boldsymbol{x}_n \equiv 0 \iff \alpha_0 + \alpha_1 t + \dots + \alpha_n t^n \equiv 0.$$

Ненулевой многочлен степени $\leqslant n$, стоящий в левой части, не может иметь более n корней, т.е. существует точка t_0, в которой $\alpha_0 + \alpha_1 t_0 + \dots + \alpha_n t_0^n \neq 0$, противоречие.

5.5. Докажите, что семейство функций $f_1(x) = e^{px}$, $f_2(x) = xe^{px}$, $\ldots$, $f_n(x) = x^{n-1}e^{px}$, $x \in \mathbb{R}$, линейно независимо.

5.5. Данная задача сводится к упражнению 5.4.

5.6. Выясните, являются ли линейно зависимыми следующие функции:
(а) $f_1(x) = \arcsin x, f_2(x) = \arccos x, f_3(x) = 1$, $x \in (-1;1)$;
(б) $g_1(x) = x, g_2(x) = |x|$, $x \in \mathbb{R}$.

5.6. (а) Поскольку $\arcsin x + \arccos x = \pi/2$, видим, что данные функции линейно зависимы:

$$1 \cdot f_1(x) + 1 \cdot f_2(x) - \frac{\pi}{2} \cdot f_3(x) = 0.$$

(б) Выясним, при каких коэффициентах α_1, α_2 равенство

$$\alpha_1 g_1(x) + \alpha_2 g_2(x) = 0$$

выполняется при всех $x \in \mathbb{R}$. При $x > 0$ это равенство даёт $\alpha_1 x + \alpha_2 x = 0 \Leftrightarrow \alpha_1 + \alpha_2 = 0$, а при $x < 0$ — $\alpha_1 x - \alpha_2 x = 0 \Leftrightarrow \alpha_1 - \alpha_2 = 0$. Система уравнений

$$\begin{cases} \alpha_1 + \alpha_2 = 0, \\ \alpha_1 - \alpha_2 = 0 \end{cases}$$

имеет лишь решение $\alpha_1 = \alpha_2 = 0$, что означает линейную независимость рассматриваемых функций.

5.7. Векторы $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k$ в n-мерном векторном пространстве $\mathcal{V}$ линейно независимы. Известно, что если в базисе $\big(\boldsymbol{e}_1, \ldots \boldsymbol{e}_n\big)$ вектор $\boldsymbol{e}_j$ заменить на вектор $\boldsymbol{x}_j$, то снова получится базис. Верно ли, что обязательно $\big(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k, \boldsymbol{e}_{k+1}, \ldots, \boldsymbol{e}_n\big)$ является базисом?

5.8. Векторы $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{m+1}$ в $\mathbb{R}^n$ линейно независимы. Докажите, что в линейной оболочке $L(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{m+1})$ имеется ненулевой вектор, у которого первые m компонент нулевые.

5.8. Пусть

$$\boldsymbol{x}_1 = \begin{pmatrix} x_1^1 \\ x_1^2 \\ \vdots \\ x_1^n \end{pmatrix}, \quad \boldsymbol{x}_2 = \begin{pmatrix} x_2^1 \\ x_2^2 \\ \vdots \\ x_2^n \end{pmatrix}, \quad \ldots, \quad \boldsymbol{x}_{m+1} = \begin{pmatrix} x_{m+1}^1 \\ x_{m+1}^2 \\ \vdots \\ x_{m+1}^n \end{pmatrix}.$$

Предположим, что у одного из векторов $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{m+1}$ первая компонента отлична от нуля; без ограничения общности можно считать, что это $\boldsymbol{x}_{m+1}$. Рассмотрим векторы

$$\boldsymbol{x}'_1 = \boldsymbol{x}_1 - \frac{x_1^1}{x_{m+1}^1}\boldsymbol{x}_{m+1}, \ \boldsymbol{x}'_2 = \boldsymbol{x}_2 - \frac{x_2^1}{x_{m+1}^1}\boldsymbol{x}_{m+1}, \ \ldots, \ \boldsymbol{x}'_m = \boldsymbol{x}_m - \frac{x_m^1}{x_{m+1}^1}\boldsymbol{x}_{m+1}.$$

Если же у всех векторов $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{m+1}$ первая компонента равна нулю, то просто отбросим один из них. В обоих случаях получим семейство m линейно независимых векторов, у которых первая компонента нулевая. Применим к этому семейству описанную процедуру для второй компоненты и т. д.

5.9. Докажите, что семейство векторов $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_p$ линейно зависимо тогда и только тогда, когда некоторый вектор $\boldsymbol{x}_k$, $1 \leqslant k \leqslant p$, этого семейства линейно выражается через *предыдущие* векторы $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{k-1}$.

5.9. Если $\boldsymbol{x}_k$, $1 \leqslant k \leqslant p$, выражается через $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{k-1}$, то семейство $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k$ линейно зависимо (предложение 5.36.3), а потому линейно зависимо и семейство $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_p$ (предложение 5.36.4). (Случай $k = 1$ означает, что $\boldsymbol{x}_1 = \boldsymbol{0}$).

Обратно, если семейство $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_p$ линейно зависимо, то существует такое наименьшее k, $1 \leqslant k \leqslant p$, что семейство $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k$ линейно зависимо ($k = 1 \;\Leftrightarrow\; \boldsymbol{x}_1 = \boldsymbol{0}$). Пусть $\alpha_1\boldsymbol{x}_1 + \cdots + \alpha_k\boldsymbol{x}_k = \boldsymbol{0}$ — равная нулевому вектору нетривиальная линейная комбинация векторов $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k$. Ясно, что $\alpha_k \neq 0$, поскольку при $\alpha_k = 0$ получится, что, вопреки предположению, линейно зависимо семейство $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{k-1}$. Отсюда получаем

$$\boldsymbol{x}_k = -\frac{\alpha_1}{\alpha_k}\boldsymbol{x}_1 - \cdots - \frac{\alpha_{k-1}}{\alpha_k}\boldsymbol{x}_{k-1}.$$

5.10. Семейство $\boldsymbol{x}_1 = \left(x_1^1, x_1^2, \ldots, x_1^n\right)^T$, $\boldsymbol{x}_s = \left(x_s^1, x_s^2, \ldots, x_s^n\right)^T$ векторов пространства $\mathbb{R}^n$ таково, что

$$\left|x_j^j\right| > \sum_{\substack{k=1 \\ k\neq j}}^{s} \left|x_k^j\right|, \quad j = 1, \ldots, s, \quad s \leqslant n.$$

Докажите, что это семейство линейно независимо.

5.10. Предположим противное, т.е. пусть $\alpha_1, \ldots, \alpha_s$ — такие коэффициенты, среди которых хотя бы один ненулевой, что

$$\alpha_1\boldsymbol{x}_1 + \ldots \alpha_s\boldsymbol{x}_s = \boldsymbol{0},$$

т.е.

$$\alpha_1 x_1^p + \ldots \alpha_s x_s^p = 0 \quad \forall p = 1, \ldots, n.$$

Пусть для определённости α_1 — наибольшее по модулю среди чисел $\alpha_1, \ldots, \alpha_s$. Так как

$$\alpha_1 x_1^1 + \alpha_2 x_2^1 + \ldots \alpha_s x_s^1 = 0,$$

то

$$\left|\alpha_1 x_1^1\right| = \left|\alpha_2 x_2^1 + \cdots + \alpha_s x_s^1\right| \leqslant \left|\alpha_1\right|\left(\left|x_2^1\right| + \cdots + \left|x_s^1\right|\right) \leqslant \left|\alpha_1\right| \cdot \left|x_2^1\right|,$$

противоречие.

Указания и ответы

1.1. Выражения (а), (б), (в) — высказывания, но их истинностные значения можно определить только при дополнительных условиях (например, азот не всегда является газом). (г), (е) не являются высказываниями, поскольку не обладают истинностными значениями. (д) является не высказыванием, а предикатом. (ж), (з) — ложное и истинное высказывания соответственно.

1.2. Нет. Предположения об истинности или ложности данного предложения приводят к противоречию.

1.3. Введём обозначения: A =«сегодняшний день солнечный», B =«сегодняшний день тёплый». Тогда (а) и (б) записываются как $A \wedge B$ и $A \wedge \neg B$. При обозначениях C =«данный четырёхугольник — квадрат», D =«данный четырёхугольник — ромб» высказывание (в) записывается в виде $C \vee D$. При обозначениях E =«это необходимо», F =«это желательно» высказывание (е) можно записать в виде $\neg E \wedge \neg F = \neg(E \vee F)$.

1.4. (а) $A \wedge B$; (б) $A \wedge \neg B$; (в) $\neg A \wedge \neg B$; (г) $\neg(A \wedge B)$.

1.5. $(A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C)$.

1.6. Импликации (а), (в), (г), (д) истинны, (б) ложна. Импликация (е) истинна в любой день, кроме понедельника.

1.7. (а) $A \Rightarrow \neg B$; (б) $A \Rightarrow B$; (в) $A \Rightarrow A$; (г) $\neg(B \Rightarrow A)$.

1.8. Если A =«данный треугольник — равносторонний», B =«углы данного треугольника равны», то истинное высказывание (а) записывается в виде $A \Rightarrow B$, а истинное высказывание (б) — в виде $B \Rightarrow A$. Если C =«число x делится на три», D =«число x делится на 6», то ложное высказывание (в) записывается в виде $C \Rightarrow D$, а истинное высказывание (г) — в виде $D \Rightarrow C$.

1.9. (а) Введём обозначения A_k = «$x_k = 0$», где $k = 1, \ldots, N$, N — число сомножителей, B = «$\prod\limits_{k=1}^{N} x_k = 0$». Тогда истинное высказывание (а) записывается в виде $B \Leftrightarrow (A_1 \vee A_2 \vee \cdots \vee A_N)$ или $B \Leftrightarrow \bigvee\limits_{k=1}^{N} A_k$.

(б) Введём обозначения C_k = «число x_k делится на 3», где $k = 1, \ldots, N$, N — число слагаемых, D = «$\sum\limits_{k=1}^{N} x_k$ делится на 3». Тогда

ложное высказывание (б) записывается в виде $(C_1 \wedge C_2 \wedge \cdots \wedge C_N) \Leftrightarrow D$ или $\bigwedge\limits_{k=1}^{N} C_k \Leftrightarrow D$. Высказывание $\bigwedge\limits_{k=1}^{N} C_k \Rightarrow D$ истинно.

(в) Введём обозначения E =«данный четырёхугольник является квадратом», F =«все углы данного четырехугольника прямые». Тогда ложное высказывание (в) записывается в виде $E \Leftrightarrow F$. Высказывание $E \Rightarrow F$ истинно.

1.10. Введём следующие высказывания:

A = «данный четырёхугольник является прямоугольником»,

B = «вокруг данного четырёхугольника можно описать окружность».

Тогда $A \Rightarrow B$ — истинное высказывание. Высказывание $B \Rightarrow A$ («если вокруг четырёхугольника можно описать окружность, то он является прямоугольником») ложно (например, окружность можно описать вокруг трапеции).

Высказывание $\neg A \Rightarrow \neg B$ («если четырёхугольник не является прямоугольником, то вокруг него нельзя описать окружность») ложно (см. предыдущий пример).

Высказывание $\neg B \Rightarrow \neg A$ («если вокруг четырёхугольника нельзя описать окружность, то он не является прямоугольником») истинно, поскольку получено из исходного истинного высказывания $A \Rightarrow B$ с помощью контрапозиции.

1.11. Построим таблицу истинности для высказывания $A \Rightarrow (B \Rightarrow A)$:

A	B	$B \Rightarrow A$	$A \Rightarrow (B \Rightarrow A)$
0	0	1	1
0	1	0	1
1	0	1	1
1	1	1	1

Последний столбец показывает, что высказывание $A \Rightarrow (B \Rightarrow A)$ истинно при любых A и B.

1.12. Доказательство сводится к заполнению таблицы истинности

A	B	$A \wedge B$	$A \vee (A \wedge B)$
0	0	0	0
0	1	0	0
1	0	0	1
1	1	1	1

(здесь использованы таблицы истинности для операций конъюнкции и дизъюнкции). Сравнивая истинностные значения высказываний A и $A \vee (A \wedge B)$, видим, что они совпадают при любых истинностных значениях высказываний A и B.

1.13.

$\neg\neg A = A$

A	$\neg A$	$\neg\neg A$
0	1	0
1	0	1

$A \vee \neg A = 1$

A	$\neg A$	$A \vee \neg A$
0	1	1
1	0	1

$A \wedge \neg A = 0$

A	$\neg A$	$A \wedge \neg A$
0	1	0
1	0	0

1.14.

Для $\neg(A \wedge B) = \neg A \vee \neg B$:

A	B	$A \wedge B$	$\neg(A \wedge B)$	$\neg A$	$\neg B$	$\neg A \vee \neg B$
0	0	0	1	1	1	1
0	1	0	1	1	0	1
1	0	0	1	0	1	1
1	1	1	0	0	0	0

Для $\neg(A \vee B) = \neg A \wedge \neg B$:

A	B	$A \vee B$	$\neg(A \vee B)$	$\neg A$	$\neg B$	$\neg A \wedge \neg B$
0	0	0	1	1	1	1
0	1	1	0	1	0	0
1	0	1	0	0	1	0
1	1	1	0	0	0	0

1.15.

Для $\neg(A \Rightarrow B) = (A \wedge \neg B)$:

A	B	$A \Rightarrow B$	$\neg(A \Rightarrow B)$	$\neg B$	$A \wedge \neg B$
0	0	1	0	1	0
0	1	1	0	0	0
1	0	0	1	1	1
1	1	1	0	0	0

Для $(A \vee B) = (\neg A \Rightarrow B)$:

A	B	$A \vee B$	$\neg A$	$\neg A \Rightarrow B$
0	0	0	1	0
0	1	1	1	1
1	0	1	0	1
1	1	1	0	1

1.16.

(а) если дифференцируемая функция имеет в некоторой точке экстремум, то её производная в этой точке обращается в нуль;

(б) если функция дифференцируема в некоторой точке, то она непрерывна в этой точке;

(в) если числовой ряд сходится, то его общий член стремился к нулю;
(г) если ограниченная числовая последовательность монотонна, то она имеет предел.

1.17.

(а) для того, чтобы производная дифференцируемой функции обращалась в нуль в некоторой точке, достаточно, чтобы в этой точке функция имела экстремум;
(б) для того, чтобы функция была дифференцируема в некоторой точке, необходимо, чтобы она была непрерывна в этой точке;
(в) для того, чтобы общий член числового ряда стремился к нулю, достаточно, чтобы ряд сходился;
(г) для того, чтобы ограниченная числовая последовательность была монотонной, необходимо, чтобы она имела предел.

1.18.

(а) для того, чтобы производная дифференцируемой функции в некоторой точке была отлична от нуля, необходимо, чтобы функция не имела экстремума в этой точке; для того, чтобы дифференцируемая функция не имела экстремума в некоторой точке, достаточно, чтобы её производная в этой точке была отлична от нуля; если производная дифференцируемой функции в некоторой точке отлична от нуля, то в этой точке функция не имеет экстремума;
(б) для того, чтобы функция не была непрерывной в некоторой точке, необходимо, чтобы она не была дифференцируемой в этой точке; для того, чтобы функция не была дифференцируемой в некоторой точке, достаточно, чтобы она не была непрерывной в этой точке; если функция не является непрерывной в некоторой точке, то она не является дифференцируемой в этой точке;
(в) для того, чтобы общий член числового ряда не стремился к нулю, необходимо, чтобы ряд не являлся сходящимся; для того, чтобы числовой ряд не являлся сходящимся, достаточно, чтобы его общий член не стремился к нулю; если общий член числового ряда не стремится к нулю, то этот ряд не является сходящимся;
(г) для того, чтобы ограниченная числовая последовательность не имела предела, необходимо, чтобы она не была монотонной; для того, чтобы ограниченная числовая последовательность не была монотонной, достаточно, чтобы она не имела предела; если ограниченная числовая последовательность не имеет предела, то она не является монотонной.

3.1. Для элемента x существует такой $y \in X$, что $y * x = e$. Тогда

$$e = y * x = y * (x * x) = (y * x) * x = e * x = x. \qquad \square$$

3.2. Сначала докажем, что из **Г2′** и **Г3′** вытекает **Г3**, т.е. из $y*x=e$ следует $x*y=e$. Имеем

$$(x*y)*(x*y)=x*\big[(y*x)*y\big]=x*\big[e*y\big]=x*y;$$

согласно результату задачи 3.2 отсюда следует, что $x*y=e$. Теперь докажем выполнение аксиомы **Г2**, т.е. убедимся, что из $e*x=x$ вытекает $x*e=x$. Пусть y — такой элемент, что $y*x=e=x*y$. Тогда

$$x*e=x*(y*x)=(x*y)*x=e*x=x.$$

Требуемый контрпример доставляет множество $X=\{a,b\}$ с операцией $x*y=y$. Эта операция ассоциативна: для любых x, y, z имеем

$$(x*y)*z=y*z=z,\quad x*(y*z)=x*z=z.$$

Элемент $a\in X$ является левым нейтральным элементом: для любого $x\in X$ имеем $a*x=x$. Поскольку $a*a=a$, правый обратный к a равен a; поскольку $b*a=a$, правый обратный к b равен a. Однако a не является правым нейтральным элементом: $b*a=a\neq b$. Кроме того, a, будучи правым обратным для b, не является левым обратным: $a*b=b\neq a$.

5.1. **(1)** $\dim=1$; базис состоит из единственного столбца $(1,1,\ldots,1)^T$; **(2)** $\dim=n-1$; базис $\boldsymbol{e}_1=(0,1,0,\ldots,0)^T$, $\boldsymbol{e}_2=(0,0,1,\ldots,0)^T$, $\ldots$, $\boldsymbol{e}_{n-1}=(0,0,0,\ldots,1)^T$; **(3)** $\dim=n-1$; базис $\boldsymbol{e}_1=(1,0,\ldots,0,-1)^T$, $\boldsymbol{e}_2=(0,1,\ldots,0,-1)^T$, $\ldots$, $\boldsymbol{e}_{n-1}=(0,0,\ldots,1,-1)^T$. **(4)** не является.

5.2. **(1)** $\dim=n(n-1)$, базис E_{21}, E_{22}, $\ldots$, E_{2n}, $\ldots$, E_{nn}, где E_{jk} — матричные единицы (см. решение задачи **??**, с. **??**); **(2)** $\dim=n$, базис $E_{11},\ldots,E_{nn}$; **(3)** $\dim=n(n+1)/2$, базис E_{11}, $\ldots$, E_{1n}, E_{22}, $\ldots$, E_{2n}, $\ldots$, E_{nn}; **(4)** $\dim=n(n+1)/2$, базис E_{11}, $\ldots$, E_{nn}, $E_{12}+E_{21}$, $E_{13}+E_{31}$, $\ldots$, $E_{n,n-1}+E_{n-1,n}$; **(5)** $\dim=n(n-1)/2$, базис $E_{12}-E_{21}$, $E_{13}-E_{31}$, $\ldots$, $E_{n,n-1}-E_{n-1,n}$. Обратите внимание, что подпространства из примеров (3) и (4) изоморфны.

5.4. Предположим, что существует нетривиальная линейная комбинация

$$\alpha_0\boldsymbol{x}_0+\alpha_1\boldsymbol{x}_1+\cdots+\alpha_n\boldsymbol{x}_n\equiv 0\iff\alpha_0+\alpha_1t+\cdots+\alpha_nt^n\equiv 0.$$

Ненулевой многочлен степени $\leqslant n$, стоящий в левой части, не может иметь более n корней, т.е. существует точка t_0, в которой $\alpha_0+\alpha_1t_0+\cdots+\alpha_nt_0^n\neq 0$, противоречие.

5.5. Данная задача сводится к упражнению 5.4.

5.6. (а) Поскольку $\arcsin x+\arccos x=\pi/2$, видим, что данные функции линейно зависимы:

$$1\cdot f_1(x)+1\cdot f_2(x)-\frac{\pi}{2}\cdot f_3(x)=0.$$

(б) Выясним, при каких коэффициентах α_1, α_2 равенство

$$\alpha_1g_1(x)+\alpha_2g_2(x)=0$$

выполняется при всех $x\in\mathbb{R}$. При $x>0$ это равенство даёт $\alpha_1x+\alpha_2x=0$ $\Leftrightarrow\ \alpha_1+\alpha_2=0$, а при $x<0$ — $\alpha_1x-\alpha_2x=0\Leftrightarrow\alpha_1-\alpha_2=0$. Система

уравнений

$$\begin{cases}\alpha_1+\alpha_2=0,\\ \alpha_1-\alpha_2=0\end{cases}$$

имеет лишь решение $\alpha_1=\alpha_2=0$, что означает линейную независимость рассматриваемых функций.

5.7. Неверно: если $\boldsymbol{x}_1=\boldsymbol{e}_1-\boldsymbol{e}_2$, $\boldsymbol{x}_2=\boldsymbol{e}_2-\boldsymbol{e}_3-\boldsymbol{e}_1$, то $\boldsymbol{x}_1+\boldsymbol{x}_2+\boldsymbol{e}_3=\boldsymbol{0}$.

5.8. Пусть

$$\boldsymbol{x}_1=\begin{pmatrix}x_1^1\\x_1^2\\\vdots\\x_1^n\end{pmatrix},\quad \boldsymbol{x}_2=\begin{pmatrix}x_2^1\\x_2^2\\\vdots\\x_2^n\end{pmatrix},\quad \ldots,\quad \boldsymbol{x}_{m+1}=\begin{pmatrix}x_{m+1}^1\\x_{m+1}^2\\\vdots\\x_{m+1}^n\end{pmatrix}.$$

Предположим, что у одного из векторов $\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_{m+1}$ первая компонента отлична от нуля; без ограничения общности можно считать, что это $\boldsymbol{x}_{m+1}$. Рассмотрим векторы

$$\boldsymbol{x}_1'=\boldsymbol{x}_1-\frac{x_1^1}{x_{m+1}^1}\boldsymbol{x}_{m+1},\ \boldsymbol{x}_2'=\boldsymbol{x}_2-\frac{x_2^1}{x_{m+1}^1}\boldsymbol{x}_{m+1},\ \ldots,\ \boldsymbol{x}_m'=\boldsymbol{x}_m-\frac{x_m^1}{x_{m+1}^1}\boldsymbol{x}_{m+1}.$$

Если же у всех векторов $\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_{m+1}$ первая компонента равна нулю, то просто отбросим один из них. В обоих случаях получим семейство m линейно независимых векторов, у которых первая компонента нулевая. Применим к этому семейству описанную процедуру для второй компоненты и т. д.

5.9. Если $\boldsymbol{x}_k$, $1\leqslant k\leqslant p$, выражается через $\boldsymbol{x}_1,\ldots,\boldsymbol{x}_{k-1}$, то семейство $\boldsymbol{x}_1,\ldots,\boldsymbol{x}_k$ линейно зависимо (предложение 5.36.3), а потому линейно зависимо и семейство $\boldsymbol{x}_1,\ldots,\boldsymbol{x}_p$ (предложение 5.36.4). (Случай $k=1$ означает, что $\boldsymbol{x}_1=\boldsymbol{0}$).

Обратно, если семейство $\boldsymbol{x}_1,\ldots,\boldsymbol{x}_p$ линейно зависимо, то существует такое наименьшее k, $1\leqslant k\leqslant p$, что семейство $\boldsymbol{x}_1,\ldots,\boldsymbol{x}_k$ линейно зависимо ($k=1\ \Leftrightarrow\ \boldsymbol{x}_1=\boldsymbol{0}$). Пусть $\alpha_1\boldsymbol{x}_1+\cdots+\alpha_k\boldsymbol{x}_k=\boldsymbol{0}$ — равная нулевому вектору нетривиальная линейная комбинация векторов $\boldsymbol{x}_1,\ldots,\boldsymbol{x}_k$. Ясно, что $\alpha_k\neq 0$, поскольку при $\alpha_k=0$ получится, что, вопреки предположению, линейно зависимо семейство $\boldsymbol{x}_1,\ldots,\boldsymbol{x}_{k-1}$. Отсюда получаем

$$\boldsymbol{x}_k=-\frac{\alpha_1}{\alpha_k}\boldsymbol{x}_1-\cdots-\frac{\alpha_{k-1}}{\alpha_k}\boldsymbol{x}_{k-1}.$$

5.10. Предположим противное, т.е. пусть $\alpha_1,\ldots,\alpha_s$ — такие коэффициенты, среди которых хотя бы один ненулевой, что

$$\alpha_1\boldsymbol{x}_1+\ldots\alpha_s\boldsymbol{x}_s=\boldsymbol{0},$$

т.е.

$$\alpha_1x_1^p+\ldots\alpha_sx_s^p=0\quad\forall p=1,\ldots,n.$$

Пусть для определённости α_1 — наибольшее по модулю среди чисел $\alpha_1,\ldots,\alpha_s$. Так как

$$\alpha_1x_1^1+\alpha_2x_2^1+\ldots\alpha_sx_s^1=0,$$

то

$$\left|\alpha_1 x_1^1\right| = \left|\alpha_2 x_2^1 + \cdots + \alpha_s x_s^1\right| \leqslant |\alpha_1|\left(|x_2^1| + \cdots + |x_s^1|\right) \leqslant |\alpha_1| \cdot |x_2^1|,$$

противоречие.