ВЫСШЕЕ
ОБРАЗОВАНИЕ

С. В. Ларин

Числовые системы

2-е издание

УМО ВО
РЕКОМЕНДУЕТ

Юрайт
издательство
biblio-online.ru

С. В. Ларин

ЧИСЛОВЫЕ СИСТЕМЫ

УЧЕБНОЕ ПОСОБИЕ ДЛЯ ВУЗОВ

2-е издание, исправленное и дополненное

Рекомендовано Учебно-методическим отделом высшего образования в качестве учебного пособия для студентов высших учебных заведений, обучающихся по естественнонаучным направлениям

Курс с практическими заданиями и дополнительными материалами доступен на образовательной платформе «Юрайт», а также в мобильном приложении «Юрайт.Библиотека»

Москва ▪ Юрайт ▪ 2024

УДК 511(075.8)
ББК 22.1я73
Л25

Автор:

Ларин Сергей Васильевич — кандидат физико-математических наук, профессор кафедры алгебры, геометрии и методики их преподавания Института математики, физики и информатики Красноярского государственного педагогического университета имени В. П. Астафьева.

Рецензенты:

Глухов М. М. — доктор физико-математических наук, профессор Академии ФСБ России;

кафедра математического анализа и методики преподавания математики Московского городского педагогического университета.

Ларин, С. В.

Л25 Числовые системы : учебное пособие для вузов / С. В. Ларин. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2024. — 130 с. — (Высшее образование). — Текст : непосредственный.

ISBN 978-5-534-19859-1

В учебном пособии даны аксиоматические определения системы натуральных, целых, рациональных, действительных чисел и кватернионов. В нем представлены свойства каждой числовой системы, доказан изоморфизм одноименных числовых систем, а также рассмотрены основные теоремы теории числовых систем.

Соответствует актуальным требованиям Федерального государственного образовательного стандарта высшего образования.

Для студентов бакалавриата, обучающихся по естественнонаучным направлениям.

УДК 511(075.8)
ББК 22.1я73

Разыскиваем правообладателей и наследников Ларина С. В.: https://www.urait.ru/inform
Пожалуйста, обратитесь в Отдел договорной работы: +7 (495) 744-00-12; e-mail: expert@urait.ru

Все права защищены. Никакая часть данной книги не может быть воспроизведена в какой бы то ни было форме без письменного разрешения владельцев авторских прав.

ISBN 978-5-534-19859-1

© Ларин С. В.,
© Ларин С. В., 2017, с изменениями
© ООО «Издательство Юрайт», 2024

Оглавление

Предисловие

Усвоение понятия числа проходит несколько этапов: от интуитивного представления о числах к анализу знаний о них, выделению в этих знаниях первичных истин, выстраиванию знаний о числах аксиоматически. В курсе «Числовые системы» студентам предоставляется возможность с высоты накопленных знаний проанализировать школьные утверждения о числах, понять, о чем порой умалчивают школьные учебники, говоря о числах, какие научные основы скрываются за упрощенным, образным изложением соответствующего материала в школе.

Пособие адресовано студентам математических специальностей педагогических вузов. В нем изложен семестровый материал по дисциплине «Числовые системы» в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки «Педагогическое образование» (уровень бакалавриат). Цель дисциплины — углубить и расширить представление будущего учителя математики о числах, перевести интуитивные знания о числах на твердую основу выводов, исходя из аксиом.

Особенностью изложения материала является его школьная направленность. При формулировке аксиоматического определения каждой числовой системы, изучаемой в школе, дается анализ школьного определения соответствующих чисел. Отрабатывается техника доказательств по индукции. Большое внимание уделяется представлению рациональных и действительных чисел десятичными дробями, что позволяет дать полное обоснование соответствующего школьного материала.

Несколько слов о месте дисциплины «Числовые системы» в общей системе подготовки школьного учителя. С одной стороны, школьный учитель не может состояться без упомянутых знаний, а значит, дисциплину нельзя исключить из бакалавриата и перенести в программу магистратуры. С другой стороны, может возникнуть искушение начать обучение в вузе с обоснования «учения о числах», а затем использовать числа в разных дисциплинах, опираясь на этот «вводный материал». Но вчерашний школьник не в состоянии, например, понять, зачем так трудно и такой долгой дорогой доказывается «очевидное» утверждение о том, что во всяком непустом подмножестве натуральных чисел есть самое маленькое число. Доказательство «очевидного с помощью непонятного» вызывает естественное отторжение. Таким образом, место дисциплины «Числовые системы» на последнем курсе подготовки ба-

калавра, что позволяет посмотреть на числа с высоты накопленных знаний и понять, что в них первично.

Несколько слов об обозначениях. Все определения и утверждения, начиная со второй главы, пронумерованы тремя числами: номер главы, номер параграфа и номер определения или утверждения в этом параграфе. В первой вводной главе нет параграфов, поэтому используется двойная нумерация. Конец доказательства помечается значком □. Знак $\Leftrightarrow$ заменяет слова «тогда и только тогда, когда». При доказательстве теоремы вида $A \Leftrightarrow B$ начало доказательства утверждения $A \Rightarrow B$ обозначается знаком ($\Rightarrow$), а начало доказательства обратного утверждения $B \Rightarrow A$ — знаком ($\Leftarrow$). Остальные не общепринятые значки вводятся и объясняются по мере надобности.

Тема 1
ПЕРВИЧНЫЕ ПОНЯТИЯ

Числовые и алгебраические системы

Числовая система — это числовое множество и некоторая совокупность операций и отношений, определенных на этом множестве. Так, с множеством натуральных чисел N мы рассмотрим системы $\langle N, + \rangle$, $\langle N, +, \cdot \rangle$, $\langle N, < \rangle$ и $\langle N, +, \cdot, < \rangle$. Например, последняя запись читается так: система с основным множеством N, бинарными операциями сложения «плюс» и умножения «точка» и бинарным отношением «меньше». Если вместо N взять произвольное множество A и через Ω_F обозначить некоторую совокупность операций, определенных на A, а через Ω_P — совокупность отношений, определенных на этом же множестве, то получим систему $\langle A, \Omega_F, \Omega_P \rangle$, которая называется *алгебраической системой*, причем A называется *основным множеством* системы.

Определяя различные числовые системы, мы будем пользоваться понятиями полугруппы, группы, кольца, поля и т. п. Определения этих понятий будут даваться по мере надобности. Их использование позволяет в краткой форме указать на выполнимость тех свойств, которые заложены в соответствующем определении. Например, систему целых чисел мы определим как кольцо, удовлетворяющее определенным условиям. Здесь одним словом «кольцо» мы заменяем целый список требований, фигурирующих в определении кольца.

Говоря о числах, нельзя не говорить об операциях сложения и умножения, а также об отношении «меньше». Поскольку нашей целью является указание некоторых твердых основ в понимании чисел, то мы должны дать общие определения бинарной операции и бинарного отношения. Проанализируем наши представления об этих понятиях. Начнем с анализа знакомого с детства сложения натуральных чисел. Эту бинарную операцию можно рассматривать как отображение, сопоставляющее всякой упорядоченной паре натуральных чисел некоторое третье число. Например, упорядоченной паре (2, 3) по правилу + ставится в соответствие число 5, что записывается в виде $2 + 3 = 5$. Этот пример показывает, что прежде чем дать определение бинарной операции, нужно предварительно определить, что такое упорядоченная пара и что такое отображение. Отношение «меньше» для натуральных чисел выступает как свойство, объединяющее эти числа в упорядоченные пары, и может быть определено полным списком соответствующих упорядоченных пар. В этой трактовке вместо $2 < 3$, $5 < 7$, $3 < 8$ говорят, что упорядоченные пары

(2, 3), (5, 7), (3, 8) принадлежат отношению «меньше», понимая под отношением «меньше» список всех упорядоченных пар, определяющий это отношение. Это наталкивает на мысль определить произвольное бинарное отношение как некоторое множество упорядоченных пар. В следующем пункте приведены строгие определения этих и других основных понятий, которые будут использованы в дальнейшем.

Заметим, что хотя нашей целью является изложение аксиоматических теорий основных числовых систем, в примерах, поясняющих абстрактные понятия, мы будем использовать числа до их аксиоматического определения. При этом N, Z, Q, R, C будут обозначать соответственно множества натуральных, целых, рациональных, действительных и комплексных чисел.

Определения основных понятий

Начиная дедуктивное изложение материала, в качестве базовых неопределяемых понятий берем понятия «множество» и «элемент множества». Если x является элементом множества A, то, как обычно, будем писать: $x \in A$, в противном случае: $x \notin A$. Например, $1 \in N$, $0 \notin N$, $0 \in Z$, $\sqrt{2} \notin Q$.

1.1. Определение. Множество называется *пустым* и обозначается $\varnothing$, если оно не содержит ни одного элемента.

Например, множество всех действительных чисел, удовлетворяющих уравнению $x^2 + 1 = 0$, пусто.

1.2. Определение. Множество A называется *подмножеством* множества B (записывается: $A \subseteq B$), если для любого x из того, что $x \in A$, следует, что $x \in B$.

Например, $N \subseteq Z \subseteq Q \subseteq R$; $\{1, 2, 2\} \subseteq \{1, 2, 3\}$. Очевидно, $A \subseteq A$ и $\varnothing \subseteq A$ для любого множества A.

1.3. Определение. Множества A и B называются *равными* (записывается: $A = B$), если $A \subseteq B$ и $B \subseteq A$.

Из этого определения вытекает единственность пустого множества.

1.4. Определение. Множество A называется *собственным подмножеством* множества B (записывается: $A \subset B$), если $A \subseteq B$ и $A \neq B$.

Запись $\{\ldots | ***\}$ означает: множество всех элементов ... таких, что ***. Например, запись $\{x | x \in Z,\ x \vdots 2\}$ читается так: «множество всех элементов x таких, что x является элементом множества Z и x делится на 2» (знак $\vdots$ обозначает «делится»). Другими словами, это множество всех четных целых чисел, которое кратко обозначается через $2Z$. Используются и такие записи: $2Z = \{x \in Z | x \vdots 2\} = \{2n | n \in Z\}$. Заменив здесь 2 на произвольное целое число m, получим $mZ = \{mn | n \in Z\}$ — множество всех целых чисел, кратных m.

1.5. Определение. *Объединением* множеств A и B называется множество $A \cup B = \{x | x \in A$ или $x \in B\}$.

Например, $2Z \cup 3Z = \{x \in Z | x \vdots 2$ или $x \vdots 3\}$.

1.6. Определение. *Пересечением* множеств A и B называется множество $A \cap B = \{x | x \in A$ и $x \in B\}$.

Например, $2Z \cap 3Z = 6Z$.

Если $A \cap B = \varnothing$, то говорят, что множества A и B *не пересекаются*. Например, множество натуральных и множество целых отрицательных чисел не пересекаются.

1.7. Определение. *Разностью* множеств A и B называется множество $A \setminus B = \{x \mid x \in A \text{ и } x \notin B\}$.

Например, $\{1,2,3\} \setminus \{1,3,5\} = \{2\}$; $\{1,3,5\} \setminus \{1,2,3\} = \{5\}$.

1.8. Определение. Множество $\{a,b\}$ с выделенным в нем первым элементом a и вторым элементом b называется *упорядоченной парой* и обозначается через (a, b). (Выделить первый и второй элементы пары можно, например, назвав упорядоченной парой множество $\{\{a\},\{a,b\}\}$).

1.9. Определение. *Прямым произведением* множеств A и B называется множество $A \times B = \{(a,b) \mid a \in A, b \in B\}$.

Например, если $A = \{1,2,3\}$, $B = \{a,b\}$, то $A \times B = \{(1,a);(1,b);(2,a);(2,b);(3,a);(3;b)\}$. Заметим, что здесь $A \times B \neq B \times A$.

1.10. Определение. *Бинарным отношением на упорядоченной паре множеств* (A, B) называется всякое подмножество прямого произведения $A \times B$. *Бинарным отношением на множестве* A называется всякое подмножество прямого произведения $A \times A$.

Если α — бинарное отношение и $(a,b) \in \alpha$, то будем писать также либо $a\alpha b$, либо $\alpha(a) = b$, либо $a^{\alpha} = b$. Выбор той или иной записи диктуется традицией. Например, принято писать $2 < 3, f(x) = y$.

Если дана некоторая последовательность (a_n), то, выделяя упорядоченные пары (a_n, a_{n+1}), $n = 0, 1, \ldots$, мы получаем бинарное отношение, которое удобно записывать в виде $a_{n+1} = a_n'$ и читать: a_{n+1} непосредственно следует за a_n. Здесь отношение «штрих» обозначает бинарное отношение «непосредственно следует за».

Выберем случайным образом несколько упорядоченных пар целых чисел: $\{(-3, 2), (5, 6), (7, 9)\}$ — это также бинарное отношение на множестве Z. Если обозначить его через α, то можно записать: $(-3,2) \in \alpha$, $5\alpha 6$, $7^{\alpha} = 9$, $\alpha(5) = 6$.

1.11. Определение. Бинарное отношение α, определенное на множестве A, называется *отношением эквивалентности*, если оно:

1) рефлексивно, т. е. для любого $a \in A$ имеет место $a\alpha a$;
2) симметрично, т. е. для любых $a, b \in A$, если $a\alpha b$, то $b\alpha a$;
3) транзитивно, т. е. для любых $a, b, c \in A$, если $a\alpha b$ и $b\alpha c$, то $a\alpha c$.

Если α — отношение эквивалентности на множестве A, то A распадается на непересекающиеся классы эквивалентных элементов. Примерами отношений эквивалентности являются: отношение равенства на множестве целых чисел, отношение коллинеарности на множестве прямых плоскости, отношение сравнимости целых чисел по данному модулю (напомним, что два целых числа a и b называются сравнимыми по модулю m, $m \in N$, если их разность делится на m. При этом пишут: $a \equiv b (\mathrm{mod}\, m)$. Например, $17 \equiv 5 (\mathrm{mod}\, 6)$). Опишите соответствующие классы эквивалентных элементов.

1.12. Определение. Бинарное отношение φ, определенное на паре множеств (A, B), называется *отображением A в B*, что записывается: $\varphi : A \to B$, если для всякого $a \in A$ существует и притом единственный элемент $b \in B$ такой, что $\varphi(a) = b$. При этом b называется *образом* элемента a. Говорят также, что элементу a *ставится в соответствие* элемент b. Образом множества A называется множество $\varphi(A) = \{\varphi(a) \mid a \in A\}$.

На рис. 1 отношения f, φ и ψ являются отображениями, а отношения α и β не являются. Почему?

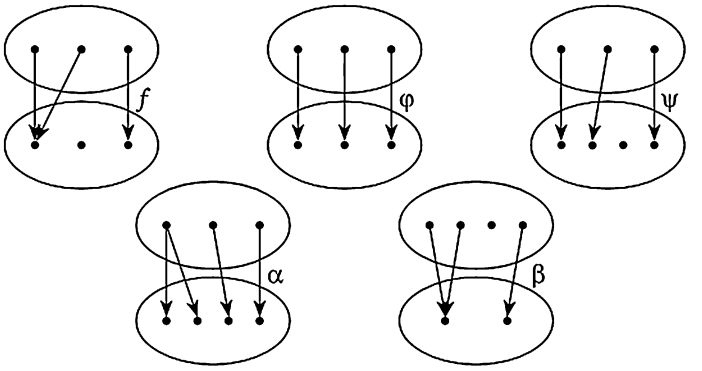

Рис. 1

1.13. Определение. Отображение $\varphi : A \to B$ называется *отображением A на B*, если для всякого $b \in B$ существует $a \in A$ такой, что $\varphi(a) = b$, т. е. всякий элемент из B является образом некоторого элемента из A.

На рис. 1 отображение φ является отображением «на», а f и ψ не являются таковыми.

1.14. Определение. Отображение $\varphi : A \to B$ называется *взаимно однозначным* (*инъективным*) *отображением A в B*, если различные элементы из A имеют разные образы в B, т. е., из $a \neq a_1$ следует $\varphi(a) \neq \varphi(a_1)$.

На рис. 1 отображения φ и ψ являются взаимно однозначными, а отображение f — нет.

1.15. Определение. Пусть φ — взаимно однозначное отображение множества A на множество B. Определим отображение $\varphi^{-1} : B \to A$, положив для любых $a \in A$, $b \in B$ $\varphi^{-1}(b) = a$, если $\varphi(a) = b$. Отображение φ^{-1} называется *обратным отображением* для φ.

На рис. 1 только для φ существует обратное отображение.

Теперь у нас все готово для определения бинарной операции.

1.16. Определение. Пусть $A \neq \varnothing$. *Бинарной операцией на множестве A* называется отображение прямого произведения $A \times A$ в множество A.

Например, сложение целых чисел есть отображение $+ : Z \times Z \to Z$.

Мы подошли к определению одного из важнейших понятий в математике, уточняющем представление об «одинаковости» двух алгебраических систем, — понятия изоморфизма. Образно говоря, две алгебраические системы, например $\langle A, +, < \rangle$ и $\langle A_1, \oplus, \lhd \rangle$, считаются одинаковыми,

если они «при наложении» «совпадают». При этом, термин «одинаковые» заменяется термином «изоморфные», «наложение» понимается как взаимно однозначное отображение φ множества A на множество A_1, а «совпадение» трактуется как «сохранение операции и отношения», которое заключается в том, что при отображении φ («наложении») сумма элементов из A отображается в («накладывается на») сумму образов этих элементов, и в A один элемент «меньше» другого тогда и только тогда, когда в A_1 образ первого элемента «меньше» образа второго элемента (рис. 2).

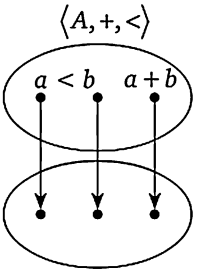

Рис. 2

Дадим строгие определения изоморфизма лишь для алгебраических систем тех видов, которые будем рассматривать в дальнейшем.

1.17. Определение. Системы с одной бинарной операцией $\langle A, + \rangle$ и $\langle A_1, \oplus \rangle$ называются *изоморфными*, если существует взаимно однозначное отображение φ множества A на множество A_1, которое сохраняет операцию, т. е. для любых $x, y \in A$ $\varphi(x + y) = \varphi(x) \oplus \varphi(y)$. Системы с двумя бинарными операциями $\langle A, +, \cdot \rangle$ и $\langle A_1, \oplus, \bullet \rangle$ называются *изоморфными*, если существует взаимно однозначное отображение φ множества A на множество A_1, при котором сохраняются обе операции, т. е. для любых $x, y \in A$ $\varphi(x + y) = \varphi(x) \oplus \varphi(y)$ и $\varphi(x \cdot y) = \varphi(x) \bullet \varphi(y)$. Системы с одним бинарным отношением $\langle A, < \rangle$ и $\langle A_1, \lhd \rangle$ называются *изоморфными*, если существует взаимно однозначное отображение φ множества A на множество A_1, при котором сохраняется отношение, т. е. для любых $x, y \in A$, $x < y$ тогда и только тогда, когда $\varphi(x) \lhd \varphi(y)$. Наконец, системы с двумя бинарными операциями и одним бинарным отношением $\langle N, +, \cdot, < \rangle$ и $\langle A_1, \oplus, \bullet, \lhd \rangle$ называются *изоморфными*, если существует взаимно однозначное отображение φ множества A на множество A_1, при котором сохраняются операции и отношение. При этом, в каждом случае φ называется *изоморфизмом* первой алгебраической системы на вторую. Вторая система называется *изоморфным образом* первой системы.

Например, системы $\langle Z, +, < \rangle$ и $\langle 2Z, +, < \rangle$ изоморфны (одинаковы), так как взаимно однозначное отображение $\varphi : Z \to 2Z$, при котором для любого $x \in Z$ $\varphi(x) = 2x$, сохраняет операцию сложения и отношение «меньше»: $\varphi(x + y) = 2(x + y) = 2x + 2y = \varphi(x) + \varphi(y)$, и $x < y$ тогда и только тог-

да, когда $2x < 2y$, т. е. $\varphi(x) < \varphi(y)$. Образно говоря, при «наложении» φ системы $\langle Z, +, < \rangle$ и $\langle 2Z, +, < \rangle$ «совпадают».

Иногда наложение изоморфных алгебраических систем одной на другую приносит реальные плоды. Например, система $\langle R^+, \cdot \rangle$, где R^+ — положительные действительные числа, изоморфна системе $\langle R, + \rangle$, так как для любых $x, y \in R^+$ $\lg(x \cdot y) = \lg x + \lg y$, т. е, отображение lg является изоморфизмом. Идея наложения системы $\langle R^+, \cdot \rangle$ на систему $\langle R, + \rangle$ привела к созданию логарифмической линейки с логарифмическими шкалами. На такой шкале строится число $\lg(x)$, а соответствующая точка обозначается числом x (рис. 3).

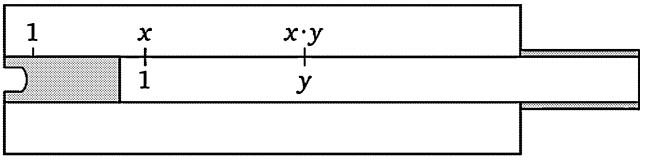

Рис. 3

В результате, выполняя на логарифмической линейке механическое сложение (находясь в $\langle R, + \rangle$), мы считываем результат умножения (переходя в $\langle R^+, \cdot \rangle$).

Тема 2
НАТУРАЛЬНЫЕ ЧИСЛА

§ 1. Натуральный ряд

Формирование определения

Использование натуральных чисел при счете формирует представление о них как о бесконечно длинном «числовом строе» с единицей «во главе»:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, … .

Постараемся сформулировать наиболее существенные свойства этого «числового строя» и его описание примем за аксиоматическое определение натурального ряда. Замечаем, что взаимное расположение чисел можно охарактеризовать с помощью словосочетания «непосредственно следует за». Так, за 1 непосредственно следует 2, за 2 непосредственно следует 3, и т. д. Помечая отношение «непосредственно следует за» значком «штрих», можно записать: $1' = 2$, $2' = 3$, … .

Рассматриваемое множество натуральных чисел обозначим через N. Отметим в нем наличие первого числа — и это даст нам первую аксиому, описывающую натуральный ряд: *в N существует натуральное число* 1, *которое непосредственно не следует ни за каким натуральным числом*. Далее, видим, что *за каждым натуральным числом непосредственно следует и притом только одно натуральное число* — это вторая аксиома натурального ряда. Третья аксиома подмечает, что *всякое натуральное число непосредственно следует не более чем за одним натуральным числом*, учитывая, что 1 не следует ни за каким натуральным числом. Наконец, четвертая аксиома дает признак, когда подмножество натуральных чисел совпадает со всем множеством N. Она утверждает, что *если подмножество* $M \subseteq N$ *содержит единицу* (первое условие) и *вместе с каждым своим числом содержит непосредственно следующее за ним число* (второе условие), *то M должно совпадать с N*. К такому заключению нас приводят следующие рассуждения. По первому условию $1 \in M$, но тогда по второму условию $2 \in M$, так как 2 непосредственно следует за 1; снова по второму условию заключаем, что $3 \in M$, и т. д. Таким образом, мы убеждаемся, что $M = N$. Четвертая аксиома формализует метод рассуждений по принципу «и т. д». Кроме того, эта аксиома, как будет показано в дальнейшем, позволяет обо-

сновать доказательства по индукции, поэтому ее называют *аксиомой индукции*.

Итак, натуральный ряд описывается четырьмя подмеченными аксиомами, которые называются аксиомами Пеано по имени итальянского математика Дж. Пеано (1858—1932). Сформулируем строгое определение натурального ряда.

2.1.1. Определение. *Натуральным рядом* называется система $\langle N, ' \rangle$ с основным множеством N, элементы которого называются *натуральными числами*, бинарным отношением «штрих», которое записывается в виде $n = m'$, читается: «*n непосредственно следует за m*», причем выполняются следующие *аксиомы Пеано*.

P_1. В N существует элемент 1, называемый единицей, который непосредственно не следует ни за каким натуральным числом, т. е. $1 \neq n'$ для любого $n \in N$.

P_2. За каждым натуральным числом непосредственно следует и притом только одно натуральное число. Другими словами, для всякого $m \in N$ существует $n \in N$ такое, что $n = m'$, причем если $m = k$, то $m' = k'$.

P_3. Каждое натуральное число непосредственно следует не более чем за одним натуральным числом, т. е. для любых $m, k \in N$, если $m' = k'$, то $m = k$.

P_4 (аксиома индукции). Пусть подмножество $M \subseteq N$ удовлетворяет следующим условиям:

1) $1 \in M$ (другими словами, M содержит элемент, который непосредственно не следует ни за каким натуральным числом);

2) для любого натурального числа n если $n \in M$, то $n' \in M$.

Тогда M совпадает с N.

Подчеркнем абстрактный характер определения натурального ряда. Множество N может быть любой природы, отношение «штрих» может быть как угодно задано, но если выполняются аксиомы Пеано, то система $\langle N, ' \rangle$ является натуральным рядом. Так, натуральным рядом можно было бы назвать номерки на бесконечно длинной вешалке, бесконечно длинный поезд с локомотивом в начале поезда, бесконечную очередь за дефицитом с первым счастливчиком в начале очереди, и т. д.

С натуральным рядом тесно связано понятие последовательности.

2.1.2. Определение. Пусть A — непустое множество. Всякое отображение $f : N \to A$ называется *последовательностью*. Образ элемента $n \in N$ при отображении f называется n-м членом последовательности. Если $f(n) = a_n$ для любого $n \in N$, то последовательность записывается в виде (a_n).

Всякую последовательность (a_n) можно превратить в натуральный ряд, введя отношение непосредственного следования естественным образом: $a'_n = a_{n'}$ для любого $n \in N$. Если N_1 — множество всех членов последовательности, то система $\langle N_1, ' \rangle$, очевидно, удовлетворяет всем аксиомам Пеано, а значит, является натуральным рядом. Здесь «единицей» будет первый член последовательности a_1, за «единицей» непосредственно следует «натуральное число» a_2, и т. д.

Независимость аксиом Пеано

Естественно возникает вопрос: не является ли одна из аксиом Пеано лишней, вытекающей из остальных аксиом? Чтобы доказать независимость каждой из аксиом от остальных, достаточно для каждого $i=1,2,3,4$ построить такую систему $\langle N_i,'\rangle$, для которой аксиома P_i не выполняется, а остальные аксиомы Пеано выполняются. Реализуем эту идею.

2.1.3. Теорема. *Система аксиом Пеано независима.*

Доказательство. 1. Докажем независимость аксиомы P_1 от остальных аксиом Пеано. Для этого на множестве $N_1=\{1,2,3\}$ определим отношение «штрих», положив $1'=2$, $2'=3$, $3'=1$ (на рис. 4 непосредственное следование помечено стрелками). Рассмотрим систему $\langle N_1,'\rangle$. Очевидно, аксиома P_1 не выполняется, так как всякий элемент из N_1 непосредственно следует за некоторым элементом этого множества. Остальные же аксиомы Пеано выполняются. Выполнимость аксиомы P_4 следует из того, что в N_1 нет подмножеств, содержащих элемент, который непосредственно не следовал бы ни за каким элементом.

2. Независимость аксиомы P_2. Аксиома P_2 содержит два утверждения: о существовании непосредственно следующего элемента и о его единственности. Установим независимость каждого из этих утверждений от остальных аксиом Пеано.

На множестве $N_{21}=\{1,2\}$ определим $1'=2$ и рассмотрим систему $\langle N_{21},'\rangle$. Первая часть аксиомы P_2, а значит и вся аксиома, не выполняется, а все остальные аксиомы Пеано выполняются.

Далее, пусть $N_{22}=\{1,2,3,a_3,4,a_4,\ldots\}$. Положим $1'=2$, $2'=3$, $3'=4$, …, $2'=a_3$, $a_3'=a_4$, … . Рассмотрим систему $\langle N_{22},'\rangle$ (рис. 5). Легко видеть, что вторая часть аксиомы P_2, а значит и вся аксиома, не выполняется, а все остальные аксиомы выполняются.

3. Независимость аксиомы P_3.

Пусть $N_3=\{1,2,3,4\}$. Положим $1'=2$, $2'=3$, $3'=4$, $4'=2$ (рис. 6). Очевидно, система $\langle N_3,'\rangle$ не удовлетворяет аксиоме P_3, но удовлетворяет остальным аксиомам Пеано.

4. Независимость аксиомы P_4.

Пусть $N_4=\{1,a_1,2,a_2,3,a_3,\ldots\}$. Определим $1'=2$, $2'=3$, …, $a_1'=a_2$, $a_2'=a_3$, … (рис. 7). Очевидно, система $\langle N_4,'\rangle$ удовлетворяет первым трем аксиомам Пеано. Докажем, что аксиома P_4 не выполняется. Рассмотрим подмножество $M=\{1,2,3,\ldots\}\subseteq N_4$. Имеем: 1) $1\in M$; 2) если $n\in M$, то $n'\in M$. Но $M\neq N$.

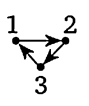

Рис. 4

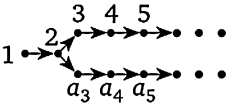

Рис. 5

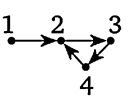

Рис. 6

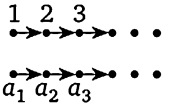

Рис. 7

О непротиворечивости аксиоматической теории натуральных чисел

Нет ли противоречия в аксиоматическом определении натуральных чисел 2.1.1? Чтобы положительно ответить на этот вопрос, Д. Гильберт (1862—1943) предложил формализовать аксиоматическую теорию натуральных чисел так, чтобы доказательства в ней превратились в «механическое манипулирование» с основными понятиями теории по определенным правилам, не допускающим появления противоречий, а затем средствами самой теории доказать ее непротиворечивость, т. е. невозможность появления в ней одновременно некоторого утверждения A и его отрицания $\overline{A}$ (не A). Формальная аксиоматическая теория характеризуется заданием языка теории, аксиом теории и правил вывода. Однако в 1931 г. К. Гедель (1906—1978) доказал, что непротиворечивость любой формальной аксиоматической теории, включающей в себя формальную арифметику (т. е. теорию натуральных чисел), не может быть доказана средствами самой теории. Это вытекает из другого поразительного результата, известного под названием теоремы Геделя о неполноте. Она утверждает, что если формальная аксиоматическая теория, включающая в себя формальную арифметику, непротиворечива, то она не полна, т. е. содержит утверждение, которое нельзя ни доказать, ни опровергнуть средствами этой теории. С привлечением дополнительных средств, не формализуемых в самой теории, Г. Генцен в 1936 г. установил непротиворечивость формальной арифметики. Независимо эта же задача была решена П. С. Новиковым (1901—1974).

В дальнейшем, исходя из непротиворечивости теории натуральных чисел, мы докажем непротиворечивость каждой из последующих числовых систем. Для этого мы построим каждую следующую числовую систему из материала предыдущей. Так, целые числа будут «сделаны» из натуральных, рациональные — из целых и т. д. Таким образом, если бы в теории какой-то из числовых систем было противоречие, то оно оказалось бы следствием аксиом Пеано, что противоречило бы непротиворечивости аксиоматической теории натуральных чисел. Имея в виду эту цепочку построений и особую роль в ней натуральных чисел, хочется повторить знаменитые слова Л. Кронекера (1823—1891) в несколько вольном переводе: «натуральные числа сотворил господь бог, а все прочее — дело рук человеческих». Кронекер полагал, что в основе всей математики должна лежать арифметика.

Принцип полной математической индукции

Аксиома индукции служит для обоснования мощного метода доказательства теорем, который основан на следующем утверждении.

2.1.4. Теорема (принцип полной математической индукции). *Предложение $T(n)$ с переменной $n \in N$ верно для любого натурального числа n, если выполнены следующие условия*:

1) *это предложение верно для* $n = 1$, *т. е.* $T(1)$ *истинно*;

2) *каково бы ни было натуральное число* n, *из предположения о том, что это предложение верно для* n, *следует, что оно верно для непосредственно следующего натурального числа* n', *т. е. если* $T(n)$ *истинно, то и* $T(n')$ *истинно.*

Доказательство. Обозначим через M множество всех натуральных чисел, для которых $T(n)$ истинно:

$$M = \{n \in N \mid (n) \text{ истинно}\}.$$

Из условия 1) следует, что $1 \in M$. Пусть натуральное число $n \in M$. Тогда $T(n)$ истинно и, по условию 2), должно быть истинно $T(n')$, а значит, $n' \in M$. Таким образом, оба условия аксиомы индукции P_4 выполнены, следовательно, $M = N$. Но это и означает, что $T(n)$ верно для любого $n \in N$. □

Доказательство на основании принципа полной математической индукции называется *доказательством методом полной математической индукции*. При этом, говорят кратко: докажем $T(n)$ индукцией по n. Проверка истинности утверждения $T(1)$ называется *началом индукции*, предположение об истинности $T(n)$ называется *индуктивным предположением*, а доказательство истинности $T(n')$, исходя из истинности $T(n)$, называется *шагом индукции*. Эта терминология восходит к наглядному представлению о процессе доказательства по индукции, изображенному на рис. 8.

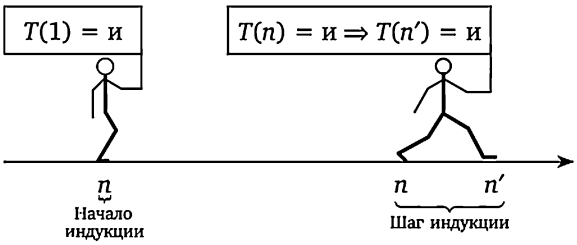

Рис. 8

Приведем типичный пример доказательства по индукции и обсудим технику записи доказательства.

Пример

Докажите, что сумма первых n нечетных натуральных чисел равна n^2.
В нашем случае утверждение $T(n)$ имеет вид

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

Доказательство.

1) $n = 1$. *Проверим, что* $1 = 1^2$. Очевидно, это равенство *верно*.

2) *Пусть* $1+3+5+\ldots+(2n-1)=n^2$.

Докажем, что $1+3+5+\ldots+(2n+1)=(n+1)^2$. *Имеем*:

$$1+3+5+\ldots+(2n-1)+(2n+1) \overset{\text{и.п.}}{=} n^2+(2n+1)=(n+1)^2. \square$$

Выделенный курсивом текст составляет «бланк доказательства». Если убрать все остальное, то «бланк» готов для нового заполнения — доказательства нового утверждения. В п. 1) запись $T(1)$ получается из предложения $T(n)$ формальной заменой всюду n на 1. В п. 2) запись «*пусть..., докажем, что...*» понимается как «*пусть $T(n)$ истинно для фиксированного n, докажем, что $T(n+1)$ истинно*». При этом, $T(n+1)$ получается из $T(n)$ чисто формально: заменой n на $n+1$. Момент использования индуктивного предположения полезно выделять, помечая буквами «и.п.». Преобразования после использования индуктивного предположения можно охарактеризовать как «подгонка под ответ», так как речь идет о получении заранее сформулированного результата. Такая стандартизация доказательства по индукции позволяет выполнять его почти автоматически. Единственный момент, требующий размышлений, — это «подгонка под ответ».

§ 2. Сложение. Аддитивная полугруппа натуральных чисел

Сложение натуральных чисел

Продолжим построение аксиоматической теории натуральных чисел и введем на множестве N операцию сложения.

2.2.1. Определение. *Сложением натуральных чисел* называется бинарная операция $+$, определенная на N, которая удовлетворяет следующим условиям:

a) $m+1=m'$ для любого $m\in N$;

b) $m+n'=(m+n)'$ для любых $m,n\in N$.

Первое условие (или аксиома) сложения показывает, как к натуральному числу m прибавить единицу: для этого надо перейти к непосредственно следующему числу m'. Второе условие (или вторая аксиома) сложения показывает, как к m прибавить число n', если известна сумма $m+n$: для этого нужно перейти к непосредственно следующему за $m+n$ числу $(m+n)'$.

2.2.2. Теорема. *Сложение натуральных чисел существует и единственно.*

Доказательство. Сначала докажем существование не более одного сложения натуральных чисел. Пусть существует сложение $\oplus$, удовлетворяющее аналогичным условиям:

a') $m\oplus 1=m'$ для любого $m\in N$;

b') $m\oplus n'=(m\oplus n)'$ для любых $m,n\in N$.

Зафиксируем натуральное число m и индукцией по n докажем, что $m+n=m\oplus n$ для любых $m,n\in N$. При $n=1$ имеем:

$$m+1\overset{a)}{=}m'\overset{a')}{=}m\oplus 1.$$

(Значки над равенствами указывают на использование соответствующих свойств.)

Пусть $m+n=m\oplus n$, докажем, что $m+n'=m\oplus n'$. Имеем:

$$m+n' \overset{b)}{=} (m+n)' \overset{\text{и.п.}}{=} (m\oplus n)' \overset{b')}{=} m\oplus n'$$

(«и.п.» над равенством означает использование индуктивного предположения). Итак, доказано, что сложения + и ⊕ совпадают.

Докажем существование сложения натуральных чисел. Индукцией по m докажем, что для натурального числа m и произвольного натурального числа n существует и притом только одно натуральное число $m + n$ такое, что выполняются условия a) и b). Для $m = 1$ и произвольного натурального числа n определим $1+n=n'$. Проверим выполнимость условий a) и b). Пользуясь данным определением, получаем: $1 + 1 = 1'$, и для любого n имеем: $1+n'=(n')'=(1+n)'$. Следовательно, условия a) и b) выполняются.

Пусть для натурального числа m и произвольного натурального числа n существует однозначно определенное натуральное число $m + n$ такое, что выполняются условия a) и b). Для натурального числа m' и произвольного натурального числа n определим $m'+n=(m+n)'$. Проверим выполнимость условий a) и b) для $m' + n$. Имеем:

$$m'+1 \overset{\text{опр.}}{=} (m+1)' \overset{\text{и.п.}, a)}{=} (m')'$$

(«опр.» означает равенство по определению). Следовательно, условие a) выполняется. Для любого n имеем:

$$m'+n' \overset{\text{опр.}}{=} (m+n')' \overset{\text{и.п.}, b)}{=} ((m+n)')' \overset{\text{опр.}}{=} (m'+n)'$$

Следовательно, условие b) также выполняется. □

Пример

Пусть дан натуральный ряд $\langle N,'\rangle$ с единицей 1. Обозначим $1' = 2$, $2' = 3$, $3' = 4$, $4' = 5$. Пользуясь определением сложения 2.2.1 и введенными обозначениями, находим:

$$3+2=3+1' \overset{b)}{=} (3+1)' \overset{a)}{=} (3')'=4'=5.$$

Найдите аналогично 2 + 3.

Иронизируя по поводу этого примера, приведем слова М. Клайна из [7]: «...в 90-е годы XIX в., через каких-нибудь шесть тысяч лет (!) после того как египтяне и вавилоняне “пустили в оборот” целые числа, дроби и иррациональные числа, математики смогли наконец доказать, что 2 + 2 = 4».

Доказательство теоремы 2.2.2, отличаясь внешней простотой, содержит некоторые недомолвки. Дело в том, что сложение натуральных

чисел представляет собой отображение множества $N \times N$ в N, сопоставляющее всякой упорядоченной паре натуральных чисел (m, n) однозначно определенное натуральное число $m + n$, причем выполняются условия $a)$ и $b)$. В приведенном доказательстве речь идет в неявной форме о существовании и единственности именно этого отображения. Наметим доказательство теоремы 2.2.2 на языке отображений.

Замечаем, что при фиксированном первом слагаемом m отображение $N \times N$ в N определяет отображение $f_m : N \to N$, а условия $a)$ и $b)$ преобразуются в условия:

$a_m)$ $f_m(1) = m'$;

$b_m)$ $f_m(n') = (f_m(n))'$ для любого $n \in N$.

Для доказательства существования не более одного сложения натуральных чисел достаточно установить существование не более одного отображения $f_m : N \to N$, удовлетворяющего условиям $a_m)$ и $b_m)$. Предположим, что существует еще отображение $h_m : N \to N$, удовлетворяющее аналогичным условиям:

$c_m)$ $h_m(1) = m'$;

$d_m)$ $h_m(n') = (h_m(n))'$ для любого $n \in N$.

Индукцией по n легко доказать, что $f_m(n) = h_m(n)$ для любого $n \in N$, т. е. отображения f_m и h_m совпадают и это доказывает существование не более одного сложения натуральных чисел.

Теперь индукцией по m докажем, что для любого натурального числа m существует, а стало быть, только одно отображение $f_m : N \to N$, удовлетворяющее условиям $a_m)$ и $b_m)$. При $m = 1$ определим отображение $f_1 : N \to N$, положив $f_1(n) = n'$ для любого $n \in N$. Легко проверить, что f_1 удовлетворяет условиям $a_1)$ и $b_1)$.

Пусть существует отображение $f_m : N \to N$, удовлетворяющее условиям $a_m)$ и $b_m)$. Определим отображение $f_{m'} : N \to N$, положив $f_{m'}(n) = (f_m(n))'$ для любого $n \in N$. Нетрудно доказать, что $f_{m'}$ удовлетворяет условиям $a'_m)$ и $b'_m)$.

Итак, доказано, что для любого m существует и притом только одно отображение $f_m : N \to N$, удовлетворяющее условиям $a_m)$ и $b_m)$. Определим отображение множества $N \times N$ в N, сопоставляя всякой упорядоченной паре натуральных чисел (m, n) натуральное число $f_m(n)$, которое будем обозначать через $m + n$. Проверим выполнимость условий $a)$ и $b)$. Имеем:

$$m+1 \overset{\text{опр.}}{=} f_m(1) \overset{a_m)}{=} m'$$

для любого $m \in N$, и

$$m+n' \overset{\text{опр.}}{=} f_m(n') \overset{b_m)}{=} (f_m(n))' \overset{\text{опр.}}{=} (m+n)'$$

для любых $m, n \in N$. Следовательно, так определенное отображение $N \times N$ в N является сложением натуральных чисел.

Основные свойства сложения

Исходя из определения сложения натуральных чисел, докажем привычные свойства этой операции. При этом, как и выше, значки *a*) и *b*) над равенствами будут обозначать ссылки на соответствующие аксиомы сложения, а «и.п.» будет обозначать равенство по индуктивному предположению.

2.2.3. Предложение. *Сложение натуральных чисел ассоциативно*: $(k+m)+n=k+(m+n)$ *для любых* $k, m, n \in N$.

Доказательство — индукцией по n при произвольно выбранных k и m. При $n = 1$ получаем:

$$(k+m)+1 \overset{a)}{=} (k+m)' \overset{b)}{=} k+m' \overset{a)}{=} k+(m+1).$$

Пусть $(k+m)+n=k+(m+n)$, докажем, что $(k+m)+n'=k+(m+n')$. Имеем:

$$(k+m)+n' \overset{b)}{=} ((k+m)+n)' \overset{\text{и.п.}}{=} (k+(m+n))' \overset{b)}{=} k+(m+n)' \overset{b)}{=} k(m+n'). \square$$

2.2.4. Предложение. *Сложение натуральных чисел коммутативно*: $m + n = n + m$ *для любых* $m, n \in N$.

Доказательство. Вначале индукцией по m докажем, что $m + 1 = 1 + m$ для любого $m \in N$. При $m = 1$ утверждение очевидно. Пусть $m + 1 = 1 + m$, докажем, что $m'+1=1+m'$. Имеем:

$$m'+1 \overset{a)}{=} (m+1)+1 \overset{\text{и.п.}}{=} (1+m)+1 \overset{2.2.3}{=} 1+(m+1) \overset{a)}{=} 1+m'.$$

Теперь зафиксируем $m \in N$ и индукцией по n докажем, что $m+n=n+m$ для любого $n \in N$. При $n = 1$ утверждение доказано. Пусть $m+n=n+m$, докажем, что $m+n'=n'+m$. Имеем:

$$m+n' \overset{b)}{=} (m+n)' \overset{\text{и.п.}}{=} (n+m)' \overset{b)}{=} n+m' \overset{a)}{=} n+(m+1) = n+(1+m) \overset{2.2.3}{=}$$

$$= (n+1)+m \overset{a)}{=} n'+m. \square$$

2.2.5. Предложение. *Операция сложения натуральных чисел обладает свойством сократимости: если* $k+n=m+n$, *то* $k = m$ *каковы бы ни были* $k, m, n \in N$.

Доказательство проведем индукцией по n при произвольно выбранных k и m. При $n = 1$ условие принимает вид: $k+1=m+1$, откуда по аксиоме сложения *a*) получаем $k' = m'$ и по аксиоме P_3 заключаем, что $k = m$.

Пусть из равенства $k + n = m + n$ следует $k = m$, докажем, что из равенства $k+n'=m+n'$ следует $k = m$. По аксиоме сложения *b*), из равенства $k+n'=m+n'$ получаем $(k+n)'=(m+n)'$, откуда по аксиоме P_3 $k+n=m+n$ и по индуктивному предположению $k = m$. $\square$

Имея перед собой систему $\langle N, + \rangle$ в качестве образца, дадим общее определение системы с одной бинарной операцией, обладающей свойствами, которыми обладает сложение натуральных чисел.

2.2.6. Определение. Система $\langle A, * \rangle$ с основным множеством A и бинарной операцией $*$ называется *полугруппой*, если операция $*$ ассоциативна. Если она к тому же и коммутативна, то полугруппа называется *коммутативной*. Наконец, полугруппа $\langle A, * \rangle$ называется *полугруппой с сокращением*, если операция $*$ обладает *свойством сократимости*: если $a*c=b*c$ или $c*a=c*b$, то $a = b$, каковы бы ни были $a, b, c \in A$. Если операция в полугруппе обозначается значком $+$, то она называется *сложением*, а сама полугруппа называется *аддитивной*. Если же операция обозначается $\cdot$, то она называется *умножением*, а сама полугруппа — *мультипликативной*.

Из доказанных выше свойств сложения натуральных чисел вытекает, что система $\langle N, + \rangle$ является коммутативной полугруппой с сокращением.

2.2.7. Определение. Пусть дан произвольный натуральный ряд, т. е. система $\langle N, ' \rangle$, удовлетворяющая аксиомам Пеано, и $+$ является операцией сложения натуральных чисел в соответствии с определением 2.2.1. Тогда система $\langle N, + \rangle$ называется *аддитивной полугруппой натуральных чисел*.

§ 3. Умножение. Полукольцо натуральных чисел

Умножение натуральных чисел

Определим аксиоматически умножение натуральных чисел. Структура этого определения такая же, как и для сложения. Первая аксиома умножения покажет, как произвольное натуральное число умножить на единицу, а вторая аксиома объяснит, как найти произведение $m \cdot n'$, если известно произведение $m \cdot n$.

2.3.1. Определение. *Умножением натуральных чисел* называется бинарная операция $\cdot$, определенная на множестве N, которая удовлетворяет следующим условиям (или аксиомам):

c) $m \cdot 1 = m$ для любого $m \in N$;

d) $m \cdot n' = m \cdot n + m$ для любых $m, n \in N$.

В школе произведение $m \cdot n$ трактуется как сумма n слагаемых, каждое из которых равно m:

$$m \cdot n = \underbrace{m + m + \ldots + m}_{n}.$$

Рассматривая наше определение умножения с этой точки зрения, можно сказать, что оно одновременно разъясняет, что следует понимать под суммой n слагаемых. По первой аксиоме произведение $m \cdot 1$ (сумма одного слагаемого) — это m. По второй аксиоме произведение $m \cdot n'$ равно произведению $m \cdot n$, сложенному с m (т. е. сумма n' слагаемых равна сумме n слагаемых, сложенной с m).

2.3.2. Теорема. *Умножение натуральных чисел существует и единственно.*

Доказательство. Сначала установим, что умножений натуральных чисел существует не более чем одно. Предположим, что существует умножение $\circ$, удовлетворяющее аналогичным условиям:

c_1) $m \circ 1 = m$ для любого $m \in N$;

d_1) $m \circ n' = m \circ n + m$ для любых $m, n \in N$.

Индукцией по n легко доказать, что $m \cdot n = m \circ n$ для любого n при фиксированном m. Следовательно, умножения $\cdot$ и $\circ$ совпадают.

Теперь докажем существование умножения. Индукцией по m докажем, что для любых натуральных чисел m и n существует и притом только одно натуральное число, обозначаемое $m \cdot n$, такое, что выполняются условия c) и d). Для $m = 1$ и произвольного натурального числа n определим $1 \cdot n = n$. Тогда $1 \cdot 1 = 1$, т. е. условие c) выполняется. Далее, пользуясь данным определением и аксиомой сложения a), получаем:

$$1 \cdot n' \overset{\text{опр.}}{=} n' \overset{a)}{=} n + 1 \overset{\text{опр.}}{=} 1 \cdot n + 1,$$

т. е. условие d) также выполняется.

Пусть для натурального числа m и произвольного натурального числа n существует $m \cdot n$ с условиями c) и d). Определим $m' \cdot n = m \cdot n + n$ для любого $n \in N$. Проверим выполнимость условий c) и d). Имеем:

$$m' \cdot 1 \overset{\text{опр.}}{=} m \cdot 1 + 1 \overset{\text{и.п.,}\,c)}{=} m + 1 \overset{a)}{=} m',$$

т. е. условие c) для m' выполняется. Далее,

$$m' \cdot n' \overset{\text{опр.}}{=} m \cdot n' + n' \overset{\text{и.п.,}\,d)}{=} m \cdot n + m + n' \overset{a)}{=} m \cdot n + m + n + 1 =$$
$$= (m \cdot n + n) + (m + 1) \overset{\text{опр.}}{=} m' \cdot n + (m + 1) \overset{a)}{=} m' \cdot n + m',$$

т. е. условие d) для m' также выполняется. □

Пример

Пусть дан натуральный ряд $\langle N, ' \rangle$ с единицей 1. Обозначим $1' = 2$, $2' = 3$, $3' = 4$, $4' = 5$, $5' = 6$. Пользуясь введенными обозначениями и определениями умножения (2.3.1) и сложения (2.2.1) натуральных чисел, находим:

$$3 \cdot 2 = 3 \cdot 1' \overset{d)}{=} 3 \cdot 1 + 3 \overset{c)}{=} 3 + 3 =$$
$$= 3 + 2' = (3 + 2)' = (3 + 1')' = ((3 + 1)')' = ((3')')' = ((4)')' = 5' = 6.$$

Найдите аналогично произведение $2 \cdot 3$.

Иногда говорят: «это просто как дважды два — четыре». Теперь читатель знает, как доказать этот «символ простоты»: дорога к доказательству ведет от аксиом Пеано.

Для большей формализации доказательства теоремы 2.3.2 заметим, что умножение натуральных чисел представляет собой отображение

множества $N \times N$ в N, которое при фиксированном первом сомножителе m определяет отображение $g_m : N \to N$. При этом аксиомы c) и d) превращаются в условия:

c_m) $g_m(1) = m$;

d_m) $g_m(n') = g_m(n) + m$ для любого $n \in N$.

Таким образом, доказательство существования и единственности умножения натуральных чисел сводится к доказательству существования и единственности отображения g_m для любого $m \in N$, удовлетворяющего условиям c_m) и d_m). Вначале доказывается, что любые два таких отображения совпадают, а затем индукцией по m устанавливается существование отображения g_m. Далее, отображение множества $N \times N$ в N, сопоставляющее всякой упорядоченной паре натуральных чисел (m, n) натуральное число $g_m(n)$, обозначаемое через $m \cdot n$, удовлетворяет, как легко проверить, условиям c) и d), т. е. является умножением натуральных чисел.

Основные свойства умножения

Докажем привычные свойства умножения. Введем обычный порядок выполнения операций: сначала умножение, а потом сложение. Эта условность поможет нам экономить на скобках. Договоримся также не писать знак умножения, если это не вызывает недоразумений.

2.3.3. Предложение. *Умножение натуральных чисел дистрибутивно относительно сложения*: $k(m+n) = km + kn$ *и* $(m+n)k = mk + nk$ *для любых* $k, m, n \in N$.

Доказательство. Первое равенство докажем индукцией по $n \neq 1$ при произвольно выбранных k и m. При $n = 1$ имеем:

$$k(m+1) \overset{a)}{=} km' \overset{d)}{=} km + k \overset{c)}{=} km + k \cdot 1.$$

Пусть $k(m+n) = km + kn$. Докажем, что $k(m+n') = km + kn'$. Имеем:

$$k(m+n') \overset{b)}{=} k(m+n)' \overset{d)}{=} k(m+n) + k \overset{\text{и.п.}}{=} (km + kn) + k =$$

$$= km + (kn + k) \overset{d)}{=} km + kn'.$$

Второе равенство дистрибутивности доказывается аналогично индукцией по k. □

2.3.4. Предложение. *Умножение натуральных чисел ассоциативно, т. е.* $(km)n = k(mn)$ *для любых* $k, m, n \in N$.

Доказательство индукцией по n. При $n = 1$ получаем:

$$(km)1 \overset{c)}{=} km \overset{c)}{=} k(m1).$$

Пусть $(km)n = k(mn)$, докажем, что $(km)n' = k(mn')$. Имеем:

$$(km)n' \overset{d)}{=} (km)n + km \overset{\text{и.п.}}{=} k(mn) + km \overset{2.2.3}{=} k(mn + m) \overset{d)}{=} k(mn'). \square$$

2.3.5. Предложение. *Умножение натуральных чисел коммутативно: $mn = nm$ для любых $m, n \in N$.*

Доказательство (по образцу доказательства 2.2.4) предоставляется читателю.

В дальнейшем мы докажем, что умножение натуральных чисел (как и сложение) обладает свойством сократимости.

Итак, сложение и умножение натуральных чисел ассоциативны, коммутативны и связаны дистрибутивным законом. Введем название для алгебраической системы, обладающей такими же свойствами.

2.3.6. Определение. *Полукольцом* называется система $\langle A, +, \cdot \rangle$, удовлетворяющая следующим условиям:

1) сложение + ассоциативно и коммутативно, т. е. система $\langle A, + \rangle$ является коммутативной полугруппой, она называется *аддитивной полугруппой полукольца*;

2) умножение $\cdot$ ассоциативно, т. е. система $\langle A, \cdot \rangle$ является полугруппой, она называется *мультипликативной полугруппой полукольца*;

3) умножение дистрибутивно относительно сложения: $(a + b)c = ac + bc$, $c(a+b) = ca + cb$ для любых $a, b, c \in A$.

Если умножение коммутативно, то полукольцо называется коммутативным.

Из доказанных выше свойств сложения и умножения натуральных чисел вытекает, что система $\langle N, +, \cdot \rangle$ является коммутативным полукольцом. Закрепим этот факт в виде определения, подчеркивающего генеалогию этого понятия.

2.3.7. Определение. Пусть дан натуральный ряд $\langle N, ' \rangle$ и в соответствии с определениями 2.2.1 и 2.3.1 на N определены операции сложения + и умножения $\cdot$. Тогда система $\langle N, +, \cdot \rangle$ называется *полукольцом натуральных чисел.*

§ 4. Отношение «меньше». Линейно упорядоченное множество натуральных чисел

Вспомогательные утверждения

Докажем ряд вспомогательных утверждений, которые, в частности, помогут нам определить отношение «меньше» для натуральных чисел и доказать его свойства.

2.4.1. Предложение. *Всякое натуральное число $n \neq 1$ непосредственно следует за некоторым натуральным числом.*

Доказательство. Обозначим через M множество, содержащее 1, и всякое натуральное число, которое непосредственно следует за некоторым натуральным числом. Тогда $1 \in M$, и если $n \in M$, то $n' \in M$. По аксиоме индукции, $M = N$. Таким образом, всякое натуральное число либо совпадает с единицей, либо непосредственно следует за некоторым натуральным числом. □

2.4.2. Предложение. *Для любых* $m, n \in N$ *если* $m \neq n$, *то* $m' \neq n'$.

Доказательство. Если предположить, что $m' = n'$, то по аксиоме P_3 получаем $m = n$, что противоречит условию. □

2.4.3. Предложение. *Для любых* $m, n \in N$ *выполняется неравенство* $m + n \neq n$.

Доказательство проведем индукцией по n при произвольно зафиксированном m. При $n = 1$ имеем: $m + 1 = m' \neq 1$ по аксиоме P_1. Пусть $m + n \neq n$, тогда по 2.4.2 $(m + n)' \neq n'$, откуда по аксиоме сложения b) получаем $m + n' \neq n'$. □

2.4.4. Следствие. *Для любого* $n \in N$ $n' \neq n$.

К следующему утверждению мы неоднократно будем обращаться в дальнейшем. Оно, в частности, лежит в основе определения отношения «меньше» для натуральных чисел.

2.4.5. Теорема. Для любых натуральных чисел a и b имеет место одно и только одно из соотношений:

1) существует $k \in N$ такое, что $b = a + k$;
2) $a = b$;
3) существует $m \in N$ такое, что $a = b = m$.

Доказательство. Существование по крайней мере одного из соотношений докажем индукцией по b при произвольно зафиксированном a. Пусть $b = 1$. Если $a = 1$, то имеет место соотношение 2). Если $a \neq 1$, то по 2.4.1 существует $m \in N$ такое, что $a = m'$. Отсюда $a = m + 1 = 1 + m$, т. е. для a и $b = 1$ имеем соотношение 3).

Предположим, что для a и b имеет место одно из соотношений 1)—3) и докажем, что для a и b' имеет место одно из соотношений указанного типа.

Если $b = a + k$, то по аксиоме Пеано P_2 и аксиоме сложения b) получаем: $b' = (a + k)' = a + k'$, т. е. для a и b' имеет место соотношение типа 1).

Если $a = b$, то $b' = a' = a + 1$, т. е. для a и b' получаем соотношение типа 1).

Наконец, если $a = b = m$, то при $m = 1$ получаем $a = b + 1 = b'$ — соотношение типа 2), а при $m \neq 1$ по 2.4.1 существует натуральное число k такое, что $m = k'$, и мы получаем: $a = b + m = b + k' = b + k + 1 = (b + 1) + k = b' + k$ — соотношение типа 3) для a и b'.

Докажем, что не могут выполняться сразу два из соотношений 1)—3). Предположим, например, что одновременно имеют место соотношения 1) и 3). Тогда $b = a + k = (b + m) + k = b + (m + k)$, что противоречит 2.4.3. Аналогично рассматриваются остальные случаи. □

Отношение «меньше» для натуральных чисел

Введем отношение «меньше» для натуральных чисел, используя сложение.

2.4.6. Определение. Будем говорить, что натуральное число a меньше натурального числа b и писать $a < b$, если существует натуральное число k такое, что $b = a + k$.

В нашем представлении натуральные числа можно «выстроить в линейку», используя отношение $<$. При этом мы пользуемся тем, что про любые два натуральных числа a и b можно однозначно сказать: либо $a < b$, либо $a = b$, либо $b < a$. Это свойство называется свойством трихотомии, что в переводе означает «одно из трех». Важным свойством отношения «меньше» является также возможность сравнить числа a и c «транзитом» через «посредника» b: если $a < b$ и $b < c$, то $a < c$. Это так называемое свойство транзитивности. Уточним эти наши интуитивные представления в виде строгих определений.

2.4.7. Определение. Система $\langle A, < \rangle$ с основным множеством A и бинарным отношением $<$ (меньше) называется *линейно упорядоченным множеством*, если выполнены следующие два условия:

1) (*свойство трихотомии*). Для любых $a, b \in A$ имеет место одно и только одно из соотношений: $a < b$, $a = b$, $b < a$;

2) (*свойство транзитивности*). Для любых $a, b, c \in A$, если $a < b$, $b < c$, то $a < c$.

При этом отношение $<$ называется *отношением линейного порядка*.

2.4.8. Теорема. *Система $\langle N, < \rangle$ является линейно упорядоченным множеством.*

Доказательство. Свойство трихотомии отношения $<$ вытекает из 2.4.5. Докажем свойство транзитивности. Пусть для a, b, $c \in N$ имеют место соотношения $a < b$ и $b < c$. По 2.4.6, это означает, что $b = a + k$ и $c = b + m$ при некоторых $k, m \in N$. Отсюда $c = (a + k) + m = a + (k + m)$, что означает $a < c$. □

Введем отношения $>$, $\leq$, $\geq$ в наиболее общей ситуации.

2.4.9. Определение. Пусть дано линейно упорядоченное множество $\langle A, < \rangle$. Для любых $a, b \in A$ положим:

1) $a > b$ (a больше b) тогда и только тогда, когда $b < a$;

2) $a \leq b$ (a меньше или равно b) тогда и только тогда, когда $a < b$ или $a = b$;

3) $a \geq b$ (a больше или равно b) тогда и только тогда, когда $a > b$ или $a = b$.

2.4.10. Предложение. *Отношение $\leq$ обладает следующими свойствами*:

1) рефлексивности: $a \leq a$ для любого $a \in A$;

2) антисимметричности: для любых $a, b \in A$ если $a \leq b$ и $b \leq a$, то $a = b$;

3) транзитивности: для любых $a, b \in A$ если $a \leq b$ и $b \leq c$, то $a \leq c$;

4) линейности: для любых $a, b \in A$ $a \leq b$ или $b \leq a$.

Доказательство. Рефлексивность следует из того, что $a = a$. Докажем антисимметричность. Предположим, что $a \leq b$ и $b \leq a$, но $a \neq b$. Тогда получаем $a < b$ и $b < a$, что противоречит свойству трихотомии. Транзитивность отношения $\leq$ следует из транзитивности отношений $<$ и $=$. Свойство линейности вытекает из свойства трихотомии. □

Заметим, что иногда линейно упорядоченное множество определяют как систему $\langle A, \leq \rangle$, где бинарное отношение $\leq$ рефлексивно, антисим-

метрично, транзитивно и линейно. Тогда говорят, что $a < b$ (a строго меньше b), если $a \leq b$ и $a \neq b$. Легко доказать, что так определенное отношение строгого порядка $<$ обладает свойствами трихотомии и транзитивности.

Основные свойства линейно упорядоченного множества натуральных чисел

Дадим одно общее определение.

2.4.11. Определение. Пусть дано линейно упорядоченное множество $\langle A, < \rangle$ и $M \subseteq A$. Элемент $m \in M$ ($n \in M$) называется *наименьшим* (соответственно, *наибольшим*) в M, если $m \leq x$ (соответственно, $x \leq n$) для любого $x \in M$.

2.4.12. Предложение. *Единица* 1 — *наименьший элемент в* N.

Доказательство. Установим, что $1 \leq n$ для любого $n \in N$. Если $n = 1$, то утверждение очевидно. Если же $n \neq 1$, то по 2.4.1 существует натуральное число m такое, что $n = m' = m + 1$, откуда $1 < n$, а значит, $1 \leq n$. □

2.4.13. Предложение (свойство *дискретности*). *Для любого* $a \in N$ *не существует* $x \in N$ *такого, что* $a < x < a + 1$, *т. е. между* a *и* $a + 1 = a'$ *нет натурального числа.*

Доказательство. Предположим противное, пусть для некоторого $a \in N$ существует $x \in N$ такой, что $a < x < a + 1$. Из $a < x$ получаем $x = a + k$ для некоторого $k \in N$. Если $k = 1$, то $x = a + 1$, что противоречит предположению. Если же $k \neq 1$, то, по 2.4.1, существует $m \in N$ такое, что $k = m' = m + 1$, откуда $x = a + m + 1$, т. е. $a + 1 < x$, что снова противоречит предположению. □

2.4.14. Следствие. *Для любых* $a, b \in N$ *если* $a < b'$, *то* $a \leq b$, *и если* $a < b$, *то* $a' \leq b$.

Доказательство. Предположение противного ведет к противоречию с 2.4.13. □

2.4.15. Определение. Пусть дано линейно упорядоченное множество $\langle A, < \rangle$. Непустое подмножество $M \subseteq A$ называется *ограниченным сверху* (*снизу*), если существует элемент $b \in A$ ($c \in A$) такой, что для любого $x \in M$ $x \leq b$ ($c \leq x$). При этом b называется *верхней границей* (а c — *нижней границей*) подмножества M.

2.4.16. Теорема. *В линейно упорядоченном множестве натуральных чисел всякое непустое ограниченное сверху подмножество имеет наибольший элемент.*

Доказательство. Индукцией по b докажем, что если натуральное число b есть верхняя граница некоторого непустого подмножества натуральных чисел, то это подмножество имеет наибольший элемент. При $b = 1$ утверждение тривиально. Пусть утверждение верно для натурального числа b и b' — верхняя граница непустого подмножества $M \subseteq N$. Если $b' \in M$, то b' и является наибольшим элементом в M. Если же $b' \notin M$, то для любого $x \in M$ имеем $x < b'$, откуда по 2.4.14 $x \leq b$. Следовательно, b есть верхняя граница подмножества M, и по индуктивному предположению в M есть наибольший элемент. □

Теорема 2.4.16 в 3.3.19 будет распространена на целые числа, при этом мы установим одновременно и симметричное утверждение относительно существования наименьшего элемента для всякого непустого ограниченного снизу подмножества целых чисел. Докажем, что для натуральных чисел симметричное утверждение также верно, причем в этом случае условие ограниченности снизу выполняется автоматически, так как одной из нижних границ любого подмножества натуральных чисел будет 1. Предварительно введем соответствующее понятие.

2.4.17. Определение. Линейно упорядоченное множество называется *вполне упорядоченным*, если всякое его непустое подмножество имеет наименьший элемент.

2.4.18. Теорема. *Линейно упорядоченное множество натуральных чисел вполне упорядочено.*

Доказательство. Пусть $\varnothing \neq A \subseteq N$. Обозначим через M множество всех натуральных чисел, не превосходящих всякого $a \in A$: $M = \{x \in N \mid x \leq a$ для любого $a \in A\}$ (рис. 9).

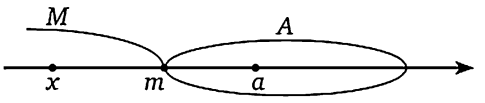

Рис. 9

Поскольку $1 \in M$, следовательно, M — непустое подмножество, ограниченное сверху всяким элементом из A. Согласно 2.4.16 в M есть наибольший элемент, который обозначим через m. Тогда $m \leq a$ для любого $a \in A$, и нам остается лишь установить, что $m \in A$. Предположим, что это не так. Тогда для любого $a \in A$ имеем $m < a$ и по 2.4.14 $m' \leq a$, откуда $m' \in M$. Но $m < m+1 = m'$ — пришли в противоречие с предположением о том, что m — наибольший элемент в M. Остается принять, что $m \in A$ и является там наименьшим элементом. □

§ 5. Различные виды доказательств по индукции

Усиленный принцип полной математической индукции

Докажем принцип полной математической индукции, в котором делается более сильное индуктивное предположение.

2.5.1. Теорема (усиленный принцип полной математической индукции). *Предложение $T(n)$, зависящее от натуральной переменной n, верно для любого натурального числа, если выполнены следующие условия*:

1) $T(n)$ верно для $n = 1$, т. е. $T(1)$ истинно;

2) каково бы ни было натуральное число m, из предположения о том, что $T(n)$ истинно для всех $n < m$, следует, что оно верно и для m, т. е. $T(m)$ истинно.

Доказательство от противного. Предположим, что $T(n)$ верно не для всякого натурального числа. Тогда множество A всех натуральных чисел, для которых $T(n)$ не верно, не пусто и по 2.4.18 имеет наименьший элемент, который обозначим через m. По условию 1), $m \neq 1$, следовательно, существуют натуральные числа, меньшие m. Так как m — наименьший элемент в A, то все натуральные числа, меньшие m, уже A не принадлежат, а значит, для них утверждение $T(n)$ верно. Но тогда, по условию 2), оно должно быть верно и для m — пришли к противоречию. Остается принять, что $A = \varnothing$. Но это означает, что $T(n)$ верно для любого натурального числа. □

Обобщенный принцип полной математической индукции

Иногда истинность утверждения $T(n)$ нужно доказать для всех натуральных чисел, начиная с некоторого натурального числа a. Тогда используется следующая теорема.

2.5.2. Теорема (обобщенный принцип полной математической индукции). *Пусть $a \in N$. Предложение $T(n)$ верно для любого натурального числа $n \geq a$, если выполнены следующие условия*:

1) *предложение $T(n)$ верно для $n = a$, т. е. $T(a)$ истинно*;

2) *каково бы ни было натуральное число $n \geq a$, из предположения о том, что $T(n)$ истинно, следует, что $T(n')$ истинно.*

Доказательство. Обозначим через M множество, содержащее все натуральные числа, меньшие a, и все n, для которых $T(n)$ истинно. Пользуясь принципом полной математической индукции, докажем, что $n \in M$ для любого $n \in N$. По условию 1), $a \in M$, а так как $1 \leq a$, то $1 \in M$. Пусть $n \in M$, тогда либо $n < a$, либо $T(n)$ истинно. В первом случае $n' \leq a$, откуда $n' \in M$, а во втором — по условию 2), $n' \in M$. Таким образом, $M = N$. Отсюда следует истинность $T(n)$ для любого $n \geq a$. □

Обобщенный усиленный принцип полной математической индукции

Докажем принцип полной математической индукции, который соединяет в себе черты усиленного и обобщенного принципов.

2.5.3. Теорема. *Пусть $a \in N$. Предложение $T(n)$ верно для любого натурального числа $n \geq a$, если выполнены следующие условия*:

1) *предложение $T(n)$ верно для $n = a$, т. е. $T(a)$ истинно*;

2) *каково бы ни было натуральное число $m \geq a$, из предположения о том, что $T(n)$ истинно для всех натуральных n таких, что $a \leq n < m$, следует истинность $T(m)$.*

Доказательство. Обозначим через M множество, содержащее все натуральные числа, меньшие a, и все n, для которых $T(n)$ истинно. Пользуясь усиленным принципом полной математической индукции, нетрудно доказать, что всякое натуральное число принадлежит M. Это и доказывает теорему. □

§ 6. Упорядоченное полукольцо натуральных чисел

Связь между операциями +, · и отношением <

2.6.1. Предложение. *Сложение и умножение натуральных чисел монотонны, т. е. для любых* $a, b, c \in N$ *если* $a < b$, *то* $a+c<b+c$ *и* $a \cdot c < b \cdot c$.

Доказательство. Из условия $a < b$ следует, что $b = a + k$ при некотором $k \in N$. Тогда $b+c=a+k+c$ и $bc=(a+k)c=ac+kc$, откуда $a+c<b+c$ и $a \cdot c < b \cdot c$. □

Рассматривая систему $\langle N, +, \cdot, < \rangle$, приходим к следующему общему понятию.

2.6.2. Определение. Система $\langle K, +, \cdot, < \rangle$ с основным множеством K, бинарными операциями сложения + и умножения · и бинарным отношением < называется *упорядоченным полукольцом*, если выполнены следующие условия:

1) $\langle K, +, \cdot \rangle$ — полукольцо, содержащее более одного элемента;

2) $\langle K, < \rangle$ — линейно упорядоченное множество.

Операции сложения и умножения монотонны: для любых $a, b, c \in K$, если $a < b$, то $a+c<b+c$ (*монотонность сложения*), и если $a<b$, $c<c+c$, то $a \cdot c < b \cdot c$ и $c \cdot a < c \cdot b$ (*монотонность умножения*).

2.6.3. Определение. Система $\langle N, +, \cdot, < \rangle$ называется *упорядоченным полукольцом натуральных чисел.*

2.6.4. Определение. Пусть дано полукольцо $\langle K, +, \cdot \rangle$. Элемент $0 \in K$ называется *нулем* (а элемент $e \in K$ называется *единицей*), если для любого $a \in K$ $a+0=0+a=a$ (соответственно, $a \cdot e = e \cdot a = a$).

Очевидно, (упорядоченное) полукольцо натуральных чисел не содержит нуля, но содержит единицу.

Заметим также, что если упорядоченное полукольцо содержит нуль 0, то условие $c<c+c$ эквивалентно условию $c > 0$.

Основные свойства упорядоченного полукольца натуральных чисел

2.6.5. Предложение. *В упорядоченном полукольце натуральных чисел неравенства одинакового смысла можно почленно складывать и перемножать.*

Доказательство. Докажем, что если $a<b$, $c<d$, то $a+c<b+d$. Из условия $a < b$ следует $a+c<b+c$, а из $c < d$ получаем $b+c<b+d$. Отсюда, пользуясь транзитивностью отношения <, заключаем, что $a+c<b+d$. Возможность умножения неравенств доказывается аналогично. □

2.6.6. Предложение. *Сложение и умножение натуральных чисел обладают свойствами сократимости, т. е. для любых* $a, b, c \in N$ *если* $a+c=b+c$ *или* $a \cdot c = b \cdot c$, *то* $a = b$.

Доказательство. Если предположить, что $a \neq b$, то по свойству трихотомии либо $a < b$, либо $b < a$. Но если, например, $a < b$, то по свойству монотонности сложения и умножения получаем $a+c<b+c$ и $a \cdot c < b \cdot c$, что противоречит условию. □

2.6.7. Предложение. *В упорядоченном полукольце натуральных чисел выполняется аксиома Архимеда: для любых $a, b \in N$ существует натуральное число n такое, что $na > nb$.*

Доказательство. Так как $1 \le a$ и $b < b+1$, то по 2.6.5 $b < (b+1)\cdot a$, откуда при $n = n+1$ получаем $na > nb$. □

Несложно доказывается следующая общая теорема.

2.6.8. Теорема. *Пусть дано упорядоченное полукольцо $\langle K, +, \cdot, < \rangle$ и $a, b, c, d \in K$.*

1) *Если $a < b$, $c < d$, то $a + c < b + d$, и если $a \le b$, $c \le d$, то $a + c \le b + d$.*

2) *Если 0 — нуль в K и $0 < a < b$, $0 < c < d$, то $a \cdot c < b \cdot d$, и если $0 \le a \le b$, $0 \le c \le d$, то $a \cdot c \le b \cdot d$.*

§ 7. Индуктивные определения

Обоснование индуктивных определений

Индуктивное задание последовательности (x_n) заключается в том, что задают один или несколько первых членов последовательности и правило образования следующего члена последовательности через предыдущие, которое называется *рекуррентным соотношением*. Например, зададим последовательность (x_n), положив:

a) $x_1 = 5$;

b) $x_{n+1} = 2x_n - 7$.

Наша уверенность в том, что условия *a)* и *b)* действительно определяют последовательность, основана на том, что мы можем найти одно за другим любое число ее членов: $x_1 = 5$, $x_2 = 2x_1 - 7 = 2 \cdot 5 - 7 = 3$, $x_3 = 2x_2 - 7 = 2 \cdot 3 - 7 = -1$, и т. д. Однако это «и т. д.» нельзя считать доказательством того, что существует и притом только одна последовательность (x_n), удовлетворяющая условиям *a)* и *b)*. Докажем, что условия *a)* и *b)* действительно однозначно определяют последовательность.

Чтобы понять, что именно нужно доказывать, проанализируем наш пример. Начнем с того, что последовательность будем рассматривать как отображение $f : N \to Z$. Далее, если рассмотреть отображение $g : Z \to Z$, при котором $g(x) = 2x - 7$ для любого $x \in Z$, то правило образования $f(n+1) = x_{n+1}$ по $f(n) = x_n$ можно записать в виде $f(n+1) = g(f(n))$. Кроме того, введем одно необходимое понятие.

2.7.1. Определение. *Начальным отрезком натурального ряда* назовем всякое подмножество $\overline{1, n} = \{x \in N \mid 1 \le x \le n\}$. При этом будем говорить кратко: отрезок $\overline{1, n}$.

Теперь у нас все готово, чтобы сформулировать и доказать нужную теорему.

2.7.2. Теорема (об индуктивных определениях). *Пусть A — непустое множество, $a \in A$ и g — отображение A в A. Существует и притом только одно отображение $f : N \to A$ такое, что:*

a) $f(1) = a$;

b) $f(n+1) = g(f(n))$ для любого $n \in N$.

Доказательство. Естественно напрашивается следующее построение искомого отображения f множества N в множество A.

1-й шаг. Положим $f(1) = a$.

2-й шаг. Найдем $g(f(1))$ и положим $f(2) = g(f(1))$, $(f(2) = g(a))$.

3-й шаг. Найдем $g(f(2))$ и положим $f(3) = g(f(2))$.

.....

n'-й шаг. Найдем $g(f(n))$ и положим $f(n') = g(f(n))$.

.....

Другими словами, мы строим последовательно отображения отрезков $\overline{1,1}$, $\overline{1,2}$, $\overline{1,3}$, ... во множество A так, чтобы отображение каждого следующего отрезка являлось продолжением отображения предыдущего отрезка, причем на первом шаге обеспечиваем выполнение условия a), а на каждом последующем шаге обеспечиваем выполнение условия b).

Реализуем эту идею в более строгом изложении. Индукцией по m докажем, что для любого натурального числа m существует и единственное отображение f_m отрезка $\overline{1,m}$ во множество A такое, что:

a_m) $f_m(1) = a$;

b_m) если $m > 1$, то $f_m(n') = g(f_m(n))$ для любого n, удовлетворяющего неравенствам $1 \le n < m$.

Для $m = 1$ отрезок $\overline{1,1} = \{1\}$, поэтому требование b_1) отпадает, и, очевидно, единственным отображением отрезка $\overline{1,1}$ в A, удовлетворяющим условию a_1), является $f_1(1) = a$.

Пусть существует единственное отображение f_m отрезка $\overline{1,m}$ во множество A, удовлетворяющее условиям a_m) и b_m). Докажем существование и притом только одно отображения f'_m отрезка $\overline{1,m'}$ в A, удовлетворяющего условиям a'_m) и b'_m). Определим

$$f_{m'}(n) = \begin{cases} f_m(n), & \text{если } n \in \overline{1,m}, \\ g(f_m(m)), & \text{если } n = m'. \end{cases}$$

Очевидно, f'_m является отображением отрезка $\overline{1,m'}$ в A, продолжающим отображение f_m. Докажем, что оно удовлетворяет условиям a'_m) и b'_m). Так как $1 \in \overline{1,m}$, то $f_{m'}(1) = f_m(1) = a$, т. е. f'_m удовлетворяет условию a'_m).

Пусть натуральное число n удовлетворяет неравенствам $1 \le n < m'$. Тогда либо $1 < n' \le m$, либо $n' = m'$. В первом случае мы можем перейти к отображению f_m : $f_{m'}(n') = f_m(n') = g(f_m(n)) = g(f_{m'}(n))$. Во втором случае, используя определение отображения f'_m, получаем $f_{m'}(m') = g(f_m(m)) = g(f_{m'}(m))$. Таким образом, отображение f'_m удовлетворяет условию b'_m.

Докажем единственность отображения f'_m. Пусть существует отображение $h_{m'} : \overline{1,m'} \to A$, удовлетворяющее условиям:

c'_m) $h_{m'}(1) = a$;

d'_m) $h_{m'}(n') = g(h_{m'}(n))$ для любого n, удовлетворяющего неравенствам $1 \le n < m'$.

Отображения f'_m и h'_m на отрезке $\overline{1,m}$ удовлетворяют условиям a_m) и b_m) и по индуктивному предположению совпадают. В то же время, $f_{m'}(m') = g(f_m(m)) = g(h_m(m)) = h_{m'}(m')$. Следовательно, отображения f'_m и h'_m совпадают на отрезке $\overline{1,m'}$.

Итак, для любого $m \in N$ доказано существование и единственность отображения f_m отрезка $\overline{1,m}$ в A, удовлетворяющего условиям a_m) и b_m). Определим отображение $f : N \to A$, положив $f(m) = f_m(m)$ для любого $m \in N$. Легко видеть, что отображение f удовлетворяет условиям a) и b) и является единственным отображением с этими условиями. □

Иногда приходится прибегать к индуктивным определениям более общего характера. Например, при задании последовательности ее $(n+1)$-й член может зависеть не только от $f(n)$, но и от n, т. е. рекуррентное соотношение имеет вид $f(n') = g(f(n), n)$; или может $f(n')$ зависеть от всех предыдущих членов последовательности и от n, т. е. $f(n') = g(f(1), f(2), \ldots, f(n), n)$. Соответствующие теоремы об обосновании таких индуктивных определений доказываются аналогично.

В качестве приложения этой теоремы наметим еще одно доказательство существования и единственности умножения натуральных чисел. Эта операция представляет собой отображение, ставящее в соответствие всякой упорядоченной паре натуральных чисел (m, n) натуральное число $m \cdot n$, причем выполняются два условия — аксиомы умножения. При фиксированном m оно превращается в отображение $f_m : N \to N$, удовлетворяющее условиям: c_m) $f_m(1) = m$ и d_m) $f_m(n') = f_m(n) + m$ для любого $n \in N$. По теореме 2.7.2 для любого m отображение f_m существует и единственно, что доказывает существование и единственность умножения натуральных чисел.

Подобным образом можно было бы доказать существование и единственность сложения натуральных чисел. Но в нашем доказательстве теоремы 2.7.2 используется отношение $<$, которое, в свою очередь, определено с помощью сложения натуральных чисел. Получился бы порочный круг. Вместе с тем теорему 2.7.2 можно доказать без использования сложения натуральных чисел, и тогда ее можно применить для доказательства существования и единственности этой операции.

Сумма и произведение нескольких элементов

Приведем индуктивное определение суммы n слагаемых в наиболее общей форме.

2.7.3. Определение. Пусть дана аддитивная полугруппа $\langle A, + \rangle$ и $a_1, a_2, \ldots, a_n \in A$. Положим по определению:

1) $\sum_{i=1}^{1} a_i = a_1$;

2) $\sum_{i=1}^{n+1} a_i = \left(\sum_{i=1}^{n} a_i \right) + a_{n+1}$.

При этом $\sum_{i=1}^{n} a_i$ называется *суммой n слагаемых* и записывается также в виде $a_1 + a_2 + \ldots + a_n$. Если здесь все слагаемые равны a, то мы получаем определение *натурального кратного* (точнее, n-кратного) элемента a, которое обозначается через na.

Заметим, что если полукольцо $\langle K, +, \cdot \rangle$ содержит полукольцо натуральных чисел $\langle N, +, \cdot \rangle$, то для любых $a \in K$, $n \in N$, имеем $na = n \cdot a$.

Переведя определение 2.7.3 на мультипликативный язык, получаем определение *произведения n сомножителей* $\prod_{i=1}^{n} a_i$ (или $a_1 \cdot a_2 \cdot \ldots \cdot a_n$) и *степени с натуральным показателем* a^n.

Отметим основные свойства натуральных кратных и степеней с натуральными показателями (они легко доказываются индукцией по n).

2.7.4. Предложение. *Для любых элементов a и b полукольца $\langle K, +, \cdot \rangle$ и любых $m, n \in N$, имеют место соотношения*:

1) $(m+n)a = ma + na$, $a^{m+n} = a^m \cdot a^n$;
2) $(mn)a = m(na)$, $a^{mn} = (a^m)^n$;
3) $ma \cdot nb = (mn)(a \cdot b)$;
4) если $ab = ba$, то $a^n \cdot b^n = (a \cdot b)^n$.

Если a и b — элементы упорядоченного полукольца $\langle K, +, \cdot, < \rangle$ с нулем 0, то для любого $n \in N$:

1) *если $a < b$, то $na < nb$;*
2) *если $0 < a < b$, то $a^n < b^n$.*

В следующих темах определения натурального кратного и степени с натуральным показателем будут дополнены и введены понятия целого кратного и степени с целым, а затем — с рациональным и действительным показателями.

§ 8. Изоморфизм одноименных систем натуральных чисел

Чем могут отличаться одноименные системы натуральных чисел?

Исходя из определения натурального ряда $\langle N, ' \rangle$, мы определили последовательно аддитивную полугруппу натуральных чисел $\langle N, + \rangle$, полукольцо натуральных чисел $\langle N, +, \cdot \rangle$, линейно упорядоченное множество $\langle N, < \rangle$ и упорядоченное полукольцо $\langle N, +, \cdot, < \rangle$ натуральных чисел. Возьмем другой натуральный ряд $\langle N_1, '' \rangle$ и, исходя из него, определим аналогичные системы $\langle N_1, \oplus \rangle$, $\langle N_1, \oplus, \otimes \rangle$, $\langle N_1, \lhd \rangle$, $\langle N_1, \oplus, \otimes, \lhd \rangle$. Чем могут отличаться системы с основным множеством N от соответствующих систем с основным множеством N_1? Оказывается, весьма несущественным: лишь обозначениями элементов, отношений и операций. Существует взаимно однозначное отображение («наложение») φ множества N на множество N_1, при котором сохраняются: отношение непосредственного следования, операции сложения и умножения, а также отношение «меньше», т. е. для любых $m, n \in N$, $n = m'$ тогда и только тогда,

когда $\varphi(n) = (\varphi(m))''$; $\varphi(m+n) = \varphi(m) \oplus \varphi(n)$, $\varphi(m \cdot n) = \varphi(m) \otimes \varphi(n)$; и $m < n$ тогда и только тогда, когда $\varphi(m) \lhd \varphi(n)$. Другими словами, одноименные системы изоморфны. Докажем это.

2.8.1. Теорема. *Изоморфны любые два натуральных ряда, любые две аддитивные полугруппы натуральных чисел, любые два полукольца натуральных чисел, любые два линейно упорядоченных множества и любые два упорядоченных полукольца натуральных чисел.*

Доказательство. Пусть даны два натуральных ряда $\langle N, ' \rangle$ и $\langle N, '' \rangle$ с единицами 1 и e соответственно. По 2.7.2, существует отображение $\varphi : N \to N_1$, заданное индуктивно следующим образом:

a) $\varphi(1) = e$;

b) $\varphi(n') = (\varphi(n))''$ для любого $n \in N$.

Докажем сначала, что отображение φ сохраняет операции сложения и умножения, а также отношение «меньше».

Индукцией по n докажем, что для любых $m, n \in N$, имеет место равенство $\varphi(m+n) = \varphi(m) \oplus \varphi(n)$.

1. При $n = 1$, пользуясь последовательно первой аксиомой сложения $+$, свойством *b*) отображения φ, первой аксиомой сложения $\oplus$ и свойством *a*), получаем:

$$\varphi(m+1) = \varphi(m') = (\varphi(m))'' = \varphi(m) \oplus e = \varphi(m) \oplus \varphi(1).$$

2. Пусть $\varphi(m+n) = \varphi(m) \oplus \varphi(n)$, докажем, что $\varphi(m+n') = \varphi(m) \oplus \varphi(n')$. Пользуясь последовательно второй аксиомой сложения $+$, свойством *b*) отображения φ, индуктивным предположением, второй аксиомой сложения $\oplus$ и снова свойством *b*), получаем:

$$\varphi(m+n') = \varphi((m+n)') = (\varphi(m+n))'' = (\varphi(m) \oplus \varphi(n))'' = \varphi(m) \oplus (\varphi(n))'' = \\ = \varphi(m) \oplus \varphi(n').$$

Таким образом, φ сохраняет операцию сложения. Аналогично доказывается, что φ сохраняет операцию умножения.

Вспомним, что для натуральных чисел a и b имеет место неравенство $a < b$ тогда и только тогда, когда существует натуральное число k такое, что $b = a + k$. Поскольку φ сохраняет сложение, то отношение «меньше» при φ также сохраняется.

Теперь докажем, что φ является взаимно однозначным отображением N в N_1. Пусть $\varphi(m) = \varphi(n)$, докажем, что $m = n$. Предположим, что $m \neq n$, тогда по свойству трихотомии либо $m < n$, либо $n < m$. Не нарушая общности, предположим, что $m < n$. Но тогда получаем $\varphi(m) \lhd \varphi(n)$, что противоречит предположению. Наконец, докажем, что φ — отображение на N_1. Для этого докажем, что всякий элемент $n_1 \in N_1$ имеет прообраз в N. Если $n_1 = e$, то по *a*) прообразом n_1 будет $1 \in N$. Если же $n_1 \neq e$, то существует $k_1 \in N_1$ такое, что $n_1 = k_1''$. По индуктивному предположению существует $k \in N$ такое, что $\varphi(k) = k_1$. Но тогда по условию *b*) для φ получаем $\varphi(k') = (\varphi(k))'' = k_1'' = n_1$.

Итак, φ — взаимно однозначное отображение N на N_1. Отсюда следует, что равенство $n = m'$ имеет место тогда и только тогда, когда $\varphi(n) = \varphi(m')$. По условию b) получаем $\varphi(n) = (\varphi(m))''$, т. е. φ сохраняет отношение непосредственного следования. □

2.8.2. Теорема. *Изоморфный образ натурального ряда, аддитивной полугруппы, полукольца, линейно упорядоченного множества и упорядоченного полукольца натуральных чисел есть соответственно натуральный ряд, аддитивная полугруппа, полукольцо, линейно упорядоченное множество и упорядоченное полукольцо натуральных чисел.*

Доказательство. Пусть даны натуральный ряд $\langle N, ' \rangle$ и его изоморфный образ $\langle N, '' \rangle$ при изоморфизме φ. По определению 1.17, это означает, что для любых $m, n \in N$, имеет место $n = m'$ тогда и только тогда, когда $\varphi(n) = \varphi(m)''$, что равносильно условию $\varphi(m') = (\varphi(m))''$ для любого $m \in N$. Легко доказать, что система $\langle N, '' \rangle$ является натуральным рядом с единицей $\varphi(1) = e$, т. е. удовлетворяет аксиомам P_1 — P_4.

Пусть система $\langle N_1, \oplus \rangle$ является изоморфным образом аддитивной полугруппы натуральных чисел при изоморфизме ψ и $\psi(1) = e$. Определим на N_1 отношение непосредственного следования, положив $n_1' = n_1 \oplus e$ для любого $n_1 \in N_1$. Если $\psi(n) = n_1$, то $\psi(n') = \psi(n+1) = \psi(n) \oplus \psi(1) = n_1 \oplus e = n_1'$. Следовательно, ψ является изоморфизмом натурального ряда $\langle N, ' \rangle$ на систему $\langle N_1, ' \rangle$ и, по доказанному, последняя является натуральным рядом. В соответствии с определением аддитивной полугруппы натуральных чисел 2.2.7 нам остается лишь убедиться в том, что операция $\oplus$ удовлетворяет аксиомам сложения a) и b) из 2.2.1. Для любых $m_1, n_1 \in N_1$, имеем: $m_1 \oplus e = m_1'$ и $m_1 \oplus n_1' = m_1 \oplus (n_1 \oplus e) = (m_1 \oplus n_1) \oplus e = (m_1 \oplus n_1)'$.

Итак, система $\langle N_1, \oplus \rangle$ является аддитивной полугруппой натуральных чисел.

Аналогично доказывается, что изоморфный образ полукольца натуральных чисел есть полукольцо натуральных чисел.

Пусть система $\langle N_1, \lhd \rangle$ является изоморфным образом линейно упорядоченного множества натуральных чисел $\langle N, < \rangle$ при изоморфизме f. Отношение «меньше» для натуральных чисел определяется с помощью сложения (см. 2.4.6). Определим на N_1 операцию сложения $\oplus$, положив $m_1 \oplus n_1 = f(m+n)$. Для любых $m_1 = f(m)$, $n_1 = f(n)$ из N_1. Тогда f — изоморфизм $\langle N, + \rangle$ на $\langle N_1, \oplus \rangle$ и, по доказанному, последняя система является аддитивной полугруппой натуральных чисел. Легко видеть, что $m_1 \lhd n_1$ тогда и только тогда, когда существует $k_1 \in N$ такой, что $n_1 = m_1 \oplus k_1$. Следовательно, $\langle N_1, \lhd \rangle$ является линейно упорядоченным множеством натуральных чисел.

Используя уже доказанное, нетрудно установить, что изоморфный образ упорядоченного полукольца натуральных чисел есть упорядоченное полукольцо натуральных чисел. □

§ 9. Конечные и счетные множества

Определение и основное свойство конечного множества

Натуральные числа используются при счете. Образно говоря, счет — это «присвоение номерков» элементам пересчитываемого множества M. Точнее, счет — это установление взаимно однозначного отображения множества M на некоторый начальный отрезок натурального ряда. Если элементы множества M удается пересчитать, то множество M называют конечным. Уточним это понятие в строгом определении. Предварительно введем одно вспомогательное понятие.

2.9.1. Определение. Два множества называются *равномощными*, если существует взаимно однозначное отображение одного множества на другое.

2.9.2. Определение. Множество M называется *конечным*, если оно либо пусто, либо равномощно некоторому начальному отрезку $\overline{1,n}$ натурального ряда.

Существует два основных способа сравнения множеств по количеству элементов. Например, два конечных множества можно пересчитать и сравнить полученные числа. Однако этот способ не годится при сравнении бесконечных множеств. Второй способ сравнения обходится без чисел. Можно считать, что два множества содержат «одинаковое количество элементов», если они равномощны. Например, взаимно однозначное отображение $\varphi(n) = 2n$ для любого $n \in N$ убеждает нас, что множества N и $2N$ равномощны, содержат «одинаковое количество элементов». Здесь мы видим пример взаимно однозначного отображения множества на свое собственное подмножество. Докажем, что конечное множество нельзя взаимно однозначно отобразить на свое собственное подмножество. Для этого нам понадобится следующее утверждение.

2.9.3. Лемма. *Если существует взаимно однозначное отображение множества $\{a\} \cup B$ на свое собственное подмножество, то существует взаимно однозначное отображение множества B на свое собственное подмножество.*

Доказательство. Если $a \in B$, то утверждение очевидно, поэтому будем считать, что $a \notin B$. Пусть φ — взаимно однозначное отображение множества $\{a\} \cup B$ на свое собственное подмножество, которое обозначим через D, т. е. $\varphi(\{a\} \cup B) = D \subset \{a\} \cup B$. Если $a \notin D$ или $\varphi(a) = a$, то, удалив из рассмотрения пару $(a, \varphi(a))$, получим искомое взаимно однозначное отображение множества B на свое собственное подмножество.

Пусть $a \in D$ и $\varphi(a) \neq a$. Тогда существует $b \in B$ такой, что $b \neq a$ и $\varphi(b) = a$. Изменим отображение φ, заменив пару $(a, \varphi(a))$ парой (a, a), а пару (b, a) — парой $(b, \varphi(a))$, оставив остальные пары соответствующих элементов неизменными. Другими словами, определим отображение ψ, положив:

$$\psi(x) = \begin{cases} a, & \text{если } x = a; \\ \varphi(a), & \text{если } x = a; \\ \varphi(x), & \text{если } x \neq a,\ x \neq b. \end{cases}$$

Тогда получим $\psi(a) = a$ и придем к рассмотренному случаю. □

2.9.4. Теорема (основное свойство конечного множества). *Конечное множество не равномощно своему собственному подмножеству.*

Доказательство. Достаточно установить, что для любого $n \in N$ отрезок $\overline{1,n}$ нельзя взаимно однозначно отобразить на свое собственное подмножество. Докажем это индукцией по n. При $n = 1$ отрезок $\overline{1,1} = \{1\}$ и единственным его собственным подмножеством является $\varnothing$, так что для $\overline{1,1}$ утверждение верно.

Пусть утверждение верно для отрезка $\overline{1,n}$, докажем, что оно верно для отрезка $\overline{1,n+1}$. Предположим противное: пусть существует взаимно однозначное отображение отрезка $\overline{1,n+1} = \overline{1,n} \cup \{n+1\}$ на свое собственное подмножество. Тогда по лемме 2.9.3 существует взаимно однозначное отображение отрезка $\overline{1,n}$ на свое собственное подмножество, что противоречит индуктивному предположению. □

2.9.5. Следствие. *Любое непустое конечное множество равномощно только одному начальному отрезку натурального ряда.*

Доказательство. Пусть множество M равномощно отрезкам $\overline{1,m}$ и $\overline{1,n}$. Если предположить, что $m < n$, то взаимно однозначное отображение $\overline{1,n} \to M \to \overline{1,m}$ будет взаимно однозначным отображением отрезка $\overline{1,n}$ на свое собственное подмножество $\overline{1,m}$, что противоречит 2.9.4. Следовательно, $m = n$. □

Доказанное следствие позволяет ввести следующее понятие.

2.9.6. Определение. Будем говорить, что множество M *содержит n элементов*, и писать $|M| = n$, если M равномощно начальному отрезку $\overline{1,n}$ натурального ряда.

2.9.7. Определение. Множество называется *бесконечным*, если оно не является конечным.

2.9.8. Следствие. *Множество натуральных чисел бесконечно.*

Доказательство вытекает из того, что множество N равномощно своему собственному подмножеству $2N$. □

Число элементов объединения и прямого произведения двух конечных множеств

2.9.9. Теорема. *Если A и B — непустые конечные множества и $A \cap B = \varnothing$, то $A \cup B$ конечно и $|A \cup B| = |A| + |B|$.*

Доказательство. Пусть $|A| = m$, $|B| = n$. По определению 2.9.7, это означает, что множества A и B равномощны отрезкам соответственно $\overline{1,m}$ и $\overline{1,n}$. Обозначим $\overline{m+1, m+n} = \{x \in N \mid m+1 \le x \le m+n\}$ и определим отображение $\varphi : \overline{1,n} \to \overline{m+1, m+n}$, положив $\varphi(y) = m + y$ для любого $y \in \overline{1,n}$. Легко видеть, что φ — взаимно однозначное отображение отрезка $\overline{1,n}$ на отрезок $\overline{m+1, m+n}$. Но тогда существует взаимно однозначное отображение множества $A \cup B$ на отрезок $\overline{1, m+n} = \overline{1,n} \cup \overline{m+1, m+n}$. Это и означает, что $|A \cup B| = m + n = |A| + |B|$. □

2.9.10. Предложение. *Если непустые множества A и B конечны, то множество $A \times B$ конечно и $|A \times B| = |A| \cdot |B|$.*

Доказательство. Пусть $|A|=m$, $|B|=n$. Равенство $|A\times B|=m\cdot n$ докажем индукцией по n.

При $n = 1$ получаем $B=\{b\}$ и $A\times B=\{(a,b)\,|\,a\in A\}$. Для любого $a\in A$ положим $\varphi(a)=(a,b)$. Очевидно, φ — взаимно однозначное отображение множества A на прямое произведение $A\times B$, следовательно, $|A\times B|=|A|=m=m\cdot 1$.

Пусть для натурального числа n утверждение верно и $|B|=n+1$. Тогда B можно представить в виде $B=B_1\cup\{b_1\}$, где $B_1\cap\{b_1\}=\varnothing$. Тогда $A\times B=(A\times B_1)\cup(A\times\{b_1\})$ и $(A\times B_1)\cap(A\times\{b_1\})=\varnothing$. Используя 2.9.9 и индуктивное предположение, получаем $|A\times B|=|A\times B_1|+|A\times\{b_1\}| = m\cdot n+m = m\cdot(n+1)$. □

Счетные множества

2.9.11. Определение. Множество называется *счетным*, если оно равномощно множеству натуральных чисел.

2.9.12. Теорема. *Всякое подмножество счетного множества либо конечно, либо счетно.*

Доказательство. Пусть A — счетное множество и $M\subseteq A$. Если M конечно, то доказывать нечего. Предположим, что M бесконечно. По определению 2.9.11 существует взаимно однозначное отображение $\varphi: A\to N$. Проще говоря, элементы множества A занумерованы натуральными числами. Пусть элемент $m\in M$ имеет в этой нумерации наименьший номер. Присвоим ему номер 1 и обозначим его через m_1. Пусть уже выбраны элементы $m_1, m_2, \ldots, m_n$. Рассмотрим подмножество остальных элементов из M и, выбрав среди них элемент с наименьшим номером, присвоим ему новый номер $n + 1$, получим элемент m_{n+1}. Всякий элемент из M на конечном шаге получит свой новый номер. Следовательно, M счетно.

2.9.13. Теорема. *Всякое бесконечное множество содержит счетное подмножество.*

Доказательство. Пусть множество A бесконечно. Выберем в нем счетное подмножество. Первый элемент выберем произвольно, пусть это будет a_1. Пусть уже выбраны элементы $a_1, a_2, \ldots, a_n\in A$. Поскольку множество A бесконечно, то подмножество остальных элементов из A не пусто. Выберем произвольно один из них и присвоим ему номер $n + 1$, пусть это будет a_{n+1}. В итоге получим счетное подмножество множества A. □

Заметим, что приведенное доказательство носит упрощенный характер. Более формальное доказательство опирается на так называемую аксиому выбора. Мы не останавливаемся на этих тонких вопросах.

2.9.14. Теорема. *Множество рациональных чисел счетно.*

Доказательство. Рассмотрим множество рациональных чисел в виде $Q=\left\{\dfrac{m}{n}\,\middle|\,m\in Z, n\in N\right\}$. Занумеруем рациональные числа по возрастанию суммы $|m|+n$, а при одинаковой сумме — по возрастанию знаменателя, при равных же знаменателях — по возрастанию числителя. При этом повторяющимся рациональным числам будем присваивать номер лишь

при первом их появлении. Понятно, что в результате всякое рациональное число получит свой натуральный номер. □

2.9.15. Теорема. *Множество действительных чисел не является счетным.*

Доказательство. Достаточно доказать, что подмножество действительных чисел $(0,1)=\{x\in R\,|\,0<x<1\}$ нельзя занумеровать натуральными числами. Предположим противное: пусть все числа множества (0, 1) можно занумеровать натуральными. Представим эти числа в виде десятичных дробей и составим список дробей в порядке возрастания номеров:

$$1)\ 0,\alpha_{11}\alpha_{12}\alpha_{13}\ldots$$

$$2)\ 0,\alpha_{21}\alpha_{22}\alpha_{23}\ldots$$

$$3)\ 0,\alpha_{31}\alpha_{32}\alpha_{33}\ldots$$

$$\ldots\ldots\ldots\ldots\ldots$$

Сконструируем десятичную дробь $0,\beta_1\beta_2\beta_3\ldots$, где цифра $\beta_1\neq\alpha_{11}$, цифра $\beta_2\neq\alpha_{22}$, цифра $\beta_3\neq\alpha_{33}$, и т. д. Очевидно, дробь $0,\beta_1\beta_2\beta_3\ldots\in(0,1)$ и поэтому должна присутствовать в списке. С другой стороны, эта дробь не может совпадать ни с одной дробью из списка, так как для любого $i=1, 2, \ldots$ цифра $\beta_i\neq\alpha_{ii}$. Полученное противоречие доказывает теорему. □

Тема 3
ЦЕЛЫЕ ЧИСЛА

§ 1. Определение системы целых чисел

Формирование определения

Множество целых чисел мы представляем себе как объединение натуральных чисел, нуля и чисел, противоположных натуральным. Целые числа можно складывать и перемножать, причем эти операции обладают всеми свойствами, которыми они обладают для натуральных чисел. Кратко можно сказать, что множество целых чисел относительно сложения и умножения образует полукольцо. Но это полукольцо, в отличие от полукольца натуральных чисел, содержит нуль и для всякого целого числа содержит противоположное ему число. Эти дополнительные свойства превращают полукольцо в кольцо в смысле следующего определения.

3.1.1. Определение. Система $\langle K, +, \cdot \rangle$ называется *кольцом*, если выполнены следующие условия:

1) система $\langle K, + \rangle$ является коммутативной группой (она называется *аддитивной группой кольца*), т. е.:

a) сложение + *ассоциативно* и *коммутативно*,

b) существует элемент $0 \in K$, называемый *нулем*, такой что $a + 0 = a$ для любого $a \in K$,

c) для всякого $a \in K$ существует элемент $-a \in K$, называемый *противоположным для a*, такой что $a + (-a) = 0$;

2) система $\langle K, \cdot \rangle$ является *полугруппой* (она называется *мультипликативной полугруппой кольца*), т. е. умножение *ассоциативно*;

3) умножение *дистрибутивно* относительно сложения, т. е. $a(b+c) = ab + ac$ и $(b+c)a = ba + ca$ для любых $a, b, c \in K$.

Если умножение в кольце коммутативно, то кольцо называется *коммутативным*.

Таким образом, полукольцо является кольцом, если его аддитивная полугруппа является группой.

Итак, систему целых чисел мы представляем себе как кольцо, основное множество которого состоит из натуральных чисел, нуля и чисел, противоположных натуральным. Закрепим это представление в виде определения.

3.1.2. Определение. *Системой целых чисел* называется кольцо $\langle Z, +, \cdot \rangle$, которое удовлетворяет следующим условиям:

1) оно содержит полукольцо натуральных чисел $\langle N, +, \cdot \rangle$;

2) всякий элемент из Z принадлежит одному из подмножеств: N, $\{0\}$ и $-N = \{-n \mid n \in N\}$. Элементы множества Z называются *целыми числами*, а система $\langle Z, +, \cdot \rangle$ называется *кольцом целых чисел*.

Определяя систему целых чисел как кольцо, мы тем самым в краткой форме указываем на выполнимость свойств сложения и умножения, перечисленных в определении кольца.

Существуют кольца, далеко не похожие на кольцо целых чисел. Например, кольцо квадратных матриц порядка $n > 1$, элементы которых целые числа, не коммутативно. Кольцо классов вычетов по модулю m конечно, оно содержит m элементов. Кольцо с условием 1) из 3.1.2 бесконечно и, наряду с множеством натуральных чисел N, содержит 0 и $-N$ — числа, противоположные натуральным. Но, помимо этих элементов, такое кольцо может содержать и другие элементы. Так, кольцо рациональных чисел, кроме этих множеств, содержит еще дробные числа. Условие 2) из 3.1.2 требует, чтобы в кольце $\langle Z, +, \cdot \rangle$, кроме названных подмножеств, не было посторонних элементов.

Кольцо целых чисел как расширение полукольца натуральных чисел

Напомним определение подкольца.

3.1.3. Определение. Пусть дано кольцо $\langle K, +, \cdot \rangle$. Подмножество $H \subseteq K$ называется *подкольцом*, если выполнены следующие условия:

1) H замкнуто относительно сложения и умножения, т. е. если $a, b \in H$, то $a + b \in H$ и $a \cdot b \in H$;

2) $0 \in H$;

3) если $a \in H$, то $-a \in H$.

В полукольце натуральных чисел уравнение вида $a + x = b$ не всегда разрешимо. Поставим перед собой задачу: найти минимальное полукольцо, которое содержало бы полукольцо натуральных чисел и в котором было бы разрешимо названное уравнение. Но полукольцо, в котором разрешимо уравнение $a + x = b$ для любых элементов a и b, является кольцом (докажите это). Таким образом, нужно найти кольцо, которое содержало бы полукольцо натуральных чисел и не содержало бы собственных подколец, содержащих натуральные числа (свойство минимальности).

Докажем, что кольцо целых чисел решает поставленную задачу. Вместе с тем получим новое краткое по формулировке определение системы целых чисел.

3.1.4. Теорема. *Система $\langle K, +, \cdot \rangle$ есть система целых чисел тогда и только тогда, когда она является минимальным кольцом, содержащим полукольцо натуральных чисел.*

Доказательство. ($\Rightarrow$) По определению 3.1.2, система целых чисел $\langle Z, +, \cdot \rangle$ является кольцом, содержащим полукольцо натуральных чисел $\langle N, +, \cdot \rangle$. Докажем свойство минимальности. Пусть H — подкольцо, со-

держащее N. По определению подкольца (3.1.3), $0 \in H$ и $-N \subseteq H$. Но тогда $Z = N \cup \{0\} \cup -N \subseteq H$. Следовательно, $H = Z$.

($\Leftarrow$) Пусть система $\langle K, +, \cdot \rangle$ является минимальным кольцом, содержащим полукольцо натуральных чисел $\langle N, +, \cdot \rangle$. Докажем, что $\langle K, +, \cdot \rangle$ является системой целых чисел в соответствии с определением 3.1.2. Для этого остается лишь установить, что $K = N \cup \{0\} \cup -N$. Обозначим $N \cup \{0\} \cup -N = Z$. Легко видеть, что Z является подкольцом, содержащим N. По свойству минимальности $Z = K$. □

Доказанная теорема позволяет определить систему целых чисел как *минимальное кольцо, содержащее полукольцо натуральных чисел.*

Определение кольца целых чисел с помощью понятия разности натуральных чисел

Как уже отмечалось, кольцо имеет перед полукольцом то преимущество, что в кольце однозначно разрешимо уравнение $a + x = b$ для любых элементов кольца a и b. Это, в частности, и отличает кольцо целых чисел от полукольца натуральных чисел. Возможность всегда однозначно решить такое уравнение позволяет определить в кольце новую операцию — вычитание.

3.1.5. Определение. Пусть дано кольцо $\langle K, +, \cdot \rangle$. Для любых $a, b \in K$ определим $b - a$ как решение уравнения $a + x = b$. Отображение $K \times K \to K$, сопоставляющее всякой упорядоченной паре элементов (b, a) элемент $b - a$, называется *вычитанием*, а элемент $b - a$ называется *разностью* элементов b и a.

Непосредственной проверкой убеждаемся, что элемент $b + (-a)$ является решением уравнения $a + x = b$, а из единственности решения получаем $b - a = b + (-a)$.

Используя понятие разности элементов кольца, установим еще одну характеризацию системы целых чисел, которую также можно взять в качестве ее определения.

3.1.6. Теорема. *Система $\langle K, +, \cdot \rangle$ есть система целых чисел тогда и только тогда, когда она является кольцом, содержащим полукольцо натуральных чисел $\langle N, +, \cdot \rangle$, причем всякий элемент из K представим в виде разности натуральных чисел, т. е. для любого $a \in K$ существуют $m, n \in N$, такие, что $a = m - n$.*

Доказательство. ($\Rightarrow$) Пусть $\langle K, +, \cdot \rangle$ есть система целых чисел и $a \in K$. Докажем, что элемент a представим в виде разности натуральных чисел. По условию 2) из определения 3.1.2, $K = Z = N \cup \{0\} \cup -N$. Если $a \in N$, то $a = (a + 1) - 1$; если $a \in \{0\}$, то $a = n - n$, где $n \in N$; если же $a \in -N$, то $a = -n$ и $a = 1 - (n + 1)$.

($\Leftarrow$) Пусть теперь кольцо $\langle K, +, \cdot \rangle$ содержит полукольцо натуральных чисел $\langle N, +, \cdot \rangle$ и всякий элемент из K представим в виде разности натуральных чисел. Докажем, что $K = N \cup \{0\} \cup -N = Z$. По условию, для любого $a \in K$ существуют $m, n \in N$, такие, что $a = m - n$. Но для нату-

ральных чисел m и n имеет место одно и только одно из соотношений: либо $m = n + k$ при некотором $k \in N$, либо $m = n$, либо $n = m + l$ при некотором $l \in N$. В первом случае получаем $a = m - n = k \in N$, во втором $a = m - n = 0 \in \{0\}$, а в третьем $a = m - n = -l \in -N$. □

§ 2. Существование системы целых чисел

Вводные соображения

Существует ли определенная нами система целых чисел? Не ведет ли к противоречию ее аксиоматическое определение 3.1.2? Отвечая на эти вопросы, мы построим систему целых чисел, используя натуральные числа, и тем самым покажем, что если бы наше определение целых чисел было противоречивым, то противоречие оказалось бы следствием аксиом Пеано. Но, как было отмечено в п. 3 § 1 гл. 2, аксиоматическая теория натуральных чисел, основанная на аксиомах Пеано, непротиворечива. Тем самым будет доказана непротиворечивость аксиоматической теории целых чисел, основанной на определении 3.1.2.

Теорема 3.1.6 утверждает, что всякое целое число можно представить в виде разности натуральных чисел. Это наталкивает на мысль «смоделировать» целое число $z = a - b$, где $a, b \in N$, в виде упорядоченной пары натуральных чисел (a, b). Например, число $5 = 6 - 1$ изобразится в виде упорядоченной пары $(6, 1)$. Однако целое число представляется в виде разности натуральных чисел неоднозначно. Например, $5 = 6 - 1 = 7 - 2 = 8 - 3 = \ldots$, поэтому пары $(6, 1)$, $(7, 2)$, $(8, 3)$, ... следует считать «моделями» одного и того же целого числа 5. Очевидно, $a - b = a_1 - b_1$ тогда и только тогда, когда $a + b_1 = b + a_1$. Поэтому если выполняется последнее равенство, то будем считать, что упорядоченные пары натуральных чисел (a, b) и (a_1, b_1) изображают одно и то же целое число. Такие пары назовем эквивалентными. Класс пар, эквивалентных паре (a, b), обозначим через $\overline{(a, b)}$ — он «моделирует» целое число $a - b$. Как определить сложение и умножение классов эквивалентных пар, чтобы получить кольцо целых чисел? Найдем сумму и произведение разностей натуральных чисел:

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

Следовательно, суммой классов $\overline{(a, b)}$ и $\overline{(c, d)}$ целесообразно считать класс $\overline{(a + c, b + d)}$, а их произведением — класс $\overline{(ac + bd, ad + bc)}$. Теперь понятно, как нужно строить кольцо целых чисел из натуральных чисел. Реализуем намеченную программу.

Построение кольца целых чисел

На множестве $N \times N = \{(a, b) \mid a, b \in N$ определим отношение $\sim$, положив $(a, b) \sim (a_1, b_1)$ тогда и только тогда, когда $a + b_1 = a_1 + b$. Покажем, что $\sim$ есть отношение эквивалентности.

Рефлексивность: для любой пары (a, b) очевидно имеем $(a, b) \sim (a, b)$.

Симметричность: если $(a,b) \sim (a_1, b_1)$, то $a + b_1 = a_1 + b$, откуда $(a_1, b_1) \sim (a, b)$.

Транзитивность: если $(a,b) \sim (a_1, b_1)$ и $(a_1, b_1) \sim (a_2, b_2)$, то $a + b_1 = a_1 + b$ и $a_1 + b_2 = a_2 + b_1$. Сложив эти равенства, получим $a + b_1 + a_1 + b_2 = a_1 + b + a_2 + b_1$, откуда $a + b_2 = b + a_2$, т. е. $(a, b) \sim (a_2, b_2)$.

По отношению эквивалентности $\sim$ множество $N \times N$ распадается на непересекающиеся классы эквивалентных пар. Обозначим $\overline{(a,b)} = \{(x, y) \mid (x, y) \sim (a, b)\}$. Таким образом, $\overline{(a,b)} = \overline{(a_1, b_1)}$ тогда и только тогда, когда $a + b_1 = a_1 + b$. Множество всех классов эквивалентных пар обозначим через $\overline{Z}$, а всякий класс $\overline{(a,b)}$ назовем целым числом.

Определим на $\overline{Z}$ сложение формулой $\overline{(a,b)} \oplus \overline{(c,d)} = \overline{(a+c, b+d)}$. Покажем, что сумма классов определяется своими слагаемыми однозначно. Пусть $\overline{(a,b)} = \overline{(a_1, b_1)}$, $\overline{(c,d)} = \overline{(c_1, d_1)}$, докажем, что $\overline{(a,b)} \oplus \overline{(c,d)} = \overline{(a_1, b_1)} \oplus \overline{(c_1, d_1)}$. Из равенства $\overline{(a,b)} = \overline{(a_1, b_1)}$ следует $a + b_1 = a_1 + b$, а из $\overline{(c,d)} = \overline{(c_1, d_1)}$ следует $c + d_1 = c_1 + d$. Отсюда $a + b_1 + c + d_1 = a_1 + b + c_1 + d$. Следовательно, $\overline{(a+c, b+d)} = \overline{(a_1 + c_1, b_1 + d_1)}$, откуда $\overline{(a,b)} \oplus \overline{(c,d)} = \overline{(a_1, b_1)} \oplus \overline{(c_1, d_1)}$.

Определим на $\overline{Z}$ операцию умножения классов, положив $\overline{(a,b)} \otimes \overline{(c,d)} = \overline{(ac + bd, ad + bc)}$. Как и для сложения, легко доказать, что произведение классов однозначно определяется своими сомножителями.

3.2.1. Теорема. *Система* $\langle \overline{Z}, \oplus, \otimes \rangle$ *является кольцом целых чисел.*

Доказательство. 1. Установим, что система $\langle \overline{Z}, \oplus, \otimes \rangle$ является кольцом.

1) Система $\langle \overline{Z}, \oplus \rangle$ является коммутативной группой. В самом деле:

a) сложение коммутативно и ассоциативно, что проверяется непосредственно с использованием соответствующих свойств сложения натуральных чисел,

b) нулевым элементом является класс $\overline{0} = \overline{(n, n)}$, где $n \in N$, так как для любого класса $\overline{(a,b)} \in \overline{Z}$ имеем: $\overline{(a,b)} \oplus \overline{0} = \overline{(a,b)} \oplus \overline{(n,n)} = \overline{(a+n, b+n)} = \overline{(a,b)}$,

c) для класса $\overline{(a,b)}$ противоположным будет класс $\overline{(b,a)}$, так как $\overline{(a,b)} \oplus \overline{(b,a)} = \overline{(a+b, b+a)} = \overline{0}$.

2) Система $\langle \overline{Z}, \otimes \rangle$ является полугруппой. Ассоциативность умножения проверяется непосредственно.

3) Умножение $\otimes$ дистрибутивно относительно сложения $\oplus$, что также проверяется непосредственным подсчетом.

2. Рассмотрим множество $\overline{N} = \{\overline{(n+1, 1)} \mid n \in N\}$. Докажем замкнутость этого множества относительно сложения и умножения. Обозначим $\overline{n} = \overline{(n+1, 1)}$ для любого $n \in N$. Тогда $\overline{m} \oplus \overline{n} = \overline{(m+1, 1)} \oplus \overline{(n+1, 1)} = \overline{(m+1+n+1, 1+1)} = \overline{(m+n+1, 1+1)} = \overline{m+n} \in \overline{N}$.

Аналогично для умножения. Так как изоморфный образ полукольца натуральных чисел есть полукольцо натуральных чисел (см. 2.8.2), то остается лишь установить изоморфизм $\langle N, +, \cdot \rangle$ на $\langle \overline{N}, \oplus, \otimes \rangle$. Лег-

ко проверить, что искомым изоморфизмом является отображение $\varphi: N \to \overline{N}$, при котором $\varphi(n) = \overline{n}$ для любого $a = b(-q) + r$. Итак, доказано, что кольцо $\langle \overline{Z}, \oplus, \otimes \rangle$ содержит полукольцо натуральных чисел $\langle \overline{N}, \oplus, \otimes \rangle$.

3. Докажем, что $\overline{Z} = \overline{N} \cup \{\overline{0}\} \cup -\overline{N}$. Пусть $\overline{(a,b)} \in \overline{Z}$. Для натуральных чисел a и b имеет место одно из соотношений: $a = b + k$, $a = b$, $b = a + m$, где $k, m \in N$. Если $a = b + k$, то $\overline{(a,b)} = \overline{(b+k,b)} = \overline{(k+1,1)} = \overline{k} \in \overline{N}$; если $a = b$, то $\overline{(a,b)} = \overline{(b,b)} = \overline{0} \in \{\overline{0}\}$; если же $b = a + m$, то $\overline{(a,b)} = \overline{(a,a+m)} = \overline{(1,m+1)} = -\overline{(m+1,1)} \in -\overline{N}$. □

§ 3. Основные свойства системы целых чисел

Основные свойства колец

Исходя из определения 3.2.2 целых чисел, докажем известные свойства этих чисел. По определению, система целых чисел является прежде всего кольцом, поэтому на нее распространяются общие свойства колец. Докажем основные из них.

3.3.1. Предложение. *Пусть* $\langle K, +, \cdot \rangle$ *— кольцо и* $a, b, c \in K$. *Имеют место следующие свойства*:

1) (свойство нуля) $a \cdot 0 = 0 \cdot a = 0$;

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

3) (дистрибутивность умножения относительно вычитания) $a \cdot (b - c) = a \cdot b - a \cdot c$, $(b - c) \cdot a = b \cdot a - c \cdot a$.

Доказательство. 1. $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$. Следовательно, $a \cdot 0 = a \cdot 0 + a \cdot 0$. Прибавив к обеим частям этого равенства по $-(a \cdot 0)$, получим $0 = a \cdot 0$. Аналогично доказывается, что $0 \cdot a = 0$.

2. Пользуясь дистрибутивностью умножения относительно сложения и доказанным свойством нуля, получаем $a \cdot (-b) + a \cdot b = a \cdot (-b + b) = a \cdot 0 = 0$. Отсюда следует, что элемент $a \cdot (-b)$ является противоположным для $a \cdot b$, т. е. $a \cdot (-b) = -(a \cdot b)$. Аналогично доказывается, что $(-a) \cdot b = -(a \cdot b)$. Пользуясь доказанным свойством, получаем $(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b)) = a \cdot b$.

3. Используя определение вычитания, дистрибутивность умножения относительно сложения и правила знаков, получаем $a \cdot (b - c) = a \cdot (b + (-c)) = a \cdot b + a \cdot (-c) = a \cdot b + (-(a \cdot c)) = a \cdot b - a \cdot c$. Аналогично доказывается второе равенство. □

Дополним определение 2.7.3 натурального кратного элемента кольца.

3.3.2. Определение. Пусть $\langle K, +, \cdot \rangle$ — кольцо с нулем 0. Для любого $a \in K$ положим $0a = 0$ и для любого $n \in N$ будем считать, что $(-n)a = -(na)$. Элемент ma, где $m \in Z$, называется *целым кратным* элемента a.

Обобщим свойства натуральных кратных из 2.7.4 на целые кратные.

3.3.3. Предложение. *Пусть* $\langle K, +, \cdot \rangle$ *— кольцо. Для любых* $a, b \in K$ *и* $m, n \in Z$ *имеют место равенства*: $(m + n)a = ma + na$; $(mn)a = m(na)$; $ma \cdot nb = (mn)(a \cdot b)$.

Доказательство (с использованием 2.7.4) предоставляется читателю. □

Область целостности

В определении 3.1.2 кольца целых чисел не фигурирует требование коммутативности умножения. Оказывается, это свойство можно доказать исходя из этого определения.

3.3.4. Предложение. *Умножение целых чисел коммутативно.*

Доказательство. По 3.1.7, всякое целое число представимо в виде разности натуральных чисел. Если $x = a - b$, $y = c - d$, где $a, b, c, d \in N$, то, пользуясь свойствами колец 3.3.1 и коммутативностью умножения натуральных чисел, получаем: $x \cdot y = (a-b)\cdot(c-d) = a\cdot c - a\cdot d - b\cdot c + b\cdot d = c\cdot a - d\cdot a - c\cdot b + d\cdot b = (c-d)\cdot(a-b) = y\cdot x$. □

3.3.5. Предложение. *В кольце целых чисел* $\langle Z, +, \cdot \rangle$ *множества* N, $\{0\}$ *и* $-N$ *попарно не пересекаются.*

Доказательство. Если предположить, что $n = 0$ для некоторого $n \in N$, то $n' = n + 1 = 1$, что противоречит первой аксиоме Пеано. Следовательно, $N \cap \{0\} = \varnothing$. Отсюда следует, что $-N \cap \{0\} = \varnothing$ и $N \cap -N = \varnothing$. □

3.3.6. Предложение. *Квадрат любого целого числа, отличного от нуля, есть число натуральное.*

Доказательство. Пусть $0 \neq z \in Z$. Тогда либо $z \in N$, откуда $z^2 \in N$; либо $z \in -N$, откуда $z = -n$, где $n \in N$, и тогда $z^2 = (-n)\cdot(-n) = n^2 \in N$. □

3.3.7. Предложение. *Если произведение двух целых чисел равно нулю, то хотя бы один из сомножителей равен нулю.*

Доказательство. Предположим противное, пусть существуют целые числа a и b такие, что $a \cdot b = 0$, хотя $a \neq 0$ и $b \neq 0$. Тогда, по 3.3.6, $a^2, b^2 \in N$, откуда $0 = a^2 b^2 \in N$, что противоречит 3.3.5. □

3.3.8. Определение. Пусть $\langle K, +, \cdot \rangle$ — кольцо. Элементы $a, b \in K$ называются *делителями нуля*, если $a \neq 0$, $b \neq 0$, но $a \cdot b = 0$.

Например, в кольце классов вычетов Z_6 классы вычетов $\overline{2}$ и $\overline{3}$ являются делителями нуля, так как $\overline{2} \neq \overline{0}$ и $\overline{3} \neq \overline{0}$, но $\overline{2}\cdot\overline{3} = \overline{6} = \overline{0}$. Отметим, что в кольце целых чисел нет такой «экзотики».

3.3.9. Предложение. *В кольце целых чисел нет делителей нуля.*

Доказанные свойства целых чисел стимулируют введение следующего общего понятия.

3.3.10. Определение. *Областью целостности* называется коммутативное кольцо с единицей, отличной от нуля, в котором нет делителей нуля.

Из доказанных выше свойств целых чисел вытекает следующая теорема.

3.3.11. Теорема. *Кольцо целых чисел является областью целостности.*

Другим примером области целостности является кольцо многочленов с целыми коэффициентами от одной переменной.

Упорядоченное кольцо целых чисел

Введем на множестве целых чисел отношение «меньше».

3.3.12. Определение. Для любых целых чисел a и b положим $a < b$ тогда и только тогда, когда $b - a \in N$.

3.3.13. Теорема. *Система* $\langle Z, < \rangle$ *является линейно упорядоченным множеством.*

Доказательство. Согласно определению 2.4.7 линейно упорядоченного множества нужно установить свойства трихотомии и транзитивности отношения $<$. Из определения системы целых чисел 3.1.2 и свойства 3.3.5 следует, что для любых $a, b \in Z$ разность $b - a$ принадлежит одному и только одному из подмножеств N, $\{0\}$, $-N$. Если $b - a \in N$, то по 3.3.12 $a < b$, если $b - a \in \{0\}$, то $a = b$, а если $b - a \in -N$, то $a - b \in N$, откуда $b < a$.

Докажем свойство транзитивности. Пусть $a, b, c \in Z$ и $a < b$, $b < c$. Тогда $b - a \in N$ и $c - b \in N$, откуда $c - a = (c - b) + (b - a) \in N$. Следовательно, $a < c$. □

3.3.14. Определение. *Упорядоченным кольцом* называется система $\langle K, +, \cdot, < \rangle$, удовлетворяющая следующим условиям:

1) $\langle K, +, \cdot \rangle$ — ненулевое кольцо;

2) $\langle K, < \rangle$ — линейно упорядоченное множество;

3) сложение и умножение *монотонны*, т. е. для любых $a, b, c \in K$, если $a < b$, то $a + c < b + c$ (*монотонность сложения*), и если $a < b$ и $c < 0$, то $a \cdot c < b \cdot c$ (*монотонность умножения*).

Легко видеть, что система $\langle Z, +, \cdot, < \rangle$ является упорядоченным кольцом, которое называется *упорядоченным кольцом целых чисел.*

Из определения отношения $<$ (3.3.12) следует, что среди целых чисел натуральные числа и только они положительны. Отсюда, по 3.3.6, получаем, что квадрат любого целого числа, отличного от нуля, положителен. Рассмотрим эти свойства в общей ситуации.

3.3.15. Предложение. *В упорядоченном кольце* $\langle K, +, \cdot, < \rangle$, *если* $a \in K$ *и* $a \neq 0$, *то* $a^2 > 0$, *и если* e *— единица кольца, то для любого* $n \in N$ *имеем* $ne > 0$.

Доказательство. Из условия следует, что либо $a > 0$, либо $a < 0$. Если $a > 0$, то, по свойству монотонности умножения, получаем $a^2 > 0$. Если же $a < 0$, то $-a > 0$ и по доказанному $(-a)(-a) > 0$, откуда по правилу знаков снова получаем $a^2 > 0$.

Напомним, что ne обозначает сумму n слагаемых, каждое из которых равно e (см. 2.7.3). Неравенство $ne > 0$ докажем индукцией по n. При $n = 1$ получаем $1e = e = e^2 > 0$. Пусть $ne > 0$. Тогда, пользуясь свойством монотонности сложения, получаем $(n+1)e = ne + e > e > 0$. □

3.3.16. Теорема. *В упорядоченном кольце целых чисел* $\langle Z, +, \cdot, < \rangle$ *выполняется аксиома Архимеда: для любых целых чисел* $a > 0$ *и* b *существует натуральное число* n *такое, что* $ne > b$.

Доказательство. Если $b \leq 0$, то можно взять $n = 1$. Для натуральных же a и b утверждение доказано в 2.6.7. □

Забегая вперед, скажем, что аксиома Архимеда будет доказана также и для рациональных чисел. Таким образом, для натуральных, целых и рациональных чисел она является теоремой, и название «аксиома Архимеда» — лишь дань традиции. Только в определении системы действительных чисел это предложение встретится в качестве аксиомы, т. е. первичного свойства.

3.3.17. Теорема. *В упорядоченном кольце целых чисел всякое непустое ограниченное сверху (снизу) подмножество содержит наибольший (соответственно, наименьший) элемент.*

Доказательство. Пусть $\varnothing \neq M \subseteq Z$ и M ограничено сверху целым числом b. Если $M \cap N \neq \varnothing$, то $M \cap N$ — подмножество натуральных чисел, ограниченное сверху натуральным числом b. По 2.4.16 оно имеет наибольший элемент, который, очевидно, будет наибольшим в M. Если $M \cap N = \varnothing$, но $0 \in M$, то 0 и является наибольшим числом в M. Если же $M \subseteq -N$, то $-M \subseteq -N$ и по 2.4.18 $-M$ содержит наименьший элемент, который обозначим через $-m$. Но тогда m — наибольший в M.

Пусть, наконец, M — непустое подмножество целых чисел, ограниченное снизу целым числом c. Тогда подмножество $-M$ ограничено сверху целым числом $-c$ и по доказанному имеет наибольший элемент k. Очевидно, $-k$ является наименьшим элементом в M.

Деление с остатком

Поскольку понятие модуля нам понадобится не только для целых чисел, то определим его в наиболее общей ситуации.

3.3.18. Определение. Пусть a — элемент упорядоченного кольца. *Модулем элемента* a называется наибольший из элементов a и $-a$. Обозначается $|a|$.

3.3.19. Теорема (о делении с остатком). *Для любых целых чисел* a и $b \neq 0$ *существуют и притом единственные целые числа* q и r *такие, что* $a = bq + r$, *причем* $0 \leq r < |b|$.

Числа q и r называются соответственно *неполным частным* и *остатком*.

При положительном b сама теорема и ее доказательство становятся очевидными, если обратиться к рис. 10. На нем числовая прямая разбита на отрезки длины b точками $0, b, -b, 2b, -2b, \ldots$. Очевидно, где бы ни была расположена точка a, она обязательно попадет в один из этих отрезков. При этом можно считать, что a не совпадает с правым концом отрезка, так как если бы это произошло, то мы рассмотрели бы следующий отрезок, для которого a является левым концом.

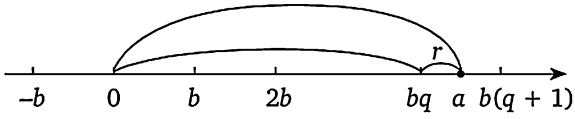

Рис. 10

Пусть точка a попала в отрезок $[bq, b(q+1)]$. Тогда $bq \leq a < bq + b$, откуда получаем $0 \leq a - bq < b$. Обозначив $r = a - bq$, получим $a = bq + r$ и $0 \leq r < b$, что и требовалось доказать.

Это наглядное доказательство вполне приемлемо в школе. Однако, чтобы вписать его в развиваемую нами аксиоматическую теорию целых чисел, нам нужно ввести понятие числовой прямой и доказать тот

«очевидный» факт, что число a обязательно попадет в один из рассматриваемых отрезков.

Приведем доказательство, которое не опирается на наглядность, а использует лишь тот материал, который уже получил обоснование в нашей аксиоматической теории целых чисел. Читателю предлагается увидеть в нем обоснование приведенного выше наглядного доказательства.

Доказательство теоремы. 1. Существование чисел q и r. Пусть $b > 0$. Рассмотрим множество $M = \{bn \mid n \in Z, bn \le a\}$ (т. е. множество целых чисел, кратных b и не превосходящих a). По аксиоме Архимеда (3.3.16), существует натуральное число n такое, что $nb > -a$, откуда $-nb > a$, значит, $b(-n) \in M$. Следовательно, M — непустое подмножество целых чисел, ограниченное сверху целым числом a. По 3.3.17. в M существует наибольший элемент, пусть это будет bq. Обозначим $r = a - bq$, тогда $a = bq + r$. Поскольку $bq \in M$, то $bq \le a$, откуда $0 \le a - bq = r$. Так как bq — наибольшее число в M, то $b(q+1) \notin M$, поэтому $a < bq + b$, откуда $r = a - bq < b = |b|$. Таким образом, $0 \le r < b$.

Если теперь $b < 0$, то $-b > 0$ и по доказанному существуют целые числа q и r такие, что $a = (-b)q + r$ и $0 \le r < |-b|$. Но тогда $a = b(-q) + r$ и $0 \le r < |b|$.

2. Единственность чисел q и r. Пусть $a = bq + r = bq_1 + r_1$, где $q, q_1, r, r_1 \in Z$ и $0 \le r < |b|$, $0 \le r_1 < |b|$. Если предположить, что $r \ne r_1$, например $r < r_1$, то получаем $0 < r_1 - r < |b|$ и $r_1 - r = bq - bq_1 = b(q - q_1)$. Отсюда $0 < b(q - q_1) < |b|$ — противоречие. Следовательно, $r = r_1$, но тогда $q = q_1$. □

Деление с остатком, как известно, является составной частью алгоритма Евклида, который, в частности, используется для нахождения наибольшего общего делителя двух целых чисел. Области целостности, на которые переносится деление с остатком, называются *евклидовыми кольцами* (см. [2, 5]). Примером евклидова кольца является кольцо многочленов от одной переменной над произвольным полем.

Представление целого числа в десятичной системе счисления

Введем множество цифр десятичной системы счисления.

3.3.20. Определение. Пусть дано упорядоченное кольцо целых чисел $\langle Z, +, \cdot, < \rangle$ с нулем 0 и единицей 1. Обозначим $2 = 1 + 1$, $3 = 2 + 1$, $4 = 3 + 1$, $5 = 4 + 1$, $6 = 5 + 1$, $7 = 6 + 1$, $8 = 7 + 1$, $9 = 8 + 1$, $10 = 9 + 1$. Всякий элемент множества $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ назовем *цифрой*.

3.3.21. Теорема. *Для любого натурального числа a существует и единственный набор цифр $a_n, a_{n-1}, \ldots, a_0$ такой, что $a = a_n 10^n + a_{n-1} 10^{n-1} + \ldots + a_0$, причем $a_n \ne 0$.*

Доказательство. 1. Существование. Для $a = 1$ утверждение верно. Пусть для всех натуральных чисел, меньших a, утверждение верно, докажем его для a. По теореме 3.3.19 о делении с остатком, существуют целые числа q и a_0 такие, что $a = 10q + a_0$, где $0 \le a_0 < 10$, т. е. a_0 — цифра. Легко видеть, что $q \ge 0$. Если $q = 0$, то $a = a_0$ и утверж-

дение доказано для a. Если же $q > 0$, то $0 < q < a$ и по индуктивному предположению существует упорядоченный набор цифр $a_n, a_{n-1}, \ldots, a_1$ такой, что $q = a_n 10^{n-1} + a_{n-1} 10^{n-2} + \ldots + a_1$, причем $a_n \neq 0$. Но тогда $a = 10(a_n 10^{n-1} + a_{n-1} 10^{n-2} + \ldots + a_1) + a_0 = a_n 10^n + a_{n-1} 10^{n-1} + \ldots + 10a_1 + a_0$.

2. Единственность. При $a = a_0$ утверждение очевидно. Пусть единственность представления имеет место для всех натуральных чисел, меньших a, и $a = a_n 10^n + a_{n-1} 10^{n-1} + \ldots + a_0 = b_m 10^m + b_{m-1} 10^{m-1} + \ldots + b_0$, где $a_n, a_{n-1}, \ldots, a_0$ и $b_m, b_{m-1}, \ldots, b_0$ — цифры, причем $a_n \neq 0$ и $b_m \neq 0$. Имеем:

$$10(a_n 10^{n-1} + a_{n-1} 10^{n-2} + \ldots + a_1) + a_0 =$$
$$= 10(b_m 10^{m-1} + b_{m-1} 10^{m-2} + \ldots + b_1) + b_0,$$

откуда, в силу единственности деления на 10 с остатком, получаем равенство остатков: $a_0 = b_0$ и неполных частных: $a_n 10^{n-1} + a_{n-1} 10^{n-2} + \ldots + a_1 = b_m 10^{m-1} + b_{m-1} 10^{m-2} + \ldots + b_1$. По индуктивному предположению $n = m$ и $a_i = b_i$ для $i = 1, 2, \ldots, n$. □

3.3.22. Определение. Если натуральное число a представимо в виде $a = a_n 10^n + a_{n-1} 10^{n-1} + \ldots + a_0$, где $a_n, a_{n-1}, \ldots, a_0$ — цифры и $a_n \neq 0$, то запись $a = a_n a_{n-1} \ldots a_0$ называется *представлением* натурального числа a *в десятичной системе счисления*, или просто *десятичной записью* числа a. Десятичной записью числа $-a$ называется $-a_n a_{n-1} \ldots a_0$, а десятичной записью нуля является 0.

Таким образом, всякое целое число имеет единственную десятичную запись. Заметим, что 10 можно заменить произвольным натуральным числом $g > 1$ и получить g-ичную запись целого числа. При этом, g называется *основанием* системы счисления.

Изоморфизм систем целых чисел

Уточняя привычное представление о единственности целых чисел, докажем, что любые два кольца целых чисел изоморфны, и только отождествляя соответствующие при изоморфизме элементы, можно считать, что существует лишь одно кольцо целых чисел.

3.3.23. Теорема. *Любые два кольца (упорядоченных кольца) целых чисел изоморфны.*

Доказательство. Пусть дано кольцо целых чисел $\langle Z, +, \cdot \rangle$, содержащее полукольцо натуральных чисел $\langle N, +, \cdot \rangle$, и кольцо целых чисел $\langle Z_1, +, \cdot \rangle$, содержащее полукольцо натуральных чисел $\langle N_1, +, \cdot \rangle$. По 2.8.1, существует изоморфизм φ первого полукольца натуральных чисел на второе. Используя φ, определим отношение $f : Z \to Z_1$ следующим образом. По 3.1.6, всякое целое число $x \in Z$ представимо в виде разности натуральных чисел: $x = a - b$, где $a, b \in N$. Положим $f(x) = \varphi(a) - \varphi(b)$ и докажем, что f — искомый изоморфизм $\langle Z, +, \cdot \rangle$ на $\langle Z_1, +, \cdot \rangle$.

1. f — отображение, т. е. для любых $x, y \in Z$, если $x = y$, то $f(x) = f(y)$. В самом деле, пусть $x = a - b$, $y = c - d$, где $a, b, c, d \in N$. Если $x = y$, то $a - b =$

$= c - d$, откуда последовательно получаем: $a + d = b + c$, $\varphi(a + d) = \varphi(b + c)$, $\varphi(a) + \varphi(d) = \varphi(b) + \varphi(c)$, $\varphi(a) - \varphi(b) = \varphi(c) - \varphi(d)$, $f(x) = f(y)$.

2. Отображение f взаимно однозначно, что доказывается проведением предыдущих рассуждений в обратном порядке.

3. Очевидно, f является отображением на все множество Z_1.

4. Отображение f сохраняет операции сложения и умножения. В самом деле, для любых $x, y \in Z$, где $x = a - b$, $y = c - d$, $a, b, c, d \in N$, получаем:

$$f(x + y) = f((a - b) + (c - d)) = f((a + c) - (b + d)) =$$
$$= \varphi(a + c) - \varphi(b + d) = (\varphi(a) + \varphi(c)) - (\varphi(b) + \varphi(d)) =$$
$$= (\varphi(a) - \varphi(b)) + (\varphi(c) - \varphi(d)) = f(x) + f(y).$$

Аналогично доказывается, что $f(x \cdot y) = f(x) \cdot f(y)$. Таким образом, f — изоморфизм кольца целых чисел $\langle Z, +, \cdot \rangle$ на кольцо целых чисел $\langle Z_1, +, \cdot \rangle$.

5. Для доказательства изоморфизма соответствующих упорядоченных колец целых чисел $\langle Z, +, \cdot, < \rangle$ и $\langle Z_1, +, \cdot, < \rangle$ остается установить, что $x < y$ тогда и только тогда, когда $\varphi(x) < \varphi(y)$.

Предварительно докажем, что $f(N) = N_1$. Для любого $n \in N$ имеем: $f(n) = f((n + 1) - 1) = \varphi(n + 1) - \varphi(1) = \varphi(n) + \varphi(1) - \varphi(1) = \varphi(n) \in N_1$. Пользуясь тем, что φ — отображение на N_1, получаем $f(N) = N_1$.

По определению отношения «меньше» (3.3.12) для целых чисел x и y имеем $x < y$ тогда и только тогда, когда $y - x \in N$, что по доказанному эквивалентно включению $f(y - x) \in N_1$. Но $f(y - x) = f(y) - f(x)$. Итак, $x < y$ тогда и только тогда, когда $f(y) - f(x) \in N_1$, что означает $f(x) < f(y)$. □

Системы с основным множеством целых чисел

Подводя итог, перечислим упоминавшиеся выше числовые системы с основным множеством Z:

1) $\langle Z, + \rangle$ — аддитивная группа целых чисел;
2) $\langle Z, \cdot \rangle$ — мультипликативная полугруппа целых чисел;
3) $\langle Z, +, \cdot \rangle$ — кольцо целых чисел;
4) $\langle Z, < \rangle$ — линейно упорядоченное множество целых чисел;
5) $\langle Z, +, \cdot, <; \rangle$ — упорядоченное кольцо целых чисел.

Сравните эти числовые системы с соответствующими системами с основным множеством натуральных чисел N и отметьте их новые свойства.

Тема 4
РАЦИОНАЛЬНЫЕ ЧИСЛА

§ 1. Определение системы рациональных чисел

Формирование определения

Рациональные числа мы представляем себе в виде объединения множества целых чисел и множества дробей, т. е. отношений целых чисел. Но тут же замечаем, что всякое целое число можно рассматривать как отношение со знаменателем 1. Таким образом, множество рациональных чисел в нашем понимании есть множество всех отношений целых чисел. Рациональные числа можно складывать и перемножать, причем эти операции обладают теми же свойствами, что и для целых чисел, т. е. свойствами, характеризующими область целостности. Кроме того, для всякого рационального числа, отличного от нуля, существует обратное рациональное число. Это новое для области целостности свойство превращает ее в поле. Приведем определение этого понятия.

4.1.1. Определение. Система $\langle P, +, \cdot \rangle$ называется *полем*, если выполнены следующие условия.

1. Система $\langle P, + \rangle$ — коммутативная группа (она называется *аддитивной группой поля*), т. е.:

a) сложение + ассоциативно и коммутативно;

b) существует элемент $0 \in P$, называемый *нулем*, такой что для любого $a \in P$ имеем $a + 0 = a$;

c) для всякого элемента $a \in P$ существует *противоположный* элемент $-a \in P$ такой, что $a + (-a) = 0$.

2. Если $P^* = P \setminus \{0\}$, то $\langle P^*, \cdot \rangle$ — коммутативная группа (она называется *мультипликативной группой поля*), т. е.:

a) умножение ассоциативно и коммутативно;

b) существует элемент $e \in P^*$, называемый *единицей*, такой что для любого $a \in P^*$ имеем $a \cdot e = a$;

c) для всякого $a \in P^*$ существует *обратный* элемент a^{-1} такой, что $a \cdot a^{-1} = e$.

3. Умножение дистрибутивно относительно сложения.

Непосредственно из определения вытекает, что в поле нуль не равен единице. Используя понятие кольца, можно сказать, что поле — это коммутативное кольцо с единицей, не равной нулю, в котором для всякого ненулевого элемента есть обратный.

4.1.2. Определение. Пусть $\langle P,+,\cdot\rangle$ — поле, $a,b\in P$ и $b\neq 0$. Элемент $a\cdot b^{-1}$ называется *отношением* элементов a и b и записывается в виде $\frac{a}{b}$.

Дадим определение системы рациональных чисел, отражающее наше представление о ней.

4.1.3. Определение. *Системой рациональных чисел* называется поле $\langle Q,+,\cdot\rangle$, удовлетворяющее следующим условиям:

1) оно содержит кольцо целых чисел $\langle Z,+,\cdot\rangle$;

2) всякий элемент из Q представим в виде отношения целых чисел, т. е. для любого $q\in Q$ существуют $a,b\in Z$ такие, что $b\neq 0$ и $q=\frac{a}{b}$.

Всякий элемент из Q называется *рациональным числом*, а система $\langle Q,+,\cdot\rangle$ называется *полем рациональных чисел*.

4.1.4. Теорема. *Изоморфный образ поля рациональных чисел есть поле рациональных чисел.*

Доказательство. Утверждение вытекает из того, что изоморфный образ поля есть поле, а изоморфный образ кольца целых чисел есть кольцо целых чисел. □

Поле рациональных чисел как расширение кольца целых чисел

Рациональные числа появляются в связи с решением следующей задачи. В кольце целых чисел уравнение $ax=b$ не всегда разрешимо. Требуется найти минимальную область целостности, которая содержала бы кольцо целых чисел и в которой было бы разрешимо названное уравнение для любых $a\neq 0$ и b. Нетрудно сообразить, что область целостности, в которой для любых $a\neq 0$ и b разрешимо уравнение $ax=b$, является полем. Поэтому нужно найти минимальное поле, содержащее кольцо целых чисел. Докажем, что таким минимальным полем как раз и является поле рациональных чисел. Но сначала напомним определение подполя.

4.1.5. Определение. *Подполем* поля $\langle P,+,\cdot\rangle$ называется подмножество $H\subseteq P$, удовлетворяющее следующим условиям:

1) H замкнуто относительно сложения и умножения, т. е. если $a,b\in H$, то $a+b\in H$ и $a\cdot b\in H$;

2) нуль и единица поля принадлежат H;

3) если $a\in H$, то $-a\in H$, и если, кроме того, $a\neq 0$, то $a^{-1}\in H$.

4.1.6. Теорема. *Система $\langle P,+,\cdot\rangle$ есть система рациональных чисел тогда и только тогда, когда она является минимальным полем, содержащим кольцо целых чисел.*

Доказательство. ($\Rightarrow$) По определению 4.1.3, система рациональных чисел $\langle Q,+,\cdot\rangle$ есть поле, содержащее кольцо целых чисел $\langle Z,+,\cdot\rangle$. Докажем свойство минимальности. Пусть H — подполе поля $\langle Q,+,\cdot\rangle$ и $Z\subseteq H$. Докажем, что $H=Q$. По определению, всякий элемент $q\in Q$ представим в виде $q=\frac{a}{b}$, где $a,b\in Z$, $b\neq 0$. Поскольку $Z\subseteq H$, то, по определению подполя, $a,b^{-1}\in H$, откуда $q=\frac{a}{b}=a\cdot b^{-1}\in H$. Следовательно, $H=Q$.

($\Leftarrow$) Пусть система $\langle P,+,\cdot\rangle$ является минимальным полем, содержащим кольцо целых чисел $\langle Z,+,\cdot\rangle$. Обозначим $H=\left\{\frac{a}{b}\,|\,a,b\in Z,b\neq 0\right\}$. Легко видеть, что H является подполем, содержащим кольцо целых чисел, и по свойству минимальности $H=Q$. Следовательно, всякий элемент из P представим в виде отношения целых чисел и, в соответствии с определением 4.1.3, $\langle P,+,\cdot\rangle$ является системой рациональных чисел. □

Доказанная теорема позволяет определить систему рациональных чисел как *минимальное поле, содержащее кольцо целых чисел.*

§ 2. Существование системы рациональных чисел

Вводные соображения

Исходя из существования системы целых чисел, построим систему рациональных чисел и тем самым докажем непротиворечивость аксиоматической теории рациональных чисел (относительно теории целых чисел). Уже само определение системы рациональных чисел подсказывает нам мысль «смоделировать» рациональное число $\frac{a}{b}$ в виде упорядоченной пары целых чисел (a,b). При этом мы используем идею, хорошо зарекомендовавшую себя при построении системы целых чисел. Так как мы пойдем путем, проторенным в предыдущей главе (см. п. 2 § 2 гл. 2), то дальнейшее изложение будет более кратким. Впрочем, пропущенные доказательства легко восстанавливаются и представляют собой несложные, но весьма полезные упражнения.

Построение поля рациональных чисел

Рассмотрим множество $Q_0=\{(a,b)\,|\,a,b\in Z,b\neq 0\}$ и определим на нем отношение $\sim$, положив $(a,b)\sim(a_1,b_1)$ тогда и только тогда, когда $ab_1=a_1b$. Такое определение отношения $\sim$ мотивируется тем, что в поле рациональных чисел равенство $\frac{a}{b}=\frac{a_1}{b_1}$ имеет место тогда и только тогда, когда $ab_1=a_1b$. Легко доказать, что отношение $\sim$ является отношением эквивалентности на множестве Q_0. По этому отношению множество Q_0 распадается на классы эквивалентных пар. Класс пар, содержащий пару (a,b), будем обозначать через $\overline{(a,b)}$. Этот класс «моделирует» рациональное число $\frac{a}{b}$. Отметим, что $\overline{(a,b)}=\overline{(a_1,b_1)}$ тогда и только тогда, когда $ab_1=a_1b$.

Множество всех классов эквивалентных пар обозначим через $\overline{Q}$. На этом множестве определим операции сложения $\oplus$ и умножения $\otimes$, положив

$$\overline{(a,b)}\oplus\overline{(c,d)}=\overline{(ad+bc,bd)},\ \overline{(a,b)}\otimes\overline{(c,d)}=\overline{(ac,bd)}.$$

Эти определения подсказаны равенствами: $\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$, $\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}$.

Проверьте, что сложение и умножение классов эквивалентных пар не зависят от выбора пар — представителей классов.

4.2.1. Теорема. *Система* $\langle \overline{Q}, \oplus, \otimes \rangle$ *является системой рациональных чисел.*

Доказательство. Наметим лишь план доказательства, реализацию которого оставляем читателю.

1. Система $\langle \overline{Q}, \oplus, \otimes \rangle$ — поле. Для доказательства этого надо установить следующее:

1) $\langle \overline{Q}, \oplus \rangle$ — коммутативная группа, т. е.:

a) сложение $\oplus$ ассоциативно и коммутативно, что проверяется непосредственно с использованием соответствующих свойств сложения целых чисел,

b) класс $\overline{0}=\overline{(0,1)}$ является нулевым элементом,

c) $-\overline{(a,b)}=\overline{(-a,b)}$;

2) обозначим $\overline{Q}^*=\overline{Q}\setminus\{\overline{0}\}$. Тогда $\langle \overline{Q}^*, \otimes \rangle$ — коммутативная группа, т. е.:

a) умножение $\otimes$ ассоциативно и коммутативно, что проверяется непосредственно,

b) класс $\overline{1}=\overline{(1,1)}$ является единичным элементом,

c) если $\overline{(a,b)}\neq\overline{0}$, то $\overline{(a,b)}^{-1}=\overline{(b,a)}$;

3) умножение дистрибутивно относительно сложения, что проверяется непосредственным подсчетом левой и правой частей соответствующего равенства.

2. Обозначим $\overline{Z}=\{\overline{(a,1)}\mid a\in Z\}$. Легко доказать, что отображение $\varphi: Z\to\overline{Z}$, при котором $\varphi(a)=\overline{(a,1)}$ для любого $a\in Z$, является изоморфизмом кольца целых чисел $\langle Z,+,\cdot\rangle$ на систему $\langle \overline{Z}, \oplus, \otimes \rangle$, в силу чего последняя также является кольцом целых чисел.

3. Наконец, для любого $\overline{(a,b)}\in\overline{Z}$ имеем: $\overline{(a,b)}=\overline{(a,1)}\otimes\overline{(b,1)}^{-1}$. □

Заметим, что почти дословным повторением этого доказательства устанавливается существование поля частных для произвольной области целостности, т. е. минимального поля, содержащего данную область целостности.

§ 3. Основные свойства системы рациональных чисел

Основные свойства полей

По определению система рациональных чисел является полем, поэтому свойства полей являются также свойствами рациональных чисел. Рассмотрим основные свойства поля.

4.3.1. Теорема. *Пусть дано поле* $\langle P,+,\cdot\rangle$ *с нулем* 0 *и единицей e. Для любых элементов* $a,b,c,d\in P$:

1) если $ab=e$, то $a\neq 0$ и $b=a^{-1}$;

2) (отсутствие делителей нуля) если $ab=0$, то $a=0$ или $b=0$;

3) (свойство сократимости для умножения) если $ac = bc$ и $c \neq 0$, то $a = b$;

4) $\frac{a}{b} = \frac{c}{d}$ тогда и только тогда, когда $ad = bc$;

5) $\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd}$;

6) $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$;

7) $-\frac{a}{b} = \frac{-a}{b}$;

8) если $a \neq 0$, то $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$;

9) (основное свойство дроби) $\frac{ac}{bc} = \frac{a}{b}$.

Доказательство. 1. Пусть $ab = e$. Если предположить, что $a = 0$, то получим $e = ab = 0 \cdot b = 0$ — пришли к противоречию. Следовательно, $a \neq 0$ и существует элемент a^{-1}. Умножив равенство $ab = e$ на a^{-1}, получим $b = a^{-1}$.

2. Пусть $ab = 0$. Если $a = 0$, то доказывать нечего. Если же $a \neq 0$, то существует элемент a^{-1}. Умножив равенство $ab = 0$ на a^{-1}, получим $b = 0$.

3. Доказательство свойства сводится к умножению данного равенства на c^{-1}.

4. Пусть $\frac{a}{b} = \frac{c}{d}$, тогда $ab^{-1} = cd^{-1}$. Умножив обе части равенства на bd, получим $ad = bc$. Обратное утверждение получаем теми же рассуждениями в обратном порядке.

Доказательство остальных свойств отношений предоставляется читателю. □

Упорядоченное поле рациональных чисел

Введем отношение «меньше» для рациональных чисел с помощью отношения «меньше» для целых чисел. При этом будем считать, что для любого рационального числа $\frac{a}{b}$ знаменатель $b > 0$.

Для любых $\frac{a}{b}, \frac{c}{d} \in Q$ положим $\frac{a}{b} < \frac{c}{d}$ тогда и только тогда, когда $ad < bc$.

Легко доказать, что система $\langle Q, < \rangle$ является линейно упорядоченным множеством. Кроме того, как и для целых чисел, операции сложения и умножения монотонны. Введем общее понятие, частным случаем которого является система $\langle Q, +, \cdot, < \rangle$.

4.3.2. Определение. *Упорядоченным полем* называется система $\langle P, +, \cdot, < \rangle$, удовлетворяющая следующим условиям:

1) $\langle P, +, \cdot \rangle$ — поле;

2) $\langle P, < \rangle$ — линейно упорядоченное множество;

3) для любых $x, y, z \in P$ если $x < y$, то $x + z < y + z$ (*монотонность сложения*), и если $x < y$, $z > 0$, то $xz < yz$ (*монотонность умножения*).

Таким образом, система $\langle Q,+,\cdot,<\rangle$ является упорядоченным полем, которое называется *упорядоченным полем рациональных чисел.*

Рассмотрим произвольное упорядоченное поле $\langle P,+,\cdot,<\rangle$ и его единицу обозначим через 1. Проведем следующие не вполне строгие рассуждения. Поскольку P замкнуто относительно сложения, последовательно получаем: $2=1+1\in P$, $3=2+1\in P$, ... Поскольку $1>0$, то $2>0$, $3>0$, ... Таким образом, мы получаем, что все новые и новые натуральные числа принадлежат P. В итоге убеждаемся, что $N\subseteq P$. Но поле вместе с каждым своим элементом содержит ему противоположный, следовательно, $-N\subseteq P$. Итак, $Z=N\cup\{0\}\cup -N\subseteq P$. Но в поле из того, что $m,n\in Z\subseteq P$ и $n\neq 0$, следует, что $m,n^{-1}\in P$, откуда $\frac{m}{n}=m\cdot n^{-1}\in P$. Таким образом, $Q=\left\{\frac{m}{n}\,|\,m,n\in Z,n\neq 0\right\}\subseteq P$, т. е. всякое упорядоченное поле содержит упорядоченное поле рациональных чисел (образно говоря, ухватившись за единицу, мы втянули в P все множество Q). Докажем это утверждение в более строгом виде.

4.3.3. Теорема. *Всякое упорядоченное поле содержит упорядоченное подполе, изоморфное упорядоченному полю рациональных чисел.*

Доказательство. Пусть дано упорядоченное поле $\langle P,+,\cdot,<\rangle$ с единицей e. Обозначим $Q_1=\left\{\frac{me}{ne}\,|\,m,n\in Z,n\neq 0\right\}$ и определим отображение $\varphi: Q\to Q_1$, положив $\varphi\left(\frac{m}{n}\right)=\frac{me}{ne}$ для любого $\frac{m}{n}\in Q$. Докажем, что φ является изоморфизмом $\langle Q,+,\cdot,<\rangle$ на $\langle Q_1,+,\cdot,<\rangle$.

1. φ — взаимно однозначное отображение. Пусть $\varphi\left(\frac{m}{n}\right)=\varphi\left(\frac{m_1}{n_1}\right)$, докажем, что $\frac{m}{n}=\frac{m_1}{n_1}$. Из условия $\varphi\left(\frac{m}{n}\right)=\varphi\left(\frac{m_1}{n_1}\right)$ получаем $\frac{me}{ne}=\frac{m_1e}{n_1e}$, откуда $me\cdot n_1e=m_1e\cdot ne$ и $mn_1e=m_1ne$. Предположим, что $mn_1\neq m_1n$, пусть, например, $mn_1<m_1n$. Тогда $m_1n-mn_1>0$, т. е. $m_1n-mn_1\in N$ и $(m_1n-mn_1)e=0$. Но в 3.3.15 доказано, что в упорядоченном кольце, а значит и в упорядоченном поле, для любого натурального числа k имеем $ke>0$ — пришли к противоречию. Следовательно, $mn_1=m_1n$, откуда $\frac{m}{n}=\frac{m_1}{n_1}$.

2. Очевидно, φ — отображение на Q_1.

3. Докажем, что φ сохраняет операции сложения и умножения, а также отношение «меньше». Для любых $\frac{m}{n},\frac{m_1}{n_1}\in Q$ имеем:

$$\varphi\left(\frac{m}{n}+\frac{m_1}{n_1}\right)=\varphi\left(\frac{mn_1+m_1n}{nn_1}\right)=\frac{(mn_1+m_1n)e}{(nn_1)e}=$$

$$=\frac{me\cdot n_1e+m_1e\cdot ne}{ne\cdot n_1e}=\frac{me}{ne}+\frac{m_1e}{n_1e}=\varphi\left(\frac{m}{n}\right)+\varphi\left(\frac{m_1}{n_1}\right).$$

Для умножения — аналогично. Наконец, φ сохраняет отношение «меньше», так как $\frac{m}{n}<\frac{m_1}{n_1}$ при $n>0$, $n_1>0$ тогда и только тогда, когда $m\cdot n_1<m_1\cdot n$. Но это равносильно $m_1\cdot n-m\cdot n_1\in N$, и по 3.3.15, $(m_1\cdot n-m\cdot n_1)e>0$, откуда $me\cdot n_1e<m_1e\cdot ne$ и $\frac{me}{ne}<\frac{m_1e}{n_1e}$, что означает $\varphi\left(\frac{m}{n}\right)<\varphi\left(\frac{m_1}{n_1}\right)$. □

Нетрудно видеть, что изоморфный образ упорядоченного поля рациональных чисел есть упорядоченное поле рациональных чисел, поэтому из доказанной теоремы получаем следующую краткую характеризацию этой числовой системы.

4.3.4. Следствие. *Система $\langle P,+,\cdot,<\rangle$ есть упорядоченное поле рациональных чисел тогда и только тогда, когда она является минимальным упорядоченным полем.*

Если между целыми числами n и $n+1$ нет ни одного целого числа, то между любыми двумя различными рациональными числами можно найти новое рациональное число. Отметим это свойство в наиболее общем виде.

4.3.5. Предложение. *Во всяком упорядоченном поле $\langle P,+,\cdot,<\rangle$ для любых элементов $a,b\in P$, где $a<b$, существует элемент $c\in P$ такой, что $a<c<b$.*

Доказательство. Можно взять, например, $c=\frac{a+b}{2}\in P$.

4.3.6. Теорема. *Упорядоченное поле рациональных чисел удовлетворяет аксиоме Архимеда: для любого положительного $a\in Q$ и любого $b\in Q$ существует натуральное число n такое, что $na>b$.*

Доказательство. Пусть $a=\frac{m}{k}$, где $k,m\in N$, и $b=\frac{p}{q}$, где $p\in Z$, $q\in N$. По аксиоме Архимеда для целых чисел, для целого числа $mq>0$ и целого числа kp существует натуральное число n такое, что $nmq>kp$. Пользуясь монотонностью умножения, разделим это неравенство на $kq>0$. Получим $n\frac{m}{k}>\frac{p}{q}$, т. е. $na>b$. □

Изоморфизм (упорядоченных) полей рациональных чисел

4.3.7. Теорема. *Любые два (упорядоченных) поля рациональных чисел изоморфны.*

Доказательство. Пусть дано поле рациональных чисел $\langle Q,+,\cdot\rangle$, содержащее кольцо целых чисел $\langle Z,+,\cdot\rangle$, и другое поле рациональных чисел $\langle Q_1,\oplus,\otimes\rangle$, содержащее кольцо целых чисел $\langle Z_1,\oplus,\otimes\rangle$. По 3.3.23, существует изоморфизм φ кольца $\langle Z,+,\cdot\rangle$ на кольцо $\langle Z_1,\oplus,\otimes\rangle$. Используя φ, определим отображение $f:Q\to Q_1$, положив $f\left(\frac{a}{b}\right)=\frac{\varphi(a)}{\varphi(b)}$ для лю-

бого числа $\frac{a}{b} \in Q$. Легко доказать, что отображение f является искомым изоморфизмом поля $\langle Q, +, \cdot \rangle$ на поле $\langle Q_1, \oplus, \otimes \rangle$, причем $f(Z) = Z_1$. Но тогда для упорядоченных полей рациональных чисел $\langle Q, +, \cdot, < \rangle$ и $\langle Q_1, \oplus, \otimes, \lhd \rangle$ нетрудно доказать, что для $\frac{a}{b}, \frac{c}{d} \in Q$ имеем $\frac{a}{b} < \frac{c}{d}$ тогда и только тогда, когда $f\left(\frac{a}{b}\right) \lhd f\left(\frac{c}{d}\right)$, т. е. f является изоморфизмом $\langle Q, +, \cdot, < \rangle$ на $\langle Q_1, \oplus, \otimes, \lhd \rangle$. □

Системы с основным множеством рациональных чисел

Перечислим основные числовые системы, связанные с множеством рациональных чисел:

1) $\langle Q, + \rangle$ — аддитивная группа рациональных чисел;

2) $\langle Q^*, \cdot \rangle$ — мультипликативная группа рациональных чисел, отличных от нуля;

3) $\langle Q, +, \cdot \rangle$ — поле рациональных чисел;

4) $\langle Q, < \rangle$ — линейно упорядоченное множество рациональных чисел;

5) $\langle Q, +, \cdot, < \rangle$ — упорядоченное поле рациональных чисел.

Сравните эти системы с соответствующими системами с основным множеством целых чисел и отметьте новые свойства.

§ 4. Представление рациональных чисел десятичными дробями

Десятичные дроби

Хорошо известно, что, например, дробь $\frac{28}{23}$ можно записать в виде десятичной дроби, стоит только числитель «уголком» разделить на знаменатель. Точно так же можно поступить с любым рациональным числом. Наша задача — установить этот факт, используя уже доказанные свойства рациональных чисел. При этом мы уточним понятие десятичной дроби и понятие представимости числа десятичной дробью.

4.4.1. Определение. *Десятичной дробью* называется последовательность целых чисел $a_0, a_1, a_2, \ldots$, где $a_1, a_2, \ldots$ — цифры десятичной системы счисления (см. 3.3.20), которая записывается в виде $a_0, a_1 a_2 \ldots$ (читается: a_0 целых, a_1, a_2 и т. д), причем цифра 9 не повторяется бесконечное число раз подряд, т. е. для любого номера m существует номер $k > m$ такой, что $a_k \neq 9$. Целое число a_0 называется *целой частью десятичной дроби* и записывается в десятичной системе счисления.

Образно говоря, десятичная дробь по определению не имеет «хвоста» из девяток. Только при этом условии нам удастся доказать един-

ственность представления десятичной дробью всякого рационального, а затем и всякого действительного числа. (Устраняется неоднозначность типа $1 = 1{,}000\ldots$ и $1 = 0{,}999\ldots$.)

Приведем примеры десятичных дробей: $3{,}035\ldots$ (читается: три целых, ноль, три, пять и т. д); $7{,}00\ldots$ (читается: семь целых, ноль, ноль и т. д). Если целая часть десятичной дроби отрицательна, то знак «минус» будем писать над первой цифрой целой части. Например, $\overline{1}23{,}0101\ldots$ (читается: сто двадцать три целых с минусом, ноль, один, ноль, один и т. д).

4.4.2. Определение. Две десятичные дроби *равны*, $a_0,a_1a_2\ldots = b_0,b_1b_2\ldots$, тогда и только тогда, когда $a_i = b_i$ для любого $i = 0,1,2,\ldots$.

4.4.3. Определение. Десятичная дробь называется *периодической*, если существуют m и k такие, что для любого $i = 1,2,\ldots$ выполняется равенство $a_{m+k+i} = a_{m+i}$. Наименьшее m называется *количеством цифр до периода*, а наименьшее k — *количеством цифр в периоде*. При этом повторяющаяся группа цифр $a_{m+1}a_{m+2}\ldots a_{m+k}$ называется *периодом*, а сама дробь записывается в виде $a_0,a_1a_2\ldots a_m(a_{m+1}a_{m+2}\ldots a_{m+k})$.

Например, $28{,}4370505\ldots = 28{,}437(05)$ (читается: 28 целых, 4, 3, 7 и 0, 5 в периоде). Эта десятичная дробь содержит три цифры до периода и две цифры в периоде.

Уточним понятие представимости числа десятичной дробью, причем сделаем это в наиболее общей форме для элементов произвольного упорядоченного поля. Это позволит нам впоследствии использовать введенное понятие и для действительных чисел. При этом мы считаем, ввиду 4.3.4, что всякое упорядоченное поле содержит упорядоченное поле рациональных чисел.

4.4.4. Определение. Пусть дано упорядоченное поле $\langle P,+,\cdot,<\rangle$. Будем говорить, что элемент $a \in P$ *представим в виде десятичной дроби* $a_0,a_1a_2\ldots$, если для любого номера $n = 0,1,2,\ldots$ выполняются неравенства

$$a_0 + \frac{a_1}{10} + \ldots + \frac{a_n}{10^n} \le a < a_0 + \frac{a_1}{10} + \ldots + \frac{a_n}{10^n} + \frac{1}{10^n}.$$

Рациональные числа $A_n = a_0 + \frac{a_1}{10} + \ldots + \frac{a_n}{10^n}$ и $A'_n = A_n + \frac{1}{10^n}$ называются *приближенными значениями* элемента a соответственно по недостатку и по избытку (с точностью до $\frac{1}{10^n}$).

Способ представления рационального числа десятичной дробью

Пусть дана положительная правильная дробь $\frac{a}{b}$. Рассмотрим в общем виде деление «уголком» натурального числа a на натуральное число $b > a$.

$$
\begin{array}{l|l}
a & b \\
\hline
0, &
\end{array}
\qquad
\begin{array}{l|ll}
\_10a & b & \\
\hline
bc_1 & 0, & c_1 \\
r_1 & &
\end{array}
\qquad
\begin{array}{l|ll}
\_10a & b & \\
\hline
bc_1 & 0, & c_1c_2 \\
\_10r_1 & & \\
\hline
bc_2 & & \\
r_2 & &
\end{array}
$$

Поскольку $a<b$, то в частном ставим «ноль целых» и делимое увеличиваем в 10 раз. После этого $10a$ делим на b с остатком: берем по c_1 и в остатке получаем r_1. Затем, остаток r_1 увеличиваем в 10 раз и делим на b с остатком: берем по c_2 и в остатке получаем r_2. И дальше повторяется то же самое. Зафиксируем в виде определения этот процесс деления уголком.

4.4.5. Определение. *Алгоритм деления «уголком»* натурального числа a на натуральное число $b>a$ состоит в следующем.

1 (начало алгоритма). Делимое a увеличиваем в 10 раз и делим на b с остатком.

2 (шаг алгоритма). Остаток увеличиваем в 10 раз и делим на b с остатком.

В результате получаем последовательность неполных частных $0, c_1, c_1, \ldots$.

4.4.6. Теорема. *Всякое рациональное число представимо в виде периодической десятичной дроби.*

Доказательство. Произвольное рациональное число q можно представить в виде $q=c_0+\frac{a}{b}$, где a, b, c_0 — целые числа, причем $0\le a<b$. Поэтому задача сводится к представлению в виде десятичной дроби положительной правильной дроби $\frac{a}{b}$.

Запишем шаги алгоритма деления «уголком» числа a на число b:

$$
\begin{aligned}
&10a = bc_1 + r_1, \quad 0\le r_1<b;\\
&10r_1 = bc_2 + r_2, \quad 0\le r_2<b;\\
&\ldots\ldots\ldots\ldots \quad \ldots\ldots\ldots\ldots\\
&10r_{n-1} = bc_n + r_n, \quad 0\le r_n<b;\\
&10r_n = bc_{n+1} + r_{n+1}, \quad 0\le r_{n+1}<b;\\
&\ldots\ldots\ldots\ldots \quad \ldots\ldots\ldots\ldots
\end{aligned}
\qquad (1)
$$

Наша задача состоит в том, чтобы доказать, что в результате этого алгоритма получается периодическая десятичная дробь $0,c_1c_2\ldots$, которая является представлением числа $\frac{a}{b}$ в точном соответствии с определением этого понятия (см. 4.4.4).

1. Индукцией по n докажем равенство

$$\frac{a}{b}=\frac{c_1}{10}+\ldots+\frac{c_n}{10^n}+\frac{r_n}{10^n b}. \qquad (2)$$

Разделив обе части первого равенства из (1) на $10b$, получим $\frac{a}{b}=\frac{c_1}{10}+\frac{r_1}{10b}$, т. е. при $n = 1$ равенство (2) верно.

Пусть для натурального числа n равенство (2) верно. Разделив обе части $(n + 1)$-го равенства из (1) на $10^{n+1}b$, будем иметь: $\frac{r_n}{10^n b}=$ $=\frac{c_{n+1}}{10^{n+1}}+\frac{r_{n+1}}{10^{n+1}b}$. Отсюда, используя индуктивное предположение, получаем:

$$\frac{a}{b}=\frac{c_1}{10}+\ldots+\frac{c_n}{10^n}+\frac{r_n}{10^n b}=\frac{c_1}{10}+\ldots+\frac{c_n}{10^n}+\frac{c_{n+1}}{10^{n+1}}+\frac{r_{n+1}}{10^{n+1}b}.$$

Итак, равенство (2) доказано.

2. Для любого n имеют место неравенства

$$\frac{c_1}{10}+\ldots+\frac{c_n}{10^n}\le\frac{a}{b}<\frac{c_1}{10}+\ldots+\frac{c_n}{10^n}+\frac{1}{10^n}.$$

Эти неравенства непосредственно вытекают из (2), достаточно лишь заметить, что из $0\le r_n<b$ следует, что $\frac{r_n}{10^n b}<\frac{1}{10^n}$.

3. Докажем, что последовательность неполных частных $0, c_1, c_2, \ldots$ из (1), записанная в виде $0,c_1c_2\ldots$, является десятичной дробью. Для этого нужно доказать, что $c_1, c_2, \ldots$ — цифры и в записи $0,c_1c_2\ldots$ нет «хвоста» из девяток.

Из первого равенства в (1) получаем $c_1=\frac{10a-r_1}{b}$, откуда $0\le c_1<10$, т. е. c_1 — цифра. Аналогично, рассматривая n-е равенство из (1), убеждаемся, что c_n — цифра.

Докажем, что в записи $0,c_1c_2\ldots$ девятка не может повторяться бесконечное число раз подряд. Предположим противное, пусть последовательность цифр имеет вид $0,c_1c_2,\ldots c_m99\ldots$. Обозначим $C_m=\frac{c_1}{10}+\ldots+\frac{c_m}{10^m}$. По (2) для любого $i = 1, 2, \ldots$

$$C_m+\frac{9}{10^{m+1}}+\ldots+\frac{9}{10^{m+i}}\le\frac{a}{b}<C_m+\frac{9}{10^{m+1}}+\ldots+\frac{9}{10^{m+i}}+\frac{1}{10^{m+i}}=C_m+\frac{1}{10^m}.$$

Отсюда $0<C_m+\frac{1}{10^m}-\frac{a}{b}\le\frac{1}{10^{m+i}}$, т. е. $10^{m+i}\left(C_m+\frac{1}{10^m}-\frac{a}{b}\right)\le1$ для любого натурального числа i, что противоречит аксиоме Архимеда для рациональных чисел. Итак, $0,c_1c_2\ldots$ является десятичной дробью.

4. Число $\frac{a}{b}$ представимо в виде десятичной дроби $0,c_1c_2\ldots$, что вытекает из (2). Но тогда данное рациональное число q представимо в виде десятичной дроби $c_0,c_1c_2\ldots$.

5. Докажем, что дробь $c_0,c_1c_2\ldots$ периодическая. Обратимся к соотношениям (1). Поскольку $0 \le r_n < b$ для любого n, все остатки r_n не могут быть различными. Следовательно, при делении a на b «уголком» на некотором шаге мы получим остаток, который ранее уже встречался. Но тогда, начиная с этого момента, цифры частного также будут повторяться, и мы получим период. □

Тема 5
ДЕЙСТВИТЕЛЬНЫЕ ЧИСЛА

§ 1. Определение системы действительных чисел

Формирование определения

Подыскивая определение системы действительных чисел, прежде всего отметим, что действительные числа, как и рациональные, можно складывать и перемножать, а также сравнивать, используя отношение «меньше», причем выполняются те же свойства, что и для рациональных чисел. Короче говоря, систему действительных чисел следует определить как некоторое упорядоченное поле $\langle R, +, \cdot, < \rangle$. Далее, как известно, действительные числа можно изображать точками числовой прямой. Числовая прямая — это прямая, на которой выбраны начало отсчета, положительное направление и единичный отрезок. Поэтому числовое множество R должно обладать теми же свойствами, что и множество точек прямой.

Характерным свойством прямой является ее непрерывность, которая понимается нами как возможность начертить прямую, не отрывая карандаша от бумаги. Мы легко можем представить, что если из прямой удалить одну точку, то образовавшийся пробел лишает ее непрерывности: такую прямую уже не начертишь, не отрывая карандаша от бумаги. Сформулируем требования, которые заставили бы нас вернуть на прямую удаленную точку и тем самым восстановить ее непрерывность. Эти требования дадут нам аксиомы непрерывности системы действительных чисел.

Пусть мы удалили из прямой точку B, расположенную правее начальной точки 0. Нам надо обнаружить этот пробел и устранить его. Сначала сформулируем требование, позволяющее нам дойти до пробела и перешагнуть через него, шагая по прямой от точки 0 шагами произвольной длины a. Требование, которое позволило бы нам преодолеть любое расстояние b (до точки B), можно сформулировать следующим образом (рис. 11).

Для любого положительного $a \in R$ (a — длина шага) и любого $b \in R$ (b — предложенное расстояние) существует натуральное число n (n — число шагов) такое, что $na > b$. Замечаем, что высказанное требование — это знакомая нам аксиома Архимеда, сформулированная для элементов множества R.

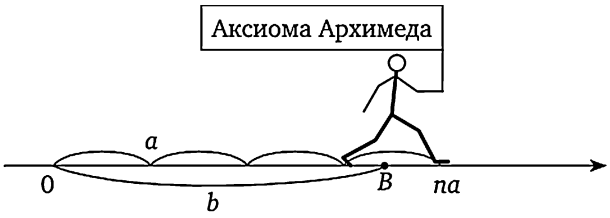

Рис. 11

Итак, пользуясь аксиомой Архимеда, мы можем дойти до пробела и перешагнуть через него. Другими словами, найти отрезок $[X_0, Y_0]$, содержащий этот пробел. Разделим этот отрезок пополам и через $[X_1, Y_1]$ обозначим ту половину, которая содержит пробел. Полученный отрезок снова разделим пополам и через $[X_2, Y_2]$ обозначим ту половину, которая содержит пробел, и т. д. Продолжая этот процесс, мы получим последовательность вложенных один в другой отрезков $[X_0, Y_0], [X_1, Y_1], [X_2, Y_2], \ldots$, каждый из которых содержит пробел, образовавшийся в результате удаления точки B. Причем, если предположить, что кроме удаленной точки B еще некоторая точка C принадлежит всем отрезкам последовательности, то и весь отрезок BC содержался бы в каждом из построенных отрезков. Но это невозможно, так как длины отрезков неограниченно убывают. Таким образом, удаленная точка — это единственная точка прямой, которая принадлежала всем отрезкам построенной последовательности. Требование, которое заставило бы нас вернуть на прямую удаленную точку и восстановить ее непрерывность, можно сформулировать так: для любой последовательности вложенных отрезков должна существовать точка, принадлежащая всем отрезкам последовательности (рис. 12).

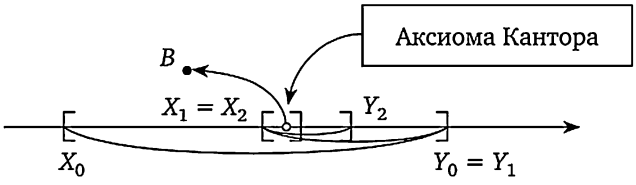

Рис. 12

Это требование называется аксиомой Кантора. Заменяя в нем точки соответствующими числами, мы получим аксиому Кантора, сформулированную на языке чисел множества R.

Подводя итог, можно сказать, что аксиома Архимеда позволяет нам дойти до пробела и построить последовательность вложенных отрезков, содержащих пробел, а аксиома Кантора требует устранения этого пробела. Таким образом, систему действительных чисел целесообразно определить как упорядоченное поле, в котором выполняются аксиома Архимеда и аксиома Кантора.

Уточним понятия, используемые в этом определении.

5.1.1. Определение. Пусть дано линейно упорядоченное множество $\langle P, < \rangle$, $a, b \in P$ и $a \le b$. *Отрезком* называется множество $[a, b] = \{x \in P \mid a \le x \le b\}$. Элементы a и b называются *концами* этого отрезка.

5.1.2. Определение. Последовательность отрезков $([a_n, b_n])$ линейно упорядоченного множества $\langle P, < \rangle$ называется *последовательностью вложенных отрезков*, если $a_n \le a_{n+1}$, $b_{n+1} \le b_n$ для любого n.

5.1.3. Определение. Будем говорить, что в линейно упорядоченном множестве $\langle P, < \rangle$ (в упорядоченном поле $\langle P, +, \cdot, < \rangle$) выполняется *аксиома Кантора*, если для любой последовательности вложенных отрезков из P существует элемент в P, принадлежащий всем отрезкам последовательности.

Итак, приходим к следующему определению действительных чисел.

5.1.4. Определение. *Системой действительных чисел* называется упорядоченное поле $\langle R, +, \cdot, < \rangle$, в котором выполняются аксиома Архимеда и аксиома Кантора. Обе аксиомы в совокупности называются *аксиомами непрерывности* упорядоченного поля. Всякий элемент множества R называется *действительным числом*, а системы $\langle R, +, \cdot \rangle$ и $\langle R, +, \cdot, < \rangle$ называются соответственно *полем* и *упорядоченным полем действительных чисел*.

Обсуждение определения

Изложенный выше подход к определению системы действительных чисел позволяет считать, что прямая (точнее, числовая прямая) и система действительных чисел — синонимы. Переход к геометрической терминологии осуществляется простой заменой слова «число» словом «точка». Говорят, например, что точки 0 и 23 являются концами отрезка [0, 23], а его длиной является число 23, если в качестве единичного отрезка взять отрезок [0, 1]. При этой единице измерения для любых $a, b \in R$ длиной отрезка $[a, b]$ будет число $b - a$. Таким образом, действительные числа полностью обеспечивают задачу об измерении отрезков.

Из 4.3.4 вытекает, что упорядоченное поле действительных чисел содержит упорядоченное поле рациональных чисел.

5.1.5. Предложение. *В упорядоченном поле $\langle P, +, \cdot, < \rangle$ аксиома Архимеда эквивалентна каждому из следующих утверждений.*

1. *Для любого $b \in P$ существует $n \in N$ такое, что $n > b$.*
2. *Для любого положительного $a \in P$ существует $n \in N$ такое, что* $\frac{1}{n} < a$.
3. *Для любого положительного $a \in P$ и любого $b \in P$ существует $n \in N$ такое,* что $10^n a > b$.

Доказательство предоставляется читателю в качестве упражнения. □

По 4.3.7, в упорядоченном поле рациональных чисел выполняется аксиома Архимеда. Не выполняется ли в нем аксиома Кантора? Ответ дает следующая теорема.

5.1.6. Теорема. *В упорядоченном поле рациональных чисел аксиома Кантора не выполняется.*

Доказательство. Для всякого $n = 0, 1, \ldots$ рассмотрим множество целых чисел, квадраты которых не превосходят $2 \cdot 10^{2n}$, и наибольшее число в этом множестве обозначим через x_n. Тогда $a_n = \dfrac{x_n}{10^n}$ является наибольшей из дробей со знаменателем 10^n, квадраты которых не превосходят 2. Пусть $a'_n = a_n + \dfrac{1}{10^n}$.

Покажем, что последовательность отрезков $([a_n, a'_n])$ является последовательностью вложенных отрезков. В силу выбора дроби a_{n+1} для любого номера n получаем: $a_n = \dfrac{x_n}{10^n} = \dfrac{10 \cdot x_n}{10^{n+1}} \le \dfrac{x_{n+1}}{10^{n+1}} = a_{n+1}$. Покажем, что $a'_{n+1} \le a'_n$ для любого n. Предположим противное: пусть $a'_n < a'_{n+1}$ для некоторого n, т. е. $\dfrac{x_n}{10^n} + \dfrac{1}{10^n} < \dfrac{x_{n+1}}{10^{n+1}} + \dfrac{1}{10^{n+1}}$. Тогда $\dfrac{x_n + 1}{10^n} \le \dfrac{x_{n+1}}{10^{n+1}} = a_{n+1}$ и $\left(\dfrac{x_n + 1}{10^n}\right)^2 \le a_{n+1}^2 \le 2$, откуда $(x_n + 1)^2 \le 2 \cdot 10^{2n}$, что противоречит выбору числа x_n. Таким образом, $a'_{n+1} \le a'_n$ для любого n, и последовательность $([a_n, a'_n])$ является последовательностью вложенных отрезков.

Предположим, что рациональное число c принадлежит всем отрезкам этой последовательности. Известно, что не существует рационального числа, квадрат которого равен двум, поэтому либо $c^2 > 2$, либо $c^2 < 2$. Предположим, что $c^2 > 2$, и найдем натуральное число k такое, что $\left(c - \dfrac{1}{k}\right)^2 > 2$. Это неравенство равносильно неравенству $c^2 - \dfrac{2c}{k} + \dfrac{1}{k^2} > 2$, а последнее будет выполняться, если $c^2 - \dfrac{2c}{k} > 2$, что равносильно неравенству $k > \dfrac{2c}{c^2 - 2}$. По аксиоме Архимеда, существует натуральное число k, удовлетворяющее этому неравенству, а значит, и исходному неравенству $\left(c - \dfrac{1}{k}\right)^2 > 2$. Но тогда для любого n имеем $a_n^2 < 2 < \left(c - \dfrac{1}{k}\right)^2$, а так как $a_n > 0$ и $c - \dfrac{1}{k} > 0$, то $a_n < c - \dfrac{1}{k} < c \le a'_n$. Отсюда для любого n получаем: $\dfrac{1}{k} = c - \left(c - \dfrac{1}{k}\right) < a'_n - a_n = \dfrac{1}{10^n}$. Значит $k > 10^n$ для любого натурального n, что противоречит аксиоме Архимеда.

В случае $c^2 < 2$ аналогично находим натуральное число m такое, что $\left(c + \dfrac{1}{m}\right)^2 < 2$, а так как $(a'_n)^2 > 2$ для любого n, то $a_n \le c < c + \dfrac{1}{m} \le a'_n$, что снова ведет к противоречию.

Итак, для последовательности вложенных отрезков $([a_n, a'_n])$ не существует рационального числа, принадлежащего всем отрезкам этой последовательности, и аксиома Кантора для упорядоченного поля рациональных чисел не выполняется. □

Доказанная теорема, в частности, говорит о том, что $Q \ne R$.

5.1.7. Определение. Всякое действительное число, не являющееся рациональным, называется *иррациональным*.

Таким образом, множество действительных чисел представляет собой объединение множества рациональных и множества иррациональных чисел.

§ 2. Существование системы действительных чисел

Вводные соображения

Рассмотрим процесс измерения отрезков. Предположим, что нам нужно измерить отрезок OA единичным отрезком OE. Сначала находим целое число единичных отрезков OE в измеряемом отрезке OA. Если единичный отрезок OE уложился в отрезке OA целое число a_0 раз, то процесс измерения закончен и длина отрезка OA равна целому числу a_0. Если же этого не произошло, то мы единичный отрезок OE делим на 10 равных частей и находим длину отрезка OA с точностью до десятых: a_0, a_1. Если полученная десятичная дробь еще не является длиной отрезка OA, то делим единичный отрезок на 100 равных частей и находим длину с точностью до сотых: a_0, a_1a_2 и т. д. Таким образом, получаем, что действительное число, являющееся длиной отрезка OA, изображается некоторой десятичной дробью и процесс измерения обнаруживает последовательно все новые и новые ее десятичные знаки. Это подсказывает нам идею «смоделировать» действительное число в виде десятичной дроби и при конструировании системы действительных чисел в качестве основного множества взять множество S всех десятичных дробей (понятие десятичной дроби дано в определении 4.4.1). Сначала на множестве S мы определим отношение «меньше» $<$ и получим линейно упорядоченное множество $\langle S, < \rangle$. Докажем, что оно удовлетворяет аксиоме Кантора. После этого выделим в S множество конечных десятичных дробей, определим их сложение $+$ и умножение $\cdot$, а затем эти операции распространим на все множество S. Получим систему $\langle S, +, \cdot, < \rangle$, которая и будет системой действительных чисел в соответствии с определением 5.1.4. Реализуем намеченную программу.

Линейно упорядоченное множество десятичных дробей

5.2.1. Определение. Пусть даны две десятичные дроби $a_0, a_1a_2\ldots$ и $b_0, b_1b_2\ldots$. Будем считать, что первая десятичная дробь меньше второй, и писать $a_0, a_1a_2\ldots < b_0, b_1b_2\ldots$ тогда и только тогда, когда существует номер k такой, что $a_k < b_k$, а для всех номеров $i < k$ имеет место равенство $a_i = b_i$.

5.2.2. Определение. Если $\alpha, \beta \in S$, то условимся писать $\alpha \leq \beta$ тогда и только тогда, когда $\alpha < \beta$ или $\alpha = \beta$. Будем писать $\alpha > \beta$ в значении $\beta < \alpha$, и $\alpha \geq \beta$ —— в значении $\beta \leq \alpha$.

5.2.3. Теорема. *Система* $\langle S, < \rangle$ *есть линейно упорядоченное множество.*

Доказательство. Докажем, что для любых $\alpha, \beta, \gamma \in S$ из $\alpha < \beta$, $\beta < \gamma$ следует $\alpha < \gamma$. Пусть $\alpha = a_0, a_1 a_2 \ldots$, $\beta = b_0, b_1 b_2 \ldots$, $\gamma = c_0, c_1 c_2 \ldots$. По условию, $\alpha < \beta$, значит, существует номер k такой, что $a_k < b_k$, а для всех номеров $i < k$ имеет место равенство $a_i = b_i$. Аналогично $\beta < \gamma$ влечет существование номера m такого, что $b_m < c_m$, а для номеров $j < m$ имеем $b_j = c_j$. Если теперь $n = \min\{k, m\}$, то $a_n < c_n$, и для номеров $l < n$ получаем $a_l = c_l$. Значит, $\alpha < \gamma$, и свойство транзитивности доказано.

Из свойства трихотомии для целых чисел следует свойство трихотомии для десятичных дробей. □

5.2.4. Теорема. *В линейно упорядоченном множестве* $\langle S, < \rangle$ *выполняется аксиома Кантора.*

Доказательство. Пусть дана последовательность вложенных отрезков $([\alpha_n, \beta_n])$ из S. Построим десятичную дробь, принадлежащую всем отрезкам этой последовательности. Для этого рассмотрим множество M всех десятичных дробей, каждая из которых не меньше любого из левых концов данных отрезков. Целая часть любой десятичной дроби из M не меньше целой части дроби α_0, поэтому существует десятичная дробь в M с наименьшей целой частью, эту наименьшую целую часть обозначим через c_0. Пусть M_0 — множество всех десятичных дробей из M с целой частью c_0. Наименьшую из первых цифр всех десятичных дробей из M_0 обозначим через c_1 и рассмотрим множество M_1 всех десятичных дробей с целой частью c_0 и первой десятичной цифрой c_1. Продолжая описанный процесс, мы получим последовательность знаков c_0, c_1, c_2, … . Докажем, что $\gamma = c_0, c_1 c_2 \ldots$ является десятичной дробью. Для этого остается показать, что γ не имеет «хвоста» из девяток. Предположим противное, пусть $\gamma = c_0, c_1 c_2 \ldots c_n 99 \ldots$. По построению γ, в M должна существовать десятичная дробь вида $\gamma = c_0, c_1 c_2 \ldots c_n \ldots$, причем, по определению десятичной дроби, после цифры c_n есть цифра, отличная от девятки. Пусть $\beta = c_0, c_1 c_2 \ldots c_n d_{n+1} d_{n+2} \ldots$ — одна из таких дробей, у которой первая не равная девяти цифра d_{n+k} появляется раньше, чем у других дробей такого вида. Тогда приходим к противоречию с выбором девятки в качестве $(n + k)$-го знака для γ: ведь для γ мы выбирали наименьшую из возможных цифр. Полученное противоречие обязывает нас принять, что γ не имеет «хвоста» из девяток, т. е. является десятичной дробью.

Докажем, что γ и есть общий элемент всех отрезков данной последовательности. В силу выбора десятичной дроби γ она не превосходит любой дроби из M, а так как $\beta_n \in M$, то $\gamma \leq \beta_n$ для любого номера n.

Остается показать, что $\alpha_n \leq \gamma$ для любого n. Предположим противное: пусть существует номер m такой, что $\gamma < \alpha_m$ и $\alpha_m = a_0, a_1 a_2 \ldots$. Тогда существует номер k такой, что $c_k < a_k$, и для каждого номера $i < k$ имеет место равенство $c_i = a_i$. В силу выбора десятичной дроби γ во множестве M существует десятичная дробь $\delta = c_0, c_1 c_2 \ldots c_k t_{k+1} t_{k+2} \ldots$. Но тогда

$\delta < \alpha_m$, что противоречит определению множества M. Итак, $\alpha_n \le \gamma \le \beta_n$ для любого n, т. е. γ принадлежит всем отрезкам данной последовательности. □

Конечные десятичные дроби

5.2.5. Определение. *Конечной десятичной дробью* называется десятичная дробь вида $a_0, a_1 a_2 \dots a_n 00\dots$. При записи такой дроби «хвост» нулей будем отбрасывать и записывать конечную десятичную дробь в виде $a_0, a_1 a_2 \dots a_n$.

Для удобства символом 10^{-n} будем обозначать конечную десятичную дробь 0,00...01, где 1 стоит на n-м месте после запятой.

5.2.6. Предложение (свойство усиленной плотности). *Для любых десятичных дробей α и β, если $\alpha < \beta$, то существуют конечные десятичные дроби λ и μ такие, что $\alpha < \lambda < \mu \le \beta$.*

Доказательство. Пусть $\alpha = a_0, a_1 a_2 \dots$, $\beta = b_0, b_1 b_2 \dots$ и $\alpha < \beta$. По определению отношения «меньше», существует номер k такой, что $a_k < b_k$, и для каждого номера $i < k$ имеет место равенство $a_i = b_i$. Но тогда $a_k + 1 \le b_k$, так что если $\mu = a_0, a_1 \dots a_{k-1}(a_k + 1)$, то $\alpha < \mu \le \beta$. По определению десятичной дроби, существует номер $m > k$ такой, что цифра $a_m \ne 9$. Но тогда $a_m + 1$ является цифрой, и если $\lambda = a_0, a_1 \dots a_k \dots a_{m-1}(a_m + 1)$, то $\alpha < \lambda < \mu \le \beta$. □

Определим сложение и умножение конечных десятичных дробей через операции над соответствующими рациональными числами.

5.2.7. Определение. Положим $a_0, a_1 \dots a_k + b_0, b_1 \dots b_m = c_0, c_1 \dots c_n$, если

$$\left(a_0 + \frac{a_1}{10} + \dots + \frac{a_k}{10^k}\right) + \left(b_0 + \frac{b_1}{10} + \dots + \frac{b_m}{10^m}\right) = c_0 + \frac{c_1}{10} + \dots + \frac{c_n}{10^n},$$

и $a_0, a_1 \dots a_k \cdot b_0, b_1 \dots b_m = c_0, c_1 \dots c_n$, если

$$\left(a_0 + \frac{a_1}{10} + \dots + \frac{a_k}{10^k}\right) \cdot \left(b_0 + \frac{b_1}{10} + \dots + \frac{b_m}{10^m}\right) = d_0 + \frac{d_1}{10} + \dots + \frac{d_l}{10^l}.$$

Из этого определения следует, что сложение и умножение конечных десятичных дробей ассоциативны, коммутативны и связаны дистрибутивным законом. Кроме того, для них выполняется аксиома Архимеда.

Сложение произвольных десятичных дробей

Распространим операции сложения и умножения конечных десятичных дробей на все множество десятичных дробей S. Для этого введем одно важное понятие.

5.2.8. Определение. *Последовательностью стягивающихся отрезков* из S назовем такую последовательность вложенных отрезков $([\alpha_n, \beta_n])$, концы которых α_n и β_n являются конечными десятичными дробями, и для любого натурального числа m существует номер k такой, что для всех $n > k$ выполняется неравенство $\beta_n - \alpha_n < 10^{-m}$ (т. е. при возрастании n длины отрезков бесконечно убывают).

5.2.9. Лемма. *Для любой последовательности стягивающихся отрезков* $([\alpha_n, \beta_n])$ *существует и притом только одна десятичная дробь, которая принадлежит всем отрезкам этой последовательности.*

Доказательство. По аксиоме Кантора (5.2.4), существует десятичная дробь γ, принадлежащая всем отрезкам данной последовательности. Пусть десятичная дробь δ также принадлежит всем отрезкам этой последовательности и $\gamma \neq \delta$. Для определенности положим $\gamma < \delta$. По свойству усиленной плотности (5.2.6), существуют конечные десятичные дроби λ и μ такие, что $\gamma < \lambda < \mu \leq \delta$. Тогда для любого n получаем $\alpha_n \leq \gamma < \lambda < \mu \leq \delta \leq \beta_n$, откуда $0 < \mu - \lambda < \beta_n - \alpha_n$ (напомним, что по определению 5.2.8, α_n и β_n являются конечными десятичными дробями, так что разность $\beta_n - \alpha_n$ определена). По определению 5.2.8, для любого натурального числа m существует номер k такой, что для всех $n > k$ выполняется неравенство $\beta_n - \alpha_n < 10^{-m}$, откуда $0 < \mu - \lambda < 10^{-m}$ и $0 < 10^m(\mu - \lambda) < 1$, что противоречит аксиоме Архимеда для конечных десятичных дробей. Следовательно, γ — единственная десятичная дробь, принадлежащая всем отрезкам данной последовательности. □

5.2.10. Определение. Пусть дана десятичная дробь $\alpha = a_0, a_1 a_2 \ldots$. Для любого $n = 0, 1, \ldots$ конечные десятичные дроби $\alpha_n = a_0, a_1 \ldots a_n$ и $\alpha'_n = a_0, a_1 \ldots a_n + 10^{-n}$ называются *приближенными значениями* данной десятичной дроби α.

Всюду в дальнейшем приближенные значения десятичной дроби будем обозначать той же буквой, что и саму дробь, только с индексом внизу. Например, приближенные значения десятичной дроби β будем обозначать через β_n и β'_n, дроби γ — через γ_n и γ'_n, и т. д.

5.2.11. Предложение. *Десятичная дробь* α *является единственным элементом, принадлежащим всем отрезкам последовательности* $([\alpha_n, \alpha'_n])$.

Доказательство. Очевидно, $([\alpha_n, \alpha'_n])$ является последовательностью вложенных отрезков, и для любого n имеем: $\alpha_n \leq \alpha < \alpha'_n$, т. е. α принадлежит всем отрезкам этой последовательности. В то же время, $\alpha'_n - \alpha_n = 10^{-n}$ для любого n, откуда следует, что это последовательность стягивающихся отрезков, и по лемме 5.2.9, α является единственным общим элементом всех отрезков этой последовательности. □

Пусть α и β — конечные десятичные дроби. Для любого n имеем: $\alpha_n \leq \alpha < \alpha'_n$ и $\beta_n \leq \beta < \beta'_n$, откуда $\alpha_n + \beta_n \leq \alpha + \beta < \alpha'_n + \beta'_n$. Таким образом, дробь $\gamma = \alpha + \beta$ принадлежит всем отрезкам последовательности $([\alpha_n + \beta_n, \alpha'_n + \beta'_n])$. Это наталкивает на мысль и в случае произвольных десятичных дробей α и β их суммой $\alpha + \beta$ назвать ту десятичную дробь, которая принадлежит всем отрезкам последовательности $([\alpha_n + \beta_n, \alpha'_n + \beta'_n])$. Но прежде нужно доказать существование и единственность такой десятичной дроби.

5.2.12. Предложение. *Для любых десятичных дробей* α *и* β *существует и притом только одна десятичная дробь* γ, *принадлежащая всем отрезкам последовательности* $([\alpha_n + \beta_n, \alpha'_n + \beta'_n])$.

Доказательство. Для любого $n = 0, 1, \ldots$ имеем: $\alpha_n \le \alpha_{n+1} \le \alpha'_{n+1} \le \alpha'_n$ и $\beta_n \le \beta_{n+1} \le \beta'_{n+1} \le \beta'_n$, откуда $\alpha_n + \beta_n \le \alpha_{n+1} + \beta_{n+1} \le \alpha'_{n+1} + \beta'_{n+1} \le \alpha'_n + \beta'_n$. Следовательно, $([\alpha_n + \beta_n, \alpha'_n + \beta'_n])$ является последовательностью вложенных отрезков. В то же время, $(\alpha'_n + \beta'_n) - (\alpha_n + \beta_n) = (\alpha'_n - \alpha_n) + (\beta'_n - \beta_n) = 10^{-n} + 10^{-n}$, откуда следует, что рассматриваемая последовательность является последовательностью стягивающихся отрезков, и по лемме 5.2.9, существует и единственная десятичная дробь γ, которая принадлежит всем отрезкам этой последовательности. □

Доказанное предложение позволяет дать следующее определение сложения произвольных десятичных дробей.

5.2.13. Определение. *Суммой* произвольных десятичных дробей α и β назовем ту единственную десятичную дробь γ, которая принадлежит всем отрезкам последовательности $([\alpha_n + \beta_n, \alpha'_n + \beta'_n])$. При этом, будем писать: $\alpha + \beta = \gamma$. Отображение $S \times S \xrightarrow{+} S$, сопоставляющее всякой упорядоченной паре (α, β) десятичную дробь $\gamma = \alpha + \beta$, называется *сложением* десятичных дробей.

Основные свойства сложения десятичных дробей

Покажем, что так определенное сложение $+$ на множестве S обладает всеми свойствами, которыми должно обладать сложение действительных чисел в соответствии с определением 5.1.4.

Коммутативность сложения непосредственно вытекает из определения этой операции и из коммутативности сложения конечных десятичных дробей.

5.2.14. Предложение. *Сложение десятичных дробей слабо монотонно, т. е. для любых $\alpha, \beta, \gamma \in S$, если $\alpha \le \beta$, то $\alpha + \gamma \le \beta + \gamma$.*

Доказательство. Из условия $\alpha \le \beta$ следует, что $\alpha_n \le \beta_n$ для любого n, откуда, по свойству слабой монотонности сложения конечных десятичных дробей, $\alpha_n + \gamma_n \le \beta_n + \gamma_n$ для любого n. По определению сложения, $\beta_n + \gamma_n \le \beta + \gamma$, и если предположить, что $\beta + \gamma < \alpha + \gamma$, то получим $\alpha_n + \gamma_n \le \beta_n + \gamma_n \le \beta + \gamma < \alpha + \gamma \le \alpha'_n + \gamma'_n$ для любого n, т. е. $\beta + \gamma$ и $\alpha + \gamma$ являются различными десятичными дробями, принадлежащими всем отрезкам последовательности $([\alpha_n + \gamma_n, \alpha'_n + \gamma'_n])$. Но это противоречит утверждению 5.2.12. Таким образом, $\alpha + \gamma \le \beta + \gamma$. □

Пользуясь доказанным свойством слабой монотонности сложения, нетрудно доказать, что нестрогие неравенства одинакового смысла можно почленно складывать, т. е. если $\alpha \le \beta$ и $\gamma \le \delta$, то $\alpha + \gamma \le \beta + \delta$ для любых $\alpha, \beta, \gamma, \delta \in S$.

5.2.15. Предложение. *Сложение десятичных дробей ассоциативно.*

Доказательство. Пусть α, β, γ — произвольные десятичные дроби. Для любого номера n имеем: $\alpha_n \le \alpha < \alpha'_n, \beta_n \le \beta < \beta'_n, \gamma_n \le \gamma < \gamma'_n$, откуда, по свойству слабой монотонности сложения, $\alpha_n + \beta_n + \gamma_n \le (\alpha + \beta) + \gamma < \alpha'_n + \beta'_n + \gamma'_n$, $\alpha_n + \beta_n + \gamma_n \le \alpha + (\beta + \gamma) < \alpha'_n + \beta'_n + \gamma'_n$. Таким образом, дроби $(\alpha + \beta) + \gamma$ и $\alpha + (\beta + \gamma)$ принадлежат всем отрезкам последовательности $([\alpha_n + \beta_n + \gamma_n, \alpha'_n + \beta'_n + \gamma'_n])$, которая является последовательностью стягиваю-

щихся отрезков, так как $\alpha'_n+\beta'_n+\gamma'_n-(\alpha_n+\beta_n+\gamma_n)=3\cdot10^{-n}$ для любого n. Следовательно, по лемме 5.2.9, дроби $(\alpha+\beta)+\gamma$ и $\alpha+(\beta+\gamma)$ совпадают. □

5.2.16. Предложение. *Для любой десятичной дроби α существует противоположная десятичная дробь $-\alpha$.*

Доказательство. Легко видеть, что последовательность $([-\alpha'_n,-\alpha_n])$ является последовательностью вложенных отрезков, и по аксиоме Кантора существует десятичная дробь β, принадлежащая всем отрезкам этой последовательности, т. е. $-\alpha'_n\le\beta\le-\alpha_n$ для любого n. Так как $\alpha_n\le\alpha<\alpha'_n$ для любого n, то, по свойству слабой монотонности сложения, $\alpha_n-\alpha'_n\le\alpha+\beta\le\alpha'_n-\alpha_n$ для любого n. Но, очевидно, $\alpha_n-\alpha'_n\le0\le\alpha'_n-\alpha_n$, следовательно, $\alpha+\beta$ и 0 принадлежать всем отрезкам последовательности $([\alpha_n-\alpha'_n,\alpha'_n-\alpha_n])$, которая является последовательностью стягивающихся отрезков, так как $\alpha'_n-\alpha_n-(\alpha_n-\alpha'_n)=2\cdot10^{-n}$. Таким образом, по лемме 5.2.9, $\alpha+\beta=0$, т. е. $\beta=-\alpha$. □

5.2.17. Предложение. *Сложение десятичных дробей монотонно, т. е. для любых $\alpha,\beta,\gamma\in S$,* если $\alpha<\beta$, то $\alpha+\gamma<\beta+\gamma$.

Доказательство. По свойству слабой монотонности сложения, неравенство $\alpha<\beta$ влечет $\alpha+\gamma\le\beta+\gamma$. Предположим, что $\alpha+\gamma=\beta+\gamma$. По 5.2.16, существует дробь $-\gamma$. Прибавив ее к обеим частям последнего равенства, получим $\alpha=\beta$, что противоречит условию. Следовательно, $\alpha+\gamma<\beta+\gamma$. □

5.2.18. Теорема. *Для десятичных дробей справедлива аксиома Архимеда: для любых десятичных дробей $\alpha>0$ и β существует натуральное число n такое, что $n\alpha>\beta$.*

Доказательство. По условию, $\alpha>0$, поэтому найдется номер k такой, что $\alpha_k>0$. По аксиоме Архимеда для рациональных чисел, существует натуральное число n такое, что $n\alpha_k>\beta'_0$. Но тогда, используя монотонность сложения, получаем: $n\alpha\ge n\alpha_k>\beta'_0>\beta$. □

Умножение произвольных десятичных дробей

Перейдем к умножению десятичных дробей. Здесь наш путь во многом будет напоминать тот, который мы проделали, рассматривая операцию сложения. Начнем с предложения, аналогичного 5.2.12.

5.2.19. Предложение. *Для любых десятичных дробей $\alpha\ge0$ и $\beta\ge0$ существует и притом только одна десятичная дробь γ, принадлежащая всем отрезкам последовательности* $([\alpha_n\cdot\beta_n,\alpha'_n\cdot\beta'_n])$.

Доказательство аналогично доказательству 5.2.12. □

На основании 5.2.19 можно дать следующее определение умножения произвольных десятичных дробей.

5.2.20. Определение. Пусть даны десятичные дроби α и β:

1) если $\alpha\ge0$ и $\beta\ge0$, то $\alpha\cdot\beta$ есть та единственная десятичная дробь, которая принадлежит всем отрезкам последовательности $([\alpha_n\cdot\beta_n,\alpha'_n\cdot\beta'_n])$;
2) если $\alpha<0$, $\beta\ge0$, то положим $\alpha\cdot\beta=-((-\alpha)\cdot\beta)$;
3) если $\alpha\ge0$, $\beta<0$, то примем $\alpha\cdot\beta=-(\alpha\cdot(-\beta))$;
4) если $\alpha<0$, $\beta<0$, то будем считать $\alpha\cdot\beta=(-\alpha)\cdot(-\beta)$.

Докажем, что умножение произвольных десятичных дробей обладает всеми свойствами, которыми должно обладать умножение действительных чисел.

5.2.21. Предложение. *Умножение десятичных дробей коммутативно.*

Доказательство. Коммутативность умножения неотрицательных десятичных дробей вытекает непосредственно из определения этой операции и из коммутативности умножения конечных десятичных дробей. Если теперь $\alpha < 0$, $\beta \geq 0$, то, пользуясь определением умножения, получаем: $\alpha \cdot \beta = -((-\alpha)\cdot\beta) = -(\beta\cdot(-\alpha)) = \beta\cdot\alpha$.

Аналогично доказывается коммутативность умножения в остальных случаях. □

5.2.22. *Умножение десятичных дробей слабо монотонно, т. е. для любых $\alpha, \beta, \gamma \in S$, если $\alpha \leq \beta$ и $\gamma \geq 0$, то $\alpha\cdot\gamma \leq \beta\cdot\gamma$.*

Доказательство для случая $0 \leq \alpha \leq \beta$ аналогично доказательству слабой монотонности сложения (5.2.14).

Если $\alpha \leq 0 \leq \beta$, то $0 \leq \beta\cdot\gamma$ и $0 \leq -\alpha$, откуда $0 = 0\cdot\gamma \leq (-\alpha)\cdot\gamma = -(\alpha\cdot\gamma)$ и $\alpha\cdot\gamma \leq 0$. Следовательно, $\alpha\cdot\gamma \leq 0 \leq \beta\cdot\gamma$.

Если же $\alpha \leq \beta \leq 0$, то $0 \leq -\beta \leq -\alpha$, откуда последовательно получаем: $(-\beta)\cdot\gamma \leq (-\alpha)\cdot\gamma$, $-(\beta\cdot\gamma) \leq -(\alpha\cdot\gamma)$, $\alpha\cdot\gamma \leq \beta\cdot\gamma$. □

Пользуясь слабой монотонностью умножения, можно доказать, что если $0 \leq \alpha \leq \beta$, $0 \leq \gamma \leq \delta$, то $0 \leq \alpha\cdot\gamma \leq \beta\cdot\delta$.

5.2.23. Предложение. *Умножение десятичных дробей ассоциативно.*

Доказательство. Ассоциативность умножения десятичных дробей $\alpha \geq 0$, $\beta \geq 0$, $\gamma \geq 0$ устанавливается подобно 5.2.15. Если же, например, $\alpha < 0$, $\beta \geq 0$, $\gamma < 0$, то, пользуясь определением умножения, получаем:

$$(\alpha\cdot\beta)\cdot\gamma = (-((-\alpha)\cdot\beta))\cdot\gamma = ((-\alpha)\cdot\beta))\cdot(-\gamma) =$$
$$= (-\alpha)\cdot(\beta\cdot(-\gamma)) = \alpha\cdot(-(\beta\cdot(-\gamma))) = \alpha\cdot(\beta\cdot\gamma)$$

Остальные случаи рассматриваются аналогично. □

Подобным образом доказывается следующее предложение.

5.2.24. Предложение. *Умножение десятичных дробей дистрибутивно относительно сложения.*

5.2.25. Предложение. *Для всякой десятичной дроби $\alpha \neq 0$ существует обратная десятичная дробь α^{-1}, т. е. такая, что $\alpha\cdot\alpha^{-1} = 1$.*

Доказательство. Предположим вначале, что α — положительная конечная десятичная дробь. Тогда она является положительным рациональным числом и, согласно 4.4.6, рациональное число α^{-1} представимо в виде некоторой десятичной дроби β, т. е., по 4.4.4, для любого n имеем $\beta_n \leq \alpha^{-1} < \beta'_n$. Но $\alpha_n \leq \alpha < \alpha'_n$, откуда, пользуясь монотонностью умножения рациональных чисел, получаем $\alpha_n\cdot\beta_n \leq \alpha\cdot\alpha^{-1} < \alpha'_n\cdot\beta'_n$ для любого n. Таким образом, 1 принадлежит всем отрезкам последовательности $([\alpha_n\cdot\beta_n, \alpha'_n\cdot\beta'_n])$. Но, по определению умножения, единственной десятичной дробью, принадлежащей всем отрезкам этой последовательности, является произведение $\alpha\cdot\beta$. Следовательно, $\alpha\cdot\beta = 1$ и $\beta = \alpha^{-1}$.

Пусть теперь α — произвольная положительная десятичная дробь. Тогда существует натуральное число k такое, что $\alpha_{k+n} > 0$ для любого $n = 0, 1, \ldots$, а значит, по доказанному, существуют десятичные дроби α_{k+n}^{-1} и $(\alpha'_{k+n})^{-1}$. Рассмотрим последовательность $([(\alpha'_{k+n})^{-1}, \alpha_{k+n}^{-1}])$. Легко видеть, что она является последовательностью вложенных отрезков. Кроме того,

$$\alpha_{k+n}^{-1} - (\alpha'_{k+n})^{-1} = (\alpha_{k+n} \cdot \alpha'_{k+n})^{-1}(\alpha'_{k+n} - \alpha_{k+n}) \le \alpha_k^{-2} \cdot 10^{-(k+n)}$$

для любого n. Отсюда следует, что рассматриваемая последовательность является последовательностью стягивающихся отрезков, и, по лемме 5.2.9, существует и единственная десятичная дробь γ, принадлежащая всем отрезкам последовательности, т. е. $(\alpha'_{k+n})^{-1} \le \gamma \le \alpha_{k+n}^{-1}$ для любого n. Так как $\alpha_{k+n} \le \alpha < \alpha'_{k+n}$, то, по свойству слабой монотонности умножения, получаем: $\alpha_{k+n} \cdot (\alpha'_{k+n})^{-1} \le \alpha \cdot \gamma \le \alpha'_{k+n} \cdot \alpha_{k+n}^{-1}$, т. е. $\alpha \cdot \gamma$ принадлежит всем отрезкам последовательности $([\alpha_{k+n} \cdot (\alpha'_{k+n})^{-1}, \alpha'_{k+n} \cdot \alpha_{k+n}^{-1}])$. Но, очевидно, 1 принадлежит всем отрезкам этой последовательности. В то же время, легко видеть, что эта последовательность является последовательностью стягивающихся отрезков, и, по лемме 5.2.9, $\alpha \cdot \gamma = 1$, т. е. $\gamma = \alpha^{-1}$.

Наконец, если $\alpha < 0$, то $-\alpha > 0$ и $\alpha^{-1} = -(-\alpha)^{-1}$. □

5.2.26. Предложение. *Умножение десятичных дробей монотонно.*

Доказательство аналогично доказательству 5.2.17. □

Подводя итог, получаем следующую теорему.

5.2.27. Теорема. *Система $\langle S, +, \cdot, < \rangle$ является системой действительных чисел.*

В силу этой теоремы всякую десятичную дробь можно назвать действительным числом и множество всех действительных чисел представлять себе как множество всех десятичных дробей. При этом, периодические десятичные дроби — это рациональные числа, а непериодические десятичные дроби — иррациональные числа.

§ 3. Представление действительных чисел десятичными дробями

Последовательность стягивающихся отрезков

Получив в предыдущем параграфе уверенность в существовании по крайней мере одной системы действительных чисел, приступим к изучению одной из них, т. е. произвольного упорядоченного поля $\langle R, +, \cdot, < \rangle$, в котором выполняются аксиома Архимеда и аксиома Кантора. Начнем с введения понятия последовательности стягивающихся отрезков, которое хорошо зарекомендовало себя при рассмотрении десятичных дробей.

5.3.1. Определение. Пусть дано упорядоченное поле действительных чисел $\langle R, +, \cdot, < \rangle$. *Последовательностью стягивающихся отрезков*

называется такая последовательность вложенных отрезков $([a_n, b_n])$ из R, что для любого натурального числа m существует номер k такой, что для всех $n > k$ выполняется неравенство $b_n - a_n < \frac{1}{m}$.

Легко видеть, что это определение можно сформулировать для произвольного упорядоченного поля. Если его рассматривать на упорядоченном поле десятичных дробей $\langle S, +, \cdot, < \rangle$, то оно эквивалентно определению 5.2.8.

Следующее свойство последовательности стягивающихся отрезков, аналогичное свойству 5.2.9, будет многократно использоваться в дальнейшем.

5.3.2. Предложение. *Для любой последовательности стягивающихся отрезков существует и притом только одно действительное число, принадлежащее всем отрезкам последовательности.*

Доказательство. Пусть дана последовательность стягивающихся отрезков $([a_n, b_n])$ из R. По аксиоме Кантора, существует действительное число c, принадлежащее всем отрезкам последовательности. Пусть действительное число d также принадлежит всем отрезкам этой последовательности и пусть $c < d$. Тогда $a_n \le c < d \le b_n$ для любого n, откуда $0 < d - c \le b_n - a_n$. По определению последовательности стягивающихся отрезков, для любого $m \in N$ существует номер k такой, что для всех $n > k$ выполняется неравенство $b_n - a_n < \frac{1}{m}$. Отсюда $0 < d - c < \frac{1}{m}$, что противоречит аксиоме Архимеда (см. 5.1.5). Следовательно, c — единственное число, принадлежащее всем отрезкам последовательности $([a_n, b_n])$. □

Целая часть действительного числа

5.3.3. Предложение. *Для любого действительного числа a существует и притом только одно целое число m такое, что $m \le a < m + 1$.*

Доказательство. Существование. Рассмотрим подмножество целых чисел $M = \{n \in Z \mid n \le a\}$. По аксиоме Архимеда, для числа $-a$ существует натуральное число n такое, что $n > -a$. Но тогда $-n < a$, откуда $M \ne \varnothing$. Снова, по аксиоме Архимеда, существует натуральное число k такое, что $k > a$, откуда для любого $n \in M$ имеем $n \le a < k$. Таким образом, M — непустое подмножество целых чисел, ограниченное сверху целым числом k. Такое подмножество, по 3.3.17, имеет наибольший элемент, который обозначим через m. Тогда $m \le a < m + 1$.

Единственность. Пусть для целого числа m_1 также выполняются неравенства $m_1 \le a < m_1 + 1$. Тогда в силу выбора m имеем $m_1 \le m$. Предположим, что $m_1 > m$. Тогда $m_1 + 1 \le m \le a$ — пришли к противоречию. Следовательно, $m_1 = m$. □

5.3.4. Определение. *Целой частью* действительного числа a называется целое число, обозначаемое через $[a]$, такое что $[a] \le a < [a] + 1$.

Существование и единственность целой части действительного числа вытекает из 5.3.3.

Представление действительного числа десятичной дробью

5.3.5. Теорема. *Всякое действительное число однозначно представимо в виде десятичной дроби.*

Доказательство. В соответствии с определением 4.4.4, нужно доказать, что для всякого действительного числа a существует и притом только одна десятичная дробь $a_0, a_1a_2\ldots$ такая, что для любого $n = 0, 1, \ldots$ выполняются неравенства

$$a_0 + \frac{a_1}{10} + \ldots + \frac{a_n}{10^n} \le a < a_0 + \frac{a_1}{10} + \ldots + \frac{a_n}{10^n} + \frac{1}{10^n}. \qquad (1)$$

Сначала докажем, что существует не более чем одна десятичная дробь, являющаяся представлением действительного числа a. Для этого выясним, как числа $a_0, a_1, a_2, \ldots$ выражаются через число a. При $n = 0$ из (1) получаем $a_0 \le a < a_0 + 1$, откуда вытекает, что $a_0 = [a]$. Далее, используя обозначение $A_{n-1} = a_0 + \frac{a_1}{10} + \ldots + \frac{a_{n-1}}{10^{n-1}}$ при $n > 0$, получаем $A_{n-1} + \frac{a_n}{10^n} \le a < A_{n-1} + \frac{a_n}{10^n} + \frac{1}{10^n}$. Отсюда $a_n \le 10^n(a - A_{n-1}) < a_n + 1$. Следовательно, $a_n = [10^n(a - A_{n-1})]$. Из единственности целой части числа заключаем, что десятичная дробь однозначно определяется числом a.

Теперь ясно, как нужно доказывать существование искомой десятичной дроби. По данному действительному числу a определим $a_0 = [0]$, и если числа $a_0, a_1, \ldots, a_{n-1}$ уже найдены, то обозначим $A_{n-1} = a_0 + \frac{a_1}{10} + \ldots + \frac{a_{n-1}}{10^{n-1}}$ и положим $a_n = [10^n(a - A_{n-1})]$. Докажем, что при так определенных $a_0, a_1, a_2, \ldots$ имеют место неравенства (1). По определению целой части числа, из формулы для a_0 получаем $a_0 \le a < a_0 + 1$, а из формулы для a_n при $n > 0$ будем иметь: $a_n \le 10^n(a - A_{n-1}) < a_n + 1$, откуда легко получить (1).

Докажем, что запись $a_0, a_1, a_2, \ldots$ является десятичной дробью. Для этого нужно доказать, что $a_1, a_2, \ldots$ являются цифрами и нет «хвоста» из девяток.

Из неравенств $a_0 \le a < a_0 + 1$ получаем $0 \le a - a_0 < 1$, откуда $0 \le 10 \times (a - a_0) < 10$, значит, $0 \le [10(a - a_0)] < 10$. Но $a_1 = [10(a - a_0)]$, следовательно, $0 \le a_1 < 10$, т. е. a_1 — цифра. Аналогично при $n > 0$ из неравенств $a_n \le 10^n(a - A_{n-1}) < a_n + 1$ получаем последовательно $0 \le 10^n \times \left(a - A_{n-1} - \frac{a_n}{10^n}\right) < 1$, $0 \le 10^{n+1}\left(a - \left(A_{n-1} + \frac{a_n}{10^n}\right)\right) < 10$, $0 \le 10^{n+1}(a - A_n) < 10$, $0 \le [10^{n+1}(a - A_n)] < 10$, $0 \le a_{n+1} < 10$, т. е. a_{n+1} — цифра.

Докажем отсутствие «хвоста» из девяток. Предположим противное, пусть, начиная с номера $m + 1$, всюду стоят девятки: $a_0, a_1a_2\ldots a_m 999\ldots$. Воспользуемся доказанными неравенствами (1).

Для любого $i = 1, 2, \ldots$ имеем:

$$A_m + \frac{9}{10^{m+1}} + \ldots + \frac{9}{10^{m+i}} \le a < A_m + \frac{9}{10^{m+1}} + \ldots + \frac{9}{10^{m+i}} + \frac{1}{10^{m+i}} = A_m + \frac{1}{10^m}.$$

Отсюда последовательно получаем: $0 < A_m + \frac{1}{10^m} - a \le \frac{1}{10^{m+i}}$, $0 < \frac{1}{10^{m+i}} \le 10^{m+i}\left(A_m + \frac{1}{10^m} - a\right) \le 1$ для любого $i = 1, 2, \ldots$, что противоречит аксиоме Архимеда. Таким образом, $a_0, a_1 a_2 \ldots$ является десятичной дробью, представляющей действительное число a. □

Докажем, что требование однозначной представимости каждого элемента упорядоченного поля некоторой десятичной дробью эквивалентно аксиоме Архимеда.

5.3.6. Теорема. *В упорядоченном поле аксиома Архимеда выполняется тогда и только тогда, когда всякий его элемент однозначно представим в виде некоторой десятичной дроби.*

Доказательство. Проследив доказательство теоремы 5.3.5, убеждаемся, что в нем, говоря о действительных числах, мы нигде не использовали аксиому Кантора, работала лишь аксиома Архимеда. Таким образом, на самом деле доказано более общее утверждение: если в упорядоченном поле выполняется аксиома Архимеда, то всякий его элемент однозначно представим в виде некоторой десятичной дроби.

Предположим теперь, что произвольный элемент b упорядоченного поля $\langle P, +, \cdot, < \rangle$ представим в виде десятичной дроби $b_0, b_1 b_2$. Тогда $b_0 + 1 > b$. По аксиоме Архимеда для целых чисел, существует натуральное число n такое, что $n > b_0 + 1$. Тогда $n > b$, что, по 5.1.5, эквивалентно аксиоме Архимеда. □

5.3.7. Теорема. *Всякая десятичная дробь является представлением единственного действительного числа.*

Доказательство. Пусть дана десятичная дробь $a_0, a_1 a_2 \ldots$. Для любого $n = 0, 1, \ldots$ обозначим $A_n = a_0 + \frac{a_1}{10} + \ldots + \frac{a_n}{10^n}$, $A'_n = A_n + \frac{1}{10^n}$.

Очевидно, последовательность $([A_n, A'_n])$ является последовательностью стягивающихся отрезков, и, по 5.3.2, существует и притом только одно действительное число a, принадлежащее всем отрезкам этой последовательности, т. е. для любого n выполняются неравенства $A_n \le a \le A'_n$.

Предположим, что $a = A'_m$ для некоторого номера m. Тогда $A'_{m+k-1} = A'_{m+k}$ для любого $k = 1, 2, \ldots$, т. е. $A_{m+k-1} + \frac{1}{10^{m+k-1}} = A_{m+k-1} + \frac{a_{m+k}}{10^{m+k}} + \frac{1}{10^{m+k}}$, откуда $a_{m+k} = 9$. Таким образом, получаем «хвост» из девяток, что противоречит определению десятичной дроби. Следовательно, $A_n \le a < A'_n$ для любого n. В соответствии с определением 4.4.4 это означает, что число a представимо в виде данной десятичной дроби $a_0, a_1 a_2 \ldots$. □

Проследив доказательство теоремы 5.3.7, замечаем, что на самом деле доказана следующая более общая теорема.

5.3.8. Теорема. *Если в упорядоченном поле для всякой последовательности стягивающихся отрезков существует и притом только один элемент, принадлежащий всем отрезкам последовательности, то всякая десятичная дробь является представлением единственного элемента этого упорядоченного поля.*

Теоремы 5.3.5 и 5.3.7 устанавливают взаимно однозначное отображение множества всех действительных чисел R на множество всех десятичных дробей S, которое, как будет установлено в дальнейшем, является изоморфизмом упорядоченного поля действительных чисел на упорядоченное поле десятичных дробей.

Связь между отношениями линейного порядка на множествах R и S

5.3.9. Предложение. *Если действительные числа a и b представимы в виде десятичных дробей соответственно α и β, то $a < b$ тогда и только тогда, когда $\alpha < \beta$.*

Доказательство. ($\Rightarrow$) Докажем, что если $\alpha < \beta$, то $a < b$. Предположим противное, пусть $\alpha < \beta$, но $b \le a$. Если $\alpha = a_0, a_1 a_2 \ldots$, $\beta = b_0, b_1 b_2 \ldots$, то из условия $\alpha < \beta$ следует существование номера k такого, что $a_k < b_k$, а для всех номеров $i < k$ имеет место равенство $a_i = b_i$. Но тогда $a_k + 1 \le b_k$, откуда $A'_k \le B_k$ и $B_k \le b \le a < A'_k \le B_k$ — противоречие. Следовательно, из $\alpha < \beta$ следует $a < b$.

($\Leftarrow$) Предположим $a < b$. Поскольку всякая десятичная дробь является представлением не более одного действительного числа, то $\alpha \ne \beta$. Если предположить, что $\beta < \alpha$, то, по доказанному, $b < a$, что по условию не так. Следовательно, $\alpha < \beta$. □

Заметим, что на самом деле доказана следующая более общая теорема.

5.3.10. Теорема. *Пусть всякая десятичная дробь является представлением не более одного элемента упорядоченного поля $\langle P, +, \cdot, < \rangle$. Если элементы a и b из P представимы в виде десятичных дробей соответственно α и β, то $a < b$ тогда и только тогда, когда $\alpha < \beta$.*

Охарактеризуем систему действительных чисел с помощью понятия представимости элемента упорядоченного поля десятичной дробью.

5.3.11. Теорема. *Упорядоченное поле является системой действительных чисел тогда и только тогда, когда всякий его элемент однозначно представим в виде некоторой десятичной дроби и всякая десятичная дробь является представлением единственного элемента этого упорядоченного поля.*

Доказательство. ($\Rightarrow$) Из 5.3.5 и 5.3.7 вытекает, что система действительных чисел обладает указанными в теореме свойствами.

($\Leftarrow$) Предположим теперь, что всякий элемент упорядоченного поля $\langle P, +, \cdot, < \rangle$ представим в виде некоторой десятичной дроби и всякая десятичная дробь является представлением единственного элемента из P.

По 5.3.6, в данном упорядоченном поле выполняется аксиома Архимеда. Далее, по 5.3.10, если элементы a и b из P представимы в виде десятичных дробей соответственно α и β, то $a<b$ тогда и только тогда, когда $\alpha<\beta$. Отсюда следует, что выполнимость аксиомы Кантора для десятичных дробей (см. 5.2.4) влечет выполнимость ее для данного упорядоченного поля. Следовательно, $\langle P,+,\cdot,<\rangle$ является системой действительных чисел. □

Другая трактовка понятия представимости действительного числа десятичной дробью

Напомним определения необходимых понятий.

5.3.12. Определение. Действительное число a называется *пределом последовательности* действительных чисел (y_n), если для любого действительного числа $\varepsilon>0$ существует номер k такой, что для всех номеров $n<k$ выполняется неравенство $|a-y_n|<\varepsilon$. Записывается: $\lim\limits_{n\to\infty} y_n = a$. При этом говорят, что последовательность (y_n) *сходится* к числу a.

5.3.13. Определение. Пусть дана последовательность действительных чисел $x_0, x_1, x_2, \ldots$. Выражение вида $x_0+x_1+x_2+\ldots$ называется *рядом*. Для любого $n=0,1,2,\ldots$ число $y_n = x_0+x_1+\ldots+x_n$ называется *частичной суммой* этого ряда. Если существует $\lim\limits_{n\to\infty} y_n = a$, то a называется *суммой* данного ряда. При этом пишут: $a = x_0+x_1+x_2+\ldots$.

5.3.14. Предложение. *Действительное число a представимо в виде десятичной дроби $a_0, a_1a_2\ldots$ тогда и только тогда, когда* $a = a_0+\dfrac{a_1}{10}+\dfrac{a_2}{10^2}+\ldots$.

Доказательство. ($\Rightarrow$) Пусть действительное число a представимо в виде десятичной дроби $a_0, a_1a_2\ldots$. По 4.4.4, это означает, что для любого номера n выполняются неравенства $A_n \le a < A_n'$. Тогда $|a-A_n| = a-A_n < A_n'-A_n = \dfrac{1}{10^n}$. Отсюда следует, что $\lim\limits_{n\to\infty} A_n = a$. Очевидно, приближенные значения A_n являются частичными суммами ряда $a_0+\dfrac{a_1}{10}+\dfrac{a_2}{10^2}+\ldots$. Следовательно, a есть сумма этого ряда: $a = a_0+\dfrac{a_1}{10}+\dfrac{a_2}{10^2}+\ldots$.

($\Leftarrow$) Предположим теперь, что дана десятичная дробь $a_0, a_1a_2\ldots$ и $a = a_0+\dfrac{a_1}{10}+\dfrac{a_2}{10^2}+\ldots$. Докажем, что число a представимо в виде этой десятичной дроби. По 5.3.7, существует, и притом только одно, действительное число b, которое представимо в виде данной десятичной дроби $a_0, a_1a_2\ldots$, а по доказанному, b есть сумма ряда: $b = a_0+\dfrac{a_1}{10}+\dfrac{a_2}{10^2}+\ldots$. Из единственности суммы ряда вытекает, что $a = b$. □

Характеризация рационального числа через его представление в виде десятичной дроби

5.3.15. Теорема. *Действительное число a является рациональным тогда и только тогда, когда оно представимо в виде периодической десятичной дроби.*

Доказательство. По 4.4.6, рациональное число представимо в виде периодической десятичной дроби.

Обратно, пусть действительное число a представимо в виде периодической десятичной дроби α, докажем, что a — рациональное число. Рассмотрим типичный пример. Пусть $\alpha = 23{,}56(375)$. Передвинем запятую вправо до периода, для чего обе части равенства умножим на 10^2. Получим $10^2\alpha = 2356{,}(375)$. Теперь передвинем запятую вправо на один период, для чего равенство умножим на 10^3. Получим $10^3 \cdot 10^2\alpha = 2356376(375)$. Из последнего равенства вычтем предпоследнее: $10^3 \cdot 10^2\alpha - 10^2\alpha = 2356375$. Окончательно получаем:

$$\alpha = \frac{2\,356\,375 - 2356}{10^2(10^3 - 1)} = \frac{235 - 2356}{99\,900}.$$

Следовательно, α — рациональное число, равное найденному отношению. Замечаем, что числитель полученной дроби представляет собой разность между числом, записанным цифрами, стоящими до второго периода, и числом, записанным цифрами, стоящими до первого периода, а знаменатель записывается сначала девятками в количестве, равном числу цифр в периоде, а затем нулями в количестве, равном числу цифр от запятой до первого периода.

Теперь не представляет труда провести те же рассуждения в общем виде. Если ограничиться положительными числами, то получаем:

$$\alpha = a_{-n}a_{-(n-1)}\dots a_0, a_1a_2\dots a_m(a_{m+1}a_{m+2}\dots a_{m+k}),$$

где $a_{-n}a_{-(n-1)}\dots a_0$ — десятичная запись целой части данной десятичной дроби α. Выполняя преобразования по той же схеме, как и в примере, в итоге получим:

$$\alpha = \frac{a_{-n}a_{-(n-1)}\dots a_0a_1a_2\dots a_ma_{m+1}a_{m+2}\dots a_{m+k} - a_{-n}a_{-(n-1)}\dots a_0a_1a_2\dots a_m}{\underbrace{99\dots9}_{k}\underbrace{00\dots0}_{m}}. \square$$

§ 4. Изоморфизм упорядоченных полей действительных чисел

Представление в виде десятичной дроби суммы и произведения двух действительных чисел

5.4.1. Предложение. *Если действительные числа a и b представимы в виде десятичных дробей соответственно α и β, то $a + b$ и $a \cdot b$ представимы в виде десятичных дробей, равных соответственно $\alpha + \beta$ и $\alpha \cdot \beta$.*

Доказательство. Для любого n имеем: $A_n \le a < A'_n$, $B_n \le a < B'_n$, откуда $A_n + B_n \le a + b < A'_n + B'_n$. Очевидно, A_n, A'_n и B_n, B'_n представимы в виде конечных десятичных дробей соответственно α_n, α'_n и β_n, β'_n и, по определению 5.2.7, $A_n + B_n$ и $A'_n + B'_n$ представимы в виде конечных десятичных дробей, соответственно равных $\alpha_n + \beta_n$ и $\alpha'_n + \beta'_n$. Число $a + b$ представимо в виде некоторой десятичной дроби γ, а по 5.3.9, при переходе от действительных чисел к соответствующим десятичным дробям отношение $<$ сохраняется. Следовательно, из соотношений $A_n + B_n \le a + b < A'_n + B'_n$ следует $\alpha_n + \beta_n \le \gamma < \alpha'_n + \beta'_n$. Отсюда, по определению сложения десятичных дробей, $\gamma = \alpha + \beta$.

Подобным образом можно установить, что если $a \ge 0$, $b \ge 0$, то произведение $a \cdot b$ представимо в виде десятичной дроби, равной $\alpha \cdot \beta$. Легко доказать также, что число $-a$ представимо в виде десятичной дроби $-\alpha$. Если теперь $a < 0$, $b \ge 0$, то $-a > 0$ и произведение $(-a) \cdot b$ представимо в виде десятичной дроби, равной $(-\alpha) \cdot \beta$, но тогда произведение $a \cdot b = -((-a) \cdot b)$ представимо в виде десятичной дроби, равной $-((-\alpha) \cdot \beta = \alpha \cdot \beta$. Рассматривая аналогично остальные случаи, получаем, что всегда произведение $a \cdot b$ представимо в виде десятичной дроби, равной $\alpha \cdot \beta$. □

Изоморфные отображения упорядоченного поля действительных чисел

5.4.2. Теорема. *Изоморфный образ упорядоченного поля действительных чисел есть упорядоченное поле действительных чисел.*

Доказательство несложно и предоставляется читателю. □

5.4.3. Теорема. *Любые два упорядоченных поля действительных чисел изоморфны.*

Доказательство. Пусть дано произвольное упорядоченное поле действительных чисел $\langle R, +, \cdot, < \rangle$. Обозначим через φ отображение R в S, сопоставляющее всякому действительному числу его представление в виде десятичной дроби. Из 5.3.5 и 5.3.7 вытекает, что φ является взаимно однозначным отображением R на S. Для любых $a, b \in R$, по 5.3.9, $a < b$ тогда и только тогда, когда $\varphi(a) < \varphi(b)$, а по 5.4.1, $\varphi(a+b) = \varphi(a) + \varphi(b)$, $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$. Следовательно, φ является изоморфизмом упорядоченного поля действительных чисел $\langle R, +, \cdot, < \rangle$ на упорядоченное поле десятичных дробей $\langle S, +, \cdot, < \rangle$. Отсюда следует, что любые два упорядоченных поля действительных чисел, будучи изоморфными одному и тому же упорядоченному полю десятичных дробей, изоморфны между собой. □

5.4.4. Теорема. *Изоморфное отображение упорядоченного поля действительных чисел в себя является тождественным, т. е. образ всякого действительного числа совпадает с ним самим.*

Доказательство. Пусть φ — изоморфное отображение упорядоченного поля действительных чисел $\langle P, +, \cdot, < \rangle$ в себя. Последовательно получаем: $\varphi(1) = 1$ (свойство изоморфизма); для любого $k \in N$ имеем $\varphi(k) = k$ (доказывается индукцией по k); для любого $m \in Z$ имеем $\varphi(m) = m$

(рассматриваются случаи $m \in N$, $m = 0$, $m \in -N$); наконец, для любых $m, n \in Z$, где $n \neq 0$, получаем $n \cdot \varphi\left(\frac{m}{n}\right) = \varphi(n) \cdot \varphi\left(\frac{m}{n}\right) = \varphi\left(n \cdot \frac{m}{n}\right) = \varphi(m) = m$, откуда $\varphi\left(\frac{m}{n}\right) = \frac{m}{n}$. Итак, φ действует тождественно на рациональных числах.

Пусть A_n, A'_n — приближенные значения числа $a \in R$, тогда $A_n \leq a < A'_n$ для любого n. Но тогда $A_n = \varphi(A_n) \leq \varphi(a) < \varphi(A'_n) = A'_n$, т. е. a и $\varphi(a)$ принадлежат всем отрезкам последовательности $([A_n, A'_n])$ и, по 5.3.2, $\varphi(a) = a$. Таким образом, φ является тождественным отображением. □

Еще один аспект понятия представимости действительного числа десятичной дробью

Мы уже имеем два аспекта понятия представимости действительного числа десятичной дробью (см. 4.4.4 и 5.3.14). Установим еще одну интерпретацию этого понятия.

5.4.5. Предложение. *Действительное число a представимо в виде десятичной дроби $\alpha = a_0, a_1 a_2 \ldots$ тогда и только тогда, когда существует изоморфизм φ упорядоченного поля действительных чисел $\langle R, +, \cdot, < \rangle$ на упорядоченное поле десятичных дробей $\langle S, +, \cdot, < \rangle$, при котором $\varphi(a) = \alpha$.*

Доказательство. Необходимость установлена при доказательстве 5.4.3. Докажем достаточность. Пусть φ — изоморфизм упорядоченного поля действительных чисел $\langle R, +, \cdot, < \rangle$ на упорядоченное поле десятичных дробей $\langle S, +, \cdot, < \rangle$, при котором $\varphi(a) = \alpha$, и пусть действительное число a представимо в виде десятичной дроби $\beta \in S$. По теореме 5.4.3, существует изоморфизм $\psi : R \to S$, при котором $\psi(a) = \beta$. Очевидно, отображение $f = \psi^{-1}\varphi$ является изоморфизмом упорядоченного поля действительных чисел $\langle R, +, \cdot, < \rangle$ на себя, которое, по 5.4.4, является тождественным: $\psi^{-1}\varphi = \varepsilon$, откуда $\varphi = \psi$ и $\alpha = \varphi(a) = \psi(a) = \beta$. □

§ 5. Аксиома Архимеда и усиленная аксиома Кантора в упорядоченных полях

Упорядоченные поля, удовлетворяющие аксиоме Архимеда

Установим ряд свойств, эквивалентных аксиоме Архимеда.

5.5.1. Теорема. *В упорядоченном поле выполняется аксиома Архимеда тогда и только тогда, когда всякий его элемент является пределом некоторой последовательности рациональных чисел.*

Доказательство. ($\Rightarrow$) Если упорядоченное поле удовлетворяет аксиоме Архимеда, то по 5.3.6 всякий его элемент a представим в виде некоторой десятичной дроби. Но тогда a является пределом последовательности приближенных значений: $a = \lim\limits_{n \to \infty} A_n$ и $A_n \in Q$.

($\Leftarrow$) Пусть всякий элемент упорядоченного поля $\langle P,+,\cdot,<\rangle$ является пределом некоторой последовательности рациональных чисел и $0<a\in P$. Тогда $a=\lim\limits_{n\to\infty} q_n$, где $q_n\in Q$ для любого n. Для 1 существует номер k такой, что $|a-q_k|<1$, откуда $a=|a-q_k+q_k|\le|a-q_k|+|q_k|<1+|q_k|$. По аксиоме Архимеда для рациональных чисел, существует натуральное число m такое, что $1+|q_k|<m$, откуда $a<m$. Итак, для произвольного $a>0$ существует натуральное число m такое, что $a<m$. Следовательно, по 5.1.5 аксиома Архимеда выполняется. □

5.5.2. Теорема. *В упорядоченном поле $\langle P,+,\cdot,<\rangle$ выполняется аксиома Архимеда тогда и только тогда, когда оно обладает свойством усиленной плотности: для любых $a,b\in P$, если $a<b$, то существует рациональное число $\frac{m}{n}$ такое, что $a<\frac{m}{n}<b$.*

Доказательство. ($\Rightarrow$) Пусть упорядоченное поле $\langle P,+,\cdot,<\rangle$ удовлетворяет аксиоме Архимеда и $a,b\in P$, $a<b$. Тогда $b-a>0$ и, по аксиоме Архимеда, существует натуральное число n такое, что $n(b-a)>1$, откуда $na+1<nb$. Снова, по аксиоме Архимеда, существует натуральное число m такое, что $m>na$. Пусть m — наименьшее натуральное число с этим свойством. Тогда $m-1<na$, откуда $m\le na+1<nb$. Но тогда $na<m<nb$ и $a<\frac{m}{n}<b$.

($\Leftarrow$) Предположим теперь, что упорядоченное поле $\langle P,+,\cdot,<\rangle$ обладает свойством усиленной плотности. Докажем, что для любого $a>0$ существует натуральное число n такое, что $n>a$. Предположим противное, т. е. существует элемент $a\in P$, $a>0$, такой, что $n\le a$ для любого натурального числа n. По свойству усиленной плотности, существует рациональное число $\frac{k}{m}$ такое, что $a<\frac{k}{m}<2a$. Таким образом, для любого натурального числа n получаем: $n<\frac{k}{m}$, т. е. $nm<k$, что противоречит аксиоме Архимеда для целых чисел. □

Докажем, что все упорядоченные поля, удовлетворяющие аксиоме Архимеда, исчерпываются, по существу, подполями упорядоченного поля действительных чисел.

5.5.3. Теорема. *Упорядоченное поле, в котором выполняется аксиома Архимеда, изоморфно некоторому подполю упорядоченного поля действительных чисел.*

Доказательство. По 5.3.6, всякий элемент данного упорядоченного поля $\langle P,+,\cdot,<\rangle$ однозначно представим в виде десятичной дроби. Докажем, что отображение φ, сопоставляющее всякому элементу $a\in P$ его представление в виде десятичной дроби, является взаимно однозначным. Пусть $a,b\in P$, $\varphi(a)=\alpha$, $\varphi(b)=\beta$ и $\alpha=\beta$. Тогда приближенные значения элементов a и b также равны, т. е. для любого n имеем: $A_n=B_n$, $A'_n=B'_n$. Предположим, что $a\ne b$. Пусть, например, $a<b$. По 5.5.2, дан-

ное упорядоченное поле обладает свойством усиленной плотности, значит, существуют рациональные числа q_1 и q_2 такие, что $a < q_1 < q_2 \le b$. Но тогда для любого n получаем: $A_n \le a < q_1 < q_2 \le b < B'_n = A'_n$, откуда $0 < q_2 - q_1 < A'_n - A_n = \frac{1}{10^n}$, что противоречит аксиоме Архимеда. Остается принять, что $a = b$. Итак, φ — взаимно однозначное отображение P в S, а по 5.3.10 и 5.4.2 φ является изоморфизмом данного упорядоченного поля в упорядоченное поле десятичных дробей, которое, по 5.2.26, является упорядоченным полем действительных чисел. □

5.5.4. Определение. Упорядоченное поле назовем *максимальным с данным свойством*, если оно не изоморфно собственному подполю никакого упорядоченного поля, обладающего данным свойством.

5.5.5. Теорема. *Система $\langle P, +, \cdot, < \rangle$ есть система действительных чисел тогда и только тогда, когда она является максимальным упорядоченным полем, удовлетворяющим аксиоме Архимеда.*

Доказательство. ($\Rightarrow$) Пусть дана система действительных чисел $\langle R, +, \cdot, < \rangle$. Предположим, что существует упорядоченное поле $\langle K, +, \cdot, < \rangle$, удовлетворяющее аксиоме Архимеда, и φ — изоморфное отображение R в K, при котором $\varphi(R) \ne K$. По 5.5.3, существует изоморфизм ψ упорядоченного поля $\langle K, +, \cdot, < \rangle$ на некоторое подполе упорядоченного поля действительных чисел $\langle R, +, \cdot, < \rangle$. Тогда $\psi\varphi$ есть изоморфное отображение R в себя, и, по 5.4.5, оно является тождественным отображением, т. е. для любого $a \in R$ имеем $\psi\varphi(a) = a$. Отсюда $\varphi(a) = \psi^{-1}(a)$ для любого $a \in R$. Следовательно, $\varphi = \psi^{-1}$ и $\varphi(R) = K$ — пришли к противоречию. Остается принять, что упорядоченное поле действительных чисел является максимальным упорядоченным полем, удовлетворяющим аксиоме Архимеда.

($\Leftarrow$) Предположим, что $\langle P, +, \cdot, < \rangle$ есть максимальное упорядоченное поле, удовлетворяющее аксиоме Архимеда. По 5.5.3, существует изоморфизм данного упорядоченного поля в упорядоченное поле действительных чисел $\langle R, +, \cdot, < \rangle$, который, по условию максимальности, является отображением на R. Следовательно, $\langle P, +, \cdot, < \rangle$ само является упорядоченным полем действительных чисел. □

Усиленная аксиома Кантора

5.5.6. Определение. Будем говорить, что упорядоченное поле удовлетворяет *усиленной аксиоме Кантора*, если для любой последовательности стягивающихся отрезков существует и единственный элемент, который принадлежит всем отрезкам последовательности.

5.5.7. Теорема. *Упорядоченное поле удовлетворяет усиленной аксиоме Кантора тогда и только тогда, когда оно является упорядоченным полем действительных чисел.*

Доказательство. ($\Rightarrow$) Из 5.3.2 вытекает, что упорядоченное поле действительных чисел удовлетворяет усиленной аксиоме Кантора.

($\Leftarrow$) Пусть упорядоченное поле $\langle P, +, \cdot, < \rangle$ удовлетворяет усиленной аксиоме Кантора. Докажем, что оно удовлетворяет аксиоме Архимеда. В соответствии с 5.1.5 достаточно доказать, что для любого положительного элемента $a \in P$ существует натуральное число n такое, что $n > a$. Предположим противное: пусть существует элемент $a > 0$ такой, что для любого натурального числа n выполняется неравенство $n \leq a$. Тогда a не является натуральным числом, а значит, $n < a$ для любого n. Отсюда $\frac{1}{a} < \frac{1}{n}$ и последовательность $\left(\left[\frac{1}{a}, \frac{1}{n}\right]\right)$ является последовательностью вложенных отрезков.

Пусть m — произвольное натуральное число. Для любого натурального числа $n > m$ имеем: $(n-m)a > -mn$, откуда $-mn < na - ma$ и $\frac{1}{n} - \frac{1}{a} < \frac{1}{m}$. Следовательно, рассматриваемая последовательность является последовательностью стягивающихся отрезков. В то же время различные элементы $\frac{1}{a}$ и $\frac{2}{a}$ принадлежат всем отрезкам данной последовательности, что противоречит усиленной аксиоме Кантора. Таким образом, упорядоченное поле $\langle P, +, \cdot, < \rangle$ удовлетворяет аксиоме Архимеда, и по 5.3.6, 5.3.8, 5.3.11 является системой действительных чисел. □

§ 6. Степени и логарифмы

Степень с целым показателем

Дополним понятие степени с натуральным показателем (см. 2.7.3).

5.6.1. Определение. Для любого действительного числа $\alpha \neq 0$ и любого натурального n положим $a^{-n} = (a^n)^{-1} = \frac{1}{a^n}$ и $a^0 = 1$. Если m — целое число, то a^m называется *степенью с целым показателем*.

Обратим внимание на то, что нуль в отрицательной и нулевой степени не определены. Докажем основные свойства степени с целым показателем.

5.6.2. Теорема. *Для любых* $0 \neq a \in R$, $0 \neq b \in R$ *и* $m, n \in Z$ *имеют место следующие соотношения*:

1) $a^{m+n} = a^m \cdot a^n$;
2) $a^{m \cdot n} = (a^m)^n$;
3) $a^n \cdot b^n = (a \cdot b)^n$;
4) *если* $0 < a < b$, $m > 0$, *то* $a^m < b^m$;
5) *если* $a > 1$ *и* $m > 0$, *то* $a^m > 1$;
6) *если* $a > 1$ *и* $m < n$, *то* $a^m < a^n$.

Доказательство. При натуральных m и n равенство 1) вытекает из 2.8.5. Если по крайней мере одно из чисел m и n равно нулю,

то равенство 1) очевидно. Пусть $m > 0$, $n < 0$, тогда $n = -n_1$, где $n_1 \in N$ и $a^m \cdot a^n = a^m \cdot a^{-n_1} = a^m \cdot \frac{1}{a^{n_1}} = \frac{a^m}{a^{n_1}}$. Если $-n_1 < m$, то $m - n_1 \in N$ и, пользуясь равенством 1) для натуральных показателей и основным свойством дроби, получаем $a^m \cdot a^n = \frac{a^m}{a^{n_1}} = \frac{a^{m-n_1} \cdot a^{n_1}}{a^{n_1}} = a^{m-n_1} = a^{m+n}$. Если $m = n_1$, то $a^m \cdot a^n = \frac{a^m}{a^{n_1}} = 1 = a^0 = a^{m-n_1} = a^{m+n}$. Если же $m < n_1$, то $n_1 - m \in N$, и мы получаем $a^m \cdot a^n = \frac{a^m}{a^{n_1}} = \frac{a^m}{a^{n_1-m} \cdot a^m} = \frac{1}{a^{n_1-m}} = a^{-(n_1-m)} = a^{m-n_1} = a^{m+n}$. Случай $m < 0$, $n > 0$ получается из рассмотренного переменой мест m и n. Наконец, если $m < 0$, $n < 0$, то $m = -m_1$, $n = -n_1$, $m_1, n_1 \in N$ и $a^m \cdot a^n = a^{-m_1} \cdot a^{-n_1} = \frac{1}{a^{m_1}} \cdot \frac{1}{a^{n_1}} = \frac{1}{a^{m_1+n_1}} = a^{-(m_1-n_1)} = a^{-m_1+(-n_1)} = a^{m+n}$.

Равенства 2) и 3) также доказываются рассмотрением всевозможных случаев относительно m и n. Свойство 4) легко доказать индукцией по m. Свойство 5) вытекает из 4).

Докажем 6). Из условия $m < n$ следует, что $n - m \in N$, и по 5) получаем $a^{n-m} > 1$. Отсюда $a^n = a^{n-m} \cdot a^m > a^m$. □

Степень с рациональным показателем

Как уже отмечалось, уравнение $x^2 = 2$ в поле рациональных чисел решения не имеет. Имеет ли оно решение в поле действительных чисел? Ответ дает следующая теорема.

5.6.3. Теорема. *Для любого действительного числа $a > 0$ и любого натурального числа n существует, и притом только одно, положительное действительное число b такое, что $b^n = a$.*

Доказательство. Существование. По 3.3.17, всякое непустое ограниченное сверху подмножество целых чисел содержит наибольшее число, поэтому существует наибольшее целое число b_0 такое, что $b_0^n \le a$. Если целые числа $b_0, b_1, \ldots, b_{k-1}$ уже определены, то через b_k обозначим наибольшее целое число такое, что $\left(b_0 + \frac{b_1}{10} + \ldots + \frac{b_{k-1}}{10^{k-1}} + \frac{b_k}{10^k}\right)^n \le a$. Существование числа b_k также опирается на 3.3.17. Таким образом, индуктивно определена последовательность целых чисел $b_0, b_1, \ldots, b_k \ldots$. Пусть $B_k = b_0 + \frac{b_1}{10} + \ldots + \frac{b_k}{10^k}$, $B_k' = B_k + \frac{1}{10^k}$, $k = 0, 1, \ldots$. Легко видеть, что $([B_k, B_k'])$ является последовательностью вложенных отрезков и, по аксиоме Кантора, существует действительное число b, которое принадлежит всем отрезкам последовательности. Вместе с тем, последовательность $([B_k^n, (B_k')^n])$ является последовательностью стягивающихся отрезков, и числа b^n и a принадлежат всем отрезкам этой последовательности. Следовательно, по 5.3.2, $b^n = a$. Для любого номера k имеем $b_k \ge 0$, откуда $b \ge 0$. Но $b^n = a > 0$, поэтому $b > 0$.

Единственность. Пусть $b^n = a$ и $b_1^n = a$, причем $b > 0$ и $b_1 > 0$. Тогда $b^n = b_1^n$, и если предположить, например, что $b < b_1$, то, по свойству 4) из 5.6.2, получим $b^n < b_1^n$ — противоречие. Следовательно, $b = b_1$. □

5.6.4. Определение. Пусть действительное число $a > 0$ и $n \in N$.

1. Положим $a^{1/n} = b$ тогда и только тогда, когда $b > 0$ и $b^n = a$. Число $a^{1/n}$ записывается также в виде $\sqrt[n]{a}$ и называется *арифметическим корнем n-й степени из положительного числа a*.

2. Для любого рационального числа m/n, где $n > 0$, положим $a^{m/n} (a^{1/n})^m$.

3. Если $(m/n) > 0$, то будем считать $0^{m/n} = 0$.

Число $a^{m/n}$ называется *степенью с рациональным показателем*.

Рассмотрим основные свойства степеней с рациональными показателями.

5.6.5. Теорема. *Для любых действительных чисел $a > 0$, $b > 0$ и любых рациональных чисел m/n, p/q имеют место следующие соотношения*:

1) $(a^m)^{1/n} = a^{m/n}$;
2) $a^{m/n} \cdot a^{p/q} = a^{m/n+p/q}$;
3) $a^{m/n} \cdot b^{m/n} = (ab)^{m/n}$;
4) $a^{-(m/n)} = (a^{-1})^{m/n} = (a^{m/n})^{-1}$;
5) $(a^{m/n})^{p/q} = a^{(m/n)\cdot(p/q)}$;
6) *если* $0 < a < b$, $(m/n) > 0$, *то* $a^{m/n} < b^{m/n}$;
7) *если* $a > 1$ *и* $(m/n) < (p/q)$, *то* $a^{m/n} < a^{p/q}$.

Доказательство. 1. По определению 5.6.4, $(a^{1/n})^n = a$. Используя это равенство и свойства целых степеней (5.6.2), получаем $((a^{1/n})^m)^n = (a^{1/n})^{mn} = ((a^{1/n})^n)^m = a^n$, откуда, по определению 5.6.4, $(a^m)^{1/n} = (a^{1/n})^m = a^{m/n}$.

2. По доказанному, $a^{m/n+p/q} = a^{(mq+np)/nq} = (a^{mq+np})^{1/nq}$, поэтому в соответствии с определением 5.6.4 для доказательства соотношения 2) достаточно показать, что $(a^{m/n} \cdot a^{p/q})^{nq} = a^{mq+np}$. Докажем это равенство, пользуясь свойствами целых степеней и соотношением 1). Имеем:

$$(a^{m/n} \cdot a^{p/q})^{nq} = (a^{m/n})^{nq} \cdot (a^{p/q})^{nq} = (((a^m)^{1/n})^n)^q \cdot (((a^p)^{1/q})^n =$$
$$= (a^m)^q \cdot a^p)^n = a^{mq} \cdot a^{pn} = a^{mq+np}.$$

3. $(a^{m/n} \cdot b^{m/n})^n = (a^{m/n})^n \cdot (b^{m/n})^n = ((a^m)^{1/n})^n \cdot ((b^m)^{1/n})^n = a^m \cdot b^m = (ab)^m$, откуда $a^{m/n} \cdot b^{m/n} = ((ab)^m)^{1/n} = (ab)^{m/n}$.

4. Пользуясь свойством 2), получаем $a^{-(m/n)} \cdot a^{m/n} = a^{-(m/n)+m/n} = a^0 = 1$, откуда $a^{-(m/n)} = (a^{m/n})^{-1}$. Аналогично, пользуясь соотношением 3), получаем $(a^{-1})^{m/n} \cdot a^{m/n} = (a^{-1} \cdot a)^{m/n} = 1$, откуда $a^{-(m/n)} = (a^{m/n})^{-1}$.

5. Заметим, что $a^{(m/n)\cdot(p/q)} = a^{mp/nq} = (a^{mp})^{1/nq}$. Для доказательства равенства 5) остается доказать, что $((a^{(m/n)})^{p/q})^{nq} = a^{mp}$. Докажите это самостоятельно.

6. Докажем вначале, что если $0 < a < b$ и $n \in N$, то $a^{1/n} < b^{1/n}$. Предположим противное: $b^{1/n} \le a^{1/n}$. Тогда, пользуясь свойством 8) из 2.8.5, получаем $(b^{1/n})^n \le (a^{1/n})^n$, откуда $b \le a$, что противоречит условию. Остается принять, что $a^{1/n} < b^{1/n}$, откуда $a^{m/n} < b^{m/n}$.

7. Предположим противное, пусть $a > 1$, $(m/n) < (p/q)$, но $a^{p/q} \le a^{m/n}$. Тогда, по 6), $(a^{p/q})^{nq} \le (a^{m/n})^{nq}$, откуда $a^{pn} \le a^{mq}$. С другой стороны, по условию, $(m/n) < (p/q)$, откуда $mq < pn$ и, по свойству 6) из 5.6.2, $a^{mq} < a^{pn}$ — пришли к противоречию. Остается принять, что $a^{m/n} < a^{p/q}$. □

Степень с действительным показателем

5.6.6. Теорема. *Пусть a и b — действительные числа, $a \ge 1$ и b представимо в виде десятичной дроби $b_0, b_1 b_2 \ldots$, причем $B_k = b_0 + \frac{b_1}{10} + \ldots + \frac{b_k}{10^k}$, $B'_k = B_k + \frac{1}{10^k}$, $k = 0, 1, \ldots$. Существует, и притом только одно, действительное число, принадлежащее всем отрезкам последовательности $([a^{B_k}, a^{B'_k}])$.*

Доказательство. Если $a = 1$, то утверждение очевидно. Пусть $a > 1$. Для любого $k = 0, 1, \ldots$ имеем: $B_k \le B_{k+1}$ и $B'_{k+1} \le B'_k$, откуда, по 7) из 5.6.5, получаем $a^{B_k} \le a^{B_{k+1}}$ и $a^{B'_{k+1}} \le a^{B'_k}$. Следовательно, последовательность $([a^{B_k}, a^{B'_k}])$ является последовательностью вложенных отрезков. Вместе с тем, используя пункты 2) и 7) из 5.6.5, получаем $a^{B'_k} - a^{B_k} = a^{B_k}(a^{B'_k - B_k} - 1) < a^{B_0+1}(a^{1/10^k} - 1)$.

Правая часть этого неравенства при возрастании k стремится к нулю, значит, рассматриваемая последовательность является последовательностью стягивающихся отрезков, и, по 5.3.2, существует единственное действительное число, принадлежащее всем отрезкам последовательности. □

5.6.7. Определение. Пусть a и b — действительные числа.

1. Если $a > 1$, то a^b есть то единственное действительное число, которое, по 5.6.6, принадлежит всем отрезкам последовательности $([a^{B_k}, a^{B'_k}])$.
2. Если $0 < a < 1$, то полагаем $a^b = ((a^{-1})^b)^{-1}$.
3. Если $b > 0$, то $0^b = 0$.

Число a^b называется степенью с действительным показателем.

5.6.8. Теорема. Для любых действительных чисел $a > 0$, b, c имеют место следующие соотношения:

1) $(a^{-1})^b = (a^b)^{-1}$;
2) $a^b \cdot a^c = a^{b+c}$;
3) $a^{-b} = (a^b)^{-1}$;
4) если $b > 0$, то $a^c \cdot b^c = (ab)^c$;
5) $(a^b)^c = a^{bc}$;
6) если $0 < a < b$, $c > 0$, то $a^c < b^c$;
7) если $a > 1$ и $b < c$, то $a^b < a^c$.

Доказательство. 1. По определению 5.6.7, при $0 < a < 1$ имеем $a^b = ((a^{-1})^b)^{-1}$, откуда $(a^b)^{-1} = (a^{-1})^b$. Если $a = 1$, то утверждение очевидно. Если $a > 1$, то $0 < a^{-1} < 1$, и, по определению 5.6.7, $(a^{-1})^b = (((a^{-1})^{-1})^b)^{-1}$, откуда $(a^{-1})^b = (a^b)^{-1}$.

2. Пусть b, c и $d = b + c$ представлены в виде десятичных дробей соответственно $b_0, b_1 b_2 \ldots$, $c_0, c_1 c_2 \ldots$, $d_0, d_1 d_2 \ldots$ и $B_k = b_0 + \frac{b_1}{10} + \ldots + \frac{b_k}{10^k}$,

$B'_k = B_k + \frac{1}{10^k}$; $C_k = c_0 + \frac{c_1}{10} + \ldots + \frac{c_k}{10^k}$, $C'_k = C_k + \frac{1}{10^k}$; $D_k = d_0 + \frac{d_1}{10} + \ldots + \frac{d_k}{10^k}$, $D'_k = D_k + \frac{1}{10^k}$. Так как $B_k \le b < B'_k$, $C_k \le c < C'_k$ для любого k, то $B_k + C_k \le b + c < B'_k + C'_k$, откуда $B_k + C_k \le D_k$ и $D'_k \le B'_k + C'_k$ для любого k.

Пусть $a \ge 1$. По определению 5.6.7, $a^{B_k} \le a^b \le a^{B'_k}$, $a^{C_k} \le a^c \le a^{C'_k}$, откуда, используя монотонность умножения и свойство 2) из 5.6.5, получим $a^{B_k + C_k} \le a^b \cdot a^c \le a^{B'_k + C'_k}$.

С другой стороны, пользуясь утверждением 7) из 5.6.5 и определением 5.6.7, получаем $a^{B_k + C_k} \le a^{D_k} \le a^d \le a^{D'_k} \le a^{B'_k + C'_k}$. Следовательно, $a^b \cdot a^c$ и a^{b+c} принадлежат всем отрезкам последовательности $([a^{B_k + C_k}, a^{B'_k + C'_k}])$, которая, как легко доказать, является последовательностью стягивающихся отрезков. По 5.3.2, $a^b \cdot a^c = a^{b+c}$.

Если $0 < a < 1$, то $a^{-1} > 1$, и, по доказанному, $(a^{-1})^b \cdot (a^{-1})^c = (a^{-1})^{b+c}$, откуда, по свойству 1), получаем $(a^b)^{-1} \cdot (a^c)^{-1} = (a^{b+c})^{-1}$ и $a^b \cdot a^c = a^{b+c}$.

3. Пользуясь доказанным утверждением 2), получаем $a^{-b} \cdot a^b = a^{-b+b} = a^0 = 1$, откуда $a^{-b} = (a^b)^{-1}$. Равенство $(a^b)^{-1} = (a^{-1})^b$ доказывается на основании п. 2 из 5.6.7.

4. Предположим вначале, что $a \ge 1$ и $b \ge 1$, тогда $ab \ge 1$. По определению 5.6.7, $a^{C_k} \le a^c \le a^{C'_k}$, $b^{C_k} \le b^c \le b^{C'_k}$ для любого k, откуда, по 3) из 5.6.5, $(ab)^{C_k} \le a^{C_k} b^{C_k} \le a^c b^c \le a^{C'_k} b^{C'_k} = (ab)^{C'_k}$. С другой стороны, по определению 5.6.7, для любого k имеем $(ab)^{C_k} \le (ab)^c \le a^{C'_k}$. Следовательно, числа $a^c b^c$ и $(ab)^c$ принадлежат всем отрезкам последовательности $([(ab)^{C_k}, (ab)^{C_k}])$, которая, как легко доказать, является последовательностью стягивающихся отрезков, и, по 5.3.2, $a^c \cdot b^c = (ab)^c$.

Пусть $0 < a < 1$, $b \ge 1$, $ab \ge 1$. Тогда $a^{-1} > 1$ и, по доказанному, $(a^{-1})^c \times (ab)^c = (a^{-1} \cdot ab)^c = b^c$. Отсюда $((a^{-1})^c)^{-1} \cdot b^c = (ab)^c$ и $a^c \cdot b^c = (ab)^c$.

Пусть $0 < a < 1$, $b \ge 1$, $ab < 1$. Тогда $a^{-1} > 1$, $(ab)^{-1} > 1$ и, по доказанному, $((ab)^{-1})^c \cdot b^c = ((ab)^{-1} \cdot b)^c = (a^{-1})b^c$, откуда $((ab)^c)^{-1} \cdot b^c = (a^c)^{-1}$ и $a^c \cdot b^c = (ab)^c$.

Наконец, если $0 < a < 1$, $0 < b < 1$, то $a^{-1} > 1$, $b^{-1} > 1$ и, по доказанному, $(a^{-1})^c \cdot (b^{-1})^c = (a^{-1}b^{-1})^c = ((ab)^{-1})^c$, откуда $(a^c)^{-1} \cdot (b^c)^{-1} = ((ab)^c)^{-1}$ и $a^c \cdot b^c = (ab)^c$.

5. Предположим, что $a \ge 1$. По определению 5.6.7, $a^{B_k} \le a^b \le a^{B'_k}$ для любого k, откуда $a^{B_k C_k} = (a^{B_k})^{C_k} \le (a^b)^{C_k} \le (a^b)^c \le (a^b)^{C'_k} \le (a^{B'_k})^{C'_k} = a^{B'_k C'_k}$.

С другой стороны, обозначим $ab = t$ и пусть t представимо в виде десятичной дроби $t_0, t_1 t_2 \ldots$ и $T_k = t_0 + \frac{t_1}{10} + \ldots + \frac{t_k}{10^k}$, $T'_k = T_k + \frac{1}{10^k}$, $k = 0, 1, \ldots$. Так как $B_k \le b < B'_k$, $C_k \le c < C'_k$, то $B_k C_k \le t < B'_k C'_k$, откуда $B_k C_k \le T_k$, $T'_k \le B'_k C'_k$ для любого k. Но тогда $a^{B_k C_k} \le a^{T_k} \le a^{bc} \le a^{T'_k} \le a^{B'_k C'_k}$. Следовательно, $(a^b)^c$ и a^{bc} принадлежат всем отрезкам последовательности $([a^{B_k C_k}, a^{B'_k C'_k}])$, которая, как легко доказать, является последовательностью стягивающихся отрезков, и, по 5.3.2, $(a^b)^c = a^{bc}$.

Предположим теперь, что $0 < a < 1$, тогда $a^{-1} > 1$ и, по доказанному, $((a^{-1})^b)^c = (a^{-1})^{bc}$, откуда $(a^b)^c = a^{bc}$.

6. Предположим противное: пусть $b^c \le a^c$. Так как $c > 0$, то $C_k \ge 0$ для любого k, и из условия $a < b$ следует, что $a^{C_k} \le b^{C_k} \le b^c \le a^c \le a^{C_k'}$, т. е. a^c и b^c принадлежат всем отрезкам последовательности $([a^{C_k}, a^{C_k'}])$. По 5.3.2, $a^c = b^c$. Но тогда $(a^c)^{c^{-1}} = (b^c)^{c^{-1}}$, откуда $a \le b$ — пришли к противоречию. Остается принять, что $a^c < b^c$.

7. По условию, $a > 1$ и $c - b > 0$, откуда, по доказанному утверждению 6), $a^{c-b} > 1$. Так как $a^b > 0$, то $a^{c-b} > a^b$, откуда $a^b < a^c$. □

Логарифмы

5.6.9. Теорема. *Для любых действительных чисел a и c таких, что $a > 0$, $a \ne 1$ и $c > 0$, существует, и притом только одно, действительное число b такое, что $a^b = c$.*

Доказательство. Существование. Пусть $a > 1$. Обозначим через b_0 наибольшее целое число такое, что $a^{b_0} \le c$. Пусть целые числа $b_0, \dots, b_{k-1}$ уже выбраны и $B_{k-1} = b_0 + \frac{b_1}{10} + \dots + \frac{b_{k-1}}{10^{k-1}}$. Обозначим через b_k наибольшее целое число такое, что если $B_k = B_{k-1} + \frac{b_k}{10^k}$, то $a^{b_k} \le c$. Таким образом, индуктивно определена последовательность чисел $b_0, b_1, \dots$. Пусть $B_k' = B_k + \frac{1}{10^k}$, $k = 0, 1, \dots$. Легко видеть, что $([B_k, B_k'])$ является последовательностью стягивающихся отрезков, значит, существует единственное число b, которое принадлежит всем отрезкам последовательности. Используя свойство 7) из 5.6.8, легко доказать, что число a^b принадлежит всем отрезкам последовательности стягивающихся отрезков $([a^{B_k}, a^{B_k'}])$. Но число c также принадлежит всем отрезкам этой последовательности, следовательно, $a^b = c$.

Если же $0 < a < 1$, то $a^{-1} > 1$ и, по доказанному, существует число b такое, что $(a^{-1})^b = c^{-1}$, откуда $a^b = c$.

Единственность. Пусть $c = a^b = a^d$. Если $a > 1$, то из предположения $b < d$, по свойству 7) из 5.6.8, получаем $a^b < a^d$, что противоречит условию. Следовательно, $b = d$. Если же $0 < a < 1$, то $a^{-1} > 1$ и, пользуясь свойством 1) из 5.6.8, получаем $(a^{-1})^b = (a^b)^{-1} = (a^d)^{-1} = (a^{-1})^d$, откуда, по доказанному, $b = d$. □

5.6.10. Определение. Пусть даны действительные числа $a > 0$, $a \ne 1$ и $c > 0$. Действительное число b называется *логарифмом числа c по основанию a*, если $a^b = c$. При этом пишут: $b = \log_a c$.

Непосредственно из определения вытекает, что $a^{\log_a b} = b$.

Отметим основные свойства логарифмов.

5.6.11. Теорема. *Для любых действительных чисел $a > 0$, $a \ne 1$, $b > 0$, $c > 0$ имеют место следующие свойства*:

1) $\log_a(bc) = \log_a b + \log_a c$;

2) $\log_a \frac{b}{c} = \log_a b - \log_a c$;

3) $\log_a b^c = c \log_a b$;

4) $\log_a 1 = 0$;
5) $\log_a a = 1$.
Доказательство свойств предоставляется читателю. □

§ 7. Другие определения системы действительных чисел

Определения системы действительных чисел с помощью понятий сечения и верхней границы

Впервые теория действительных чисел была построена выдающимся немецким математиком Р. Дедекиндом. Она основана на понятии сечения.

5.7.1. Определение. Пусть дано линейно упорядоченное множество $\langle P, < \rangle$. Упорядоченная пара подмножеств (A, B) из P называется *сечением*, если выполняются следующие условия: 1) $A \neq \varnothing$, $B \neq \varnothing$; 2) $A \cap B = \varnothing$; 3) $A \cup B = P$; 4) для любых $a \in A$, $b \in B$ выполняется неравенство $a < b$.

5.7.2. Определение. Пусть (A, B) — сечение линейно упорядоченного множества. Наибольший элемент в A и наименьший элемент в B (если они существуют) называются *граничными элементами* сечения.

Нетрудно понять, что всякое сечение может иметь не более двух граничных элементов. Покажем, что все три оставшиеся возможности реализуются.

Пример сечения с двумя граничными элементами. Рассмотрим линейно упорядоченное множество натуральных чисел $\langle N, < \rangle$ и в нем подмножества $A = \{a \in N \mid a \leq 3\}$ и $B = \{b \in N \mid b > 3\}$. Понятно, что (A, B) — сечение и числа 3 и 4 являются его граничными элементами.

Пример сечения с одним граничным элементом. Рассмотрим линейно упорядоченное множество действительных чисел $\langle R, < \rangle$ и в нем подмножества $A = \{a \in R \mid a \leq \sqrt{3}\}$ и $B = \{b \in R \mid b > \sqrt{3}\}$. Ясно, что (A, B) — сечение и единственным его граничным элементом является $\sqrt{3}$ — наибольшее число в A.

Пример сечения, не имеющего граничных элементов. Рассмотрим линейно упорядоченное множество рациональных чисел $\langle Q, < \rangle$ и в нем подмножества $A = \{a \in Q \mid a \leq \sqrt{3}\}$ и $B = \{b \in Q \mid b > \sqrt{3}\}$. Понятно, что (A, B) — сечение. Поскольку $\sqrt{3}$ не является рациональным числом, то граничного элемента нет.

Определение системы действительных чисел по Дедекинду формулируется следующим образом.

5.7.3. Определение. *Системой действительных чисел* называется упорядоченное поле, в котором выполняется аксиома Дедекинда: *всякое сечение упорядоченного поля имеет граничный элемент.*

Вспомним, что геометрическим представлением множества действительных чисел является числовая прямая. Понятно, что если из прямой удалить некоторую точку, то она перестает быть непрерывной,

оставшееся множество точек уже нельзя начертить, не прерываясь. В то же время, образовавшийся пробел разделяет прямую на два подмножества точек A и B, причем пара (A, B) образует сечение оставшегося множества точек. Это сечение не имеет граничного элемента, так как ни в A нет наибольшего элемента, ни в B нет наименьшего. Требование выполнимости аксиомы Дедекинда заставляет нас вернуть на прямую удаленную точку и тем самым восстановить ее непрерывность. Таким образом, аксиома Дедекинда, сформулированная для точек прямой, наглядно выражает ее непрерывность.

Не менее наглядное выражение свойства непрерывности прямой, а вместе с тем и системы действительных чисел, дает аксиома о точной верхней границе. Дадим определение соответствующих понятий. Напомним, что понятия верхней и нижней границ данного множества даны в 2.4.15.

5.7.4. Определение. Пусть A — непустое подмножество линейно упорядоченного множества $\langle P, < \rangle$. Верхняя граница c множества A называется *точной верхней границей* этого множества, если для любой верхней границы b выполняется неравенство $c < b$. Точная верхняя граница множества A обозначается $\sup A$ (читается: супремум A).

5.7.5. Определение. *Системой действительных чисел* называется упорядоченное поле $\langle R, +, \cdot, < \rangle$, в котором выполняется аксиома о точной верхней границе: *всякое непустое ограниченное сверху подмножество из R имеет в R точную верхнюю границу.*

Установим эквивалентность определений системы действительных чисел 5.1.4, 5.7.3 и 5.7.5 по следующей схеме: 5.1.4 $\Rightarrow$ 5.7.3 $\Rightarrow$ 5.7.5 $\Rightarrow$ 5.1.4.

5.7.6. Теорема. *Если в упорядоченном поле выполняются аксиома Архимеда и аксиома Кантора, то выполняется и аксиома Дедекинда.*

Доказательство. Пусть в упорядоченном поле $\langle P, +, \cdot, < \rangle$ выполняются аксиома Архимеда и аксиома Кантора и пусть (A, B) — сечение в P. Поскольку $A \neq \varnothing$ и $B \neq \varnothing$, то существуют $a_0 \in A$, $b_0 \in B$. Разделим отрезок $[a_0, b_0]$ пополам точкой $\dfrac{a_0 + b_0}{2}$ и через $[a_1, b_1]$ обозначим ту из половин отрезка $[a_0, b_0]$, для которой $a_1 \in A$, $b_1 \in B$. Отрезок $[a_1, b_1]$ разделим пополам и через $[a_2, b_2]$ обозначим ту половину, для которой $a_2 \in A$, $b_2 \in B$, и т. д. В результате получим последовательность вложенных отрезков $([a_n, b_n])$, для которой, по аксиоме Кантора, существует элемент $c \in P$, принадлежащий всем отрезкам последовательности. По определению сечения, либо $c \in A$, либо $c \in B$.

Пусть $c \in A$, докажем, что c является наибольшим элементом в A. Предположим противное: пусть существует элемент $a \in A$ такой, что $c < a$. Тогда для любого $n \in N$ имеем: $a_n \leq c < a < b_n$, откуда $0 < a - c < b_n - a_n = \dfrac{b_0 - a_0}{2^n}$ и $2^n(a - c) < b_0 - a_0$, что противоречит аксиоме Архимеда. Следовательно, $a < c$ для любого $a \in A$, т. е. c — наибольший элемент в A.

Если предположить, что $c \in B$, то аналогично можно доказать, что c является наименьшим элементом в B. Итак, c — граничный элемент сечения (A, B). □

5.7.7. Теорема. *Если в упорядоченном поле выполняется аксиома Дедекинда, то выполняется и аксиома о точной верхней границе.*

Доказательство. Пусть в упорядоченном поле $\langle P, +, \cdot, < \rangle$ выполняется аксиома Дедекинда и пусть M — непустое подмножество в P, ограниченное сверху некоторым элементом $c \in P$. Если в M есть наибольший элемент, то он и является точной верхней границей этого подмножества. Предположим, что в M нет наибольшего элемента. Рассмотрим подмножества (рис. 13): $A = \{a \in P \mid$ существует $x \in M$ такой, что $a \le x\}$, $B = \{b \in P \mid x < b$ для любого $x \in M\}$.

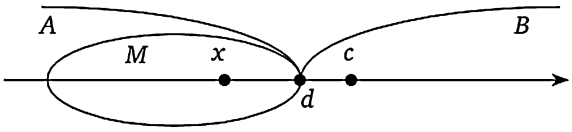

Рис. 13

Следуя определению 5.7.1, докажем, что пара подмножеств (A, B) является сечением. Множество A содержит непустое подмножество M, значит $A \neq \varnothing$.

Так как элемент c, по условию, является верхней границей множества M и, по предположению, в M нет наибольшего элемента, то для любого $x \in M$ имеем: $x < c$. Следовательно, $c \in B$ и $B \neq \varnothing$.

Непосредственно из определения подмножеств A и B вытекает, что $A \cap B = \varnothing$ и $A \cup B = P$.

Пусть $a \in A$, $b \in B$. Тогда, по определению подмножеств A и B, существует $x \in M$ такой, что $a \le x < b$, откуда $a < b$.

Итак, (A, B) — сечение, и, по аксиоме Дедекинда, существует граничный элемент этого сечения, который обозначим через d. Предположим, что $d \in A$. Тогда существует $x \in M$ такой, что $d \le x$. С другой стороны, так как d — наибольший элемент в A и $M \subseteq A$, то $x \le d$. Таким образом $d = x \in M$ и является там наибольшим элементом, что противоречит предположению относительно множества M. Следовательно, $d \in B$. Очевидно, всякая верхняя граница множества M принадлежит B, а так как d — наименьший элемент в B, то $d = \sup M$. □

5.7.8. Теорема. *Если в упорядоченном поле выполняется аксиома о точной верхней границе, то выполняются также аксиома Архимеда и аксиома Кантора.*

Доказательство. Пусть в упорядоченном поле $\langle P, +, \cdot, < \rangle$ выполняется аксиома о точной верхней границе. Установим сначала выполнимость аксиомы Архимеда. Пусть $a, b \in P$ и $a > 0$. Докажем существование натурального числа n такого, что $na > b$. Предположим противное, пусть $na \le b$ для любого $n \in N$. Тогда множество $M = \{na \mid n \in N\}$ не пусто и ограничено сверху элементом b. По условию, существует $c = \sup M$. Так как $a > 0$, то $c - a < c$, и $c - a$ уже не является верхней границей

множества M. Следовательно, существует натуральное число k такое, что $ka > c - a$. Отсюда $(k+1)a > c$ — пришли к противоречию, ибо c есть верхняя граница множества M. Таким образом, существует натуральное число n такое, что $na > b$.

Докажем теперь выполнимость аксиомы Кантора. Пусть дана последовательность вложенных отрезков $([a_n, b_n])$. Множество $A = \{a_n \mid n \in N\}$ не пусто, и всякий элемент b_n является его верхней границей. По условию, существует $\sup M = d$. Но тогда d принадлежит всем отрезкам данной последовательности. □

Определение системы действительных чисел с помощью понятия фундаментальной последовательности

5.7.9. Определение. Последовательность элементов (x_n) упорядоченного поля $\langle P, +, \cdot, < \rangle$ называется *фундаментальной*, если для любого положительного $\varepsilon \in P$ существует номер k такой, что для всех $r > k$, $s > k$ выполняется неравенство $|x_r - x_s| < \varepsilon$.

Напомним, что если в упорядоченном поле $\lim\limits_{n\to\infty} x_n = a$, то говорят, что последовательность (x_n) сходится (к элементу a).

5.7.10. Теорема. *Если упорядоченное поле удовлетворяет аксиоме Архимеда, то оно удовлетворяет аксиоме Кантора тогда и только тогда, когда всякая его фундаментальная последовательность сходится.*

Доказательство. ($\Rightarrow$) Докажем, что в упорядоченном поле действительных чисел (в смысле определения 5.1.4) произвольная фундаментальная последовательность (x_n) сходится.

Сначала установим существование отрезка, содержащего все члены последовательности. По определению фундаментальной последовательности, для числа $\varepsilon > 0$ существует номер r такой, что для любого $s > r$ выполняется неравенство $|x_s - x_r| < 1$, откуда $|x_s| = |(x_s - x_r) + x_r| \le$ $\le |x_s - x_r| + |x_r| < 1 + |x_r|$. Если $m = \max\{|x_0|, \ldots, |x_r|, 1 + |x_r|\}$, то $|x_n| \le m$ для любого n, т. е. $-m \le x_n \le m$. Обозначив $a_0 = -m$, $b_0 = m$, получим, что все члены данной последовательности принадлежат отрезку $[a_0, b_0]$.

Положим $x_{i_0} = x_0$. Разделим отрезок $[a_0, b_0]$ пополам и через $[a_1, b_1]$ обозначим ту его половину, которая содержит бесконечное множество элементов данной последовательности, а через x_{i_1} обозначим произвольный член последовательности (x_n), принадлежащий отрезку $[a_1, b_1]$. Отрезок $[a_1, b_1]$ снова разделим пополам и аналогично выберем половину $[a_2, b_2]$ и член последовательности x_{i_2}, содержащийся в ней. В результате получим последовательность вложенных отрезков $([a_n, b_n])$ и подпоследовательность (x_{i_n}) данной последовательности (x_n). По аксиоме Кантора, существует число c, принадлежащее всем отрезкам последовательности $([a_n, b_n])$. Докажем, что $\lim\limits_{n\to\infty} x_n = c$.

Пусть ε — произвольное положительное действительное число. Из аксиомы Архимеда следует существование натурального числа m такого, что $b_0 - a_0 < 2^{m-1}\varepsilon$, откуда $b_m - a_m = \dfrac{b_0 - a_0}{2^m} < \dfrac{\varepsilon}{2}$. Очевидно, для всех

$n > m$ имеем: $x_{i_n} \in [a_n, b_n] \subseteq [a_m, b_m]$, откуда $|x_{i_n} - c| \le b_n - a_n < b_m - a_m < \frac{\varepsilon}{2}$. Из определения фундаментальной последовательности вытекает, что для $\frac{\varepsilon}{2}$ существует номер k такой, что для всех $n > k$, $i_n > k$ выполняется неравенство $|x_n - x_{i_n}| < \frac{\varepsilon}{2}$. Пусть $t = \max\{k, m\}$. Тогда для всех $n > t$ имеем: $|x_n - c| = |x_n - x_{i_n} + x_{i_n} - c| \le |x_n - x_{i_n}| + |x_{i_n} - c| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$. Следовательно, $\lim\limits_{n\to\infty} x_n = c$.

($\Leftarrow$) Предположим теперь, что в упорядоченном поле $\langle P, +, \cdot, < \rangle$ выполняется аксиома Архимеда и всякая фундаментальная последовательность сходится. Рассмотрим последовательность $([a_n, b_n])$ вложенных отрезков из P и докажем существование в P элемента, принадлежащего всем отрезкам этой последовательности. Обозначим $a_0 = x_0, b_0 = y_0$ и разделим отрезок $[x_0, y_0]$ пополам. Если середина отрезка $\frac{x_0 + y_0}{2}$ принадлежит всем отрезкам данной последовательности, то утверждение доказано. Пусть существует отрезок данной последовательности, не содержащий $\frac{x_0 + y_0}{2}$. Тогда он содержится в одной из половин отрезка $[x_0, y_0]$, которую обозначим через $[x_1, y_1]$. Разделим этот отрезок снова пополам и повторим рассуждения. В результате либо на некотором шаге мы обнаружим элемент, который принадлежит всем отрезкам данной последовательности, либо построим последовательность вложенных отрезков $[x_n, y_n]$, каждый из которых содержит некоторый отрезок данной последовательности $([a_n, b_n])$.

Предположим, что имеет место второй случай. Обозначим $z_{2n} = x_n$, $z_{2n+1} = y_n$, $n = 0, 1, \ldots$. Легко доказать, что последовательность (z_n) является фундаментальной. По условию, существует $\lim\limits_{n\to\infty} z_n = c$; очевидно, c принадлежит всем отрезкам последовательности $([x_n, y_n])$. Докажем, что c принадлежит всем отрезкам данной последовательности $([a_n, b_n])$. Предположим противное: пусть существует номер k такой, что $c \notin [a_k, b_k]$. Тогда либо $c < a_k \le b_k$, либо $a_k \le b_k < c$. Рассмотрим первый случай (во втором случае рассуждения аналогичны). Так как $\lim\limits_{n\to\infty} z_n = c$, то существует номер m такой, что $y_m - c < a_k - c$, откуда $y_m < a_k$. Но тогда отрезки $[x_m, y_m]$ и $[x_k, y_k]$ не имеют общих элементов, а значит, отрезок $[x_m, y_m]$ не содержит ни одного отрезка данной последовательности $([a_n, b_n])$, что противоречит предположению. □

Доказанная теорема показывает, что систему действительных чисел можно определить следующим образом.

5.7.11. Определение. *Системой действительных чисел* называется упорядоченное поле, в котором выполняется *аксиома Архимеда* и *всякая фундаментальная последовательность сходится.*

§ 8. *p*-адические числа

Кольцо *m*-адических чисел

Рассмотрим десятичную дробь 273,35. Если после цифры 5 поставить многоточие, то получим бесконечную десятичную дробь: 273,35... . Поставленные три точки означают, что после пятерки следует бесконечный «хвост» цифр. Примем смелое решение и перед первой цифрой рассматриваемого числа поставим многоточие с аналогичным смыслом, т. е. считаем, что в записи ...273,35 цифре 2 предшествует вполне определенная «дорожка» цифр. Полученную таким образом запись будем называть 10-*адическим числом.* Обобщим эту ситуацию и введем общее понятие.

5.8.1. Определение. Зафиксируем натуральное число $m > 1$ и назовем *m-адическим числом* всякую запись вида $\ldots a_n a_{n-1} \ldots a_1 a_0, a_{-1} \ldots a_{-k}$, где буквы с индексами обозначают цифры m-ичной системы счисления, а многоточие в начале записи указывает на наличие вполне определенной бесконечной последовательности цифр. Если цифры после запятой отсутствуют, то запись называется *целым m-адическим числом.*

Например, 10-адическими числами будут ...0023; ...273; ...36,273; ...00,00. При $m = 7$ получаем 7-адические числа, например $\ldots 352{,}03_7$, $\ldots 26{,}06_7, 10_7$. Если основание системы счисления указано отдельно, то в записи числа его можно опускать.

5.8.2. Определение. Два m-адических числа будем называть *равными*, если равны их соответствующие цифры.

Множество всех m-адических чисел обозначим через Q_m. Определим на этом множестве сложение, вычитание и умножение по известным правилам «столбиком». Например, для 7-адических чисел имеем:

...236,045	...236,045	...236,04
$+$ ...025,362	$-$ ...025,362	$\times$ ...025,36
...264,440	...210,353	...1 2133
		...4 415
		...2 26
		...1 1
		...2,3213

Заметим, что для перехода от привычной десятичной записи «обыкновенного» целого положительного числа к записи его в виде целого 10-адического числа достаточно приписать к нему слева «дорожку» нулей, т. е. записать с нулем в периоде. Например, целое число 24 запишется в виде...0024, или кратко: (0)24. Найдем 10-адическую запись отрицательного целого числа, например –24. Для этого по правилу вычитания «столбиком» найдем разность:

$$\begin{array}{r} \_\ldots0000 \\ \underline{\ldots0024} \\ \ldots9976 \end{array}$$

Для проверки сложите «столбиком» числа...9976 и ...0024. Таким образом, отрицательные целые числа записываются в виде 10-адических чисел с «дорожкой» девяток, т. е. с девяткой в периоде: $-(0)24 = (9)76$.

При произвольном m положительные целые числа записываются в виде целых m-адических чисел с нулем в периоде, а отрицательные — с $(m-1)$ в периоде. Таким образом, можно считать, что $Z \subset Q_m$.

По аналогии с приближенными значениями десятичных дробей введем аналогичное понятие для m-адических чисел.

5.8.3. Определение. Для m-адического числа $\alpha = \ldots a_n a_{n-1} \ldots a_1 a_0, a_{-1} a_{-2} \ldots a_{-k}$ m-адическое число $\alpha_n = \ldots 00 a_n a_{n-1} \ldots a_1 a_0, a_{-1} a_{-2} \ldots a_{-k}$ назовем *приближенным значением* числа α. Аналогичный смысл имеют обозначения $\beta_n, \gamma_n, \delta_n, \ldots$ для m-адических чисел $\beta, \gamma, \delta, \ldots$.

Понятно, что два m-адических числа равны тогда и только тогда, когда для любого номера n их n-е приближенные значения совпадают.

Из способа сложения «столбиком» вытекает, что у суммы m-адических чисел $\alpha+\beta$ и суммы их приближенных значений $\alpha_n+\beta_n$ все цифры с начальными номерами до цифры с номером n включительно совпадают. То же самое справедливо и для произведений $\alpha \cdot \beta$ и $\alpha_n \cdot \beta_n$. Используя это, легко доказать, что сложение и умножение m-адических чисел коммутативны, ассоциативны и умножение дистрибутивно относительно сложения.

Докажем, например, свойство ассоциативности сложения. Из сказанного выше вытекает, что сумма $(\alpha+\beta)+\gamma$ и сумма приближенных значений $(\alpha_n+\beta_n)+\gamma_n$ имеют одинаковые цифры вплоть до n-й. То же самое можно сказать относительно $\alpha+(\beta+\gamma)$ и $\alpha_n+(\beta_n+\gamma_n)$. Но $(\alpha_n+\beta_n)+\gamma_n = \alpha_n+(\beta_n+\gamma_n)$, отсюда и следует совпадение цифр у чисел $(\alpha+\beta)+\gamma$ и $\alpha+(\beta+\gamma)$. Следовательно, $(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)$.

Очевидно, целые числа 0 и 1, которые теперь записываются в виде m-адических чисел соответственно $\ldots 00{,}00\ldots 0$ и $..001{,}00\ldots 0$ (с любым количеством нулей после запятой), играют роль соответственно нуля при сложении и единицы при умножении. Для всякого m-адического числа α существует противоположное m-адическое число $-\alpha$. Таким образом, множество Q_m относительно сложения и умножения образует кольцо, которое называется *кольцом m-адических чисел*. Напомним, что оно содержит кольцо целых чисел.

Перейдем к делению m-адических чисел. Рассмотрим пример деления «уголком» для целых 5-адических чисел. При этом частное будем формировать «справа налево»:

$$
\begin{array}{l}
\_\ldots 1324 \,|\, \underline{\ldots 3213} \\
\quad \underline{\ldots 0144}\ldots 3013 \\
\_\ldots 113 \\
\quad \underline{\ldots 213} \\
\_\ldots 40 \\
\quad \underline{\ldots 00} \\
\_\ldots 4 \\
\quad \underline{\ldots 4} \\
\quad \ldots
\end{array}
$$

Итак, $\ldots1324_5 : \ldots3213_5 = \ldots3013_5$. Поясним вычисления. Сначала находим крайнюю правую цифру частного. Нужно найти такую цифру x, чтобы произведение $3x$, записанное в пятеричной системе счисления, оканчивалось цифрой 4. Заметим, что НОД(3,5) = 1, поэтому, если в выражении $3x$ переменная x пробегает значения 0, 1, 2, 3, 4, то остатки от деления $3x$ на 5 будут пробегать эти же числа лишь в другом порядке. Остаток от деления $3x$ на 5 как раз и дает последнюю цифру числа $3x$. В нашем случае при $x = 3$ получаем число $9_{10} = 14_5$. Умножая делитель $\beta = \ldots3213$ на 3, получим 5-адическое число $\ldots0144$, которое записываем под делимым $\alpha = \ldots1324$, и производим вычитание. В остатке получаем $\ldots113$ (последний ноль не записываем). Теперь аналогично подбираем следующую цифру частного так, чтобы произведение делителя на эту цифру частного оканчивалось цифрой 3. В нашем случае второй цифрой частного следует взять 1. И т. д.

В общем случае, если мы делим m-адическое число α на m-адическое число $\beta \neq 0$ и последняя цифра делителя, обозначим ее через b, взаимно проста с m, то числа $b \cdot 0, b \cdot 1, b \cdot 2, \ldots, b \cdot (m-1)$ при делении на m дают различные остатки, а значит, множество остатков совпадает с множеством цифр 0, 1, 2, …, $m - 1$. Таким образом, в этом случае возможность подбора очередной цифры частного гарантирована и деление возможно. В частности, когда $m = p$ — простое число, деление возможно всегда. Действительно, в этом случае делитель $\beta \neq 0$ можно представить в виде $\beta = \beta' \cdot (10_p)^n$, где β' — целое p-адическое число, не оканчивающееся нулем, т. е. последняя цифра числа β' взаимно проста с p. Деление на β' возможно, а деление на β добавляет еще перемещение запятой на соответствующее число знаков (влево, если $n < 0$, и вправо, что сводится к приписыванию нулей, если $n > 0$). Таким образом, кольцо Q_p при простом p является полем.

Пусть при делении «уголком» произвольного целого m-адического числа α на целое m-адическое число $\beta \neq 0$ «под уголком» получили m-адическое число $\gamma = \ldots c_n c_{n-1} \ldots c_0$. Докажем, что γ действительно является частным от деления α на β, т. е. $\beta \cdot \gamma = \alpha$. Рассмотрим шаги алгоритма деления «уголком»:

$$
\begin{array}{ll}
\alpha & \mid \beta \\
\underline{\beta \cdot c_0} & \ldots c_2 c_1 c_0 \\
r_0 \cdot (10_m) & \\
\underline{\beta \cdot c_1 (10_m)} & \\
r_1 \cdot (10_m)^2 & \\
\underline{\beta \cdot c_2 (10_m)^2} & \\
r_2 \cdot (10_m)^3 & \\
\ldots\ldots\ldots\ldots &
\end{array}
$$

Сначала подбираем цифру c_0 и находим разность: $\alpha - \beta c_0 = r_0(10_m)$, отсюда $\alpha = \beta c_0 + r_0(10_m) = \beta \cdot \gamma_0 + r_0(10_m)$. Затем подбираем цифру c_1 и находим

разность: $r_0(10_m)-\beta c_1(10_m)=r_1(10_m)^2$, откуда $r_0(10_m)=\beta c_1(10_m)+r_1(10_m)^2$ и $\alpha=\beta c_0+\beta c_1(10_m)+r_1(10_m)^2 = \beta(c_0+c_1(10_m))+r_1(10_m)^2=\beta\cdot\gamma_1+r_1(10_m)^2$. На следующем шаге деления получим $\alpha=\beta(c_0+c_1(10_m)+c_2(10_m)^2)+$ $+r_2(10_m)^3=\beta\cdot\gamma_2+r_2(10_m)^3$, и т. д. Таким образом, для любого $n=0,1,\ldots$ имеем: $\alpha=\beta\cdot\gamma_n+r_n(10_m)^n$, откуда $\alpha-\beta\cdot\gamma_n=r_n(10_m)^n$. Отсюда следует, что у m-адических чисел α и $\beta\cdot\gamma$ все цифры с начальными номерами вплоть до цифры с номером n совпадают, каково бы ни было n. Следовательно, $\alpha=\beta\cdot\gamma$.

Отметим, что при любом m в кольце Q_m деление возможно на любое натуральное число β. В самом деле, пусть $m=p_1^{n_1}p_2^{n_2}\ldots p_k^{n_k}$ — каноническое разложение числа m на простые множители. Число β можно представить в виде $\beta=\beta'\cdot p_1^{m_1}p_2^{m_2}\ldots p_k^{m_k}$, где β' взаимно просто с m. Найдутся целые неотрицательные числа $x_1, x_2, \ldots, x_k$ такие, что $p_1^{m_1+x_1}p_2^{m_2+x_2}\ldots p_k^{m_k+x_k}=m^n$ при некотором натуральном n. В этом случае $\dfrac{\alpha}{\beta}=\dfrac{\alpha\cdot p_1^{x_1}p_2^{x_2}\ldots p_k^{x_k}}{\beta'\cdot(10_m)^n}$. Таким образом, деление α на β сводится к делению числа $\alpha\cdot p_1^{x_1}p_2^{x_2}\ldots p_k^{x_k}$ на β', что обеспечивается взаимной простотой чисел β' и m, с последующим перенесением запятой на n знаков.

Подметим особенность m-адической записи рационального числа. Рассмотрим два характерных примера при $m=5$:

```
_...002324 | ...003          _...00002 | ...003
  ...000014  ...00423            ...00022  ...31314
_...00231                    _...4443
  ...00011                     ...0003
_...0022                     _...444
  ...0022                      ...014
  ...000                       ...43
                               ...03
                               ...44
```

Итак, $\ldots002324:\ldots003_5=\ldots00423_5=(0)423_5$ и $\ldots002_5:\ldots003_5=$ $=\ldots31314_5=(31)4_5$. В обоих случаях получаем периодические 5-адические числа. Докажем, что это не случайно. Рассмотрим пристальнее остатки в алгоритме деления «уголком» целого m-адического числа $\alpha=\ldots00a_n\ldots a_1a_0$ на целое m-адическое число $\beta=\ldots.00b_n\ldots b_1b_0\neq 0$. Каждый остаток имеет в периоде либо 0, либо $m-1$. Предположим, что каждый остаток имеет 0 в периоде (как в первом примере). Поскольку в каждом следующем остатке количество цифр после нулевого периода все время уменьшается, то на конечном шаге получим нулевой остаток, а значит, в частном будем иметь 0 в периоде. Если же некоторый остаток имеет цифру $m-1$ в периоде (во втором примере уже

первый остаток...443 имеет 4 в периоде), то и все последующие остатки имеют эту же цифру в периоде. Количество цифр остатка, идущих после периода, не превосходит количества цифр произведения числа, записанного цифрами делителя β, идущими после нулевого периода, на очередную цифру частного (во втором примере в каждом остатке после периода из четверок количество цифр не превосходит количества цифр произведения 3 на очередную цифру частного). Поэтому наступит момент, когда мы получим остаток, который ранее уже встречался. Но тогда, начиная с этого момента, цифры частного начнут повторяться, и мы получим в частном периодическое m-адическое число. Таким образом, всякое рациональное число записывается в виде периодического m-адического числа.

Обратно, всякое периодическое m-адическое число является записью некоторого рационального числа. Покажем на двух характерных примерах, как по данной периодической 5-адической записи найти соответствующее рациональное число. Сначала выполним проверку представления $\frac{2}{3}$ в виде 5-адического числа $\alpha = (31)4_5$. Умножим это равенство на $100_5 = (10_5)^2$ (поскольку в периоде две цифры). Получим $\alpha \cdot (10_5)^2 = (31)4 \cdot (10_5)^2 = (31)400_5$. Тогда $\alpha \cdot (10_5)^2 - \alpha = (31)400_5 - (31)4_5$. Выполним вычитание «столбиком»:

$$\begin{array}{r} \_...3131400 \\ \underline{...3131314} \\ ...0000031 \end{array}$$

Следовательно, $\alpha \cdot (10_5)^2 - \alpha = (0)31_5$. Но $\alpha \cdot (10_5)^2 - \alpha = \alpha \cdot ((10_5)^2 - 1) = \alpha \cdot (...0044_5)$. Таким образом, $\alpha = \frac{...0031_5}{...0044_5} = \frac{31_5}{44_5} = \frac{2_5 \cdot 13_5}{3_5 \cdot 13_5} = \frac{2_5}{3_5}$.

Еще пример. Пусть $\beta = (243)1_5$. Найдем соответствующее рациональное число. Умножим это равенство на $(10_5)^3$ (поскольку в периоде три цифры). Получим $\beta \cdot (10_5)^3 = (243)1000_5$. Найдем разность: $\beta \cdot (10_5)^3 - \beta = (243)1000_5 - (243)1_5 = (4)3014_5$. Отсюда

$$\beta = \frac{...443014_5}{...00444_5} = \frac{-...001431_5}{...00444_5} = -\frac{1431_5}{444_5}.$$

Наконец, рассмотрим общий случай и найдем рациональное число по его записи в виде периодического m-адического числа. Всякое m-адическое число можно представить в виде суммы целого m-адического числа и дробной части, которая, очевидно, является записью рационального числа. Поэтому можно ограничиться рассмотрением периодического целого m-адического числа $\gamma = (a_{n+k}a_{n+k-1}\dots a_{n+1})a_n a_{n-1}\dots a_0$. Умножим это равенство на $(10_m)^k$ (поскольку в периоде k цифр). Получим $\gamma \cdot (10_m)^k = (a_{n+k}a_{n+k-1}\dots a_{n+1})a_n a_{n-1}\dots a_0 \underbrace{00\dots0}_{k}$.

Найдем разность: $\gamma\cdot(10_m)^k-\gamma=(a_{n+k}a_{n+k-1}\dots a_{n+1})a_na_{n-1}\dots a_1a_0\underbrace{00\dots0}_{k}-$

$-(a_{n+k}a_{n+k-1}\dots a_{n+1})a_na_{n-1}\dots a_1a_0=(d)c_{n+k}c_{n+k-1}\dots c_1c_0$, где d — цифра 0 либо цифра $(m-1)$, что соответствует либо положительному, либо отрицательному целому числу. В результате получаем рациональное число $\gamma=\dfrac{(d)c_{n+k}c_{n+k-1}\cdots c_1c_0}{(10_m)^k-1}$. Итак, рациональные числа и только они записываются в виде периодических m-адических чисел. Таким образом, $Q\subset Q_m$.

10-адические числа

Как уже отмечалось, деление m-адических чисел проходит без проблем только при простом $\alpha=\beta\cdot\gamma$. Если же m составное, то деление возможно далеко не всегда. Уже единицу можно разделить не на всякое m-адических число $\alpha\neq0$. Если α^{-1} существует, то число α называют *обратимым* или *делителем единицы*. В связи с этим напомним, что элемент $\alpha\neq0$ кольца K называется *делителем нуля*, если существует в K элемент $\beta\neq0$ такой, что произведение $\alpha\cdot\beta=0$. Предположим, что в этом случае α^{-1} существует. Умножив равенство $\alpha\cdot\beta=0$ на α^{-1}, получаем $\beta=0$, что противоречит условию. Следовательно, для делителя нуля не существует обратного. В то же время при составном m кольцо Q_m содержит делители нуля. Мы докажем это для характерного случая $m=10$. Одновременно будет дано описание элементов кольца Q_{10}.

Построим 10-адическое число $\gamma=\dots c_2c_1c_0$ следующим образом. Положим $c_0=5$, так что $\gamma=\dots5$ и $\gamma_0=5$. Возводим γ_0 в квадрат: $\gamma_0^2=25$ и в качестве c_1 берем вторую цифру полученного числа, т. е. $c_1=2$, $\gamma=\dots25$ и $\gamma_1=25$. Теперь находим $\gamma_1^2=625$ и в качестве c_2 берем третью цифру полученного числа, т. е. $c_2=6$, $\gamma=\dots625$ и $\gamma_2=625$. Далее γ_2 возводим в квадрат: $x_2^2=390625$ и четвертую цифру результата берем в качестве c_3, т. е. $c_3=0$, $\gamma=\dots.0625$, $\gamma_3=0625$. И так далее. На 30-м шаге будем иметь $\gamma=\dots1066199773922562599182128906 25$.

Похожим образом построим число $\delta=\dots d_2d_1d_0$. В качестве начальной цифры возьмем $d_0=2$, так что $\delta=\dots2$ и $\delta_0=2$. Теперь δ_0 возведем в пятую степень и вторую цифру результата (цифру с номером 1) возьмем в качестве d_1 для δ. Так что $\delta=\dots32$ и $\delta_1=32$. Число δ_1 возводим в пятую степень и третью цифру результата (цифру с номером 2) берем в качестве d_2. Имеем: $\delta_1^5=32^5=33554432$, так что $d_2=4$, $\delta=\dots432$ и $\delta_2=432$. И так далее. На 30-м шаге будем иметь $\delta=\dots.5304078398041032634998791864 32$.

5.8.4. Лемма. $\gamma(\gamma-1)=0$ *и* $\delta(\delta^4-1)=0$. *Следовательно, числа* γ *и* $\gamma-1$, *а также* δ *и* δ^4-1 *являются делителями нуля.*

Доказательство для числа γ (для δ аналогично). Достаточно доказать индукцией по n, что $\gamma_n^2-\gamma_n$ делится на 10^{n+1}. При $n=0$ получаем $\gamma_0^2-\gamma_0=5^2-5=20\vdots10$. Пусть $\gamma_n^2-\gamma_n\vdots10^{n+1}$, докажем, что $\gamma_{n+1}^2-\gamma_{n+1}\vdots10^{n+2}$. Из индуктивного предположения следует, что у чисел γ_n^2 и γ_n цифры с но-

мерами $0, 1, \ldots, n$ совпадают. По выбору цифры c_{n+1} числа γ_{n+1}, эта цифра такая же, как у числа γ_n^2 на том же месте. Следовательно, $\gamma_n^2 - \gamma_{n+1} \vdots 10^{n+2}$. Но тогда

$$\gamma_{n+1}^2 - \gamma_{n+1} = (\gamma_n + c_{n+1}10^{n+1})^2 - \gamma_{n+1} =$$
$$= (\gamma_n^2 - \gamma_{n+1}) + 2\gamma_n c_{n+1}10^{n+1} + c_{n+1}^2 10^{2n+2} \vdots 10^{n+2},$$

так как $(\gamma_n^2 - \gamma_{n+1}) \vdots 10^{n+2}$ по индуктивному предположению и $2\gamma_n \vdots 10$. □

5.8.5. Лемма. $\delta^3 + \delta = 0$.

Доказательство. По 5.8.4, $\delta^5 - \delta = 0$, отсюда $(\delta^2 - 1)(\delta^3 + \delta) = 0$. Но число $\delta^2 - 1$ обратимо, поскольку оканчивается цифрой 3, следовательно, на него можно сократить. Таким образом, $\delta^3 + \delta = 0$. □

Установим связь между числами β и $b = b_0 + b_1 10_p + b_2 (10_p)^2 + \ldots$.

5.8.6. Лемма. $\delta^2 - \gamma + 1 = 0$.

Доказательство. Поскольку $\gamma\delta = 0$, $\gamma^2 - \gamma = 0$ и $\delta^3 + \delta = 0$, то $(\delta^2 - \gamma + 1) \times$ $\times (\gamma + \delta) = \delta^2\gamma - \gamma^2 + \gamma + \delta^3 - \gamma\delta + \delta = 0$, а так как число $\gamma + \delta$ обратимо, то $\delta^2 -$ $- \gamma + 1 = 0$. □

Следующая теорема дает классификацию 10-адических чисел.

5.8.7. Теорема. *Для любого 10-адического числа $\alpha \neq 0$ имеет место одно и только одно из трех*: *либо $\alpha = \beta \cdot \gamma$, либо $\alpha = \beta \cdot \delta$ при некотором обратимом β.*

Доказательство. Не нарушая общности, можно считать, что α — целое 10-адическое число. Предположим вначале, что существуют наибольшие показатели k и m такие, что $\alpha = 2^k 5^m \alpha'$. Тогда последняя цифра числа α' взаимно проста с 10, а значит, число α' обратимо. Вместе с тем, если $n = \max\{k, m\}$, то $\dfrac{1}{\alpha} = \dfrac{2^{n-k}5^{n-m}}{\alpha' \cdot 10^n}$, т. е. число α обратимо.

Предположим теперь, что α делится на любую степень числа 5. Тогда, так как δ делится на любую степень двойки, то $\alpha \cdot \delta = 0$, откуда $\alpha \cdot \delta^2 = 0$. Но по 5.8.6 $\delta^2 = \gamma - 1$, откуда $\alpha(\gamma - 1) = 0$ и $\alpha = \alpha\gamma$. Если предположить, что α делится на любую степень двойки, то поскольку γ делится на любую степень пятерки, получаем $\alpha = \alpha\gamma = 0$, что противоречит условию. Следовательно, существует максимальный показатель n такой, что $\alpha = 2^n \alpha''$, где последняя цифра числа α'' нечетная. Очевидно, $\alpha = 2^n(\alpha'' + \lambda\delta)\gamma$ при любом λ, и существует такое λ, что последняя цифра числа $\alpha'' + \lambda\delta$ взаимно проста с 10, т. е. это число обратимо. Но тогда число $\beta = 2^n(\alpha'' + \lambda\delta)$ обратимо и $\alpha = \beta\gamma$.

Наконец, пусть α делится на любую степень двойки. Тогда $\alpha\gamma = 0$, откуда по 5.8.6 $\alpha(\delta^2 + 1) = 0$ и $\alpha = (-\alpha\delta)\delta$. Обозначим $\beta' = -\alpha\delta$, тогда $\alpha = \beta'\delta$. Если предположить, что β' делится на любую степень пятерки, то получаем $\alpha = 0$, что противоречит условию. Следовательно, существует максимальный показатель n такой, что $\beta' = 5^n\beta''$, где последняя цифра числа β'' отлична от 0 и 5. Очевидно, $\alpha = 5^n(\beta'' + \mu\gamma)\delta$ при любом μ, и существует такое μ, что последняя цифра числа $\beta'' + \mu\gamma$ взаимно проста с 10, т. е. это число обратимо. Но тогда число $\beta = 5^n(\beta'' + \mu\gamma)$ обратимо и $\alpha = \beta\delta$.

Докажем единственность каждого из трех случаев. Поскольку $\beta\gamma$ и $\beta\delta$ делители нуля, то они не могут быть обратимыми. Предположим, что одновременно $\alpha=\beta\gamma$ и $\alpha=\beta'\delta$, где β и β' обратимы. Тогда $\beta\gamma=\beta'\delta$ и $\gamma=\gamma^2=\gamma\cdot\beta^{-1}\beta'\delta=0$ — противоречие. □

Используя арсенал понятий теории колец, заимствованный из курса алгебры, можно описать связь между кольцом целых 10-адических чисел Z_{10} и кольцами целых 2-адических чисел Z_2 и целых 5-адических чисел Z_5. Для любого целого 10-адического числа α определим $S_2(\alpha)$ и как записи числа α соответственно в 2-ичной и в 5-ичной системах счисления. Легко видеть, что S_2 и S_5 являются гомоморфизмами кольца Z_{10} на кольца соответственно Z_2 и Z_5. Ядра этих гомоморфизмов обозначим соответственно $A=\ker S_2$ и $B=\ker S_5$. Тогда A и B являются главными идеалами: $A=\langle\delta\rangle$, $B=\langle\gamma\rangle$. При этом всякое 10-адическое число α однозначно представимо в виде $\alpha=a+b$, где $a\in A$, $b\in B$. Это означает, что кольцо Z_{10} представляет собой прямую сумму идеалов: $Z_{10}=A\oplus B$. Используя теорему о гомоморфизмах для колец, получаем, что Z_2 изоморфно фактор-кольцу $Z_{10}/\ker S_2=Z_{10}/A$, которое в свою очередь изоморфно кольцу B. Аналогично устанавливаем, что Z_5 изоморфно A. Следовательно, кольцо Z_{10} изоморфно прямой сумме колец $Z_5\oplus Z_2$. Напомним, что элементами этой прямой суммы являются всевозможные пары вида (α, β), где $\alpha\in Z_5$. При этом изоморфизме числам γ и δ^4 соответствуют пары $(0_5, 1_2)$ и $(1_5, 0_2)$ соответственно. Поскольку $(0_5,1_2)+(1_5,0_2)=(1_5,1_2)$ — образ единицы, то $\gamma+\delta^4=1$. Впрочем, это равенство можно получить из леммы 5.8.6.

m-адическая норма

После введения операций сложения и умножения m-адических чисел хотелось бы осмыслить формальную запись m-адического числа $\alpha=\ldots a_n a_{n-1}\ldots a_1 a_0$ в виде «суммы разрядных единиц», т. е. показать, что

$$\alpha=a_0+a_1(10_m)+\ldots+a_n(10_m)^n+\ldots. \qquad (1)$$

Приведем некоторые наводящие соображения, сознательно допуская определенные неточности. Равенство (1) означает, что α является пределом последовательности частичных сумм: $\alpha=\lim\limits_{n\to\infty} S_n$, где $S_n=a_0+a_1(10_m)+\ldots+a_n(10_m)^r$.

Очевидно, $S_n=\alpha_n$. Найдем разность:

$$\alpha-S_n=\alpha-\alpha_n=\ldots a_{n+2}a_{n+1}a_n a_{n-1}\ldots a_1 a_0-\ldots 00 a_n a_{n-1}\ldots a_1 a_0=$$
$$=\ldots a_{n+2}a_{n+1}\underbrace{00\ldots.0}_{n+1}=\ldots. a_{n+2}a_{n+1}\cdot(10_m)^{n+1}.$$

Если определить модуль этой разности как $\dfrac{1}{(10_m)^{n+1}}=\dfrac{1}{m^{n+1}}$, то при $n\to\infty$ получим $|\alpha-S_n|=\dfrac{1}{m^{n+1}}\to 0$ и можно считать, по определению, что $\alpha=\lim\limits_{n\to\infty} S_n$. Таким образом, α будет суммой указанного выше ряда,

откуда и вытекает равенство (1). Осуществим эту идею. Вместе с тем, «модуль» m-адического числа α будем называть *m-адической нормой* и обозначать $|\alpha|_m$.

Для осуществления задуманного нам нужно ввести некоторую стандартную запись m-адического числа.

5.8.8. Определение. *Стандартной формой* m-адического числа $\alpha \neq 0$ называется запись его в виде $\alpha = \alpha' \cdot (10_m)^n$, где n — некоторое целое число, а α' — целое m-адическое число, не оканчивающееся нулем.

5.8.9. Определение. Будем считать, что *m-адическая норма* числа 0 равна нулю, и писать: $|0|_m = 0$. Если же m-адическое число $\alpha \neq 0$ и $\alpha = \alpha' \cdot (10_m)^n$ — стандартная форма числа α, то определим его *m-адическую норму* как $|\alpha|_m = \dfrac{1}{m^n}$.

5.8.10. Определение. m-адическое число α называется пределом последовательности m-адических чисел $(\beta_{(n)})$ по m-адической норме $|\ |_m$, если для любого рационального числа $\varepsilon > 0$ существует номер n_0 такой, что для всех $n > n_0$ выполняется неравенство $|\alpha - \beta_{(n)}|_m < \varepsilon$.

Здесь $\beta_{(n)}$ означает n-й член последовательности $(\beta_{(n)})$. Номера членов последовательности мы вынуждены заключать в скобки, поскольку обозначение β_n уже занято и является записью приближенного значения m-адического числа β.

5.8.11. Определение. m-адическое число β называется *суммой ряда* $\beta_{(0)} + \beta_{(1)} + \ldots + \beta_{(n)} + \ldots$, если $\beta = \lim\limits_{n\to\infty} S_n$, где $S_n = \beta_{(0)} + \beta_{(1)} + \ldots + \beta_{(n)}$ — *частичная сумма данного ряда*. При этом пишут: $\beta = \beta_{(0)} + \beta_{(1)} + \ldots + \beta_{(n)} + \ldots$.

Теперь у нас все готово для осуществления задуманного: трактовки m-адического числа как «суммы разрядных единиц».

5.8.12. Теорема. *Если m-адическое число $\alpha = \ldots a_n a_{n-1} \ldots a_1 a_0$, то α есть сумма ряда*: $\alpha = a_0 + a_1(10_m) + \ldots + a_n(10_m)^n + \ldots$.

Доказательство. Частичная сумма рассматриваемого ряда равна $S_n = a_0 + a_1(10_m) + \ldots + a_n(10_m)^n = a_n \ldots a_1 a_0 = a_n \ldots a_1 a_0$ и $\alpha - S_n = \ldots a_n a_{n-1} \ldots a_1 a_0 - a_n \ldots a_1 a_0 = \ldots a_{n+2} a_{n+1} \underbrace{00\ldots0}_{n+1} = \ldots a_{n+2} a_{n+1} \cdot (10_m)^{n+1}$. Отсюда $|\alpha - S_n|_m \le \dfrac{1}{m^{n+1}} \to 0$ при $n \to \infty$. Следовательно, $\alpha = \lim\limits_{n\to\infty} S_n$. Но это и означает, что $\alpha = a_0 + a_1(10_m) + \ldots + a_n(10_m)^n + \ldots$. □

5.8.13. Следствие. *Если $\alpha = \ldots a_n a_{n-1} \ldots a_1 a_0, a_{-1} a_{-2} \ldots a_{-k}$, то*

$$\alpha = \frac{a_{-k}}{(10_m)^k} + \ldots + \frac{a_{-2}}{(10_m)^2} + \frac{a_{-1}}{(10_m)} + a_0 + a_1(10_m) + \ldots + a_n(10_m)^n + \ldots .$$

Нормированные поля

Введенное выше понятие m-адической нормы появилось как аналог модуля числа. Однако аналог привычного свойства модуля: «модуль произведения равен произведению модулей» для m-адической

нормы при составном m не имеет места. В самом деле, например, при $m = 10$ имеем: $|2|_{10} = 1$, $|5|_{10} = 1$, а $|2 \cdot 5|_{10} = |10|_{10} = \frac{1}{10} \neq |2|_{10} \cdot |5|_{10}$. Если же $m = p$ — простое число, то все в порядке. Отметим основные свойства p-адической нормы при простом p.

5.8.14. Теорема. *Пусть дано поле p-адических чисел Q_p при некотором простом p с p-адической нормой $|\ |_p$. Для любых $\alpha, \beta \in P$ имеем:*

1) $|\alpha|_p = 0 \Leftrightarrow \alpha = 0$;

2) $|\alpha \cdot \beta|_p = |\alpha|_p \cdot |\beta|_p$;

3) $|\alpha + \beta|_p \leq \max\{|\alpha|_p, |\beta|_p\}$.

Доказательство. Свойства 1) и 2) доказываются совсем просто. Докажем свойство 3). Если хотя бы одно из p-адических чисел α, β равно нулю, то утверждение очевидно. Пусть $\alpha \neq 0$, $\beta \neq 0$ и $\alpha = \alpha' \cdot (10_p)^k$, $\beta = \beta' \cdot (10_p)^n$ — стандартные формы чисел α и β, и пусть $k \leq n$. Тогда $|\alpha|_p = \frac{1}{p^k} \geq \frac{1}{p^n} = |\beta|_p$, так что $\max\{|\alpha|_p, |\beta|_p\} = |\alpha|_p$. С другой стороны, имеем: $\alpha + \beta = \alpha' \cdot (10_p)^k + \beta' \cdot (10_p)^n = (\alpha' + \beta' \cdot (10_p)^{n-k}) \cdot (10_p)^k$, и если $\alpha + \beta = \gamma \cdot (10_p)^l$ — стандартная форма числа $\alpha + \beta$, то $k \leq l$. Следовательно, $|\alpha + \beta|_p = \frac{1}{p^l} \leq \frac{1}{p^k} = |\alpha|_p$. □

Так как $Q \subset Q_p$, то p-адическая норма на поле p-адических чисел индуцирует p-адическую норму на поле рациональных чисел. Пусть, например, $p = 7$, найдем 7-адическую норму числа $a = 2597_{10}$. Запишем его в виде целого 7-адического числа:

$$
\begin{array}{l}
\_2597 \mid \underline{7} \\
\ \ \underline{21}\ \ \ \_371 \mid \underline{7} \\
\_49\ \ \ \underline{35}\ \ \_53 \mid \underline{7} \\
\ \ \underline{49}\ \ \ \_21\ \ \underline{49}\ \ 7 \mid \underline{7} \\
\ \ \_7\ \ \ \ \underline{21}\ \ \ \ 4\ \ \underline{7}\ \ 1 \\
\ \ \ \underline{7}\ \ \ \ \ 0\ \ \ \ \ 0 \\
\ \ \ 0
\end{array}
$$

Таким образом, $a = 2597_{10} = \ldots.0010400_7 = \ldots.00104 \cdot (10_7)^2$ — стандартная форма числа a в Q_7. Следовательно, $|a|_7 = \frac{1}{7^2}$. Замечаем, что если $a_1 = \ldots.00104_7$, то $a = a_1 \cdot 7^2$ и $(a_1, 7) = 1$. Из этого примера подмечаем, что для нахождения p-адической нормы целого числа $a \neq 0$ его надо представить в виде $a = a_1 \cdot p^n$, где $(a_1, p) = 1$, и тогда $|a|_p = \frac{1}{p^n}$.

Пусть теперь дано рациональное число $\alpha = \frac{a}{b}$, где a и b целые, $b \neq 0$. Тогда $\alpha \cdot b = a$, откуда $|\alpha \cdot b|_p = |\alpha|_p \cdot |b|_p = |a|_p$. Следовательно, $|\alpha|_p = \frac{|a|_p}{|b|_p}$.

Представим a и b в виде $a = a_1 \cdot p^n$, $b = b_1 \cdot p^m$, где $(a_1, p) = 1$, $(b_1, p) = 1$. Тогда $\frac{a}{b} = \frac{a_1 \cdot p^n}{b_1 \cdot p^m} = \frac{a_1}{b_1} p^{n-m}$, $|a|_p = \frac{1}{p^n}$, $|b|_p = \frac{1}{p^m}$ и $|\alpha|_p = \frac{|a|_p}{|b|_p} = \frac{p^m}{p^n} = \frac{1}{p^{n-m}}$. Отсюда вытекает следующая стратегия нахождения p-адической нормы ненулевого рационального числа $\frac{a}{b}$: нужно его представить в виде $\frac{a}{b} = \frac{a_1}{b_1} p^k$, где НОД $(a_1, p) = 1$, НОД$(b_1, p) = 1$, и тогда $\left|\frac{a}{b}\right|_p = \frac{1}{p^k}$.

Итак, на элементах поля рациональных чисел Q можно определить понятие модуля числа обычным способом $|\ |$ и в виде p-адической нормы $|\ |_p$. Введем общее понятие, объединяющее оба примера.

5.8.15. Определение. Поле P называется *нормированным*, если для каждого элемента $a \in P$ однозначно определено неотрицательное действительное число $\|a\|$, называемое *нормой элемента* a, причем выполняются следующие условия:

$$\|a\| = 0 \Leftrightarrow a = 0;$$

$$\|a \cdot b\| = \|a\| \cdot \|b\|;$$

$$\|a + b\| \le \|a\| + \|b\|.$$

Заметим, что это определение можно сделать еще более общим, если в нем $\|a\|$ определить как неотрицательный элемент фиксированного упорядоченного поля.

Норма $\|\ \|$ называется *тривиальной*, если $\|0\| = 0$ и $\|a\| = 1$ для всякого $a \neq 0$. Таким образом, поле рациональных чисел может быть превращено в нормированное поле по меньшей мере тремя принципиально различными способами: введением тривиальной нормы, введением нормы $|\ |$ или нормы $|\ |_p$. Теорема Островского утверждает, что на поле рациональных чисел этими примерами по существу исчерпываются все возможные нормы. Но прежде чем привести эту теорему, введем необходимые понятия.

5.8.16. Определение. Элемент a нормированного поля P с нормой $\|\ \|$ называется *пределом последовательности* (a_n) *по норме* $\|\ \|$, если для любого рационального числа $\varepsilon > 0$ существует номер n_0 такой, что для всякого $n > n_0$ выполняется неравенство $\|a - a_n\| < \varepsilon$. При этом пишут: $\lim\limits_{n \to \infty} a_n = a$, непременно добавляя: *по норме* $\|\ \|$. Последовательность (a_n) называют *сходящейся по норме* $\|\ \|$ (к элементу a).

5.8.17. Определение. Пусть дано нормированное поле P с нормой $\|\ \|$. Последовательность элементов (a_n) поля P называется *фундаментальной по норме* $\|\ \|$ (или *последовательностью Коши*), если для любого рационального числа $\varepsilon > 0$ существует номер n_0 такой, что для всех номеров $k > n_0$, $m > n_0$ выполняется неравенство $\|a_k - a_m\| < \varepsilon$.

5.8.18. Определение. Пусть дано нормированное поле P с нормой $\| \|$. Две фундаментальные по норме $\| \|$ последовательности (a_n) и (b_n) называются *эквивалентными по норме* $\| \|$, если $\lim\limits_{n\to\infty}(a_n - b_n) = 0$.

Легко доказать, что так определенное отношение на множестве всех фундаментальных последовательностей рефлексивно, симметрично и транзитивно, т. е. является отношением эквивалентности. Таким образом, множество всех фундаментальных последовательностей разбивается на классы эквивалентных последовательностей.

5.8.19. Определение. Два нормирования поля P называются *эквивалентными*, если классы эквивалентных по той и другой норме фундаментальных последовательностей совпадают.

5.8.20. Теорема Островского. *Каждая нетривиальная норма* $\| \|$ *на поле рациональных чисел* Q *эквивалентна либо* p*-адической норме* $| |_p$, *либо норме* $| |$.

Доказательство теоремы мы опускаем (его можно найти, например, в [7]).

Обратим внимание на условие 3) в определении 5.8.15 и заметим, что p-адическая норма $| |_p$ на поле p-адических чисел Q_p (а значит, и на поле рациональных чисел Q) удовлетворяет более сильному условию, доказанному в теореме 5.8.14: $|\alpha+\beta|_p \le \max\left\{|\alpha|_p, |\beta|_p\right\}$ для любых $\alpha, \beta \in Q_p$. Это приводит к следующему общему понятию.

5.8.21. Определение. Норма $\| \|$ нормированного поля P называется *неархимедовой*, если $\|a+b\| \le \max\{\|a\|, \|b\|\}$ для любых элементов $a, b \in P$. В противном случае норма называется *архимедовой*.

Таким образом, p-адическая норма $| |_p$ на поле p-адических чисел Q_p является примером неархимедовой нормы, а норма $| |$ на поле действительных чисел R является архимедовой.

Абстрактная характеризация поля p-адических чисел и поля действительных чисел с помощью понятия нормы

Перепишем для нормированного поля определение суммы ряда. Это поможет нам абстрактно (аксиоматически) охарактеризовать поле p-адических чисел.

5.8.22. Определение. Элемент a нормированного поля P с нормой $\| \|$ называется *суммой ряда* $a_0 + a_1 + \ldots$ *по норме* $\| \|$, если $a = \lim\limits_{n\to\infty} S_n$ по норме $\| \|$, где $S_n = a_0 + a_1 + \ldots + a_n$ — *частичная сумма ряда.*

5.8.23. Определение. Пусть дано нормированное поле P с неархимедовой нормой $\| \|$, содержащее поле рациональных чисел Q. Будем говорить, что *элемент* $a \in P$ *представим в виде* p*-адического числа* $\alpha = \ldots a_m a_{m-1} \ldots a_0, a_{-1} \ldots a_{-k}$ *по неархимедовой норме* $\| \|$, если a есть сумма ряда по норме $\| \|$: $a = a_{-k}(10_p)^{-k} + \ldots + a_{-1}(10_p)^{-1} + a_0 + a_1(10_p) + \ldots + a_m(10_p)^m + \ldots$.

Введем аналогичное понятие представимости элемента нормированного поля десятичной дробью.

5.8.24. Определение. Пусть дано нормированное поле P с архимедовой нормой $\| \ \|$, содержащее поле рациональных чисел Q. Будем говорить, что *элемент $a \in P$ представим в виде десятичной дроби $a_0, a_1 a_2 \ldots$ по архимедовой норме $\| \ \|$*, если a есть сумма ряда по норме $\| \ \|$: $a = a_0 + a_1 10^{-1} + a_2 10^{-2} + \ldots$.

5.8.25. Теорема. *Поле P изоморфно полю p-адических чисел Q_p тогда и только тогда, когда P содержит поле рациональных чисел Q и на P можно так определить нетривиальную неархимедову норму $\| \ \|$, что всякий элемент из P представим в виде единственного p-адического числа и всякое p-адическое число является представлением единственного элемента из P.*

Доказательство. ($\Rightarrow$) Пусть φ — изоморфизм поля P на поле p-адических чисел Q_p. Поскольку поле Q_p содержит поле рациональных чисел, то таким же свойством обладает и поле P. Не нарушая общности, можно считать, что Q_p и P содержат поле рациональных чисел Q и φ действует на нем тождественно.

Для любого $a \in P$ положим $\|a\| = |\varphi(a)|_p$. Тогда $\|a\| = 0 \Leftrightarrow |\varphi(a)|_p = 0 \Leftrightarrow \varphi(a) = 0 \Leftrightarrow a = 0$. Далее, для любых $a, b \in P$ имеем: $\|a \cdot b\| = |\varphi(a \cdot b)|_p = |\varphi(a) \cdot \varphi(b)|_p = |\varphi(a)|_p \cdot |\varphi(b)|_p = \|a\| \cdot \|b\|$. Наконец, $\|a + b\| = |\varphi(a + b)|_p = |\varphi(a) + \varphi(b)|_p \le \max\{|\varphi(a)|_p, |\varphi(b)|_p\} = \max\{\|a\|, \|b\|\}$. Следовательно, $\| \ \|$ — нетривиальная неархимедова норма на поле P.

Пусть $\varphi(a) = \alpha$. По следствию 5.8.13, α является пределом последовательности своих приближенных значений: $\alpha = \lim\limits_{n \to \infty} \alpha_n$ по норме $| \ |_p$. Это означает, что для любого рационального числа $\varepsilon > 0$ существует номер n_0 такой, что для всех номеров $n > n_0$ выполняется неравенство $|\alpha - \alpha_n|_p < \varepsilon$. Отсюда следует $|\varphi(a) - \varphi(\alpha_n)|_p = |\varphi(a - \alpha_n)|_p < \varepsilon$, откуда $\|a - \alpha_n\| < \varepsilon$. Таким образом, $a = \lim\limits_{n \to \infty} \alpha_n$ по норме $\| \ \|$, откуда следует, что элемент a представим в виде p-адического числа α. Если предположить, что элемент a представим в виде p-адического числа β, то по определениям 5.8.24 и 5.8.23 $a = \lim\limits_{n \to \infty} \beta_n$ по норме $\| \ \|$. Это означает, что для любого рационального числа $\varepsilon > 0$ существует номер n_0 такой, что для всех номеров $n > n_0$ выполняется неравенство $\|a - \beta_n\| < \varepsilon$. Но тогда $|\varphi(a - \beta_n)|_p = |\varphi(a) - \varphi(\beta_n)|_p = |\varphi(a) - \beta_n)|_p < \varepsilon$, откуда $\alpha = \varphi(a) = \lim\limits_{n \to \infty} \varphi(\beta_n) = \lim\limits_{t \to \infty} \beta_n = \beta$ по норме $| \ |_p$ в Q_p.

Так как φ является отображением на Q_p, то для любого $\alpha \in Q_p$ существует элемент $a \in P$ такой, что $\varphi(a) = \alpha$. По доказанному, элемент a представим в виде p-адического числа α. Если предположить, что элемент $b \in P$ представим в виде p-адического числа α, то из единственности суммы ряда вытекает $a = b$.

($\Leftarrow$) Пусть поле P содержит поле рациональных чисел Q и на P так определена нетривиальная неархимедова норма $\| \ \|$, что всякий элемент из P представим в виде единственного p-адического числа и всякое p-адическое число является представлением единственного элемента из P. По теореме Островского, норма $\| \ \|$ на Q эквивалентна q-адической норме $| \ |_q$ при некотором простом q. По условию для любого p-адического числа $\beta = \ldots b_2 b_1 b_0$ существует элемент $b \in P$, который представим в виде p-адического числа β, т. е. $b = b_0 + b_1 10_p + b_2 (10_p)^2 + \ldots$ по норме $\| \ \|$. Отсюда следует, что последовательность (β_n) фундаментальна по норме $\| \ \|$, а значит, и по эквивалентной ей норме $| \ |_q$. Итак, последовательность приближенных значений (β_n) фундаментальна по норме $| \ |_p$ и по норме $| \ |_q$. Отсюда вытекает, что $p = q$.

Для любого $a \in P$ положим $\varphi(a) = \alpha$, если элемент a представим в виде p-адического числа $a \in Q_p$. Из условий следует, что φ является взаимно однозначным отображением P на Q_p. Можно считать, что поля P и Q_p содержат одно и то же поле рациональных чисел Q и φ является на нем тождественным отображением.

Докажем, что φ сохраняет операции сложения и умножения. Обозначим $\varphi(a) = \alpha$, $\varphi(b) = \beta$ и пусть $\alpha + \beta = \gamma$. Из определения сложения p-адических чисел вытекает, что $\lim\limits_{n\to\infty}(\alpha_n + \beta_n) = \lim\limits_{n\to\infty} \gamma_n$ по норме $| \ |_p$. Отсюда следует, что это равенство имеет место и в P по норме $\| \ \|$. Таким образом, по норме $\| \ \|$ имеем: $a + b = \lim\limits_{n\to\infty} \alpha_n + \lim\limits_{n\to\infty} \beta_n = \lim\limits_{n\to\infty}(\alpha_n + \beta_n) = \lim\limits_{n\to\infty} \gamma_n$. Но это означает, что элемент $a + b$ представим в виде p-адического числа γ. Следовательно, $\varphi(a + b) = \gamma = \alpha + \beta = \varphi(a) + \varphi(b)$.

Для умножения рассуждения аналогичны. Таким образом, φ является изоморфизмом поля P на поле p-адических чисел Q_p. □

Аналогично доказывается слдующая теорема.

5.8.26. Теорема. *Поле P изоморфно полю действительных чисел R тогда и только тогда, когда P содержит поле рациональных чисел Q и на P можно так определить нетривиальную архимедову норму $\| \ \|$, что всякий элемент из P представим в виде некоторой десятичной дроби и всякая десятичная дробь является представлением некоторого элемента из P.*

Теоремы 5.8.26 и 5.8.27 позволяют сформулировать следующие аксиоматические определения системы p-адических чисел и системы действительных чисел.

5.8.27. Определение. *Системой p-адических чисел* называется нормированное поле с неархимедовой нормой, содержащее поле рациональных чисел, всякий элемент которого однозначно представим в виде некоторого p-адического числа и всякое p-адическое число является представлением единственного элемента этого нормированного поля.

5.8.28. Определение. *Системой действительных чисел* называется нормированное поле с архимедовой нормой, содержащее поле рациональных чисел, всякий элемент которого однозначно представим в виде

некоторой десятичной дроби и всякая десятичная дробь является представлением единственного элемента данного нормированного поля.

В заключение наметим общую схему построения поля действительных чисел и поля p-адических чисел из поля рациональных чисел. Рассмотрим поле рациональных чисел с нетривиальной нормой $\| \ \|$. Класс эквивалентных фундаментальных по норме $\| \ \|$ последовательностей рациональных чисел, содержащий последовательность (a_n), будем обозначать через $\overline{(a_n)}$. Определим сложение и умножение классов эквивалентных последовательностей формулами: $\overline{(a_n)}+\overline{(b_n)}=\overline{(a_n+b_n)}$, $\overline{(a_n)}\cdot\overline{(b_n)}=\overline{(a_n\cdot b_n)}$. Доказывается, что в результате получаем поле, которое обозначим через $Q_{\| \ \|}$. По теореме Островского, нетривиальная норма $\| \ \|$ эквивалентна либо норме $| \ |$, либо норме $| \ |_p$. Оказывается, что $Q_{\| \ \|}$ в первом случае является полем действительных чисел, а во втором случае — полем p-адических чисел. Это придает вид логической завершенности обобщениям чисел, связанным с понятием нормы.

Тема 6
КОМПЛЕКСНЫЕ, ДВОЙНЫЕ И ДУАЛЬНЫЕ ЧИСЛА

§ 1. Комплексные числа

Формирование определения

В упорядоченном поле действительных чисел R уравнение $x^n = a$, где $n \in N$, разрешимо при любом положительном a. Но уже при $a = -1$ и $n = 2$ уравнение $x^2 = -1$ неразрешимо, так как квадрат любого неотрицательного действительного числа есть число неотрицательное. Отсутствие в R решения уравнения $x^2 = -1$ побуждает нас заняться поиском такой числовой системы, в которой оно имело бы решение. Обозначим через C искомую числовую область и сформулируем наши требования к ней.

Во-первых, элементы из C мы хотели бы складывать и умножать, а также сравнивать с помощью отношения «меньше», причем эти операции обладали бы привычными свойствами, характеризующими упорядоченное поле. Во-вторых, эта числовая система должна содержать упорядоченное поле действительных чисел. И в-третьих, в новой системе уравнение $x^2 = -1$ было бы разрешимо, т. е. существовал бы элемент $i \in C$ такой, что $i^2 = -1$. Однако, совместить все эти требования невозможно, так как в упорядоченном поле должно выполняться неравенство $i^2 \geq 0$. Придется пожертвовать отношением линейного порядка, оставив требование, чтобы C было полем.

Наконец, потребуем, чтобы C было минимальным полем с заданными свойствами. Назвав новую числовую систему системой комплексных чисел, приходим к следующему ее определению.

6.1.1. Определение. *Системой комплексных чисел* называется минимальное поле, содержащее поле действительных чисел и элемент i такой, что $i^2 = -1$. Другими словами, система $\langle C, +, \cdot \rangle$ называется системой комплексных чисел, если выполнены следующие условия:

1) $\langle C, +, \cdot \rangle$ — поле;

2) поле действительных чисел $\langle R, +, \cdot \rangle$ содержится в поле $\langle C, +, \cdot \rangle$;

3) существует элемент $i \in C$ такой, что $i^2 = -1$;

4) (свойство минимальности) если C_0 — подполе, содержащее R и i, то $C_0 = C$.

Всякий элемент из C называется *комплексным числом*, а элемент i — *мнимой единицей*. Система $\langle C, +, \cdot \rangle$ называется *полем комплексных чисел*.

6.1.2. Определение. *Числовым полем* называется всякое подполе поля комплексных чисел.

Таким образом, «самым маленьким» числовым полем является поле рациональных чисел, а «самым большим» — поле комплексных чисел.

Алгебраическая форма комплексного числа

Предположив, что поле комплексных чисел существует, докажем признак, который часто фигурирует в качестве определения системы комплексных чисел.

6.1.3. Теорема. *Система $\langle C, +, \cdot \rangle$ является системой комплексных чисел тогда и только тогда, она удовлетворяет условиям* 1)—3) *из* 6.1.1 *и следующему условию*:

4′) *всякий элемент из C представим в виде $a + bi$, где $a, b \in R$.*

Доказательство. ($\Rightarrow$) Пусть система $\langle C, +, \cdot \rangle$ является полем комплексных чисел в соответствии с определением 6.1.1. Рассмотрим в C подмножество $C_0 = \{a + bi \mid a, b \in R\}$. Оно содержит R и i, причем C_0 является подполем поля комплексных чисел $\langle C, +, \cdot \rangle$. По условию 4) из определения 6.1.1 $C_0 = C$. Поэтому всякое комплексное число представимо в виде $a + bi$, где $a, b \in R$.

($\Leftarrow$) Пусть система $\langle C, +, \cdot \rangle$ удовлетворяет условиям 1)—3) и 4′). Докажем, что она удовлетворяет условию 4). Пусть C_0 — подполе поля $\langle C, +, \cdot \rangle$, содержащее R и i. Тогда из определения подполя следует, что $a + bi \in C_0$ для любых $a, b \in R$. Отсюда по условию 4′) $C_0 = C$. □

6.1.4. Определение. Представление комплексного числа в виде $a + bi$, где $a, b \in R$, называется его *алгебраической формой*. При этом a называется его *действительной частью*, а b — *мнимой частью*.

Отсюда и название «комплексное число», т. е. комплекс из действительной части, мнимой части и мнимой единицы.

Существование поля комплексных чисел

Пусть $\overline{C} = \{(a, b) \mid a, b \in R\}$. Определим на $\overline{C}$ операции сложения $+$ и умножения $\cdot$, положив для любых (a, b), $(c, d) \in \overline{C}$,

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

Целесообразность таких определений вытекает из того, что в поле комплексных чисел, которое мы моделируем, выполняются равенства

$$(a + bi) + (c + di) = (a + c) + (b + d)i,$$
$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i.$$

6.1.5. Теорема. *Система $\langle \overline{C}, +, \cdot \rangle$ является системой комплексных чисел.*

Наметим план доказательства, реализацию которого оставляем читателю.

1. Система $\langle \overline{C}, +, \cdot \rangle$ является полем, причем нулем и единицей являются соответственно $\overline{0} = (0,0)$ и $\overline{1} = (1,0)$; противоположной для пары (a, b) будет пара $(-a, -b)$; если пара $(a,b) \neq \overline{0}$, то обратным элементом для пары (a, b) является пара $(a,b)^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2} \right)$.

2. Обозначим $\overline{R} = \{\overline{a} = (a,0) \mid a \in R\}$ и определим отображение φ, положив $\varphi(a) = (a,0)$ для любого $a \in R$. Тогда φ является изоморфизмом поля $\langle R, +, \cdot \rangle$ на $\langle \overline{R}, +, \cdot \rangle$, а поэтому последняя система является полем действительных чисел.

3. Обозначим $\overline{i} = (0,1)$, тогда $\overline{i}^2 = (0,1) \cdot (0,1) = (-1,0) = -\overline{1}$.

4. Всякий элемент из $\overline{C}$ представим в алгебраической форме: $(a,b) = (a,0) + (b,0) \cdot (0,1) = \overline{a} + \overline{b} \cdot \overline{i}$. □

§ 2. Основные свойства комплексных чисел

Единственность алгебраической формы. Об отношении линейного порядка на множестве комплексных чисел

Свойства комплексных чисел рассматриваются в курсе алгебры и теории чисел (см., например, [5]), поэтому здесь мы рассмотрим лишь два принципиально важных свойства.

6.2.1. Теорема. *Алгебраическая форма комплексного числа единственна.*

Доказательство. Пусть $a + bi = c + di$, $a, b, c, d \in R$, докажем, что $a = c$, $b = d$. Имеем: $a - c = (d - b)i$. Если предположить, что $b \neq d$, то $i = \frac{a-c}{d-b} \in R$, что невозможно, так как квадрат любого действительного числа неотрицателен. Следовательно, $b = d$, откуда $a = c$. □

6.2.2. Теорема. *На множестве комплексных чисел можно определить отношение линейного порядка так, чтобы операция сложения была монотонной, но поле комплексных чисел нельзя превратить в упорядоченное поле.*

Доказательство. На множестве комплексных чисел C определим отношение $\lhd$, положив $a + bi \lhd c + di$ тогда и только тогда, когда $a < c$ или же $a = c$, но $b < d$. Легко доказать, что система $\langle C, \lhd \rangle$ есть линейно упорядоченное множество, причем сложение монотонно.

Предположим, что на множестве комплексных чисел удалось ввести отношение линейного порядка $<$ так, что система $\langle C, +, \cdot, < \rangle$ — упорядоченное поле. По свойству трихотомии, либо $0 < i$, либо $i = 0$, либо $i < 0$. В первом случае, по свойству монотонности умножения, получаем $0 \cdot i < i \cdot i$, откуда $0 < -1$, значит, $1 < 0$. Но из $0 < -1$ следует, что $0 < (-1)^2 = 1$ — пришли к противоречию. Если $i = 0$, то $-1 = i^2 = 0$ — противоречие. Если же $i < 0$, то $0 < -i$, откуда $0 < (-i) \cdot (-i) = i^2 = -1$, что снова ведет к противоречию. □

Изоморфизм

6.2.3. Теорема. *Изоморфный образ поля комплексных чисел есть поле комплексных чисел.*

Доказательство. По 5.4.3, изоморфный образ поля действительных чисел есть поле действительных чисел, остальное сводится к несложной проверке. □

6.2.4. Теорема. *Любые два поля комплексных чисел изоморфны.*

Доказательство. Пусть даны два поля комплексных чисел $\langle C,+,\cdot\rangle$ и $\langle C_1,+,\cdot\rangle$, причем первое из них содержит поле действительных чисел $\langle R,+,\cdot\rangle$ и мнимую единицу i, а второе — поле действительных чисел $\langle R_1,+,\cdot\rangle$ и мнимую единицу i_1. В предыдущей главе установлено, что любые два поля действительных чисел изоморфны, поэтому существует изоморфизм φ поля $\langle R,+,\cdot\rangle$ на поле $\langle R_1,+,\cdot\rangle$. Используя φ, определим отображение f, положив $f(a+bi)=\varphi(a)+\varphi(b)\cdot i_1$ для любого $a+bi\in C$. Легко доказать, что f — искомый изоморфизм $\langle C,+,\cdot\rangle$ на $\langle C_1,+,\cdot\rangle$. □

Расширения числовых систем, связанные с решением уравнений

Введение целых чисел мотивировалось необходимостью обеспечить решение уравнения $a + x = b$ (не всегда разрешимого в натуральных числах), введение рациональных чисел было связано с решением уравнений вида $ax = b$ (не всегда разрешимых в целых числах), комплексных — с решением уравнения $x^2 = -1$. При введении действительных чисел также отмечались уравнения, например $x^2 = 2$, которые не разрешимы в поле рациональных чисел, но получают решение в поле действительных чисел. Однако решающую роль в формировании определения системы действительных чисел сыграли геометрические соображения: обеспечение решения задачи об измерении отрезков. Дело в том, что если бы мы, расширяя поле рациональных чисел, заботились лишь о том, чтобы получить поле, в котором разрешимо всякое уравнение с рациональными коэффициентами, то получили бы так называемое поле алгебраических чисел. Напомним, что число называется алгебраическим, если оно является корнем некоторого многочлена с рациональными (а значит, и некоторого многочлена с целыми) коэффициентами. Всякое рациональное число является алгебраическим. Действительные числа $\sqrt{2}$ и $\sqrt[3]{5}$ являются алгебраическими, а значит, их сумма, разность, произведение и частное также являются алгебраическими (найдите многочлены с целыми коэффициентами, корнями которых они являются). Вообще, множество всех алгебраических чисел замкнуто относительно сложения и умножения, причем образует поле. Действительные числа π, e не являются алгебраическими, такие числа называются *трансцендентными*. Таким образом, поле действительных чисел не совпадает с полем алгебраических чисел. С другой стороны, поле алгебраических чисел «захватывает» часть комплексных

чисел. Например, числа i, $2 + 3i$, $\sqrt{2}+3\sqrt[3]{5}i$ являются алгебраическими (докажите это). На рис. 14 показано взаимное расположение множества алгебраических чисел A и множества чисел Q, R и C.

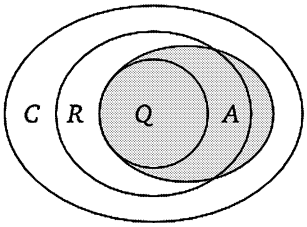

Рис. 14

Поражает неожиданностью тот факт, что во множестве действительных чисел трансцендентных чисел существенно «больше», чем алгебраических: трансцендентных чисел «столько же», сколько всех действительных чисел, в то время как алгебраических действительных чисел «столько же», сколько натуральных чисел. Точнее, множество алгебраических действительных чисел счетно, а множество трансцендентных чисел равномощно множеству всех действительных чисел, а значит, в частности, не является счетным.

При введении поля комплексных чисел мы стремились лишь обеспечить разрешимость уравнения $x^2 = -1$, но достигли большего: всякий многочлен степени большей или равной 1 с комплексными коэффициентами имеет по крайней мере один комплексный корень. В этом состоит алгебраическая замкнутость поля комплексных чисел, впервые доказанная К. Ф. Гауссом (1777—1855). Таким образом, с введением поля комплексных чисел идея расширения числовых множеств, связанная с разрешимостью уравнений, получает свое завершение. Дальнейшие расширения связаны с другими идеями.

§ 3. Двойные и дуальные числа

Определение и существование двойных и дуальных чисел

Рассмотрим числа, по форме напоминающие комплексные числа.

6.3.1. Определение. *Кольцом двойных чисел* называется коммутативное кольцо $\langle D_1, +, \cdot \rangle$, содержащее поле действительных чисел $\langle R, +, \cdot \rangle$, элемент $i_1 \notin R$ такой, что $i_1^2 = 1$ и всякий элемент из D_1 представим в виде $a + bi_1$, где $a, b \in R$. Элементы из D_1 называются *двойными числами*, а запись двойного числа в виде $a + bi_1$ называется его *алгебраической формой*.

6.3.2. Определение. *Кольцом дуальных чисел* называется коммутативное кольцо $\langle D_0, +, \cdot \rangle$, содержащее поле действительных чисел $\langle R, +, \cdot \rangle$, элемент $i_0 \notin R$ такой, что $i_0^2 = 0$ и всякий элемент из D_0 представим в виде $a + bi_0$, где $a, b \in R$. Элементы из D_0 называются *двойными*

числами, а запись двойного числа в виде $a+bi_0$ называется его *алгебраической формой*.

Для доказательства существования двойных и дуальных чисел достаточно рассмотреть множество упорядоченных пар действительных чисел $\{(a,b)\,|\,a,b\in R\}$ и определить на нем соответствующим образом операции сложения и умножения.

Общий взгляд на комплексные, двойные и дуальные числа

Следующая теорема позволяет бросить общий взгляд на комплексные, двойные и дуальные числа.

6.3.3. Теорема. *Следующие утверждения эквивалентны*:

1) *система* $\langle K,+,\cdot\rangle$ *есть либо поле комплексных чисел, либо кольцо двойных чисел, либо кольцо дуальных чисел*;

2) *система* $\langle K,+,\cdot\rangle$ *есть коммутативное кольцо, которое содержит поле действительных чисел* $\langle R,+,\cdot\rangle$ *и элемент* $j\notin R$ *такой, что всякий элемент из* K *представим в виде* $a+bj$, *где* $a,b\in R$.

Доказательство. Очевидно, из 1) следует 2). Докажем, что из 2) следует 1). Пусть коммутативное кольцо $\langle K,+,\cdot\rangle$ содержит поле действительных чисел $\langle R,+,\cdot\rangle$ и элемент j такой, что $j\notin R$ и всякий элемент из K представим в виде $a+bj$, где $a,b\in R$. Тогда существуют $u,v\in R$ такие, что $j^2=u+vj$. Отсюда $j^2-vj=u$. Дополняя левую часть равенства до полного квадрата, получаем $\left(j-\frac{v}{2}\right)^2=u+\frac{v^2}{4}$. Рассмотрим три возможных случая.

1. $u+\frac{v^2}{4}<0$. Тогда $u+\frac{v^2}{4}=-k^2$ для некоторого $k\in R$ и $\left(j-\frac{v}{2}\right)^2=-k^2$. Отсюда $\left(\frac{1}{k}j-\frac{v}{2k}\right)^2=-1$. Обозначив $i=\frac{1}{k}j-\frac{v}{2k}$, будем иметь $i^2=-1$ и $j=\frac{v}{2}+ki$. Но тогда всякий элемент $a+bj\in K$ представим в виде $a+bj=a+b\left(\frac{v}{2}+ki\right)=\left(a+b\frac{v}{2}\right)+bki$. Следовательно, всякий элемент из K представим в виде $c+di$, где $c,d\in R$. Легко доказать, что всякий такой элемент, отличный от нуля, обратим. Следовательно, $\langle K,+,\cdot\rangle$ — поле комплексных чисел.

2. $u+\frac{v^2}{4}>0$. Тогда $u+\frac{v^2}{4}=-m^2$ для некоторого $m\in R$ и $\left(j-\frac{v}{2}\right)^2=m^2$. Отсюда $\left(\frac{1}{m}j-\frac{v}{2m}\right)^2=1$. Обозначив $j_1=\frac{1}{m}j-\frac{v}{2m}$, будем иметь $j_1^2=1$. Если предположить, что $j_1\in R$, то получим $j\in R$, что противоречит

условию. Следовательно, $j_1 \notin R$ и $j = \frac{\nu}{2} + mj_1$. Но тогда всякий элемент $a + bj \in K$ представим в виде $a + bj = c + dj_1$ при некоторых $c, d \in R$. Таким образом, $\langle K, +, \cdot \rangle$ — кольцо двойных чисел.

3. $u + \frac{\nu^2}{4} = 0$. Тогда $\left(j - \frac{\nu}{2}\right)^2 = 0$. Обозначив $j_0 = j - \frac{\nu}{2}$, будем иметь $j_0^2 = 0$ и $j = \frac{\nu}{2} + j_0$. Легко видеть, что $j_0 \notin R$ и всякий элемент K представим в виде $c + dj_0$, где $c, d \in R$. Таким образом, $\langle K, +, \cdot \rangle$ — кольцо дуальных чисел. □

Тема 7
АЛГЕБРЫ НАД ПОЛЕМ ДЕЙСТВИТЕЛЬНЫХ ЧИСЕЛ

§ 1. Кватернионы

Формирование определения

По аналогии с системой комплексных чисел попытаемся определить новую числовую систему, заменяя R на C. Будем искать систему $\langle K, +, \cdot \rangle$ со свойствами:

1) $\langle K, +, \cdot \rangle$ — поле;

2) в поле $\langle K, +, \cdot \rangle$ содержится поле комплексных чисел $\langle C, +, \cdot \rangle$ с мнимой единицей i ($i^2 = -1$);

3) в K существует новая мнимая единица $j \notin C$, $j^2 = -1$;

4) всякий элемент из K представим в виде $x + yj$, где x и y — комплексные числа.

Однако в поле умножение коммутативно, поэтому $(j - i)(j + i) = j^2 + ji - ij - i^2 = -1 - (-1) = 0$, а так как в поле нет делителей нуля, то $j - i = 0$ или $j + i = 0$. Отсюда либо $j = i$, либо $j = -i$, что противоречит условию 3). Таким образом, от требования коммутативности умножения придется отказаться. Этот отказ приводит к понятию кольца с делением или тела.

7.1.1. Определение. *Телом* называется ненулевое кольцо с единицей, в котором всякий ненулевой элемент имеет обратный.

Уменьшив свои требования, будем искать тело K со свойствами 2)—4). Понятно, что умножение в K зависит от правила умножения мнимых единиц i и j. Каковы должны быть эти правила? В 1843 г. Гамильтон нашел их. Оказывается, надо потребовать, чтобы $(ji)^2 = -1$.

Определение и существование системы кватернионов

7.1.2. Определение. *Системой кватернионов* называется тело $\langle K, +, \cdot \rangle$, удовлетворяющее следующим условиям:

1) оно содержит поле комплексных чисел $\langle C, +, \cdot \rangle$ с полем действительных чисел $\langle R, +, \cdot \rangle$ и мнимой единицей i, $i^2 = -1$;

2) оно содержит новую мнимую единицу j, т. е. $j \in K \setminus C$, $j^2 = -1$, причем мнимая единица j перестановочна с любым действительным числом.

3) $(ij)^2 = -1$;

4) $K = C + Cj = \{x + yj \mid x, y \in C\}$

Всякий элемент из K называется *кватернионом*, а система $\langle K, +, \cdot \rangle$ называется *телом кватернионов*.

Обозначим $ij = k$, тогда получаем $i^2 = j^2 = k^2 = ijk = -1$. Схема умножения мнимых единиц i, j, k изображена на рис. 15.

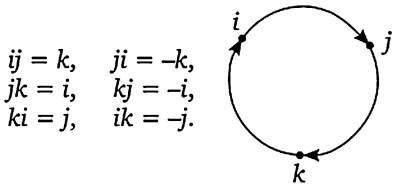

Рис. 15

Перемножая две соседние мнимые единицы в порядке, указанном стрелками, в результате получаем следующую по кругу мнимую единицу. Если же перемножить две соседние мнимые единицы против направления стрелок, то получим третью мнимую единицу со знаком «минус».

Если $x = a + bi$, $y = c + di$, $a, b, c, d \in R$, то $x + yj = (a + bi) + (c + di)j = a + bi + cj + dk$. Такое представление кватерниона называется его *алгебраической формой*. Она объясняет название «кватернион», т. е. «четверное» число.

Легко доказать, что множество единиц $G = \{1, -1, i, -i, j, -j, k, -k\}$ образует относительно умножения группу. Она называется *группой кватернионов*.

Используя свойства тела и правила умножения мнимых единиц, можно найти сумму и произведение кватернионов в алгебраической форме.

Доказывая существование тела кватернионов, в качестве «модели» кватерниона $a + bi + cj + dk$ следует взять упорядоченную четверку действительных чисел (a, b, c, d), т. е. в качестве основного множества взять $R \times R \times R \times R$. Взгляд на результаты сложения и умножения кватернионов в алгебраической форме подсказывает определение сложения и умножения упорядоченных четверок действительных чисел, чтобы получить тело кватернионов. (Проделайте это самостоятельно.)

§ 2. Общая характеризация некоторых числовых систем

Необходимые сведения из курса алгебры

Чтобы единообразно охарактеризовать действительные, комплексные, двойные, дуальные числа и кватернионы, напомним необходимые понятия, известные из курса алгебры.

7.2.1. Определение. *Векторным пространством над полем P* называется множество V, элементы которого называют векторами, причем

на V определена операция сложения векторов так, что система $\langle V, + \rangle$ является коммутативной группой, определено умножение произвольного элемента $a \in P$ на произвольный вектор $\alpha \in V$, результатом которой является вектор $a\alpha \in V$ (т. е. определено отображение $P \times V \to V$), и выполняются следующие условия: для любых $a, b \in P$ и любых векторов $\alpha, \beta \in P$

$$(ab)\alpha = a(b\alpha),\ a(\alpha+\beta) = a\alpha + a\beta,\ (a+b)\alpha = a\alpha + b\alpha,\ 1\alpha = \alpha,$$

где 1 — единица поля P. При этом говорят кратко: «V есть векторное пространство над полем P». Нулевой элемент группы $\langle V, + \rangle$ называется *нулевым вектором*, будем обозначать его через θ.

Напомним одно свойство векторного пространства, которое будем использовать в дальнейшем.

7.2.2. Предложение. *Пусть дано векторное пространство V над полем P и $a \in P$, $\alpha \in V$. Тогда $a\alpha = 0$ тогда и только тогда, когда $a = 0$ или $\alpha = \theta$.*

Напомним также, что система векторов $\alpha_1, \alpha_2, \ldots, \alpha_n$ из V называется *линейно зависимой*, если существуют $a_1, a_2, \ldots, a_n \in P$, среди которых имеются отличные от нуля, такие что $a_1\alpha_1 + a_2\alpha_2 + \ldots + a_n\alpha_n = \theta$. В противном случае система векторов называется *линейно независимой*. Таким образом, система векторов $\alpha_1, \alpha_2, \ldots, \alpha_n$ является линейно независимой, если из того, что $a_1\alpha_1 + a_2\alpha_2 + \ldots + a_n\alpha_n = \theta$, следует, что $a_1 = 0,\ a_2 = 0, \ldots, a_n = 0$.

Максимальная линейно независимая система векторов называется *базисом* векторного пространства. Любые два базиса содержат одинаковое количество векторов. *Размерностью* векторного пространства называется число векторов его базиса. Векторное пространство называется *n-мерным*, если его размерность равна n.

Из курса алгебры известно следующее.

7.2.3. Предложение. *Любые $n + 1$ векторов n-мерного векторного пространства линейно зависимы.*

Напомним, что многочлен степени $n \geq 1$ с коэффициентами из поля P называется *неприводимым* над данным полем, если он не представим в виде произведения двух многочленов степени ≥ 1 над тем же полем. В курсе алгебры доказывается следующее.

7.2.4. Предложение. *Неприводимыми над полем комплексных чисел являются многочлены первой степени, и только они. Неприводимыми над полем действительных чисел являются только многочлены первой степени и второй степени с отрицательными дискриминантами.*

Характеризация комплексных, двойных и дуальных чисел как алгебр над полем действительных чисел

Обратим внимание на то, что множество действительных чисел можно рассматривать как 1-мерное векторное пространство над полем R, множество комплексных чисел, а также множества двойных и дуальных чисел — как 2-мерные векторные пространства над полем R, а множество кватернионов — как 4-мерное векторное пространство

над полем R. Но, кроме того, двойные и дуальные числа образуют кольца, R и C являются полями, а множество кватернионов является телом. Пытаясь охватить эти частные примеры некоторым общим понятием, приходим к следующему определению.

7.2.5. Определение. *Алгеброй над полем P* называется кольцо $\langle A, +, \cdot \rangle$, аддитивная группа которого $\langle A, + \rangle$ является n-мерным векторным пространством над полем P, причем для любого $a \in P$ и любых $\alpha, \beta \in A$ выполняются равенства $(a\alpha)\cdot\beta = \alpha\cdot(a\beta) = a(\alpha\cdot\beta)$. При этом говорят кратко: «*A есть алгебра над полем P*». *Рангом* алгебры A над полем P называется размерность n векторного пространства A. Обозначается $\operatorname{rang} A = n$. Единица ε кольца $\langle A, +, \cdot \rangle$ называется *единицей* алгебры.

Очевидно, R есть алгебра над полем R ранга 1, комплексные, двойные и дуальные числа являются алгебрами над полем R ранга 2, а алгебра кватернионов над полем R имеет ранг 4.

7.2.6. Лемма. *Алгебра A с единицей ε над полем P содержит подполе $H = \{a\varepsilon \mid a \in P\}$, изоморфное полю P. Отождествляя соответствующие при этом изоморфизме элементы, можно считать, что поле $\langle P, +, \cdot \rangle$ содержится в кольце $\langle A, +, \cdot \rangle$ и всякий элемент из P перестановочен со всяким элементом из A.*

Доказательство. Легко видеть, что множество $H = \{a\varepsilon \mid a \in P\}$ является подполем, а отображение $\varphi : P \to H$, при котором $\varphi(a) = a\varepsilon$ для любого $a \in P$, является, в силу 7.2.2, взаимно однозначным отображением P на H. Кроме того, как легко проверить, φ сохраняет операции сложения и умножения. Таким образом, φ является изоморфизмом P на H. Отождествим соответствующие при φ элементы a и $a\varepsilon$. Тогда для любого элемента $\alpha \in A$ имеем $a + \alpha = a\varepsilon + \alpha$, $a\cdot\alpha = a\varepsilon\cdot\alpha = a(\varepsilon\cdot\alpha) = a\alpha$ и $\alpha\cdot a = \alpha\cdot a\varepsilon = a(\alpha\cdot\varepsilon) = a\alpha$. Таким образом, можно считать, что поле $\langle P, +, \cdot \rangle$ содержится в кольце $\langle A, +, \cdot \rangle$, причем всякий элемент из P перестановочен со всяким элементом из A. □

7.2.7. Теорема. *Алгебра с единицей, отличной от нуля, над полем действительных чисел ранга 2 есть либо алгебра комплексных чисел, либо алгебра дуальных чисел, либо алгебра двойных чисел.*

Доказательство. Пусть A — алгебра с единицей ε (отличной от нуля) ранга 2 над полем R. Тогда она имеет базис $\{\varepsilon, j\}$ и всякий элемент из A представим в виде $a\varepsilon + bj$ при некоторых $a, b \in R$. Отождествление элементов a и $a\varepsilon$ для любого $a \in R$ приводит к равенству $a\varepsilon + bj = a + bj$. Пользуясь перестановочностью действительных чисел с элементами из A, получаем перестановочность любых элементов из A. Теперь утверждение теоремы вытекает из 6.3.3. □

Общий взгляд на действительные, комплексные числа и кватернионы

Обратимся к алгебрам действительных, комплексных чисел и кватернионов. В каждой из них возможно деление. Это приводит к следующему общему понятию, которое поможет нам единообразно охарактеризовать эти алгебры.

7.2.8. Определение. *Алгеброй с делением* называется алгебра A над полем P в случае, когда кольцо $\langle A, +, \cdot \rangle$ является телом.

7.2.9. Теорема Фробениуса. *Алгебра A над полем R является алгеброй с делением конечного ранга над полем действительных чисел тогда и только тогда, когда $\langle A, +, \cdot \rangle$ есть либо поле действительных чисел, либо поле комплексных чисел, либо тело кватернионов.*

Доказательство. ($\Leftarrow$) Очевидно, поле действительных чисел, поле комплексных чисел и тело кватернионов являются алгебрами с делением над полем действительных чисел рангов соответственно 1, 2 и 4.

($\Rightarrow$) Пусть алгебра A над полем R является алгеброй с делением конечного ранга над полем действительных чисел. Докажем, что A есть либо поле действительных чисел, либо поле комплексных чисел, либо тело кватернионов. Доказательство разобьем на ряд лемм (7.2.10—7.2.15).

Начнем с очевидного факта, который непосредственно следует из 7.2.6.

7.2.10. Лемма. *Если A есть алгебра с делением над полем R ранга 1, то $\langle A, +, \cdot \rangle$ является полем действительных чисел.*

7.2.11. Лемма. *Всякий ненулевой элемент алгебры с делением A конечного ранга над полем P является корнем некоторого многочлена, неприводимого над этим полем.*

Доказательство. Пусть $\operatorname{rang} A = n$ и $0 \neq \alpha \in A$. По 7.2.3 элементы $\alpha^0 = 1, \alpha, \ldots, \alpha^n$ линейно зависимы, т. е. существуют не равные одновременно нулю элементы $a_0, a_1, \ldots, a_n$ поля P такие, что $a_0 1 + a_1 \alpha + \ldots + a_n \alpha^n = 0$. Следовательно, α является корнем многочлена $a_0 + a_1 x + \ldots + a_n x^n$. Обозначим через $\varphi(x)$ многочлен наименьшей степени из $P[x]$, имеющий корень α. Тогда степень $\varphi(x)$ не меньше единицы. Предположим, что многочлен $\varphi(x)$ приводим над P: $\varphi(x) = \varphi_1(x) \cdot \varphi_2(x)$, где $\varphi_1(x), \varphi_2(x) \in P[x]$ и степень каждого из многочленов $\varphi_1(x)$ и $\varphi_2(x)$ не меньше единицы. Тогда $0 = \varphi(\alpha) = \varphi_1(\alpha) \cdot \varphi_2(\alpha)$, а так как тело не имеет делителей нуля, то $\varphi_1(\alpha) = 0$ или $\varphi_2(\alpha) = 0$, т. е. α оказывается корнем многочлена, степень которого меньше степени $\varphi(x)$ — пришли к противоречию. Следовательно, $\varphi(x)$ неприводим над P.

7.2.12. Лемма. *Если A — алгебра с делением конечного ранга над полем комплексных чисел C, то $A = C$.*

Доказательство. По 7.2.6, $C \subseteq A$. Далее, по 7.2.11, всякий отличный от нуля элемент $\alpha \in A$ является корнем некоторого неприводимого над C многочлена $\varphi(x) \in C[x]$. По 7.2.4, степень этого многочлена равна единице, т. е. $\varphi(x) = ax + b$ при некоторых $a, b \in C$, $a \neq 0$. Но тогда $0 = \varphi(\alpha) = a\alpha + b$, откуда $\alpha = -\dfrac{b}{a} \in C$. Следовательно, $A = C$.

7.2.13. Лемма. *Если алгебра с делением A над полем R имеет ранг больше* единицы, *то она содержит поле комплексных чисел.*

Доказательство. По лемме 7.2.6, $R \subseteq A$, а так как $\operatorname{rang} A > 1$, то $A \neq R$. Пусть $\alpha \in A \setminus R$. По 7.2.11, α является корнем некоторого неприводимого над R многочлена $\varphi(x) \in R[x]$, а по 7.2.4 степень $\varphi(x)$ равна либо единице,

либо двум. Но в первом случае $\varphi(x) = ax + b$, $a \neq 0$, откуда $0 = \varphi(\alpha) = a\alpha + b$ и $\alpha = -\frac{b}{a} \in R$ — противоречие. Во втором случае $\varphi(x) = ax^2 + bx + c \cdot a \neq 0$ и дискриминант $b^2 - 4ac < 0$. Но тогда $4ac - b^2 > 0$ и существует число $d \in R$ такое, что $d^2 = 4ac - b^2$. Имеем $0 = \varphi(\alpha) = a\alpha^2 + b\alpha + c$, откуда $0 = 4a^2\alpha^2 + 4ab\alpha + 4ac = (2a\alpha + b)^2 + 4ac - b^2 = (2a\alpha + b)^2 + d^2$ и $\frac{(2a\alpha + b)^2}{d^2} = -1$. Обозначим $i = \frac{2a\alpha + b}{d}$, тогда $i^2 = -1$. Вместе с тем, $C = R + Ri$ — поле комплексных чисел, содержащееся в A.

7.2.14. Лемма. *Если A есть алгебра с делением над полем R и* $\operatorname{rang} A = 2$, *то A является полем комплексных чисел.*

Доказательство. По 7.2.13, $C \subseteq A$. Но $\operatorname{rang} C = 2 = \operatorname{rang} A$, откуда $C = A$.

7.2.15. Лемма. *Если алгебра с делением A над полем R имеет ранг > 2, то* она *является телом кватернионов.*

Доказательство. По 7.2.13, A содержит поле комплексных чисел C. Пусть i — мнимая единица поля C. Рассмотрим множество $U = \{\alpha \in A \mid \alpha i = i\alpha\}$ и $V = \{\beta \in A \mid \beta i = -i\beta\}$. Проверкой легко установить, что для любого $\gamma \in A$ имеем $\gamma - i\gamma i \in U$, $\gamma + i\lambda i \in V$ и $\gamma = \frac{1}{2}(\gamma - iji) + \frac{1}{2}(\gamma + ii) \in U + V$. Следовательно, $A = U + V$. Если предположить, что $\delta \in (U \cap V)$, то $d \in U$, откуда $\delta i = i\delta$, и $\delta \in (U \cap V)$, откуда $\delta i = -i\delta$. Следовательно, $i\delta = -i\delta$ и $2i\delta = 0$, а так как тело не имеет делителей нуля, то $\delta = 0$. Таким образом, $U \cap V = \{0\}$.

Выясним строение подмножеств U и V. Легко видеть, что U и V являются векторными пространствами над полем R, причем U даже является алгеброй с делением над полем C (проверьте!). По 7.2.12, $U = C$.

По условию, $\operatorname{rang} A > 2$, а так как $\operatorname{rang} C = 2$ (относительно поля R), то $\operatorname{rang} V \geq 1$, т. е. V — ненулевое подпространство и существует $0 \neq \beta \in V$. По 7.2.11 β, является корнем некоторого неприводимого над R многочлена $\varphi(x)$, а по 7.2.4, его степень равна либо единице, либо двум. Но в первом случае $\varphi(x) = ax + b$, $a \neq 0$ и $0 = \varphi(\beta) = a\beta + b$, откуда $\beta = -\frac{b}{a} \in R \subset C = U$, т. е. $0 \neq \beta \in (U \cap V)$ — противоречие. Во втором случае $\varphi(x) = ax^2 + bx + c$, $a \neq 0$ и дискриминант $b^2 - 4ac < 0$. Имеем: $0 = \varphi(\beta) = a\beta^2 + b\beta + c$ и если предположить, что $b \neq 0$, то получаем $\beta = -\frac{a\beta^2 + c}{b} \in U$, так как $\beta^2 \in U$ (проверьте это). Снова приходим к противоречию с тем, что $U \cap V = \{0\}$. Остается принять, что $b = 0$, но тогда $a\beta^2 + c = 0$ и $\beta^2 = -\frac{c}{a}$. Так как дискриминант $b^2 - 4ac < 0$, то $\frac{c}{a} > 0$ и существует $d = \sqrt{\frac{c}{a}}$. Тогда $\beta^2 = -d^2$ и $\frac{\beta^2}{d^2} = -1$. Обозначив $j = \frac{\beta}{d}$, получаем $j^2 = -1$.

Докажем, что $V = Cj$. Так как $j \in V$, то $(ij)i = i(ji) = i(-ij) = -i^2 j = j$, $i(ij) = i^2 j = -j$, откуда $(ij)i = -i(ij)$, значит, $ij \in V$. Но тогда для любого $a + bi \in C$ имеем $(a + bi)j = aj + bij \in V$. Таким образом, $Cj \subseteq V$. Обратно, для любого $\beta \in V$ получаем $(\beta j)i = \beta(ji) = \beta(-ij) = -(\beta i)j = -(-i\beta)j = i(\beta j)$, отсюда $\beta j \in U = C$ и $\beta \in Cj$. Следовательно, $V = Cj$. Итак, $A = C + Cj$ и, в соответствии с определением 7.1.2, A является телом кватернионов, остается лишь заметить, что $(ij)^2 = -1$. Вместе с тем, теорема 7.2.9 доказана. □

Гиперкомплексные числа

Как уже отмечалось, расширение поля действительных чисел до поля комплексных чисел сопровождается «потерей качества»: поле комплексных чисел нельзя превратить в упорядоченное поле. Дальнейшие расширения связаны с еще большими потерями. Так, умножение кватернионов уже не коммутативно.

Теорема Фробениуса утверждает, что нельзя придумать «новую числовую систему», которая, так же как и тело кватернионов, была бы, с одной стороны, телом, а с другой — конечномерным векторным пространством над полем R. Это утверждение придает вид завершенности теории числовых систем. Однако ценой отказа от ассоциативности умножения можно получить бесконечно много неассоциативных конечномерных алгебр с делением над полем R. Если, например, в определении тела свойство ассоциативности умножения заменить на свойство альтернативности $(a \cdot a)b = a(a \cdot b)$, $(b \cdot a)a = b(a \cdot a)$ для любых элементов a, b и повторить определение 7.2.5 с учетом этих изменений, то получим определение *альтернативной* алгебры с делением над полем. В этом случае алгебру с делением в смысле определения 7.2.5 называют *ассоциативной* алгеброй с делением. Понятно, что всякая ассоциативная алгебра является альтернативной. Обобщенная теорема Фробениуса утверждает, что единственной альтернативной неассоциативной конечномерной алгеброй с делением над полем R является алгебра октав, придуманная А. Кели. Она содержит восемь базисных единиц, всякий ее элемент записывается в виде их линейной комбинации с действительными коэффициентами и реализуется как вектор из R^8.

Итак, можно сделать следующие выводы:

1) поле действительных чисел — это единственная алгебра с делением над полем действительных чисел R ранга 1;

2) поле комплексных чисел — это единственная коммутативная и ассоциативная алгебра с делением над полем R конечного ранга $r > 1$;

3) тело кватернионов — это единственная ассоциативная, но не коммутативная алгебра с делением над полем R конечного ранга;

4) алгебра октав — это единственная альтернативная, но не ассоциативная алгебра с делением над полем R конечного ранга.

Кватернионы и октавы называют *гиперкомплексными числами*, подчеркивая тем самым их родословную. Дальнейшие сведения о гиперкомплексных числах можно найти, например, в [5].

Список литературы

1. *Боревич, З. И.* Теория чисел / З. И. Боревич, И. Р. Шафаревич. — 2-е изд. — Москва : Наука, 1972.
2. *Бухштаб, А. А.* Теория чисел / А. А. Бухштаб. — 2-е изд. — Москва : Просвещение, 1966.
3. *Ван дер Варден, Б. Л.* Алгебра / Б. Л. Ван дер Варден. — Москва : Наука, 1976.
4. *Гонин, Е. Г.* Теоретическая арифметика / Е. Г. Гонин. — Москва : Учпедгиз, 1959.
5. *Ильиных, А. П.* Числовые системы : учебное пособие / А. П. Ильиных. — Екатеринбург, 2003.
6. *Кантор, И. Л.* Гиперкомплексные числа / И. Л. Кантор, А. С. Солодовников. — Москва : Наука, 1973.
7. *Клайн, М.* Математика. Утрата определенности / М. Клайн. — Москва : Мир, 1984.
8. *Коблиц, Н.* p-адические числа, p-адический анализ и дзета-функция / Н. Коблиц. — Москва : Мир, 1982.
9. *Куликов, Л. Я.* Алгебра и теория чисел : учебное пособие для педагогических институтов / Л. Я. Куликов. — Москва : Высшая школа, 1979.
10. *Ляпин, Е. С.* Алгебра и теория чисел. Ч. 1. Числа / Е. С. Ляпин, А. Е. Евсеев. — Москва : Просвещение, 1974.
11. *Куратовский К.* Теория множеств / К. Куратовский, А. Мостовский. — Москва : Мир, 1970.
12. *Мальцев, А. И.* Алгебраические системы / А. И. Мальцев. — Москва : Наука, 1970.
13. *Нечаев, В. И.* Числовые системы / В. И. Нечаев. — Москва : Просвещение, 1975.
14. *Новиков, П. С.* Элементы математической логики / П. С. Новиков. — 2-е изд. — Москва : Наука, 1973.
15. *Понтрягин, Л. С.* Обобщения чисел / Л. С. Понтрягин. — Москва : Наука, 1986.
16. *Проскуряков, И. В.* Числа и многочлены / И. В. Проскуряков. — Москва : Просвещение, 1965.
17. *Стеклов, В. А.* Математика и ее значение для человечества / В. А. Стеклов. — Москва : Издательство Юрайт, 2017.
18. *Столл, Р. Р.* Множества. Логика. Аксиоматические теории / Р. Р. Столл. — Москва : Просвещение, 1968.
19. *Феферман, С.* Числовые системы / С. Феферман. — Москва : Наука, 1971.

Наши книги можно приобрести:

Учебным заведениям и библиотекам:
в отделе по работе с вузами
тел.: (495) 744-00-12, e-mail: vuz@urait.ru

Частным лицам:
список магазинов смотрите на сайте urait.ru
в разделе «Частным лицам»

Магазинам и корпоративным клиентам:
в отделе продаж
тел.: (495) 744-00-12, e-mail: sales@urait.ru

Отзывы об издании присылайте в редакцию
e-mail: gred@urait.ru

Новые издания и дополнительные материалы доступны
на образовательной платформе «Юрайт» urait.ru,
а также в мобильном приложении «Юрайт.Библиотека»

Учебное издание

Ларин Сергей Васильевич

ЧИСЛОВЫЕ СИСТЕМЫ

Учебное пособие для вузов

Формат $70\times100\,^{1}/_{16}$.
Гарнитура «Charter». Печать цифровая.
Усл. печ. л. 10,09.

ООО «Издательство Юрайт»
111123, г. Москва, ул. Плеханова, д. 4а.
Тел.: (495) 744-00-12. E-mail: izdat@urait.ru, www.urait.ru