МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение
высшего образования

«Дальневосточный федеральный университет»

ГОРНОСТАЕВ О.М.

ЧИСЛОВЫЕ СИСТЕМЫ

(учебное пособие)

УССУРИЙСК 2018

Предисловие

Целью этого пособия является систематизация знаний студентов об основных числовых системах. В педагогических ВУЗах этот материал изучается, в основном, после, или в конце курса алгебры, что имеет свои преимущества. К этому времени накоплен богатый фактический материал, натуральные, целые, действительные и комплексные числа довольно подробно изучены в курсах алгебры и математического анализа. Достигнут и определенный уровень математической культуры. Но, вместе с тем, нет общего взгляда на истоки наших знаний о числах, на то, что понятие числа – фундамент математики. Кроме того, в основном курсе математики мало затрагиваются вопросы непротиворечивости математических теорий. Для учителя математики важно также понимать, что некая "абсолютная" непротиворечивость математики недоказуема.

Однако можно привести и доводы в пользу как можно более раннего изучения этого материала. Прежде всего, это обретение логического фундамента для таких наук, как теория чисел и математический анализ. Понимание круга рассматриваемых здесь вопросов очень желательно для изучения более тонких и сложных разделов алгебры и анализа. Поэтому, для студентов младших курсов в начале изложения приводятся необходимые определения и факты.

Мы отдаем предпочтение аксиоматическому подходу к построению и расширению числовых систем. Во многих учебных пособиях и монографиях числовые системы вводятся как конкретные алгебраические системы, то есть представлена единственная модель соответствующей системы аксиом и неясно, существуют ли другие ее модели и, если – да, то изоморфны ли они представленной? Такой подход, несомненно, сужает взгляд на проблематику в целом. Основное внимание мы уделяем самим системам аксиом, доказательству их категоричности и построению моделей и сравнительно немного времени отводим на изучение многих свойств числовых систем. Последними вопросами занимаются теория чисел, математический анализ, алгебра и т.д.

Особенностью этого пособия является большое количество упражнений, некоторые из которых призваны восполнить пробелы в доказатель-

ствах и, поэтому, появляются прямо в ходе рассуждений. Некоторые – имеют самостоятельное значение, а часть задач дается для тренировки и закрепления материала. Если в упражнении имеется лишь текст некоторого утверждения, то это утверждение надо доказать. При самостоятельном изучении желательно выполнять все упражнения именно в порядке их появления. Отметим также, что некоторые общепринятые обозначения никак не комментируются.

Материал пособия может служить основой семестрового курса, при этом многие дополнительные вопросы и часть упражнений можно рассмотреть на практических занятиях.

О.М.Горностаев

Глава 1

Основные понятия

1.1 Операции над множествами

Всюду, в дальнейшем, через $\{x|P(x)\}$ будем обозначать множество всех элементов, обладающих свойством P. Например: $\{x|x \in Z \wedge x^2 > 4\}$ — множество всех целых чисел, квадраты которых больше 4, $\{x|x \neq x\}$ — пустое множество, обозначаемое $\emptyset$, $\{a, b, c, \ldots\}$ — множество, состоящее из элементов $a, b, c \ldots$.

Буквами $A, B, C, \ldots$, или $A_1, A_2, \ldots$ будем обозначать произвольные множества. Поскольку здесь мы не обсуждаем аксиомы теории множеств, то и понятие "множество" также не обсуждается.

Определение 1. $A \cap B \stackrel{def}{=} \{x|x \in A \wedge x \in B\}$ — пересечение множеств.

Определение 2. $A \cup B \stackrel{def}{=} \{x|x \in A \vee x \in B\}$ — объединение.

Определение 3. $A \setminus B \stackrel{def}{=} \{x|x \in A \wedge x \notin B\}$ — разность.

Определение 4. $A = B \stackrel{def}{\Longleftrightarrow} \forall x(x \in A \Longleftrightarrow x \in B)$.

Определение 5. $A \subseteq B \stackrel{def}{\Longleftrightarrow} \forall x(x \in A \Longrightarrow x \in B)$.

Последнее условие часто записывают в виде:

$\forall x \in A(x \in B)$ и говорят, что множество A является подмножеством множества B.

Определение 6. Если $A \subseteq B$, то $A'_B \stackrel{def}{=} B \setminus A$ называется дополнением A в B.
Если известно, что все расматриваемые множества являются подмножествами какого-либо одного множества, то пишут A' вместо A'_B.
Если $A \subseteq B$ и $A \neq B$, то будем записывать $A \subset B$, множество A при этом называется собственным подмножеством множества B.

Упражнение 1. Доказать, что для любых множеств A, B, C выполняются следующие свойства:

1. $A \cup A = A$;
2. $A \cup B = B \cup A$;
3. $A \cup (B \cup C) = (A \cup B) \cup C$;
4. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
5. $(A')' = A$;
6. $(A \cup B)' = A' \cap B'$;
7. $A \cup (B \cap B') = A$.

Докажем, например, пятое свойство. Будем опираться на определение равенства двух множеств: $x \in (A')'$, тогда и только тогда, когда $x \notin A'$, а это верно тогда и только тогда, когда $x \in A$, следовательно, $(A')' = A$.

Упражнение 2. Доказать, что верны и равенства, двойственные к равенствам 1 - 7 из упражнения 1, то есть получающиеся из последних заменой $\cup$ на $\cap$ и наоборот.

Упражнение 3. Привести 6 примеров из школьного курса геометрии, где используются (может быть неявно) операции пересечения и объеди-

нения множеств.

Упражнение 4. Доказать утверждения:

1. $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$;
2. $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$;
3. $(A \setminus B) \setminus C = (A \setminus C) \setminus B$;
4. $(A \setminus B) \setminus C = (A \setminus C) \setminus (B \setminus C)$;
5. $(A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$;
6. $A \setminus (A \setminus B) = A \cap B$;
7. $A \setminus B = A \cap B'$;
8. $A \cup \emptyset = A$;
9. $A \cap \emptyset = \emptyset$;
10. $(A \setminus B)' = A' \cup (A \cap B)$;
11. $A \setminus B = A \iff A \cap B = \emptyset$;
12. $(A \cup B) \setminus (A \cap B) = \emptyset \iff A = B$;
13. $A = B \cup C \Longrightarrow A \setminus B \subseteq C$;
14. $A \setminus B = A \iff B \setminus A = B$;
15. $C \subseteq A \cap B \iff C \subseteq A \wedge C \subseteq B$.

Упражнение 5. Доказать, что множество $\{1, 2, \ldots, n\}$ имеет 2^n различных подмножеств.

Определение 7. Множество всех подмножеств множества A называется булеаном A и обозначается $P(A)$.

1.2 Отношения

Декартово произведение множеств

Определение 1. Декартовым произведением множеств $A_1, A_2, \ldots, A_n$ называется множество
$A_1 \times A_2 \times \ldots \times A_n \stackrel{def}{=} \{(x_1, \ldots, x_n) | x_i \in A_i, i \leq n\}$,
где $(x_1, \ldots, x_n)$ — упорядоченный набор элементов $x_1, \ldots, x_n$.

Упражнение 6. Найти $\{1, 2\} \times \{a, b, c\}$.

Упражнение 7. Изобразить на декартовой плоскости множества:

1. $[0, 1] \times [0, 2]$;
2. $(-\infty, 1) \times (-1, 1)$;
3. $[0, 1] \times (0, 2]$;
4. $(0, 1] \times \{x | x \leq 3\}$.

Упражнение 8. Доказать следующие утверждения для произвольных множеств A, B, C, D:

1. $(A \cup B) \times C = (A \times C) \cup (B \times C)$;
2. $(A \cap B) \times C = (A \times C) \cap (B \times C)$;
3. $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$;
4. $A \times B = \emptyset \Longleftrightarrow A = \emptyset \vee B = \emptyset$;
5. $A \subseteq B \Longrightarrow A \times C \subseteq B \times C$;
6. $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$.

n-местные отношения

Определение 2. Всякое подмножество множества
$A_1 \times \ldots \times A_n$ называется n-местным отношением на системе множеств $A_1, \ldots, A_n$. Если $A_1 = A_2 = \ldots A_n = A$, то декартово произведение данных множеств обозначаем A^n и называем n-й степенью множества A, а соответствующее n-местное (n-арное) отношение – n-арным отношением на множестве A.

Упражнение 9. Когда в школе впервые появляется понятие n-арного отношения, декартова произведения?

Бинарные отношения (соответствия)

Бинарные (2-х местные) отношения на паре множеств
A, B называют также соответствиями между A и B.

Определение 3. Пусть $A \times B \supseteq \rho$ — бинарное отношение на паре множеств A, B, тогда множество $D(\rho) \stackrel{def}{=} \{x|(x,y) \in \rho\}$ называется областью определения отношения ρ, а множество
$Im(\rho) \stackrel{def}{=} \{y|(x,y) \in \rho\}$ — множеством значений ρ.
Иногда, вместо $(x,y) \in \rho$ пишут $x\rho y$, или $\rho(x,y)$.

Поскольку бинарные отношения представляют собой множества пар элементов, они могут быть представлены в виде графиков, графов, таблиц.
Примеры.

1. На множествах $A_1 = A_2 = \mathbf{R}$, $\rho = \{(x,y)|y = x^2\}$. График данного отношения представляет собой параболу.

2. На паре множеств $A_1 = \{1,2,3\}$, $A_2 = \{a,b\}$,
$\rho = \{(1,a),(1,b),(2,a)\}$ граф отношения ρ выглядит так:

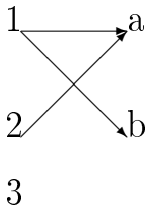


Таблица отношения ρ выглядит так:

	a	b
1	$\times$	$\times$
2	$\times$	
3		

3. Отношение параллельности на множестве всех прямых плоскости.

4. $A = \{1, 2, \ldots, 9\}$, $\rho = \{(a, b) | a \vdots b\}$.

5. $A = \{1, 2, 3\}, \rho = \{(1, 1), (1, 2), (1, 3), (2, 3), (2, 2), (3, 3)\}$.

6. A – множество всех людей, $\rho = \{(a, b) | a, b$ – однофамильцы $\}$.

Упражнение 10. Найти области определения и множества значений всех отношений из примеров 1 – 6.

Определение 4. Пусть ρ – бинарное отношение на паре множеств A, B. Тогда $\rho^{-1} \stackrel{def}{=} \{(y, x) | (x, y) \in \rho\}$ называется отношением, обратным к отношению ρ.

Упражнение 11. Найти отношения, обратные к отношениям, приведенным в примерах 1 – 6.

Свойства бинарных отношений

В дальнейшем, в этом разделе, мы будем рассматривать бинарное отношение ρ на множестве A.

Определение 5.
ρ – рефлексивно $\overset{def}{\Longleftrightarrow} \forall x \in A(x\rho x)$.

Определение 6.
ρ – симметрично $\overset{def}{\Longleftrightarrow} \forall x, y \in A(x\rho y \Longrightarrow y\rho x)$.

Определение 7.
ρ – транзитивно $\overset{def}{\Longleftrightarrow} \forall x, y, z \in A(x\rho y \wedge y\rho z \Longrightarrow x\rho z)$.

Определение 8.
ρ – антирефлексивно $\overset{def}{\Longleftrightarrow} \forall x \in A\neg(x\rho x)$.

Определение 9.
ρ – антисимметрично $\overset{def}{\Longleftrightarrow} \forall x, y \in A(x\rho y \wedge y\rho x \Longrightarrow x = y)$.

Определение 10.
ρ – связно $\overset{def}{\Longleftrightarrow} \forall x, y \in A(x\rho y \vee y\rho x \vee x = y)$.

Упражнение 12. Какими из перечисленных свойств обладает отношение перпендикулярности прямых на плоскости, скрещиваемости прямых в трехмерном пространстве ?

Упражнение 13. Какими свойствами обладают отношения из примеров 1, 3 – 6 предыдущего пункта?

Упражнение 14. Какими свойствами обладают следующие отношения на множестве $\mathbf{R}$ – действительных чисел?

1. $\rho = \{(x, y)|x = y\}$;
2. $\rho = \{(x, y)|y = x^2\}$;
3. $\rho = \{(x, y)|y = \ln x\}$;

4. $\rho = \{(x, y)|y = \sin x\}$;

5. $\rho = \{(x, y)|y = \frac{1}{x}\}$.

Упражнение 15. На множестве всех рейсовых автобусов в городе зададим отношение $\rho = \{(x, y)|x, y$ ездят по одному маршруту$\}$. Какими свойствами обладает это отношение?

1.3 Отношение эквивалентности. Фактор-множество

Определение 1. Бинарное отношение на множестве A называется отношением эквивалентности, если оно рефлексивно, симметрично и транзитивно.

Упражнение 16. Какие из рассмотренных ранее отношений являются отношениями эквивалентности (эквивалентностями)?

Упражнение 17. Привести 4 примера эквивалентностей из школьного курса геометрии и 1 пример – из алгебры.

Упражнение 18. Доказать, что отношение сравнимости целых чисел по данному модулю есть эквивалентность.

С каждым отношением эквивалентности на множестве A можно связать разбиение A на классы, т.е. на такие непустые подмножества, что каждый элемент из A содержится точно в одном из них.

Упражнение 19. Доказать, что $\{\bar{x_\rho} \mid \bar{x_\rho} = \{y|y \in A \wedge x\rho y\}\}_{x \in A}$ есть разбиение A, если ρ – эквивалентность на A.

Упражнение 20. Если $\{A_i\}_{i \in I}$ — разбиение множества A, то $\rho = \{(x, y)|x, y \in A_i, i \in I\}$ — отношение эквивалентности на A.

Определение 2. Элементы $\bar{x_\rho}$ из упр.19 называются классами эквивалентности, а x – представителем класса $\bar{x_\rho}$ по отношению эквивалентности ρ. Если ясно, о каком отношении эквивалентности идет речь, то нижний индекс в обозначении класса эквивалентности в дальнейшем писать не будем.

Упражнение 21. $\bar{x}=\bar{y} \Longleftrightarrow x \rho y$, то есть класс эквивалентности можно обозначать с помощью любого его представителя.

Упражнение 22. Найти все классы эквивалентности отношения сравнимости целых чисел по модулю 5.

Определение 3. Множество всех классов эквивалентности по отношению эквивалентности ρ на множестве A называется фактор-множеством множества A по отношению ρ и обозначается A/ρ.

Упражнение 23. Построить фактор-множества по всем отношениям эквивалентности, встречавшимся выше.

Упражнение 24. У царя Гороха было три сына. У каждого из пятидесяти его потомков было по три сына (дочерей – не было), а остальные потомки умерли бездетными. Какова численность всей династии (включая самого царя)?

Упражнение 25. Доказать, что из k натуральных чисел всегда можно выбрать несколько (может быть – одно) таких, что их сумма делится на k.

Упражнение 26. Сколько различных отношений эквивалентности можно задать на 4-х элементном множестве?

Упражнение 27. Придумайте 5 отношений эквивалентности на мно-

жестве студентов Вашей группы.

1.4 Отношение порядка. Линейный порядок

Определение 1. Антисимметричное и транзитивное отношение ρ на множестве A называется отношением (частичного) порядка на A. Множество A называется при этом упорядоченным множеством.

Определение 2. Связное отношение порядка на множестве A называется отношением линейного порядка (линейным порядком) на A. Множество A, в этом случае, называется линейно упорядоченным, или – цепью, а количество элементов в A (если A – конечно) называется длиной цепи A.

Определение 3. Порядок ρ на множестве A называется строгим, если ρ – антирефлексивное отношение, и – нестрогим, если ρ – рефлексивное отношение.

Примеры:
1) Обычные отношения порядка (строгие и нестрогие) на множествах $\mathbf{N}, \mathbf{Q}, \mathbf{R}$ – линейные порядки.
2) Отношение (строгого) включения на $P(A)$ – множестве всех подмножеств множества A есть (частичный) порядок.

При изображении графа отношения порядка, элементы, стоящие в паре первыми, располагают ниже (выше) элементов, стоящих вторыми и соединяют их не стрелками, а отрезками. При этом, если $x\rho y$ и $y\rho z$, то точки x и z отрезками не соединяют. Например, если
$A = \{1, 2, 3, 4\}, \rho = \{(x, y)|x \vdots y\}$, то граф выглядит так:

В этом случае известно, что отношение рефлексивно и петли у каждой точки можно не изображать.

Упражнение 28. Являются ли отношениями порядка следующие отношения на множестве N – натуральных чисел?

1. $\rho = \{(x,y)|x^2 = y\}$;
2. $\rho = \{(x,y)|2x = y\}$;
3. $\rho = \{(x,y)|y < 3x\}$;
4. $\rho = \{(x,y)|x \vdots y\}$;
5. $\rho = \{(x,y)|(x-y) \vdots 5\}$;
6. $\rho = \{(1,2),(3,5),(2,5),(1,3),(2,3),(1,5)\}$.

Упражнение 29. В прямоугольнике, изображенном ниже, рассмотрим отношение включения "подпрямоугольников". Является ли это отношение порядком на множестве всех изображенных здесь прямоугольников?

3	2	1
6	8	5
7	9	4

Например: $6 \subset 3, 6 \subset 5$.

Упражнение 30. На множестве $A = \{1,2,\ldots,9\}$ задано отношение $\rho = \{(x,y)|x \vdots y\}$. Является ли ρ порядком? Изобразить его граф.

Упражнение 31. На множестве всех точек плоскости задать линейный порядок.

Пусть ρ – отношение порядка на множестве A и $a\rho b$, тогда будем говорить, что элемент a меньше элемента b. Понятным становится, поэтому, происхождение следующих терминов.

Определение 4. Элемент $e \in A$, называется минимальным элементом упорядоченного множества A с порядком ρ, если
$\forall x \in A(x\rho e \Longrightarrow x = e)$.

Определение 5. Элемент $e \in A$, называется максимальным в (A, ρ), если $\forall x \in A(e\rho x \Longrightarrow e = x)$.

Определение 6. Элемент $e \in A$, называется наименьшим (наибольшим) в (A, ρ), если $\forall x \in A(e\rho x \vee e = x)$ $(\forall x \in A(x\rho e \vee e = x))$.

Определение 7. Пусть $B \subset A$. Элемент $e \in A$ называется верхней (нижней) границей множества B в (A, ρ), если $\forall x \in B(x\rho e \vee x = e)$ $(\forall x \in B(e\rho x \vee e = x))$.

Определение 8. Наименьшая (наибольшая) из верхних (нижних) границ подмножества B в (A, ρ), если она существует, называется точной верхней (нижней) границей множества B в (A, ρ), сокращенно, т.в.г., т.н.г.

Упражнение 32. Каковы минимальные, максимальные, наименьшие, наибольшие элементы в упорядоченных множествах из упражнений 29, 30?

Упражнение 33. Пусть $\rho = \{(x, y)|y \vdots x\}$ задано на множестве $\mathbf{N}$, $A = \{2, 3, 8\}$. Найти точную нижнюю границу и точную верхнюю грани-

цу для A в $(\mathbf{N}, \rho)$.

Упражнение 34. Пусть $A \subset P(B)$. Найти т.н.г. и т.в.г. для A в $(P(B), \subset)$.

Упражнение 35. В $(\mathbf{R}, <)$ найти т.в.г. и т.н.г. для множества $A = \{x | 0 \leq x < 1\}$.

Упражнение 36. В $(\mathbf{N}, \vdots)$ найти минимальные, максимальные, наибольший, наименьший элементы.

Определение 9. Порядок ρ на множестве A называется плотным, если $\forall x, y \in A \; \exists z \in A (x \rho y \Longrightarrow x \rho z \wedge z \rho y \wedge z \neq x \wedge z \neq y)$.

Определение 10. Порядок на множестве A называется полным, если любое непустое подмножество множества A содержит наименьший элемент.

Определение 11. Высотой упорядоченного множества (A, ρ) называется наибольшая из длин содержащихся в A цепей. Если такого числа не существует, то говорят, что (A, ρ) имеет бесконечную высоту.

Шириной упорядоченного множества (A, ρ) называется наибольшее число попарно не сравнимых в A элементов, если же такого числа нет, то говорят,что ширина (A, ρ) – бесконечна.

Упражнение 37. Являются ли плотными (полными) порядки на множествах: $(\mathbf{N}, <)$, $(\mathbf{Z}, \leq)$, $(\mathbf{Q}, <)$, $(\mathbf{N}, \vdots)$? На множествах из упражнений 29–31?

Упражнение 38. Доказать, что множество, у которого конечны высота и ширина — конечно.

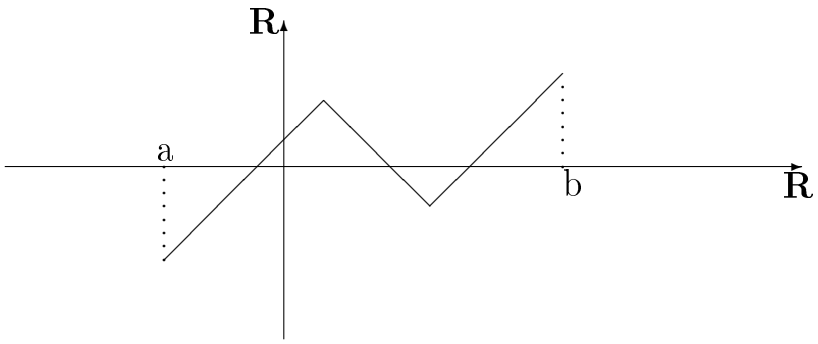
Упражнение 39. Пусть ρ и σ – отношения порядка на множестве A.

Являются ли $\rho \cap \sigma$ и $\rho \cup \sigma$ отношениями порядка на A?

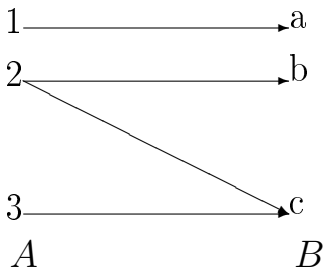
Упражнение 40. Приведите примеры:
1) плотно упорядоченого конечного множества с непустым отношением порядка;
2) линейно упорядоченного множества бесконечной ширины;
3) вполне упорядоченного множества ширины 2.

1.5 Функции (отображения). Свойства функций

Определение 1. Бинарное отношение (соответствие) φ между множествами A и B называется функцией из A в B, если
$\forall x \in A \; \exists! y \in B \, ((x, y) \in \varphi)$.
Примеры:
1)Является ли функцией бинарное отношение, график которого изображен ниже?



Данный вопрос некорректен, так как не указано на какой паре множеств определено отношение φ.
2) Данное в примере 1 отношение φ на паре множеств $\mathbf{R}$, $\mathbf{R}$ не является функцией.
3) На паре множеств $[a, b]$, $\mathbf{R}$ отношение φ – функция.
4) Является ли функцией на паре множеств A, B отношение φ, граф которого изображен ниже?



φ – не функция из A в B,
т.к. $(2,b) \in \varphi$ и $(2,c) \in \varphi$.

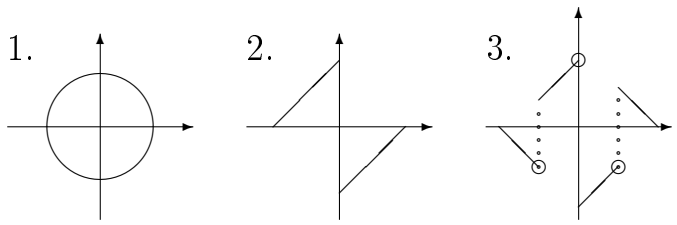
Далее мы будем вместо $(a,b) \in \varphi$ записывать $\varphi(a) = b$, где φ – функция из A в B, при этом элемент b называется образом элемента a, элемент a – прообразом b.

Определение 2. Пусть f – функция из A в B (пишем $f : A \to B$). $A' \subseteq A$, $B' \subseteq B$. Множество $f(A') = \{f(x) | x \in A'\}$ называется образом множества A' при отображении f, а множество $\{x | f(x) \in B'\}$, обозначаемое $f^{-1}(B')$, называется полным прообразом множества B' при отображении f.

Определение 3. Если f – функция из A в B и f^{-1} – функция из B в A, то f^{-1} называтся функцией, обратной к f, а функция f – обратимой функцией.

Упражнение 41. Сравните данное нами определение функции с тем, что дается в школьных учебниках. Прокомментируйте различия.

Упражнение 42. Какими должны быть множества A и B, чтобы бинарные отношения на $\mathbf{R}$, графики которых изображены ниже, были функциями из A в B?



Определение 4. Функция $f : A \to B$ называется инъективной, если

$\forall x, y \in A\,(x \neq y \Longrightarrow f(x) \neq f(y))\,.$

Определение 5. Функция $f : A \to B$ называется сюръективной, если $\forall y \in B\ \exists x \in A\,(f(x) = y)\,.$

Определение 6. Функция $f : A \to B$ называется биективной, если она инъективна и сюръективна.

Упражнение 43. Доказать, что функция биективна тогда и только тогда, когда она обратима.

Упражнение 44. Какими из перечисленных в определениях 4 – 6 свойств обладают функции, рассмотренные в этом параграфе?

Упражнение 45. Какие из данных отношений являются функциями? Какими свойствами обладают эти функции?

1. $f = \{(x, y) | y = x^2\} \subset \mathbf{R} \times \mathbf{R}\,;$
2. $f = \{(x, y) | y = x^3\} \subset \mathbf{R} \times \mathbf{R}\,;$
3. $f = \{(x, y) | y = x^2\} \subset [0, \infty) \times [0, \infty)\,;$
4. $f = \{(x, y) | y = \sin x\} \subset \mathbf{R} \times [1, \infty)\,;$
5. $f = \{(x, y) | x = y^2\} \subset \mathbf{R} \times \mathbf{R}\,;$
6. $f = \{(x, y) | x = y^2\} \subset \mathbf{R}^+ \times \mathbf{R}^+\,;$
7. $f = \{(x, y) | y = \operatorname{tg} x\} \subset \mathbf{R} \times \mathbf{R}\,;$
8. $f = \{(x, y) | y = \operatorname{tg} x\} \subset (-\pi/2, \pi/2) \times \mathbf{R}\,;$
9. $f = \{(x, y) | y = |x|\} \subset \mathbf{R} \times \mathbf{R}\,;$
10. $f = \{(x, y) | X^2 + y^2 = 1\} \subset \mathbf{R} \times \mathbf{R}\,;$
11. $f = \{(x, y) | x^2 + y^2 = 1\} \subset [-1, 1] \times \mathbf{R}\,;$

12. $f = \{(x,y)|x^2+y^2=1\} \subset [-1,1]\times[-1,1]$;

13. $f = \{(x,y)|x^2+y^2=1\} \subset [-1,1]\times \mathbf{R}^+$;

14. $f = \{(x,y)|x^2+y^2=1\} \subset [0,1]\times[0,1]$.

Определение 7. Пусть $\varphi \subseteq A\times B$, $\psi \subseteq B\times C$ – бинарные отношения. Отношение
$\varphi\cdot\psi = \{(x,z)\in A\times C\,|\exists y\in B(\varphi(x)=y\wedge\psi(y)=z\}$ — называется композицией отношений φ и ψ.

Упражнение 46. Доказать, что композиция функций $\varphi: A\to B$ и $\psi: B\to C$ есть функция из A в C.

Упражнение 47. Если $\varphi: A\to B$ и $\psi: B\to C$ — инъективны (биективны), то $\varphi\cdot\psi$ – инъективна (биективна).

Упражнение 48. Пусть $f: A\to B$ – сюръективно. Тогда, для любых отображений $\varphi: B\to A$, $\psi: B\to A$, если $f\cdot\varphi = f\cdot\psi$, то $\varphi=\psi$.

Заметим, что композиция двух отображений φ и ψ есть их последовательное выполнение, т.е. $(\varphi\cdot\psi)(x) = \psi(\varphi(x))$.

Упражнение 49. Пусть $\varphi: A\to B$ и $\psi: B\to C$ — биекции. Тогда $(\varphi\cdot\psi)^{-1} = \psi^{-1}\cdot\varphi^{-1}$ и $\varphi\cdot\varphi^{-1}$ – тождественное отображение.

Упражнение 50. Привести примеры функций из школьного учебника:
1) инъективной, но не сюръективной;
2) сюръективной, но не инъективной;
3) биективной.

Упражнение 51. Привести пример функции из $\mathbf{R}$ в $\mathbf{R}$, заданной формулой, сюръективной, но не инъективной.

Обычно, когда задают функцию формулой, подразумевают, что ее область определения равна области допустимых значений для этой формулы.

Упражнение 52. Доказать, что если $f : A \to B$ – отображение и $A_1, A_2 \subseteq A,\ B_1, B_2 \subseteq B$, то:

1. $f(A_1 \cup\ A_2) = f(A_1) \cup f(A_2)$;
2. $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$;
3. $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$;
4. $f^{-1}(B_1) \cap f^{-1}(B_2) = f^{-1}(B_1 \cap B_2)$.

Упражнение 53. Доказать, что в любой случайной компании людей найдутся два человека с одинаковым числом знакомых из этой же компании.

1.6 Мощность множеств. Счетные и несчетные множества

Для конечных множеств определено понятие количества элементов и такие множества можно сравнивать по этому признаку. Если же множество бесконечно, то понятие "количество элементов" становится бессмысленным. С другой стороны, для того, чтобы узнать в каком из двух конечных множеств элементов больше, не обязательно пересчитывать все элементы этих множеств, можно установить биекцию между одним из множеств и частью другого и сразу станет ясно, в каком множестве есть "лишние" элементы. Например, для того, чтобы узнать хватит ли всем присутствующим стульев, можно попросить всех сесть на имеющиеся стулья, вместо того, чтобы сравнивать количество людей и стульев.

Идея инъективного отображения одного множества в другое служит для обобщения понятия количества элементов на случай бесконечных

множеств. Например, если мы, применяя этот принцип, попытаемся установить каких чисел больше: четных или нечетных, то придем к выводу, что существуют биективные отображения этих множеств друг на друга, то есть в каждом из этих множеств элементов не больше (в нашем обобщенном смысле), чем в другом. Естественно считать эти множества в чем-то похожими. В дальнейшем, это "что-то" и будет называться мощностью множества.

Определение 1. Множества A и B называются равномощными (эквивалентными), если существует биекция A на B.

Упражнение 54. Доказать, что в классе всех множеств отношение равномощности является отношением эквивалентности.

Если множество A равномощно множеству B, будем записывать $A \simeq B$. Возможны следующие случаи:
1. $A \simeq B' \subseteq B$ и $B \simeq A' \subseteq A$;
2. $A \simeq B' \subseteq B$ и B не эквивалентно никакому подмножеству A;
3. $B \simeq A' \subseteq A$ и A не эквивалентно никакому подмножеству B;
4. Ни одно из множеств A, B не эквивалентно подмножеству другого.

Упражнение 55. Доказать, что четвертая из приведенных возможностей не выполняется для любых двух конечных множеств.

Без доказательства примем утверждение о невозможности четвертого случая для произвольной пары бесконечных множеств.

Теорема 1.6.1 (Кантора – Бернштейна) *Для произвольных множеств* A, B, *если* $A \simeq B' \subseteq B$ *и* $B \simeq A' \subseteq A$ *то* $A \simeq B$.

Доказательство.
Пусть $f : A \to B$, $g : B \to A$ – инъективные отображения. Положим $C = A \cup B$. Элемент $x \in C$ назовем предком элемента $y \in C$, если y может быть получен из x последовательным выполнением конечного

числа раз отображений f и g. Элемент y при этом называется потомком элемента x.

Каждый элемент имеет либо конечное множество предков, либо – бесконечное (не конечное). Если предков – конечное множество, то их число может быть четным, или нечетным.

Таким образом, каждое из множеств A и B разбивается на три подмножества: A_∞, A_1, A_2, B_∞, B_1, B_2 – подмножества, состоящие из элементов с бесконечным, нечетным и четным числом предков соответственно.
Ясно, что если $x \in A_\infty$, то $f(x) \in B_\infty$, и, если $y \in B_\infty$, то существует $x \in A_\infty$ такой, что $y = f(x)$ $(x = f^{-1}(y))$. Поэтому $f(A_\infty) = B_\infty$, то есть $A_\infty \simeq B_\infty$ (отображение f).
Если $x \in A_2$, то $f(x) \in B_1$. Если $y \in B_1$, то
$\exists x \in A_2$ $(f(x) = y)$, то есть $A_2 \simeq B_1$ (отображение f).
Если $y \in B_2$, то $g(y) \in A_1$. Если $x \in A_1$, то
$\exists y \in B_2$ $(g(y) = x)$, то есть $A_1 \simeq B_2$ (отображение g).
Определим биекцию $h : A \to B$ следующим образом:

$$h(x) = \begin{cases} f(x), \text{если } x \in A_2 \cup B_\infty \\ g^{-1}(x), \text{если } x \in A_1. \end{cases}$$

Поэтому, $A \simeq B$. Теорема доказана.

Еще раз напомним, что для двух множеств невозможна ситуация, когда каждое из них не эквивалентно никакому подмножеству другого.

Определение 2. Говорят, что мощность множества B меньше мощности A, если $B \simeq C \subset A$ и A не эквивалентно никакому подмножеству множества B. Записывают это так: $|B| < |A|$. Если $A \simeq B$, то пишут $|A| = |B|$.

Из теоремы Кантора-Бернштейна следует, что для двух множеств A, B имеет место в точности один из случаев:
$|A| < |B|$, $|B| < |A|$, $|B| = |A|$.
Для конечных множеств $|A| < |B|$, если в A элементов меньше, чем в B, $|A| = |B|$, если A и B состоят из одинакового количества элементов.

Поэтому, для конечных множеств, различать понятия мощности и количества элементов не имеет смысла. Для бесконечных же множеств (хотя мы еще не определили это понятие) сравнивать мощности имеет смысл лишь в том случае, если существуют множества различной мощности.

Теорема 1.6.2 (Кантор) $|A| < |P(A)|$.

Доказательство.
Предположим, что существует биекция f множества A на множество $P(A)$ – всех его подмножеств. Рассмотрим множество
$X = \{x | x \notin f(x)\} \subseteq A$. $X \neq \emptyset$, так как $\exists y \in A\,(f(y) = \emptyset)$, то есть $y \notin f(y)$. Так как $X \in P(A)$, то $\exists a \in A\,(f(a) = X)$, но тогда, если $a \in X$, то $a \notin f(a) = X$ –противоречие, если же $a \notin X$, то $a \in f(a) = X$ – противоречие. Следовательно, $|A| < |P(A)|$. Теорема доказана.

Упражнение 56. Если A – конечно и состоит из n элементов (то есть $|A| = n$), то $|P(A)| = 2^n$.

Упражнение 57. Доказать, что $P(A)$ эквивалентно множеству всех отображений из A в $\{0,\ 1\}$.

Интуитивно ясно, что конечное множество не может быть равномощно своему собственному подмножеству. Это свойство мы будем считать характеристикой конечных множеств.

Определение 3. Множество, не эквивалентное никакому своему собственному подмножеству, называется конечным.

Определение 4. Множество, не являющееся конечным, называется бесконечным.

Определение 5. Множество называется счетным, если оно эквивалентно множеству всех натуральных чисел $\mathbf{N}$.

Упражнение 58. Всякое множество, содержащее бесконечное подмножество, само бесконечно.

Определение 6. Отрезком $\bar{n}$ натурального ряда называется множество всех натуральных чисел, меньших n.

Упражнение 59. Любой отрезок натурального ряда – конечное множество.

Упражнение 60. Множество, эквивалентное конечному (бесконечному) множеству – конечно (бесконечно).

Упражнение 61. Счетное множество – бесконечно.

Упражнение 62. Множество конечно тогда и только тогда, когда оно эквивалентно отрезку натурального ряда.

Упражнение 63. Во всяком бесконечном множестве есть счетное подмножество.

Замечание. В некоторых доказательствах используется аксиома выбора, которую на данном этапе можно сформулировать так: из любого непустого подмножества данного множества можно выбрать один элемент.

Упражнение 64. Всякое подмножество счетного множества конечно, или счетно.

Упражнение 65. Объединение конечного множества конечных множеств – конечно.

Упражнение 66. Объединение счетного множества конечных множеств – не более, чем счетно.

Упражнение 67. Объединение конечного множества счетных множеств – счетно.

Упражнение 68. Объединение счетного множества счетных множеств – счетно.

Упражнение 69. Если A – бесконечно, B – конечно, то $A \setminus B \simeq A \cup B \simeq A$.

Упражнение 70. Если A – бесконечно, B – счетно, то $A \cup B \simeq A$.

Упражнение 71. Если A – бесконечно и несчетно, B – счетно, то $A \setminus B \simeq A$.

Лемма 1.6.1 *Если* $A \simeq A_1$, $B \simeq B_1$, *то* $A \times B \simeq A_1 \times B_1$.

Доказательство.
Пусть заданы биекции $f : A \to A_1$, $g : B \to B_1$. Рассмотрим отображение $h : A \times B \to A_1 \times B_1$, где $h(a, b) = (f(a), g(b))$. Отображение h – биекция. Действительно, если $(a, b) \neq (a_1, b_1)$, то $a \neq a_1$, или $b \neq b_1$, но тогда $f(a) \neq f(a_1)$, или $g(b) \neq g(b_1)$, то есть $(f(a), g(b)) \neq (f(a_1), g(b_1))$. Следовательно, h – инъективно.
Если $(a_1, b_1) \in A_1 \times B_1$, то $h(f^{-1}(a_1), g^{-1}(b_1)) = (a_1, b_1)$, то есть h – сюръективно. Лемма доказана.

Упражнение 72. Декартово произведение двух счетных множеств – счетное множество.

Упражнение 73. Декартово произведение n счетных множеств – счетное множество.

Упражнение 74. Множество рациональных чисел $\mathbf{Q}$ – счетно.

Упражнение 75. Множество конечных последовательностей элементов счетного множества – счетно.

Упражнение 76. Множество всех алгебраических чисел – счетно.

Упражнение 77. Любое множество попарно не пересекающихся отрезков на прямой, прямоугольников на плоскости, параллелепипедов в пространстве не более, чем счетно.

Теорема 1.6.3 *Множество* $\Pi(A)$ *всех последовательностей элементов счетного множества* A *равномощно* $P(A)$ *– множеству всех подмножеств множества* A*.*

Доказательство. В силу доказанных ранее утверждений, в качестве A можно взять множество $\mathbf{N}$ – всех натуральных чисел.
Каждому подмножеству множества $\mathbf{N}$ поставим в соответствие последовательность его элементов, расположенных в порядке возрастания. Это отображение, очевидно, инъективно.
Всякая последовательность натуральных чисел есть множество пар (x, n) натуральных чисел, где n – номер элемента x в данной последовательности. Если последовательности различны, то и соответствующие им множества пар – различны. Таким образом, если каждому элементу x с номером n поставить в соответствие пару (x, n), то каждой последовательности будет соответствовать множество пар натуральных чисел. Легко видеть, что полученное отображение $\Pi(\mathbf{N})$ в $P(\mathbf{N} \times \mathbf{N})$ – инъективно. Но $\mathbf{N} \times \mathbf{N} \simeq \mathbf{N}$, следовательно, $\Pi(\mathbf{N}) \simeq P(\mathbf{N})$. Теорема доказана.
Замечание. При доказательстве теоремы мы использовали то, что если $A \simeq B$, то $P(A) \simeq P(B)$. Докажите это.

Теорема 1.6.4 *Множество* $\mathbf{R}$ *действительных чисел – несчетно.*

Доказательство. Мы докажем, что в $\mathbf{R}$ есть несчетное подмножество. Тогда, в силу упражнения 64, будет доказано, что $\mathbf{R}$ не является счетным множеством.

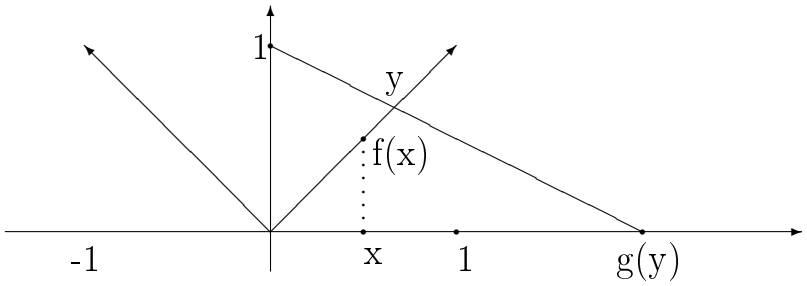
Рассмотрим множество всех действительных чисел из отрезка $[0,1]$ и напомним, что каждое действительное число представимо в виде десятичной дроби, причем из двух представлений, например, $1,000\ldots$ и $0,999\ldots$ числа 1 будем выбирать второе.
Предположим, что множество всех чисел отрезка $[0,1]$ счетно. Тогда каждое из них имеет номер. Рассмотрим дробь a из отрезка $[0,1]$, отличающуюся от i-го числа из $[0,1]$ i-ой цифрой после запятой, для всех i из $\mathbf{N}$. Эта дробь отличается от любого числа из $[0,1]$ – противоречие. Следовательно, $[0,1]$ – несчетное множество, но тогда и $\mathbf{R}$ – несчетно. Теорема доказана.

Упражнение 78. Доказать, что существуют трансцендентные числа.

Определение 7. Будем говорить, что множество имеет мощность континуума, если оно эквивалентно $\mathbf{R}$.

Упражнение 79. Доказать, что следующие множества имеют мощность континуума:
1) множество всех иррациональных чисел;
2) множество всех трансцендентных чисел;
3) множество всех отрезков числовой оси, имеющих длину 1.

Пример. Докажем, что открытый отрезок (-1,1) имеет мощность континуума.
Доказательство проведем с помощью чертежа, где пунктиром показана биекция f из (-1,1) на часть графика функции $y = |x|$, а сплошной линией – биекция g этой части графика на $\mathbf{R}$. Композиция $f \cdot g$ есть биекция (-1,1) на $\mathbf{R}$.



Упражнение 80. Любой отрезок прямой, состоящий более, чем из одной точки, имеет мощность континуума.

Упражнение 81. Объединение счетного множества множеств мощности континуума имеет мощность континуума.

Теорема 1.6.5 *Если A и B – множества мощности континуума, то $A \times B$ имеет мощность континуума.*

Доказательство. Докажем, что $[0,1] \times [0,1] \simeq \mathbf{R}$. Для этого рассмотрим отображение $f : [0,1] \times [0,1] \to [0,1]$, где
$f((0, a_1a_2 \ldots; 0, b_1b_2 \ldots)) = 0, a_1b_1a_2b_2 \ldots$. Ясно, что f – биекция и, так как $[0,1] \simeq \mathbf{R}$, то получаем требуемое. Теорема доказана.

Упражнение 82. Доказать, что $A_1 \times A_2 \times \ldots \times A_n \simeq \mathbf{R}$, если все сомножители эквивалентны $\mathbf{R}$.

Упражнение 83. Любая фигура на плоскости, содержащая подмножество мощности континуума, имеет мощность континуума.

Теорема 1.6.6 $P(\mathbf{N}) \simeq \mathbf{R}$.

Доказательство. Всякое действительное число отрезка
$[0,1]$ можно однозначно (с точностью, указанной выше) представить в виде десятичной дроби, то есть в виде последовательности натуральных чисел. Таким образом, существует инъекция $f : [0,1] \to \Pi(\mathbf{N})$. Но, по теореме 1.6.3, $\Pi(\mathbf{N}) \simeq P(\mathbf{N})$, следовательно существует инъекция из $[0,1]$ в $P(\mathbf{N})$.
Рассмотрим отображение $g : P(\mathbf{N}) \to [0,1]$ такое, что для $A \in P(\mathbf{N})$,

$g(A) = 0, a_1 a_2 \ldots$, где $a_i = 1$, если $i \in A$ и $a_i = 0$, если $i \notin A$. Легко доказать, что g – инъекция. Следовательно, по теореме Кантора-Бернштейна, $P(\mathbf{N}) \simeq [0,1]$. Теорема доказана.

Упражнение 84. Если A – счетно, то $P(A) \simeq \mathbf{R}$.

Упражнение 85. Множество всех функций из $\mathbf{R}$ в $[0,1]$ равномощно множеству $P(\mathbf{R})$.

Упражнение 86. Множество всех числовых функций имеет мощность, большую мощности континуума.

Упражнение 87. Множество $F(\mathbf{R})$ всех числовых функций, эквивалентно $P(\mathbf{R})$.

Континуум-гипотеза. Не существует множество A такое, что $|\mathbf{N}| < |A| < |\mathbf{R}|$.

Обобщенная континуум-гипотеза. Невозможно $|A| < |B| < |P(A)|$. Континуум-гипотеза была сформулирована Кантором и безуспешные попытки доказать ее предпринимались до тех пор, пока в трудах Геделя и Коэна не было показано, что средствами аксиоматической теории множеств ее невозможно ни доказать, ни опровергнуть.

Глава 2

Алгебраические системы

2.1 Алгебраические операции

В этом разделе мы повторим, в основном, определения и свойства, которые изучались в начальных разделах курса алгебры.

Определение 1. n-местной операцией на множестве A называется отображение множества A^n в A, где A^n – декартова n-я степень множества A.

Примеры.

1. Определим отображение $f : R \to R$ такое, что $f(x) = x^2$. Это отображение – одноместная (унарная) операция на R.

2. Соответствие $\{(x, \sqrt{x}) | x \in R\}$ не является операцией на R. Это соответствие можно назвать частичной операцией на R.

3. Бинарными операциями на соответствующих множествах являются обычные сложение и умножение на N, Z, Q, R, C.

4. Вычитание натуральных чисел – не операция на N.

Упражнение 1. Приведите примеры унарных операций в школьном курсе математики, пример трехместной операции на множестве целых чисел.

Далее, в этом параграфе, речь идет только о бинарных операциях – наиболее распространенных как в математике, так и в построении математических моделей реальных объектов и процессов.

Пусть на множестве A задана бинарная операция $*$. Вместо $*(x,y)=z$, будем записывать $x*y=z$.

Определение 2.

1) $*$ – ассоциативна $\overset{def}{\Longleftrightarrow} \forall x,y,z\in A\,(x*(y*z)=(x*y)*z)$;

2) $*$ – коммутативна $\overset{def}{\Longleftrightarrow} \forall x,y\in A\,(x*y=y*x)$;

3) $*$ – сократима слева $\overset{def}{\Longleftrightarrow} \forall\in A\,(z*x=z*y\Longrightarrow x=y)$;

4) $*$ – обратима слева $\overset{def}{\Longleftrightarrow} \forall a,b\in A\,\exists x\in A\,(x*a=b)$;

5) элемент e называется нейтральным относительно операции $*$ $\overset{def}{\Longleftrightarrow}$ $\forall x\in A\,(x*e=e*x=x)$;

6) элемент x называется симметричным для элемента y относительно операции $*$ $\overset{def}{\Longleftrightarrow} x*y=y*x=e$, где e – нейтральный относительно $*$ элемент. Элементы x и y называются при этом обратимыми;

7) элемент θ называется нулевым относительно операции $*$, если $\forall x\in A\,(x*\theta=\theta*x=\theta)$.

Правая и двухсторонняя сократимость и обратимость определяются аналогично понятиям, данным выше.

Проиллюстрируем эти определения на следующем примере: пусть S_3 – множество всех биекций (подстановок) трехэлементного множества $\{1,2,3,\}$ на себя, операция – композиция отображений.

Легко проверить, что эта операция ассоциативна, не коммутативна, тождественная подстановка является нейтральным элементом, нулевого элемента нет, для каждого элемента имеется симметричный относительно данной операции. Заметим также, что подстановки:

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

образуют подмножество в S_3 такое, что композиция подстановок из этого подмножества принадлежит ему же. Это важное для дальнейшего изло-

жения свойство – частный случай более общего определения.

Определение 3. Подмножество A множества B с операцией $*$ называется замкнутым относительно $*$, если $\forall x, y \in A\ (x * y \in A)$.

Определение 4. Если на множестве A заданы две операции $*$ и $\circ$, то будем говорить, что $*$ дистрибутивна слева относительно $\circ$, если $\forall x, y, z \in A\ (x * (y \circ z) = (x * y) \circ (x * z))$.
Аналогично определяются дистрибутивность справа и двусторонняя дистрибутивность.

Упражнение 2. Доказать, что если операция $*$ коммутативна и дистрибутивна слева относительно $\circ$, то $*$ дистрибутивна справа относительно $\circ$.

2.2 Полугруппы

В этом разделе мы познакомимся с простейшими свойствами полугрупп, так как нашей задачей в настоящее время не является подробное изучение этих алгебраических систем, что могло бы составить отдельный большой курс. То же можно сказать и по отношению к следующим разделам, посвященным знакомству с группами, кольцами и полями.

Определение 1. Полугруппой называется множество с заданной на нем ассоциативной бинарной операцией.

Примеры полугрупп:
1) Полугруппа преобразований множества A – множество всех отображений множества A в себя с операцией композиции отображений;
2) Полугруппа слов над алфавитом A – множество всех конечных наборов (слов) элементов из множества A с операцией приписывания справа одного слова к другому, т.е., если u и v – слова над A, то $u * v \stackrel{def}{=} uv$,

где $*$ – символ операции приписывания.
3) Множества натуральных, целых, рациональных, действительных, комплексных чисел относительно обычных операций сложения или умножения являются полугруппами.

Если на множестве S задана операция $*$, то будем говорить, что пара $(S, *)$ является алгебраической системой с носителем S и операцией $*$. Если ясно о какой операции идет речь, то эту алгебраическую систему обозначаем просто S. Аналогичные соглашения и обозначения будем использовать для множеств с несколькими операциями и отношениями.

Пусть дана полугруппа S, в которой есть нейтральный элемент, операцию в S назовем умножением.Тогда выполняются следующие свойства.

Упражнение 3. Для каждого элемента из S существует не более, чем один симметричный элемент.

Упражнение 4. Произведение обратимых элементов – обратимый элемент.

Определение 2. Подмножество полугруппы S, замкнутое относительно операции, называется подполугруппой полугруппы S.

Упражнение 5. В любой полугруппе непустое пересечение подполугрупп является подполугруппой.

Определение 3. Пусть A – подмножество полугруппы S. Пересечение всех подполугрупп полугруппы S, содержащих A как подмножество, называется подполугруппой, порожденной в S множеством A и обозначается $[A]_S$.
Когда ясно, о какой полугруппе идет речь, будем обозначать подполугруппу, порожденную множеством A просто [A].

Рассмотрим некоторые примеры.
1) В полугруппе $(N, +)$ – натуральных чисел по сложению подполугруппа, порожденная множеством $\{2,\ 5\}$ состоит из всех натуральных чисел вида $2a + 5b$, где a и b – натуральные. Действительно, множество чисел такого вида, очевидно, замкнуто относительно сложения, т.е. является подполугруппой и, кроме того, все числа этого вида содержатся в любой подполугруппе, в которой есть числа 2 и 5, а значит и в пересечении всех таких подполугрупп.
2) Множество всех нечетных натуральных чисел не является подполугруппой $(N, +)$, так как оно не замкнуто относительно сложения, но это множество является подполугруппой полугруппы $(N, \cdot)$ – натуральных чисел по умножению и порождается в ней множеством всех нечетных простых чисел. Это следует из основной теоремы арифметики.

Первый из этих примеров наталкивает нас на предположение о строении подполугруппы, порожденной множеством в полугруппе. А именно: подполугруппа полугруппы $(S, \cdot)$, порожденная множеством A, состоит из всевозможных конечных произведений элементов из A.

Лемма 2.2.1 *Пусть S – полугруппа, $A \subset S$, тогда*

$$[A]_S = \{b_1 b_2 \dots b_n \mid n \in N,\ b_i \in A\}.$$

(Здесь мы будем операцию называть умножением и не ставить ее знак между сомножителями.)

Доказательство. Очевидно, что поскольку $[A]_S$ – подполугруппа в S, содержащая все элементы из A, то в ней содержатся и все конечные произведения этих элементов. С другой стороны, множество в правой части доказываемого равенства замкнуто относительно умножения и содержит все элементы из A, то есть является подполугруппой, содержащей A, а поэтому $[A]_S$ в нее включается. Лемма доказана.

Определение 4. Пусть $(S_1, \cdot)$ и $(S_2, *)$ – полугруппы. Отображение $f : S_1 \to S_2$ называется гомоморфизмом полугрупп, если

$\forall x, y \in S_1\ (f(x \cdot y) = f(x) * f(y)$. Биективный гомоморфизм такой, что f^{-1} – гомоморфизм из S_2 в S_1 называется изоморфизмом.

Рассмотрим некоторые примеры гомоморфизмов полугрупп.
1) Пусть $(S, *)$ – полугруппа слов над алфавитом $\{a, b\}$,
$(N, +)$ – полугруппа натуральных чисел по сложению.
Зададим отображение $f : S \to N$ такое, что для любого слова u из S $f(u) = n(u)$, где $n(u)$ – длина слова u, т.е. количество букв в этом слове. Легко видеть, что f – гомоморфизм полугрупп.

2) Пусть f – отображение полугруппы натуральных чисел по сложению в себя такое, что $f(x) = 2x$ для любого натурального x.
$f(x + y) = 2(x + y) = 2x + 2y = f(x) + f(y)$, поэтому f –гомоморфизм.

3) Пусть $(Z, \cdot)$ – полугруппа целых чисел по умножению,
$(\{0,\ 1\}, \cdot)$ – подполугруппа данной полугруппы. И пусть

$$f(k) = \begin{cases} 0, \text{если } k - \text{четное} \\ 1, \text{если } k - \text{нечетное} \end{cases}$$

Очевидно, что f – гомоморфизм.

4) Пусть $(Z, \cdot)$ – полугруппа целых чисел по умножению,
$(\{0,\ 1,\ 2\},\ \cdot(mod 3))$ — полугруппа состоящая из элементов 0, 1, 2 с операцией умножения по модулю 3. Каждому целому числу поставим в соответствие остаток от деления этого числа на 3. Это отображение является гомоморфизмом.

Упражнение 6. Доказать, что при гомоморфизме
$f : S \to G$ гомоморфный образ полугруппы S является подполугруппой полугруппы G.

С понятием гомоморфизма тесно связано понятие конгруенции — отношения эквивалентности, "выдерживающего" операции и позволяющего из имеющихся полугрупп строить новые полугруппы, наследующие некоторые свойства исходных. Дадим более точное определение.

Определение 5. Отношение эквивалентности ρ в полугруппе $(S, \cdot)$ называется конгруенцией, если
$\forall a, b, c \in S\ (a\rho b \Rightarrow ac\rho bc \wedge ca\rho cb)$.

Например, в полугруппе $(N, \cdot)$ – натуральных чисел по умножению, отношение
$\rho = \{(a, b)|a, b$ имеют одинаковую четность$\}$ является конгруенцией.

Другим примером конгруенции может служить отношение
$\rho = \{(u, v)|u, v$ состоят из одинакового числа букв$\}$ в полугруппе слов над произвольным алфавитом.

Важным примером конгруенции является также отношение сравнимости целых чисел по данному модулю в полугруппах целых чисел по сложению и по умножению.

Лемма 2.2.2 *Пусть $(S, \cdot)$ – полугруппа, ρ – конгруенция на S. На фактормножестве S/ρ определим отношение $* \stackrel{def}{=} \{(\bar{a}, \bar{b}, \bar{c})|a \cdot b = c\}$. Тогда $*$ – операция на S/ρ и $(S/\rho, *)$ – полугруппа, (которую мы будем называть факторполугруппой полугруппы $(S, \cdot)$ по конгруенции ρ и обозначать S/ρ).*

Упражнение 7. Доказать лемму.

Теорема 2.2.1 *1) Пусть S – полугруппа, ρ – конгруенция на S, тогда отображение $f : S \to S/\rho$ такое, что $\forall a \in S\ (f(a) = \bar{a})$ является гомоморфизмом полугруппы S на факторполугруппу S/ρ.*
2) Пусть S и G – полугруппы, f – гомоморфизм S в G, тогда отношение $\rho = \{(a, b)|a, b \in S \wedge f(a) = f(b)\}$ является конгруенцией на S и факторполугруппа S/ρ изоморфна полугруппе $f(S)$.

Упражнение 8. Доказать теорему.

Упражнение 9. Пусть $f : S_1 \to S_2$ – гомоморфизм полугруппы S_1 в полугруппу S_2, $\varphi : S_2 \to S_3$ – гомоморфизм полугруппы S_2 в полугруппу S_3. Доказать что композиция $f \cdot \varphi$ является гомоморфизмом S_1 в S_3.

Упражнение 10. Доказать, что отношение "быть изоморфными" на произвольном множестве полугрупп является отношением эквивалентности.

Упражнение 11. Пусть $f : S \to G$ – гомоморфизм полугруппы S **на** полугруппу G. Доказать, что образ нейтрального в S элемента является нейтральным элементом в G и образ обратимого в S элемента — обратим в G.

Упражнение 12. Всегда ли гомоморфный образ полугруппы с сократимой операцией является полугруппой с сократимой операцией ?

Далее, в этом параграфе, речь пойдет об упорядоченных полугруппах и их простейших свойствах, следующих непосредственно из определений.

Определение 6. Полугруппа $(S, *)$ называется упорядоченной полугруппой, если на S задано отношение порядка $\leq$ и
$\forall a, b, c \in S\ (a \leq b \Rightarrow a * c \leq b * c\ \wedge\ c * a \leq c * b)$.

Таким образом, упорядоченная полугруппа представляет собой множество, на котором задана одна бинарная операция и одно бинарное отношение, т.е. систему вида $(S, *, \leq)$.

Примерами упорядоченных полугрупп могут служить полугруппы натуральных чисел по сложению и умножению с обычным отношением порядка, аддитивная полугруппа целых чисел с обычным отношением порядка.

Мультипликативная полугруппа целых чисел с обычным порядком, очевидно, не является упорядоченной полугруппой.

В полугруппе S – слов над алфавитом $\{a, b\}$ зададим отношение $\preceq$ следующим образом: $u \preceq v \overset{def}{\iff} n(u) < n(v)\ \vee$
$(n(u) = n(v)\ \wedge\ \exists w_1, w_2, w_3 \in S\ (u = w_1 a w_2\ \wedge\ v = w_1 b w_3))$.

Упражнение 13. Доказать, что определенное выше отношение является отношением порядка на множестве слов над алфавитом $\{a, b\}$.

Определение 7. Отображение f упорядоченной полугруппы $(S, \circ, \leq)$ в упорядоченную полугруппу $(G, *, \preceq)$ называется гомоморфизмом упорядоченных полугрупп, если f – гомоморфизм полугрупп и $\forall x, y \in S\ (x \leq y \Rightarrow f(x) \preceq f(y))$.

В качестве примера гомоморфизма упорядоченных полугрупп приведем отображение f упорядоченной полугруппы слов, определенной выше, в полугруппу $(Z, +, \leq)$ – целых чисел по сложению с обычным отношением порядка такое, что $f(u) = n(u)$ для произвольного слова u.

Однако, если мы зададим отображение f для тех же полугрупп так, что $f(u) =$ (число вхождений a в слово u), то такое отображение не является гомоморфизмом упорядоченных полугрупп. Действительно, для слов aa и ba имеем $aa \preceq ba$, но $f(ba) \leq f(aa)$.

Упражнение 14. Доказать, что в упорядоченной полугруппе $(S, \cdot, \leq)$ из того, что $a_1 \leq a_2$ и $b_1 \leq b_2$ следует $a_1 b_1 \leq a_2 b_2$ и $b_1 a_1 \leq b_2 a_2$ для произвольных $a_1, a_2, b_1, b_2 \in S$.

2.3 Группы

Определение 1. Группой называется полугруппа, в которой существует нейтральный элемент и каждый элемент которой обратим.

Группами являются, например, полугруппы целых, рациональных, действительных, комплексных чисел по сложению. Множество матриц заданного размера с целыми элементами — группа относительно сложения матриц. Множество подстановок n-элементного множества является группой, если операцией служит композиция отображений (подстановок).

Упражнение 15. Проверить, что полугруппы, в приведенных примерах действительно являются группами.

Упражнение 16. В любой группе G уравнения $ax = b$ и $ya = b$ имеют единственные решения для произвольных a и b из G.

Упражнение 17. Группа является полугруппой с сокращением.

Определение 2. Подмножество группы называется подгруппой, если оно замкнуто относительно операции и относительно взятия симметричного элемента.
Примерами подгрупп могут служить:
1) подмножество всех четных целых чисел в группе целых чисел по сложению;
2) подмножество группы, состоящее из одного нейтрального элемента;
3) вся группа;
4) множество всех поворотов плоскости – подгруппа группы всех преобразований плоскости.

Упражнение 18. Доказать, что пересечение любого семейства подгрупп некоторой группы является подгруппой этой группы.

Определение 3. Пусть G – группа, $A \subseteq G$. Пересечение всех подгрупп, включающих A, называется подгруппой, порожденной множеством A в группе G (обозначается $[A]_G$).

Теорема 2.3.1 $[A]_G = \{a_1^{i_1} a_2^{i_2} \dots a_n^{i_n} \mid a_i \in A,\ i_n \in \{-1, 1\}\}$.

Доказательство. Множество указанных произведений включено в любую подгруппу, содержащую A, в силу замкнутости последней. Поэтому оно включается и в пересечение всех этих подгрупп. С другой стороны очевидно, что само это подмножество является подгруппой, содержащей A, а значит $[A]_G$ в нем содержится.

Упражнение 19. Сколько элементов содержит подгруппа группы поворотов плоскости, порожденная поворотом на угол 120° вокруг данной точки ?

Упражнение 20. Почему подгруппа, порожденная множеством $\{5, 8\}$ в группе целых чисел по сложению совпадает со всей группой ?

Определение 4. Если множество A порождает группу G, то оно называется порождающим множеством для G, если, при этом, $A = \{a\}$, то группа называется циклической с порождающим элементом a.

Упражнение 21. Привести четыре примера групп из школьного курса математики.

Определение 5. Отображение φ группы G_1 в группу G_2 называется гомоморфизмом, если φ — гомоморфизм G_1 в G_2 как полугрупп.

Упражнение 22. Доказать, что если φ – гомоморфизм группы G в группу S, то выполняютя следующие свойства:
1) Образ нейтрального элемента групы G является нейтральным элементом в $\varphi(G)$;
2) Для любого элемента a из G $\varphi(a^{-1}) = (\varphi(a))^{-1}$;
3) $\varphi(G)$ есть подгруппа в группе S.

Понятия конгруенции и факторгруппы вводятся аналогично тому, как это было сделано для полугрупп. Так же, как для полугрупп, формулируется теорема о гомоморфизме.

Упражнение 23. Назовем подгруппу H группы G нормальной подгруппой, если $\forall x \in G\ (xH = Hx)$, где $xH = \{xh | h \in H\}$. Пусть ρ – конгруенция на G. Доказать, что $[e]_\rho$ – нормальная подгруппа в группе G, если e – нейтральный в G элемент.

2.4 Кольца

Определение 1. Кольцом называется множество K с двумя бинарными операциями $+$ и $\cdot$, удовлетворяющими свойствам:
1. $(a+b)+c = a+(b+c)$;
2. $a+b = b+a$;
3. $\exists e \in K\ \forall a \in K\ (e+a=a)$;
4. $\forall x \in K\ \exists y \in K\ (x+y=e)$, где e – из п.3.;
5. $a\cdot(b+c) = a\cdot b + a\cdot c\ \wedge\ (b+c)\cdot a = b\cdot a + c\cdot a$.

Если операция $\cdot$ – коммутативна, то кольцо называется коммутативным, если $\cdot$ – ассоциативна, то кольцо – ассоциативно.

Очевидно, что можно было определить кольцо как множество с двумя бинарными операциями, относительно одной из которых (называемой сложением) оно является коммутативной группой и выполняются законы дистрибутивности умножения относительно сложения слева и справа. В дальнейшем мы будем рассматривать только ассоциативные кольца и называть их просто кольцами.

Упражнение 24. Какие из следующих алгебраических систем являются кольцами?
1. $(Z,\ +,\ \cdot)$, где $+,\cdot$ – обычные сложение и умножение целых чисел.
2. Множество классов вычетов по модулю m, где $\bar{a}+\bar{b} = \overline{a+b}$, $\bar{a}\cdot\bar{b} = \overline{a\cdot b}$.
3. $(Z\times Z,\ +,\ \cdot)$, где $(a,b)+(c,d) \stackrel{def}{=} (a+c, b+d)$, $(a,b)\cdot(c,d) \stackrel{def}{=} (ad, bc)$.
4. Множество целых чисел, кратных k, с обычными операциями сложения и умножения.

Ясно, что для сложения в кольце выполняются те же свойства, что для коммутативных групп, так что мы можем ввести операцию вычита-

ния, полагая $a - b \stackrel{def}{=} a + (-b)$.

Упражнение 25. Доказать, что в произвольном кольце выполняются следующие утверждения:
1. $(-a)b = a(-b) = -(ab)$;
2. $(b - a)c = bc - ac$;
3. $-(a - b) = b - a$;
4. $0x = x0 = 0$.

Здесь, для удобства, не пишем знак умножения в кольце и нейтральный по сложению элемент кольца обозначаем 0.

Определение 2. Подкольцом кольца K называется непустое подмножество K, замкнутое относительно сложения, умножения и взятия противоположного элемента.

Упражнение 26. Доказать, что подмножество кольца является подкольцом тогда и только тогда, когда оно замкнуто относительно умножения и вычитания.

Примерами подколец могут служить подмножества чисел, кратных n в кольце целых чисел. Подмножество, состоящее из одного нулевого элемента кольца, а также все кольцо, очевидно, являются подкольцами данного кольца.

Упражнение 27. Проверить, что в кольце классов вычетов по модулю 6 подмножество $\{\bar{0}, \bar{2}, \bar{4}\}$ является подкольцом.

Упражнение 28. Доказать, что в любом кольце произвольное пересечение подколец является подкольцом.

Определение 3. Пусть K – кольцо, $M \subseteq K$, тогда пересечение всех подколец кольца K, содержащих M как подмножество, называется подкольцом, порожденным подмножеством M в кольце K (обозначается

$[M]_K$).

Например, $[\{5,8\}]_Z = Z$, в то время, как $[\{4,6\}]_Z \neq Z$. Подумайте, какими должны быть числа a, b, чтобы
$[\{a,b\}]_Z = Z$?

Упражнение 29. Докажите, что для того, чтобы получить подкольцо $[M]_K$ нужно сначала породить при помощи M подполугруппу в K относительно умножения, а затем этой полугруппой породить группу относительно сложения.

Определение 4. Отображение $f : K_1 \to K_2$ кольца K_1 в кольцо K_2 называется гомоморфизмом, если
$f(a_1 + a_2) = f(a_1) + f(a_2)$, $f(a_1 a_2) = f(a_1) f(a_2)$ для любых элементов a_1, a_2 кольца K_1.

Упражнение 30. 1. Докажите, что, в обозначениях предыдущего определения, гомоморфный образ кольца K_1 является подкольцом кольца K_2.
2. Гомоморфный образ нулевого элемента кольца K_1 – нулевой элемент в K_2.
3. $f(-a) = -f(a)$ для любого a из K_1.
4. $f(a - b) = f(a) - f(b)$.

Определение 5. Биективный гомоморфизм колец называется изоморфизмом (обозначение: $K_1 \cong K_2$).

Упражнение 31. Доказать, что:
1. Каждое кольцо изоморфно себе;
2. Если $K_1 \cong K_2$, то $K_2 \cong K_1$;
3. Если $K_1 \cong K_2$ и $K_2 \cong K_3$, то $K_1 \cong K_3$.

Примером гомоморфизма колец может служить отображение

$f : Z \to Z_{(2)}$ кольца целых чисел в кольцо классов вычетов по модулю 2 такое, что $f(2n) = 0,\ f(2n+1) = 1$ для любого целого n.
Другой пример – отображение $f : Z \to Z_2$ кольца целых чисел в кольцо четных целых чисел такое, что $f(x) = 2x$ для любого $x \in Z$.

Определение 6. Отношение эквивалентности ρ в кольце K называется конгруенцией, если
$\forall a, b, c \in K\ (a\rho b \Longrightarrow (a+c)\rho(b+c) \wedge ac\rho bc \wedge ca\rho cb)$.

Пример: в кольце целых чисел отношение
$\rho = \{(a,b) | a - b = 2k,\ k \in Z\}$ является конгруенцией.

Легко доказать, что если в кольце K задана конгруенция ρ, то на фактормножестве K/ρ можно определить операции следующим "стандартным" образом: $\bar{x} + \bar{y} = \overline{x+y},\ \bar{x}\bar{y} = \overline{xy}$ и полученная система сама является кольцом, которое мы будем называть факторкольцом кольца K по конгруенции ρ. Рассмотрев, например, факторкольцо кольца целых чисел по конгруенции из последнего примера, нетрудно заметить, что оно изоморфно кольцу классов вычетов по модулю 2. Обобщая это наблюдение, сформулируем теорему.

Теорема 2.4.1 (О гомоморфизме) *1. Если K – кольцо, ρ – конгруенция на K, то отображение $\varphi : K \to K/\rho$, где $\varphi(x) = \bar{x}$, является гомоморфизмом.*
2. Если $\varphi : K \to G$ – гомоморфизм колец, то отношение
$\rho = \{(x,y) | \varphi(x) = \varphi(y)\}$ *– конгруенция на K и $K/\rho \cong \varphi(K)$.*

Доказательство этой теоремы принципиально не отличается от соответствующего доказательства для групп или для полугрупп и состоит из проверки определений.

Определение 7. Кольцо K называется упорядоченным, если на нем задано отношение линейного порядка $\leq$ такое, что выполняются условия:

1. $\forall x, y, z \in K\ (x \leq y \Longrightarrow x + z \leq y + z)$;
2. $\forall x, y, z \in K\ (x \leq y\ \wedge\ 0 \leq z \Longrightarrow xz \leq yz\ \wedge\ zx \leq zy)$.

В любом упорядоченном кольце выполняются следующие свойства, доказательство которых предоставляется читателю.

Упражнение 32.
1. $a \leq b\ \wedge\ c \leq d \Longrightarrow a + c \leq b + d$;
2. $0 \leq a \leq b\ \wedge\ 0 \leq c \leq d \Longrightarrow ac \leq bd\ \wedge\ ca \leq db$;
3. $a \leq b \Longrightarrow -b \leq -a$;

В заключение, дадим еще одно определение, подбор иллюстраций для которого не представляет особых сложностей.

Определение 8. Отображение $\varphi : K_1 \to K_2$ упорядоченного кольца K_1 в упорядоченное кольцо K_2 называется гомоморфизмом упорядоченных колец, если φ – гомоморфизм колец и
$\forall x, y \in K_1\ (x \leq y \Longrightarrow \varphi(x) \leq \varphi(y))$.

2.5 Поля

Определение 1. Коммутативное кольцо с единицей называется полем, если для всякого ненулевого элемента этого кольца найдется обратный элемент (т.е. симметричный относительно умножения).

Упражнение 33. Доказать, что если K – поле, то $K^* = K \setminus \{0\}$ – группа относительно умножения.

В качестве примеров укажем следующие поля:
1. Кольца классов вычетов по простому модулю;
2. Кольца рациональных, действительных, комплексных чисел с обычными операциями.

3. Множество $Q(\sqrt{2}) \stackrel{def}{=} \{a + b\sqrt{2} \mid a, b \in Q\}$ с обычными операциями сложения и умножения действительных чисел.
4. Множество рациональных дробей, в числителе и знаменателе которых стоят многочлены от одной переменной с целыми коэффициентами и знаменатель – не нулевой многочлен.

Ясно, что поскольку всякое поле является кольцом, то все перечисленные выше свойства колец выполняются и в полях, поэтому приведем некоторые свойства полей, не обязательно выполняющиеся в произвольном кольце.

1. В любом поле уравнение $ax = b$, при $a \neq 0$, имеет единственное решение. Действительно, таким решением является элемент ba^{-1}. Если же y – еще одно решение данного уравнения, то имеем $ax = ay$, откуда, домножая обе части на a^{-1}, получим $x = y$. Элемент ab^{-1}, при $b \neq 0$, будем, в дальнейшем, записывать как $\frac{a}{b}$ и называть дробью.

Упражнение 34.
$$\frac{a}{b} = \frac{c}{d} \Longleftrightarrow ad = bc.$$

Упражнение 35.
$$-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}.$$

Упражнение 36.
$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

Упражнение 37.
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Упражнение 38.

$$\frac{a}{b} = \frac{ac}{bc},\ (c \neq 0).$$

Упражнение 39.

$$\frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd}.$$

Упражнение 40.

$$\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{ad}{bc}.$$

Упражнение 41.

$$ab = 0 \Longleftrightarrow a = 0 \vee b = 0.$$

Упражнение 42.

$$ac = bc \ \wedge \ c \neq 0 \Longrightarrow a = b.$$

Упражнение 43.

$$\frac{0}{a} = 0.$$

Определение 2. Подмножество, содержащее единицу поля, называется подполем, если оно замкнуто относительно сложения, умножения, взятия противоположного элемента и взятия обратного к ненулевому элементу.

Например, поле рациональных чисел является подполем поля действительных чисел, поле $\{a+b\sqrt{2}\,|a,b\in Q\}$ – подполе поля действительных чисел.

Упражнение 44. Пересечение любой совокупности подполей данного поля является подполем этого поля.

Определение 3. Подполем, порожденным множеством A в поле P называется пересечение всех подполей поля P, включающих в себя множество A.

Например, множество $\{\sqrt{2}\}$ порождает в R подполе $\{a+b\sqrt{2}\,|a,b\in Q\}$.

Упражнение 45. Докажите, что поле рациональных чисел порождается в поле действительных чисел множеством, состоящим из произвольного ненулевого рационального числа.

Определение 4. Если упорядоченное кольцо является полем, то оно называется упорядоченным полем.

Теорема 2.5.1 *Если поле упорядоченно, то оно бесконечно.*

Доказательство. Через $n1$ будем обозначать сумму n единиц данного поля. Предположим, что упорядоченное поле конечно, тогда, для некоторых $n,k\in N$, имеем $n1=k1$, если $n<k$, то отсюда следует $(k-n)1=0$. Но тогда, предположив, что $1<0$, получим $0<0$, сложив $k-n$ раз предпоследнее неравенство с собой. Аналогичное противоречие получится из предположения $0<1$.

Упражнение 46. Доказать, что в упорядоченном поле уравнение $x^2+1=0$ не имеет решения.

Упражнение 47.

$$a \leq b \ \wedge \ 0 < c \Longrightarrow \frac{a}{c} \leq \frac{b}{c}.$$

Упражнение 48.

$$a \leq b \ \wedge \ c < 0 \Longrightarrow \frac{b}{c} \leq \frac{a}{c}.$$

Введем еще одно важное свойство упорядоченности, а именно, непрерывную упорядоченность – одно из свойств системы действительных чисел, отличающих ее от системы рациональных чисел.

Определение 5. Если в упорядоченном поле даны подмножества A и B и все элементы из A меньше, либо равны всем элементам из B, то множества A и B называются сравнимыми и пишем $A \preceq B$.

Определение 6. Упорядоченное поле P называется непрерывно упорядоченным (по Дедекинду), если для любых двух сравнимых подмножеств A и B существует "промежуточный" элемент x такой, что $A \preceq \{x\} \preceq B$.

Определение 7. Упорядоченное поле называется непрерывно упорядоченным (по Вейерштрассу), если в нем каждое ограниченное сверху подмножество имеет точную верхнюю границу.

Определение 8. В упорядоченном поле подмножество $[a, b] \stackrel{def}{=} \{x \mid a \leq x \leq b\}$ называется отрезком. Множество отрезков $\{u_i\}_{i \in I}$, где I – линейно упорядоченное множество индексов, называется системой вложенных отрезков, если $\forall i, j \in I \ (i < j \Longrightarrow u_j \subseteq u_i)$.

Определение 9. Упорядоченное поле называется непрерывно упорядоченным (по Кантору), если в нем любая система вложенных отрезков

имеет непустое пересечение.

Упражнение 49. Проверить, эквивалентны ли между собой данные выше определения непрерывно упорядоченного поля.

Глава 3

Натуральные числа

3.1 Система натуральных чисел

Нашей целью в этом параграфе является аксиоматическое определение системы натуральных чисел, такое, чтобы ее свойства соответствовали интуитивно понятным свойствам натуральных чисел, которыми мы привыкли пользоваться, не особенно задумываясь над их обоснованием. Наши представления о числовых системах вообще мы уже использовали при построении примеров полугрупп, групп и т.д., теперь, как говорится, настала пора "поверить алгеброй гармонию".

Определение 1. Системой натуральных чисел называется алгебраическая система $N = (N, +, \cdot, <)$
(где $+$, $\cdot$ – символы бинарных операций, $<$ – символ бинарного отношения), в которой истинны следующие аксиомы:
1. $x + y = y + x$ – коммутативность сложения;
2. $(x + y) + z = x + (y + z)$ – ассоциативность сложения;
3. $x + z = y + z \Longrightarrow x = y$ – сократимость относительно сложения;
4. $xy = yx$ – коммутативность умножения;
5. $(xy)z = x(yz)$ – ассоциативность умножения;
6. $xz = yz \Longrightarrow x = y$ – сократимость относительно умножения;
7. $\exists e \forall x(xe = x)$ – существование нейтрального элемента относительно умножения;
8. $x(y + z) = xy + xz$ – дистрибутивность сложения относительно умно-

жения;
9. Для любых элементов x, y из N имеет место только одно из соотношений: $x < y,\ y < x,\ x = y$;
10. $a < b \Longleftrightarrow \exists x\ (a + x = b)$ – положительность отношения;
11. $a < b \Longrightarrow a + x < b + x$ – стабильность $<$ относительно операции $+$;
12. $a < b \Longrightarrow ax < bx$ – стабильность $<$ относительно $\cdot$;
13.Каждое непустое подмножество M множества N содержит наименьший элемент (т.е. такой элемент a, что $\forall x \in M\ (a \leq x)$) – аксиома полноты.

Здесь, для удобства, мы обозначили алгебраическую систему той же буквой, что и ее несущее множество, кроме того, там, где это не вызывает недоразумений, мы будем вместо $x \cdot y$ писать просто xy, наконец, запись $a \leq b$ означает $a < b \ \vee \ a = b$. Следует отметить, что приведенная система аксиом избыточна, то есть некоторые аксиомы являются следствиями других, однако, используя такую систему аксиом, мы сразу получаем более полное и наглядное представление об изучаемом объекте.

Упражнение 1. Доказать, что аксиомы 3, 6, 11, 12 являются следствиями остальных аксиом, то есть, если в некоторой алгебраической системе выполняются эти остальные аксиомы, то выполняются и перечисленные.

3.2 Свойства системы натуральных чисел

В дальнейшем, элементы множества N будем называть натуральными числами. Если $a < x \wedge x < b$ будем говорить, что x лежит между a и b.

Свойство 1. В системе натуральных чисел существует единственный нейтральный по умножению элемент.

Действительно, относительно умножения множество N является полугруппой, а в полугруппе это свойство имеет место. Этот нейтральный элемент будем обозначать символом 1.

Свойство 2. Если $a < b \wedge b < c$, то $a < c$, то есть отношение $<$ – транзитивно.

Доказательство. По аксиоме 10, $\exists y\,(a+y=b)$ и $\exists z\,(b+z=c)$, откуда получаем $(a+y)+z=c$. Тогда, по аксиоме 2, $a+(y+z)=c$ и, вновь по аксиоме 10, $a<c$.

Свойство 3. 1 – наименьший элемент в N.

Доказательство. Пусть 1 – не наименьший элемент в N. По аксиоме 13, наименьший элемент в N существует, обозначим его a. Тогда $a<1$ и, по аксиоме 12, $aa<1a$, то есть $aa<a$. В силу аксиомы 9, $aa\neq a$, поэтому, так как a – наименьший элемент, то $a<aa$. Итак, мы получили $aa<a$ и $a<aa$, что противоречит аксиоме 9. Таким образом, 1 — наименьший элемент в N.

Свойство 4. Каким бы ни было натуральное число n, между n и $n+1$ не существует натуральных чисел.

Доказательство. Предположим, что существует такое натуральное число x, что $n<x\wedge x<n+1$. Тогда, по аксиоме 10, существует такое натуральное y, что $x=n+y$. Если $y=1$, то $x=n+1$ и, вместе с предположением, это противоречит аксиоме 9. Если $y\neq 1$, то, по свойству 3, $1<y$, то есть, по аксиоме 11, $n+1<n+y$ и, так как $n+y=x$, то $n+1<x$, что, вместе с предположением, противоречит аксиоме 9. Следовательно, такого натурального x не существует.

Свойство 5. Если $a<b$, то существует единственный элемент x та-

кой, что $a + x = b$.

Доказательство. Существование следует из аксиомы 10. Докажем единственность. Предположим, что $a < b, a + x = b$ и $a + x_1 = b$, тогда, по аксиомам 1 и 3, получим $x = x_1$.

В дальнейшем, если $a < b$, то элемент x такой, что $a + x = b$ будем называть разностью между b и a и обозначать $b - a$. Заметим, что из определения разности следует, что $(b - a) + a = b$.

Упражнение 2. Доказать, что если $b < a$, то $x(a - b) = xa - xb$.

Упражнение 3. Если $a + c < b + c$, то $a < b$.

Упражнение 4. Если $a < b$ и $b < c$, то $b - a < c - a$.

Упражнение 5. Если $a < b$, $c < d$, то $ac < bd$ и $a + c < b + d$.

Упражнение 6. Если $ac < bc$, то $a < b$.

Упражнение 7. $(b - a) + (d - c) = (b + d) - (a + c)$.

Свойство 6. Отношение $<$ – антисимметрично. Это следует из аксиомы 9.

Свойства 2 и 6 и аксиомы 9 и 13 позволяют нам заключить, что $<$ – отношение полного порядка.

Свойство 7. Отношение $<$ является архимедовым порядком, то есть $\forall x, y \in N\ \exists n \in N\ (y < nx)$.

Доказательство. Пусть $x, y \in N$, положим $n = y + 1$, тогда

$nx = (y+1)x = yx + x$, откуда следует, $yx < nx$. Так как $1 \leq x$, то $y \leq yx$. В силу транзитивности порядка, получаем $y < nx$.

3.3 Принцип математической индукции

В этом параграфе мы получим обоснование для метода доказательства по индукции, который широко применялся нами ранее, как интуитивно ясный.

Определение 1. Подмножество A множества натуральных чисел N называется индуктивным, если оно замкнуто относительно прибавления единицы, т.е. $\forall x\ (x \in A \Longrightarrow x+1 \in A)$.

Теорема 3.3.1 (О математической индукции) *Всякое индуктивное множество, содержащее единицу, совпадает с N.*

Доказательство. Пусть A – индуктивно и $1 \in A$. Предположим, что $A \neq N$. Тогда в непустом множестве $N \setminus A$, по аксиоме 13, есть наименьший элемент, обозначим его b. Так как $b \neq 1$, то $1 < b$, то есть существует x такой, что $1+x = b$, следовательно, $x = b-1$ и, по аксиоме 10, $x < b$. В силу выбора элемента b, имеем $b-1 \in A$, а так как A – индуктивно, то $(b-1)+1 \in A$. Но $(b-1)+1 = x+1 = b$. Мы получили $b \in A$, что противоречит выбору b. Таким образом, наше предположение неверно, следовательно $A = N$, что и требовалось доказать.

В этом доказательстве мы использовали аксиомы 9 и 1, не упоминая об этом. В дальнейшем мы будем поступать аналогично, то есть пропускать очевидные ссылки на аксиомы и на ранее доказанные свойства.

Теперь мы можем сформулировать следующий **принцип математической индукции**: Пусть имеется утверждение (формула) о натуральных числах, либо такое утверждение, где аргументом служит натуральное число. Обозначим это утверждение $P(x)$. Известно, что $P(1)$ – истинно и для любого натурального n из истинности $P(n)$ следует

истинность $P(n+1)$. Тогда утверждение $P(x)$ выполняется для всех натуральных чисел.

Упражнение 8. Доказать принцип математической индукции, сформулированный выше. Для доказательства рассмотреть множество всех натуральных чисел, для которых данное утверждение выполняется.

Часто удобно пользоваться другой формой принципа математической индукции, которую называют полной, или возвратной индукцией.

Теорема 3.3.2 (О полной математической индукции.) *Пусть подмножество A множества натуральных чисел N таково, что $1 \in A$ и $\forall k(\forall x < k(x \in A) \Longrightarrow k \in A)$. Тогда $A = N$.*

Упражнение 9. Доказать эту теорему.

Упражнение 10. Сформулировать и доказать принцип полной математической индукции.

Все, сказанное выше, является обоснованием важного и часто применяемого метода доказательства, называемого методом математической индукции. В нашем случае он применяется для доказательства утверждений о натуральных числах и состоит в следующем: если надо доказать истинность утверждения $P(n)$, то
1) проверяем истинность утверждения для $n = 1$;
2) предполагаем, что P истинно для произвольного $n = k$;
3) доказываем, что из (1) и (2) следует истинность P для $n = k + 1$.

Упражнение 11. Сформулировать и обосновать метод полной математической индукции.

Для проверки того, насколько хорошо читатель понял метод математической индукции, предлагаем найти ошибку в известном шуточном доказательстве.

Упражнение 12. Найти ошибку в доказательстве.
Теорема. Все лошади имеют одинаковую масть.
Доказательство. Сформулируем это утверждение более четко. Пусть $P(n)$ означает "любые n лошадей имеют одинаковую масть тогда теорема будет выглядеть так:
$\forall n \in N\ P(n)$.
1) $P(1)$ – истинно, так как любая (одна) лошадь имеет одинаковую масть сама с собой.
2) Предположим, что P истинно для некоторого $k \in N$, то есть "любые k лошадей имеют одинаковую масть".
3) Докажем, что $P(k+1)$ – истинно. Действительно, если у нас имеется $k+1$ лошадь, то выведя из этого "табуна" одну лошадь, мы, по предположению индукции, получим k лошадей одинаковой масти. Поместив эту лошадь обратно и выведя другую, мы, в силу предположения, убедимся, что лошадь, которую мы выводили первой, не отличается по масти от остальных. Таким образом, все $k+1$ лошадей имеют одинаковую масть. Теорема доказана.

Упражнение 13. Доказать, что каждое натуральное число есть единица, или сумма единиц.

Упражнение 14. Верно ли неравенство $(1,001)^{1000} \geq 2$?

Упражнение 15. Доказать неравенство (Бернулли):
$(1+a)^n \geq 1+na$, где $n \in N,\ a \in R$.

Упражнение 16. Доказать, что $P(A)$ состоит из 2^n элементов, где A – n-элементное множество, $P(A)$ – множество всех подмножеств множества A.

Упражнение 17. На какое наибольшее число частей n прямых могут разделить плоскость ?

3.4 Категоричность системы аксиом натуральных чисел

Целью данного параграфа является доказательство того, что любые две системы натуральных чисел изоморфны между собой. Вообще, система аксиом называется категоричной, если любые ее модели изоморфны между собой. Следует, однако, заметить, что понятие "модель" в данном случае точно не определяется, в отличие от случая формальных теорий первого порядка. Рассматриваемая нами система аксиом не является ни элементарной, ни формальной, так как аксиома 13 не эквивалентна никакой элементарной формуле и даже – никакому множеству элементарных формул (т.е. формул, не содержащих переменных для множеств). Под моделью системы аксиом здесь будем понимать алгебраическую систему, в которой выполняются все данные аксиомы. То доказательство категоричности системы аксиом натуральных чисел, которое мы здесь приводим, основано на аксиоме индукции, не элементарной по сути. Поэтому, такое доказательство не применимо к случаю формальной теории натуральных чисел первого порядка. Более того, формальная теория натуральных чисел имеет и неизоморфные модели. Подробнее об этом можно узнать при изучении математической логики.

Теорема 3.4.1 *Система аксиом натуральных чисел категорична.*

Доказательство. Пусть $(N,\ +,\ \cdot,\ <)$ и $(N',\ +,\ \cdot,\ <)$ – две модели системы аксиом из параграфа 1. Для удобства мы обозначили операции и отношения в N и N' одинаковыми знаками. Рассмотрим отображение $f : N \to N'$, заданное следующим образом:
$f(1) = 1'$, где $1'$ – единица в N'; $f(x+1) = f(x) + 1'$.
Область определения f равна N. Докажем это.
Пусть $M = \{x \in N \mid \exists x' \in N'(f(x) = x')\}$. Ясно, что $1 \in M$, далее, если $a \in M$, то $f(a+1) = f(a) + 1'$, то есть $a+1 \in M$. Следовательно, по теореме о математической индукции, $M = N$.

Докажем, что f – гомоморфизм. Рассмотрим множество
$M = \{y \in N \mid \forall x \in N(f(x+y) = f(x) + f(y))\}$. $1 \in M$, так как
$f(x+1) = f(x) + 1' = f(x) + f(1)$, по определению f. Если $y \in M$, то

$\forall x \in N(f(x+y) = f(x)+f(y))$, тогда $\forall x(f(x+(y+1)) = f((x+y)+1) = f(x+y)+f(1) = (f(x)+f(y))+f(1) = f(x)+(f(y)+f(1)) = f(x)+f(y+1)$, то есть $y+1 \in M$. По теореме о математической индукции, получаем $M = N$.

Упражнение 18. Доказать: $\forall x, y \in N(f(xy) = f(x)f(y))$.

Упражнение 19. Доказать: $\forall x, y \in N(x < y \Longrightarrow f(x) < f(y))$.

Докажем теперь, что f – инъективно. Пусть $a \neq b$, но $f(a) = f(b)$. По аксиоме 9, имеем $a < b$, или $b < a$. Пусть, например, $a < b$, но тогда, по предыдущему упражнению, $f(a) < f(b)$, что, вместе с предположением, противоречит аксиоме 9. Аналогичное противоречие получим предположив, что $b < a$. Таким образом, если $a \neq b$, то $f(a) \neq f(b)$, то есть f – инъективно.

Докажем сюръективность f.
Пусть $M' = Imf = \{x' \in N' \mid \exists x \in N(f(x) = x')\}$. $1' \in M'$, так как $f(1) = 1'$. Пусть $a' \in M'$, т.е. $\exists a \in N\ (f(a) = a')$. Тогда $f(a+1) = f(a) + 1' = a' + 1'$, то есть $a' + 1' \in M$. По теореме о математической индукции, $M' = N'$, т.е. f – сюръективно.

Все, доказанное выше, означает, что f – изоморфизм. Теорема доказана.

Напомним еще раз, что приведенное доказательство в принципе не применимо для случая формальной теории натуральных чисел, которая имеет неизоморфные модели.

Мы не будем касаться вопроса о существовании модели системы аксиом натуральных чисел. Можно считать таковой обычный натуральный ряд — это, так называемая, стандартная модель. Как заявил один известный математик: "Натуральные числа придумал Бог, а остальное – дело рук человеческих". Этим высказыванием мы и будем руководствоваться в дальнейшем и модели для других числовых систем будем строить сами.

Глава 4

Целые числа

4.1 Определение и свойства системы целых чисел.

Потребность в расширении системы натуральных чисел в практике людей возникла, очевидно, в связи с потребностями экономического характера, например, измерением долгов, а также с такими ситуациями, где приходилось измерять температуру, или уровень жидкости от фиксированной отметки. "Научно выражаясь скажем, что возникла потребность решать уравнения вида $a + x = b$, где a, b – произвольные натуральные числа. Таким образом, нам необходимо определить систему целых чисел так, чтобы она была расширением системы натуральных чисел и обладала всеми свойствами целых чисел, известными нам из математической практики.

Определение 1. Системой целых чисел называется упорядоченное коммутативное кольцо с единицей, порождающей это кольцо.

Будем обозначать это кольцо так: $(Z, +, \cdot, <)$, а когда не возникает недоразумений – просто Z.

Рассмотрим некоторые свойства системы целых чисел, следующие из определения.

Свойство 1. Система целых чисел содержит подсистему, изоморфную системе натуральных чисел.

Доказательство. Через e обозначим единицу кольца Z. Рассмотрим множество N' – всевозможных конечных сумм вида $e+e+\ldots+e$. Сумму из n таких слагаемых будем обозначать ne. Будем считать, что $1e = e$, тогда ясно, что $ne + me = (n + m)e$ и $ne \cdot me = (nm)e$.

Пусть $(N,\ +,\ \cdot,\ <)$ – система натуральных чисел. Для удобства, операции и отношения порядка в системе натуральных чисел и в кольце целых чисел будем обозначать одинаково. Зададим отображение $f : N \to Z$ следующим образом: $f(n) = ne$. Очевидно, что $ne \neq me$ при $n \neq m$ (в противном случае Z нельзя было бы упорядочить). Таким образом, f – инъективно. Проверим, что $Imf = N'$. Действительно, произвольный элемент x из N' представляет из себя сумму k единиц, для некоторого натурального k. Но тогда $f(k) = ke = x$. Итак, f – биекция N на N'. Кроме того, $f(k + m) = (k + m)e = ke + me = f(k) + f(m)$, $f(km) = (km)e = (ke)(me) = f(k)f(m)$. Пусть, наконец, $k < m$. Рассмотрим суммы ke и me. Если $ke = me$, то $k = m$ (см. выше), если $me < ke$, то $(m - k)e < 0$ – противоречит тому, что в упорядоченном кольце с единицей $0 < e$. Таким образом, остается $ke < me$. Все, доказанное выше, показывает, что f – изоморфизм N и N', что и требовалось доказать.

Напомним, что каждое натуральное число есть сумма единиц, и каждое положительное целое число также есть сумма единиц (почему?). Поэтому, в дальнейшем, мы можем отождествить натуральные числа с целыми положительными числами. Благодаря свойству 1, мы считаем, что система натуральных чисел содержится в системе целых чисел и тогда становится понятен смысл следующего утверждения.

Свойство 2. Каждое целое число можно представить в виде разности двух натуральных чисел.

Доказательство. Пусть N – система натуральных чисел, содержащаяся в кольце целых чисел Z. Рассмотрим в Z множество $M = \{m-n \mid m, n \in N\}$. $1 \in M$, так как $1 = (n+1)-n$, где 1 – единица кольца Z. Докажем, что M – подкольцо кольца Z. Действительно, $(m-n)+(k-p) = (m+k)-(n+p)$, $(m-n)(k-p) = (mk+np)-(mp+nk)$, это следует из свойств колец. Таким образом, M замкнуто относительно

операций сложения и умножения.

Если $m-n \in M$, то $n-m=-(m-n) \in M, 0=m-m \in M$. Таким образом, M – подкольцо кольца Z, содержащее единицу, а, так как Z порождается единицей, то $M=Z$. Это завершает наше доказательство.

Свойство 3. Порядок на Z не является полным и не является плотным.

Доказательство. Чтобы доказать то, что порядок на Z не является полным, достаточно найти в Z подмножество, в котором нет наименьшего элемента. Таким подмножеством является, например, множество $M=\{x \mid x<0\}$. В M нет наименьшего элемента, так как $\forall x \in M(x-1<x)$.

Если бы порядок в Z был плотным, то для любого целого k существовал бы элемент $x \in Z$ такой,что $k<x<k+1$. Пользуясь свойствами упорядоченных колец, получим $0<x-k<1$, но ранее было доказано, что всякий элемент в Z есть либо сумма единиц, (т.е. - положителен), либо противоположен сумме единиц (т.е. - отрицателен). В нашем случае $0<x-k$, следовательно, $x-k$ есть сумма единиц. Однако, как легко видеть, всякая сумма единиц - больше единицы. Полученное противоречие означает, что порядок в Z не является плотным.

Упражнение 1. Привести полное доказательство предыдущего свойства.

Свойство 4. Порядок на множестве целых чисел архимедов, то есть $\forall x, y \in Z^{+} \exists n \in N(y<nx)$.

Упражнение 2. Доказать свойство 4.

Продолжая изучение свойств целых чисел, можно ввести отношение делимости, понятия наибольшего общего делителя, простого числа и т.д., а затем доказать выполнимость всех свойств, рассмотренных в разделе "Теория чисел". Однако, в данном курсе это не является нашей задачей.

4.2 Категоричность системы аксиом целых чисел

В данном параграфе мы будем доказывать категоричность системы аксиом целых чисел, не забывая о тех замечаниях относительно формальной теории, которые были высказаны для натуральных чисел.

Теорема 4.2.1 *Система аксиом целых чисел категорична.*

Доказательство. Пусть $(Z,\ +,\ \cdot,\ <)$ и $(Z',\ +,\ \cdot,\ <)$ — два кольца целых чисел. Здесь операции и отношения, для простоты, обозначены одинаково.

Зададим отображение $f : Z \to Z'$ следующим образом:
$f(1) = 1'$, где 1 и $1'$ – единицы в кольцах Z и Z' соответственно;
$f(n1) = n1',\ f(-(n1)) = -(n1'),\ f(0) = 0'$, где 0 и $0'$ – нулевые элементы данных колец. Поскольку мы доказывали ранее, что каждый элемент кольца целых чисел есть сумма единиц, либо противоположен сумме единиц, либо является нулем, то область определения нашего отображения есть Z. По той же причине $Imf = Z'$. Дальнейшее доказательство предоставляется читателю.

Упражнение 3. Доказать, что отображение f, определенное в доказательстве этой теоремы, является изоморфизмом колец.

Изоморфность колец Z и Z' можно доказать используя то, что оба кольца целых чисел содержат системы натуральных чисел, категоричность системы аксиом натуральных чисел и то, что любое целое число представимо в виде разности двух натуральных чисел. Пусть N и N' – системы натуральных чисел, содержащиеся в Z и Z' соответственно, φ – изоморфизм между N и N'. Зададим отображение $f : Z \to Z'$ следующим образом: $f(m - n) = \varphi(m) - \varphi(n)$.

Упражнение 4. Доказать, что отображение f, заданное выше, есть изоморфизм колец.

4.3 Построение модели системы аксиом целых чисел

Наша задача состоит в построении упорядоченного коммутативного кольца с единицей, порождающей это кольцо. "Материалом" для построения такого кольца может быть только система натуральных чисел, существование которой мы предположили в предыдущей главе. Опираясь на наш математический опыт, мы предполагаем построить желаемое кольцо как множество разностей натуральных чисел, однако, та же математическая практика сообщает нам, что одно и то же целое число можно представить как разность натуральных чисел различными способами. Следовательно, нам потребуется объединить разности натуральных чисел, представляющие одно и то же целое число в один класс, и уже такие классы называть целыми числами. Все, сказанное выше, позволяет несколько прояснить наши дальнейшие действия и сделать понятной их интуитивную основу.

Рассмотрим систему натуральных чисел $(N,\ +,\ \cdot,\ <)$. На множестве $N \times N$ введем операции $+$, $\cdot$ и отношение $<$ следующим образом:
$(a,b) + (c,d) \stackrel{def}{=} (a+c, b+d)$;
$(a,b) \cdot (c,d) \stackrel{def}{=} (ac+bd, ad+bc)$;
$(a,b) < (c,d) \stackrel{def}{\Longleftrightarrow} a+d < b+c$.
Чтобы не усложнять запись, определяемые операции и отношения мы обозначаем такими же знаками, как для натуральных чисел. Кроме того, как обычно, мы будем опускать знак умножения там, где это не вызовет недоразумений.

Упражнение 5. Проверить, что $(N \times N,\ +,\ \cdot,\ <)$ не является упорядоченным кольцом с единицей.

Определим на множестве $N \times N$ отношение $\sim$ следующим образом:
$(a,b) \sim (c,d) \stackrel{def}{\Longleftrightarrow} a+d = b+c$.

Упражнение 6. Доказать, что $\sim$ – отношение эквивалентности.

Упражнение 7. Доказать, что если $(a, b) \sim (c, d)$, то для любой пары (m, n), $(a, b) + (m, n) \sim (c, d) + (m, n)$ и $(a, b)(m, n) \sim (c, d)(m, n)$.

Упражнение 8. Доказать, что если $(a, b) < (c, d)$ и $(a', b') \sim (a, b)$, $(c', d') \sim (c, d)$, то $(a', b') < (c', d')$.

Упражнение 9. Доказать, что отношение $<$, определенное выше на множестве $N \times N$, является стабильным отношением порядка, т.е., если $n < m$ и $(a, b) < (c, d)$, то $(a, b)(m, n) < (c, d)(m, n)$ и для любых m, n из того, что $(a, b) < (c, d)$ следует, что $(a, b) + (m, n) < (c, d) + (m, n)$.

Упражнение 10. Доказать, что отношение $<$ не является линейным порядком на $N \times N$.

Утверждения, сформулированные в упражнениях, позволяют нам заключить, что отношение эквивалентности $\sim$ является конгруенцией в алгебраической системе $(N \times N, +, \cdot, <)$. Нам остается проверить, что фактор-система $(N \times N/\sim, +', \cdot', <')$ является кольцом целых чисел.

Упражнение 11. Доказать последнее сформулированное утверждение.

Глава 5

Рациональные числа

5.1 Определение и свойства системы рациональных чисел

Необходимость делить некоторые величины на доли естественным образом привела к понятию рационального числа, иначе говоря, возникла потребность в создании числовой системы, расширяющей систему целых чисел, в которой было бы разрешимо уравнение $ax = b$ для любых целых чисел a, b, где $a \neq 0$.

Мы будем определять систему рациональных чисел аксиоматически, руководствуясь теми же соображениями, что и в двух предыдущих главах.

Определение 1. Системой рациональных чисел называется простое упорядоченное поле.

Напомним, что поле называется простым, если в нем нет собственных подполей.

Упражнение 1. Запишите все аксиомы системы рациональных чисел.

Свойство 1. Система рациональных чисел содержит подсистему, изо-

морфную системе целых чисел.

Доказательство. Пусть $(Q,\ +,\ \cdot,\ <)$ – упорядоченное поле рациональных чисел. Рассмотрим в Q подкольцо, порожденное единицей, т.е. – множество $Z' = \{\pm n1 \mid n \in N \cup \{0\}\ \}$ – всевозможных конечных сумм единиц поля Q и противоположных к ним элементов, $(01 \stackrel{def}{=} 0)$.

Упражнение 2. Доказать, что Z изоморфно Z', где Z – кольцо целых чисел.

Указание. Обратите внимание на то, что конечное поле нельзя упорядочить.

Свойство 2. Каждое рациональное число есть частное двух целых чисел.

Доказательство. В силу свойства 1, можно считать, что множество Z – целых чисел является подмножеством множества Q – рациональных чисел. Рассмотрим множество $M = \{mn^{-1} \mid m, n \in Z\ \wedge\ n \neq 0\}$ в поле рациональных чисел.

Упражнение 3. Доказать, что $(M,\ +,\ \cdot)$ – подполе поля рациональных чисел.

Так как M – подполе поля рациональных чисел Q, а Q – простое поле, то $M = Q$, что и требовалось доказать.

Свойство 3. Порядок в поле рациональных чисел – плотный.

Доказательство. Пусть $a < b$, где $a, b \in Q$. Докажем, что существует элемент $c \in Q$ такой, что $a < c \wedge c < b$. Символом "2" обозначим сумму $1 + 1$. Рассмотрим элемент $(a + b)2^{-1}$. Так как $a < b$, то $a + a < a + b$ и, так как $0 < 1$, то $0 < 1 + 1$. В упорядоченном поле $0 < 2^{-1}$, поэтому, $a{+}a = 1a{+}1a = a(1{+}1) = a2 < a{+}b$. Следовательно, $a2{\cdot}2^{-1} < (a{+}b)2^{-1}$, то есть $a < (a + b)2^{-1}$. Аналогично доказывается, что $(a + b)2^{-1} < b$.

Свойство 4. Порядок в поле рациональных чисел архимедов, т.е. $\forall x, y \in Q \exists n \in N (0 < x \wedge 0 < y \Longrightarrow y < nx)$. Здесь N – множество натуральных чисел, nx – сумма n слагаемых x.

Доказательство. Если в условии утверждения $y < x$, то $n = 1$, если $y = x$, то $n = 2 = 1+1$. Пусть $x < y$. Тогда, по свойству 2, $x = ml^{-1}$, $y = kt^{-1}$ для некоторых $m, l, k, t \in Z$.*Можно считать, что $m, l, k, t \in Z^+$, где Z^+ – множество всех положительных целых чисел.*

Упражнение 4. Докажите отмеченное знаками "*" утверждение.

Тогда $ml^{-1} < kt^{-1}$, т.е. $mt < kl$ и, в силу архимедовости порядка в системе целых чисел и свойства 2, получим, что существует такое $n \in N$, что $kl < (mt)n$. Следовательно, $kt^{-1} < ml^{-1}n$, или $y < nx$, что и требовалось доказать.

Свойство 5. В поле рациональных чисел уравнение $x^2 - 2 = 0$ не имеет решения.

Доказательство. Предположим обратное. Пусть a – корень данного уравнения. Ясно, что тогда и $-a$ – корень этого уравнения, поэтому мы можем считать что $0 < a$ и что $a = mn^{-1}$, где $m, n \in N$, $n \neq 0$, m, n – взаимно-простые числа. Тогда $m^2 = 2n^2$ и, пользуясь свойствами взаимно-простых чисел, получим, что m делится на n. Получено противоречие. Следовательно, данное уравнение не имеет рациональных корней.

Следует отметить, что при доказательстве свойства 5 мы подразумевали, что используемые здесь свойства целых чисел могут быть получены из аксиом системы целых чисел. Заметим также, что из свойства 5 следует, что на числовой оси есть точки, не соответствующие никакому рациональному числу. Например, точка, расстояние от которой до точки 0 равно длине диагонали квадрата со стороной, равной 1.

Свойство 6. В системе рациональных чисел не всякое ограниченное

сверху подмножество имеет точную верхнюю границу.

Доказательство. Примером такого подмножества является множество $M = \{x \mid x^2 < 2\}$. Необходимо доказать, что для любой верхней границы a этого множества найдется его верхняя граница q такая, что $q < a$.

Пусть $a \in M$ и $a > 0$. Существует $h \in Q$ такое, что $0 < h < 1$ и $h < \frac{2-a^2}{2a+1}$. Положим $b = a + h$, тогда
$b^2 = a^2 + (2a + h)h < a^2 + (2a + 1)h < a^2 + (2 - a^2) = 2$, то есть $b \in M$ и $a < b$. Таким образом, в M нет наибольшего элемента. Поэтому, если a – верхняя граница M, то $a^2 > 2$.

Пусть a – верхня граница M. Положим $q = a - \frac{a^2-2}{2a} = \frac{a}{2} + \frac{1}{a}$. Тогда $0 < q < a$ и $q^2 = a^2 - (a^2 - 2) + (\frac{a^2-2}{2a})^2 > a^2 - (a^2 - 2) = 2$. Что и требовалось доказать.

Последние два свойства позволяют нам сделать вывод о том, что хотя между любыми двумя рациональными числами существует третье рациональное число, все же рациональные числа "заполняют" числовую прямую "с пробелами" (конечно, если исходить из наших интуитивных представлений о непрерывности числовой прямой).

5.2 Категоричность системы аксиом рациональных чисел

В этом параграфе мы докажем, категоричность системы аксиом рациональных чисел, опираясь на то, что категорична система аксиом целых чисел. Доказательство не содержит каких-либо новых идей и, поэтому, предоставляется, в основном, читателю.

Теорема 5.2.1 *Система аксиом рациональных чисел категорична.*

Доказательство. Пусть $(Q,\ +,\ \cdot,\ <)$ и $(Q',\ +,\ \cdot,\ <)$ – две системы рациональных чисел (здесь, как и прежде, мы обозначаем операции и отношения в разных системах одинаковыми знаками). Обе системы содержат, в качестве подсистем, системы целых чисел Z и Z' соответственно.

Но Z и Z' изоморфны. Пусть $f : Z \to Z'$ – изоморфизм этих систем целых чисел.

В силу свойства 2 предыдущего параграфа, каждое рациональное число есть частное двух целых чисел. Зададим отображение $\varphi : Q \to Q'$ так, что $\varphi(mn^{-1}) = f(m)f(n)^{-1}$.

Упражнение 5. Доказать, что φ – изоморфизм систем рациональных чисел, рассмотренных в теореме.

5.3 Построение модели системы аксиом рациональных чисел.

Пусть $(Z,\ +,\ \cdot,\ <)$ – система целых чисел, N – множество натуральных чисел и $N \subset Z$. Рассмотрим множество $M = Z \times N$. На этом множестве определим операции $+'$, $\cdot'$ и отношение $<'$ следующим образом:
$(x,n) +' (y,m) \stackrel{def}{=} (xm + yn, mn)$;
$(x,n) \cdot' (y,m) \stackrel{def}{=} (xy, mn)$;
$(x,n) <' (y,m) \stackrel{def}{\Longleftrightarrow} xm < yn$.

Упражнение 6. Проверить, что $(M,\ +',\ \cdot',\ <')$ – не является упорядоченным полем.

На множестве M зададим отношение $\sim$ следующим образом:
$(x,n) \sim (y,m) \stackrel{def}{\Longleftrightarrow} xm = yn$.

Упражнение 7. Доказать, что $\sim$ – конгруенция на $(M,\ +',\ \cdot',\ <')$.

Упражнение 8. Доказать, что если $(x,n) <' (y,m)$, $(x',n') <' (y',m')$, $(x,n) \sim (x',n')$, $(y,m) \sim (y',m')$, то $(x',n') <' (y',m')$.

Из всего доказанного сделаем вывод: фактор-система $Q = (M/\sim,\ \oplus,\ \odot,\ \prec)$, где операции и отношение определены стандартным способом, является упорядоченным полем.

Осталось установить простоту этого поля, чтобы убедиться в том, что нами построена модель системы аксиом рациональных чисел. Действительно, прежде всего отметим, что единичным элементом поля Q является класс $\overline{(1,1)}$. Для класса $\overline{(a,n)}$ обратным является класс $\overline{(n',a')}$, где $a' = |a|$ и $n' = n$, если $a > 0$, $n' = -n$, если $a < 0$. Тогда $\overline{(1,n)} = (\underbrace{\overline{(1,1)} + \ldots + \overline{(1,1)}}_{n \text{ раз}})^{-1}$ и, если $0 \leq a$, то $\overline{(a,n)} = \overline{(a,1)} \odot \overline{(1,n)}$, а если $a < 0$, то $\overline{(a,n)} = -\overline{(|a|,1)} \odot \overline{(1,n)}$.

Таким образом, мы видим, что поле Q порождается своим единичным элементом и, следовательно, является простым.

Упражнение 9. Доказать все утверждения, сформулированные после предыдущего упражнения.

Глава 6

Действительные числа

6.1 Определение, свойства, категоричность

Как мы уже видели, поле рациональных чисел не является непрерывно упорядоченным. Для чего же нам нужна непрерывно упорядоченная числовая система? Какие интуитивные доводы имеются в пользу существования такой системы? Обсудим эти вопросы немного подробнее.

Во-первых, мы предполагаем, что числа являются мерами длины. Если выбран единичный отрезок, то мы хотим иметь возможность выражать длину любого отрезка некоторым числом. Таким образом, выбрав на прямой начало координат, мы любой точке прямой поставим в соответствие некоторое число — расстояние от этой точки до начала координат (если выбранная точка расположена справа от начала координат). На первый взгляд, для этого достаточно одних рациональных чисел, поскольку мы можем с какой угодно точностью выразить длину отрезка рациональным числом и, кроме того, множество рациональных чисел плотно упорядочено. Однако, существует отрезок, квадрат длины которого равен, например, 2 — это гипотенуза прямоугольного треугольника с катетами длины 1. Рационального числа a, такого, что $a^2 = 2$ не существует. Опираясь на интуицию, можно заключить, что длина такого отрезка должна быть точной нижней границей множества $\{x|\ x > 0 \wedge x^2 > 2\}$. Тем самым, свойство непрерывной упорядоченности мы интуитивно связываем с "заполнением" всей прямой числами.

Опишем некоторые ожидаемые свойства обсуждаемой числовой систе-

мы. Поскольку длины любых отрезков можно сравнивать, эта числовая система должна быть упорядоченной. Так как мы хотим расширить поле рациональных чисел, не потеряв при этом свойств чисел как мер длины, то искомая система должна быть полем. Но в любом упорядоченном поле $x^2 \geq 0$ для любого элемента x, поэтому, в таком поле не имеет решения уравнение $x^2 + 1 = 0$. В то же время такое уравнение, как $x^2 - 2 = 0$ должно в этом поле иметь решение. Мы хотим также, чтобы любое уравнение вида $x^n - a = 0$, где $a \geq 0$ имело решение в этом поле, другими словами, мы хотим иметь возможность извлекать корни любой натуральной степени из неотрицательных чисел.

Итак, задачей этой главы является доказательство существования и единственности непрерывно упорядоченного поля. Для этого нам понадобится ввести ряд новых понятий и доказать некоторые вспомогательные утверждения.

Определение 1. Линейно упорядоченная система $(A, <)$ без наибольшего и наименьшего элементов называется непрерывно упорядоченной, если $(A, <)$ — плотно упорядоченна и каждое непустое, ограниченное снизу подмножество множества A имеет точную нижнюю границу.

Упражнение 1. Доказать, что $(A, <)$ — непрерывно упорядоченная система, тогда и только тогда, когда всякое ограниченное сверху подмножество имеет точную верхнюю границу.

Определение 2. Пусть $(S, <)$ — линейно упорядоченная система. Подмножество A множества S называется верхним классом в $(S, <)$, если выполняются следующие условия:
(1) $A \neq \emptyset$ и $A \neq S$;
(2) если $x \in A$ и $x < x'$, то $x' \in A$;
(3) в A нет наименьшего элемента.
Система $(S, <)$ называется непрерывно упорядоченной, если она плотно упорядоченна, не содержит наибольшего и наименьшего элементов и любой верхний класс имеет точную нижнюю границу. Совокупность всех верхних классов для $(S, <)$ обозначим $U(S)$.

Упражнение 2. Доказать эквивалентность данных выше определений непрерывной упорядоченности.

Пусть $(S,\ <)$ — плотно упорядоченная система, не содержащая наибольшего и наименьшего элементов и пусть $u, v \in U(S)$. Положим $u \prec v \overset{def}{\Longleftrightarrow} v \subset u$. Можно доказать, что система $(U(S),\ \prec)$ — непрерывно упорядоченна и содержит подсистему, изоморфную $(S,\ <)$. Такой подсистемой является множество всех верхних классов $C_a = \{x \in S |\ a < x\}$, где $a \in S$. Доказательство предоставляем читателю.

Можно также доказать, что если $(S,\ <)$ — непрерывно упорядоченная система, то $(U(S),\ \prec)$ изоморфна $(S,\ <)$.

Одну плотно упорядоченную систему без наибольшего и наименьшего элементов мы уже построили, это — $(Q,\ <)$, таким образом, $(U(Q),\ \prec)$ — непрерывно упорядоченная система. Но существование непрерывно упорядоченного расширения системы $(Q,\ <)$ пока не означает для нас, что существует непрерывно упорядоченное поле, являющееся расширением поля рациональных чисел.

Определение 3. Непрерывно упорядоченное поле называется полем действительных чисел.

Ранее было доказано, что всякое упорядоченное поле бесконечно, а значит содержит подполе, изоморфное полю рациональных чисел. Основываясь на этом факте, докажем единственность поля действительных чисел.

Теорема 6.1.1 *Любые два поля действительных чисел изоморфны.*

Доказательство этого утверждения разобьем на ряд этапов.

Лемма 6.1.1 *Если* $(P, +, \cdot, <)$ *– непрерывно упорядоченное поле, то:*
(1) $\forall a \in P\ \exists n \in N(a < n)$;
(2) $\forall a > 0\ \exists n \in N(\frac{1}{n} < a)$;
(3) $\forall a, b \in P$ *(если* $a < b$, *то существует такое* $x \in Q$, *что* $a < x < b$*).*

Доказательство.(1) Предположим, что существует элемент $a \in P$ такой, что $\forall n \in N(n \leq a)$, тогда N – ограничено сверху и, следовательно, в P существует $\sup(N)$. Пусть $b = \sup(N)$. Имеем $\forall n \in N(n + 1 \leq b)$, но тогда $\forall n \in N(n \leq b - 1)$, то есть $b - 1$ – верхняя граница для N и, поскольку $b - 1 < b$, получаем противоречие.

(2) Из (1) следует, что для элемента $\frac{1}{a}$ существует такое $n \in N$, что $\frac{1}{a} < n$, но тогда $\frac{1}{n} < a$.

(3) Пусть $a < b$, тогда существует $n \in N$ такое, что $\frac{1}{n} < b - a$. Рассмотрим множество $A = \{m \in Z |\ a < \frac{m}{n}\}$. A – непустое, так как существует $k \in N$ такое, что $a < k$, то есть $a < \frac{nk}{n}$. Если $m \in A$, $m < t$, то $t \in A$. Кроме того, $A \neq Z$, так как для $(-a)$ существует $l \in N$ такое, что $(-a) < l$, тогда $(-l) < a$, а, значит $\frac{(-l)n}{n} < a$, то есть $(-l)n \notin A$. Но во всяком ограниченном снизу множестве целых чисел есть наименьший элемент. Пусть m – наименьший в A элемент. Тогда $\frac{m-1}{n} \leq a < \frac{m}{n}$, откуда $\frac{m-1}{n} + \frac{1}{n} \leq a + \frac{1}{n}$ и учитывая, что $\frac{1}{n} < b - a$ (то есть $\frac{1}{n} + a < b$), получим $\frac{m}{n} < b$. Окончательно, $a < \frac{m}{n} < b$. Лемма доказана.

Упражнение 3. Доказать, что условие (1) леммы эквивалентно архимедовости порядка в P: если $0 < a < b$, то существует $n \in N$ такое, что $b < na$.

Лемма 6.1.2 *В непрерывно упорядоченном поле* $(P, +, \cdot, <)$ *выполняются следующие условия:*
(1) если $a \in P$, *то* $C_a \stackrel{def}{=} \{x \in Q |\ a < x\} \in U(Q)$;
(2) если $a, b \in P$ *и* $a < b$, *то* $C_a \prec C_b$;

(3) если $A \in U(Q)$, *то существует единственный* $a \in P$ *такой, что* $A = C_a$.

Доказательство. (1) Прежде всего отметим, что из пункта (1) предыдущей леммы следует, что $C_a \neq \emptyset$. Из пункта (3) леммы 6.1.1 следует, что $C_a \neq Q$, так как существует $x \in Q$ такой, что $a - 1 < x < a$, то есть $x \notin C_a$. Ясно, что если $x \in C_a$ и $x < x'$, где $x' \in Q$, то $x' \in C_a$. В C_a нет наименьшего элемента, так как, если $x \in C_a$, то $a < x$, а, по лемме 6.1.1, существует $x' \in Q$ такой, что $a < x' < x$, то есть $x' \in C_a$. Поэтому, $C_a \in U(Q)$.

(2) Следует из определений и условия (3) леммы 6.1.1.

(3) Пусть $A \in U(Q)$, тогда $A \neq \emptyset$ и A ограниченно снизу в P. Пусть $a = \inf(A)$ в P, $a \notin A$, так как в A нет наименьшего элемента. Следовательно, если $x \in A$, то $a < x$ откуда $x \in C_a$, то есть $A \subseteq C_a$.

Пусть $x \in C_a$, тогда $a < x$ и $x \in Q$. Если бы для любого $x' \in A$ было $x \leq x'$, то $a \neq \inf(A)$. Поэтому, существует $x' \in A$ такой, что $x' < x$, но тогда $x \in A$. Таким образом, $C_a \subseteq A$, а значит $C_a = A$. Единственность a следует из пункта (2) этой леммы. Лемма доказана.

Теперь мы можем расмотреть отображение $f : P \longrightarrow U(Q)$ такое, что $f(a) = C_a$. Из доказанного выше следует, что f – биекция, сохраняющая порядок. Определим на $U(Q)$ операции $\oplus, \otimes, \ominus$ следующим образом:
$C_a \oplus C_b \stackrel{def}{=} C_{a+b}$;
$C_a \otimes C_b \stackrel{def}{=} C_{ab}$;
$\ominus C_a \stackrel{def}{=} C_{(-a)}$.

Лемма 6.1.3 *Непрерывно упорядоченное поле* $(P,\ +,\ \cdot,\ -,\ 0,\ 1)$ *изоморфно системе* $(U(Q),\ \oplus,\ \otimes,\ \ominus,\ C_0,\ C_1)$.

Доказательство. Как мы уже видели, отображение $f : P \longrightarrow U(Q)$ такое, что $f(a) = C_a$ сохраняет порядок и является биекцией.

Определения операций $\oplus$, $\otimes$, $\ominus$ на $U(Q)$ позволяют заключить, что f – гомоморфизм. Лемма доказана.

Теперь, чтобы доказать утверждение теоремы покажем, что определения операций $\oplus$, $\otimes$, $\ominus$ не зависят от поля P. Для этого необходимо определить эти операции только через свойства поля Q, а именно, доказать следующее утверждение.

Лемма 6.1.4 *Пусть* $A, B \in U(Q)$, *тогда:*
(1) $A \oplus B = \{x + y |\ x \in A,\ y \in B\}$;
(2) $\ominus A = \{u \in Q |\ \exists z \in Q(z < u \wedge \forall x \in A(-x < z))\}$;
(3) если $A \prec C_0$, *то* $C_0 \prec \ominus A$;
(4) если $C_0 \preceq A \wedge C_0 \preceq B$, *то* $A \otimes B = \{xy |\ x \in A,\ y \in B\}$;
(5) если $A \prec C_0,\ C_0 \preceq B$, *то* $A \otimes B = \ominus((\ominus A) \otimes B)$;
(6) если $C_0 \preceq A,\ B \prec C_0$, *то* $A \otimes B = \ominus(A \otimes (\ominus B))$;
(7) если $A \prec C_0,\ B \prec C_0$, *то* $A \otimes B = (\ominus A) \otimes (\ominus B)$.

Доказательство предоставляем читателю.

Таким образом, любые два поля действительных чисел изоморфны полю $(U(Q),\ \oplus,\ \otimes,\ \ominus, C_0,\ C_1)$, следовательно, изоморфны между собой. Теорема доказана.

Теперь мы можем построить непрерывно упорядоченное поле, считая свойства (1), (2), (4)—(7) определениями операций $\oplus$, $\otimes$, $\ominus$ на $U(Q)$. Доказательство того, что так определенная система
$(U(Q),\ \oplus,\ \otimes,\ \prec,\ C_0,\ C_1)$ является непрерывно упорядоченным полем достаточно громоздко и здесь мы не будем его проводить.

Существует другой способ построения непрерывно упорядоченного поля. Он больше похож на ранее рассмотренные способы построения числовых систем. Кроме того, при детальном осуществлении предлагаемого плана, можно получить интересные попутные результаты. Опишем этот способ.

Пусть Q^N — множество всех последовательностей рациональных чисел. Элементы из Q^N будем обозначать (a_k), (b_k) и т.п. Определим на Q^N бинарные операции $\oplus$, $\odot$ следующим образом:
$(a_k) \oplus (b_k) \stackrel{def}{=} (a_k + b_k)$, $(a_k) \odot (b_k) \stackrel{def}{=} (a_k \cdot b_k)$.

Последовательность (a_k) из Q^N называется фундаментальной, если для любого положительного элемента $\varepsilon \in Q$ существует $n_0 \in N$ такое, что $|a_k - a_n| < \varepsilon$ для всех k, n больших n_0. Множество всех фундаментальных последовательностей рациональных чисел обозначим $F(Q)$.

Можно доказать, что $F(Q)$ замкнуто относительно операций $\oplus, \odot$ и система $(F(Q),\ \oplus,\ \odot)$ является коммутативным кольцом с единицей.

Далее, введем на $F(Q)$ отношение $\sim$ следующим образом:
$(a_k) \sim (b_k) \stackrel{def}{\Longleftrightarrow} (a_k - b_k)$ сходится к нулю (здесь мы считаем известным определение предела числовой последовательности).
Легко доказать, что отношение $\sim$ является конгруенцией в кольце $(F(Q),\ \oplus,\ \odot)$, а также то, что фактор-кольцо кольца $(F(Q),\ \oplus,\ \odot)$ по конгруенции $\sim$ является полем. Обозначим это поле $(F,\ +,\ \cdot)$, а его элементы (классы по $\sim$) будем обозначать $[(a_k)]$, $[(b_k)]$ и т.д.

На $F(Q)$ введем отношение $<$:
$(a_k) < (b_k) \stackrel{def}{\Longleftrightarrow}$ существуют $n_0 \in N$ и рациональное положительное ε такие, что $b_k - a_k \geq \varepsilon$ для любого $k \geq n_0$.
Отношение $<$ является отношением порядка на $F(Q)$, причем, если $(a_k) < (b_k)$, $(a_k) \sim (c_k)$, $(b_k) \sim (d_k)$, то $(c_k) < (d_k)$. Поэтому корректно следующее определение порядка на F: $[(a_k)] < [(b_k)] \stackrel{def}{\Longleftrightarrow} (a_k) < (b_k)$.
Здесь, чтобы не загромождать текст, мы использовали одинаковые обозначения для отношений порядка в различных системах.

Можно доказать, что система $(F,\ +,\ \cdot,\ <)$ — архимедовски упорядоченное поле, в котором всякая фундаментальная последовательность сходится, а это эквивалентно тому, что поле $(F,\ +,\ \cdot,\ <)$ — непрерывно упорядоченно. Последнее утверждение, конечно, также нуждается в доказательстве.

На этом изложение нашего плана построения непрерывно упорядоченного поля завершается. Доказательство всех сформулированных в нем утверждений предоставляем читателю. В дальнейшем, поле действительных чисел будем обозначать R.

После того, как мы доказали существование и единственность поля действительных чисел, можно ввести понятия модуля числа, предела функции, непрерывности функции и т.д. Можно, например, убедиться в возможности извлечения корня n-й степени из положительных чисел.

Теорема 6.1.2 *Пусть a – положительное действительное число. Тогда* $\forall n \in N\ \exists! b \in R(b^n = a \wedge b > 0)$.

Доказательство. Функция $f = x^n - a$ — непрерывна на интервале $[0,\ a+1]$ и на концах этого интервала принимает значения разных знаков. Тогда, по известной теореме о промежуточном значении, существует число $b \in [0,\ a+1]$ такое, что $f(b) = 0$, то есть $b^n = a$. Так как $b \in [0,\ a+1],\ b \neq 0$, то $b > 0$.

Пусть $c^n = a$ для некоторого положительного $c \in R$. Если $c < b$, то $c^n < b^n = a$ — противоречие. Если $b < c$, то $a = b^n < c^n$ — противоречие. Следовательно, $b = c$. Теорема доказана.

В заключение отметим, что в поле R не существуют корни уравнений вида $x^{2n} + a = 0$, где $a > 0,\ n \in N$, то есть не существует корней четной степени из отрицательных чисел. Реализовать возможность извлечения таких корней позволяет система комплексных чисел, о которой идет речь в следующей главе.

Глава 7

Комплексные числа

7.1 Обоснование, категоричность, модель

Считая числа мерами длины и желая иметь возможность решать различные уравнения, мы расширили систему натуральных чисел до системы действительных чисел, которая удовлетворяет всем нашим потребностям, связанным с измерениями. Однако, в поле действительных чисел разрешимы далеко не всякие уравнения. Например, уравнение $x^2 + 1 = 0$ не имеет действительных корней. Нетрудно видеть, что если бы в некотором поле, содержащем R, существовал корень этого уравнения, то были бы разрешимы и все уравнения вида $x^{2n} + a = 0$, то есть мы имели бы возможность извлекать корни четной степени из отрицательных чисел. Возникает вопрос: существует ли такое поле?

Прежде, чем ответить на поставленный вопрос, исследуем некоторые свойства, которыми должно обладать поле, определенное сформулированными условиями. Ясно, например, что это поле не может быть упорядоченным, так как в любом упорядоченном поле $x^2 \geq 0$, для любого x и $1 > 0$, поэтому $x^2 + 1 > 0$. Некоторые другие свойства перечислены в следующей теореме.

Теорема 7.1.1 *Пусть* $(P, +, \cdot)$ *— поле, содержащее* R *в качестве подполя. Пусть в* P *существует элемент* u *такой, что* $u^2 = -1$. *Тогда для любых* $a, b, c, d \in R$

(1) $a+bu=c+du \Longleftrightarrow a=c \wedge b=d$ *;*
(2) $(a+bu)+(c+du)=(a+c)+(b+d)u$ *;*
(3) $-(a+bu)=(-a)+(-b)u$ *;*
(4) $(a+bu)\cdot(c+du)=(ac-bd)+(ad+bc)u$ *;*
(5) $(a+bu)\cdot(a-bu)=a^2+b^2$ *;*
(6) если $a+bu\neq 0$*, то* $a^2+b^2>0$ *и* $\frac{1}{a+bu}=\frac{a}{a^2+b^2}+\frac{-b}{a^2+b^2}u$ *;*
(7) $D=\{a+bu|\ a,b\in R\}$ *— подполе поля* P*.*

Доказательство. (1) Пусть $a+bu=c+du$, тогда $a-c=(d-b)u$, то есть $(a-c)^2=-(d-b)^2$. Так как $(a-c)^2\geq 0$, $-(d-b)^2\leq 0$, то $(a-c)^2=(d-b)^2=0$. Следовательно, $a=c$, $b=d$.
(2)—(5) следуют из определения поля.
(6) Если $a+bu\neq 0$, то $a+bu\neq 0+0u$, тогда, по (1), $a\neq 0$, или $b\neq 0$, откуда, $a^2+b^2>0$ и (6) следует из (5).
(7) Из (2)—(6) следует, что D замкнуто относительно $+$ и $\cdot$ и содержит $0=0+0u$, $1=1+0u$, противоположный для каждого $x\in D$ элемент, обратный — для каждого ненулевого элемента. Кроме того, $R\subset D$, так как $\forall x\in R\,(x=x+0u)$.

Эта теорема указывает способ построения поля P, содержащего подполе, изоморфное R, причем в P существует элемент u такой, что $u^2=-1$.

Теорема 7.1.2 *Существует поле* $(P+,\ \cdot)$ *такое, что*
(1) $R'\subseteq P$*, где* R' *– подполе поля* P *и* $R'\cong R$ *;*
(2) $\exists u\in P\,(u^2=-1)$ *;*
(3) $\forall z\in P\ \exists a,b\in R'\,(z=a+bu)$*.*

Доказательство. Пусть $P=R\times R$. определим на P операции: $(a,b)+(c,d)\stackrel{def}{=}(a+c,b+d)$, $(a,b)\cdot(c,d)\stackrel{def}{=}(ac-bd,ad+bc)$. Здесь операции в P обозначены, для упрощения записи, так же, как в R.

Достаточно просто доказать, что $(P,\ +,\ \cdot)$ – поле, в котором нулевой элемент $\bar{0}=(0,0)$, единичный элемент $\bar{1}=(1,0)$, $-(a,b)=(-a,-b)$. Для $(a,b)\neq(0,0)$, $(a,b)^{-1}=(\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2})$. Пару $(0,1)$ обозначим u. Очевидно, $u^2=-\bar{1}$.

Пусть $R' = \{(a,0) |\ a \in R\}$. Нетрудно проверить, что R' – подполе в P и отображение $f : R \longrightarrow R'$ такое, что $f(a) = (a,0)$ является изоморфизмом между R и R'. Теорема доказана.

Теорема 7.1.3 *Если* $(P,\ +,\ \cdot)$ *и* $(P',\ +',\ \cdot')$ *– поля, удовлетворяющие условиям (1)–(3) предыдущей теоремы, то* $(P,\ +,\ \cdot) \cong (P',\ +',\ \cdot')$.

Доказательство. Поля P и P' содержат, соответственно, подполя R_1 и R_2, изоморфные полю R. Следовательно, $R_1 \cong R_2$ и пусть φ – изоморфизм R_1 на R_2.

Зададим отображение $f : P \longrightarrow P'$ следующим образом:
$f(a+bu) \stackrel{def}{=} \varphi(a) +' \varphi(b)u'$, где $u^2 = -1$ в P и $(u')^2 = -1'$ в P'. Проверка того, что отображение f является изоморфизмом тривиальна и предоставляется читателю.

В дальнейшем, полем комплексных чисел можно называть некоторое конкретное поле $(C,\ +,\ \cdot)$ и через i обозначать элемент из C, удовлетворяющий условиям:
(1) $R \subset C$ и R – подполе в $(C,\ +,\ \cdot)$;
(2) $i^2 = -1$;
(3) $\forall z \in C\ \exists! a \in R\ \exists! b \in R\ (z = a + bi)$.

Построение поля комплексных чисел на множестве $R \times R$ наводит на мысль о представлении комплексных чисел точками, или векторами на плоскости. Развивая эту тему, можно ввести понятие тригонометрической формы комплексного числа и получить различные результаты о комплексных числах и их геометрическую интерпретацию. Однако, рассмотрение этих вопросов не входит в наши задачи, здесь нас интересует лишь доказательство существования и единственности определенной числовой системы, а этой цели мы достигли.

Подводя итог, отметим, что расширяя систему действительных чисел, мы "потеряли" такое свойство, как упорядоченность. Дальнейшие исследования показывают, что попытки расширить поле комплексных чисел,

сохранив основные, важные для нас "алгебраические" свойства приводят к потере коммутативности умножения, а дальнейшие шаги в этом направлении — к потере возможности деления. Получающиеся на этом пути алгебраические системы уже не являются полями. Эти соображения позволяют считать комплексные числа, в некотором смысле, наибольшей числовой системой.

Глава 8

Расширения числовых систем

В этой главе мы докажем сформулированный в конце главы 7 тезис, а именно, опишем алгебраические системы, являющиеся расширением поля комплексных чисел и сохраняющие некоторые основные свойства числовых систем. Для проведения доказательств нам необходимо ввести несколько новых понятий. Кроме того, будем считать известными из курса алгебры основные сведения о векторных пространствах.

Упражнение 1. Вспомните определения и докажите следующие утверждения.
В векторном пространстве над полем P:
1) если часть системы векторов линейно зависима, то и вся система линейно зависима;
2) если система векторов линейно независима, то любая ее непустая часть линейно независима;
3) если система векторов $a_1, ..., a_n$ линейно независима и $\lambda_1, ..., \lambda_n$ - ненулевые скаляры, то система $\lambda_1 a_1, ..., \lambda_n a_n$ - линейно независима;
4) если система векторов $a_1, ..., a_n$ - линейно независима и $i \neq 1$, то система $a_1 - a_i, a_2, ..., a_n$ - линейно независима.

8.1 Ассоциативные линейные алгебры

Определение 1. Ассоциативной линейной алгеброй ранга n над полем действительных чисел $\mathbf{R}$ называется n-мерное векторное пространство $\mathbf{V}$ над $\mathbf{R}$, в котором определена операция умножения векторов и выполняются следующие свойства:
1. $\forall \alpha \in \mathbf{R} \forall u, v \in \mathbf{V}(\alpha(uv) = u(\alpha v))$;
2. $\forall u, v, w \in \mathbf{V}(u(vw) = (uv)w)$;
3. $\forall u, v, w \in \mathbf{V}(u(v+w) = uv + uw \wedge (v+w)u = vu + wu)$.

Из определения следует, что ассоциативная линейная алгебра $(\mathbf{V}, +, \cdot)$, где $+$ и $\cdot$ - операции сложения и умножения векторов соответственно, является кольцом (в общем случае - некоммутативным).

В дальнейшем ассоциативную линейную алгебру над полем $\mathbf{R}$ будем называть просто алгеброй. Нулевой элемент алгебры (нулевой вектор) будем обозначать θ.

Пусть $\mathbf{K}$ - алгебра ранга n, тогда в $\mathbf{K}$ есть базис $e_1, \ldots, e_n$. Если $a, b \in \mathbf{K}$, то $a = \sum_{i=1}^{n} \alpha_i e_i$, $b = \sum_{j=1}^{n} \beta_j e_j$ – линейные комбинации векторов базиса. Согласно определению,
$ab = \sum_{i=1}^{n} \alpha_i e_i \sum_{j=1}^{n} \beta_j e_j = \sum_{i=1}^{n} \sum_{j=1}^{n} (\alpha_i \beta_j)(e_i e_j)$.

Можно записать $ab = \sum_{i,j=1}^{n} (\alpha_i \beta_j)(e_i e_j)$, то есть произведение ab является линейной комбинацией n^2 слагаемых вида $e_i e_j$. Но любой элемент $e_i e_j$, в свою очередь, является линейной комбинацией векторов базиса:
$e_i e_j = \sum_{k=1}^{n} \gamma_{ijk} e_k$.

Коэффициенты γ_{ijk} называются структурными константами данной алгебры. Количество структурных констант равно n^3 и ими полностью определяется умножение элементов алгебры $\mathbf{K}$.

Если умножение в алгебре коммутативно, то для любых i, j, k выполняется $\gamma_{ijk} = \gamma_{jik}$ и алгебра $\mathbf{K}$ называется коммутативной.

Определение 2. Алгебра $\mathbf{K}$ называется алгеброй с делением, если для любых элементов a, $b \in \mathbf{K}$, где $a \neq 0$, уравнения $ax = b$ и $ya = b$ имеют единственные решения. При этом, элемент x называется левым

частным, а элемент y – правым частным при делении b на a.

Так как кольцо с делением называется телом, то алгебра с делением является телом. Если в алгебре K существует нейтральный элемент относительно умножения, то он называется единицей алгебры $\mathbf{K}$.

Поскольку первые примеры алгебр с единицей появились в качестве расширений поля комплексных чисел, они получили название "гиперкомплексные системы а их элементы стали называть гиперкомплексными числами. В настоящее время это название устарело, так как подобные примеры дают далеко не исчерпывающее представление об ассоциативных линейных алгебрах. Тем не менее, в рамках данной книги алгебры с единицей нас интересуют, прежде всего, как расширения числовых систем, поэтому мы сохраним за ними наименование гиперкомплексные системы.

Рассмотрим некоторые примеры ассоциативных линейных алгебр.

Пример 1. Алгебра произвольного ранга, в которой произведение любых базисных элементов равно нулевому элементу. Очевидно, что в этом случае все структурные константы равны нулю и произведение любых элементов равно нулевому элементу алгебры.

Пример 2. Трехмерное арифметическое векторное пространство с векторным умножением. Если e_1, e_2, e_3 – стандартный базис, то $e_1^2 = e_2^2 = e_3^2 = \theta$, $e_1e_2 = e_3$, $e_2e_1 = -e_3$, $e_2e_3 = e_1$, $e_3e_2 = -e_1$, $e_3e_1 = e_2$, $e_1e_3 = -e_2$.
Легко найти все структурные константы, например, $\gamma_{123} = 1$, $\gamma_{213} = -1$.

Пример 3. Поле действительных чисел, рассматриваемое как одномерное векторное пространство над $\mathbf{R}$ с обычным умножением действительных чисел является гиперкомплекскной системой. Единичным элементом является число 1, $1^2 = 1$, единственная структурная константа равна 1.

Понятно, что отображение $f : a1 \to a$ является изоморфизмом этой

гиперкомплексной системы (как поля) и поля действительных чисел.

Пример 4. Рассмотрим гиперкомплексную систему $\mathbf{K}$ ранга 2 с базисными элементами $e_1,\ e_2$ и равенствами $e_1^2 = e_1,\ e_1e_2 = e_2e_1 = e_2,\ e_2^2 = -e_1$. Отображение $f : \mathbf{K} \to \mathbf{C}$ такое, что $f(\alpha e_1 + \beta e_2) = \alpha + \beta i$ является гомоморфизмом. Действительно
$f(\alpha_1 e_1 + \alpha_2 e_2) + (\beta_1 e_1 + \beta_2 e_2)) = f((\alpha_1 + \beta_1)e_1 + (\alpha_2 + \beta_2)e_2) = (\alpha_1 + \beta_1) + (\alpha_2 + \beta_2)i = (\alpha_1 + \alpha_2 i) + (\beta_1 + \beta_2 i) = f(\alpha_1 e_1 + \alpha_2 e_2) + f(\beta_1 e_1 + \beta_2 e_2)$,
$f((\alpha_1 e_1 + \alpha_2 e_2)(\beta_1 e_1 + \beta_2 e_2)) = f((\alpha_1\beta_1 - \alpha_2\beta_2)e_1 + (\alpha_1\beta_2 + \alpha_2\beta_1)e_2) = (\alpha_1\beta_1 - \alpha_2\beta_2) + (\alpha_1\beta_2 + \alpha_2\beta_1)i = (\alpha_1 + \alpha_2 i)(\beta_1 + \beta_2 i) = f(\alpha_1 e_1 + \alpha_2 e_2)f(\beta_1 e_1 + \beta_2 e_2)$.
Таким образом, данная гиперкомплексная система является полем, изоморфным полю комплексных чисел.

Пример 5. Если немного изменим структурные константы в примере 4, а именно, в гиперкомплексной системе ранга 2 положим $e_1^2 = e_1,\ e_1e_2 = e_2e_1 = e_2,\ e_2^2 = \theta$, получим систему, так называемых, дуальных чисел. Эта система коммутативна, e_1 – единичный элемент. Уравнение $e_2x = e_1$ не имеет решения. Действительно, если элемент a является решением этого уравнения, то $e_2a = e_1 \Rightarrow e_2(e_2a) = e_2e_1 \Rightarrow (e_2e_2)a = e_2 \Rightarrow \theta a = e_2 \Rightarrow e_2 = \theta$ – противоречие.
Таким образом, в этой гиперкомплексной системе деление не всегда выполнимо.

Упражнение 2. Для каждого ли ненулевого элемента гиперкомплексной системы ранга 2, где $e_1^2 = e_1,\ e_1e_2 = e_2e_1 = e_2,\ e_2^2 = e_1$ существует обратный элемент?

8.2 Тело кватернионов

Особое внимание в этом разделе мы обращаем на построенную ниже гиперкомплексную систему H ранга 4 с делением – тело кватернионов. Эта система была построена в 1850 году английским математиком У.Гамильтоном и в дальнейшем изложении играет важную роль.

Базисные элементы традиционно обозначаются следующим образом: $e_1 = 1,\ e_2 = i,\ e_3 = j,\ e_4 = k$. Элемент 1 – нейтральный по умножению и определяются соотношения: $i^2 = j^2 = k^2 = -1,\ jk = i,\ kj = -i,\ ij = k,\ ji = -k,\ ki = j,\ ik = -j$. Элементы этой системы называются кватернионами.

Легко проверить, что подкольца, порожденные в системе кватернионов множествами $\{1, i\},\ \{1, j\},\ \{1, k\}$, изоморфны полю комплексных чисел. Например, отображение $f : \mathbf{C} \to H$, такое что $f(a+bi) = a1+bk$, является одним из указанных изоморфизмов. Таким образом, система H является расширением поля комплексных чисел, однако, сама не является полем, поскольку умножение в ней не коммутативно.

Докажем, что система H – тело. Кватернион $\bar{q} = a - bi - cj - dk$ называется сопряженным кватерниону $q = a + bi + cj + dk$. Найдем произведение $q\bar{q},\ q\bar{q} = (a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2 + (ab-ab-cd+cd)i+(ac-ac-bd+bd)j+(ad-ad-bc+bc)k = a^2+b^2+c^2+d^2$. Здесь, в силу указанного изоморфизма, элемент e_1 отождествлен с действительным числом 1, а элемент вида $a1$ – с действительным числом a. Число $a^2+b^2+c^2+d^2$ называется нормой кватерниона $q = a+bi+cj+dk$ и обозначается $N(q)$. Ясно, что $N(q) = N(\bar{q})$ и, если $q \neq \theta$, то $N(q) > 0$. Далее, если $q \neq \theta$, то $q(\frac{\bar{q}}{N(q)}) = \frac{N(q)}{N(q)} = 1$ и $(\frac{\bar{q}}{N(q)})q = \frac{N(q)}{N(q)} = 1$. Следовательно, $q^{-1} = \frac{\bar{q}}{N(q)}$ – кватернион, обратный q и возможность деления становится очевидной. Левые и правые частные от деления q_1 на q не обязательно совпадают, так как $q(q^{-1}q_1) = q_1,\ (q_1q^{-1})q = q_1$, то есть левое частное равно $q^{-1}q_1$, а правое – q_1q^{-1}.

Упражнение 3. Доказать, что для любых кватернионов $p,\ q$ выполняются равенства: $\overline{p+q} = \bar{p} + \bar{q},\ \overline{pq} = \bar{q}\bar{p},\ N(pq) = N(p)N(q)$.

В кватернионе $q = a + bi + cj + dk$ число a называется действительной частью, а $di + cj + dk$ – мнимой частью. Между множеством всех "мнимых" кватернионов с действительной частью равной нулю и множеством всех трехмерных векторов над полем $\mathbf{R}$ можно установить биекцию. Рассмотрим произведение $(x_1i + x_2j + x_3k)(y_1i + y_2j + y_3k) =$

$-(x_1y_1 + x_2y_2 + x_3y_3) + (x_2y_3 - x_3y_2)i + (x_3y_1 - x_1y_3)j + (x_1y_2 - x_2y_1)k$.
Если вспомнить свойства скалярного и векторного произведений в трехмерном евклидовом пространстве, то получим $pq = -(p,q) + [p,q]$, где круглыми скобками обозначено скалярное произведение, а квадратными – векторное произведение векторов.

Мы видим, что произведение мнимых кватернионов устанавливает новую для нас связь между скалярным и векторным произведениями векторов. Это свойство позволяет применять кватернионы в геометрии, а значит и в тех науках, где используется геометрия, например, в механике.

8.3 Теорема Фробениуса

Теперь мы можем приступить к доказательству утверждения, устанавливающего некоторый предел расширения числовых систем, при условии, что таковыми расширениями будем считать гиперкомплексные системы. Это доказательство, в основном, соответствует доказательству, проведенному в [1].
Сделаем предварительные замечания и докажем вспомогательные утверждения.

Лемма 8.3.1 *Гиперкомплексная система с делением (тело с единицей) не содержит делителей нуля.*

Доказательство. Если $ab = \theta$ и $b \neq \theta$, то существует b^{-1} такой, что $bb^{-1} = e$, где e – единица данного тела. Тогда $(ab)b^{-1} = \theta b^{-1}$, следовательно, $a(bb^{-1}) = ae = a = \theta$. Таким образом, хотя бы один из элементов a, b равен θ.

В гиперкомплексной системе с делением и единицей e над полем $\mathbf{R}$ множество элементов вида αe изоморфно полю $\mathbf{R}$. Поэтому, в дальнейшем, элемент e будем обозначать 1, а элементы вида αe – через α и называть их действительными числами.

Лемма 8.3.2 *Каждый элемент гиперкомплексной системы, отличный от действительного числа, является корнем уравнения вида* $(x-c)^2+d^2=0$, *где* c, d – *действительные числа и* $d\neq 0$.

Доказательство. Пусть $\mathbf{K}$ – гиперкомплексная система ранга n, $a\in\mathbf{K}$ и $a\notin\mathbf{R}$. Система $1,\ a,\ a^2,\ldots,a^n$ линейно зависима, так как состоит из n+1 элемента. Тогда $\alpha_n a^n+\ldots+\alpha_1 a+\alpha_0=0$ для некоторых действительных чисел $\alpha_0,\ldots\alpha_n$, не равных одновременно нулю.

Таким образом, a – корень многочлена $f(x)=\alpha_n x^n+\ldots+\alpha_1 x+\alpha_0$ с действительными коэффициентами, а такой многочлен, как известно из курса алгебры, можно представить в виде произведения неприводимых многочленов первой степени и второй степени с отрицательным дискриминантом, то есть $f(x)=f_1(x)f_2(x)\ldots f_r(x)$. Так как $f(a)=0$, то $f_1(a)\ldots f_r(a)=0$. По предыдущей лемме, хотя бы один из сомножителей $f_i(a)$ равен нулю, но так как $a\notin\mathbf{R}$, то a не может быть корнем многочлена первой степени над $\mathbf{R}$. Поэтому, a – корень многочлена x^2+px+q, где $\frac{p^2}{4}-q<0$ (ясно, что $q>0$).

Уравнение $x^2+px+q=0$ можно записать в виде $(x-c)^2+d^2=0$, где $c=-\frac{p}{2}$, $d=\sqrt{q-\frac{p^2}{4}}$. Что и требовалось доказать.

Лемма 8.3.3 *В гиперкомплексной системе ранга n существует базис* $1,\ i_2,\ i_3,\ldots,\ i_n$ *такой, что* $i_2^2=i_3^2=\ldots=i_n^2=-1$.

Доказательство. Из курса алгебры известно, что любую линейно независимую систему векторов векторного пространства можно дополнить до базиса этого пространства. Рассмотрим базис $1,\ t_2,\ t_3,\ldots,\ t_n$. Элементы $t_2,\ \ldots,\ t_n$ не являются действительными числами (иначе эта система векторов была бы линейно зависима). Тогда, по предыдущей лемме, каждый элемент t_ν $(\nu=2,\ldots,\ n)$ удовлетворяет равенству $(t_\nu-c_\nu)^2+d_\nu^2=0$, то есть $\left(\frac{t_\nu-c_\nu}{d_\nu}\right)^2=-1$. Положим $i_\nu=\frac{t_\nu-c_\nu}{d_\nu}$. Тогда $i^2=-1$ и, по упражнению 1, система $1,\ i_2,\ldots,\ i_n$ – линейно независима, то есть является базисом.

Лемма 8.3.4 *Если в гиперкомплексной системе элементы 1* a, b *линейно независимы и* $a^2=b^2=-1$, *то* $ab+ba=2c$, *где* $c\in\mathbf{R}$ *и* $-1<c<1$.

Доказательство. Так как элементы $a+b$ и $a-b$ не являются действительными числами (почему?), то они являются, соответственно, корнями квадратных уравнений $x^2+px+q=0$ и $x^2+p_1x+q_1=0$ с действительными коэффициентами. Из этого следует $(a+b)^2+p(a+b)+q=0$ и $(a-b)^2+p_1(a-b)+q_1=0$, то есть $(a+b)^2=-p(a+b)-q$, $(a-b)^2=-p_1(a-b)-q_1$. Кроме того, $(a+b)^2=a^2+b^2+ab+ba=-2+ab+ba$, $(a-b)^2=a^2+b^2-ab-ba=-2-ab-ba$. Имеем равенства
(1) $-2+ab+ba=-p(a+b)-q$ и (2) $-2-ab-ba=-p_1(a-b)-q_1$.
Сложив их почленно, получим $-4=-(p+p_1)a-(p-p_1)b-(q+q_1)$, или $(p+p_1)a+(p-p_1)b+(q+q_1-4)=0$.
Так как a, b, 1 – линейно независимы, то $p+p_1=p-p_1=q+q_1-4=0$, то есть $p=p_1=0$ и равенства (1), (2) принимают вид $-2+ab+ba=-q$, $-2-ab-ba=-q_1$. Таким образом, получаем $ab+ba=2c$, где $2c=2-q=q_1-2\in\mathbf{R}$. Так как $q>0$, $q_1>0$, то $2-q<2$, $q_1-2>-2$. Окончательно получаем $-2<2c<2$, то есть $-1<c<1$.

Теорема 8.3.1 (Фробениус) *Гиперкомплексная система с делением над полем действительных чисел является или полем действительных чисел, или полем комплексных чисел, или телом кватернионов.*

Доказательство. Пусть $\mathbf{K}$ – гиперкомплексная система с делением над полем действительных чисел ранга n. Согласно лемме 8.3.3, в $\mathbf{K}$ существует базис $1, i_2, \ldots, i_n$, такой что $i_2^2=i_3^2=\ldots=i_n^2=-1$. Рассмотрим возможные случаи:

1. Если $n=1$, то все элементы в $\mathbf{K}$ имеют вид $1a$, где $a\in\mathbf{R}$, то есть $\mathbf{K}$ – поле действительных чисел.

2. Если $n=2$, то $\mathbf{K}=\{a+bi_2 \mid i_2^2=-1,\ a\in\mathbf{R}\}$ – поле комплексных чисел.

3. Пусть $n>2$. Если 1, i_2, i_3 – три первых элемента базиса, то, по лемме 8.3.4, $i_2i_3+i_3i_2=2c$, где $-1<c<1$. Пусть $j=\frac{ci_2+i_3}{\sqrt{1-c^2}}$. Тогда $j^2=\frac{c^2i_2^2+ci_3i_2+ci_2i_3+i_3^2}{1-c^2}=-1$ и $i_2j+ji_2=0$. Элементы 1, i_2, j линейно независимы (упражнение 1). Докажем, что элементы 1, i_2, j, i_2j тоже

линейно независимы. Действительно, если бы эти элементы были линейно зависимы, то выполнялось бы равенство $i_2 j = \lambda_0 + \lambda_1 i_2 + \lambda_2 j$. Умножив это равенство слева на i_2, получим $-j = \lambda_0 i_2 - \lambda_1 + \lambda_2 i_2 j = \lambda_0 i_2 - \lambda_1 + \lambda_2(\lambda_0 + \lambda_1 i_2 + \lambda_2 j)$, то есть $(\lambda_2\lambda_0 - \lambda_1) + (\lambda_0 + \lambda_2\lambda_1)i_2 + (\lambda_2^2 + 1)j = 0$. Так как 1, i_2, j – линейно независимы, то все коэффициенты в последнем равенстве – нулевые, в частности, $\lambda_2^2 + 1 = 0$ чего не может быть, так как $\lambda_2 \in \mathbf{R}$.

Из наших рассуждений следует, что в рассматриваемой гиперкомплексной системе имеется, по крайней мере, четыре линейно независимых элемента, то есть гиперкомплексной системы ранга 3 не существует.

Пусть $i_2 j = k$. Тогда $k^2 = (i_2 j)(i_2 j) = i_2(j(i_2 j)) = i_2((j i_2)j) = i_2((-i_2 j)j) = i_2(-i_2(jj)) = i_2 i_2 = -1$. Таким образом, $k^2 = -1$. Если i_2 обозначить через i, то $i^2 = j^2 = k^2 = -1$, $ij = k$, $ji = -k$. Легко проверить, что $jk = i$, $kj = -i$, $ki = j$, $ik = -j$. Окончательно получаем, что гиперкомплексная система ранга 4 есть тело кватернионов.

4. Пусть $n > 4$. Рассмотрим базис $1, i, j, k, i_5, \ldots, i_n$. По лемме 8.3.4, существуют такие c_1, c_2, c_3, что $ii_5 + i_5 i = 2c_1$, $ji_5 + i_5 j = 2c_2$, $ki_5 + i_5 k = 2c_3$. Тогда $i_5 k = i_5(ij) = (i_5 i)j = (2c_1 - ii_5)j = 2c_1 j - i(i_5 j) = 2c_1 j - i(2c_2 - j i_5) = 2c_1 j - 2c_2 i + (ij)i_5 = 2c_1 j - 2c_2 i + k i_5 = 2c_1 j - 2c_2 i + (2c_3 - i_5 k)$. Таким образом, $i_5 k = 2c_1 j - 2c_2 i + 2c_3 - i_5 k$, то есть $i_5 k = c_1 j - c_2 i + c_3$. Умножим обе части последнего равенства справа на k: $i_5 k^2 = c_1(jk) - c_2(ik) + c_3 k$ и, учитывая, что $k^2 = -1$, $ik = -j$, $jk = i$, получим $i_5 = -c_1 i - c_2 j - c_3 k$, а это означает, что система 1, i, j, k, i_5 – линейно зависима, что противоречит условию. Следовательно, гиперкомплексные системы ранга большего 4 не существуют.
Теорема доказана.

Заканчивая главу, отметим, что критериев для того, чтобы считать систему числовой мы не устанавливаем. Если бы среди таких критериев была коммутативность умножения, то построение числовых систем закончилось бы на системе комплексных чисел. Возможно, что это разумно, так как в настоящее время сам термин "гиперкомплексные числа" не часто используется. Однако, нам представляется важным и интересным "мировоззренческий" аспект проведенных рассуждений, а также полу-

ченный результат: нельзя бесконечно расширять классические числовые системы, сохраняя все их свойства и получая новые возможности.

Литература

1. Блох А.Ш. Числовые системы.— Минск, 1982, 160 с.

2. Куликов Л.Я. Алгебра и теория чисел.— М., 1979, 560 с.

3. Ляпин Е.С., Евсеев А.Е. Алгебра и теория чисел.— М., 1974, 832 с.

4. Мальцев А.И. Алгебраические системы.— М., 1970, 392 с.

5. Мендельсон Э. Введение в математическую логику.—
М., 1984, 320 с.

6. Нечаев В.И. Числовые системы.— М., 1975, 200 с.

7. Феферман С. Числовые системы.— М., 1971, 440 с.

Оглавление