В·И·НЕЧАЕВ

ЧИСЛОВЫЕ СИСТЕМЫ

В. И. НЕЧАЕВ

ЧИСЛОВЫЕ СИСТЕМЫ

Допущено Министерством просвещения СССР в качестве учебного пособия для студентов физико-математических факультетов педагогических институтов.

МОСКВА «ПРОСВЕЩЕНИЕ» 1975

517
Н59

Нечаев В. И.

Н59 Числовые системы. Пособие для студентов пед. ин-тов. М., «Просвещение», 1975

199 с. с ил.

Н $\frac{60602 - 619}{103(03) - 75}$ **30—75** **517**

ПРЕДИСЛОВИЕ

Книга написана в соответствии с программой курса «Числовые системы» для математических и физико-математических факультетов педагогических институтов. Важный вопрос школьного курса математики — построение основных числовых систем рассматривается в ней с позиций современной науки.

В этой книге глубокие математические идеи, с которыми студенты знакомятся в курсах математического анализа, алгебры и теории чисел, применяются для последовательного построения основных числовых систем — натуральных, целых, рациональных, действительных, комплексных, а также p-адических чисел и кватернионов.

Книга построена с учетом выделения части материала для самостоятельного изучения студентами и для проработки на семинарских занятиях. Этому способствуют вопросы, сопутствующие каждому параграфу. Некоторые из них затрагивают дополнительный материал, который может служить основой курсовых работ.

Автор признателен всем лицам и особенно Л. Л. Степановой, высказавшим свои замечания по рукописи этой книги.

§ 1. ВВЕДЕНИЕ

1.1. Понятие числа является исходным для многих математических теорий, а задача построения основных числовых систем — одной из важнейших задач школьного курса математики.

В этой книге изучаются основные числовые системы — *натуральные, целые, рациональные, действительные* и *комплексные* числа, а также системы, естественным образом связанные с ними,— *кватернионы* и *p-адические числа*.

Мы ставим цель — выделить те простейшие свойства чисел, из которых можно строго вывести все то, что нам известно о числах.

Почему в математике принято заботиться о строгости рассуждений?

Для любой науки главным является вопрос о соответствии ее с действительностью, вопрос об истинности ее суждений. Но способ установления истинности суждений специфичен для каждой научной дисциплины. В математике эта специфика реализуется в требовании строгости доказательств. Вот почему в математике проблема строгости математических рассуждений и вопросы обоснования всегда занимали и занимают важное место. Однако отчетливую формулировку задача обоснования математики и отдельных ее частей получила только в XIX в. Тогда же были сделаны серьезные попытки ее решения.

Возможно ли окончательное решение проблемы строгости математических рассуждений?

При строгом построении математической теории приходится опираться на другие теории и во всяком случае пользоваться теми или иными способами рассуждений, а также средствами передачи этих рассуждений.

Такие теории и способы рассуждений, а также средства передачи обычно явно или неявно предполагаются более надежными, чем та теория, которая строится. Надежность такой основы, очевидно, относительна, так как сразу возникает проблема обоснования используемых средств и т. д.

Таким образом, обоснование математической теории возможно только относительно тех теорий и средств, которые избираются в качестве «надежной» основы этого обоснования.

Надо заметить, что какой бы ни была «надежной» основа математической теории, наступает момент, когда «надежность» этой основы перестает удовлетворять математиков.

1.2. Каковы те вспомогательные средства, которые будут служить основой для построения числовых систем?

Это прежде всего **язык.** Он нам необходим, чтобы формулировать и обосновывать суждения, определять понятия. Мы не собираемся указывать полный состав языка и рассуждать на тему, возможно ли это вообще. Назовем лишь несколько терминов, о которых условимся, что смысл их не нуждается в каких-либо пояснениях:

«один», «два», «три», «первый», «второй», «левый», «правый», «символ», «обозначает», «существует», «все», «некоторые», «множество», «элемент множества», «высказывание».

Мы не рассматриваем возможность сведения некоторых из них к другим.

Далее **логика.** Это обычная классическая логика, та логика, на которой строится традиционный курс алгебры, анализа или теории чисел. От более точной характеристики нашей логики мы отказываемся.

Мы будем употреблять логические символы $\wedge$, $\vee$, $\neg$, $\Rightarrow$, $\Leftrightarrow$, $\in$, $\forall$, $\exists$, $\exists!$ в их обычном смысле, что поясняется следующей сводкой обозначений:

1) $\wedge$ — «конъюнкция»;
2) $\vee$ — «дизъюнкция»;
3) $\neg$ — «отрицание»;
4) $\Rightarrow$ — «следует»;
5) $\Leftrightarrow$ — «тогда и только тогда» или «если и только если»;
6) $a \in A$ — «a — элемент множества A»;
7) $\forall\, (a \in A)$ — «для всякого элемента a множества A...»;
8) $\forall\, (a, b \in A)$ — «каковы бы ни были элементы a и b множества A...»;
9) $\exists\, (a, b \in A)$ — «существуют такие элементы a и b множества A; что...»;
10) $\exists!\ (a \in A)$ — «существует и только один элемент a множества A такой, что...».

Мы полагаем, что не будем испытывать затруднений в выборе и использовании символов для обозначения рассматриваемых объектов. Мы считаем понятным различие между символом и его смыслом без каких-либо дополнительных пояснений. К примеру, в согласии с обычной практикой, вместо того чтобы сказать, что знаком n обозначается некоторое натуральное число, мы говорим «n — натуральное число».

Идеальной была бы возможность иметь для каждого объекта теории свой символ. Эту возможность реализовать трудно, хотя бы из соображений краткости. Понятно, например, что множество из элемента a и сам этот элемент—разные объекты. Тем не менее в тех случаях, когда нам кажется, что недоразумения произойти не может, тот и другой объекты мы обозначаем одной буквой a. Впрочем,

если один и тот же знак встречается в различных ситуациях мы вправе этот знак наделять особым смыслом в каждой ситуации. Так, например, смысл знака $+$ в выражениях $2 + 3$ и $+3$ не один и тот же. Если $\langle 2, 3, 1\rangle$ и $\langle 1, 0, 2\rangle$ трехмерные векторы, то в записи $\langle 2, 3, 1\rangle + \langle 1, 0, 2\rangle = \langle 2 + 1, 3 + 0, 1 + 2\rangle$ смысл знака $+$ в левой части равенства отличается от смысла этого знака в правой.

Мы пользуемся обычной интуитивной теорией равенства, основанной на представлении, что знаком $=$ можно соединять лишь символы, обозначающие один и тот же объект.

При введении нового символа для обозначения какого-либо объекта мы будем употреблять знак $\rightleftharpoons$ («равно по определению»).

Чтобы избежать двусмысленности в записи выражений, будем употреблять скобки и считать известными соглашения об использовании скобок.

Отметим далее двоякую роль языка и логики в исследовании математической теории. Язык и логика необходимы не только для того, чтобы формулировать и выводить **суждения теории,** но и для того, чтобы высказывать и обосновывать **суждения о самой теории.** При более строгом подходе следовало бы отличать язык и логику, нужные для **описания высказываний теории,** от языка и логики, употребляемых для **описания высказываний об этой теории.** Такое различие мы не намерены проводить при изложении всех тем. Однако будут даны отдельные фрагменты математических теорий, где это отличие учитывается.

1.3. Мы будем предполагать известными элементы интуитивной теории множеств. В частности, мы будем пользоваться понятиями: *пустое множество, подмножество, собственное подмножество, объединение множеств, пересечение множеств, разность множеств.*

Мы будем употреблять синонимы:

1) «множество», «совокупность», «класс»;

2) «подмножество», «часть множества»;

3) «собственное подмножество», «правильная часть множества».

Мы будем пользоваться обозначениями:

1) $\varnothing$ — «пустое множество»;

2) $A \subset B$ — «A подмножество B»;

3) $A \cup B$ — «объединение множеств A и B»;

4) $\bigcup\limits_{\alpha \in M} A_\alpha$ — «объединение всех множеств A_α таких, что $\alpha \in M$»;

5) $A \cap B$ — «пересечение множеств A и B»;

6) $\bigcap\limits_{\alpha \in M} A_\alpha$ — «пересечение всех множеств A_α таких, что $\alpha \in M$»;

7) $A \setminus B$ — «разность множеств A и B»;

8) $\{a\}$ — «множество, состоящее из одного элемента a»;

9) $\{a, b, c\}$ — «множество, состоящее из элементов a, b, c»;

10) $\{a \mid \ldots\}$ — «множество, содержащее те и только те элементы a, которые обладают свойством...».

Мы предполагаем известными следующие утверждения:

Если A, B, C — любые множества, то:

1.3.1. $\varnothing \subset A$;

1.3.2. $A \subset A$;

1.3.3. $A \subset B \wedge B \subset A \Leftrightarrow A = B$;

1.3.4. $A \subset B \wedge B \subset C \Rightarrow A \subset C$;

1.3.5. $A \cup B = B \cup A$;

1.3.6. $(A \cup B) \cup C = A \cup (B \cup C)$;

1.3.7. $A \subset B \Rightarrow A \cup B = B$;

1.3.8. $A \cap B = B \cap A$;

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

1.3.10. $A \subset B \Rightarrow A \cap B = A$;

1.3.11. $A \setminus B = \varnothing \Leftrightarrow A \subset B$;

1.3.12. $A \setminus B = A \Leftrightarrow A \cap B = \varnothing$;

1.3.13. $A \subset B \Rightarrow (C \setminus B) \subset (C \setminus A)$;

1.3.14. $A \subset B \Rightarrow (A \cup C) \subset (B \cup C)$;

1.3.15. $A \cap C = \varnothing \Rightarrow A \cup (B \setminus C) = (A \cup B) \setminus C$;

1.3.16. $C \subset A \Rightarrow A \setminus (B \setminus C) = (A \setminus B) \cup C$;

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

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

Если A и B — любые множества и для каждого μ из $A \cup B$ символом C_μ обозначается некоторое множество, то:

1.3.19. $\bigcup\limits_{\mu \in (A \cup B)} C_\mu = (\bigcup\limits_{\mu \in A} C_\mu) \cup (\bigcup\limits_{\mu \in B} C_\mu)$;

1.3.20. $\bigcap\limits_{\mu \in (A \cup B)} C_\mu = (\bigcap\limits_{\mu \in A} C_\mu) \cap (\bigcap\limits_{\mu \in B} C_\mu)$.

Мы будем считать допустимыми такие способы образования множеств:

1.3.21. Из множества объектов можно выделить часть посредством точно сформулированного признака.

1.3.22. Если имеется совокупность множеств, то можно получить новое множество, являющееся объединением множеств этой совокупности.

1.3.23. Для каждого множества можно образовать множество всех его подмножеств.

1.3.24. Для любой пары множеств можно образовать новое множество, являющееся их произведением (определение 2.1.2).

1.4. Другие математические теории (алгебра, анализ, теория чисел, геометрия, ...) не используются нами при построении числовых систем. Ряд фактов из этих теорий иногда привлекаются нами только в качестве примеров для иллюстрации некоторых высказываний.

Исключение составляют отдельные свойства групп, колец и полей, которые дальше все будут точно указаны, а также простейшие

теоремы линейной алгебры, доказательства которых воспроизвести нетрудно.

Впрочем, после завершения построения какой-либо числовой системы мы вправе пользоваться теми фрагментами любых математических теорий, которые опираются на соответствующую систему.

Основной текст почти каждого пункта сопровождают упражнения, примеры и вопросы. Они выполняют двоякую роль. Прежде всего они иллюстрируют, поясняют общие положения соответствующего раздела. В связи с этим в них может использоваться материал, относящийся к другим разделам. С другой стороны, в них иногда содержатся высказывания, на которые опираются высказывания, принадлежащие другим последующим разделам. В последнем случае эти утверждения являются, по существу, теоремами другого раздела, и поэтому там могут быть использованы. В том, что тут нет какого-либо порочного круга, легко убедиться в каждом конкретном случае отдельно.

В заключение следует отметить, что конструкции, используемые нами при исследовании числовых систем, применяются в различных отделах математики, например в алгебре, теории чисел и анализе.

В изложении мы исходим из того, что нет необходимости давать подробное доказательство каждой сформулированной теоремы. Мы опускаем детали рассуждений всякий раз, когда читатель подготовлен к этому предшествующим материалом.

Для решения наиболее трудных вопросов в конце книги даны указания или достаточно подробные разъяснения. Во многих случаях решение одного вопроса указывает путь для решения следующего.

§ 2. СИСТЕМЫ С ОТНОШЕНИЯМИ И АЛГЕБРАИЧЕСКИМИ ОПЕРАЦИЯМИ

Система натуральных чисел будет рассматриваться в § 4. Поэтому понятием произвольного натурального числа без каких-либо ограничений можно пользоваться только в разделах, следующих за § 4. В настоящем параграфе мы, однако, вводим понятие n-членного отношения и n-арной алгебраической операции. Это не противоречит сказанному выше, так как в § 4 мы не рассматриваем отношения, отличные от унарных, бинарных и тернарных.

В настоящем параграфе вводятся термины *конечная группа, конечная полугруппа, конечное кольцо;* следует в связи с этим заметить, что эти термины мы собираемся употреблять только тогда, когда понятие *конечного* множества будет определено.

2.1. Прямое произведение

Определение 2.1.1. Пусть a и b — какие-нибудь предметы, множество $\{\{a, b\}, b\}$ называют *парой элементов* a и b и обозначают символом $\langle a, b\rangle$.

Таким образом,

$$\langle a, b\rangle \rightleftharpoons \{\{a, b\}, b\}.$$

Элемент a называют *первым* (левым) *компонентом пары* $\langle a, b\rangle$, элемент b — *вторым* (правым).

Легко видеть, что

$$\langle a, b\rangle = \langle a', b'\rangle \Longleftrightarrow a = a' \wedge b = b'.$$

Иногда множество $\{a, b\}$ называют *неупорядоченной парой элементов* a и b, а пару $\langle a, b\rangle$ — *упорядоченной парой элементов* a и b.

Пример 2.1.1. $\{1, 2\} = \{2, 1\}$, но $\langle 1, 2\rangle \neq \langle 2, 1\rangle$.

Пару $\langle\langle a, b\rangle, c\rangle$ называют *тройкой* или *кортежем из элементов* a, b, c и обозначают символом $\langle a, b, c\rangle$. Так можно продолжать и далее. Саму пару $\langle a, b\rangle$ называют также *кортежем из элементов* a, b, а элемент a называют *кортежем из одного элемента* a.

Определение 2.1.2. Пусть A и B — какие-нибудь не обязательно различные множества. *Произведением множеств* A и B называют множество всех пар $\langle a, b\rangle$, где $a \in A$ и $b \in B$, и обозначают символом $A \times B$.

Таким образом,

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

При этом $A \times B = \varnothing \Leftrightarrow A = \varnothing \vee B = \varnothing$.

Наряду с термином «произведение множеств» в литературе приняты термины «прямое произведение множеств» и «декартово произведение множеств».

Упражнения: 2.1.1. Найти прямое произведение $\{1, 2\} \times \{a, b, c\}$.

2.1.2. Найти прямое произведение $\{1, 2, 3\} \times \{1, 2, 3\}$.

Определение 2.1.3. Пусть A, B, C, D — любые множества. Полагаем:

$$A \times B \times C \rightleftharpoons (A \times B) \times C;$$

$$A \times B \times C \times D \rightleftharpoons (A \times B \times C) \times D.$$

Определение 2.1.4. Пусть A — любое множество. Полагаем $A^0 \rightleftharpoons \varnothing$, $A^1 \rightleftharpoons A$, $A^2 \rightleftharpoons A \times A$, $A^3 \rightleftharpoons A \times A \times A$. Множества A^0, A^1, A^2, A^3 называют соответственно *нулевой, первой, второй* и *третьей степенью множества* A.

Вопросы: 2.1.1. Доказать, что $A \times B = B \times A$ в том и только в том случае, если $A = B$ или если $A \times B = B \times A = \varnothing$.

2.1.2. Доказать, что $(A \times B) \times C = A \times (B \times C)$ в том и только том случае, если хотя бы одно из множеств A, B, C пусто.

2.1.3. Доказать, что для любых множеств A, B, C, D:

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

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

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

2.1.4. Какие из равенств вопроса 2.1.3. остаются верными после замены знака $\cap$ на $\cup$?

2.2. *n*-членные отношения и *n*-арные алгебраические операции

Определение 2.2.1. Пусть $n \geqslant 1$ (значений n, отличных от 1, 2 или 3, нам не потребуется); $A_1, \ldots, A_n$ — какие-либо множества. Всякое подмножество ω прямого произведения $A_1 \times \ldots \times A_n$ (т. е. A_1, если $n = 1$, $A_1 \times A_2$, если $n = 2$, и $A_1 \times A_2 \times A_3$, если $n = 3$) называют *n-членным отношением,* заданным во множествах $A_1, \ldots, A_n$, а число n — *рангом отношения* ω. В частности, если $A_1 = \ldots = A_n = A$, то отношение ω называют *отношением, заданным во множестве* A.

Отношения ранга 1, 2, 3 называют соответственно *унарным, бинарным* и *тернарным*. Вместо термина «бинарное отношение» часто употребляют термин «отношение».

Пусть ω — отношение, заданное во множествах $A_1, \ldots, A_{n+1}$ ($n = 0$, 1 или 2). Тогда, каковы бы ни были элементы $a_1 \in A_1, \ldots, a_n \in A_n$, символом

$$\omega a_1, \ldots, a_n, \tag{2.2.1}$$

в частности символом

$$\omega \tag{2.2.2}$$

при $n = 0$, обозначают множество, состоящее из тех и только тех элементов a_{n+1} множества A_{n+1}, для которых кортеж $\langle a_1, \ldots, a_{n+1}\rangle \in \omega$. Очевидно, в зависимости от отношения ω и элементов $a_1, \ldots, a_n$ символ (2.2.1) может обозначать пустое множество или множество, состоящее из одного и более элементов. В частности, если $A_1 = \ldots = A_{n+1} = A$ и, каковы бы ни были элементы $a_1, \ldots, a_n \in A$, множество (2.2.1) (соответственно (2.2.2) при $n = 0$) не пусто и состоит из одного элемента, то $(n+1)$-членное отношение ω называют также *n-арной алгебраической операцией,* заданной на множестве A, а число n — *рангом операции* ω.

В случае, если при тех же предположениях о множествах A_i и элементах a_i множество (2.2.1) состоит не более чем из одного элемента, $(n + 1)$-членное отношение ω называют также *n-арной частичной алгебраической операцией,* заданной во множестве A.

Алгебраическую операцию ранга 0, 1 и 2 называют соответственно *нульарной, унарной* и *бинарной*. Вместо термина «бинарная алгебраическая операция» употребляют также термины «алгебраическая операция» и «закон композиции». Унарную алгебраическую операцию называют также *оператором*.

Из сказанного выше следует, что любое подмножество A можно рассматривать как унарное отношение, заданное в A, а подмножество A, состоящее из одного элемента, и как нульарную алгебраическую операцию на A.

В случае, если ω — бинарное отношение, заданное в A, запись

$$a\omega b$$

означает то же, что

$$\langle a, b\rangle \in \omega.$$

Для обозначения бинарного отношения употребляют символы:

$$=,\ \sim,\ \cong,\ >,\ \geqslant,\ <,\ \leqslant \text{ и др.}$$

В случае, если ω — тернарное отношение, заданное в A, запись

$$a\omega b \tag{2.2.3}$$

означает то же, что

$$\omega ab.$$

Другими словами, символ (2.2.3) обозначает множество всех таких элементов c из A, для которых тройка $\langle a, b, c\rangle$ входит в ω.

Чтобы задать тернарное отношение ω на множестве A, можно указать все тройки элементов, принадлежащие ω, а можно поступать иначе: для каждой пары $\langle a, b\rangle$ элементов множества A указывать множество ωab, т. е. множество таких элементов c, что

$$\langle a, b, c\rangle \in \omega.$$

Имея в виду сказанное выше, мы при задании тернарного отношения ω в каком-либо множестве A будем говорить: «Сопоставим с каждой парой $\langle a, b\rangle$ элементов множества A элемент x такой, что...»

Из этой фразы вовсе не следует ни что такой x (т. е. с условием...) найдется, ни что, если найдется, то только один. Поэтому, если нашей целью является задание алгебраической операции ω, мы должны еще убедиться в том, что, во-первых, хотя бы один x с условием... существует и, во-вторых, что только один.

Примеры 2.2.1. $\omega \rightleftharpoons \{\langle n, n+1\rangle \mid n \in N\}$, т. е. ω — множество пар $\langle n, n+1\rangle$ натуральных чисел с условием, что n — любое натуральное число. Легко видеть, что $\omega \subset N^2$. Поэтому ω — бинарное отношение, заданное во множестве N. Заметим, что

$$\forall (a, b \in N)\, \langle a, b\rangle \in \omega \Leftrightarrow b = a + 1,$$

другими словами, каковы бы ни были натуральные числа a и b, пара $\langle a, b\rangle$ принадлежит множеству ω (находится в отношении ω) тогда и только тогда, если $b = a + 1$. Итак, отношение «непосредственно следует за» — бинарное отношение в N. А так как для каждого натурального числа существует и только одно натуральное число b такое, что $b = a + 1$, то это отношение является вместе с тем и унарной алгебраической операцией (оператором), определенной на множестве N.

2.2.2. $\omega \rightleftharpoons \{\langle n \cdot m, n\rangle \mid n, m \in Z\}$, другими словами, пара целых чисел $\langle a, n\rangle$ принадлежит множеству ω тогда и только тогда, если найдется целое число m такое, что $a = n \cdot m$. Множество ω определяет бинарное отношение в Z — отношение делимости. Если $\langle a, n\rangle \in \omega$, то говорят, что число a делится на n и употребляют обозначение $a \vdots n$. Отношение делимости не является унарной алгебраической операцией.

2.2.3. ω — множество всех простых чисел. Поэтому

$$\forall (a \in N) \quad a \in \omega \Leftrightarrow a \text{ — простое число.}$$

Следовательно, свойство «быть простым» может рассматриваться как унарное отношение в N.

2.2.4. Вычитание — во множестве натуральных чисел — тернарное отношение. Множество $a - b$ состоит из одного элемента или пусто в зависимости от того, a больше b или нет. Поэтому вычитание является вместе с тем бинарной частичной алгебраической операцией, заданной во множестве натуральных чисел.

Определение 2.2.2. Пусть $A_1, \ldots, A_n$ — какие-либо множества и $A_1', \ldots, A_n'$ — их подмножества, т. е. $A_1' \subset A_1, \ldots, A_n' \subset A_n$. Пусть ω —

n-членное отношение, заданное во множествах $A_1, \ldots, A_n$. Тогда $\omega' \rightleftharpoons (A_1' \times \ldots \times A_n') \cap \omega$ есть подмножество прямого произведения $A_1' \times \ldots \times A_n'$ и, таким образом, является отношением, заданным во множествах $A_1', \ldots, A_n'$. Говорят, что *отношение* ω' *индуцировано отношением* ω во множествах $A_1', \ldots, A_n'$ или во множестве A', если $A_1 = \cdots = A_n = A$, $A_1' = \cdots = A_n' = A'$, а отношение ω называют *продолжением отношения* ω' во множествах $A_1, \ldots, A_n$ или во множестве A, если $A_1 = \cdots = A_n = A$ и $A_1' = \cdots = A_n' = A'$.

Примеры 2.2.5. Вычитание —, заданное во множестве целых чисел, продолжает вычитание —, заданное во множестве натуральных чисел. Этот пример также показывает, что, хотя продолжение некоторого отношения является алгебраической операцией, само отношение может и не быть таковой.

2.2.6. Отношение порядка $>$ (больше), заданное во множестве целых чисел, является продолжением порядка, заданного во множестве натуральных чисел.

2.2.7. Пусть T — множество точек плоскости, P — множество ее прямых. Отношение принадлежности точки прямой является бинарным отношением, заданным во множествах T и P.

2.2.8. Пусть T — множество точек плоскости. Зададим тернарное отношение ω в T следующим образом. Тройку точек $\langle A, B, C\rangle$ плоскости отнесем к ω в случае, если C — середина отрезка AB. Легко видеть, что ω — алгебраическая операция, заданная на множестве T.

Определение 2.2.3. Бинарное отношение ω, заданное во множестве A, называют:

а) *связным,* если $\forall (a, b \in A)\, a \neq b \Rightarrow a\omega b \vee b\omega a$;

б) *рефлексивным,* если $\forall (a \in A)\, a\omega a$;

в) *антирефлексивным,* если $\forall (a \in A) \neg a\omega a$;

г) *симметричным,* если $\forall (a, b \in A)\, a\omega b \Rightarrow b\omega a$;

д) *антисимметричным,* если $\forall (a, b \in A)\, a\omega b \wedge b\omega a \Rightarrow a = b$;

е) *асимметричным,* если $\forall (a, b \in A)\, a\omega b \Rightarrow \neg b\omega a$;

ж) *транзитивным,* если $\forall (a, b, c \in A)\, a\omega b \wedge b\omega c \Rightarrow a\omega c$;

з) в случае, если на множестве A задан сверх того закон композиции $\top$, бинарное отношение ω называют *монотонным* относительно закона $\top$, если

$$\forall (a, b, c \in A)\, a\omega b \Rightarrow (a \top c)\, \omega\, (b \top c) \wedge (c \top a)\, \omega\, (c \top b).$$

Определение 2.2.4. *Закон композиции* $\top$ элементов множества A (т. е. бинарную операцию, заданную на A) называют:

а) *коммутативным,* если

$$\forall (a, b \in A)\, a \top b = b \top a;$$

б) *ассоциативным*, если

$$\forall (a, b, c \in A)\ (a \top b) \top c = a \top (b \top c).$$

Пусть $\top$ — закон композиции элементов множества A; элемент θ из A называют *нейтральным элементом* относительно закона $\top$, если

$$\forall (a \in A)\ a \top \theta = \theta \top a = a.$$

Элемент a' из A называют *симметричным* элементу a из A относительно композиции $\top$ с нейтральным элементом θ, если

$$a \top a' = a' \top a = \theta.$$

Если на множестве A заданы два закона композиции $\top$ и $\perp$, то говорят, что закон композиции $\top$ *дистрибутивен* относительно закона $\perp$, если

$$\forall (a, b, c \in A)\ (a \perp b) \top c = (a \top c) \perp (b \top c) \wedge$$
$$\wedge\, c \top (a \perp b) = (c \top a) \perp (c \top b).$$

Законы композиции часто обозначают знаками $+$ или $\cdot$; в первом случае композицию элементов a и b обозначают $a + b$, во втором $a \cdot b$, или ab, а законы композиции называют соответственно *сложением* и *умножением;* при этом говорят, что для закона композиции принято соответственно *аддитивное* и *мультипликативное* обозначение. При аддитивном и мультипликативном обозначении для записи композиции трех и более элементов необходимы скобки.

Вопросы: 2.2.1. Доказать, что всякое антирефлексивное и транзитивное отношение асимметрично.

2.2.2. Доказать, что бинарное отношение асимметрично тогда и только тогда, если оно антирефлексивно и антисимметрично.

2.2.3. Показать, что умножение на множестве матриц второго порядка с целыми элементами — некоммутативно.

2.2.4. Показать, что закон композиции примера 2.2.5 неассоциативен.

2.2.5. Является ли деление (см. определение 2.2.5) частичной алгебраической операцией во множестве натуральных, целых и рациональных чисел?

2.2.6. Сопоставим с каждой парой $\langle a, b \rangle$ положительных чисел степень a^b. Будет ли введенное нами бинарное отношение алгебраической операцией на множестве положительных чисел? Обладает ли эта операция свойствами коммутативности и ассоциативности?

Определение 2.2.5. Пусть на множестве A определена бинарная операция умножение; $a, b \in A$. Если существует и только один элемент x такой, что

$$ax = xa = b,$$

то элемент x называют *частным* элементов b и a и этот элемент обозначают символом $\frac{b}{a}$.

Таблица терминов и обозначений, употребляемых в разных записях закона композиции (бинарной операции)

Бинарная операция на множестве A ω	Закон композиции элементов множества A $\top$	Сложение элементов множества A $+$	Умножение элементов множества A $\cdot$
Образ пары $\langle a, b\rangle$ ωab	Композиция элементов a и b $a \top b$	Сумма элементов a и b $a + b$	Произведение элементов a и b $a \cdot b$ или ab
Коммутативность операции $\omega ab = \omega ba$	$a \top b = b \top a$	$a + b = b + a$	$ab = ba$
Ассоциативность $\omega\omega abc = \omega a \omega bc$	$(a \top b) \top c =$ $= a \top (b \top c)$	$(a + b) + c =$ $= a + (b + c)$	$(ab)\, c = a\,(bc)$
Нейтральный элемент операции $\omega a \theta = \omega \theta a = a$	θ $a \top \theta = \theta \top a = a$	0 (нуль) $a + 0 =$ $= 0 + a = a$	1 (единица) $a \cdot 1 =$ $= 1 \cdot a = a$
Симметричный элементу a элемент a' $\omega a a' = \omega a' a = \theta$	a' $a \top a' = a' \top a = \theta$	$-a$ (противоположный элементу a элемент) $a + (-a) =$ $= (-a) + a = 0$	a^{-1} (обратный элементу a элемент) $a \cdot a^{-1} =$ $= a^{-1} \cdot a = 1$
Монотонность бинарного отношения $\sim$ относительно бинарной операции ω $a \sim b \Rightarrow \omega ac \sim \omega bc \wedge$ $\wedge \omega ca \sim \omega cb$	$a \sim b \Rightarrow$ $\Rightarrow (a \top c) \sim (b \top c) \wedge$ $\wedge (c \top a) \sim (c \top b)$	$a \sim b \Rightarrow$ $\Rightarrow a + c \sim$ $\sim b + c \wedge$ $\wedge c + a \sim c + b$	$a \sim b \Rightarrow$ $\Rightarrow ac \sim bc \wedge$ $\wedge ca \sim cb$

Сопоставляя с каждой парой элементов множества A их частное, мы определяем тернарное отношение, называемое *делением*. Вообще говоря, не для каждой пары элементов определено их частное. Частичную операцию «деление» называют операцией, обратной умножению.

В случае аддитивной записи бинарной операции употребляют соответственно термин *разность*, обозначение «$b - a$», а операцию, обратную сложению, называют *вычитанием*.

Если частичная операция деление (вычитание) выполнима для пары элементов $\langle b, a\rangle$, то говорят, что частное $\frac{b}{a}$ (разность $b - a$) имеет смысл.

2.3. Отображения

Определение 2.3.1. Пусть ω — бинарное отношение, заданное во множествах A и B. Тогда множество всех пар $\langle b, a\rangle$ таких, что $\langle a, b\rangle \in \omega$, является отношением, заданным во множествах B и A. Это отношение называют отношением *обратным* к отношению ω и обозначают символом ω^{-1}.

Если ω — бинарное отношение, заданное во множествах A и B, и

$$\langle a, b\rangle \in \omega,$$

то элемент b называют *образом элемента* a во множестве B относительно отношения ω, а элемент a — *прообразом элемента* b. *Множество всех образов элемента* a обозначают символом ωa, а *множество всех прообразов элемента* b — символом $\omega^{-1}b$; если A' — какое угодно подмножество A, то символом $\omega A'$ или $\omega(A')$ обозначают *множество всех образов элементов из* A'.

Определение 2.3.2. Бинарное отношение ω, заданное во множествах A и B, называют *отображением* (также соответствием) A в B, если

$$\forall (a \in A)\, \omega a \neq \varnothing.$$

Если к тому же

$$\forall (b \in B)\, \omega^{-1} b \neq \varnothing,$$

то отображение ω называют *отображением* A *на* B.

Определение 2.3.3. Отображение ω множества A во множество B (соответственно A на B) называют *однозначным отображением* A в B (соответственно A на B), если

$$\forall (a \in A)\, \exists !\, (b \in B)\, b \in \omega a,$$

другими словами, если каждый элемент A имеет и только один образ в B.

Однозначное отображение ω множества A на B называют также *функцией с областью определения* A *и областью значений* B.

Однозначное отображение ω множества A в множество B называют *функцией из* A *в* B. Для обозначения функции ω из A в B употребляют запись:

$$\omega : A \to B.$$

Образ элемента a в однозначном отображении ω множества A в B обозначают также символом $\omega(a)$. Запись $\omega : a \mapsto b$ означает, что b есть образ элемента a в отображении ω. Множество всех однозначных отображений множества A в множество B обозначают символом B^A. Однозначное отображение множества A в A называют *преобразованием множества* A.

Вопрос 2.3.1. Показать, что всякое однозначное отображение множества A во множество B индуцирует однозначное отображение любого подмножества A в B.

Однозначное отображение некоторого подмножества множества A во множество B называют *частичной функцией* из A в B.

Пусть n — натуральное число ($n = 2$ или $n = 3$) и φ — однозначное отображение множества A в множество B. Тогда соответствие

$$\psi\colon \langle a_1, \ldots, a_n\rangle \mapsto \langle \varphi(a_1), \ldots, \varphi(a_n)\rangle$$

определяет однозначное отображение множества A^n в B^n, которое мы будем обозначать символом $\varphi^{(n)}$.

Определение 2.3.4. Пусть ω — какое-либо n-членное отношение, заданное во множестве A, и φ — однозначное отображение A в B. Тогда $\varphi^{(n)}\omega$ является подмножеством B^n и, таким образом, n-членным отношением, заданным в B. Это отношение мы называем *отношением, наведенным отношением* ω *в отображении* φ *множества* A в B.

Пример 2.3.1. Пусть m — натуральное число, Z_m — множество классов вычетов целых чисел по модулю m, $(a)_m$ — *класс чисел, сравнимых с* a *по модулю* m. Рассмотрим однозначное отображение f множества целых чисел Z в Z_m, определяемое условием

$$f\colon a \mapsto (a)_m.$$

Тернарное отношение $+$ в Z_m, определяемое условием

$$(a)_m + (b)_m \Leftrightarrows (a + b)_m,$$

является отношением, наведенным отношением «сумма» во множестве Z в отображении f.

Определение 2.3.5. Однозначное отображение ω множества A во множество B (соответственно множества A на B) называют *взаимно-однозначным отображением* (или взаимно-однозначным *преобразованием*) множества A в B (соответственно A на B), если

$$\forall (a, b \in A)\ a = b \Leftrightarrow \omega(a) = \omega(b).$$

Определение 2.3.6. Если задано взаимно-однозначное отображение множества A на B или оба множества A и B пусты, то говорят, что *множество* A *равномощно множеству* B и употребляют обозначение

$$A \cong B.$$

Обозначение

$$\omega\colon A \cong B$$

употребляют в случае, если ω — взаимно-однозначное отображение множества A на множество B.

Вопросы: 2.3.2. Пусть ω — взаимно-однозначное преобразование множества A; $B \subset A$. Доказать, что:

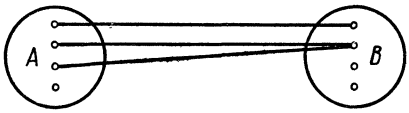
1) $\omega(B) \cap \omega(A \setminus B) = \varnothing$;

2) $(A \setminus \omega(A)) \cap \omega(A \setminus B) = \varnothing$.

2.3.3. Пусть на множестве A задано n-членное отношение ω и пусть φ — взаимно-однозначное отображение A на множество B. Показать, что отношение ω является алгебраической операцией на A тогда и только тогда, если отношение, наведенное отношением ω

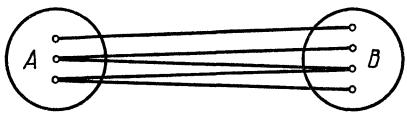
во взаимно-однозначном отображении φ A на B, является алгебраической операцией.

Бинарное отношение ω, заданное в конечных множествах A и B, можно представить графом, вершины которого изображают элементы множеств A и B, а ребра соединяют такие пары вершин, которые соответствуют парам элементов A и B, принадлежащим отношению ω.

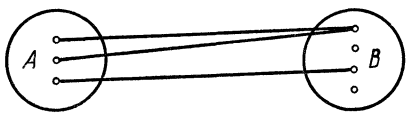


(2.3.1)

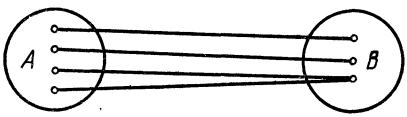
(2.3.2)



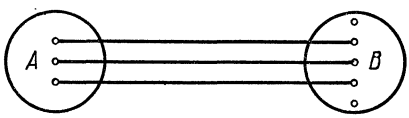
(2.3.3)



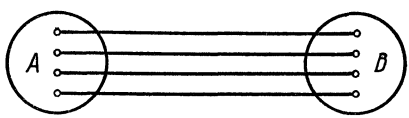
(2.3.4)



(2.3.5)



(2.3.6)



(2.3.7)

Примеры: 2.3.2. Граф (2.3.1) изображает отношение, которое не является отображением. Все остальные графы изображают отображения множества A в B.

2.3.3. Отображения (2.3.2), (2.3.4), (2.3.6) являются отображениями A в B, отображения (2.3.3), (2.3.5), (2.3.7) — отображениями A на B.

2.3.4.* Отображения (2.3.2) и (2.3.3) не являются однозначными отображениями A в B; отображения (2.3.4), (2.3.5), (2.3.6), (2.3.7) — однозначные отображения A в B.

2.3.5. Отображения (2.3.6) и (2.3.7) являются взаимно-однозначными отображениями A в B, а отображение (2.3.7) — взаимно-однозначным отображением A на B.

2.3.6. Отображение $\omega = \{\langle x,\ x^2\rangle \mid x \in N\}$ является взаимно-однозначным отображением множества натуральных чисел N в N, но не на N.

2.3.7. n-арная алгебраическая операция ω, заданная на каком-нибудь множестве A, при $n \geqslant 1$ определяет однозначное отображение A^n в $A_{\downarrow}$:

$$\omega\colon A^n \to A.$$

Вопросы: 2.3.4. Показать, что множество натуральных чисел N и множество N^2 всех пар натуральных чисел равномощны.

2.3.5. Показать, что множество натуральных чисел N и множество N^3 всех троек натуральных чисел равномощны.

2.3.6. Показать, что отношение равномощности на классе всех подмножеств данного множества рефлексивно, симметрично и транзитивно.

2.3.7. Доказать, что если A и B — какие угодно множества; $a \in A$, $b \in B$, то $A \cong B \Leftrightarrow A \setminus \{a\} \cong B \setminus \{b\}$.

2.3.8. Пусть A_1, A_2, B_1, B_2 — множества такие, что:

$$A_1 \cap B_1 = A_2 \cap B_2 = \varnothing;$$

$$A_1 \cong A_2, \quad B_1 \cong B_2.$$

Доказать, что

$$A_1 \cup B_1 \cong A_2 \cup B_2.$$

2.3.9. Пусть A_1, A_2, B_1, B_2 — множества такие, что

$$A_1 \cong A_2, \quad B_1 \cong B_2.$$

Доказать, что

1) $A_1 \times B_1 \cong A_2 \times B_2$;

2) $B_1^{A_1} \cong B_2^{A_2}$.

Для любого множества A символом $|A|$ обозначают новый объект, называемый *мощностью* множества A, и такой, что

$$|A| = |B| \Leftrightarrow A \cong B.$$

Мощности множеств называют также *кардинальными числами*. Пусть $\mathfrak{a} \rightleftharpoons |A|$, $\mathfrak{b} \rightleftharpoons |B|$; тогда:

а) под *суммой* $\mathfrak{a} + \mathfrak{b}$ понимают кардинальное число *объединения* $A \cup B$ при условии, что $A \cap B = \varnothing$;

б) под *произведением* $\mathfrak{a} \cdot \mathfrak{b}$ понимают кардинальное число *прямого произведения* $A \times B$;

в) под *степенью* $\mathfrak{a}^{\mathfrak{b}}$ понимают кардинальное число *степени* A^B.

2.3.10. Пусть $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ — кардинальные числа. Доказать, что:

1) $\mathfrak{a}+\mathfrak{b}=\mathfrak{b}+\mathfrak{a}$;
2) $(\mathfrak{a}+\mathfrak{b})+\mathfrak{c}=\mathfrak{a}+(\mathfrak{b}+\mathfrak{c})$;
3) $\mathfrak{a}\cdot\mathfrak{b}=\mathfrak{b}\cdot\mathfrak{a}$;
4) $(\mathfrak{a}\cdot\mathfrak{b})\cdot\mathfrak{c}=\mathfrak{a}\cdot(\mathfrak{b}\cdot\mathfrak{c})$;
5) $(\mathfrak{a}+\mathfrak{b})\cdot\mathfrak{c}=\mathfrak{a}\cdot\mathfrak{c}+\mathfrak{b}\cdot\mathfrak{c}$;
6) $\mathfrak{a}^{\mathfrak{b}+\mathfrak{c}}=\mathfrak{a}^{\mathfrak{b}}\cdot\mathfrak{a}^{\mathfrak{c}}$;
7) $(\mathfrak{a}\cdot\mathfrak{b})^{\mathfrak{c}}=\mathfrak{a}^{\mathfrak{c}}\cdot\mathfrak{b}^{\mathfrak{c}}$;
8) $(\mathfrak{a}^{\mathfrak{b}})^{\mathfrak{c}}=\mathfrak{a}^{\mathfrak{b}\cdot\mathfrak{c}}$.

2.3.11*. Пусть ω — взаимно-однозначное отображение множества A на подмножество $\omega(A)\subset A$; C — подмножество $A\setminus\omega(A)$; S — подмножество A такое, что

$$S=C\cup\omega(S).$$

Доказать, что

1) $S\cap\omega(A\setminus S)=\varnothing$.

Пусть, далее, ω^* — отображение множества A в A, определяемое условием:

$$\omega^*(x)\rightleftarrows\begin{cases}x, & \text{если } x\in S;\\ \omega(x), & \text{если } x\in A\setminus S.\end{cases}$$

Доказать, что

2) $\omega^*(A)=C\cup\omega(A)$;

3) ω^* — взаимно-однозначное отображение множества A на множество $C\cup\omega(A)$.

2.3.12. Пусть ω — взаимно-однозначное отображение множества A на подмножество $\omega(A)$; $C\subset(A\setminus\omega(A))$. Пусть, далее, $\omega^0(C)\rightleftarrows C$ и для каждого неотрицательного целого n

$$\omega^{n+1}\rightleftarrows\omega(\omega^n(C)).$$

Доказать, что множество $S\rightleftarrows\bigcup\limits_{n=0}^{\infty}\omega^n(C)$ удовлетворяет условиям:

1) $S\subset A$;

2) $S=C\cup\omega(S)$.

2.3.13*. Пусть ω — взаимно-однозначное отображение множества A во множество B и θ — взаимно-однозначное отображение множества B во множество A. Доказать, что существует взаимно-однозначное отображение множества A на множество B.

Пусть $\mathfrak{a}$ и $\mathfrak{b}$ — кардинальные числа множеств A и B соответственно. Если множество A равномощно какому-нибудь подмножеству множества B, то говорят, что кардинальное число $\mathfrak{a}$ не превосходит числа $\mathfrak{b}$, и употребляют обозначение $\mathfrak{a}\leqslant\mathfrak{b}$; если к тому же $\mathfrak{a}\neq\mathfrak{b}$, то говорят, что $\mathfrak{a}$ меньше $\mathfrak{b}$, и употребляют обозначение $\mathfrak{a}<\mathfrak{b}$.

2.3.14. Пусть $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ — кардинальные числа. Доказать, что:

1) $\mathfrak{a} \leqslant \mathfrak{a}$,

2) $\mathfrak{a} \leqslant \mathfrak{b} \wedge \mathfrak{b} \leqslant \mathfrak{a} \Rightarrow \mathfrak{a} = \mathfrak{b}$;

3) $\mathfrak{a} \leqslant \mathfrak{b} \wedge \mathfrak{b} \leqslant \mathfrak{c} \Rightarrow \mathfrak{a} \leqslant \mathfrak{c}$;

4) $\mathfrak{a} \leqslant \mathfrak{b} \Rightarrow \mathfrak{a} + \mathfrak{c} \leqslant \mathfrak{b} + \mathfrak{c}$;

5) $\mathfrak{a} \leqslant \mathfrak{b} \Rightarrow \mathfrak{a} \cdot \mathfrak{c} \leqslant \mathfrak{b} \cdot \mathfrak{c}$;

6) $\mathfrak{a} \leqslant \mathfrak{b} \Rightarrow \mathfrak{a}^{\mathfrak{c}} \leqslant \mathfrak{b}^{\mathfrak{c}}$;

7) $\mathfrak{a} \leqslant \mathfrak{b} \Rightarrow \mathfrak{c}^{\mathfrak{a}} \leqslant \mathfrak{c}^{\mathfrak{b}}$.

2.4. Системы с отношениями и операциями

Определение 2.4.1. Пусть A — непустое и B — какое угодно множество и пусть для каждого $\beta \in B$ в A задано n_β-членное отношение ρ_β. В таком случае упорядоченную пару $\mathbf{A}$, компонентами которой служат A и множество всех отношений ρ_β, называют *системой с отношениями* $\{\rho_\beta \mid \beta \in B\}$ или *алгебраической системой*.

Обозначение: $\mathbf{A} \rightleftharpoons \langle A; \{\rho_\beta \mid \beta \in B\}\rangle$.

Пусть A' — какое угодно подмножество A; символом $\langle A'; \{\rho_\beta \mid \beta \in B\}\rangle$ мы обозначаем систему, состоящую из множества A' и отношений, индуцированных отношениями ρ_β во множестве A'.

Понятие системы с отношениями можно обобщить. В этом случае вместо множества A берется некоторое множество таких множеств, а в качестве отношений берутся отношения, заданные в каких-нибудь совокупностях таких множеств. Точное определение системы с отношениями в этом смысле будет дано позднее. Заметим, однако, что в системы, которые мы будем рассматривать, могут входить или одно множество A, или два A_1 и A_2. В последнем случае отношения могут задаваться или во множестве A_1, или во множестве A_2, или, наконец, во множествах A_1 и A_2.

Пусть $\mathbf{A}$ — какая-нибудь система с отношениями. Обычно в системе $\mathbf{A}$ из ее множеств выделяют одно множество как основное и под *элементом системы* $\mathbf{A}$ понимают элемент этого множества, а за *подмножество системы* $\mathbf{A}$ принимают любое подмножество этого множества.

Определение 2.4.2. Пусть A — непустое множество и B — какое угодно множество, и пусть для каждого $\beta \in B$ в A задана n_β-арная алгебраическая операция ω_β. В таком случае систему с отношениями $\langle A; \{\omega_\beta \mid \beta \in B\}\rangle$ называют *алгеброй* или говорят также, что множество A — *алгебра относительно операций* $\{\omega_\beta \mid \beta \in B\}$.

Множество A и система $\langle A; \{\omega_\beta \mid \beta \in B\}\rangle$, очевидно, не одно и то же. В частности, следует отличать множество натуральных чисел от системы $\mathbf{N} \rightleftharpoons \langle N; +, \cdot, 1\rangle$ натуральных чисел. В первом слу-

чае имеют дело с некоторым множеством символов 1, 2, 3, ...; во втором случае отмечают, что на множестве N рассматриваются два тернарных и одно унарное отношение.

Понятие алгебры можно было бы обобщить примерно так же, как понятие системы с отношениями. Но в этом нет прямой необходимости.

В случае, если отношения алгебраической системы (операции алгебры) обладают определенными свойствами, то такие системы обозначают определенными терминами. В дальнейшем будут рассматриваться алгебры с одной бинарной операцией: полугруппы и группы; алгебры с двумя бинарными операциями: полукольца, кольца, тела и поля, алгебры с двумя бинарными операциями и множеством, иногда бесконечным, унарных: алгебры над полем. Некоторые из перечисленных систем рассматривались в курсе алгебры. Кроме того, будут изучаться системы с одним основным множеством и множеством отношений: упорядоченные множества, полугруппы и полукольца, а также системы, состоящие из двух множеств с операциями и отображениями одного из этих множеств в другое — нормированные поля.

При одновременном рассмотрении нескольких алгебраических систем, если нет опасности для недоразумений, отношения и операции в них мы иногда будем обозначать одними и теми же знаками.

2.5. Полугруппы и группы

Единственную бинарную операцию названных алгебр мы будем записывать мультипликативно. Это обстоятельство, очевидно, несущественно, и перевод определений и высказываний об алгебрах с мультипликативной записи на аддитивную нетруден. Впрочем, определение полугруппы и группы можно сделать и независимым явно от какого бы то ни было способа записи рассматриваемой в них операции. Аналогичное замечание можно сделать и относительно других алгебр.

Определение 2.5.1. Алгебру $\mathbf{A} \rightleftharpoons \langle A;\ \cdot \rangle$ называют *полугруппой,* если операция $\cdot$ на A бинарна и ассоциативна. Другими словами, если:

1) $\forall\, (a, b \in A)\, \exists !\, (c \in A)\, a \cdot b = c$;

2) $\forall\, (a, b, c \in A)\, (a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Полугруппу $\mathbf{A} = \langle A;\ \cdot \rangle$ называют *коммутативной,* если операция $\cdot$ коммутативна, и *конечной,* если множество A конечно. Полугруппу $\langle \mathbf{A}; \cdot \rangle$ называют *полугруппой с сокращением,* если

$$\forall\, (a, x, y \in A)\, (ax = ay \Rightarrow x = y) \wedge (xa = ya \Rightarrow x = y).$$

Таким образом, полугруппа $\langle A;\ + \rangle$ — полугруппа с сокращением, если

$$\forall (a, x, y \in A)\,(a + x = a + y \Rightarrow x = y) \wedge (x + a = y + a \Rightarrow x = y).$$

Пример 2.5.1. Рассмотрим множество $A \rightleftharpoons \{e, a\}$ из двух элементов и определим на A бинарную операцию $\cdot$ следующей таблицей:

$\cdot$	e	a
e	e	a
a	a	a

Легко проверить, что система $\mathbf{A} \rightleftharpoons \langle A;\ \cdot \rangle$ — полугруппа, и притом без сокращения.

Теорема 2.5.1. В любой полугруппе $\mathbf{A} \rightleftharpoons \langle A;\ + \rangle$ с сокращением имеется не более чем один элемент θ такой, что

$$\theta + \theta = \theta.$$

Доказательство. Предположим, что для элементов θ и φ полугруппы $\mathbf{A}$

$$\theta + \theta = \theta \wedge \varphi = \varphi + \varphi.$$

Тогда

$$(\theta + \theta) + \varphi = \theta + (\varphi + \varphi).$$

Отсюда следует, что

$$\theta = \varphi.$$

Определение 2.5.2. Полугруппу $\mathbf{A} \rightleftharpoons \langle A;\ \cdot \rangle$ называют *группой*, если

$$\forall (a, b \in A)\,\exists (x, y \in A)\, ax = b \wedge ya = b.$$

Определения 2.5.3. и 2.5.4. Пусть $\mathbf{A} \rightleftharpoons \langle A;\ \cdot \rangle$ — полугруппа и A' — подмножество A; тогда систему $\mathbf{A}' \rightleftharpoons \langle A';\cdot \rangle$ называют *подполугруппой* (соответственно *подгруппой*) полугруппы $\mathbf{A}$, если система $\mathbf{A}'$— полугруппа (соответственно группа). Другими словами, если подмножество A' множества A образует полугруппу (группу) относительно той же операции, которая рассматривается в A, то систему $\mathbf{A}'$ называют *подполугруппой (подгруппой)* полугруппы $\mathbf{A}$.

Вопросы: 2.5.1. Является ли полугруппой (группой) множество натуральных чисел относительно сложения (умножения)?

2.5.2. Доказать, что множество действительных чисел не является группой относительно возвышения в степень (вопрос 2.2.4).

2.5.3. Доказать, что если $\mathbf{A} \rightleftharpoons \langle A;\ \cdot \rangle$ — группа, то множество A содержит по крайней мере один элемент e (единицу) с условием, что

$$\forall (a \in A)\, a \cdot e = e \cdot a = a,$$

и для каждого элемента a из A хотя бы один элемент a' (обратный к a) с условием, что

$$a \cdot a' = a' \cdot a = e.$$

2.5.4. Доказать, что если $\mathbf{A} \rightleftarrows \langle A;\ \cdot \rangle$ — группа, то $\mathbf{A}$ — полугруппа с сокращением.

2.5.5. Пусть $\mathbf{A} \rightleftarrows \langle A;\ \cdot,\ e \rangle$ — алгебраическая система с бинарной операцией $\cdot$ и нульарной операцией e. Доказать, что система $\langle A;\ \cdot \rangle$ — группа, если: 1) операция $\cdot$ ассоциативна; 2) $\forall\, (a \in A)\ a \cdot e = a$; 3) $\forall\, (a \in A)\ \exists\, (a' \in A)\ a \cdot a' = e$.

2.5.6. Доказать, что если $\mathbf{A} \rightleftarrows \langle A;\ \cdot \rangle$ — группа, то A содержит только один нейтральный элемент (единицу) операции $\cdot$ и для каждого элемента a в A имеется только один симметричный (обратный) к нему элемент a^{-1}.

2.5.7. Пусть $\mathbf{A} \rightleftarrows \langle A;\ \cdot \rangle$ — группа; A' — непустое подмножество A. Доказать, что система $\langle A';\ \cdot \rangle$ тогда и только тогда подгруппа группы $\mathbf{A}$, если в A' для с каждой пары элементов содержится их частное.

2.5.8. Пусть $\mathbf{A} \rightleftarrows \langle A;\ \cdot \rangle$ — группа, M — непустое множество с условием: для каждого μ из M определена $\mathbf{A}_\mu \rightleftarrows \langle A_\mu;\ \cdot \rangle$ — подгруппа группы $\mathbf{A}$. Пусть A_0 — пересечение всех A_μ, т. е. $A_0 \rightleftarrows \bigcap\limits_{\mu \in M} A_\mu$. Доказать, что система $\langle A_0;\ \cdot \rangle$ — подгруппа группы $\mathbf{A}$.
Коротко: пересечение любого множества подгрупп группы $\mathbf{A}$ — снова подгруппа $\mathbf{A}$.

2.5.9. Пусть $\mathbf{A} \rightleftarrows \langle A;\ \cdot \rangle$ — группа. Доказать, что:

1) $\forall\, (a \in A)\ (a^{-1})^{-1} = a$;

2) $\forall\, (a, b \in A)\ (a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

2.5.10. Пусть $\mathbf{A} \rightleftarrows \langle A;\ + \rangle$ — коммутативная полугруппа с сокращением. Доказать, предполагая, что все встречающиеся разности имеют смысл, следующие равенства:

1) $\forall\, (a, b, a', b' \in A)\ a - b = a' - b' \Rightarrow a + b' = a' + b$;

2) $\forall\, (a, b, c \in A)\ (a + c) - (b + c) = a - b \wedge (a + b) - a = b$.

2.5.11. Пусть $\mathbf{A} \rightleftarrows \langle A;\ \cdot \rangle$ — коммутативная группа с единицей 1. Доказать, что:

1) $\forall\, (a \in A)\ \frac{1}{a} = a^{-1} \wedge \frac{a}{1} = a$;

2) $\forall\, (a, b \in A)\ \frac{a}{b} = a \cdot b^{-1}$;

3) $\forall\, (a, b \in A)\ \left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$;

4) $\forall\, (a, b, a', b' \in A)\ \frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}$;

5) $\forall\, (a, b, a', b' \in A)\ \dfrac{\frac{a}{b}}{\frac{a'}{b'}} = \frac{ab'}{ba'}$.

2.5.12. Пусть алгебры

$$\langle A_1;\ +\rangle \ \ldots\ \langle A_n;\ +\rangle$$

— группы; $A \rightleftharpoons A_1 \times \ldots \times A_n$. Определим на множестве A операцию $+$ условием

$$\langle a_1, \ldots, a_n\rangle + \langle b_1, \ldots, b_n\rangle \rightleftharpoons \langle a_1 + b_1, \ldots, a_n + b_n\rangle.$$

Доказать, что система $\langle A;\ +\rangle$ — группа.

Упражнения: 2.5.1. Записать в аддитивном обозначении утверждения, сформулированные в вопросах 2.5.9 и 2.5.11.

2.5.2. Сформулировать в аддитивных обозначениях вопросы 2.5.6 и 2.5.7.

Пусть $\mathbf{A} \rightleftharpoons \langle A;\ \cdot\rangle$ — группа и e — единица группы $\mathbf{A}$. В таком случае употребляют также запись $\mathbf{A} \rightleftharpoons \langle A;\ \cdot, e\rangle$; другими словами, алгебру $\mathbf{A}$ рассматривают и как систему с одной бинарной операцией $\cdot$ и одной нульарной операцией e (вопрос 2.5.5).

2.6. Полукольца, кольца, тела и поля

Определение 2.6.1. Алгебру $\mathbf{A} \rightleftharpoons \langle A;\ +,\ \cdot\rangle$ называют *полукольцом,* если $\langle A;\ +\rangle$ — коммутативная полугруппа с сокращением, $\langle A;\cdot\rangle$ —полугруппа и операции $+$ и $\cdot$ связаны законом дистрибутивности.

Другими словами, система $\mathbf{A} \rightleftharpoons \langle A;\ +,\ \cdot\rangle$ — *полукольцо,* если отношения $+$ и $\cdot$ — бинарные операции на $\mathbf{A}$, удовлетворяющие следующим условиям:

1) $\forall\,(a, b, c \in A)\quad (a + b) + c = a + (b + c)$;

2) $\forall\,(a, b \in A)\quad a + b = b + a$;

3) $\forall\,(a, b, x \in A)\quad (a + x = b + x \Rightarrow a = b) \wedge (x + a = x + b \Rightarrow$
$\Rightarrow a = b)$;

4) $\forall\,(a, b, c \in A)\quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$;

5) $\forall\,(a, b, c \in A)\quad ((a + b) \cdot c = ac + bc) \wedge (c \cdot (a + b) = ca + cb)$.

Полукольцо $\langle A;\ +,\ \cdot\rangle$ называют *коммутативным,* если операция $\cdot$ коммутативна, — *конечным,* если множество A конечно.

Элемент 0 полукольца $\mathbf{A} \rightleftharpoons \langle A;\ +,\ \cdot\rangle$ называют *нулем полукольца* $\mathbf{A}$, если $\forall\,(a \in A)\ a + 0 = 0 + a = a$.

Элемент e полукольца $\mathbf{A} \rightleftharpoons \langle A;\ +,\ \cdot\rangle$ называют *единицей полукольца* $\mathbf{A}$, если $e + e \neq e$ и

$$\forall\,(a \in A)\quad a \cdot e = e \cdot a = a.$$

Таким образом, *нуль* полукольца — нейтральный элемент сложения, а *единица* — нейтральный элемент умножения.

Полугруппу $\langle A;\ +\rangle$ полукольца $\mathbf{A} \rightleftharpoons \langle A;\ +,\ \cdot\rangle$ называют *аддитивной полугруппой* полукольца $\mathbf{A}$, полугруппу $\langle A;\ \cdot\rangle$ — его *мультипликативной полугруппой.*

Определение 2.6.2. Полукольцо $\mathbf{A} \rightleftharpoons \langle A;\ +,\ \cdot \rangle$ называют *кольцом,* если

$$\forall (a, b \in A) \quad \exists (x \in A) \quad a + x = b.$$

Другими словами, полукольцо $\mathbf{A}$ — *кольцо,* если его аддитивная полугруппа — группа.

Пример 2.6.1. Обозначим через Z_m множество всех целых чисел, кратных натуральному m, т. е. чисел c вида

$$c = mx,$$

где x — любое целое. Легко видеть, что арифметические операции $+$ и $\cdot$ (сложение и умножение) — алгебраические операции на Z_m, что Z_m — коммутативная группа относительно сложения, коммутативная полугруппа относительно умножения и обе операции связаны законом дистрибутивности. Таким образом, $\langle Z_m;\ +,\ \cdot \rangle$ — кольцо. Это кольцо коммутативно, имеет нуль и при $m \geqslant 2$ не имеет единицы.

Итак, каждое кольцо имеет нуль кольца, и притом только один (вопрос 2.5.6), но не обязательно содержит единицу.

Определение 2.6.3. Пусть $\mathbf{A} \rightleftharpoons \langle A;\ +,\ \cdot \rangle$ — кольцо, 0 — его нуль, a и b — элементы A, отличные от нуля. Если $a \cdot b = 0$, то элементы a и b называют *делителями нуля* кольца $\mathbf{A}$, а само кольцо $\mathbf{A}$ — *кольцом с делителями нуля.*

Определение 2.6.4. Кольцо $\mathbf{A} \rightleftharpoons \langle A;\ +,\ \cdot,\ 0 \rangle$ называют *телом,* если A состоит не из одного нуля и если

$$\forall (a, b \in A) \quad a \neq 0 \Rightarrow \exists (x, y \in A) \quad ax = b \wedge ya = b.$$

Определение 2.6.5. Коммутативное тело называют *полем.*

Примеры: 2.6.2. Кольцо $\mathbf{Z}/_{(m)}$ классов вычетов кольца целых чисел по модулю m (m — целое > 0). Это кольцо, конечно, состоит из m элементов, коммутативно. $\mathbf{Z}/_{(m)}$ — поле тогда и только тогда, если m простое. При составном m кольцо $\mathbf{Z}/_{(m)}$ имеет делители нуля.

2.6.3. Кольцо $\mathbf{A}[x]$ многочленов над кольцом $\mathbf{A}$ с единицей. Известно, что кольцо $\mathbf{A}[x]$ *коммутативно,* если кольцо $\mathbf{A}$ коммутативно; *без делителей нуля,* если $\mathbf{A}$ без делителей нуля.

2.6.4. Пусть A — непустое множество и $\mathbf{B} \rightleftharpoons \langle B;\ +,\ \cdot,\ 0 \rangle$ — кольцо. Рассмотрим множество O однозначных отображений A в B. Пусть f и g — какие-нибудь элементы множества O. С каждым элементом $x \in A$ сопоставим элементы $fx + gx$ и $fx \cdot gx$. Нетрудно видеть, что тем самым определены два однозначных отображения A в B. Обозначая первое через $f + g$, второе через $f \cdot g$, имеем:

$$f + g\colon \quad x \mapsto fx + gx;$$
$$f \cdot g\colon \quad x \mapsto fx \cdot gx.$$

Таким образом:

$$(f + g)\, x = fx + gx;$$
$$(f \cdot g)\, x = fx \cdot gx.$$

Легко проверить, что система $\mathbf{O} \rightleftarrows \langle O; +, \cdot \rangle$ — кольцо. Нулем кольца является отображение, которое с каждым элементом множества A сопоставляет нуль кольца $\mathbf{B}$. Если B состоит не из одного нуля и A не из одного элемента, то кольцо $\mathbf{O}$ имеет делители нуля. Кольцо $\mathbf{O}$ называют *кольцом функций* из A в $\mathbf{B}$.

2.6.5. Пусть A — отрезок $[-1, 1]$, $B \rightleftarrows R$ — множество действительных чисел. Кольцо всех однозначных отображений A в B — кольцо вещественных функций, определенных на отрезке $[-1; 1]$.

2.6.6. Пусть $\mathbf{P} \rightleftarrows \langle P; +, \cdot, 0 \rangle$ — поле. Рассмотрим множество, состоящее из 0 (нуля) и выражений вида:

$$\sum_{i=m}^{\infty} a_i x^i,$$

где m — целое (> 0, $= 0$ или < 0).

Такие выражения будем складывать и перемножать как многочлены. В результате мы получим систему, являющуюся полем. Это поле называют *полем формальных степенных рядов* от неизвестного x над полем $\mathbf{P}$.

2.6.7. Пусть $\mathbf{P} \rightleftarrows \langle P; +, \cdot, 0 \rangle$ — поле. Рассмотрим множество, состоящее из нуля и выражений вида:

$$\sum_{i \geqslant m, r \geqslant n} a_{ir} x^i y^r,$$

где m и n — любые целые, $a_{mn} \neq 0$, $a_{ir} \in P$. Складывать такие выражения будем, как в примере 2.6.6, т. е. почленно.

Под *произведением* выражений $\sum\limits_{i \geqslant m, r \geqslant n} a_{ir} x^i y^r$ и $\sum\limits_{j \geqslant p, s \geqslant q} b_{js} x^j y^s$ будем понимать выражение вида

$$\sum_{k \geqslant m+p, t \geqslant n+q} c_{kt} x^k y^t,$$

где c_{kt} есть сумма $\sum\limits_{i+j=k, r+s=t} 2^{rj} a_{ir} b_{js}$, в которой суммирование происходит по всем допустимым значениям индексов i, j, r, s. Можно проверить, что полученная система — некоммутативное тело.

Определения 2.6.6, 2.6.7 и 2.6.8. Пусть $\mathbf{A} \rightleftarrows \langle A; +, \cdot \rangle$ — кольцо, A' — подмножество A. Систему $\mathbf{A}' \rightleftarrows \langle A'; +, \cdot \rangle$ называют *подкольцом* (соответственно *подтелом, подполем*) кольца $\mathbf{A}$, если система $\mathbf{A}'$ — кольцо (соответственно тело, поле).

Вопрос 2.6.1. Пусть $\mathbf{A} \rightleftarrows \langle A; +, \cdot \rangle$ — кольцо, A' — непустое подмножество A. Доказать, что система $\langle A'; +, \cdot \rangle$ тогда и только тогда подкольцо кольца $\mathbf{A}$, если для любой пары элементов из A' их разность и произведение снова принадлежат A'.

Пример 2.6.8. Пусть A — отрезок $[-1; 1]$, $B \rightleftarrows R$ — множество всех действительных чисел. Известно, что сумма и произведение двух функций, непрерывных на отрезке,— функции, непрерывные на том же отрезке. Отсюда следует, что множество F вещественных

функций, непрерывных на отрезке $[-1; 1]$, — кольцо относительно операций, определенных в примере 2.6.4.

Вопросы: 2.6.2. Пусть $\mathbf{A} \leftrightharpoons \langle A; +, \cdot, 0\rangle$ — кольцо, A' — непустое подмножество A, состоящее не из одного элемента. Доказать, что система $\langle A'; +, \cdot\rangle$ — подтело кольца $\mathbf{A}$ тогда и только тогда, если для любой пары элементов $\langle a, b\rangle$ множества A' их разность и решение каждого из уравнений

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

при $a \neq 0$ принадлежат A' или $a = 0$.

2.6.3. Пусть $\mathbf{A} \leftrightharpoons \langle A; +, \cdot, 0\rangle$ — кольцо, A' — непустое подмножество A, состоящее не из одного элемента. Доказать, что система $\langle A', +, \cdot, 0\rangle$ — подполе кольца $\mathbf{A}$ тогда и только тогда, если A' для каждой пары не равных нулю элементов содержит их разность и частное.

2.6.4. Пусть $\mathbf{A} \leftrightharpoons \langle A; +, \cdot\rangle$ — кольцо, M — непустое множество с условием, что для каждого μ из M определено $\mathbf{A}_\mu \leftrightharpoons \langle A_\mu; +, \cdot\rangle$ — подкольцо кольца $\mathbf{A}$. Пусть A_0 — пересечение всех A_μ, т. е.

$$A_0 \leftrightharpoons \bigcap_{\mu \in M} A_\mu.$$

Доказать, что система $\langle A_0; +, \cdot\rangle$ — подкольцо кольца $\mathbf{A}$. Коротко: пересечение любого множества подколец кольца $\mathbf{A}$ снова подкольцо кольца $\mathbf{A}$.

2.6.5. Пусть в условиях вопроса 2.6.4 для каждого μ из M система $\mathbf{A}_\mu$ — подтело кольца $\mathbf{A}$. Доказать, что система $\langle A_0; +, \cdot\rangle$ — подтело кольца $\mathbf{A}$.

2.6.6*. Пусть в условиях вопроса 2.6.4 для каждого μ из M система $\mathbf{A}_\mu$ — подполе кольца $\mathbf{A}$. Доказать, что система $\langle A_0; +, \cdot\rangle$ — подполе кольца $\mathbf{A}$.

2.6.7*. Пусть система $\langle A; +, \cdot\rangle$ — полукольцо, $a, b, c, a', b' \in A$. Доказать, предполагая, что все встречающиеся разности имеют смысл, следующие равенства:

1) $(a + b)(a' + b') = (aa' + bb') + (ab' + ba')$;

2) $(a - b)(a' - b') = (aa' + bb') - (ab' + ba')$;

3) $(a - b)c = ac - bc$;

4) $c(a - b) = ca - cb$.

2.6.8. Пусть система $\langle A; +, \cdot\rangle$ — полукольцо с нулем 0. Доказать, что $\forall (a \in A)\ a \cdot 0 = 0 \cdot a = 0$.

2.6.9. Пусть система $\langle A; +, \cdot\rangle$ — кольцо без делителей нуля, A — состоит не из одного нуля и A' — множество отличных от нуля элементов множества A. Доказать, что система $\langle A', \cdot\rangle$ — полугруппа с сокращением.

2.6.10. Пусть система $\langle A; +, \cdot\rangle$ — кольцо с единицей 1, $a \in A$. Доказать, что $-a = (-1) \cdot a$.

2.6.11. Пусть система $\mathbf{A} \rightleftharpoons \langle A; +, \cdot, 0\rangle$ — тело, A' — множество отличных от нуля элементов тела $\mathbf{A}$. Доказать, что система $\langle A'; \cdot\rangle$ — группа.

2.6.12. Пусть система $\langle P; +, \cdot, 0\rangle$ — поле, $a, b, a', b' \in P$; $b \neq 0$, $b' \neq 0$. Доказать, что:

1) $\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + ba'}{bb'}$;

2) $\frac{a}{b} - \frac{a'}{b'} = \frac{ab' - ba'}{bb'}$;

3) $\frac{a}{b} \cdot \frac{a'}{b'} = \frac{a \cdot a'}{bb'}$;

4) $a' \neq 0 \Rightarrow \frac{\frac{a}{b}}{\frac{a'}{b'}} = \frac{a \cdot b'}{b \cdot a'}$;

5) $\frac{a}{b} = \frac{a'}{b'} \Leftrightarrow ab' = a'b$.

2.6.13*. Пусть $\mathbf{A} \rightleftharpoons \langle A; +, \cdot\rangle$ — некоммутативное кольцо, $\mathbf{P} \rightleftharpoons \langle P; +, \cdot\rangle$ — его подполе, перестановочное с $\mathbf{A}$, т. е.

$$\forall (\alpha \in A)\, \forall (a \in P) \quad a\alpha = \alpha a.$$

Пусть, далее, $f(x)$ и $g(x)$ — многочлены над полем $\mathbf{P}$. Доказать, что для любого элемента α кольца $\mathbf{A}$

$$[f(x) \cdot g(x)]_{x=\alpha} = [f(x)]_{x=\alpha} \cdot [g(x)]_{x=\alpha} \qquad (2.6.1)$$

2.6.14. Пусть P — множество всех пар $\langle a, b\rangle$ натуральных чисел и пусть на P определены операции $\oplus$ и $\odot$ следующими условиями:

$$\langle a, b\rangle \oplus \langle a', b'\rangle \rightleftharpoons \langle a + a', b + b'\rangle;$$
$$\langle a, b\rangle \odot \langle a', b'\rangle \rightleftharpoons \langle a \cdot a', b \cdot b'\rangle.$$

Показать, что система $\langle P; \oplus, \odot\rangle$ — коммутативное полукольцо с единицей.

2.6.15. Пусть P_1 — множество всех пар $\langle a, b\rangle$ натуральных чисел с условием $a \leqslant b$ и пусть $\oplus$ и $\odot$ — операции, определенные в вопросе 2.6.14. Показать, что система $\mathbf{P}_1 \rightleftharpoons \langle P_1; \oplus, \odot\rangle$ — коммутативное полукольцо с единицей.

2.6.16. Пусть P_2 — множество всех пар $\langle a, b\rangle$ натуральных чисел и пусть на P_2 операции $\oplus$ и $\odot$ определены следующим образом:

$$\langle a, b\rangle \oplus \langle a', b'\rangle \rightleftharpoons \langle a + a',\ b + b'\rangle;$$
$$\langle a, b\rangle \odot \langle a', b'\rangle \rightleftharpoons \langle aa' + bb',\ ab' + a'b\rangle.$$

Показать, что система $\langle P_2; \oplus, \odot\rangle$ — коммутативное полукольцо.

2.6.17. Пусть P_3 — множество всех пар $\langle a, b\rangle$ целых чисел с условием $b > 0$ и пусть на P_3 операции $\oplus$ и $\odot$ определены следующим образом:

$$\langle a, b\rangle \oplus \langle a', b'\rangle \rightleftharpoons \langle ab' + a'b,\ bb'\rangle;$$
$$\langle a, b\rangle \odot \langle a', b'\rangle \rightleftharpoons \langle aa',\ bb'\rangle.$$

Показать, что системы $\langle P_3; \oplus\rangle$ и $\langle P_3; \odot\rangle$ — коммутативные полугруппы с нейтральными элементами $\langle 0, 1\rangle$ и $\langle 1, 1\rangle$ соответственно. Показать, что система $\langle P_3; \oplus, \odot\rangle$ не является полукольцом.

2.6.18. Обозначим через P_4 множество всех пар рациональных чисел $\langle a, b\rangle$, для которых операции сложения $\oplus$ и умножения $\odot$ определены следующим образом:

$$\langle a, b\rangle \oplus \langle a', b'\rangle \rightleftharpoons \langle a + a', b + b'\rangle;$$
$$\langle a, b\rangle \odot \langle a', b'\rangle \rightleftharpoons \langle aa' + 2bb', ab' + a'b\rangle.$$

Показать, что $\langle P_4; \oplus, \odot\rangle$ — поле.

2.6.19. Обозначим через P_5 множество всех пар действительных чисел $\langle a, b\rangle$, для которых операции сложения $\oplus$ и умножения $\odot$ определены следующим образом:

$$\langle a, b\rangle \oplus \langle a', b'\rangle \rightleftharpoons \langle a + a', b + b'\rangle;$$
$$\langle a, b\rangle \odot \langle a', b'\rangle \rightleftharpoons \langle aa' - bb', ab' + a'b\rangle.$$

Показать, что $\langle P_5; \oplus, \odot\rangle$ — поле, а пары $\langle 0, 0\rangle$ и $\langle 1, 0\rangle$ — нуль и единица этого поля.

2.6.20. Обозначим через M_2 множество матриц второго порядка над кольцом комплексных чисел, т. е. с комплексными элементами, для которых сложение $\oplus$ и умножение $\odot$ определены обычным образом, т. е.:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \oplus \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \rightleftharpoons \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix};$$
$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \odot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \rightleftharpoons \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}.$$

Доказать, что $\langle M_2; \oplus, \odot\rangle$ — некоммутативное кольцо с делителями нуля.

2.6.21*. Для каждого комплексного числа $\alpha = a + bi$ символом $\bar{\alpha}$ будем обозначать число, сопряженное с α, т. е. число $a - bi$ (a, b — действительные числа, $i^2 = -1$). Известно, что:

$$\overline{\alpha + \beta} = \bar{\alpha} + \bar{\beta}; \quad \overline{\alpha \cdot \beta} = \bar{\alpha} \cdot \bar{\beta}.$$

Символом M_2' обозначим множество матриц второго порядка с комплексными элементами вида

$$q \rightleftharpoons \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}.$$

Доказать, что $\langle M_2'; \oplus, \odot\rangle$ — тело.

2.6.22. Пусть K — множество всех конечных множеств натуральных чисел. Если $A \in K$ и $B \in K$, то под суммой $A + B$ (соот-

ветственно произведением $A \cdot B$) множеств A и B будем понимать множество всех сумм $a + b$ (соответственно произведений $a \cdot b$) таких, что $a \in A$, $b \in B$. Показать, что определенные так тернарные отношения в K — бинарные операции на K. Почему система $\langle K; +, \cdot \rangle$ не является коммутативным полукольцом?

2.6.23. Пусть θ — любой комплексный корень уравнения $x^3 = 2$ и $Q(\theta)$ — множество всех комплексных чисел вида

$$a_0 + a_1\theta + a_2\theta^2,$$

где a_0, a_1, a_2 — произвольные рациональные числа. Показать, что $\mathbf{Q}(\theta) \rightleftharpoons \langle Q(\theta); +, \cdot \rangle$ — поле, если $+$ и $\cdot$ — сложение и умножение комплексных чисел.

2.7. Векторные пространства и линейные алгебры

Определение 2.7.1. Пусть $\mathbf{P} \rightleftharpoons \langle P; +, \cdot, 0, 1\rangle$—поле, $\langle A; +, \theta\rangle$— коммутативная группа, и пусть для каждого элемента k поля $\mathbf{P}$ на множестве A задана унарная операция ω_k. Систему $\mathbf{A} \rightleftharpoons \langle A; +, \theta, \{\omega_k | k \in P\}\rangle$ называют *векторным пространством* над полем $\mathbf{P}$, если $\langle A; +, \theta; \{\omega_k | k \in P\}\rangle$ выполнены следующие условия:

1) $\forall (a \in A) \quad \omega_1 a = a$;
2) $\forall (a, b \in A) \quad \forall (k \in P) \quad \omega_k (a + b) = \omega_k a + \omega_k b$;
3) $\forall (a \in A) \quad \forall (k, l \in P) \quad \omega_{k+l} a = \omega_k a + \omega_l a$;
4) $\forall (a \in A) \quad \forall (k, l \in P) \quad \omega_{kl} a = \omega_k (\omega_l a) = \omega_l (\omega_k a)$.

Любой элемент векторного пространства $\mathbf{A}$, т. е. любой элемент множества A, называют *вектором*.

Множество $\{\omega_k | k \in P\}$ унарных операций пространства $\mathbf{A}$ определяет такое однозначное отображение прямого произведения $P \times A$ в множество A, в котором паре $\langle k, a\rangle$ соответствует элемент $\omega_k a$ пространства $\mathbf{A}$. Обычно этот элемент называют *произведением* элементов k и a и обозначают символом $k \cdot a$. Таким образом,

$$ka \rightleftharpoons \omega_k a.$$

В соответствии с этим условия 1) — 4) записываются так:

1) $\forall (a \in A) \quad 1 \cdot a = a$;
2) $\forall (a, b \in A) \quad \forall (k \in P) \quad k(a + b) = ka + kb$;
3) $\forall (a \in A) \quad \forall (k, l \in P) \quad (k + l) a = ka + la$;
4) $\forall (a \in A) \quad \forall (k, l \in P) \quad (kl) a = k(la) = l(ka)$.

В связи с этим естественно вместо записи $\langle A; +, \theta, \{\omega_k | k \in P\}\rangle$ употреблять обозначение $\langle A; +, \theta, \mathbf{P}\rangle$.

Пример 2.7.1. Пусть $\mathbf{P} \rightleftharpoons \langle P;\ +,\ \cdot,\ 0,\ 1\rangle$ — поле; определим для n-кортежей элементов поля $\mathbf{P}$ сложение, как в вопросе 2.5.13, а умножение на элементы поля $\mathbf{P}$ условием:

$$k \cdot \langle a_1,\ \ldots,\ a_n\rangle \rightleftharpoons \langle ka_1,\ \ldots,\ ka_n\rangle.$$

Легко видеть, что введенными операциями определяется векторное пространство над полем $\mathbf{P}$.

Определение 2.7.2. Пусть $\mathbf{A} \rightleftharpoons \langle A;\ +,\ \theta;\ \mathbf{P}\rangle$ — векторное пространство над полем $\mathbf{P}$; систему элементов

$$a_1,\ \ldots,\ a_n \tag{2.7.1}$$

пространства $\mathbf{A}$ называют *линейно зависимой* над полем $\mathbf{P}$, если в поле $\mathbf{P}$ можно найти такие не все равные нулю элементы $k_1,\ \ldots,\ k_n$, что

$$k_1a_1 + \cdots + k_na_n = \theta.$$

Систему (2.7.1) называют *линейно независимой* над полем $\mathbf{P}$, если

$$k_1a_1 + \cdots + k_na_n \neq \theta,$$

каковы бы ни были не все равные нулю элементы $k_1,\ \ldots,\ k_n$ поля $\mathbf{P}$.

Пусть $b \in A$; элемент b линейно над полем $\mathbf{P}$ выражается через систему (2.7.1), если в поле $\mathbf{P}$ можно найти такие элементы $b_1,\ \ldots, b_n$, что

$$b = b_1a_1 + \cdots + b_na_n.$$

Так как строки (столбцы) любой прямоугольной над полем $\mathbf{P}$ матрицы можно рассматривать как векторы одного пространства над полем $\mathbf{P}$ (пример 2.7.1), то без особых пояснений ясен смысл терминов: «строки данной матрицы линейно зависимы (независимы) над полем $\mathbf{P}$», «данная строка матрицы M линейно над полем $\mathbf{P}$ выражается через остальные строки этой матрицы».

Вопросы: 2.7.1. Доказать, что конечная система векторов пространства над полем $\mathbf{P}$ линейно зависима, если ее какая-нибудь подсистема линейно зависима.

2.7.2. Присоединим к какой-нибудь матрице над полем $\mathbf{P}$ столбец, состоящий из одних нулей. Доказать, что строки данной матрицы линейно зависимы над полем $\mathbf{P}$ тогда и только тогда, если линейно зависимы над полем $\mathbf{P}$ строки полученной матрицы.

2.7.3. Пусть $s > 1$; $\mathbf{P}$ — поле, $\mathbf{A}$ — векторное пространство над полем $\mathbf{P}$; $c_2,\ \ldots,\ c_s$ — элементы поля $\mathbf{P}$; $\alpha_1,\ \ldots,\ \alpha_s,\ \beta_1,\ \ldots,\ \beta_s$ — векторы пространства $\mathbf{A}$ такие, что:

$$\begin{aligned}
\beta_1 &= \alpha_1;\\
\beta_2 &= \alpha_2 - c_2\alpha_1;\\
&\vdots\\
\beta_s &= \alpha_s - c_s\alpha_1.
\end{aligned}$$

Доказать, что система векторов $\alpha_1,\ \ldots,\ \alpha_s$ линейно зависима над полем $\mathbf{P}$ тогда и только тогда, если система $\beta_1,\ \ldots,\ \beta_s$ линейно зависима над полем $\mathbf{P}$.

2.7.4. Пусть **P** — поле, M — прямоугольная матрица над полем **P**. Доказать, что если число строк матрицы M больше числа ее столбцов, то ее строки линейно зависимы над полем **P**.

2.7.5. Пусть **P** — поле, **A** — векторное пространство над полем **P**, $\alpha_1, \ldots, \alpha_s$ и $\beta_1, \ldots, \beta_k$ — две системы векторов пространства **A**. Доказать следующее утверждение: если $k > s$ и каждый вектор второй системы линейно над полем **P** выражается через векторы первой, то вторая система линейно зависима над полем **P**.

Определение 2.7.3. Пусть $\mathbf{A} \rightleftharpoons \langle A; +, \theta, \mathbf{P}\rangle$ — векторное пространство над полем **P**. Пространство **A** называют *n-мерным векторным пространством* над полем **P**, а число n — *размерностью* этого пространства, если в пространстве **A** можно указать такие элементы:

$$e_1, \ldots, e_n, \tag{2.7.2}$$

что любой вектор α пространства **A** линейно над полем **P** и однозначно выражается через векторы системы (2.7.2). Систему (2.7.2) в этом случае называют *базисом* пространства **A**.

Легко видеть (вопрос 2.7.5), что размерность пространства не зависит от выбора ее базиса. Другими словами, число векторов в любом базисе пространства **A** одно и то же.

Определение 2.7.4. Пусть $\mathbf{P} \rightleftharpoons \langle P; +, \cdot, 0, 1\rangle$—поле, $\langle A; +, \cdot, \theta\rangle$—алгебра с двумя бинарными операциями и одной нульарной. Пусть для каждого элемента k поля **P** на множестве A задана одна унарная операция ω_k. Систему $\mathbf{A} \rightleftharpoons \langle A; +, \cdot, \theta, \{\omega_k \mid k \in P\}\rangle$ называют *линейной алгеброй* над полем **P**, если выполняются следующие условия:

1) система $\langle A; +, \theta, \{\omega_k \mid k \in P\}\rangle$ — векторное пространство над полем **P**;

2) $\forall (a, b, c \in A) \quad (a + b)c = ac + bc \wedge c(a + b) = ca + cb$;

3) $\forall (a, b \in A) \quad \forall (k \in P) \quad \omega_k(ab) = (\omega_k a)\, b = a\,(\omega_k b)$.

Как и выше, для любых $k \in P$ и $a \in A$ элемент $\omega_k a$ обычно называют *произведением* элементов k и a и употребляют обозначение

$$ka \rightleftharpoons \omega_k a.$$

В согласии с этим вместо записи $\langle A; +, \cdot, \theta, \{\omega_k \mid k \in P\}\rangle$ употребляют обозначение $\langle A; +, \cdot, \theta; \mathbf{P}\rangle$.

Линейную алгебру **A** называют *ассоциативной,* если

$$\forall (a, b, c \in A) \quad (a \cdot b) \cdot c = a \cdot (b \cdot c), \tag{2.7.3}$$

и *коммутативной, если*

$$\forall (a, b \in A) \quad a \cdot b = b \cdot a. \tag{2.7.4}$$

В случае, если для алгебры **A** выполняются условия (2.7.3.) и (2.7.4), алгебру **A** называют *ассоциативно-коммутативной.*

Линейную алгебру **A** называют *альтернативной,* если

$$\forall (a, b \in A) \quad (a \cdot a) \cdot b = a \cdot (a \cdot b) \wedge (a \cdot b) \cdot a = \\ = a \cdot (b \cdot a) \wedge (a \cdot b)\, b = a \cdot (b \cdot b). \tag{2.7.5}$$

Линейную алгебру **A** называют *алгеброй с делением,* если

$$\forall (a \cdot b \in A)\, a \neq \theta \Rightarrow \exists (x, y \in A) \quad ax = b \wedge y \cdot a = b.$$

Линейную алгебру $\langle A;\ +,\ \cdot,\ \theta;\ \mathbf{P}\rangle$ называют *алгеброй без делителей нуля,* если

$$\forall (a,\ b \subset A)\ a \neq \theta \wedge b \neq \theta \Rightarrow a \cdot b \neq \theta.$$

Определение 2.7.5. Пусть $\mathbf{A} \rightleftharpoons \langle A;\ +;\ \cdot,\ \{\omega_k \mid k \in P\}\rangle$ и $\mathbf{B} \rightleftharpoons \langle B;\ +;\ \cdot,\ \{\theta_k \mid k \in P\}\rangle$ — линейные алгебры над полем $\mathbf{P} \rightleftharpoons \langle P;\ +,\ \cdot\rangle$. Если алгебра $\langle B;\ +,\ \cdot\rangle$ — подкольцо кольца $\langle A;+,\ \cdot\rangle$ и

$$\forall (b \in B) \quad \forall (k \in P) \quad \omega_k b = \theta_k b,$$

то алгебру **B** называют *подалгеброй алгебры* **A**.

Пример 2.7.2. Пусть $\mathbf{A} \rightleftharpoons \langle A;\ +,\ \cdot\rangle$ — коммутативное кольцо, $\mathbf{P} \rightleftharpoons \langle P;\ +,\ \cdot\rangle$ — подполе кольца **A**. Полагаем

$$\forall (a \in A) \quad \forall (k \in P) \quad \omega_k a \rightleftharpoons k \cdot a.$$

Нетрудно заметить, что система $\langle A;\ +,\ \cdot,\ \{\omega_k \mid k \in P\}\rangle$ — алгебра над полем **P**. Итак, коммутативное кольцо — линейная алгебра над любым своим подполем.

Примеры: 2.7.3. Рассмотрим кольцо M_n матриц порядка n над полем $\mathbf{P} \rightleftharpoons \langle P;\ +,\ \cdot\rangle$ (см. вопрос 2.6.20). Определим *умножение* элементов множества P на матрицы порядка n следующим образом:

$$k \cdot \begin{pmatrix} a_{11}a_{12} & \dots & a_{1n} \\ a_{21}a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots \\ a_{n1}a_{n2} & \dots & a_{nn} \end{pmatrix} \rightleftharpoons \begin{pmatrix} ka_{11} & ka_{12} & \dots & ka_{1n} \\ ka_{21} & ka_{22} & \dots & ka_{2n} \\ \dots & \dots & \dots & \dots \\ ka_{n1} & ka_{n2} & \dots & ka_{nn} \end{pmatrix}.$$

Нетрудно проверить, что система $\langle M_n;\ +,\ \cdot,\ \mathbf{P}\rangle$ является ассоциативной алгеброй без деления над полем **P**.

2.7.4. Кольцо $\langle M_2';\ \oplus,\ \odot\rangle$ вопроса 2.6.21 — тело. Если умножение на действительные числа матриц множества M_2' определить, как в примере 2.7.3, то мы получим ассоциативную алгебру с делением над полем действительных чисел.

2.7.5. Кольцо $\mathbf{P}[x]$ многочленов от одного неизвестного над полем **P** является линейной алгеброй над своим подполем **P**.

Вопросы: 2.7.6. Пусть $\mathbf{A} \rightleftharpoons \langle A;\ +,\ \cdot,\ \mathbf{P}\rangle$ — алгебра над полем $\mathbf{P} \rightleftharpoons \langle P;\ +,\ \cdot\rangle$, A' — подмножество A. Доказать, что система $\mathbf{A}' \rightleftharpoons \langle A';\ +,\ \cdot,\ \mathbf{P}\rangle$ тогда и только тогда подалгебра алгебры **A**, если выполняются следующие условия:

1) $\forall (a, b \in A') \quad a - b \in A'$;

2) $\forall (a, b \in A') \quad a \cdot b \in A'$;

3) $\forall (a \in A') \quad \forall (k \in P)\, ka \in A'$.

2.7.7. Пусть $\mathbf{A} \rightleftharpoons \langle A;\ +,\ \cdot,\ \mathbf{P}\rangle$ — линейная алгебра над полем **P**; B — непустое множество с условием: для каждого β из B определена $\mathbf{A}_\beta \rightleftharpoons \langle A_\beta;\ +,\ \cdot,\ \mathbf{P}\rangle$ — подалгебра алгебры **A**. Пусть A_0 — пере-

сечение всех A_β, т. е. $A_0 \rightleftharpoons \bigcap\limits_{\beta \in B} A_\beta$. Доказать, что система $\langle A_0;\ +,\ \cdot,\ \mathbf{P}\rangle$ — подалгебра алгебры **A**. Коротко: пересечение любого множества подалгебр **A** снова подалгебра алгебры **A**.

2.7.8. Пусть **A** — ассоциативная линейная алгебра с делением над полем **P**. Тогда **A** содержит единицу и подполе, изоморфное **P**.

2.8. Гомоморфизм и изоморфизм алгебраических систем

Определение 2.8.1. Пусть $\mathbf{A} \rightleftharpoons \langle A;\ \{\omega_\beta \mid \beta \in B\}\rangle$ и $\mathbf{A}' \rightleftharpoons \langle A';\{\omega'_\beta \mid \beta \in B\}\rangle$—алгебраические системы, и пусть для каждого β из B отношения ω_β и ω'_β одного ранга n_β. *Гомоморфным отображением системы* **A** в (на) **A′** называется такое однозначное отображение f множества A в (соответственно на) A', которое удовлетворяет условию

$$\forall (\beta \in B)\, \forall (a_1, \ldots, a_{n_\beta} \in A) \quad \langle a_1, \ldots, a_{n_\beta}\rangle \in \omega_\beta \Rightarrow$$
$$\Rightarrow \langle f(a_1), \ldots, f(a_{n_\beta})\rangle \in \omega'_\beta. \qquad (2.8.1)$$

Определение 2.8.2. Пусть $\mathbf{A} \rightleftharpoons \langle A;\ \{\omega_\beta \mid \beta \in B\}\rangle$ и $\mathbf{A}' \rightleftharpoons \langle A';\ \langle \omega'_\beta \mid \beta \in B\}\rangle$ — алгебраические системы, и пусть для каждого β из B отношения ω_β и ω'_β одного ранга n_β. *Изоморфным отображением системы* **A** в (на) **A′** называют такое однозначное отображение множества A в (соответственно на) A', которое, во-первых, взаимнооднозначно и, во-вторых, удовлетворяет условию

$$\forall (\beta \in B) \quad \forall (a_1, \ldots, a_{n_\beta} \in A) \quad \langle a_1, \ldots, a_{n_\beta}\rangle \in \omega_\beta \Leftrightarrow$$
$$\Leftrightarrow \langle f(a_1, \ldots, f(a_{n_\beta})\rangle \ni \omega'_\beta. \qquad (2.8.2)$$

Замечания 1. Если ω_β и ω'_β — алгебраические операции, то из условия (2.8.1) следует условие (2.8.2).

2. Если ω_β и ω'_β — отношения, то утверждение, аналогичное высказанному в замечании 1, вообще говоря, неверно. В самом деле, пусть $A = A'$, $f(a) = a$, но ω_β — правильная часть ω'_β. В этом случае условие (2.8.1) выполняется в одну сторону $\Rightarrow$, но не выполняется в другую $\Leftarrow$.

3. Если ω_β — алгебраическая операция, то из условия (2.8.2) следует, что и ω'_β — алгебраическая операция.

Обозначение. Если f — изоморфное отображение системы **A** на **B**, то мы употребляем запись

$$f\colon\ \mathbf{A} \cong \mathbf{B}.$$

Запись «$\mathbf{A} \cong \mathbf{B}$» означает, что существует (определено) изоморфное отображение системы **A** на систему **B**.

Теорема 2.8.1. Пусть $\mathbf{A} \rightleftharpoons \langle A;\ \omega\rangle$ и $\mathbf{B} \rightleftharpoons \langle B;\ \rho\rangle$ — системы с отношениями одного ранга 3, и пусть определено изоморфное

отображение f системы **A** на систему **B**. Тогда ω — алгебраическая (бинарная) операция на A в том и только том случае, если ρ — алгебраическая операция на B.

Доказательство. Так как f — отображение A на B, то любой элемент B является образом некоторого элемента A в отображении f. Нам достаточно показать, что для любых элементов $f(a_1)$ и $f(a_2)$ из B можно найти и только один элемент $f(x) \in B$ такой, что

$$\langle f(a_1),\ f(a_2),\ f(x)\rangle \in \rho. \qquad (2.8.3)$$

Но поскольку f — изоморфное отображение **A** на **B**, то соотношение (2.8.3) выполняется тогда и только тогда, если

$$\langle a_1,\ a_2,\ x\rangle \in \omega.$$

Последним условием элемент x множества A, а значит, и $f(x)$ определяется однозначно.

Теорема 2.8.2. Пусть $\mathbf{A} \leftrightharpoons \langle A;\ \omega\rangle$ и $\mathbf{B} \leftrightharpoons \langle B;\ \rho\rangle$ — алгебры; ω и ρ — бинарные операции в них; f — гомоморфное отображение **A** на **B**. Тогда:

1) если операция ω ассоциативна, то и операция ρ ассоциативна;

2) если операция ω коммутативна, то и операция ρ коммутативна;

3) если операция ω обладает нейтральным элементом, равным θ, то и операция ρ обладает нейтральным элементом, равным $f(\theta)$;

4) если операция ω обладает нейтральным элементом θ и a' — симметричный a элемент A относительно операции ω с нейтральным элементом θ, то $f(a')$ — симметричный элементу $f(a)$ относительно операции ρ с нейтральным элементом $f(\theta)$;

5) если система **A** — группа, то и система **B** — группа.

Доказательство. Докажем первое утверждение. Пусть b_1, b_2, b_3 — любые элементы множества B. Так как f — отображение A на B, то во множестве A имеются элементы a_1, a_2, a_3 такие, что

$$f(a_1) = b_1, \quad f(a_2) = b_2, \quad f(a_3) = b_3.$$

Но f — гомоморфное отображение системы **A** на **B**, поэтому

$$\forall\,(x,\ y \in A) \quad f(\omega xy) = \rho f(x)\, f(y).$$

Отсюда легко получим

$$\rho\rho b_1 b_2 b_3 = \rho\rho f(a_1) f(a_2) f(a_3) = \rho f(\omega a_1 a_2) f(a_3) = f(\omega\omega a_1 a_2 a_3) =$$
$$= f(\omega a_1 \omega a_2 a_3) = \rho f(a_1) f(\omega a_2 a_3) = \rho f(a_1)\, \rho f(a_2) f(a_3) = \rho b_1 \rho b_2 b_3.$$

Аналогично доказываются и другие утверждения.

Теорема 2.8.3. Пусть системы $\mathbf{A} \leftrightharpoons \langle A;\ +,\ \cdot\rangle$, $\mathbf{B} \leftrightharpoons \langle B;\ \oplus,\ \odot\rangle$ — алгебры с бинарными операциями и f — гомоморфное отображение системы **A** на систему **B**. Тогда:

1) если операции системы **A** связаны законом дистрибутивности, то и операции системы **B** обладают тем же свойством;

2) если система **A** — полукольцо, то и система **B** — полукольцо, в частности коммутативное полукольцо, если таким является полукольцо **A**;

3) если система **A** — кольцо, то и система **B** — кольцо;

4) если система **A** — тело, то и система **B** — тело или состоит из одного нуля;

5) если система **A** — поле, то и система **B** — поле или состоит из одного нуля.

Доказательство этой теоремы легко получить, если воспользоваться теоремой 2.8.2.

Вопросы: **2.8.1.** Доказать, что для любых систем **A**, **B** и **C** с отношениями:

1) $\mathbf{A} \cong \mathbf{A}$;
2) $\mathbf{A} \cong \mathbf{B} \Rightarrow \mathbf{B} \cong \mathbf{A}$;
3) $\mathbf{A} \cong \mathbf{B} \wedge \mathbf{B} \cong \mathbf{C} \Rightarrow \mathbf{A} \cong \mathbf{C}$.

2.8.2. В условиях теоремы 2.8.2 показать, что если система **A** — полугруппа с сокращением, то **B** может и не обладать тем же свойством.

2.8.3. В условиях теоремы 2.8.2 показать, что если f — изоморфное отображение **A** на **B** и **A**—полугруппа с сокращением, то и B обладает тем же свойством.

2.8.4. В условиях теоремы 2.8.3 **B** не обязательно кольцо без делителей нуля, если **A** — кольцо без делителей нуля.

2.8.5. В условиях теоремы 2.8.3 показать, что если f — изоморфное отображение **A** на **B** и **A** — кольцо без делителей нуля, то и **B** — кольцо без делителей нуля.

2.8.6*. Пусть $\mathbf{A} \rightleftharpoons \langle A;\ +,\ \cdot,\ \mathbf{P}\rangle$ — линейная алгебра над полем $\mathbf{P} \rightleftharpoons \langle P;\ \oplus,\ \odot,\ 0,\ 1\rangle$ с единицей e. Доказать, что система $\langle A;\ +, \cdot e\rangle$ содержит подполе, изоморфное **P**.

2.8.7. Пусть $\mathbf{A} \rightleftharpoons \langle A; \{\omega_\mu \mid \mu \in M\}\rangle$ и $\mathbf{B} \rightleftharpoons \langle B; \{\rho_\mu \mid \mu \in M\}\rangle$ — алгебраические системы и $M' \subset M$. Доказать, что если системы **A** и **B** изоморфны, то системы $\langle A; \{\omega_\mu \mid \mu \in M'\}\rangle$ и $\langle B; \{\rho_\mu \mid \mu \in M'\}\rangle$ также изоморфны.

2.8.8. Пусть $\mathbf{A} \rightleftharpoons \langle A; \{\omega_\mu \mid \mu \in M\}\rangle$ — какая-либо алгебраическая система, B — множество и f — однозначное отображение множества A в B. Если для каждого μ из M через ρ_μ обозначить отношение в B, наведенное (определение 2.3.4) отношением ω_μ при отображении f множества A в B, то f — гомоморфное отображение системы **A** в систему $\mathbf{B} \rightleftharpoons \langle B; \{\rho_\mu \mid \mu \in M\}\rangle$. В частности, f — изоморфное отображение системы **A** на **B**, если f— взаимно-однозначное отображение A на B.

2.8.9. Пусть θ и θ' — какие-нибудь комплексные корни уравнения $x^3 = 2$, $\mathbf{Q}(\theta)$ и $\mathbf{Q}(\theta')$ — поля вопроса 2.6.23. Показать, что поля $\mathbf{Q}(\theta)$ и $\mathbf{Q}(\theta')$ — изоморфны.

2.9. Отношение эквивалентности

Определение 2.9.1. Бинарное отношение ω, заданное во множестве A, называют *отношением эквивалентности* во множестве A, если оно рефлексивно, симметрично и транзитивно. Другими словами,

если:

1) $\forall (a \in A) \quad a\omega a$;
2) $\forall (a, b \in A) \quad a\omega b \Rightarrow b\omega a$;
3) $\forall (a, b, c \in A) \quad a\omega b \wedge b\omega c \Rightarrow a\omega c$.

Пример 2.9.1. Пусть m — фиксированное натуральное число. Определим отношение ω_m в множестве целых чисел Z следующим образом:

$$\forall (a, b \in Z) \quad a\omega_m b \Leftrightarrow a \equiv b \pmod{m}.$$

Нетрудно проверить, что отношение ω_m — отношение эквивалентности. Это имеют в виду, когда говорят: «Отношение сравнения по модулю m является отношением эквивалентности во множестве целых чисел».

Вопросы: 2.9.1. Рассмотрим множество P_2 вопроса 2.6.16. Определим отношение ω в P_2 следующим образом:

$$\langle a, b\rangle \omega \langle a', b'\rangle \Leftrightarrow a + b' = a' + b.$$

Показать, что отношение ω во множестве P_2 — отношение эквивалентности.

2.9.2. Рассмотрим множество P_3 вопроса 2.6.17. Определим отношение ω в P_3 следующим образом:

$$\langle a, b\rangle \omega \langle a', b'\rangle \Leftrightarrow ab' = a'b.$$

Показать, что отношение ω во множестве P_3 — отношение эквивалентности.

Обозначение. Для отношения эквивалентности употребляют часто обозначение: $a \sim b$ (читают: a эквивалентно b).

Определение 2.9.2. Пусть ω — отношение эквивалентности во множестве A. *Классом эквивалентности любого элемента* $x \in A$ относительно отношения ω называют множество

$$\omega x \rightleftharpoons \{y / y \in A \wedge x\omega y\}.$$

Обозначение. Класс эквивалентности элемента x относительно отношения ω обозначают следующим образом: ωx, или $(x)_\omega$, или (x), или $\bar{x}$. Легко видеть, что если ω — отношение эквивалентности во множестве A, то:

1) $\forall (x \in A) \quad x \in (x)_\omega$;
2) $\forall (x, y \in A) \quad (x)_\omega \cap (y)_\omega \neq \varnothing \Leftrightarrow (x)_\omega = (y)_\omega$.

Таким образом, отношение эквивалентности ω во множестве A определяет разбиение A на попарно непересекающиеся подмножества, называемые *классами эквивалентности отношения* ω. Множество всех классов эквивалентности отношения ω называют также *фактормножеством* A относительно ω и обозначают символом A/ω.

Из сказанного выше следует, что для любой пары классов $(x)_\omega$ и $(y)_\omega$ фактормножества A/ω

$$(x)_\omega = (y)_\omega \Leftrightarrow x\omega y.$$

Определим отображение φ множества A в фактормножество A/ω следующим образом:

$$\varphi: \quad x \mapsto (x)_\omega. \tag{2.9.1}$$

Легко видеть, что φ — однозначное отображение множества A на фактормножество A/ω.

Примеры 2.9.2. Отношение равномощности во множестве вопроса 2.6.22 — отношение эквивалентности. Класс эквивалентности множества K относительно равномощности состоит из равночисленных конечных множеств натуральных чисел.

2.9.3. Классы вычетов кольца целых чисел по натуральному модулю m — классы эквивалентности множества целых чисел относительно сравнения по модулю m.

2.9.4. Пусть $\mathbf{P} \leftrightarrows \langle P; +, \cdot, 0\rangle$ — поле, $\varphi(x)$ — не равный нулю многочлен кольца $\mathbf{P}[x]$. Многочлены $f(x)$ и $g(x)$ кольца $\mathbf{P}[x]$ называют *сравнимыми* по модулю $\varphi(x)$, если

$$\varphi(x) \mid f(x) - g(x).$$

Легко видеть, что отношение сравнимости по модулю $\varphi(x)$ — отношение эквивалентности, монотонное относительно сложения и умножения в кольце $\mathbf{P}[x]$.

Теорема 2.9.1. Пусть $\mathbf{A} \leftrightarrows \langle A; +\rangle$ — алгебра с одной бинарной операцией; ω — отношение эквивалентности во множестве A, монотонное относительно указанной операции. Другими словами,

$$\forall (a, b, c \in A) \quad a\omega b \Rightarrow (a + c)\,\omega\,(b + c) \wedge (c + a)\,\omega\,(c + b).$$

Сопоставим с каждой парой классов эквивалентности $(a)_\omega$ и $(b)_\omega$ фактормножества A/ω класс $(a + b)_\omega$. Тогда определенное указанным способом тернарное отношение «+» в фактормножестве A/ω — бинарная алгебраическая операция.

Доказательство. Так как сложение в A — алгебраическая операция, то, каковы бы ни были элементы a и b из A, сумма $a + b$ входит в A и, следовательно, в класс $(a + b)_\omega$. Поэтому с каждой парой классов $(a)_\omega$ и $(b)_\omega$ в указанном соответствии сопоставляется по крайней мере один класс, а именно $(a + b)_\omega$. Нам остается показать, что этот класс определяется однозначно. Пусть

$$(a)_\omega = (a')_\omega; \quad (b)_\omega = (b')_\omega.$$

Докажем, что

$$(a + b)_\omega = (a' + b')_\omega.$$

В силу монотонности ω имеем:

$$a\omega a' \Rightarrow (a + b)\,\omega\,(a' + b);$$
$$b\omega b' \Rightarrow (a' + b)\,\omega\,(a' + b').$$

А в силу транзитивности получим

$$(a + b)\,\omega\,(a' + b')$$

и, следовательно,

$$(a + b)_\omega = (a' + b')_\omega.$$

Из доказанной теоремы следует, что система $\langle A/_\omega;\ +\rangle$ — алгебра. В каком отношении она находится к системе $\langle A;\ +\rangle$?

Теорема 2.9.2. Пусть в условиях теоремы 2.9.1. f — однозначное отображение множества A на фактормножество $A/_\omega$, определенное условием

$$f\colon\ x \mapsto (x)_\omega.$$

Тогда f — гомоморфное отображение системы $\langle A;\ +\rangle$ на систему $\langle A/_\omega;\ +\rangle$.

Доказательство. Наше утверждение справедливо, так как:

1) f — однозначное отображение A на $A/_\omega$;

2) $\forall\,(x,\ y \in A)\ \ f(x+y) = (x+y)_\omega = (x)_\omega + (y)_\omega = f(x) + f(y)$.

Теорема 2.9.3. Пусть $\mathbf{A} \rightleftharpoons \langle A;\ +,\ \cdot\rangle$ — алгебра с двумя бинарными операциями, ω — отношение эквивалентности в A, монотонное относительно каждой операции, f — однозначное отображение A на $A/_\omega$, определяемое условием

$$f(x) = (x)_\omega,$$

$+$ и $\cdot$ — тернарные отношения на $A/_\omega$, сопоставляющие с каждой парой классов $(x)_\omega$ и $(y)_\omega$ фактормножества $A/^\omega$ классы $(x+y)_\omega$ и $(x\cdot y)_\omega$ соответственно.

Тогда система $\mathbf{B} \rightleftharpoons \langle A/_\omega;\ +,\ \cdot\rangle$ — алгебра, а f — гомоморфное отображение $\mathbf{A}$ на $\mathbf{B}$.

Справедливость теоремы следует из теорем 2.9.1 и 2.9.2.

Пример 2.9.4. Кольцо целых чисел гомоморфно отображается на факторкольцо классов вычетов по модулю m.

Вопросы: 2.9.3. На фактормножестве $K/_\cong$ примера 2.9.2 определим тернарные отношения $+$ и $\cdot$, сопоставляя с каждой парой классов $(A)_\cong$ и $(B)_\cong$ классы $(A+B)_\cong$ и $(A\cdot B)_\cong$ соответственно. Пусть f — однозначное отображение K в фактормножество $K/_\cong$, определяемое условием

$$f\colon\ A \mapsto (A)_\cong.$$

Является или нет f гомоморфным отображением системы $\langle K;\ +,\ \cdot\rangle$ на систему $\langle K/_\cong;\ +,\ \cdot\rangle$?

2.9.4. Пусть $\mathbf{A} \rightleftharpoons \langle A;\ +,\ \cdot,\ 0,\ 1\rangle$ — коммутативное кольцо с единицей и без делителей нуля. Обозначим через P множество всех пар $\langle a,\ b\rangle$ элементов A таких, что $b \neq 0$. Определим в P сложение $\oplus$, умножение $\odot$ и отношение эквивалентности $\sim$ следующим образом:

$$\langle a,\ b\rangle \oplus \langle a',\ b'\rangle \rightleftharpoons \langle ab' + a'b,\ bb'\rangle;$$

$$\langle a,\ b\rangle \odot \langle a',\ b'\rangle \rightleftharpoons \langle aa',\ bb'\rangle;$$

$$\langle a,\ b\rangle \sim \langle a',\ b'\rangle \Leftrightarrow ab' = a'b.$$

Доказать, что сложение и умножение — алгебраические операции на P, что отношение $\sim$ рефлексивно, симметрично, транзитивно и

монотонно относительно обеих операций. Пусть далее $\bar{P}$ — множество классов эквивалентности множества P и пусть $\alpha \rightleftharpoons \overline{\langle a, b\rangle}$ и $\alpha' \rightleftharpoons \overline{\langle a', b'\rangle}$ — классы множества $\bar{P}$ с представителями $\langle a, b\rangle$ и $\langle a', b'\rangle$ соответственно. Полагаем:

$$\alpha + \alpha' \rightleftharpoons \overline{\langle a, b\rangle \oplus \langle a', b'\rangle};$$

$$\alpha \cdot \alpha' \rightleftharpoons \overline{\langle a, b\rangle \odot \langle a', b'\rangle}.$$

Доказать, что $\mathbf{P} \rightleftharpoons \langle \bar{P};\ +,\ \cdot\rangle$ — поле. Пусть P_1 — подмножество $\bar{P}$, определяемое условием

$$\alpha \in P_1 \overset{\text{Df}}{\Leftrightarrow} \exists (a \in A) \quad \langle a, 1\rangle \in \alpha.$$

Доказать, что $\langle P_1;\ +,\ \cdot\rangle$ — подкольцо поля $\bar{\mathbf{P}}$, изоморфное кольцу $\langle A;\ +,\ \cdot\rangle$. Доказать, что любой элемент $\bar{P}$ есть частное двух элементов из P_1.

2.10. Расширения алгебраических систем

Определение 2.10.1. Пусть

$$\mathbf{A} \rightleftharpoons \langle A;\ \{\omega_\mu \mid \mu \in M\}\rangle$$

и

$$\mathbf{B} \rightleftharpoons \langle B;\ \{\theta_\mu \mid \mu \in M\}\rangle$$

какие-нибудь алгебраические системы. Систему **A** мы называем *расширением системы* **B**, если:

1) B — подмножество A;

2) $\forall (\mu \in M)$ отношения ω_μ и θ_μ одного ранга n_μ;

3) $\forall (\mu \in M)\, \forall (b_1, \ldots, b_{n_\mu} \in B)$,

$$\langle b_1, \ldots, b_{n_\mu}\rangle \in \theta_\mu \Leftrightarrow \langle b_1, \ldots, b_{n_\mu}\rangle \in \omega_\mu.$$

Другими словами, система **A** — расширение системы **B**, если B — подмножество A и для каждого μ из M отношение θ_μ индуцировано отношением ω_μ.

Примеры: 2.10.1*. Кольцо многочленов над кольцом **A** — расширение кольца **A**.

2.10.2. Кольцо рациональных чисел не является расширением аддитивной группы кольца целых чисел.

2.10.3. Рассмотрим алгебраические системы вопросов 2.6.14 и 2.6.16. Вторая не является расширением первой.

2.10.4. Любое кольцо — расширение своего подкольца (подтела, подполя).

2.10.5. Любая алгебра — расширение своей подалгебры.

Вопросы: **2.10.1.** Доказать, что любое коммутативное кольцо $\mathbf{A} \rightleftharpoons \langle A; +, \cdot, 0,1\rangle$ с единицей и без делителей нуля можно вложить в поле. Другими словами, доказать, что существует поле, подкольцом которого является кольцо $\langle A; +, \cdot, 0,1\rangle$.

Такое поле называют *полем отношений* кольца **A**. Таким образом, в частности, кольцо многочленов от одного неизвестного над полем **P** можно вложить в поле — в поле рациональных дробей (функций) от одного неизвестного. *Поле рациональных функций* над полем **P** от неизвестного x обозначают символом $\mathbf{P}(x)$.

2.10.2. Пусть выполнено условие теоремы 2.9.3. и система **A** — кольцо. Доказать, что система **B** — кольцо.

2.10.3. Пусть выполняются условия теоремы 2.9.3, система **A** — кольцо многочленов над полем **P**, $\varphi(x)$ — неприводимый над полем **P** многочлен, ω — отношение эквивалентности примера 2.9.4. Доказать, что система **B** — поле, которое содержит подполе, изоморфное полю **P**.

§ 3. АКСИОМАТИЧЕСКИЕ ТЕОРИИ

3.1. Аксиоматическая теория

Под *аксиоматической теорией* понимают систему из двух множеств высказываний T и W, одно из которых W содержит второе T. Множество W состоит из высказываний, которые имеют смысл в рамках данной теории, а множество T — из высказываний, которые рассматриваются в ней как истинные и доказуемые.

Множество T получается следующим образом. Выбирается некоторое множество T_0 высказываний данной теории. Таким образом $T_0 \subset W$. Все высказывания этого выбранного множества объявляются аксиомами. Всякое высказывание w множества W относят к множеству T и называют *теоремой* лишь в том случае, если существует конечная последовательность высказываний:

$$w_1, \ldots, w_k; \quad w_i \in W; \quad i = 1, \ldots, k; \quad k \geqslant 1 \qquad (1)$$

такая, что выполняются следующие условия:

1) каждое высказывание w_i этой последовательности — или аксиома, или может быть выведено путем применения логических правил вывода из предшествующих высказываний этой последовательности;

2) $w = w_k$.

В частности, каждая аксиома принадлежит множеству T, т. е. является теоремой. Последовательность (1) с указанными выше свойствами называется *доказательством* или *выводом высказывания* w.

Если при описании теории система логических правил вывода предполагается известной, то теорию называют *содержательной* или *неформальной*. Если используемая система логических правил вывода явным образом включается в теорию, то такая теория называется *формальной аксиоматической теорией*. Классическая теория групп может служить примером неформальной аксиоматической теории, исчисление высказываний — примером формальной аксиоматической теории.

3.2. Схема построения неформальной аксиоматической теории

При построении аксиоматической теории обычно исходят из некоторой достаточно развитой интуитивной теории и предполагают известной интуитивную систему классической логики. В принципе можно было бы основываться и на какой-нибудь другой системе логики, например на *конструктивной*. В последней, в отличие от классической, считают неприемлемым применение закона исключенного третьего к бесконечным множествам. Утверждение, что каждое натуральное число n либо обладает, либо не обладает некоторым свойством $P(n)$, истинно с классической точки зрения. Но с конструктивной точки зрения оно истинно лишь в том случае, если известен алгоритм, который позволяет для каждого числа n за конечное число шагов убедиться, выполняется или нет свойство $P(n)$. Принятие конструктивной точки зрения приводит к ограничениям не только на высказывания, но и на определения.

Первым шагом в построении аксиоматической теории является составление перечня основных объектов данной теории и выбор символов для их обозначения. Такими символами могут быть знаки или слова, а сами они называются *первичными символами* или *терминами*. Итак, на первом шаге построения аксиоматической теории составляется перечень S_0 первичных терминов данной теории.

Вторым шагом в построении аксиоматической теории является составление перечня основных свойств отобранных объектов — высказываний об основных объектах и запись их при помощи первичных символов. Эти свойства называются *аксиомами*. Таким образом, в результате второго шага составляется перечень T_0 аксиом данной теории.

После этого, следуя принципам принятой системы логики, выводят из аксиом теоремы и определяют на основе первичных терминов другие используемые в теории термины.

Легко видеть, что принадлежность определенного высказывания к множеству T связана с тем, на какой системе логики основывается данная теория. Аналогичное замечание можно сделать и относительно терминов, используемых в данной теории.

3.3. Интерпретация и модель аксиоматической теории

Предположим, что наряду с данной аксиоматической теорией мы имеем другую теорию, аксиоматическую или даже интуитивную, основанную на той же системе логики. Если нам с каждым первичным термином данной теории удалось сопоставить какой-нибудь объект второй теории и притом так, что: 1) каждому высказыванию об объектах данной теории соответствует некоторое высказывание

второй теории о ее объектах; 2) отрицаниям высказываний данной теории отвечают отрицания соответствующих высказываний второй теории,— то такую систему объектов второй теории называют *интерпретацией* данной теории.

Пример 3.3.1. Рассмотрим множество объектов примера 2.2.5 вместе с заданной на этом множестве бинарной операцией. Легко видеть, что эта совокупность объектов является интерпретацией аксиоматической теории групп.

Если в интерпретации I данной теории аксиомам теории соответствуют теоремы, то интерпретацию называют *моделью данной теории.*

Пример 3.3.2. Интерпретация примера 3.3.1 в силу вопроса 2.2.2 не является моделью аксиоматической теории групп.

Следует заметить, что в известном смысле интуитивная теория, из которой мы исходим при построении аксиоматической теории, сама является моделью данной аксиоматической теории.

Обычно при построении аксиоматической теории предполагают известной неформальную, или интуитивную, теорию множеств и первичным терминам теории сразу придают некоторое теоретико-множественное истолкование — как некоторое множество (или некоторые множества) и отношения, с ним (с ними) связанные. Поэтому в результате первого шага построения аксиоматической теории получают не только перечень первичных терминов, но и некоторую теоретико-множественную интерпретацию теории.

Это определяет множество высказываний W теории, составляющее предмет теории как множество высказываний об элементах некоторого множества и об отношениях в нем. Можно поэтому сказать, что первый шаг в построении теории — задание множества S_0 первичных терминов теории — определяет множество W высказываний теории. Второй шаг — выбор множества аксиом T_0 — определяет множество теорем теории.

Вопросы: 3.3.1. Пусть **A** — система с отношениями, являющаяся моделью некоторой аксиоматической теории. Показать, что всякая система **B**, изоморфная **A**, является моделью той же теории.

3.3.2. Пусть $\mathbf{A} \Leftrightarrows \langle A;\ \{\omega_\mu \mid \mu \in M\}\rangle$ — система с отношениями, являющаяся моделью некоторой теории. Пусть M' — подмножество M и $\langle B;\ \{\theta_\mu \mid \mu \in M'\}\rangle$ — система, изоморфная системе $\langle A;\ \{\omega_\mu \mid \mu \in M\}\rangle$. Доказать, что на множестве B можно так определить отношения $\{\theta_\mu \mid \mu \in M \setminus M'\}$, что система $\langle B;\ \{\theta_\mu \mid \mu \in M\}\rangle$ будет изоморфной системе **A**.

В заключение заметим, что при построении некоторых теорий, которым аксиоматическая теория натуральных чисел предшествует, не ограничиваются отношениями конечного ранга, но рассматривают и отношения счетного ранга (пункт 4.7).

3.4. Формулировка аксиоматической теории

Упорядоченную пару множеств $\langle S_0, T_0\rangle$ называют *формулировкой данной аксиоматической теории*. Мы уже упоминали, что в данной аксиоматической теории наряду с первичными неопределяемыми терминами могут рассматриваться и другие — определяемые термины. Обозначим через S_1 множество определяемых терминов теории. В таком случае $S \rightleftharpoons S_0 \cup S_1$ — множество всех терминов, рассматриваемых в данной теории. Через T_0 мы обозначили множество аксиом данной теории. Если через T_1 обозначить множество остальных, отличных от аксиом, доказуемых высказываний теории, то объединение T_0 и T_1 составит множество теорем данной теории.

Возможна ли другая формулировка данной теории? Пусть S_0' — какое-нибудь подмножество S и T_0' — какое-нибудь подмножество высказываний из T, выразимых в терминах S_0'. Пара $\langle S_0', T_0'\rangle$, очевидно, тогда и только тогда является формулировкой данной теории, если каждый термин из S_0 можно определить через термины из S_0', а каждое высказывание из T_0 можно вывести из высказываний множества T_0'.

Примером аксиоматической теории может служить теория групп. Эта теория допускает различные формулировки.

В теории групп иногда за первичные термины принимают некоторое множество G, бинарную операцию $\cdot$ на нем и некоторый элемент e этого множества, а аксиомы теории формулируют следующим образом:

G_{I}. $G \neq \varnothing \wedge \forall (a, b \in G) \quad \exists ! (p \in G) \quad a \cdot b = p$;
G_{II}. $\forall (a, b, c \in G) \quad (a \cdot b)\, c = a \cdot (b \cdot c)$;
G_{III}. $e \in G \wedge \forall (a \in G) \quad a \cdot e = a$;
G_{IV}. $\forall (a \in G) \exists (a' \in G) \quad a \cdot a' = e$.

В качестве теорем можно рассматривать, например, такие высказывания:

G_{V}. $\forall (a, b \in G) \quad \exists (x \in G) \quad ax = b$;
G_{VI}. $\forall (a, b \in G) \quad \exists (y \in G) \quad ya = b$.

Таким образом, перечень T_0 аксиом состоит из теорем G_{I}, G_{II}, G_{III}, G_{IV}. Итак, мы имеем следующую формулировку теории групп:

$$\langle \{G, \cdot, e\}; \quad \{G_{\mathrm{I}}, G_{\mathrm{II}}, G_{\mathrm{IV}}\}\rangle.$$

В то же время известно (определение 2.5.2), что теория групп допускает и вторую формулировку:

$$\langle \{G, \cdot\}; \quad \{G_{\mathrm{I}}, G_{\mathrm{II}}, G_{\mathrm{V}}, G_{\mathrm{VI}}\}\rangle.$$

Вопрос 3.4.1. Указать какую-нибудь интерпретацию теории групп и выяснить, является ли она моделью этой теории.

В дальнейшем, приводя формулировки известных теорий, мы часто будем ограничиваться указанием множества S_0 — первичных

терминов; множество T_0 — аксиом — при этом будет подразумеваться. Так, например, слова «пусть система $\langle G; \cdot, e\rangle$ — группа» означают, что мы пользуемся первой формулировкой теории групп, а слова «система $\langle G; \cdot\rangle$ — группа» означают, что мы пользуемся второй формулировкой этой теории. Это замечание относится к различным формулировкам теории колец, полей и т. д.

Вопрос 3.4.2. Указать различные формулировки теории полей.

При построении конкретной содержательной аксиоматической теории из соображений краткости аксиомы иногда формулируют как высказывания о терминах данной теории, не обязательно первичных, а в качестве терминов пользуются терминами какой-нибудь из предшествующих теорий.

3.5. Свойства аксиоматических теорий

Аксиоматическую теорию называют *непротиворечивой,* если для любого высказывания w теории хотя бы одно из высказываний w или $\overline{w}$ не является теоремой. Противоречивую теорию не имеет смысла рассматривать. Как установить непротиворечивость теории?

Данная теория непротиворечива, если для нее удалось найти модель из объектов другой, но заведомо непротиворечивой теории. В самом деле, поскольку в обеих теориях мы пользуемся одной логикой, то каждому доказуемому высказыванию теории отвечает доказуемое высказывание модели, т. е. второй теории. Но противоположным высказываниям отвечают противоположные высказывания модели. Поэтому из противоречивости данной теории прямо следует противоречивость модели, а значит, и второй теории.

Это рассуждение обосновывает непротиворечивость одной теории относительно другой. Однако в случае, если моделью служит конечное множество, отсутствие противоречивости в модели иногда можно проверить непосредственно. Это позволяет решить вопрос о непротиворечивости данной теории вне зависимости от непротиворечивости каких-либо других теорий. Так, теория групп непротиворечива, поскольку ее моделью служит одноэлементное множество $\{e\}$, в котором $ee = e$.

Метод моделей, который позволяет установить непротиворечивость аксиоматической теории, да и то часто только относительную, является косвенным. Но прямой путь установления непротиворечивости неформальных аксиоматических теорий закрыт. Это связано с тем, что в таких теориях нет точного понятия доказательства. И только для формальных аксиоматических теорий в некоторых случаях удается найти прямое доказательство их непротиворечивости.

Пример 3.5.1. Исчисление высказываний непротиворечиво.

Аксиоматическую теорию называют *категоричной,* если две любые ее модели изоморфны.

Вопрос 3.5.1. Категорична или нет аксиоматическая теория групп?

Аксиоматическую теорию называют *полной,* если для любого высказывания w этой теории хотя бы одно из высказываний w или $\neg w$ является теоремой.

У нас нет средств для решения проблемы полноты содержательной аксиоматической теории. Да таких средств и не существует, поскольку в содержательной аксиоматической теории нет точного понятия доказательства — не указаны явным образом все правила вывода.

Следующее свойство характеризует формулировку теории.

Пусть $\langle S_0, T_0\rangle$ — какая-нибудь формулировка аксиоматической теории. Аксиому $A_1 \in T_0$ называют *независимой* от остальных аксиом множества T_0, если ее нельзя из них вывести. Другими словами, аксиома A_1 независима от остальных, если пара $\langle S_0, T_0 \setminus \{A_1\}\rangle$ не является другой формулировкой данной теории.

Наоборот, если пара $\langle S_0, T_0 \setminus \{A_1\}\rangle$ является другой формулировкой данной теории, то аксиома A_1 зависит от остальных аксиом данной теории.

Предположим, что данная теория непротиворечива. Как решить вопрос о независимости аксиомы A_1 этой теории?

Если непротиворечива теория, формулировкой которой служит пара $\langle S_0, T_0'\rangle$, где $T_0' \rightleftharpoons (T_0 \setminus \{A_1\}) \cup \{\neg A_1\}$, то аксиома A_1, очевидно, не зависит от остальных аксиом данной теории.

Вопрос о независимости аксиомы A_1 сведен к вопросу о непротиворечивости теории с формулировкой $\langle S_0, T_0'\rangle$. А этот вопрос обычно решают, подбирая для второй теории модель из объектов данной теории.

Пример 3.5.2. Рассмотрим аксиоматическую теорию, первичными терминами которой являются:

а) A — множество;

б) $\cdot$ — тернарное отношение в A, а аксиомами следующие высказывания:

A_{I}. $A \neq \varnothing \wedge \forall (a, b \in A) \quad a \cdot b \neq \varnothing \Rightarrow \exists ! (x \in A) \quad x \in a \cdot b;$

A_{II}. $\forall (a, b \in A) \quad \exists (x \in A) \quad b \in x \cdot a;$

A_{III}. $\forall (a, b \in A) \quad \exists (y \in A) \quad b \in a \cdot y;$

A_{IV}. $\forall (a, b, c \in A) \quad a \cdot (b \cdot c) \neq \varnothing \wedge (a \cdot b) \cdot c \neq \varnothing \Rightarrow$
$\Rightarrow a \cdot (b \cdot c) = (a \cdot b) \cdot c.$

Убедимся в *независимости аксиом* данной теории. Для этой цели достаточно указать четыре модели. На каждой из таких моделей одна аксиома не выполняется, а остальные выполняются.

M_1 — множество, состоящее из всех целых чисел, в котором трехчленное отношение $+$ определяется условием

$$\forall (a, b \in M_1) \quad a + b \rightleftharpoons \{x | x \geqslant a + b\}.$$

Легко видеть, что на системе $\langle M_1; +\rangle$ выполняются все аксиомы, кроме первой.

M_2 — множество из двух элементов p и q, на котором бинарная операция $\cdot$ задается таблицей

$\cdot$	p	q
p	p	q
q	q	q

Легко проверить, что все аксиомы, кроме второй, на этой модели выполняются. Построение модели M_3 выполняется аналогично.

M_4 — множество из трех элементов p, q, r с одной бинарной операцией $\cdot$, определенной таблицей

$\cdot$	p	q	r
p	q	p	r
q	r	q	p
r	p	r	q

На этой модели выполняются все аксиомы, кроме последней, так как

$$(p \cdot q) \cdot r \neq p \cdot (q \cdot r).$$

Вопрос 3.5.2*. Доказать, что $\langle \{A;\ \cdot\};\ \{A_I, A_{II}, A_{III}, A_{IV}\} \rangle$ является формулировкой аксиоматической теории группы.

3.6. Формальные аксиоматические теории

Формальные аксиоматические теории рассматривают в связи с задачей сделать предметом изучения саму математическую теорию. Такие теории представляют для нас интерес в связи с тем, что они могут служить моделью данной математической теории или хотя бы ее существенного фрагмента.

Естественно, что при построении формальной теории стремятся разграничить язык и логические средства формальной теории от языка и логических средств, на котором описывается и которыми пользуются при изучении этой теории. Теорию, предметом которой является данная формальная теория, и язык, на котором она описывается, называют соответственно *метатеорией* и *метаязыком* данной теории. К логическим средствам метатеории предъявляют требование надежности, что обычно отождествляют с требованием эффективности используемых при описании и изучении теории средств.

Чтобы удовлетворить условиям, предъявляемым к теории и ее метатеории, чаще всего при построении формальной теории исходят из конкретных знаков — исходных символов, а саму теорию представляют как систему весьма простых манипуляций над конечными последовательностями таких символов, называемых *выражениями*.

Предполагается, что:

а) никакая часть символа теории не является объектом теории;

б) любое выражение однозначно представляется в виде последовательности символов теории;

в) для любых двух выражений можно определить, равны они или нет;

г) в любое выражение вместо любой последовательности рядом стоящих символов можно подставить какое угодно выражение.

В классе всех выражений формальной теории выделяют класс формул. Некоторые формулы объявляют аксиомами. Наконец, во множестве формул определяют множество отношений — правил вывода. Определения формул, задание аксиом и правил вывода должны быть эффективными.

Под *доказательством* формулы w понимают любую конечную *последовательность* формул теории:

$$w_1, \ldots, w_k; \quad k \geqslant 1, \tag{1}$$

удовлетворяющую следующим условиям:

а) каждая формула последовательности (1) является либо аксиомой, либо получается путем применения одного из правил вывода к каким-нибудь предшествующим формулам той же последовательности;

б) $w = w_k$.

Под *теоремой* теории понимается любая формула теории, для которой есть доказательство. Не предполагается, что существует эффективная процедура, позволяющая установить, теорема или нет данная формула теории.

Формальную теорию называют абсолютно непротиворечивой, если не все ее формулы — теоремы. В случае, если среди символов теории имеется символ, интерпретируемый как отрицание, для теории можно пользоваться и обычным определением непротиворечивости.

Мы дадим описание простейшей формальной теории — *исчисления высказываний*. Предварительно заметим, что нетрудно указать способ эффективного задания счетной последовательности символов:

$$A_{\mathrm{I}}, A_{\mathrm{II}}, A_{\mathrm{III}}, A_{\mathrm{IIII}}, A_{\mathrm{IIIII}}, \ldots .$$

Поэтому при описании формальных теорий часто исходят из счетной последовательности символов и не останавливаются на выяснении способа образования этой последовательности.

Символы:

а) переменные высказывания: A, B, C, ...;

б) логические связки: $\neg$, $\rightarrow$;

в) вспомогательные: (,) (скобки).

Формулы:

а) переменное высказывание — формула;

б) если U и V — формулы (U и V — символы метатеории), то $\neg (U)$, $(U) \rightarrow (V)$ — формулы.

Примечание. В целях краткости записи формул вспомогательные символы иногда опускают.

Аксиомы.

Если U, V, W — формулы, то следующие формулы — аксиомы:

1) $U \to (V \to U)$;
2) $(U \to (V \to W)) \to ((U \to V) \to (U \to W))$;
3) $(\neg V \to \neg U) \to ((\neg V \to U) \to V)$.

Правило вывода (правило отделения):

$$\frac{U,\ U \to V}{V}.$$

Мы не будем заниматься доказательством каких-либо теорем этой формальной теории, убедимся лишь в ее непротиворечивости.

На множестве всех формул данной теории определим функцию φ со значениями 0 и 1 следующим образом:

а) если A — переменное высказывание, то в качестве $\varphi(A)$ выбираем произвольно 0 или 1;

б) если для формул U и V значения функции φ определены, то полагаем, что:

$$\varphi(\neg U) \rightleftharpoons 1 - \varphi(U); \quad \varphi(U \to V) \rightleftharpoons (1 - \varphi(U)) \cdot \varphi(V).$$

Непосредственно проверяется, что $\varphi(U) = 0$ для любой аксиомы, а затем, используя правило вывода, и для любой теоремы U. С другой стороны, если $\varphi(U) = 0$, то $\varphi(\neg U) = 1$. Поэтому не всякая формула данного формального исчисления — теорема. Отсюда можно заключить об абсолютной непротиворечивости исчисления высказываний.

Что касается проблемы полноты формальных теорий, то нужно заметить следующее. Не всякую формулу теории рассматривают как ее высказывание, т. е. как формулу, в отношении которой вопрос о ее доказуемости или недоказуемости имеет смысл. Не уточняя сказанного здесь относительно любых формальных теорий, отметим, что в рассмотренной нами теории за высказывание принимают лишь такую формулу U, для которой значение введенной выше функции φ не зависит от значения φ для всех входящих в U переменных высказываний. Оказывается, что если U такая формула, то либо U, либо ее отрицание доказуемы. В связи с этим говорят, что исчисление высказываний полно.

В этой книге не рассматриваются другие формальные аксиоматические теории. Вопрос о формализации данной содержательной аксиоматической теории и тем более вопрос о формализации данной содержательной теории в рамках использования определенных логических средств далеко не прост.

§ 4. СОДЕРЖАТЕЛЬНАЯ АКСИОМАТИЧЕСКАЯ ТЕОРИЯ НАТУРАЛЬНЫХ ЧИСЕЛ

4.1. Первичные термины

N — множество натуральных чисел, называемое в дальнейшем также *натуральным рядом*;

1 — *единица* — элемент множества N;

$+$ — *сумма* — тернарное отношение в N;

$\cdot$ — *произведение* — тернарное отношение в N.

Итак, в качестве первичных терминов в нашей теории выступают множество N, одно унарное отношение («быть единицей») и два тернарных отношения («быть суммой», «быть произведением»).

Обозначения.

1) Если $\exists!\ (c \in A)$, то мы пишем $A = c$,

2) Для любой пары элементов a и b из N символом

$$a + b$$

мы обозначаем множество $\{c \mid \langle a, b, c\rangle \in +\}$.

3) Для любой пары подмножеств A и B множества N символом

$$A + B$$

мы обозначаем множество $\{c \mid c \in (a + b),\ a \in A,\ b \in B\}$.

4) Если $a \in N$, $B \subset N$, то символ

$$a + B$$

означает то же, что символ $\{a\} + B$.

Аналогичным образом определяется смысл выражений $a \cdot b$, $A \cdot B$, $a \cdot B$.

Легко видеть, что, каковы бы ни были подмножества A, B, C, D множества N,

$$A \subset C \wedge B \subset D \Rightarrow A + B \subset C + D \wedge A \cdot B \subset C \cdot D.$$

Вместе с тем следует заметить, что, пока не названы аксиомы нашей теории, мы не можем сказать, пусты или нет множества $A + B$ и $A \cdot B$, каковы бы ни были A и B.

Упражнение 4.1.1. Найти $\{1, 2\} + \{1, 3, 4\}$.

4.2. Аксиомы

N_{I}. $1 \in N \wedge \forall (a, b \in N) \quad 1 \notin a + b$.

Иначе говоря, N не пусто, так как содержит единицу, и единица не есть сумма каких-либо натуральных чисел.

N_{II}. $\forall (a \in N) \quad \exists! (c \in N) \quad c \in a + 1$.

Другими словами, для каждого a из N $a + 1 \neq \varnothing$ и состоит из одного элемента.

N_{III}. $\forall (a, b \in N) \quad (a + 1) \cap (b + 1) \neq \varnothing \Rightarrow a = b$.

Но в силу аксиомы N_{II}

$$(a + 1) \cap (b + 1) \neq \varnothing \Rightarrow a + 1 = b + 1,$$

поэтому аксиому N_{III} можно сформулировать и так:

$$\forall (a, b \in N) \quad a + 1 = b + 1 \Rightarrow a = b.$$

N_{IV}. $\forall (a, b \in N) \quad a + b \neq \varnothing \Rightarrow a + (b + 1) \neq \neq \varnothing \wedge a + (b + 1) \subset (a + b) + 1$

(слабая форма ассоциативности).

N_{V}. $\forall (a \in N) \quad a \cdot 1 = a$.

N_{VI}. $\forall (a, b \in N) \quad a \cdot b + a \neq \varnothing \Rightarrow a \cdot (b + 1) \neq \neq \varnothing \wedge a \cdot (b + 1) \subset a \cdot b + a$

(слабая форма дистрибутивности).

N_{VII} (*аксиома индукции*). Пусть M — любое подмножество N, удовлетворяющее условиям:

а) $1 \in M$;
б) $\forall (a \in N) \quad a \in M \Rightarrow (a + 1) \subset M$.

Тогда $N \subset M$, т. е. $M = N$.

Вопрос 4.2.1. Пусть M — любое множество, не обязательно состоящее только из натуральных чисел. Доказать, что M содержит все натуральные числа, если удовлетворяет следующим условиям:

а) $1 \in M$;
б) $\forall (a \in N) \quad a \in M \Rightarrow a + 1 \in M$.

4.3. Свойства сложения

Теорема 4.3.1. $\forall (a, b \in N) \quad \exists ! (c \in N)\, c \in a + b$.

Доказательство. Фиксируем натуральное число a (любой элемент N). Обозначим через M_a подмножество N вида

$$M_a \rightleftharpoons \{b | \exists ! (c \in N) \quad c \in a + b\}.$$

Имеем:

а) $1 \in M_a$ по аксиоме N_{II};

б) из $b \in M_a$ по аксиоме N_{IV} следует, что $a + (b + 1) \neq \varnothing$ и $a + (b + 1) \subset (a + b) + 1$. Из аксиомы N_{II} и предположения $b \in M_a$ следует, что $(a + b) + 1$ состоит из одного элемента. Поэтому

$$a + (b + 1) = (a + b) + 1;$$

другими словами, $b + 1 \in M_a$.

По аксиоме N_{VII} $M_a = N$.

Итак, для каждого a и любого b $a + b$ не пусто и состоит из одного элемента, т. е. сложение — алгебраическая операция на N.

Следовательно, для любых натуральных чисел a и b существует и только одно натуральное число c с условием, что $c \in a + b$. В дальнейшем символом $a + b$ мы обозначаем этот элемент.

Из доказанной теоремы и аксиомы N_{IV} следует, что

$$\forall (a, b \in N) \quad a + (b + 1) = (a + b) + 1. \tag{4.3.1}$$

Теорема 4.3.2. $\forall$ $(a, b, c \in N)$

$$(a + b) + c = a + (b + c).$$

Доказательство. Фиксируем натуральные числа a и b и обозначим через $M_{a,b}$ подмножество N вида

$$M_{a,b} \rightleftharpoons \{c \mid (a + b) + c = a + (b + c)\}.$$

Имеем:

а) $1 \in M_{a,b}$ в силу (4.3.1);

б) если $c \in M_{a,b}$, то получим в силу (4.3.1)

$$(a + b) + (c + 1) = [(a + b) + c] + 1 = [a + (b + c)] + 1 =$$
$$= a + [(b + c) + 1] = a + [b + (c + 1)].$$

Таким образом, $c + 1 \in M_{a,b}$ и по аксиоме N_{VII}

$$M_{a,b} = N.$$

Теорема 4.3.3. $\forall$ $(a \in N)$

$$a + 1 = 1 + a.$$

Доказательство. Обозначим через M подмножество N с условием

$$M \rightleftharpoons \{a \mid a + 1 = 1 + a\}.$$

Имеем:

а) $1 \in M$, так как $1 + 1 = 1 + 1$;

б) если $a \in M$, то в силу теоремы 4.3.2

$$(a + 1) + 1 = (1 + a) + 1 = 1 + (a + 1).$$

Таким образом, $a + 1 \in M$ и $M = N$ по аксиоме N_{VII}.

Теорема 4.3.4. $\forall$ $(a, b \in N)$

$$a + b = b + a.$$

Доказательство. Фиксируем натуральное число a и через M_a обозначим подмножество N с условием

$$M_a \rightleftharpoons \{b \mid a + b = b + a\}.$$

Имеем:

а) $1 \in M_a$ по доказанному;

б) если $b \in M_a$, то по теоремам 4.3.2 и 4.3.3

$$a + (b + 1) = (a + b) + 1 = 1 + (a + b) = 1 + (b + a) = \\ = (1 + b) + a = (b + 1) + a.$$

Таким образом,

$$b + 1 \in M_a$$

и $M_a = N$ по аксиоме N_{VII}.

Вопрос 4.3.1. Показать, что

$$\forall (a, b, c \in N) \quad a + c = b + c \Rightarrow a = b.$$

4.4. Свойства умножения

Теорема 4.4.1. $\forall (a, b \in N)\ \exists!\ (p \in N)\ p \in a \cdot b$.

Следует из аксиом N_V, N_{VI} и теоремы 4.3.1.

Из доказанной теоремы вытекает, что множество $a \cdot b$ не пусто и состоит из одного элемента. Естественно в дальнейшем символом $a \cdot b$ обозначать указанный элемент.

Из теоремы 4.4.1 и аксиомы N_{VI} следует, что:

1) $\forall (a, b \in N) \quad a \cdot (b + 1) = a \cdot b + a$;

2) $\forall (a, b, c \in N) \quad (a + b) \cdot (c + 1) = (a + b) \cdot c + (a + b)$. (4.4.1).

Теорема 4.4.2. $\forall (a, b, c \in N)$

$$(a + b)\, c = ac + bc.$$

Доказательство. Фиксируем натуральные числа a, b и обозначим через $M_{a,b}$ подмножество N вида

$$M_{a,b} \rightleftharpoons \{c \mid (a + b)\, c = ac + bc\}.$$

Далее, пользуясь аксиомами N_V, N_{VI}, N_{VII} и доказанными теоремами, получим, что

$$M_{a,b} = N.$$

Теорема 4.4.3. $\forall (a, b \in N)$

$$a \cdot b = b \cdot a.$$

Легко следует из равенств:

$$1 \cdot (a + 1) = 1 \cdot a + 1;$$

$$a \cdot (b + 1) = a \cdot b + a.$$

Теорема 4.4.4. $\forall (a, b, c \in N)$

$$c\,(a + b) = ca + cb.$$

Теорема 4.4.5. $\forall (a, b, c \in N)$

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

Легко следует из равенства

$$(ab)(c+1) = (ab)c + ab = a(bc) + ab = \\ = a(bc+b) = a[b(c+1)].$$

Таким образом, сложение и умножение — алгебраические операции на N, а система $\langle N; +, \cdot \rangle$ — коммутативное полукольцо.

Обозначения:

$$2 \rightleftharpoons 1+1; \quad 3 \rightleftharpoons 2+1; \quad 4 \rightleftharpoons 3+1; \quad 5 \rightleftharpoons 4+1; \quad 6 \rightleftharpoons 5+1;$$
$$7 \rightleftharpoons 6+1; \quad 8 \rightleftharpoons 7+1; \quad 9 \rightleftharpoons 8+1.$$

Вопрос 4.4.1. Доказать, что:

1) $2+2=4$;
2) $2 \cdot 2 = 4$;
3) $2 \cdot 3 = 6$.

4.5. Порядок во множестве натуральных чисел

Теорема 4.5.1. $\forall\, (a \in N)\ \ a \neq 1 \Rightarrow \exists\, (n \in N)\ \ a = 1 + n$.

Доказательство. Обозначим через M' и M'' подмножества N вида

$$M' \rightleftharpoons \{1\},$$
$$M'' \rightleftharpoons \{a \mid \exists\, (n \in N)\ \ a = 1+n\}$$

и докажем, что

$$M' \cup M'' = N.$$

Имеем:

а) $1 \in M' \cup M''$, так как $1 \in M'$;
б) если $a \in N$, то $a+1 \in M' \cup M''$, так как $a+1 = 1+a \in M''$.

Этот вывод можно сделать, даже не воспользовавшись предположением, что $a \in M' \cup M''$.

Теорема 4.5.2. $\forall\, (a, b \in N)\ \ a \neq a+b$.

Доказательство. Фиксируем натуральное число b и через M_b обозначаем подмножество N вида

$$M_b \rightleftharpoons \{a \mid a \neq a+b\}.$$

Имеем:

а) $1 \in M_b$ по аксиоме N_1;
б) докажем, что из $a \in M_b \Rightarrow (a+1) \in M_b$.

Предположим, что

$$a+1 = (a+1)+b.$$

Тогда

$$a+1 = (a+b)+1$$

и по аксиоме N_{III}

$$a = a+b,$$

т. е.

$$a \notin M_b.$$

Теорема 4.5.3. Для любой пары натуральных чисел a, b имеет место и только одно из следующих утверждений:

а) $a = b$;
б) $\exists (n \in N) \quad b = a + n$;
в) $\exists (k \in N) \quad a = b + k$.

Доказательство. Несовместность любых двух утверждений следует из теоремы 4.5.2.

Фиксируем натуральное число a и через M'_a, M''_a, M'''_a обозначаем подмножества N вида:

$$M'_a \leftrightharpoons \{b \mid a = b\};$$

$$M''_a \leftrightharpoons \{b \mid \exists (n \in N) \quad b = a + n\};$$

$$M'''_a \leftrightharpoons \{b \mid \exists (k \in N) \quad a = b + k\}.$$

Полагаем

$$M \leftrightharpoons M'_a \cup M''_a \cup M'''_a.$$

Докажем, что $M = N$.

Имеем: а) $1 \in M$, так как $1 \in M'_a$, если $a = 1$ и $1 \in M'''_a$ по теореме 4.5.1, если $a \neq 1$;

б) докажем, что из $b \in M$ следует $b + 1 \in M$. Если $b \in M'_a$, то $b = a$ и $b + 1 = a + 1$; поэтому $b + 1 \in M''_a$.

Если $b \in M''_a$, то $b = a + n$ для некоторого $n \in N$ и $b + 1 = a + (n + 1)$; поэтому $b + 1 \in M''_a$.

Если $b \in M'''_a$, то $a = b + k$ для некоторого $k \in N$; поэтому $b + 1 \in M'_a$ или $b + 1 \in M'''_a$ (в зависимости от того $k = 1$ или $k \neq 1$).

Определение 4.5.1. Для натуральных чисел a и b говорят «*a больше b*» или «*b меньше a*» и употребляют запись

$$a > b \text{ или } b < a,$$

если и только если $\exists (n \in N)\ a = b + n$. Для натуральных чисел a и b говорят «*a больше или равно b*» или «*b меньше или равно a*» и употребляют запись

$$a \geqslant b \text{ или } b \leqslant a,$$

если и только если $\neg\, b > a$.

В случае, если $a > b \wedge b > c$, употребляют для краткости запись

$$a > b > c.$$

Аналогичное соглашение устанавливается для других записей подобного типа.

Определение 4.5.2. *Отрезком* натурального ряда с концами a и b для любых натуральных чисел a и b называют множество

$$\{x \mid x \in N \wedge a \leqslant x \leqslant b\}$$

и обозначают символом $[a, b]$; в частности, при $a = 1$ отрезок $[1, b]$ называют *начальным отрезком* натурального ряда.

Определение 4.5.3. Натуральное число n называют *наименьшим (наибольшим)* элементом множества $M \subset N$, если

$$n \in M$$

и

$$\forall (x \in M) \quad x \geqslant n$$

(соответственно $\forall\ (x \in M)\ x \leqslant n$).

Определение 4.5.4. Множество $M \subset N$ называют *ограниченным*, если

$$\exists (n \in N) \quad M \subset [1, n].$$

Вопросы: 4.5.1. Показать, что:

а) $3 > 2$;
б) $3 \geqslant 2$;
в) $3 \geqslant 3$.

4.5.2. Показать, что $[1; 1] = \{1\}$.

4.6. Свойства неравенств

Теорема 4.6.1. (связность):

$$\forall (a, b \in N) \quad a \neq b \Rightarrow a > b \vee b > a.$$

Теорема 4.6.2. (антирефлексивность):

$$\forall (a \in N) \ \neg\, a > a.$$

Теорема 4.6.3. (асимметричность):

$$\forall (a, b \in N) \quad a > b \Rightarrow \neg\, b > a.$$

Теорема 4.6.4. (транзитивность):

$$\forall (a, b, c \in N) \quad a > b \wedge b > c \Rightarrow a > c.$$

Теорема 4.6.5. (монотонность относительно сложения):

$$\forall (a, b, c \in N) \quad a > b \Rightarrow a + c > b + c.$$

Теорема 4.6.6. (любое натуральное число — положительно):

$$\forall (a, b \in N) \quad a + b > a.$$

Теорема 4.6.7. (монотонность относительно умножения):

$$\forall (a, b, c \in N) \quad a > b \Rightarrow ac > bc.$$

Все эти теоремы легко выводятся из теорем 4.5.2 и 4.5.3, а также из свойств сложения и умножения.

Легко доказывается и следующая теорема.

Теорема 4.6.8. Бинарное отношение $\geqslant$ во множестве натуральных чисел удовлетворяет следующим условиям:

1) $\forall (a \in N) \quad a \geqslant a$;
2) $\forall (a, b, c \in N) \quad a \geqslant b \wedge b \geqslant c \Rightarrow a \geqslant c$;

3) $\forall (a, b \in N) \quad a \geqslant b \wedge b \geqslant a \Rightarrow a = b$;
4) $\forall (a, b \in N) \quad \neg a > b \Rightarrow b \geqslant a$;
5) $\forall (a, b, c \in N) \quad a \geqslant b \Rightarrow a + c \geqslant b + c$;
6) $\forall (a, b, c \in N) \quad a \geqslant b \Rightarrow a \cdot c \geqslant b \cdot c$.

Вопросы: 4.6.1. Доказать:

$$\forall (a, b, c \in N) \quad a + c = b + c \Leftrightarrow a = b.$$

4.6.2. Доказать:

$$\forall (a, b, c \in N) \quad a + c > b + c \Leftrightarrow a > b.$$

4.6.3. Доказать:

$$\forall (a, b, c \in N) \quad a \cdot c = b \cdot c \Leftrightarrow a = b.$$

4.6.4. Доказать:

$$\forall (a, b, c \in N) \quad a \cdot c > b \cdot c \Leftrightarrow a > b.$$

4.6.5. Доказать:

$$\forall (a \in N) \quad 1 \leqslant a.$$

4.6.6. Доказать:

$$\forall (a, b \in N) \quad a \leqslant ab.$$

4.6.7. Доказать:

$$\forall (a, b \in N) \quad \exists (c \in N) \quad b \cdot c > a \text{ (теорема Архимеда).}$$

4.6.8. Доказать:

1) $\forall (a, b \in N) \quad a + 1 \geqslant b \wedge b > a \Rightarrow b = a + 1$;
2) $\forall (a, b \in N) \quad a + 1 > b \wedge b \geqslant a \Rightarrow b = a$.

4.6.9. Доказать:

$$\forall (n \in N) \quad [1, n + 1] = [1, n] \cup \{n + 1\}.$$

4.6.10. Доказать, что разность натуральных чисел a и b имеет смысл тогда и только тогда, если $a > b$.

4.6.11. Доказать, что если частное натуральных чисел a и b имеет смысл, то $a \geqslant b$.

4.6.12. Доказать, что $\neg (2 \mid 1)$, т. е. 2 не делит 1.

4.6.13. Доказать, что

$$\forall (n \in N) \quad n \neq 1 \Rightarrow \exists (x \in N) \quad n = 2x \vee n = 2x + 1.$$

4.6.14. Доказать, что

$$\forall (a, b \in N) \quad 2a \neq 2b + 1.$$

4.6.15. Доказать, что

$$\forall (a, b \in N) \neg (2 \mid (2a + 1) \cdot (2b + 1)).$$

4.6.16. Доказать, что

$$\forall (a, b \in N) \quad a^2 \neq 2b^2.$$

4.6.17. Доказать, что

$$\forall (a, b, n \in N) \quad n \neq 1 \Rightarrow a^n \neq 2b^n.$$

4.6.18. Доказать, что для любых натуральных чисел a и b отрезок $[a, b]$ пуст тогда и только тогда, если $a > b$.

4.6.19*. Пусть на множестве N определено бинарное отношение $>$ связное, антирефлексивное, антисимметричное, транзитивное, монотонное относительно сложения, и пусть $2 > 1$. Доказать, что

$$\forall (a,\ b \in N)\quad a > b \Leftrightarrow \exists (x \in N)\quad a = b + x.$$

4.6.20*. Показать, что:

а) отношение $>$ на множестве натуральных чисел однозначно определяется следующими условиями:

1) $\forall (a,\ b \in N)\quad a > b \Rightarrow a \neq b$;

2) $\forall (a,\ b \in N)\quad a > b + 1 \Rightarrow a > b$;

3) $\forall (a \in N)\quad a + 1 > a \Rightarrow (a + 1) + 1 > a + 1$;

4) $1 + 1 > 1$;

б) ни одно из четырех названных выше условий не является следствием остальных.

Теорема 4.6.9. Всякое непустое и ограниченное множество натуральных чисел имеет наибольший элемент.

Легко выводится из соотношения

$$A \subset [1,\ n + 1] \Rightarrow A \subset [1,\ n] \vee n + 1 \in A.$$

Теорема 4.6.10. Всякое непустое множество натуральных чисел имеет наименьший элемент.

Доказательство. Пусть $A \subset N$ и $A \neq \varnothing$; полагаем

$$B \Leftrightarrows \{x \mid x \in N \wedge \forall (a \in A)\ x \leqslant a\}.$$

Так как $1 \in B$, то $B \neq \varnothing$. Пусть b — наибольший элемент множества B. Тогда $b + 1 \notin B$, и, следовательно, $b \in A$. Но $b \in B$; поэтому A не содержит элементов, меньших b.

Вопросы: 4.6.21. Пусть M —подмножество N, удовлетворяющее условию

$$\forall (a \in N)\quad (\forall (x \in N)\,(x < a \Rightarrow x \in M)) \Rightarrow a \in M.$$

Доказать, что $M = N$.

4.6.22. Пусть $M \subset N$ и удовлетворяет условиям:

1) $1 \in M$;

2) $\forall (n \in N)\, n \in M \Rightarrow 2n \in M$;

3) $\forall (n \in M)\, \forall (x \in N)\, x < n \Rightarrow x \in M$.

Показать, что $M = N$.

4.7. Конечные множества

Определение 4.7.1. Множество называют *конечным,* если оно равномощно какому-либо отрезку натурального ряда, и *бесконечным* в противном случае.

Теорема 4.7.1. $\forall\ (a, b, c \in N)\ [a + c, b + c] \cong [a, b]$.

Доказательство. Можно предположить, что $b = a + n$ для некоторого натурального n. Пусть $a + n + c \geqslant x \geqslant a + c$, тогда

$$\exists!\ (y \in N)\ x = y + c \wedge a + n \geqslant y \geqslant a.$$

Полагаем $\varphi\ (x) \rightleftharpoons y$.

Соответствие φ — взаимно-однозначное отображение отрезка $[a + c, b + c]$ на отрезок $[a, b]$.

Из доказанной теоремы следует, что любое конечное множество или пусто, или равномощно начальному отрезку натурального ряда.

Теорема 4.7.2. Конечное множество A не равномощно любой своей правильной части.

Доказательство. Теорема легко сводится к случаю, когда A — отрезок натурального ряда. Если $A \rightleftharpoons \varnothing$, то теорема верна, так как пустое множество не имеет правильных частей.

В силу теоремы 4.7.1 мы можем далее предполагать, что A — начальный отрезок натурального ряда. Для каждого натурального n полагаем

$$A_n \rightleftharpoons [1,\ n].$$

Через M обозначим подмножество N вида

$$M \rightleftharpoons \{n | \forall\ (B \subset A_n)\ B \cong A_n \Rightarrow B = A_n\};$$

другими словами, к M отнесем n в том случае, если A_n не равномощно своей правильной части. Имеем:

а) $1 \in M$, так как $[1, 1]$ не имеет правильных частей, отличных от $\varnothing$;

б) покажем, что $n \in M \Rightarrow n + 1 \in M$. Предположим, что $B \subset [1, n + 1]$ и $B \cong [1, n + 1]$. Если $n + 1 \in B$, то в силу вопросов 2.3.7 и 4.6.9

$$B \setminus \{n + 1\} \cong [1,\ n].$$

А так как

$$B \setminus \{n + 1\} \subset [1,\ n],$$

то

$$B \setminus \{n + 1\} = [1,\ n]$$

и

$$B = [1,\ n + 1].$$

Пусть теперь $B \sim [1, n + 1]$, но $n + 1 \notin B$. Так как B не пусто, то

$$\exists\ (b \in N)\quad b \in B \wedge b \in [1, n].$$

В силу вопроса 2.3.7

$$B \setminus \{b\} \cong [1,\ n].$$

Вместе с тем $B \setminus \{b\}$ — правильная часть $[1, n]$, что противоречит предположению $(n \in M)$.

Теорема 4.7.3. Множество N бесконечно.

Доказательство. $N \cong N \setminus \{1\}$.

Определение 4.7.2. *Счетным* называют множество, равномощное N.

Теорема 4.7.4. Всякое конечное множество или пусто, или равномощно только одному отрезку натурального ряда.

Следует из теоремы 4.7.2.

Определение 4.7.3. Числом элементов пустого множества называют символ 0 (нуль). *Числом элементов множества,* равномощного отрезку $[1, n]$, называют число n.

Пусть $N_0 \rightleftharpoons N \cup \{0\}$. Множество N называют *расширенным рядом натуральных чисел.* В этом множестве можно ввести бинарные операции «сложение» и «умножение» и бинарное отношение «больше» так, чтобы вновь введенные отношения являлись продолжениями соответствующих отношений во множестве натуральных чисел. Для этой цели достаточно принять следующие соглашения:

1) $0 + 0 = 0 \cdot 0 \rightleftharpoons 0, \quad \neg 0 > 0;$

2) $\forall (n \in N) \quad 0 + n = n + 0 \rightleftharpoons n;$

3) $\forall (n \in N) \quad 0 \cdot n = n \cdot 0 \rightleftharpoons 0;$

4) $\forall (n \in N) \quad n > 0.$

Легко видеть, что система $\langle N_0; +, \cdot \rangle$ — коммутативное полукольцо, а отношение «больше» — связно, антисимметрично, транзитивно и монотонно относительно сложения.

Теорема 4.7.5. Всякое подмножество конечного множества конечно.

Легко выводится из следующего замечания:

$$A \subset [1, n+1] \Rightarrow A \setminus \{n+1\} \subset [1, n].$$

Теорема 4.7.6. Число элементов собственного подмножества конечного множества A либо равно нулю, либо меньше числа элементов множества A.

Символом $\mathfrak{a}_0$ обозначают *мощность* счетного множества.

Вопросы: 4.7.1. Пусть $\mathfrak{b}$ — мощность какого-нибудь непустого конечного множества. Доказать, что:

1) $\mathfrak{b} + \mathfrak{a}_0 = \mathfrak{a}_0;$

2) $\mathfrak{b} \cdot \mathfrak{a}_0 = \mathfrak{a}_0.$

4.7.2*. Доказать, что: 1) $\mathfrak{a}_0 + \mathfrak{a}_0 = \mathfrak{a}_0;$

2) $\mathfrak{a}_0 \cdot \mathfrak{a}_0 = \mathfrak{a}_0.$

Определение 4.7.4. Пусть A — непустое множество; $M \rightleftharpoons N$ или $M \rightleftharpoons [1, k]$, где k — какое-нибудь натуральное число. Всякое однозначное отображение α множества M в A называют *последовательностью* элементов множества A, в частности *конечной,* если $M = [1, k]$, и *бесконечной,* если $M = N$. Образ элемента n множества M называют n-м членом последовательности α. Если образы

всех элементов M в отображении α равны, то последовательность α называют *стационарной.*

Обозначение. Пусть a_n — образ элемента n в отображении

$$\alpha\colon M \to A.$$

В таком случае употребляют обозначение

$$\{a_n\}_{n=1}^{\infty} \rightleftharpoons \alpha,$$

если $M = N$, и

$$\{a_n\}_{n=1}^{k} \rightleftharpoons \alpha,$$

если $M = [1, k]$.
Легко видеть, что

$$A^N = \{\alpha \mid \alpha = \{a_n\}_{n=1}^{\infty};\ \forall (n \in N)\ a_n \in A\}.$$

По аналогии с отношением конечного ранга, заданным во множестве A, любое подмножество A^N мы рассматриваем как *отношение счетного ранга,* заданное во множестве A.

4.8. Сумма и произведение нескольких элементов полугруппы

Теорема 4.8.1. Пусть $n \in N$, $\mathbf{A} \rightleftharpoons \langle A;\ + \rangle$ — полугруппа, $\alpha \rightleftharpoons \langle a_x \rangle_{x=1}^{n}$ — однозначное отображение отрезка $[1, n]$ в A. Тогда существует и только одна функция f_n

$$f_n\colon [1, n] \to A,$$

удовлетворяющая условиям:

$$\left.\begin{array}{l} \text{а) } f_n(1) = a_1; \\ \text{б) } \forall (x \in N) \quad x < n \Rightarrow f_n(x+1) = f_n(x) + a_{x+1}. \end{array}\right\} \qquad (4.8.1)$$

Доказательство. Существование. Индукция по n. Пусть сначала $n = 1$. В таком случае $[1, 1] = \{1\}$,

$$\alpha = \{a_x\}_{x=1}^{1}.$$

Полагаем, т. е. определяем, f_1 следующим образом:

$$\forall (x \in [1, 1])\quad f_1(x) = a_1.$$

Легко видеть, что функция f_1 удовлетворяет предъявленным требованиям.

Пусть теперь высказывание теоремы для некоторого натурального n верно.

Пусть α — какое-нибудь однозначное отображение отрезка $[1, n+1]$ в A. Отображение α индуцирует (вопрос 2.3.1) однозначное отображение $\alpha' \rightleftharpoons \{a'_x\}_{x=1}^{n}$ отрезка $[1, n]$ в A:

$$\forall (x \in [1, n])\quad a'_x = a_x.$$

Поэтому существует функция f_n, удовлетворяющая условиям (4.8.1). Определим функцию f_{n+1} следующим образом:

$$f_{n+1}(x) \rightleftharpoons \begin{cases} f_n(x), & \text{если } x \in [1, n]; \\ f_n(n) + a_{n+1}, & \text{если } x = n+1. \end{cases}$$

Легко проверить, что:

а) $f_{n+1}(1) = a_1$;

б) $\forall (x \in N) \quad x < n+1 \Rightarrow f_{n+1}(x+1) = f_{n+1}(x) + a_{x+1}$.

Однозначность доказывается индукцией по x.

Упражнение 4.8.1. Сформулировать теорему 4.8.1. в мультипликативном обозначении.

Определение 4.8.2. Пусть $\mathbf{A} \rightleftharpoons \langle A; +\rangle$ — полугруппа, $\alpha \rightleftharpoons \{a_x\}_{x=1}^n$ — какая-нибудь конечная последовательность элементов полугруппы $\mathbf{A}$; f_n — функция, удовлетворяющая условиям (4.8.1). Для каждого $k \in [1, n]$ под *суммой k первых членов последовательности α* мы понимаем $f_n(k)$, т. е. значение функции f_n при $x = k$.

Сумму k первых членов последовательности α принято обозначать символом

$$\sum_{x=1}^{k} a_x \quad \text{или} \quad a_1 + \cdots + a_k.$$

Таким образом, имеем:

а) $\sum\limits_{x=1}^{1} a_x = a_1$;

б) $\forall (k \in N) \quad k < n \Rightarrow \sum\limits_{x=1}^{k+1} a_x = \sum\limits_{x=1}^{k} a_x + a_{k+1}$.

В случае, если последовательность α стационарна и состоит из элементов, равных a, сумму ее k первых членов называют *k-кратным* элемента a полугруппы $\mathbf{A}$ и обозначают символом $k * a$ или ka, если это не вызывает недоразумений.

Таким образом,

$$k * a \rightleftharpoons \sum_{x=1}^{k} a.$$

Упражнения: 4.8.2. Определить произведение конечного числа элементов полугруппы $\langle A; \cdot\rangle$.

4.8.3. Определить *натуральную степень* элемента a полугруппы $\langle A; \cdot\rangle$.

4.8.4. Пусть $\langle M_2; +, \cdot\rangle$ — кольцо матриц второго порядка с целыми элементами. Найти для любого элемента A из M_2 k-кратное A.

Вопросы: 4.8.1. Пусть $\langle A; +\rangle$ — полугруппа, $n, m \in N$ и $\alpha \rightleftharpoons \{a_x\}_{x=1}^{n+m}$ — последовательность элементов A. Показать, что

$$\sum_{x=1}^{n} a_x + \sum_{x=1}^{m} a_{n+x} = \sum_{x=1}^{n+m} a_x.$$

4.8.2. Пусть $\langle A; +\rangle$ — полугруппа и $\alpha \rightleftharpoons \{a_x\}_{x=1}^{n}$ — последовательность элементов A; $n_1, \ldots, n_k$ — натуральные числа с условием $n = n_1 + \cdots + n_k$, $k > 1$. Показать, что

$$\sum_{x=1}^{n_1} a_x + \cdots + \sum_{x=1}^{n_k} a_{n_1+\cdots+n_{k-1}+x} = \sum_{x=1}^{n} a_x.$$

4.8.3. Пусть $\langle A; +\rangle$ — коммутативная полугруппа, $\alpha \rightleftharpoons \{a_x\}_{x=1}^{n}$ и $\beta \rightleftharpoons \{b_x\}_{x=1}^{n}$ — последовательности элементов A. Доказать, что

$$\sum_{x=1}^{n} a_x + \sum_{x=1}^{n} b_x = \sum_{x=1}^{n} (a_x + b_x).$$

4.8.4. Пусть $\langle A; +\rangle$ — коммутативная полугруппа и $\alpha_x \rightleftharpoons \{a_{x,y}\}_{y=1}^{n}$ для каждого $x \in [1, m]$ — последовательность элементов A. Доказать, что

$$\sum_{x=1}^{m} \sum_{y=1}^{n} a_{x,y} = \sum_{y=1}^{n} \sum_{x=1}^{n} a_{x,y}.$$

4.8.5*. Пусть $\langle A; +\rangle$ — коммутативная полугруппа, $\alpha \rightleftharpoons \{a_x\}_{x=1}^{n}$ — конечная последовательность полугруппы A, S — взаимно-однозначное отображение отрезка $[1, n]$ на себя

$$S\colon x \mapsto S(x).$$

Доказать, что

$$\sum_{x=1}^{n} a_{S(x)} = \sum_{x=1}^{n} a_x.$$

4.8.6. Пусть $\langle A; +\rangle$ — полугруппа; $a \in A$. Доказать, не пользуясь результатами вопросов 4.8.1. и 4.8.2, следующие свойства натуральных кратных:

1) $\forall (n, m \in N) \quad (n + m) * a = n * a + m * a;$

2) $\forall (n, m \in N) \quad n * (m * a) = (n \cdot m) * a.$

4.8.7. Пусть $\langle A; +\rangle$ — коммутативная полугруппа; $a, b \in A$. Доказать, не пользуясь результатом вопроса 4.8.3, что

$$\forall (n \in N) \quad n * (a + b) = n * a + n * b.$$

4.8.8. Сформулировать утверждения — свойства конечных произведений и степеней элементов полугруппы с мультипликативным обозначением бинарной операции, соответствующие утверждениям вопросов 4.8.1—4.8.7.

4.8.9*. Пусть $A \leftrightharpoons \langle A;\ S,\ 1\rangle$ — система с отношениями:

а) A — множество;

б) S — бинарное отношение;

в) 1 — единица —

и аксиомами:

A_{I}. $1 \in A \wedge \forall (a \in A)\quad 1 \notin Sa$;

A_{II}. $\forall (a \in A)\cdot \exists! (b \in A)\quad b \in Sa$;

A_{III}. $\forall (a,\ b \in A)\quad Sa = Sb \Rightarrow a = b$;

A_{IV}. Всякое подмножество M множества A со свойствами:

а) $1 \in M$;

б) $\forall (a \in A)\quad a \in M \Rightarrow Sa \in M$ —

совпадает с A.

Доказать, что $\langle \{A;\ S,\ 1\},\ \{A_{\mathrm{I}},\ A_{\mathrm{II}},\ A_{\mathrm{III}},\ A_{\mathrm{IV}}\}\rangle$ — формулировка аксиоматической теории натуральных чисел (*аксиоматика Пеано*).

4.8.10*. Пусть A и B — множества; a, b — функции:

$$a\colon A \to B;$$
$$b\colon A \times N \times B \to B.$$

Доказать, что существует и только одна функция c

$$c\colon A \times N \to B,$$

удовлетворяющая условиям:

$$\left.\begin{array}{l} \forall (x \in A)\quad c(x,\ 1) = a(x); \\ \forall (x \in A)\,\forall (y \in N)\quad c(x,\ y+1) = b(x,\ y,\ c(x,\ y)). \end{array}\right\} \qquad (4.8.2)$$

4.8.11. Пусть A и B — множества; $n \in N$; $a_1,\ a_2,\ \ldots,\ a_n,\ b$ — функции:

$$a_1\colon A \to B,$$
$$\vdots$$
$$a_n\colon A \to B;$$
$$b\colon A \times N \times B^n \to B.$$

Доказать, что существует и только одна функция c

$$c\colon A \times N \to B,$$

удовлетворяющая условиям:

$$\begin{array}{l} \forall (x \in A)\quad c(x,\ 1) = a_1(x); \\ \vdots\qquad\quad \vdots\qquad\quad \vdots \\ \forall (x \in A)\quad c(x,\ n) = a_n(x); \\ \forall (x \in A)\quad \forall (y \in N)\quad c(x,\ y+n) = b(x,\ y,\ c(x,\ y),\ \ldots \\ \qquad\qquad \ldots,\ c(x,\ y+n-1)). \end{array}$$

4.8.12*. Пусть $A \rightleftharpoons \langle A; +, \cdot, 0, 1\rangle$ — поле, B — непустое подмножество множества A, удовлетворяющее условиям:

1) $0 \notin B$;
2) $\forall (x \in B) \quad x^{-1} \in B$;
3) $\forall (x, y \in B) \quad x + y \in B$.

Пусть далее $\alpha \rightleftharpoons \{a_x\}_{x=0}^{k}$ — конечная последовательность, члены которой удовлетворяют условиям:

1) $a_0 \in A$;

2) $\forall (x \in N) \quad 1 \leqslant x \leqslant k \Rightarrow a_x \in B$.

Доказать, что существует и только одна функция f_α

$$f_\alpha\colon N_0 \times N_0 \to A,$$

удовлетворяющая условиям:

1) $\forall (x \in N_0) \quad 0 \leqslant x \leqslant k \Rightarrow f_\alpha(x, x) = a_x$;

2) $\forall (x, y \in N_0) \quad 0 \leqslant x < y \leqslant k \Rightarrow f_\alpha(x, y) = a_x + \dfrac{1}{f_\alpha(x+1, y)}$.

4.8.13. Пусть $\boldsymbol{A} \rightleftharpoons \langle A; +, \cdot, 0, 1\rangle$ — поле, B — непустое подмножество множества A, удовлетворяющее условиям вопроса 4.8.12. Пусть $\alpha \rightleftharpoons \{a_x\}_{x=0}^{\infty}$ — последовательность, члены которой, кроме, быть может, a_0, принадлежат множеству B, $a_0 \in A$. Доказать, что существует только одна функция f_α

$$f_\alpha\colon N_0 \times N_0 \to A,$$

удовлетворяющая условиям:

1) $\forall (x \in N_0) \quad f_\alpha(x, x) = a_x$;

2) $\forall (x, y \in N_0) \quad x < y \Rightarrow f_\alpha(x, y) = a_x + \dfrac{1}{f_\alpha(x+1, y)}$.

Определение 4.8.3. Пусть $\alpha \rightleftharpoons \{a_x\}_{x=0}^{\omega}$ — последовательность вопроса 4.8.12 или 4.8.13. *Цепной дробью последовательности* α называют выражение вида

$$a_0 + \cfrac{1}{a_1 + \ddots + \cfrac{1}{a_k}},$$

если $\omega \rightleftharpoons k \in N_0$, и выражение вида

$$a_0 + \cfrac{1}{a_1 + \ddots + \cfrac{1}{a_n + \ddots}},$$

если $\omega \rightleftharpoons \infty$. Для каждого $n \in [0, k]$ в первом случае или для каждого $n \in N_0$ во втором случае *подходящей дробью последователь-*

ности α порядка n называют $f_\alpha(1, n)$, т. е. значение функции f_α вопроса 4.8.12 в первом случае или вопроса 4.8.13 во втором случае при $x = 1$ и $y = n$. Это значение обозначают символом $[a_0; \ldots; a_n]$.

Легко видеть, что:

1) $[a_0] = a_0$;

2) $\forall (n \in N) \quad [a_0; \ldots; a_n] = a_0 + \dfrac{1}{[a_1, \ldots, a_n]}$.

Отсюда следует, что

$$[a_0; a_1, a_2] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}}.$$

В связи с этим для обозначения подходящей дроби порядка n цепной дроби пользуются и выражением

$$a_0 + \cfrac{1}{a_1 + \ddots + \cfrac{1}{a_n}} \tag{4.8.3}$$

Иногда и термин «конечная цепная дробь порядка n» служит для обозначения подходящей дроби порядка n. Из контекста всегда ясно, когда этим термином обозначается выражение (4.8.3), а когда значение функции f_α при $x = 1$ и $y = n$.

Вопросы: 4.8.14. Пусть A и B — множества вопроса 4.8.12, $\alpha \leftrightharpoons \{a_x\}_{x=0}^{\omega}$ и $\beta \leftrightharpoons \{b_x\}_{x=0}^{\omega}$ — конечные или бесконечные последовательности элементов множества A, все члены которых, кроме, быть может, a_0 и b_0, принадлежат B.

Пусть далее n — натуральное число такое, что

$$\forall (x \in N_0) \quad 0 \leqslant x < n \Rightarrow a_x = b_x.$$

Доказать, что

$$[a_0; \ldots; a_{n-1}] = [b_0; \ldots; b_{n-1}].$$

4.8.15. Пусть $\alpha \leftrightharpoons \{a_x\}_{x=0}^{\omega}$ — последовательность вопроса 4.8.12 или 4.8.13. Доказать, что для любых натуральных n и x, если $x < n < \omega + 1$, то

$$[a_0; \ldots, a_n] = [a_0; \ldots, a_{x-1}, [a_x; \ldots, a_n]] \tag{4.8.4}$$

4.9. Независимость аксиомы индукции и роль аксиомы индукции в обосновании теории неравенств, теории делимости и свойств арифметических действий

Чтобы доказать независимость аксиомы индукции от других аксиом, достаточно указать такую интерпретацию нашей теории из объектов непротиворечивой теории, на которой аксиомы N_{I} — N_{VI} выполняются, а аксиома N_{VII} — нет. Такую интерпретацию, и даже несколько, мы построим, предполагая, что аксиоматическая теория

натуральных, а также рациональных чисел непротиворечива. В связи с тем, что при построении других числовых систем независимость аксиомы индукции нигде не используется, ссылка на утверждения, доказываемые позднее, не приведет к появлению порочного круга.

Первая интерпретация I_{I}. За $N^{(1)}$ примем множество

$$\{\langle a,\ x\rangle \mid a \in N,\ x \in \{0,\ 1\}\},$$

за единицу — пару $\langle 1,1\rangle$, сложение и умножение на $N^{(1)}$ определим так:

$$\langle a,\ x\rangle \oplus \langle b,\ y\rangle \rightleftharpoons \begin{cases} \langle a+b,\ 0\rangle, & \text{если } x = y; \\ \langle a+b,\ 1\rangle, & \text{если } x \neq y. \end{cases}$$

$$\langle a,\ x\rangle \odot \langle b,\ y\rangle \rightleftharpoons \langle ab,\ xy\rangle.$$

Легко проверить, что для интерпретации I_{I} выполняются первые шесть аксиом содержательной теории натуральных чисел. Пусть далее

$$M \rightleftharpoons \{\langle 2a,\ 0\rangle \mid a \in N\} \cup \{\langle 2a-1,1\rangle\} \mid a \in N\}.$$

Имеем:

а) $\langle 1,1\rangle \in M$; б) $\forall (\alpha \in N^{(1)})\quad \alpha \in M \Rightarrow \alpha \oplus \langle 1,1\rangle \in M$.

Вместе с тем $M \neq N^{(1)}$, так как, например, $\langle 1,0\rangle \notin M$. Итак, аксиома N_{VII} на интерпретации I_{I} не выполняется.

Предположим, что в интерпретации I_{I} определено транзитивное, антирефлексивное, связное и монотонное относительно обеих операций бинарное отношение «$>$». Тогда $\langle 1,0\rangle > \langle 1,1\rangle$ или $\langle 1,1\rangle > \langle 1,0\rangle$. В первом случае имеем:

$$\langle 2,1\rangle = (\langle 1,0\rangle \oplus \langle 1,1\rangle) > (\langle 1,1\rangle \oplus \langle 1,1\rangle) = \langle 2,0\rangle$$

и

$$\langle 2,0\rangle = (\langle 1,0\rangle \oplus \langle 1,0\rangle) > (\langle 1,1\rangle \oplus \langle 1,0\rangle) = \langle 2,1\rangle.$$

В силу транзитивности отсюда получим $\langle 2,1\rangle > \langle 2,1\rangle$, что невозможно. Аналогично опровергается и второе допущение.

Из этих рассуждений следует, что теорию неравенств нельзя обосновать без аксиомы индукции.

Вторая интерпретация I_{II}. За $N^{(2)}$ примем множество

$$\left\{\frac{a+1}{2} \mid a \in N\right\},$$

за единицу — число $1 = \frac{1+1}{2}$, сложение и умножение определяем условиями:

$$\forall (\alpha,\ \beta \in N^{(2)})\quad \alpha \oplus \beta \rightleftharpoons \alpha + \beta;\ \alpha \odot \beta \rightleftharpoons \frac{[2\alpha\beta]}{2}.$$

Легко видеть, что если α или β целое число, то

$$\alpha \odot \beta = \alpha\beta.$$

Вместе с тем

$$\frac{3}{2} \odot \frac{3}{2} = \frac{\left[\frac{9}{2}\right]}{2} = 2 \neq \frac{3}{2} \cdot \frac{3}{2}.$$

Нетрудно проверить выполнение аксиом $N_{\text{I}} - N_{\text{VI}}$. Аксиома N_{VII} не выполняется на I_{II}. В самом деле, пусть $M = N \neq N^{(2)}$. Имеем:

а) $1 \in M$;

б) $\forall (\alpha \in N^{(2)}) \quad \alpha \in M \Rightarrow \alpha \in N \Rightarrow \alpha + 1 \in N \Rightarrow \alpha \oplus 1 \in M.$

Заметим, что в интерпретации I_{II} ассоциативность и дистрибутивность умножения не имеют места, так как:

$$\frac{9}{2} = \frac{3}{2} \odot \left(\frac{3}{2} \odot 2\right) \neq \left(\frac{3}{2} \odot \frac{3}{2}\right) \odot 2 = 4;$$

$$\frac{9}{2} = \left(\frac{3}{2} \oplus \frac{3}{2}\right) \odot \frac{3}{2} \neq \frac{3}{2} \odot \frac{3}{2} \oplus \frac{3}{2} \odot \frac{3}{2} = 4.$$

Третья интерпретация I_{III}. За $N^{(3)}$ примем множество пар целых чисел

$$N^{(3)} \rightleftharpoons \{\langle n, x\rangle \mid n \in N, \quad x = 0 \quad \vee x = 1\}.$$

За единицу — пару $\langle 1,0\rangle$, а операции определяем так:

$$\langle n, x\rangle \oplus \langle m, y\rangle \rightleftharpoons \begin{cases} \langle n + m, x\rangle, & \text{если } x \cdot y = 0; \\ \langle m, 1\rangle, & \text{если } x \cdot y = 1. \end{cases}$$

$$\langle n, x\rangle \odot \langle m, y\rangle \rightleftharpoons \begin{cases} \langle nm, y\rangle, & \text{если } x = 0; \\ \langle n, 1\rangle, & \text{если } x = 1. \end{cases}$$

Можно проверить, что на I_{III} выполняются аксиомы $N_{\text{I}} - N_{\text{VI}}$, но не N_{VII}. Вместе с тем на I_{III} не имеют места коммутативность сложения и умножения, ассоциативность сложения и дистрибутивность умножения.

Из существования моделей I_{II} и I_{III} следует, что известные свойства арифметических действий не могут быть обоснованы без аксиомы индукции.

Четвертая интерпретация I_{IV}. За $N^{(4)}$ примем множество чисел вида

$$N^{(4)} \rightleftharpoons \left\{\frac{a}{b} \,\middle|\, a, b \in N \wedge a \geqslant b\right\}.$$

За единицу примем число $1 = \frac{1}{1}$; операции определим так:

$$\alpha \oplus \beta \rightleftharpoons \alpha + \beta, \quad \alpha \odot \beta \rightleftharpoons \alpha \cdot \beta.$$

Легко видеть, что $\langle N^{(4)};\ \oplus,\ \odot\rangle$ — полукольцо и

$$\forall\,(\alpha,\ \beta \in N^{(4)})\quad 1 \neq \alpha \oplus \beta.$$

Таким образом, аксиомы N_{I} — N_{VI} на I_{IV} выполняются, а аксиома N_{VII}, как легко проверить,— нет.

Интересно отметить, что на I_{IV} нет простых чисел. Пусть $\alpha \in N^{(4)}$, $\alpha \neq 1$. Тогда

$$\alpha = \frac{a}{b};\quad a > b.$$

Известно (вопрос 4.6.7), что

$$\exists\,(x \in N)\quad (a-b)\,x > b.$$

Поэтому

$$\frac{a}{b} = \frac{a \cdot x}{b(x+1)} \cdot \frac{x+1}{x}.$$

Таким образом, любой элемент $N^{(4)}$ можно разложить в произведение двух отличных от единицы множителей.

Пятая интерпретация I_{V}. Полагаем

$$N^{(5)} \rightleftharpoons \{\langle a,\ b\rangle \mid a,\ b \in N \wedge a \leqslant b\};$$

$$\langle a,\ b\rangle \oplus \langle a',\ b'\rangle \rightleftharpoons \langle a + a',\ b + b'\rangle,$$

$$\langle a,\ b\rangle \odot \langle a',\ b'\rangle \rightleftharpoons \langle a \cdot a',\ b \cdot b'\rangle.$$

За единицу примем элемент $\langle 1,1\rangle$. Аксиомы N_{I} — N_{VI} на I_{V} выполняются, но не N_{VII}. В I_{V} есть неразложимые (простые) элементы. Такими будут $\langle 2,\ 5\rangle$, $\langle 3,\ 7\rangle$, $\langle 2,\ 3\rangle$, $\langle 5,\ 7\rangle$. Имеем

$$\langle 6,35\rangle = \langle 2,5\rangle \odot \langle 3,7\rangle = \langle 2,7\rangle \odot \langle 3,5\rangle.$$

Итак, на $N^{(5)}$ нет однозначности разложения на простые множители. Из существования моделей I_{IV} и I_{V} следует, таким образом, что и теорию делимости в системе натуральных чисел нельзя обосновать без аксиомы индукции.

Вопрос 4.9.1*. Доказать независимость каждой из аксиом аксиоматической теории, первичными терминами которой являются множество N (натуральных чисел), два тернарных отношения в нем $+$ и $\cdot$ (сложение и умножение) и одно унарное — множество E (множество единиц), а аксиомы формулируются так:

1) $E \neq \varnothing \wedge \forall\,(a,\ b \in N)\quad E \cap (a+b) = \varnothing$;

2) $\forall\,(a \in N)\quad e \in E \Rightarrow \exists!\,(c \in N)\quad c \in a + e$;

3) $\forall\,(a,\ b \in N)\quad e \in E \wedge (a+e) \cap (b+e) \neq \varnothing \Rightarrow \varnothing \neq$
$\neq a + (b+e) \subset (a+b) + e.$

4) $\forall\,(a,\ b \in N)\quad e \in E \wedge a + b \neq \varnothing \Rightarrow \varnothing \neq$
$\neq a + (b+e) \subset a + b + e$;

5) $\forall\,(a \in N)\quad e \in E \Rightarrow a \cdot e = a$;

6) $\forall\,(a,\ b \in N)\quad e \in E \wedge a \cdot b + a \neq \varnothing \Rightarrow \varnothing \neq$
$\neq a(b+e) \subset a \cdot b + a$;

7) Каково бы ни было подмножество M множества N, если выполняются условия:

а) $e \in E \Rightarrow e \in M$;

б) $a \in M \wedge e \in E \Rightarrow a + e \in M$, то $N \subset M$.

4.10. Категоричность аксиоматической теории натуральных чисел

Теорема 4.10.1. Аксиоматическая теория натуральных чисел категорична.

Доказательство. В предположении, что аксиоматическая теория натуральных чисел непротиворечива, докажем, что любые две модели изоморфны. Пусть $\langle N_1; +, \cdot, 1_1\rangle$ и $\langle N_2; \oplus, \odot, 1_2\rangle$ — две модели нашей теории. Операции в этих моделях мы обозначаем разными символами, любой элемент множества N_1 снабжаем индексом 1, а любой элемент N_2 — индексом 2. Мы намереваемся определить изоморфное отображение одной системы на вторую.

Докажем, что существует взаимно-однозначное отображение φ множества N_1 на N_2, обладающее свойствами:

$$\left.\begin{array}{l} \text{а) } \varphi(1_1) = 1_2; \\ \text{б) } \forall (x_1 \in N_1) \quad \varphi(x_1 + 1_1) = \varphi(x_1) \oplus 1_2. \end{array}\right\} \qquad (4.10.1)$$

Из теоремы 4.8.1. следует, что для любого натурального n_1 существует однозначная функция φ_{n_1} — отображение отрезка $[1_1, n_1]$ в N_2, и притом только одно, удовлетворяющее условиям:

а) $\varphi_{n_1}(1_1) = 1_2$;

б) $\forall (x_1 \in N_1) \quad x_1 < n_1 \Rightarrow \varphi_{n_1}(x_1 + 1_1) = \varphi_{n_1}(x_1) \oplus 1_2$.

Пусть теперь $a_1 \in N$. Выберем любое $n_1 \in N_1$ с условием $a_1 \leqslant n_1$ и положим

$$\varphi(a_1) \rightleftarrows \varphi_{n_1}(a_1).$$

Этим условием определяется однозначное отображение N_1 в N_2. В самом деле, если $m_1 \in N_1$ и $m_1 > n_1$, то в силу теоремы 4.8.1 значения функций φ_{n_1} и φ_{m_1} совпадают на отрезке $[1_1, n_1]$.

Проверим, что условия (4.10.1) для отображения φ выполняются. Имеем:

а) $\varphi(1_1) = \varphi_{n_1}(1_1) = 1_2$;

б) $\forall (x_1, n_1 \in N_1) \quad n_1 > x_1 \Rightarrow \varphi(x_1) = \varphi_{n_1}(x_1) \wedge \varphi(x_1 + 1_1) =$

$= \varphi_{n_1}(x_1 + 1_1) = \varphi_{n_1}(x_1) \oplus 1_2 = \varphi(x_1) \oplus 1_2$.

Покажем, что φ — взаимно-однозначное отображение N_1 в N_2. Другими словами:

$$\forall (x_1, y_1 \in N_1) \quad x_1 \neq y_1 \Rightarrow \varphi(x_1) \neq \varphi(y_1). \qquad (4.10.2)$$

Проверим, что условие (4.10.2) выполняется, если $y_1 = 1_1$. В самом деле, если $x_1 \neq 1_1$, то

$$\exists (z_1 \in N_1) \quad x_1 = z_1 + 1_1.$$

Имеем

$$\varphi(x_1) = \varphi(z_1 + 1_1) = \varphi(z_1) \oplus 1_2 \neq 1_2 = \varphi(1_1).$$

Пусть для некоторого y_1 из N_1 условие (4.10.2) выполнено. Пусть $x_1 \neq y_1 + 1_1$, но

$$\varphi(x_1) = \varphi(y_1 + 1_1). \tag{4.10.3}$$

Имеем

$$\varphi(y_1 + 1_1) = \varphi(y_1) \oplus 1_2.$$

Поэтому

$$\varphi(x_1) = \varphi(y_1) \oplus 1_2 \neq 1_2,$$

и, следовательно, $x_1 \neq 1_1$. Таким образом,

$$\exists (z_1 \in N_1) \quad x_1 = z_1 + 1_1.$$

Имеем

$$\varphi(x_1) = \varphi(z_1) \oplus 1_2.$$

В силу (4.10.3) получим $\varphi(z_1) \oplus 1_2 = \varphi(y_1) \oplus 1_2$. По аксиоме N_{III} $\varphi(z_1) = \varphi(y_1)$ и $z_1 = y_1$ по предположению. Таким образом,

$$x_1 = z_1 + 1_1 = y_1 + 1_1,$$

в противоречие с условием. Наше утверждение следует из аксиомы N_{VII}.

Покажем далее, что φ — взаимно-однозначное отображение N_1 на N_2.

Прежде всего имеем

$$1_2 = \varphi(1_1).$$

Если $x_2 = \varphi(x_1)$, то $x_2 \oplus 1_2 = \varphi(x_1) \oplus 1_2 = \varphi(x_1 + 1_1)$. По аксиоме N_{VII} получим, что

$$\forall (x_2 \in N_2) \quad \exists (x_1 \in N_1) \quad x_2 = \varphi(x_1).$$

Осталось показать, что

$$\forall (x_1, y_1 \in N_1) \quad \varphi(x_1 + y_1) = \varphi(x_1) \oplus \varphi(y_1) \wedge \varphi(x_1 \cdot y_1) = \\ = \varphi(x_1) \odot \varphi(y_1).$$

Прежде всего имеем

$$\varphi(x_1 + 1_1) = \varphi(x_1) \oplus 1_2 = \varphi(x_1) \oplus \varphi(1_1).$$

Пусть

$$\varphi(x_1 + y_1) = \varphi(x_1) \oplus \varphi(y_1).$$

Тогда получим

$$\varphi(x_1 + (y_1 + 1_1)) = \varphi((x_1 + y_1) + 1_1) = \varphi(x_1 + y_1) \oplus 1_2 = \\ = [\varphi(x_1) \oplus \varphi(y_1)] \oplus 1_2 = \varphi(x_1) \oplus [\varphi(y_1) \oplus 1_2] = \varphi(x_1) \oplus \varphi(y_1 + 1_1).$$

Отсюда по аксиоме N_{VII} получаем первое равенство. Столь же легко получается и второе.

Вопросы: 4.10.1. Доказать, что в системе $\mathbf{N} \rightleftharpoons \langle N;\ +,\ \cdot,\ 1\rangle$ натуральных чисел:

а) существует бесконечно много подполугрупп, изоморфных полугруппе $\langle N;\ +\rangle$ натуральных чисел;

б) существует и только одно подполукольцо, изоморфное полукольцу $\langle N;\ +,\ \cdot\rangle$ натуральных чисел.

4.10.2. Пусть $\mathbf{T} \rightleftharpoons \langle T;\ +,\ \cdot,\ 0,\ e\rangle$ — *тело характеристики нуль;* другими словами,

$$n * e \rightleftharpoons \sum_{1}^{n} e \neq 0$$

для любого натурального n, и пусть M — множество всех натуральных кратных единице e тела $\mathbf{T}$. Доказать, что система $\langle M;\ +,\ \cdot,\ e\rangle$ есть система натуральных чисел.

4.10.3. Доказать, что всякое тело характеристики нуль содержит и только одно подполукольцо натуральных чисел.

4.10.4. Пусть $\mathbf{T} \rightleftharpoons \langle T;\ +,\ \cdot,\ 0,\ e\rangle$ — тело характеристики нуль, $\mathbf{N} \rightleftharpoons \langle N;\ +,\ \cdot,\ 1\rangle$ — система натуральных чисел. Доказать, что:

$$1)\ \forall (a \in T)\quad \forall (n \in N)\quad a \cdot (n * e) = (n * e) \cdot a,$$
$$a \cdot (n * e)^{-1} = (n * e)^{-1} \cdot a;$$

$$2)\ \forall (a \in T)\quad \forall (n,\ m \in N)\quad a \cdot \left(\frac{n * e}{m * e}\right) = \frac{n * e}{m * e} \cdot a.$$

Пусть $\langle A;\ \oplus,\ \odot\rangle$ — полукольцо, изоморфное полукольцу натуральных чисел $\langle N;\ +,\ \cdot\rangle$, и пусть φ — изоморфное отображение полукольца $\langle N;\ +,\ \cdot\rangle$ на полукольцо $\langle A;\ \oplus,\ \odot\rangle$. Легко видеть, что φ вместе с тем есть изоморфное отображение системы $\langle N;\ +,\ \cdot,\ 1\rangle$ натуральных чисел на систему $\langle A;\ \oplus,\ \odot,\ \varphi(1)\rangle$. В соответствии с этим говорят, что всякое полукольцо, изоморфное полукольцу натуральных чисел, само является полукольцом натуральных чисел.

4.11. Аксиома минимальности

Определение 4.11.1. Пусть имеется класс K каких-нибудь множеств. Под *минимальным множеством класса* K понимают множество M_0 в случае, если:

1) $M_0 \in K$;

2) $\forall (A \subset M_0)\quad A \neq M_0 \Rightarrow A \notin K$.

Пример 4.11.1. Введем обозначения. Буквой P будем обозначать множество всех простых чисел, а через N_k для каждого натурального k — множество натуральных чисел, кратных k. Класс T множеств

натуральных чисел определим так. К классу T отнесем множество M в случае, если:

1) $M \subset N$;
2) $\exists (p \in P) \quad p \in M$;
3) $\forall (p \in P) \quad p \in M \Rightarrow N_p \subset M$.

Легко видеть, что N_2, N_3, $N_2 \cup N_3$ входят, например, в класс T. При этом множество N_2 является минимальным в классе T, так как любое его собственное подмножество не входит в класс T.

Пример 4.11.2. Рассмотрим класс S_6 систем с отношениями $\langle N; +, \cdot, 1\rangle$ таких, что для каждой из них выполняются аксиомы

$$N_{\mathrm{I}}, \ N_{\mathrm{II}}, \ N_{\mathrm{III}}, \ N_{\mathrm{IV}}, \ N_{\mathrm{V}}, \ N_{\mathrm{VI}}. \qquad (4.11.2)$$

Всякое минимальное множество этого класса есть система натуральных чисел. В самом деле, пусть M_0 — минимальное множество класса S_6. Аксиомы N_{I}, N_{II}, N_{III}, N_{IV}, N_{V}, N_{VI} на M_0 выполняются. Покажем, что N_{VII} на M_0 выполняется. Пусть A — какое угодно подмножество M_0, удовлетворяющее условиям:

1) $1 \in A$;
2) $\forall (a \in M_0) \quad a \in A \Rightarrow a + 1 \in A$.

В таком случае выполняются на A, во-первых, аксиомы N_{I} и N_{II} в силу указанных условий и, во-вторых, аксиомы N_{III}, N_{IV}, N_{V}, N_{VI}, так как они выполняются на любом подмножестве M_0. Таким образом, при наших предположениях $A \in S_6$ и $A = M_0$ в силу минимальности M_0. Другими словами, и аксиома N_{VII} выполняется на M_0.

Наоборот, система $\mathbf{N} \rightleftharpoons \langle N; +, \cdot, 1\rangle$ натуральных чисел является минимальным множеством в классе S_6. Действительно, $N \in S_6$, так как аксиомы N_{I}, N_{II}, N_{III}, N_{IV}, N_{V}, N_{VI} выполнены. Пусть теперь M — подмножество N такое, что $M \in S_6$. Тогда:

1) $1 \in M$, так как аксиома N_1 выполняется на M;

2) $\forall (a \in N) \quad a \in M \Rightarrow a + 1 \in M$, так как аксиома N_{II} выполняется на M. Но на N выполнена аксиома индукции, а потому $M = N$.

Итак, $\langle N; +, \cdot\rangle$ — минимальное множество в классе S_6.

В связи с установленными здесь свойствами системы натуральных чисел аксиому индукции иногда называют *аксиомой минимальности* системы натуральных чисел.

Пример 4.11.3. Пусть $\mathbf{A} \rightleftharpoons \langle A; +, \cdot\rangle$ — подкольцо (подтело) кольца $\mathbf{B} \rightleftharpoons \langle B; +, \cdot\rangle$ и x — элемент B. Рассмотрим класс всех подколец (подтел) кольца $\mathbf{B}$ с условием, что для всякого $\mathbf{B}' \rightleftharpoons \langle B'; +, \cdot\rangle$ из K множество B' содержит A и элемент x. Этот класс не пуст, и пересечение всех колец класса K снова, как легко видеть (вопросы 2.6.4 и 2.6.5), принадлежит K и даже является минимальным множеством этого класса.

Определения 4.11.2 и 4.11.3. Пусть $\mathbf{B} \rightleftharpoons \langle B; +, \cdot\rangle$ — кольцо, $\mathbf{A} \rightleftharpoons \langle A; +, \cdot\rangle$ — его подкольцо (подтело), $x \in B$. *Кольцом (те-*

лом), полученным путем присоединения к кольцу (телу) $\mathbf{A}$ *элемента* x, называют минимальное кольцо в классе K всех подколец (подтел) кольца $\mathbf{B}$ с условием, что для всякой системы $\mathbf{B}' \rightleftharpoons \langle B'; +, \cdot\rangle$ из K множество B' содержит A и элемент x.

Обозначения. $\mathbf{A}[x]$ — кольцо, полученное путем присоединения к кольцу $\mathbf{A}$ элемента x; $\mathbf{A}(x)$ — тело, полученное путем присоединения к телу $\mathbf{A}$ элемента x. Полагают далее: $\mathbf{A}[x, y] \rightleftharpoons \mathbf{A}[x][y]$, $\mathbf{A}(x, y) \rightleftharpoons \mathbf{A}(x)(y)$.

Определение 4.11.4 и 4.11.5. Пусть $\mathbf{A} \rightleftharpoons \langle A; +, \cdot, \mathbf{P}\rangle$ — линейная алгебра над полем $\mathbf{P}$, $\mathbf{P}$ — подполе системы $\langle A; +, \cdot\rangle$; x, y — элементы множества A. *Линейной алгеброй, полученной путем присоединения к полю* $\mathbf{P}$ *элемента* x *(элементов* x *и* y*),* называют пересечение всех линейных подалгебр алгебры $\boldsymbol{A}$, содержащих поле $\mathbf{P}$ и элемент x (элементы x и y).

Вопрос 4.11.1. Пусть $\mathbf{A} \rightleftharpoons \langle A; +, \cdot, \mathbf{P}\rangle$ — линейная алгебра над полем $\mathbf{P}$, $\mathbf{P} \rightleftharpoons \langle P; +, \cdot\rangle$ — подполе системы $\langle A; +, \cdot\rangle$, $x, y \in A$. Обозначим символом $\mathbf{P}[x]$ $(\mathbf{P}[x, y])$ линейную алгебру, полученную путем присоединения к полю $\mathbf{P}$ элемента x (элементов x и y). Доказать, что:

1) $\forall (a \in A)\ \ \mathbf{P}[a] = \mathbf{P} \Rightarrow a \in \mathbf{P}$;

2) $\forall (a, b \in A)\ \ \mathbf{P}[a, b] = \mathbf{P}[b, a]$;

3) $\forall (a \in A) \forall (k, l \in P)\ \ k \neq 0 \Rightarrow \mathbf{P}[a] = \mathbf{P}[ka + l]$;

4) $\forall (a, b \in A) \forall (k, l, k', l' \in P)\ \ k \neq 0 \wedge k' \neq 0 \Rightarrow \mathbf{P}[a, b] = \mathbf{P}[ka + l, k'b + l']$;

5) $\forall (a, b \in A) \forall (k, l \in P)\ \ k \neq 0 \Rightarrow \boldsymbol{P}[a, b] = \mathbf{P}[ka + lb, b]$.

4.12. Непротиворечивость арифметики и другие вопросы

Мы заметили, что непротиворечивость неформальной (содержательной) аксиоматической теории можно установить, только указав какую-нибудь модель из объектов теории, непротиворечивость которой уже доказана, но для аксиоматической теории натуральных чисел такой модели нет.

В связи с этим рассматривают проблему непротиворечивости формальной аксиоматической теории натуральных чисел.

В 1931 г. *К. Гедель* доказал, что непротиворечивость формальной аксиоматической теории натуральных чисел не может быть обоснована средствами той же теории. Он также доказал, что всякая формальная аксиоматическая теория, включающая арифметику натуральных чисел, неполна. Отсюда следует, что формальная арифметика некатегорична. На первый взгляд этот результат противоречит теореме 4.10.1. Однако формальную и содержательную арифметику нельзя отождествить. Между ними есть по крайней мере одно существенное отличие, связанное с аксиомой индукции. С каждой формулой формальной арифметики сопоставим множество

тех натуральных чисел, для которых данная формула истинна. При этом толковании аксиома индукции в содержательной и формальной арифметике позволяет установить, если выполняются определенные условия, что данным свойством — принадлежности к некоторому множеству — обладают все натуральные числа. В содержательной арифметике рассматриваются любые их свойства без каких-либо ограничений. В формальной — лишь свойства, связанные с формулами этой теории. А это не одно и то же.

Из теоремы Геделя следует, что возможен только один путь доказательства непротиворечивости формальной арифметики — путь, основанный на использовании в таком доказательстве средств, не формализуемых в самой теории, но тем не менее достаточно надежных. В 1936 г. *Г. Генцен* получил доказательство непротиворечивости формальной арифметики. В этом доказательстве используются средства, не формализуемые в самой теории.

Непротиворечивость аксиоматических теорий других числовых систем доказывается построением модели в рамках теории, непротиворечивость которой предполагается известной, или в рамках теории, предполагаемой непротиворечивой. Так непротиворечивость аксиоматической теории целых чисел может быть сведена к непротиворечивости аксиоматической теории натуральных чисел и так далее. В каждом случае исходят из некоторого бесконечного множества объектов непротиворечивой теории и средствами интуитивной теории множеств завершают построение соответствующей модели. Такого рода подход к обоснованию числовых систем был разработан в XIX в.

Понятие бесконечности вошло в математику очень давно, с ним связаны многие достижения этой науки. Однако неосмотрительное применение к бесконечным совокупностям способов рассуждений, безотказно работающих в конечных областях, может быть причиной неожиданных неприятностей. На рубеже XIX и XX вв. в связи с обнаруженными в теории множеств парадоксами очень острым стал вопрос, какие способы рассуждений допустимы в математике. Возникшие при решении этого вопроса трудности нельзя считать преодоленными.

§ 5. УПОРЯДОЧЕННЫЕ МНОЖЕСТВА И АЛГЕБРАИЧЕСКИЕ СИСТЕМЫ

5.1. Упорядоченные множества

Определение 5.1.1. Пусть во множестве M задано бинарное отношение $\succ$ («выше» или «следует за»). Это отношение называют *отношением порядка,* а систему $\langle M; \succ \rangle$ — *упорядоченным множеством,* если это отношение:

1) транзитивно, т. е. $\forall (a, b, c \in M)\ a \succ b \wedge b \succ c \Rightarrow a \succ c$;

и

2) антисимметрично, т. е. $\forall (a, b \in M)\ a \succ b \wedge b \succ a \Rightarrow a = b$.

Вместо того чтобы сказать «a выше b», мы говорим также «b предшествует a». Если $a \succ b$ и если для любого элемента x, отличного от a и от b,

$$a \succ x \Rightarrow \neg\, x \succ b,$$

мы говорим «a непосредственно следует за b».

Отношение порядка во множестве M называют *отношением нестрогого порядка,* а систему $\langle M; \succ \rangle$ — *нестрого упорядоченным множеством,* если это отношение

3) рефлексивно, т. е. $\forall\ (a \in M)\ a \succ a$.

Отношение порядка во множестве M называют *отношением строгого порядка,* а систему $\langle M; \succ \rangle$ — *строго упорядоченным множеством,* если это отношение

4) антирефлексивно, т. е. $\forall\ (a \in M)\ \neg\, a \succ a$.

Отношение порядка во множестве M называют *отношением линейного* (или *совершенного*) *порядка,* а систему $\langle M; \succ \rangle$ — *линейно (совершенно) упорядоченным множеством,* если это отношение

5) связно, т. е. $\forall\ (a, b \in M)\ a \neq b \Rightarrow a \succ b \vee b \succ a$.

Если отношение порядка во множестве M не является отношением линейного порядка, то это отношение называют *отношением частичного порядка,* а систему $\langle M; \succ \rangle$ — *частично упорядоченным множеством.*

Следующие термины, мы думаем, понятны без объяснений: «линейно и нестрого упорядоченное множество», «линейно и строго

упорядоченное множество», «частично и нестрого упорядоченное множество», «частично и строго упорядоченное множество».

Если $\mathbf{M} \rightleftharpoons \langle M;\ \succ \rangle$ — упорядоченное множество, а M' — подмножество M, то бинарное отношение $\succ$ является отношением порядка и в M'. При этом система $\mathbf{M}' \rightleftharpoons \langle M';\succ \rangle$ — строго упорядоченное множество, если система $\mathbf{M}$ — строго упорядоченное множество; $\mathbf{M}'$ — линейно упорядоченное множество, если система $\mathbf{M}$ — линейно упорядоченное множество. В дальнейшем термин «подмножество» упорядоченного множества $\langle M;\ \succ \rangle$ используется и для обозначения подмножества множества M, и для обозначения системы $\langle M';\ \succ \rangle$, где $M' \subset M$.

Пусть $\langle M;\ \succ \rangle$ — упорядоченное множество; a, b, c — его элементы. Если $a \succ b$ и $b \succ c$, то говорят, что элемент b лежит между элементами a и c. Если система $\langle M;\ \succ \rangle$ — линейно упорядоченное множество, то хотя бы один из любой тройки элементов множества M лежит между двумя другими.

Пусть $\langle A;\ \succ \rangle$ — упорядоченное множество, B — подмножество множества A. Элемент e — множества A называют *нижней гранью* множества B, если

$$\forall (x \in B) \quad x \neq e \Rightarrow x \succ e,$$

в частности *наименьшим элементом множества* B, если к тому же $e \in B$.

Определение 5.1.2. Пусть B — подмножество упорядоченного множества $\langle A;\ \succ \rangle$. Элемент m множества B называют *минимальным элементом* множества B, если

$$\forall (x \in B) \quad x \neq m \Rightarrow \neg\, m \succ x.$$

Аналогично определяется *верхняя грань, наибольший* и *максимальный элементы* подмножества упорядоченного множества. Множество всех верхних и нижних граней множества B мы обозначаем соответственно символами $U(B)$ и $L(B)$. В частности, $U(a, b)$ — множество всех элементов множества A, следующих за элементами a и b; $U(a)$ — множество всех элементов A, следующих за элементом a.

Упорядоченное множество $\langle A;\ \succ \rangle$ называют *решеткой (структурой)*, если выполняются следующие условия:

1) $\forall (a, b \in A) \quad \exists (c \in A) \quad U(a, b) = U(c)$;
2) $\forall (a, b \in A) \quad \exists (d \in A) \quad L(a, b) = L(d)$.

Примеры: 5.1.1. Отношение $\vdots$ (делится на) делимости в N — отношение частичного и нестрогого порядка.

5.1.2. Отношение $\subset$ — включения во множестве всех подмножеств данного множества — отношение частичного и нестрогого порядка.

5.1.3. Отношение делимости во множестве всех степеней данного натурального числа — отношение линейного и нестрогого порядка.

5.1.4. Пусть M — множество, PM — множество всех его подмножеств. Тогда система $\langle PM;\ \subset \rangle$ — решетка.

5.1.5. Система $\langle N;\ \vdots\rangle$ — решетка. Если a и b — натуральные числа, то $U(a, b)$ и $L(a, b)$ множество общих кратных и множество общих делителей чисел a и b соответственно.

Вопросы 5.1.1. Какими являются отношения $>$ (больше) и $\geqslant$ (больше или равно) во множестве натуральных чисел?

5.1.2. Доказать, что

$$\forall (a,\ b \in M)\quad a > b \Rightarrow \neg\, b > a,$$

если $\langle M;\ >\rangle$ — строго упорядоченное множество.

5.1.3. Пусть $\langle M;\ >\rangle$ — линейно упорядоченное множество. Доказать, что бинарное отношение $>$ в M, определяемое условием

$$\forall (a,\ b \in M)\quad a > b \Leftrightarrow a > b \wedge a \neq b,$$

есть отношение линейного и строгого порядка.

5.1.4. Пусть $\langle M;\ >\rangle$ — линейно упорядоченное множество. Доказать, что бинарное отношение $\geqslant$ в M, определяемое условием

$$\forall (a,\ b \in M)\quad a \geqslant b \Leftrightarrow a > b \vee a = b,$$

есть отношение линейного, нестрогого порядка.

Определение 5.1.3. Если в линейно упорядоченном множестве $\langle M;\ >\rangle$ каждое непустое подмножество имеет наименьший элемент, то систему $\langle M;\ >\rangle$ называют *вполне упорядоченным множеством,* а отношение $>$ — *отношением полного порядка.*

Во вполне упорядоченном множестве любое непустое подмножество, из двух элементов в частности, имеет наименьший элемент. Поэтому для любой пары $\langle a, b\rangle$ различных элементов вполне упорядоченного множества $\langle A;\ >\rangle$ хотя бы одно из соотношений $a > b$ или $b > a$ верно. Отсюда следует, что полный порядок всегда линейный.

Пример 5.1.4. Порядок $>$ (больше) во множестве натуральных чисел является полным.

Пусть система $\mathbf{A} \rightleftharpoons \langle A;\ >\rangle$ — вполне упорядоченное множество; $a \in A$. Множество

$$P_a \rightleftharpoons \{x \mid x \in A,\ a > x,\ x \neq a\},$$

т. е. множество всех нижних граней множества $\{a\}$, неравных a, называют *интервалом, отделенным элементом* a или, короче, *интервалом упорядоченного множества* $\mathbf{A}$.

Если a — минимальный элемент множества $\mathbf{A}$, то $P_a = \varnothing$.

Теорема 5.1.1. (принцип *трансфинитной индукции*). Пусть система $\mathbf{A} \rightleftharpoons \langle A;\ >\rangle$ — вполне упорядоченное множество. Любое подмножество M множества A содержит A, если

$$\forall (a \in A)\quad P_a \subset M \Rightarrow a \in M; \qquad (5.1.1)$$

другими словами, если для каждого элемента a множества A из принадлежности к множеству M всех элементов интервала P_a следует, что и элемент a принадлежит M.

Доказательство. Пусть $M' \rightleftharpoons A \setminus M$, т. е. теоретико-множественная разность множеств A и M. Если $M' = \varnothing$ пусто, то $A = M$ и доказывать нечего. Если $M' \neq \varnothing$, то, так как $\mathbf{A}$ — вполне упорядоченное множество, множество M' содержит наименьший

элемент m. В таком случае, все элементы, предшествующие m и отличные от m, не принадлежат M' и, значит, принадлежат M. Таким образом, $P_m \subset M$. Поэтому в силу (5.1.1) $m \in M$, и, следовательно, $\neg\, m \in M'$, в противоречие с предположением.

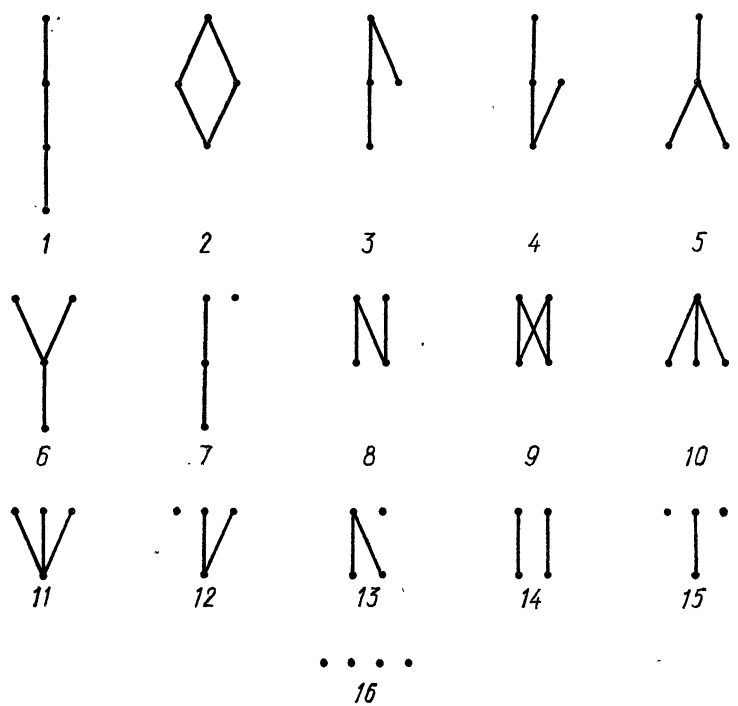
В 1904 г. итальянский математик *Цермело* доказал следующую теорему.

Теорема 5.1.2. Во всяком множестве можно ввести полный порядок.

Следует заметить, что доказательство Цермело неэффективно в том смысле, что позволяет установить существование полного порядка в данном множестве, но не дает указания, как узнать для какой-нибудь пары элементов данного множества, какой из этих элементов предшествует второму в этом порядке.

Пусть $\langle A; \succ \rangle$ — строго (или нестрого) упорядоченное множество. Мы будем предполагать, что A — конечное множество. С каждым элементом a множества A сопоставим какую-нибудь точку $T(a)$ данной плоскости так, что если элемент a непосредственно следует за элементом b, то точку $T(a)$ будем располагать выше точки $T(b)$ и соединять их отрезком. В результате мы получим граф, отвечающий данному упорядоченному множеству.

Различные типы строго (нестрого) упорядоченных четырехэлементных множеств изображаются следующими графами:



Граф 1 отвечает линейному порядку, остальные — частичному.

Вопросы: 5.1.5*. Сколькими способами можно определить линейный порядок на множестве из трех элементов? линейный и строгий? линейный и нестрогий?

5.1.6. Построить граф, отвечающий порядку «включение» во множестве всех подмножеств четырехэлементного множества, и назвать максимальный и минимальный элементы относительно этого порядка.

5.1.7. Построить граф, отвечающий порядку — отношению делимости во множестве всех натуральных чисел от 1 до 16, и назвать максимальные и минимальные элементы относительно этого порядка.

5.1.8*. Пусть $\mathbf{A} \rightleftharpoons \langle A; \succ \rangle$ — вполне упорядоченное множество; $B \subset A$. Доказать, что система $\langle B; \succ \rangle$ — вполне упорядоченное множество.

5.1.9. Пусть $\mathbf{A} \rightleftharpoons \langle A; \succ \rangle$ — вполне упорядоченное множество; P_a — интервал системы **A**. Доказать, что любой интервал системы $\langle P_a; \succ \rangle$ является интервалом системы **A**.

5.1.10. Доказать, что любой интервал вполне упорядоченного множества есть его собственное подмножество.

5.1.11*. Пусть $\mathbf{A} \rightleftharpoons \langle A; \succ \rangle$ — вполне упорядоченное множество; $b \in A$, $c \in A$. Доказать, что

$$b \succ c \Leftrightarrow P_c \subset P_b$$

в случае, если порядок $\succ$ нестрогий.

5.1.12*. Пусть $\mathbf{A} \rightleftharpoons \langle A; \succ \rangle$ —вполне упорядоченное множество; $b \in A$, $c \in A$. Доказать, что или $P_b = P_c$, или $P_b \subset P_c$, или $P_c \subset P_b$.

5.1.13*. Пусть $\mathbf{A} \rightleftharpoons \langle A; \succ \rangle$ — вполне упорядоченное множество; $B \subset A$. Доказать, что B — интервал системы **A** тогда и только тогда, если

$$\forall (x \in B) \quad \forall (y \in A \setminus B) \quad y \succ x.$$

5.1.14*. Пусть φ— изоморфное отображение вполне упорядоченного множества $\langle A; \succ \rangle$ на его подмножество $\langle B; \succ \rangle$. Доказать, что

$$\forall (a \in A) \quad \varphi(a) \succ a \; \varphi(a) = a.$$

5.1.15*. Пусть $\mathbf{A} \rightleftharpoons \langle A; \succ \rangle$— вполне упорядоченное множество; P_a — интервал системы **A**. Доказать, что системы **A** и $\langle P_a; \succ \rangle$ неизоморфны.

5.1.16. Пусть $\mathbf{A} \rightleftharpoons \langle A; \succ_1 \rangle$ и $\mathbf{B} \rightleftharpoons \langle B; \succ_2 \rangle$ — вполне упорядоченные множества такие, что $A \cap B = \varnothing$. Во множестве $A \cup B$ определим бинарное отношение $\succ$ следующими условиями:

1) если $a, b \in A$, то

$$a \succ b \Leftrightarrow a \succ_1 b;$$

2) если $a, b \in B$, то

$$a \succ b \Leftrightarrow a \succ_2 b;$$

3) если $a \in A$, $b \in B$, то

$$a \succ b.$$

Доказать, что система $\langle A \cup B;\ \succ\rangle$ — вполне упорядоченное множество.

5.1.17. Пусть $\mathbf{A} \rightleftharpoons \langle A;\ \succ_1\rangle$ и $\mathbf{B} \rightleftharpoons \langle B;\ \succ_2\rangle$ — вполне упорядоченные множества. Во множестве $A \times B$ определим бинарное отношение $\succ$ следующим условием:

$$\langle a_1,\ b_1\rangle \succ \langle a_2,\ b_2\rangle \Leftrightarrow a_1 \succ_1 a_2 \vee (a_1 = a_2 \wedge b_1 \succ_2 b_2).$$

Доказать, что система $\langle A \times B;\ \succ\rangle$ — вполне упорядоченное множество.

Для каждого вполне упорядоченного множества $\mathbf{A} \rightleftharpoons \langle A;\ \succ\rangle$ символом $\overline{\mathbf{A}}$ обозначаем новый объект, называемый *порядковым числом вполне упорядоченного множества,* и такой, что для любых вполне упорядоченных множеств **A** и **B**

$$\overline{\mathbf{A}} = \overline{\mathbf{B}}$$

в том и только том случае, если системы **A** и **B** изоморфны. Пусть $\alpha \rightleftharpoons \overline{\mathbf{A}}$, $\beta \rightleftharpoons \overline{\mathbf{B}}$; Тогда:

а) говорят, что $\alpha < \beta$ (α меньше β), если система **A** изоморфно отображается на некоторый интервал системы **B**; говорят, что $\alpha \leqslant \beta$, если $\alpha < \beta$ или $\alpha = \beta$;

б) под *суммой* $\alpha + \beta$ понимают порядковое число системы $\langle A \cup B;\ \succ\rangle$, если $A \cap B = \varnothing$ и отношение $\succ$ определено, как в условии вопроса 5.1.16;

в) под *произведением* $\alpha \cdot \beta$ понимают порядковое число системы $\langle B \times A;\ \succ\rangle$, если отношение $\succ$ определено, как в условии вопроса 5.1.17.

Порядковое число конечного вполне упорядоченного множества называют *конечным порядковым числом.*

Порядковое число называют *предельным,* если оно не имеет непосредственно предшествующего; другими словами, если между данным порядковым числом и любым, меньшим его, можно вставить третье порядковое число.

Для любого порядкового числа $\alpha \rightleftharpoons \overline{\mathbf{A}}$ символом $|\alpha|$ условимся обозначать кардинальное число множества A.

Вопросы: 5.1.18. Пусть α, β, γ — порядковые числа. Доказать, что:

1) $\neg\, \alpha < \alpha$;
2) $\alpha \leqslant \beta \wedge \beta \leqslant \alpha \Rightarrow \alpha = \beta$;
3) $\alpha < \beta \wedge \beta < \gamma \Rightarrow \alpha < \gamma$;
4) $\alpha < \beta \Rightarrow \alpha + \gamma < \beta + \gamma \wedge \gamma + \alpha < \gamma + \beta$;
5) $\alpha \leqslant \beta \Rightarrow \alpha \cdot \gamma \leqslant \beta \cdot \gamma \wedge \gamma \cdot \alpha \leqslant \gamma \cdot \beta$.

Пусть α — порядковое число; символом $W(\alpha)$ мы обозначаем множество всех порядковых чисел, строго меньших числа α. Таким образом, если α — порядковое число, то

$$\beta \in W(\alpha) \Leftrightarrow \beta < \alpha.$$

5.1.19*. Доказать, что система $\langle W(\alpha); \leqslant\rangle$ — вполне упорядоченное множество, а его порядковое число равно α.

5.1.20*. Доказать, что для любых порядковых чисел α и β

$$\neg W(\alpha) \subset W(\beta) \Rightarrow W(\beta) \subset W(\alpha).$$

5.1.21. Доказать, для для любых порядковых чисел α и β

$$\alpha \neq \beta \wedge \neg \alpha < \beta \Rightarrow \beta < \alpha.$$

5.1.22. Из теоремы Цермело вывести, что для любых кардинальных чисел $\mathfrak{a}$ и $\mathfrak{b}$

$$\mathfrak{a} \neq \mathfrak{b} \wedge \neg \mathfrak{a} < \mathfrak{b} \Rightarrow \mathfrak{b} < \mathfrak{a}.$$

5.1.23. Пусть $\mathfrak{a}$ — кардинальное число, $\Omega(\mathfrak{a})$ — множество всех кардинальных чисел, строго меньших кардинального числа $\mathfrak{a}$. Доказать, что система $\langle \Omega(\mathfrak{a}); \leqslant\rangle$ — вполне упорядоченное множество.

5.1.24. Пусть α — порядковое число; $S \rightleftharpoons W(\alpha)$; S' — множество всех предельных чисел множества S. Доказать, что:

1) любое порядковое число α из множества S можно представить и только одним способом в виде

$$\alpha = \beta + k, \tag{5.1.2}$$

где β — предельное число множества S, k — конечное порядковое число;

2) любое порядковое число, представимое в виде (5.1.2), принадлежит S;

3) $\mathfrak{a}_0 |S'| = |S|$.

5.1.25*. Пусть $\mathfrak{a}$ и $\mathfrak{b}$ —кардинальные числа такие, что $\mathfrak{b} \leqslant \mathfrak{a}$ и $\mathfrak{a}_0 \leqslant \mathfrak{a}$. Доказать, что

$$\mathfrak{b} + \mathfrak{a} = \mathfrak{a}.$$

5.1.26. Пусть α, z и γ — порядковые числа $|\alpha| = \mathfrak{a} \geqslant \mathfrak{a}_0$; $S \rightleftharpoons W(\alpha)$, $z, \gamma \in S$;

$$U \rightleftharpoons \{\langle x, y\rangle \mid x, y \in S\};$$
$$A_\gamma \rightleftharpoons \{\langle \gamma, y\rangle \mid y \in S\};$$
$$B_z \rightleftharpoons \{\langle x, y\rangle \mid x, y \in S,\ x + y = z\}.$$

Доказать, что:

1) $|U| = \mathfrak{a} \cdot \mathfrak{a}$;
2) $|A_\gamma| = |\mathfrak{a}|$;
3) $|B_z| < \mathfrak{a}$.

5.1.27*. Пусть $\mathfrak{a}$ и $\mathfrak{b}$ — кардинальные числа такие, что $\mathfrak{b} \leqslant \mathfrak{a}$ и $\mathfrak{a}_0 \leqslant \mathfrak{a}$. Доказать, что

$$\mathfrak{b} \cdot \mathfrak{a} = \mathfrak{a}.$$

5.2. Упорядоченные полугруппы

Определение 5.2.1. *Упорядоченной полугруппой* называют систему $\langle A;\ +,\ \succ\rangle$ в случае, если:

1) система $\langle A;\ +\rangle$ — полугруппа;

2) система $\langle A;\ \succ\rangle$ — упорядоченное множество;

3) отношение $\succ$ монотонно относительно групповой операции, т. е.

$$\forall (a,\ b,\ c \in A)\quad a \succ b \Rightarrow a + c \succ b + c \wedge c + a \succ c + b.$$

Упорядоченную полугруппу $\langle A;\ +,\ \succ\rangle$ называют упорядоченной группой в случае, если система $\langle A;\ +\rangle$ — группа.

Пусть система $\langle A;\ +,\ \succ\rangle$ — упорядоченная полугруппа; если порядок $\succ$ линеен во множестве A, то упорядоченную полугруппу $\langle A;\ +,\ \succ\rangle$ называют *линейно упорядоченной*. Видимо, без пояснений понятны термины: *линейно упорядоченная группа, частично упорядоченная полугруппа, частично упорядоченная группа, строго упорядоченная полугруппа* и т. д.

Примеры: 5.2.1. Рассмотрим полугруппу примера 2.5.1. Во множестве A введем отношение $\succ$ следующим образом:

$$e \succ a,\quad a \succ a,\quad \neg\, e \succ e,\quad \neg\, a \succ e.$$

Легко заметить, что система $\langle A;\ \cdot,\ \succ\rangle$ — линейно упорядоченная полугруппа. При этом порядок $\succ$ в A не является ни строгим, ни нестрогим.

5.2.2. Рассмотрим в кольце многочленов от неизвестных $x_1, \ldots, x_n$ над каким-либо полем мультипликативную полугруппу, состоящую из многочленов вида

$$x_1^{a_1} \cdot \ldots \cdot x_n^{a_n},$$

где $a_1, \ldots, a_n$ — неотрицательные целые числа. Введем в указанной полугруппе порядок $\succ$ следующим лексикографическим соглашением:

$$x_1^{a_1} \cdot \ldots \cdot x_n^{a_n} \succ x_1^{b_1} \cdot \ldots \cdot x_n^{b_n} \overset{\text{Df}}{\Leftrightarrow}$$

$$\overset{\text{Df}}{\Leftrightarrow} a_1 \succ b_1 \vee (a_1 = b_1 \wedge a_2 \succ b_2) \vee (a_1 = b_1 \wedge a_2 = b_2 \wedge a_3 \succ b_3) \vee \ldots$$

Легко проверить, что введенное бинарное отношение связно, антирефлексивно, антисимметрично, транзитивно и монотонно относительно умножения.

5.2.3. Пусть $\mathbf{N} \rightleftharpoons \langle N;\ +,\ \cdot,\ 1\rangle$ — система натуральных чисел. Отношение делимости $\vdots$ в N антисимметрично, транзитивно, рефлексивно и монотонно относительно умножения. Поэтому система $\langle N;\ \cdot,\ \vdots\rangle$ — частично упорядоченная полугруппа.

5.2.4. Пусть $\mathbf{N} \rightleftharpoons \langle N;\ +,\ \cdot, 1\rangle$ — система натуральных чисел; ω_1 — множество пар $\langle a,\ b\rangle$ натуральных чисел с условием, что $a = b + x$ для некоторого x из N; ω_2 — множество пар $\langle a,\ b\rangle$ натуральных чисел таких, что $a = b$ или $a = b + x$ для некоторого

x из N; ω_3 — множество пар $\langle a, b\rangle$ натуральных чисел с условием, что $a = b + x$ для некоторого x из N или $a = b$ для всех $a \neq 1$. Легко видеть, что каждая из систем $\langle N ; +, \omega_1\rangle$, $\langle N; +, \omega_2\rangle$ и $\langle N; +, \omega_3\rangle$ является линейной упорядоченной полугруппой; при этом первая является строго упорядоченной, вторая — нестрого упорядоченной, третья — ни той, ни другой.

5.2.5. Пусть A — множество натуральных, не равных единице, чисел, ω — множество пар $\langle a, b\rangle$ чисел из A таких, что $b \neq 3$ и $a = b + x$ для некоторого натурального x. Легко проверить, что система $\langle A; +, \omega\rangle$ — частично и строго упорядоченная полугруппа.

Группу из двух элементов линейно и строго упорядочить нельзя. В самом деле, если 0 и 1 — ее элементы (0 — нуль группы), то имеем:

$$0 + 0 = 1 + 1 = 0; \quad 1 + 0 = 0 + 1 = 1.$$

Предположим, что $1 > 0$. Тогда получим $0 = 1 + 1 = 0 + 1 = 1$.

Вопрос 5.2.1. Доказать, что всякую линейно упорядоченную полугруппу с сокращением можно линейно и строго упорядочить.

Легко доказываются следующие теоремы:

Теорема 5.2.1. Если $\langle A; +, >\rangle$ — упорядоченная полугруппа, то

$$\forall (a, b, a', b' \in A) \quad a > b \wedge a' > b' \Rightarrow a + a' > b + b'.$$

Теорема 5.2.2. Если $\langle A; +, >\rangle$ — упорядоченная полугруппа, n — натуральное число, то

$$\forall (a, b \in A) \quad a > b \Rightarrow n * a > n * b.$$

В частности, если $\langle A; +, >\rangle$ — линейно и строго упорядоченная полугруппа, то

$$\forall (a, b \in A) \quad a > b \Leftrightarrow n * a > n * b.$$

Следствие 1. Если a, b, n — натуральные числа, то

$$a > b \Leftrightarrow a^n > b^n.$$

Следствие 2. Если a, b, n — натуральные числа, то

$$a \vdots b \Rightarrow a^n \vdots b^n.$$

Теорема 5.2.3. Если $\langle A; +, >\rangle$ — линейно и строго упорядоченная полугруппа, то:

1) $\forall (a, b, c \in A) \quad (a + c = b + c \Leftrightarrow a = b \Leftrightarrow c + a = c + b)$;

2) $\forall (a, b, c \in A) \quad (a + c > b + c \Leftrightarrow a > b \Leftrightarrow c + a > c + b)$.

Итак, всякая линейно и строго упорядоченная полугруппа — полугруппа с сокращением.

Теорема 5.2.4. Если $\langle A; +, >\rangle$ — линейно и строго упорядоченная полугруппа, то:

1) $\forall (a, x \in A) \quad (a + x = x \Leftrightarrow a + a = a \Leftrightarrow x + a = x)$;

2) $\forall (a, x \in A) \quad (a + x > x \Leftrightarrow a + a > a \Leftrightarrow x + a > x)$;

3) $\forall (a, x \in A) \quad (x > a + x \Leftrightarrow a > a + a \Leftrightarrow x > x + a)$.

Для примера докажем одно из соотношений. Из теоремы 5.2.3 следует, что каковы бы ни были элементы a и x множества A,

$$a + x > x \Leftrightarrow a + a + x > a + x \Leftrightarrow a + a > a.$$

Таким образом,

$$a + x > x \Leftrightarrow a + a > a.$$

Определение 5.2.2. Пусть $\langle A; +, > \rangle$ — упорядоченная полугруппа. *Элемент a множества A называют положительным (отрицательным), если $a + a \neq a$ и $a + a > a$ (соответственно $a > a + a$).*

Теорема 5.2.5. Пусть $\langle A; +, > \rangle$ — линейно и строго упорядоченная полугруппа, $a \in A$ и $a + a \neq a$. Тогда элементы:

$$a,\ 2 * a,\ 3 * a,\ \ldots$$

все различны. Если, при тех же предположениях, система $\langle A; +, 0, > \rangle$ — группа, то все различны и элементы:

$$0,\ a,\ -a,\ 2 * a,\ -2 * a,\ 3 * a,\ -3 * a,\ \ldots$$

Доказательство. Если $a + a > a$, то индукцией по натуральному n легко доказать, что

$$\forall (n \in N) \quad (n + 1) * a > a.$$

А отсюда следует, что

$$\forall (n,\ m \in N) \quad (n + m) * a > m * a$$

и, следовательно,

$$\forall (n,\ m \in N) \quad (n + m) * a \neq m * a.$$

Второе утверждение теоремы доказывается без труда.

Теорема 5.2.6. Конечную полугруппу с сокращением, если число ее элементов $n \geqslant 2$, нельзя линейно упорядочить.

Доказательство. Вопрос 5.2.1 и теорема 5.2.5.

Теорема 5.2.7. Полугруппу с сокращением и с конечной подполугруппой из $n \geqslant 2$ элементов нельзя линейно упорядочить.

Теорема 5.2.8. Пусть $\langle A; +, > \rangle$ — линейно упорядоченная группа. Тогда

$$\forall (a,\ b \in A) \quad a > a \Leftrightarrow b > b.$$

Таким образом, всякая линейно упорядоченная группа либо строго, либо нестрого упорядочена. В любом из этих случаев, как легко проверить, можно говорить о двух отношениях линейного порядка в данной группе — строгом и нестрогом (вопросы 5.1.3 и 5.1.4). Знаком $>$ пользуются для обозначения первого из этих отношений и знаком $\geqslant$ — для обозначения второго из них.

Часто бывает полезной следующая теорема.

Теорема 5.2.9. Если система $\mathbf{A}$ — линейно упорядоченная группа, то

$$\forall (a,\ b,\ c,\ x \in A) \quad c \geqslant a > b \geqslant x \Rightarrow a - b \leqslant c - x.$$

Вопросы: 5.2.2. Доказать, что любое непустое конечное множество элементов упорядоченной полугруппы имеет наибольший и наименьший элементы.

5.2.3. Доказать, что упорядоченная полугруппа линейно упорядочена в том и только в том случае, если любое конечное множество ее элементов имеет и только один наибольший элемент.

5.2.4*. Доказать, что сумма положительных элементов коммутативной полугруппы с сокращением положительна.

5.2.5*. Доказать, что сумма положительных элементов линейно и строго упорядоченной полугруппы положительна.

5.2.6. Доказать, что всякий элемент линейно и строго упорядоченный полугруппы, больший положительного элемента, сам является положительным.

5.2.7*. Доказать, что элемент упорядоченной коммутативной полугруппы с сокращением, больший положительного элемента, не обязательно положителен.

5.2.8. Доказать, что множество положительных элементов линейно упорядоченной группы не пусто.

5.2.9*. Пусть $\mathbf{A} \rightleftharpoons \langle A; +, 0, \succ\rangle$— линейно и строго упорядоченная группа. Доказать, что элемент a системы **A** тогда и только тогда положителен, если $a \succ 0$.

5.2.10. Доказать, что существует и только один линейный и строгий порядок в аддитивной полугруппе натуральных чисел, в котором множество положительных элементов не пусто.

5.2.11. Доказать, что существует бесконечно много линейных и строгих порядков в мультипликативной полугруппе натуральных чисел с непустым множеством положительных элементов.

5.2.12. Доказать, что мультипликативную полугруппу целых чисел нельзя линейно упорядочить.

5.3. Упорядоченные полукольца

Определение 5.3.1. Систему $\mathbf{A} \rightleftharpoons \langle A; +, \cdot, \succ\rangle$ называют *упорядоченным полукольцом,* если выполняются следующие условия:

1) система $\langle A; +, \cdot\rangle$ — полукольцо;

2 система $\langle A; +, \succ\rangle$ — упорядоченная полугруппа с непустым множеством A^+ положительных элементов;

3) $\forall (a, b \in A) \forall (c \in A^+) \quad a \succ b \Rightarrow ac \succ bc \wedge ca \succ cb.$

Положительным элементом упорядоченного полукольца **A** называют любой положительный элемент упорядоченной полугруппы $\langle A; +, \succ\rangle$. Упорядоченное полукольцо $\mathbf{A} \rightleftharpoons \langle A; +, \cdot, \succ\rangle$ называют *упорядоченным кольцом* (телом, полем), если полукольцо $\langle A; +, \cdot\rangle$ — кольцо (соответственно тело, поле).

Определение 5.3.2. Пусть $\mathbf{A} \rightleftharpoons \langle A; +, \cdot, \succ\rangle$ — упорядоченное полукольцо. Порядок $\succ$ системы **A** называют *архимедовым,* а систе-

му $\mathbf{A}$ — *архимедовски упорядоченной,* если, каковы бы ни были положительные элементы a и b системы $\mathbf{A}$, можно указать такое натуральное число n, что

$$n * a \rightleftharpoons \sum_{1}^{n} a \succ b.$$

Пример 5.3.1. В кольце F примера 2.6.5 определим отношение $\succ$ («выше») условием

$$\forall (f,\ g \in F) \quad f \succ g \Leftrightarrow \forall (x \in [-1,\ 1]) \quad f(x) \geqslant g(x).$$

Нетрудно доказать, что система $\langle F;\ +,\ \cdot,\ \succ \rangle$ — неархимедовски, частично и нестрого упорядоченное кольцо.

Пример 5.3.2. В кольце примера 2.6.8 определим отношение $\succ$, как в примере 5.3.1. Легко убедиться, что в данном кольце это отношение является архимедовым, частичным и нестрогим.

Определение 5.3.3. Пусть $\mathbf{A} \rightleftharpoons \langle A; +, \cdot, \succ \rangle$ и $\mathbf{A}_1 \rightleftharpoons \langle A_1; +, \cdot, \succ \rangle$ — упорядоченные полукольца, и полукольцо $\langle A_1;\ +,\ \cdot \rangle$ — расширение полукольца $\langle A;\ +,\ \cdot \rangle$. Порядок $\succ$ в A_1 называют *продолжением порядка* в A (или говорят, что порядок в A *индуцирован* порядком в A_1), если

$$\forall (a,\ b \in A) \quad a \succ b \Leftrightarrow a \succ_1 b.$$

Теорема 5.3.1. Пусть $\mathbf{A} \rightleftharpoons \langle A;\ +,\ \cdot,\ \succ \rangle$ — линейно и строго упорядоченное полукольцо, a и b — положительные элементы системы $\mathbf{A}$. Тогда

$$\forall (a',\ b' \in A) \quad a' \succ a \wedge b' \succ b \Rightarrow a'b' \succ ab.$$

Пример 5.3.1. Полукольцо натуральных чисел с отношением $\succ$ (больше) — линейно и строго упорядоченное полукольцо.

Теорема 5.3.2. Пусть система $\mathbf{A} \rightleftharpoons \langle A;\ +,\ \cdot,\ \succ \rangle$ — упорядоченное полукольцо; система $\langle A_1;\ \oplus,\ \odot \rangle$ — полукольцо; φ — изоморфное отображение полукольца $\langle A;\ +,\ \cdot \rangle$ на полукольцо $\langle A_1;\ \oplus,\ \odot \rangle$; $\succ_1$— бинарное отношение во множестве A_1, наведенное отношением $\succ$ в отображении φ множества A на множество A_1. Тогда:

1) система $\mathbf{A}_1 \rightleftharpoons \langle A_1;\ \oplus,\ \odot,\ \succ_1 \rangle$— упорядоченное полукольцо;

2) порядок в системе $\mathbf{A}_1$ строгий тогда и только тогда, если порядок в системе $\mathbf{A}$ строгий;

3) порядок в системе $\mathbf{A}_1$ архимедов тогда и только тогда, если порядок в системе $\mathbf{A}$ архимедов;

4) порядок в системе $\mathbf{A}_1$ линеен тогда и только тогда, если порядок в системе $\mathbf{A}_1$ линеен.

Доказательство. В самом деле, имеем

$$\forall (a,\ b \in A) \quad \varphi(a) \succ_1 \varphi(b) \overset{\text{Df}}{\Leftrightarrow} a \succ b.$$

Пусть теперь $\varphi(a) \succ_1 \varphi(b)$ и $\varphi(b) \succ_1 \varphi(a)$. Тогда $a \succ b$ и $b \succ a$. Следовательно, $a = b$ и $\varphi(a) = \varphi(b)$.

Аналогично доказываются и другие утверждения.

5.4. Линейно упорядоченные кольца и тела

Для линейно упорядоченного кольца $\mathbf{A} \Leftrightarrows \langle A;\ +,\ \cdot,\ 0,\ \succ\rangle$ система $\langle A;\ +,\ 0,\ \succ\rangle$ — линейно упорядоченная группа. Отсюда легко следует, что порядок $\succ$ либо строгий, либо нестрогий. Во множестве A можно ввести (вопросы 5.1.3 и 5.1.4) новый линейный порядок $\succ_1$, который будет строгим, если порядок $\succ$ нестрогий, и — нестрогим, если порядок $\succ$ строгий. Легко проверить, что система $\langle A;\ +,\cdot,\ 0,\ \succ_1\rangle$, как и система $\mathbf{A}$, является линейно упорядоченным кольцом.

В связи с этим замечанием в линейно упорядоченном кольце $\mathbf{A}$ обычно рассматривают два бинарных отношения порядка, одно из которых — строгое — обозначают знаком $>$, а второе — нестрогое — знаком $\geqslant$. Итак, в линейно упорядоченном кольце $\mathbf{A}$:

$$\forall (a,\ b \in A)\quad a > b \Leftrightarrow a \neq b \wedge a \succ b;$$

$$\forall (a,\ b \in A)\quad a \geqslant b \Leftrightarrow a = b \vee a \succ b.$$

Из сказанного следует, что в данном кольце можно ввести линейный порядок тогда и только тогда, если в нем можно ввести линейный и строгий порядок.

Для дальнейшего полезно напомнить, что в линейно упорядоченном кольце (вопрос 5.2.9) элемент a положителен тогда и только тогда, если $a > 0$.

Теорема 5.4.1. Пусть система $\langle A;\ +,\ \cdot,\ 0,\ >\rangle$ — линейно упорядоченное кольцо. Тогда для любого элемента a из A либо $a = 0$, либо $a > 0$, либо $-a > 0$.

Доказательство этой теоремы, как и следующей, несложно. Следует только подчеркнуть, что знак $>$ обозначает отношение строгого порядка.

Теорема 5.4.2. Сумма и произведение положительных элементов линейно упорядоченного кольца положительны.

Теорема 5.4.3. Линейно упорядоченное кольцо не имеет делителей нуля.

Доказательство. В самом деле, если a и b — не равные нулю элементы упорядоченного кольца, то возможны только следующие случаи:

1) $a > 0,\ b > 0$;
2) $a > 0,\ -b > 0$;
3) $-a > 0,\ b > 0$;
4) $-a > 0,\ -b > 0$.

Отсюда следует, что либо $ab > 0$, либо $0 > ab$.

Теорема 5.4.4. В линейно упорядоченном кольце квадрат любого не равного нулю элемента положителен.

Доказательство. Если $a > 0$, то $a^2 > 0$. Если $-a > 0$, то $a^2 = (-a)\,(-a) > 0$.

Эту теорему полезно сформулировать и так: в любом линейном порядке кольца квадрат его не равного нулю элемента положителен.

Теорема 5.4.5. В линейно упорядоченном кольце сумма квадратов его не равных нулю элементов не равна нулю.

Теорема 5.4.6. В линейно упорядоченном теле $\langle T;\ +,\ \cdot,\ 0,\ e, >\rangle$, $e > 0$.

Теорема 5.4.7. Если $\mathbf{T} \rightleftharpoons \langle T;\ +,\ \cdot,\ 0,\ e,\ >\rangle$ — линейно упорядоченное тело, то:

1) $\forall (a,\ b \in T)\quad a > 0 \wedge b > 0 \Rightarrow a \cdot b^{-1} > 0 \wedge b^{-1} \cdot a > 0;$

2) $\forall (a,\ b \in T)\quad a > b \Rightarrow a > (a + b)\,(2e)^{-1} > 0.$

Теорема 5.4.8. Если $\mathbf{T} \rightleftharpoons \langle T;\ +,\ \cdot,\ 0,\ e, >\rangle$ — линейно упорядоченное тело, $\mathbf{N} \rightleftharpoons \langle N;\ +,\ \cdot,\ 1\rangle$ — система натуральных чисел, то

$$\forall (a \in T)\quad \forall (n \in N)\quad a > 0 \Rightarrow a > \frac{a}{(n+1) * e} > 0.$$

Теорема 5.4.9. Если $\mathbf{T} \rightleftharpoons \langle T;\ +,\ \cdot\ 0,\ e,\ >\rangle$ — архимедовски линейно упорядоченное тело, $\mathbf{N} \rightleftharpoons \langle N;\ +,\ \cdot,\ 1\rangle$ — система натуральных чисел, то

$$\forall (a,\ b \in T)\quad \exists (n,\ m \in N)\quad a > b \geqslant 0 \Rightarrow a > \frac{n * e}{m * e} > b.$$

Доказательство. Имеем $a - b > 0$. Поэтому $(a - b)^{-1} > 0$. Далее находим натуральное m такое, что $m * e > (a - b)^{-1}$. Легко видеть, что

$$(m * e)^{-1} < a - b \leqslant a.$$

Пусть теперь k — целое такое, что $k * (m * e)^{-1} \geqslant a$. Тогда $k \neq 1$. Выбираем наименьшее натуральное n с условием $(n + 1) * (m * e)^{-1} \geqslant a$. Неравенства

$$(n + 1) * (m * e)^{-1} \geqslant a > b \geqslant n * (m * e)^{-1}$$

в силу теоремы 5.2.9 невозможны. Поэтому $a > n * (m * e)^{-1} > b$.

Определение 5.4.1. Пусть $\mathbf{A} \rightleftharpoons \langle A;\ +,\ \cdot\ 0, >\rangle$ — линейно упорядоченное кольцо; a — элемент системы **A**. *Абсолютным значением* элемента a называют $\max(a, -a)$.

Обозначение. $|a| \rightleftharpoons \max(a, -a)$.

Замечание. Поскольку кольцо, вообще говоря, может быть линейно упорядочено несколькими способами, абсолютное значение элемента зависит не только от элемента, но и от порядка в кольце.

Теорема 5.4.10. Пусть $\mathbf{A} \rightleftharpoons \langle A;\ +,\ \cdot, 0, >\rangle$ — линейно упорядоченное кольцо. Тогда:

1) $\forall (a \in A)\quad |a| = 0 \Leftrightarrow a = 0;$
2) $\forall (a \in A)\quad |a| > 0 \Leftrightarrow a \neq 0;$
3) $\forall (a \in A)\quad |a| = |-a|;$
4) $\forall (a \in A)\quad a \leqslant |a| \wedge -a \leqslant |a|;$
5) $\forall (a,\ b \in A)\quad |a + b| \leqslant |a| + |b|;$

6) $\forall (a,\ b \in A)\quad |a \cdot b| = |a| \cdot |b|$;
7) $\forall (a,\ b \in A)\quad |a| \leqslant b \Leftrightarrow -b \leqslant a \leqslant b$;
8) $\forall (a,\ b,\ k,\ l \in A)\quad l \leqslant a \leqslant k \wedge l \leqslant b \leqslant k \Rightarrow |a - b| \leqslant k - l$.

Доказательство. Соотношения 1—4 прямо следуют из определения. Далее имеем

$$a \leqslant |a| \wedge b \leqslant |b| \Rightarrow a + b \leqslant |a| + |b|.$$

Аналогично: $-(a + b) \leqslant |a| + |b|$. Отсюда получим

$$|a + b| \leqslant |a| + |b|.$$

Легко доказать и другие соотношения.

Теорема 5.4.11. (*критерий порядка*). Кольцо $\langle A;\ +,\ \cdot,\ 0\rangle$ тогда и только тогда можно линейно и строго упорядочить (т. е. ввести линейный и строгий порядок), если множество A имеет подмножество A^+, удовлетворяющее условиям:

1) $\forall (a \in A)\quad a \in A^+ \Rightarrow a \neq 0 \wedge -a \notin A^+$;

$$a \neq 0 \Rightarrow a \in A^+ \vee -a \in A^+;$$

2) $\forall (a,\ b \in A^+)\quad a + b \in A^+ \wedge a \cdot b \in A^+$.

Доказательство. Пусть сначала $\mathbf{A} \rightleftarrows \langle A;\ +,\ \cdot,\ 0,\ >\rangle$ — линейно упорядоченное кольцо. В роли искомого подмножества A^+ в таком случае в силу теорем 5.4.1 и 5.4.2 может выступить множество положительных элементов системы **A**.

Пусть теперь A^+ — подмножество кольца $\langle A;\ +,\ \cdot,\ 0\rangle$, удовлетворяющее условиям теоремы. Попробуем ввести линейный порядок $>$ в кольце $\langle A;\ +,\ \cdot,\ 0\rangle$. Определим это отношение так:

$$\forall (a,\ b \in A)\quad a > b \overset{\text{Df}}{\Leftrightarrow} a - b \in A^+.$$

Без особых затруднений можно проверить, что введенное нами отношение связно, антирефлексивно, антисимметрично, транзитивно, монотонно относительно сложения и умножения на любой элемент из A^+.

Множество A^+ с упомянутыми в условии теоремы 5.4.11 свойствами называют *положительной частью кольца* $\langle A;\ +,\ \cdot,\ 0\rangle$. В дальнейшем при введении порядка в каком-нибудь кольце мы будем искать в нем «положительную часть». Если такая часть в кольце существует, то кольцо можно упорядочить, если нет, то нельзя, если таких несовпадающих положительных частей несколько, то — несколькими способами.

Из сказанного следует, что при определении линейно упорядоченного кольца в качестве основного отношения вместо бинарного отношения $>$ можно брать унарное отношение «положительная часть».

Теорема 5.4.12 (*критерий однозначности линейного порядка*). Пусть A^+ и A^{++} — положительные части кольца $\langle A;\ +,\ \cdot,\ 0\rangle$.

Тогда

$$A^+ = A^{++} \Leftrightarrow A^+ \subset A^{++}.$$

Доказательство. Пусть $A^+ \subset A^{++}$ и $a \in A^{++}$. В таком случае $a \neq 0$. Поэтому $a \in A^+$ либо $-a \in A^+$. Во втором случае немедленно получим $-a \in A^{++}$. Но этого не может быть, так как уже $a \in A^{++}$.

Теорема 5.4.13 (*критерий продолжения порядка*). Пусть $\mathbf{A} \rightleftharpoons \langle A;\ +,\ \cdot,\ 0,\ > \rangle$ и $\mathbf{A}_1 \rightleftharpoons \langle A_1;\ \oplus,\ \odot,\ >_1 \rangle$ — линейно упорядоченные кольца и $\langle A;\ +,\ \cdot,\ 0 \rangle$ — подкольцо кольца $\langle A_1; \oplus, \odot \rangle$. Пусть A^+ — множество положительных элементов системы $\mathbf{A}$, а A_1^+ — системы A_1. Порядок $>$ тогда и только тогда продолжает порядок $>_1$, если

$$A^+ \subset A_1^+.$$

Доказательство. Пусть $A^+ \subset A_1^+$. Если $a,\ b \in A$ и $a > b$, то $a - b \in A^+$. Отсюда следует, что $a - b \in A_1^+$ и $a >_1 b$. Пусть $a >_1 b$. Тогда $a \neq b$ и $a - b \in A_1^+$. Если $a - b \notin A^+$, то $-(a - b) \in A^+$ и, следовательно, $-(a - b) \in A_1^+$. Но этого нет.

Пример 5.4.1 (некоммутативное линейно упорядоченное тело). Пусть Q — поле рациональных чисел. Выделим в теле примера 2.6.7 подмножество, состоящее из формальных рядов вида

$$\sum_{i \geqslant m, r \geqslant n} a_{ir} x^i y^r,$$

с условием $a_{mn} > 0$. Легко видеть, что это подмножество — положительная часть данного тела.

Пример 5.4.2 (поле с не единственным архимедовым линейным порядком). Пусть $\langle R;\ +,\ \cdot,\ 0, > \rangle$ — система действительных чисел. Рассмотрим подмножество M множества R, состоящее из чисел вида

$$a + b\sqrt{2},$$

где a и b — любые рациональные числа. Можно проверить, что $\langle M;\ +,\ \cdot,\ 0 \rangle$ — поле (вопрос 2.6.3). Полагаем:

$$M^+ \rightleftharpoons \{\alpha \mid \alpha \rightleftharpoons a + b\sqrt{2},\ a,\ b \in Q \wedge a + b\sqrt{2} > 0\};$$

$$M^{++} \rightleftharpoons \{\alpha \mid \alpha \rightleftharpoons a + b\sqrt{2},\ a,\ b \in Q \wedge a - b\sqrt{2} > 0\}.$$

Легко видеть, что M^+ и M^{++} — положительные части поля $\langle M;\ +,\ \cdot,\ 0 \rangle$. А между тем они не совпадают. В архимедовости порядков, определяемых с помощью этих частей, убедиться нетрудно.

Пример 5.4.3 (поле с неархимедовым линейным порядком). Рассмотрим поле $\mathbf{Q}(x)$ рациональных функций над полем рациональных чисел (вопрос 2.10.1). Каждый не равный нулю элемент этого поля представим в виде

$$\alpha = \frac{a_k x^k + a_{k+1} x^{k+1} + \cdots + a_{k+p} x^{k+p}}{b_r x^r + b_{r+1} x^{r+1} + \cdots + b_{r+q} x^{r+q}},$$

где $a_k, \ldots, a_{k+p}, b_r, \ldots, b_{r+q}$ — рациональные числа, k, p, r, q — неотрицательные числа, $a_k \neq 0$, $b_r \neq 0$, $a_{k+p} \neq 0$, $b_{r+q} \neq 0$. Обозначим через F^+ множество, определяемое условием

$$\forall (\alpha \in \mathbf{Q}(x)) \quad \alpha \in F^+ \overset{\text{Df}}{\Leftrightarrow} a_{k+p} \cdot b_{r+q} > 0.$$

Легко проверить, что F^+ — положительная часть поля $\mathbf{Q}(x)$. Порядок в поле $\mathbf{Q}(x)$, соответствующий этой положительной части, неархимедов. В самом деле, для любого натурального числа n

$$n \cdot 1 < x.$$

Однако порядок в поле $\mathbf{Q}(x)$ можно ввести многими способами.

Пусть F^{++} — множество, определяемое условием

$$\alpha \in F^{++} \overset{\text{Df}}{\Leftrightarrow} a_k \cdot b_r > 0.$$

Легко проверить, что и F^{++} — положительная часть поля $\mathbf{Q}(x)$.

Пусть теперь F^{+++} — множество, определяемое условием:

$$\alpha = \alpha(x) \in F^{+++} \overset{\text{Df}}{\Leftrightarrow} \alpha(\pi) > 0.$$

Если воспользоваться трансцендентностью числа π, то нетрудно показать, что и F^{+++} — положительная часть поля $\mathbf{Q}(x)$. Порядок, определяемый F^{+++}, — архимедов.

Пример 5.4.4 (числовое поле, содержащее мнимые числа, с архимедовым линейным порядком). Пусть $\langle C; +, \cdot, 0, 1, i\rangle$ — поле комплексных чисел и θ — мнимый корень уравнения $x^3 = 2$. Тогда $\mathbf{Q}(\theta)$ — поле (вопрос 2.6.23). Поле $\mathbf{Q}(\theta)$ изоморфно полю $\mathbf{Q}(\sqrt[3]{2})$ (вопрос 2.8.9). Но поле $\mathbf{Q}(\sqrt[3]{2})$, как подполе поля действительных чисел, можно упорядочить. Его порядок индуцируется порядком в поле действительных чисел. Изоморфизм φ поля $\mathbf{Q}(\sqrt[3]{2})$ на поле $\mathbf{Q}(\theta)$ позволяет ввести в поле $\mathbf{Q}(\theta)$ порядок, наведенный порядком системы

$$\langle Q(\sqrt[3]{2}); +, \cdot, > \rangle.$$

В этом порядке, например:

$$\left(\theta \rightleftharpoons -\frac{1}{2} + i\frac{\sqrt{3}}{2}\right);$$

$$1 < \frac{-1 + i\sqrt{3}}{2}\sqrt{2} < 2.$$

Вопросы: 5.4.1*. Доказать, что поле примера 5.4.2 можно упорядочить и только двумя способами.

5.4.2. Пусть $\mathbf{A} \rightleftharpoons \langle A; +, \cdot, 0, > \rangle$ — упорядоченное кольцо, a — положительный элемент этого кольца. Доказать, что

$$\forall (n \leqslant N) \quad (1 + a)^n \geqslant 1 + na.$$

§ 6. СИСТЕМЫ ЦЕЛЫХ И РАЦИОНАЛЬНЫХ ЧИСЕЛ

6.1. Первичные термины и аксиомы аксиоматической теории целых чисел

Мы исходим из **определения:**

Системой целых чисел называется минимальное кольцо, которое является расширением полукольца натуральных чисел.

Следующие термины принимаются в качестве первичных:

а) Z — множество, его элементы называем целыми числами;

б) $+$ и $\cdot$ — сложение и умножение — бинарные операции на Z;

в) 0 — нуль — нейтральный элемент сложения на Z;

г) N — подмножество Z, его элементы называем натуральными числами;

д) $\oplus$ и $\odot$ — сложение и умножение — бинарные операции на N.

В согласии с данным определением называем *системой целых чисел* систему

$$\mathbf{Z} \leftrightharpoons \langle Z;\ +,\ \cdot,\ 0,\ N,\ \oplus, \odot \rangle,$$

если она удовлетворяет тринадцати аксиомам, составляющим следующие три группы:

А

Z_{I}. $\forall (a,\ b \in Z)\ \ \exists!\, (c \in Z)\ \ a + b = c$;

Z_{II}. $\forall (a,\ b,\ c \in Z)\ \ (a + b) + c = a + (b + c)$;

Z_{III}. $\forall (a,\ b \in Z)\ a + b = b + a$;

Z_{IV}. $0 \in Z \wedge \forall (a \in Z)\ \ a + 0 = a$;

Z_{V}. $\forall (a \in Z)\, \exists (a' \in Z)\ \ a + a' = 0$;

Z_{VI}. $\forall (a,\ b \in Z)\, \exists!\, (p \in Z)\ \ a \cdot b = p$;

Z_{VII}. $\forall (a,\ b,\ c \in Z)\ \ (a \cdot b) \cdot c = a \cdot (b \cdot c)$;

Z_{VIII}. $\forall (a,\ b,\ c \in Z)\ \ (a + b)\, c = ac + bc \wedge c\,(a + b) = ca + cb$.

Б

Z_{IX}. $\langle N;\ \oplus,\ \odot \rangle$ — полукольцо натуральных чисел;

Z_{X}. $N \subset Z$;

Z_{XI}. $\forall (a,\ b \in N)\ \ a + b = a \oplus b$;

Z_{XII}. $\forall (a,\ b \in N)\ \ a \cdot b = a \odot b$.

Z_{XIII} (аксиома минимальности). Всякое подмножество M множества Z, если:

а) оно включает N и б) $\forall (a, b \in M)\ a - b \in M$ совпадает с Z.

Если $\langle Z; +, \cdot, 0, N, \oplus, \odot \rangle$ — система целых чисел, то систему $\langle Z; +, \cdot, 0 \rangle$ назовем *кольцом целых чисел,* систему $\langle Z; +, 0 \rangle$ — *аддитивной группой целых чисел,* систему $\langle Z; \cdot \rangle$ — *мультипликативной полугруппой целых чисел.*

6.2. Свойства целых чисел

Мы предполагаем, что $\mathbf{Z} \leftrightharpoons \langle Z; +, \cdot, 0, N, \oplus, \odot \rangle$ — система целых чисел. Из аксиом Z_{XI} и Z_{XII} следует, что при выполнении операций в системе **N** натуральных чисел и в системе **Z** целых чисел над натуральными числами можно не пользоваться разными знаками для обозначения операций сложения и умножения. Легко показать, что и вычитание натуральных чисел в обоих случаях, если выполнимо в N, приводит к одному результату. Поэтому мы пользуемся в дальнейшем одним знаком — для обозначения вычитания натуральных чисел, независимо от того, в каком множестве рассматривается это отношение.

Теорема 6.2.1. Всякое целое число есть разность натуральных чисел, т. е.

$$\forall (a \in Z) \quad \exists (k, l \in N) \quad a = k - l.$$

При этом

$$k - l = k' - l' \Leftrightarrow k + l' = k' + l.$$

Доказательство. Обозначим через M подмножество Z всех таких целых чисел, которые представимы в виде разности натуральных чисел. Имеем:

1) $\forall (n \in N) \quad n = (n + 1) - 1 \in M$;

2) $\forall (a, b \in M) \quad \exists (k, l, m, n \in N) \quad a = k - l \wedge b = m - n.$

Поэтому (упражнение 2.5.1)

$$a - b = (k - l) - (m - n) = (k + n) - (m + l)$$

есть разность натуральных чисел и, следовательно, принадлежит M. В силу аксиомы Z_{XIII} $M = Z$.

Теорема 6.2.2. Кольцо $\langle Z; +, \cdot \rangle$ коммутативно и с единицей.

Доказательство. Имеем:

$$(k - l) \cdot (k' - l') = (kk' + ll') - (kl' + lk');$$

$$(k' - l') \cdot (k - l) = (k'k + l'l) - (k'l + l'k).$$

Теорема 6.2.3. Каждое целое число — нуль, натуральное или противоположно натуральному.

Доказательство. Теорема 6.2.1.

Теорема 6.2.4. Кольцо целых чисел можно линейно и строго упорядочить и притом единственным способом. Порядок в кольце целых

чисел архимедов и продолжает порядок в полукольце натуральных чисел.

Доказательство. Обозначим через Z^+ множество N. Из теоремы 6.2.3 и алгебраичности операций на N следует, что Z^+ — положительная часть кольца $\langle Z; +, \cdot\rangle$. Поэтому кольцо $\langle Z; +, \cdot\rangle$ можно линейно упорядочить. Пусть Z^{++} — какая-нибудь положительная часть этого кольца. Имеем по теореме 5.4.4

$$1 = 1^2 \in Z^{++}.$$

Далее, если $n \in Z^{++}$, то и $n + 1 \in Z^{++}$. Поэтому

$$Z^+ = N \subset Z^{++}.$$

В силу теоремы 5.4.12

$$Z^+ = Z^{++}.$$

Мы имеем дальше

$$\forall (a, b \in \mathbf{N})\ a > b \Leftrightarrow a - b \in Z^+ = N.$$

Поэтому порядок в $\mathbf{Z}$ продолжает порядок в $\mathbf{N}$. Заметим, наконец, что положительными в кольце целых чисел являются только натуральные числа — элементы Z^+, а отсюда следует (вопрос 4.6.7), что порядок в кольце целых чисел архимедов.

Вопросы: 6.2.1. Доказать, что кольцо целых чисел дискретно и даже

$$\forall (a, b \in Z)\,(a > b \Rightarrow a \geqslant b + 1) \wedge (a + 1 > b \Rightarrow a \geqslant b).$$

6.2.2. Доказать, что уравнение $2x = 1$ неразрешимо в $\mathbf{Z}$.

6.2.3. Доказать, что уравнение $x^2 = 2y^2$ имеет только нулевое $\langle 0,0\rangle$ решение в $\mathbf{Z}$.

6.2.4 (теорема о делении с остатком). Доказать, что для любого целого числа a и любого натурального числа b можно найти и только одну пару целых чисел $\langle q, r\rangle$ такую, что $a = bq + r$ и $0 \leqslant r < b$.

6.2.5. Доказать, что множества Z и N равномощны.

6.2.6. Перечислить аксиомы, которые используются в доказательстве теоремы 6.2.1.

6.2.7. Доказать, что аксиомы $\mathbf{Z}_{\text{III}}$, $\mathbf{Z}_{\text{VII}}$ и $\mathbf{Z}_{\text{XII}}$ можно вывести из остальных аксиом теории целых чисел.

6.2.8. Показать, что мультипликативную полугруппу целых чисел линейно и строго упорядочить нельзя.

6.2.9. Показать, что существует только один линейный и строгий порядок в аддитивной группе целых чисел, в котором 1 — положительный элемент.

6.2.10*. Показать, что:

а) линейный порядок $\succ$ в кольце целых чисел $\langle Z; +, \cdot, 0, 1\rangle$ однозначно определяется следующими условиями:

1) $\forall (a, b \in Z)\quad a \succ b \Rightarrow a \neq b,$

2) $\forall (a, b, c \in Z) \quad a \succ b \wedge b \succ c \Rightarrow a \succ c$,

3) $\forall (a, b \in Z) \quad a \succ b \Rightarrow a + 1 \succ b + 1$,

4) $\forall (a, b \in Z) \quad a \succ b \Rightarrow a - 1 \succ b - 1$,

5) $1 \succ 0$;

б) ни одно из четырех названных выше условий не является следствием остальных.

6.2.11. Пусть $\mathbf{A} \rightleftharpoons \langle A; +, \theta \rangle$ — группа. Доказать, что

$$\forall (a \in A) \quad \forall (n \in N) \quad n * (-a) = -(n * a).$$

Целое кратное любого элемента a группы $\mathbf{A} \rightleftharpoons \langle A; +, \theta \rangle$ определяется следующими соглашениями:

1) $0 * a \rightleftharpoons \theta$;

2) $\forall (n \in N) \quad n * a \rightleftharpoons \sum_{x=1}^{n} a$;

3) $\forall (n \in N) \quad (-n) * a \rightleftharpoons n * (-a)$.

6.2.12. Пусть $\mathbf{A} \rightleftharpoons \langle A; +, \theta \rangle$ — группа. Доказать, что:

1) $\forall (a \in A) \quad \forall (u, v \in Z) \quad u * a + v * a = (u + v) * a$;

2) $\forall (a \in A) \quad \forall (u, v \in Z) \quad u * (v * a) = (u, v) * a$;

3) если группа $\mathbf{A}$ коммутативна, то

$$\forall (a, b \in A) \quad \forall (z \in Z) \quad z * (a + b) = z * a + z * b.$$

6.2.13. Пусть $\mathbf{A} \rightleftharpoons \langle A; \cdot, e \rangle$ — группа. Дать определение *целой степени* любого элемента группы $\mathbf{A}$ и сформулировать свойства целой степени, аналогичные указанным в вопросе 6.2.12.

6.2.14. Пусть $\mathbf{P} \rightleftharpoons \langle P; +, \cdot, 0, e, > \rangle$ — архимедовски линейно и строго упорядоченное поле. Доказать, что для любого элемента α поля P существует и только одно целое число a такое, что

$$a * e \leqslant \alpha < (a + 1) * e.$$

Число a с указанным в вопросе 6.2.14 свойством называют *целой частью элемента* и обозначают символом $[\alpha]$.

6.3. Категоричность системы целых чисел

Теорема 6.3.1. Аксиоматическая теория целых чисел категорична.

Доказательство. В предположении, что аксиоматическая теория целых чисел непротиворечива, мы докажем, что две любые модели, на которых выполняются все тринадцать аксиом данной теории, изоморфны. Пусть:

$\langle Z_1; +, \cdot, O_1, N_1, +, \cdot \rangle$ — одна модель нашей теории;

$\langle Z_2; \oplus, \odot, O_2, N_2, \oplus, \odot \rangle$ — вторая модель.

Операции на Z_1 и N_1, а также на Z_2 и N_2 мы обозначаем одинаковыми знаками. Любой элемент множества Z_1 снабжаем индексом 1, а любой элемент множества Z_2 — индексом 2. Мы собираемся определить изоморфное отображение первой модели на вторую. Так как $\langle N_1;\ +,\ \cdot\rangle$ и $\langle N_2;\ \oplus,\ \odot\rangle$ — полукольца натуральных чисел, то существует изоморфное отображение φ первого полукольца на второе. Таким образом:

$$\forall\,(a_1, b_1 \in N_1) \quad \varphi(a_1 + b_1) = \varphi(a_1) \oplus \varphi(b_1);$$
$$\forall\,(a_1, b_1 \in N_1) \quad \varphi(a_1 \cdot b_1) = \varphi(a_1) \odot \varphi(b_1).$$

По теореме 6.2.1 любой элемент Z_1 представим в виде разности элементов N_1, а любой элемент Z_2 — в виде разности элементов N_2. Этим и воспользуемся для определения изоморфного отображения первой системы на вторую.

Пусть $c_1 \in Z_1$, тогда $\exists\ (k_1, l_1 \in N_1)$ такие, что

$$c_1 = k_1 - l_1.$$

Полагаем

$$f(c_1) \rightleftharpoons \varphi(k_1) \ominus \varphi(l_1).$$

Заметим, что $\varphi(k_1) \in N_2$, $\varphi(l_1) \in N_2$. Поэтому

$$\varphi(k_1) \ominus \varphi(l_1) \in Z_2.$$

Далее, если m_1, n_1 — такие элементы N_1, что $k_1 - l_1 = m_1 - n_1$, то $k_1 + n_1 = m_1 + l_1$ и

$$\varphi(k_1) \oplus \varphi(n_1) = \varphi(k_1 + n_1) = \varphi(m_1 + l_1) = \varphi(m_1) \oplus \varphi(l_1).$$

Поэтому

$$\varphi(k_1) \ominus \varphi(l_1) = \varphi(m_1) \ominus \varphi(n_1).$$

Отсюда следует, что f — однозначное отображение Z_1 в Z_2. Но для любого a_2 из Z_2 можно найти элементы k_2, l_2 в N_2 такие, что

$$a_2 = k_2 - l_2.$$

А так как φ — однозначное отображение N_1 на N_2, то существуют элементы k_1 и l_1 в N_1, что

$$k_2 = \varphi(k_1), \quad l_2 = \varphi(l_1).$$

Отсюда следует, что f — однозначное отображение Z_1 на Z_2. Пусть теперь для каких-нибудь элементов k_1, l_1, m_1, n_1 из N_1

$$f(k_1 - l_1) = f(m_1 - n_1).$$

Докажем, что в таком случае $k_1 - l_1 = m_1 - n_1$. В самом деле,

$$\varphi(k_1) \ominus \varphi(l_1) = \varphi(m_1) \ominus \varphi(n_1).$$

Отсюда следует, что

$$\varphi(k_1 + n_1) = \varphi(k_1) \oplus \varphi(n_1) = \varphi(m_1) \oplus \varphi(l_1) = \varphi(m_1 + l_1).$$

Но φ — взаимно-однозначное отображение N_1 на N_2. Поэтому

$$k_1 + n_1 = m_1 + l_1$$

и, следовательно,

$$k_1 - l_1 = m_1 - n_1.$$

Таким образом, отображение f — взаимно-однозначное отображение Z_1 на Z_2.

Совсем нетрудно проверить, что

$$\forall (a_1, b_1 \in Z_1) \quad f(a_1 + b_1) = f(a_1) \oplus f(b_1) \wedge$$
$$\wedge f(a_1 \cdot b_1) = f(a_1) \odot f(b_1).$$

Вопросы: 6.3.1. Пусть $\langle Z; +, \cdot \rangle$ — кольцо целых чисел. Доказать, что всякое кольцо $\langle Z_1; \oplus, \odot \rangle$, изоморфное кольцу $\langle Z; +, \cdot \rangle$, можно вложить в систему, изоморфную системе целых чисел.

6.3.2. Доказать, что два любых кольца целых чисел изоморфны.

6.3.3. Доказать, что всякое упорядоченное кольцо с единицей и без делителей нуля содержит и только одно подкольцо, изоморфное кольцу целых чисел.

6.3.4. Доказать, что кольцо матриц второго порядка над полем действительных чисел содержит бесконечно много подколец, изоморфных кольцу целых чисел.

6.4. Непротиворечивость аксиоматической теории целых чисел

Теорема 6.4.1. Аксиоматическая теория целых чисел непротиворечива. Более то́чно: мы докажем непротиворечивость аксиоматической теории целых чисел, исходя из предположения, что аксиоматическая теория натуральных чисел непротиворечива.

Доказательство. Мы построим модель, на которой выполняются все 13 аксиом нашей теории. План доказательства:

1) построение кольца;

2) включение полукольца натуральных чисел. Для этой цели мы покажем, что некоторое подполукольцо построенной интерпретации нашей теории изоморфно полукольцу натуральных чисел и, значит, само является таковым;

3) проверка выполнения аксиомы минимальности.

Пусть $\mathbf{N} \rightleftharpoons \langle N; +, \cdot, 1 \rangle$ — система натуральных чисел.

1а) Рассмотрим множество P пар $\langle a, b \rangle$ натуральных чисел и определим на P бинарные операции $\oplus$ и $\odot$ следующим образом:

$$\forall (a, b, a', b' \in N) \quad \langle a, b \rangle \oplus \langle a', b' \rangle \rightleftharpoons \langle a + a', b + b' \rangle;$$

$$\forall (a, b, a', b' \in N) \quad \langle a, b \rangle \odot \langle a', b' \rangle \rightleftharpoons \langle aa' + bb', ab' + a'b \rangle.$$

Нам известно, что система $\langle P; \oplus, \odot \rangle$ — коммутативное полукольцо (вопрос 2.6.16). Легко проверить, что эта система кольцом не является.

1б) Введем на множестве P бинарное отношение:

$$\forall (a, b, a', b' \in N) \quad \langle a, b \rangle \sim \langle a', b' \rangle \overset{\text{Df}}{\Leftrightarrow} a + b' = a' + b.$$

Нам известно (вопрос 2.9.1), что это отношение рефлексивно, симметрично и транзитивно. Нетрудно показать, что это отношение монотонно относительно обеих операций в P.

Пусть $\overline{P}$ — множество классов эквивалентности множества P относительно рассматриваемого отношения. Обозначая класс α, содержащий пару $\langle a, b\rangle$, символом $\overline{\langle a, b\rangle}$, мы имеем $\alpha \rightleftharpoons \overline{\langle a, b\rangle}$, и если $\beta \rightleftharpoons \overline{\langle a', b'\rangle}$, то

$$\alpha = \beta \Leftrightarrow \langle a, b\rangle \sim \langle a', b'\rangle.$$

В частности, $\overline{\langle a, b\rangle} = \overline{\langle a + c, b + c\rangle}$ для каждого c из N.

Из теоремы 2.9.1 следует, что тернарные отношения в $\overline{P}$, определяемые равенствами

$$\overline{\langle a, b\rangle} + \overline{\langle a', b'\rangle} \rightleftharpoons \overline{\langle a, b\rangle \oplus \langle a', b'\rangle};$$
$$\overline{\langle a, b\rangle} \cdot \overline{\langle a', b'\rangle} \rightleftharpoons \overline{\langle a, b\rangle \odot \langle a', b'\rangle},$$

бинарные алгебраические операции на $\overline{P}$. А из теоремы 2.9.2 следует, что соответствие

$$\langle a, b\rangle \mapsto \overline{\langle a, b\rangle}$$

осуществляет гомоморфное отображение системы $\langle P; \oplus, \odot\rangle$ на систему $\langle \overline{P}; +, \cdot\rangle$. В силу теоремы 2.8.3 система $\langle \overline{P}; +, \cdot\rangle$ — коммутативное полукольцо.

1в) Докажем, что эта система является кольцом. Пусть $\alpha \rightleftharpoons \overline{\langle a, b\rangle}$ и $\beta \rightleftharpoons \overline{\langle a', b'\rangle}$ — какие-нибудь классы из $\overline{P}$. Покажем, что в множестве $\overline{P}$ имеется такой класс $\xi \rightleftharpoons \overline{\langle x, y\rangle}$, что

$$\alpha + \xi = \beta. \tag{6.4.1}$$

Но

$$\forall (x, y \in N) \quad \overline{\langle a, b\rangle} + \overline{\langle x, y\rangle} = \overline{\langle a', b'\rangle} \Leftrightarrow \overline{\langle a + x, b + y\rangle} = \overline{\langle a', b'\rangle}.$$

С другой стороны,

$$\overline{\langle a + x, b + y\rangle} = \overline{\langle a', b'\rangle} \Leftrightarrow a + x + b' = a' + b + y.$$

Последнее соотношение выполняется, если положить

$$x = a' + b, \quad y = a + b'.$$

Отсюда следует, что класс $\overline{\langle a' + b, a + b'\rangle}$ есть решение уравнения (6.4.1). Другими словами,

$$\overline{\langle a', b'\rangle} - \overline{\langle a, b\rangle} = \overline{\langle a' + b, a + b'\rangle}.$$

2) Выберем в $\overline{P}$ подмножество N_0 следующим образом:

$$\forall (\alpha = \overline{\langle a, b\rangle} \in \overline{P}) \quad \alpha \in N_0 \overset{\text{Df}}{\Leftrightarrow} a > b.$$

Проверим, что принадлежность $\alpha \in N_0$ не зависит от выбора представителя класса α. В самом деле, если $a = b + n$, то

$$\langle a, b\rangle \sim \langle a', b'\rangle \Leftrightarrow a' = b' + n.$$

Сопоставим с натуральным числом n класс $\varphi(n) \Leftrightarrow \overline{\langle 1+n, 1\rangle}$. Имеем:

$$\varphi(m) = \varphi(n) \Leftrightarrow m = n.$$

Далее

$$\varphi(m+n) = \overline{\langle m+n+1, 1\rangle} = \overline{\langle 1+n+1+m, 1+1\rangle} =$$
$$= \overline{\langle 1+m, 1\rangle} + \overline{\langle 1+n, 1\rangle} = \varphi(m) + \varphi(n).$$

Аналогично

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n).$$

Таким образом, φ — изоморфное отображение полукольца $\langle N; +, \cdot\rangle$ натуральных чисел на систему $\langle N_0; +, \cdot\rangle$. Поэтому:

а) система $\langle N_0; +, \cdot\rangle$ — полукольцо натуральных чисел;

б) кольцо $\langle \overline{P}; +, \cdot\rangle$ — расширение полукольца $\langle N_0; +, \cdot\rangle$.

3) Докажем, что на построенной интерпретации аксиоматической теории целых чисел выполняется и последняя аксиома — аксиома минимальности.

Пусть M — какое угодно подмножество $\overline{P}$, содержащее N_0 и вместе с любыми элементами α и β их разность $\alpha - \beta$. Докажем, что в таком случае $M = \overline{P}$, т. е. что любой элемент $\overline{P}$ принадлежит M. Пусть $\gamma \in \overline{P}$. Тогда $\gamma \Leftrightarrow \overline{\langle n, m\rangle}$, где n и m — какие-нибудь элементы N. Покажем, что класс γ можно представить в виде разности двух элементов из N_0. Но мы имеем:

$$\langle n, m\rangle + \langle m+1, 1\rangle = \langle n+m+1, m+1\rangle;$$
$$\langle n+m+1, m+1\rangle \sim \langle n+1, 1\rangle.$$

Поэтому

$$\gamma = \overline{\langle n, m\rangle} = \overline{\langle n+1, 1\rangle} - \overline{\langle m+1, 1\rangle} \in M.$$

Вопросы: 6.4.1. Доказать, что всякое минимальное упорядоченное коммутативное кольцо с единицей изоморфно кольцу целых чисел.

6.4.2. Пусть $\mathbf{A} \Leftrightarrow \langle A; +, 0, >\rangle$ — упорядоченная группа с минимальным положительным элементом m. Другими словами, $m > 0$ и $a \geqslant m$ для любого положительного элемента a системы $\mathbf{A}$. Доказать, что группа $\langle A; +, 0\rangle$ изоморфна аддитивной группе целых чисел, если порядок в $\mathbf{A}$ архимедов, т. е. если

$$\forall (a, b \in A) \quad a > 0 \wedge b > 0 \Rightarrow \exists (n \in N) \qquad n * a > b.$$

6.4.3. Можно или нет линейно упорядочить (ввести линейный порядок) полукольцо $\langle P; \oplus, \odot\rangle$, полученное нами при доказательстве теоремы 6.4.1?

6.5. Первичные термины и аксиомы аксиоматической теории рациональных чисел

Мы исходим из **определения:** *системой рациональных чисел* называется минимальное поле, которое является расширением кольца целых чисел.

Следующие термины принимаем в качестве первичных:

а) Q — множество, его элементы называем *рациональными числами;*

б) $+$ и $\cdot$ — сложение и умножение — *бинарные операции на* Q;

в) 0 — нуль — *нейтральный элемент сложения на* Q;

г) Z — подмножество Q, его элементы называем *целыми числами*;

д) $\oplus$ и $\odot$ — сложение и умножение — *бинарные операции на* Z.

В согласии с данным определением систему $\langle Q;\ +, \cdot, 0, Z, \oplus, \odot\rangle$ мы называем *системой рациональных чисел,* если она удовлетворяет пятнадцати аксиомам, составляющим следующие три группы:

А

Q_{I}. $\forall (a, b \in Q)\ \exists!\, (c \in Q)\quad a + b = c$;

Q_{II}. $\forall (a, b, c \in Q)\quad (a + b) + c = a + (b + c)$;

Q_{III}. $\forall (a, b \in Q)\quad a + b = b + a$;

Q_{IV}. $0 \in Q \wedge \forall (a \in Q)\quad a + 0 = a$;

Q_{V}. $\forall (a \in Q)\quad \exists (a' \in Q)\quad a + a' = 0$;

Q_{VI}. $\forall (a, b \in Q)\quad \exists!\, (p \in Q)\quad a \cdot b = p$;

Q_{VII}. $\forall (a, b, c \in Q)\quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$;

Q_{VIII}. $\forall (a, b \in Q)\quad a \cdot b = b \cdot a$;

Q_{IX}. $\forall (a, b, c \in Q)\quad (a + b) \cdot c = a \cdot c + b \cdot c$;

Q_{X}. $\forall (a, b \in Q)\quad a \neq 0 \Rightarrow \exists (x \in Q)\quad a \cdot x = b$.

Б

Q_{XI}. $\langle Z;\ \oplus, \odot\rangle$ — кольцо целых чисел;

Q_{XII}. $Z \subset Q$;

Q_{XIII}. $\forall (a, b \in Z)\quad a + b = a \oplus b$;

Q_{XIV}. $\forall (a, b \in Z)\quad a \cdot b = a \odot b$.

В

Q_{XV} (аксиома минимальности). Всякое подмножество M множества Q, если:

а) включает Z

и

б) $\forall (a, b \in M)\ a \neq 0 \Rightarrow \frac{b}{a} \in M$,

совпадает с Q.

Если $\langle Q;\ +,\ \cdot,\ 0, Z, \oplus, \odot\rangle$ — система рациональных чисел, то систему $\langle Q;\ +,\ \cdot,\ 0\rangle$ будем называть *полем рациональных чисел,* систему $\langle Q;\ +,\ 0\rangle$ — *аддитивной группой рациональных чисел,* систему $\langle Q;\ \cdot\rangle$ — *мультипликативной полугруппой рациональных чисел,* систему $\langle Q \setminus \{0\};\ \cdot\rangle$ — *мультипликативной группой рациональных чисел.*

6.6. Свойства рациональных чисел

Прежде всего можно сделать замечания, аналогичные тем, которые были сделаны в начале п. 6.2.

В этом пункте система $\mathbf{N} \leftrightarrows \langle N;\ +,\ \cdot,\ 1\rangle$ — система натуральных чисел.

Теорема 6.6.1. Всякое рациональное число есть частное целых чисел, т. е.

$$\forall (a \in Q)\quad \exists (k, l \in Z)\quad l \neq 0 \ \wedge\ a = \frac{k}{l}.$$

При этом, если $l \neq 0$ и $l' \neq 0$, то

$$\frac{k}{l} = \frac{k'}{l'} \Leftrightarrow kl' = k'l.$$

Доказательство. Обозначим через M подмножество Q всех таких рациональных чисел, которые представимы в виде частного целых чисел.

Дальше рассуждаем почти так же, как при доказательстве теоремы 6.2.1.

Теорема 6.6.2. Поле рациональных чисел можно линейно и строго упорядочить, притом единственным способом. Порядок в поле рациональных чисел архимедов и продолжает порядок в кольце целых чисел.

Доказательство. Обозначим через Q^+ подмножество Q, определяемое условием

$$\forall \left(\alpha \leftrightarrows \frac{k}{l} \in Q,\ k, l \in Z\right)\quad \alpha \in Q^+ \overset{\text{Df}}{\Leftrightarrow} k \cdot l \in N.$$

Убедимся прежде всего, что принадлежность рационального α к множеству Q^+ не зависит от формы записи числа α. В самом деле, если $ll' \neq 0$, то

$$\frac{k}{l} = \frac{k'}{l'} \Leftrightarrow kl' = k'l,$$

но

$$kl' = k'l \Leftrightarrow kl\,(l')^2 = k'l'l^2.$$

Отсюда при $\alpha \neq 0$ следует, что числа kl и $k'l'$ либо оба натуральные, либо отрицательные целые.

Пусть теперь $\alpha \leftrightarrows \frac{k}{l}$; $k, l \in Z$, $l \neq 0$.

Возможны три случая:

1) $\alpha = 0 \Leftrightarrow k = 0$;

2) $\alpha \in Q^+ \Leftrightarrow kl \in N$;

3) $-\alpha \in Q^+ \Leftrightarrow -kl \in N$.

Легко доказать также, что

$$\forall (\alpha, \beta \in Q^+)\quad \alpha + \beta \in Q^+ \wedge \alpha \cdot \beta \in Q^+.$$

Таким образом, Q^+ — положительная часть поля $\langle Q;\ +,\ \cdot\rangle$. Пусть Q^{++} — какая-нибудь положительная часть поля $\langle Q;\ +,\cdot\rangle$. Докажем, что

$$Q^+ = Q^{++}.$$

Имеем по теореме 5.4.4

$$1 = 1^2 \in Q^{++}.$$

Отсюда следует, что $N \subset Q^{++}$, а в силу теоремы 5.4.7 и $Q^+ \subset Q^{++}$. По теореме 5.4.12 $Q^+ = Q^{++}$.

Легко видеть, далее, что

$$N = Z^+ = Q^+ \cap Z.$$

Отсюда следует, что порядок в Q продолжает порядок в Z.

Пусть $\alpha \rightleftharpoons \frac{k}{l} > 0$, $\beta \rightleftharpoons \frac{m}{n} > 0$; $k,\ l,\ m,\ n \in Z$; $l \neq 0$, $n \neq 0$. Так как порядок в кольце целых чисел архимедов, то для положительных целых kn и lm можно найти натуральное c такое, что

$$c \cdot kn > lm.$$

Отсюда

$$c\alpha = c\frac{k}{l} > \frac{m}{n} = \beta.$$

Таким образом, порядок в поле рациональных чисел архимедов.

Теорема 6.6.3. Всякое линейно упорядоченное поле содержит подполе, изоморфное полю рациональных чисел.

Доказательство. Пусть система $\mathbf{P} \rightleftharpoons \langle P;\ +,\ \cdot,\ 0,\ e,\ >\rangle$ — линейно упорядоченное поле. Так как система $\langle P;\ +,\ 0,\ >\rangle$ — линейно и строго упорядоченная полугруппа, то, каковы бы ни были целые числа z_1 и z_2,

$$z_1 * e = z_2 * e \Leftrightarrow z_1 = z_2.$$

Далее заметим, что для любых целых z_1 и z_2

$$(z_1 * e) \cdot (z_2 * e) = (z_1 \cdot z_2) * e.$$

Из этих замечаний легко вывести, что отображение f множества рациональных чисел Q во множество P, определяемое условием

$$\forall (a \in Z)\, \forall (n \in N) \quad f\left(\frac{a}{n}\right) \Leftrightarrow \frac{a * e}{n * e},$$

есть изоморфное отображение поля рациональных чисел на некоторое подполе поля $\langle P;\ +,\ \cdot,\ 0,\ e\rangle$.

Вопросы: **6.6.1.** Доказать, что поле рациональных чисел плотно, т. е.

$$\forall (a, b \in Q) \quad a > b \Rightarrow \exists (r \in Q) \quad a > r > b.$$

6.6.2. Доказать, что уравнение $x^2 = 2$ не имеет решений в Q.

6.6.3. Доказать, что множество Q счетно.

6.6.4. Доказать, что

$$\forall (\alpha \in Q)\, \exists! (a \in Z) \quad a \leqslant \alpha < a + 1$$

(существование целой части числа α).

6.6.5. Какие аксиомы используются при доказательстве теоремы 6.6.1?

6.6.6. Доказать, что аксиомы Q_{II}, Q_{III}, Q_{IV}, Q_V, Q_{VI} в совокупности можно вывести из остальных аксиом аксиоматической теории рациональных чисел.

6.6.7. Доказать, что мультипликативную группу рациональных чисел линейно и строго упорядочить нельзя.

6.6.8. Показать, что существует и только один линейный и строгий порядок в аддитивной группе рациональных чисел, в котором 1 — положительный элемент.

6.6.9*. Показать, что:

а) порядок $\succ$ в поле рациональных чисел однозначно определяется следующими условиями:

1) $\forall (a, b \in Q) \quad a \succ b \Rightarrow a \neq b$,

2) $\forall (a, b, c \in Q) \quad a \succ b \wedge b \succ c \Rightarrow a \succ c$,

3) $\forall (a, b, c \in Q) \quad a \succ b \Rightarrow a + c \succ b + c$,

4) $\forall (a, b \in Q) \quad a \neq b \Rightarrow a \succ b \vee b \succ a$,

5) $1 \succ 0$;

б) ни одно из пяти названных выше условий не является следствием остальных.

6.7. Категоричность аксиоматической теории рациональных чисел

Теорема 6.7.1. Аксиоматическая теория рациональных чисел категорична.

Доказательство. В предположении, что аксиоматическая теория рациональных чисел непротиворечива, докажем, что две любые модели, на которых выполняются все пятнадцать аксиом нашей теории, изоморфны. Пусть

$$\langle Q_1; +, \cdot, O_1, Z_1, +, \cdot \rangle \text{ и } \langle Q_2; \oplus, \odot, O_2, Z_2, \oplus, \odot \rangle —$$

две модели нашей теории. Так как любые кольца целых чисел изоморфны, то существует изоморфное изображение φ кольца $\langle Z_1; +, \cdot \rangle$ на кольцо $\langle Z_2; \oplus, \odot \rangle$. Но по теореме 6.6.1 любой элемент Q_1 представим в виде частного элементов из Z_1, а любой элемент из Q_2 — в виде частного элементов из Z_2. Этим и воспользуемся для задания изоморфного отображения первой системы на вторую.

Пусть $r_1 \in Q_1$ и a_1, b_1 — такие элементы из Z_1, что

$$r_1 = \frac{a_1}{b_1}.$$

Полагаем

$$f(r_1) \rightleftharpoons \frac{\varphi(a_1)}{\varphi(b_1)}.$$

Далее, рассуждая, как при доказательстве теоремы 6.3.1, мы убеждаемся, что f осуществляет изоморфное отображение одной модели на другую.

Вопросы: 6.7.1. Доказать, что любые поля рациональных чисел изоморфны.

6.7.2. Доказать, что поле, изоморфное полю рациональных чисел, само является полем рациональных чисел.

6.8. Непротиворечивость аксиоматической теории рациональных чисел

Теорема 6.8.1. Аксиоматическая теория рациональных чисел непротиворечива.

Точнее говоря, мы докажем непротиворечивость аксиоматической теории рациональных чисел относительно аксиоматической теории целых чисел.

Доказательство. Построим модель, на которой выполняются все 15 аксиом нашей теории. План доказательства:

1) построение поля;

2) включение кольца целых чисел. Для этой цели мы покажем, что некоторое подкольцо построенной интерпретации нашей теории изоморфно кольцу целых чисел и, значит, само является таковым;

3) проверка выполнения аксиомы минимальности.

Пусть $\langle Z;\ +,\ \cdot,\ 0,\ N,\ +,\ \cdot,\ 1\rangle$ — какая-нибудь система целых чисел.

1а) Рассмотрим множество P пар целых чисел $\langle a, n\rangle$ таких, что $a \in Z$ и $n \in N$. Определим на P бинарные операции $\oplus$ и $\odot$ следующим образом:

$$\forall (a, a' \in Z)\ \forall (n, n' \in N)\quad \langle a, n\rangle \oplus \langle a', n'\rangle \rightleftharpoons \langle an' + a'n,\ nn'\rangle;$$

$$\forall (a, a' \in Z)\ \forall (n, n' \in N)\quad \langle a, n\rangle \odot \langle a', n'\rangle \rightleftharpoons \langle aa',\ nn'\rangle.$$

Нам известно (вопрос 2.6.17), что системы $\langle P;\ \oplus\rangle$ и $\langle P;\ \odot\rangle$ — коммутативные полугруппы с нейтральными элементами $\langle 0,1\rangle$ и $\langle 1,1\rangle$ соответственно.

1б) Введем на множестве P бинарное отношение $\sim$ условием:

$$\forall (a, a' \in Z)\ \forall (n, n' \in N)\quad \langle a, n\rangle \sim \langle a', n'\rangle \overset{\text{Df}}{\Leftrightarrow} an' = a'n.$$

Известно (вопрос 2.9.2), что это отношение — отношение эквивалентности. Нетрудно проверить, что оно монотонно относительно обеих операций. Определив во множестве $\overline{P}$ классов эквивалентности

тернарные отношения $+$ и $\cdot$ соглашениями:

$$\overline{\langle a, n\rangle} + \overline{\langle a', n'\rangle} \rightleftharpoons \overline{\langle a, n\rangle \oplus \langle a', n'\rangle};$$
$$\overline{\langle a, n\rangle} \cdot \overline{\langle a', n'\rangle} \rightleftharpoons \overline{\langle a, n\rangle \odot \langle a', n'\rangle},$$

мы немедленно заключаем, что соответствие, по которому с парой $\langle a, n\rangle$ сопоставляется класс эквивалентности $\overline{\langle a, n\rangle}$, содержащий эту пару, есть гомоморфное отображение системы $\langle P; \oplus, \odot\rangle$ на систему $\langle \overline{P}; +, \cdot\rangle$. Из теоремы 2.8.2 следует, что системы $\langle \overline{P}; +\rangle$ и $\langle \overline{P}; \cdot\rangle$ — коммутативные полугруппы с нейтральными элементами $\overline{\langle 0,1\rangle}$ и $\overline{\langle 1,1\rangle}$ соответственно.

1в) Докажем, что система $\langle \overline{P}; +, \cdot\rangle$ — коммутативное кольцо. Прежде всего заметим, что

$$\langle a, n\rangle \oplus \langle -a, n\rangle = \langle 0, n^2\rangle \sim \langle 0, 1\rangle.$$

Проверим далее дистрибутивность умножения относительно сложения. Имеем:

$$(\langle a, m\rangle \oplus \langle a', m'\rangle) \odot \langle b, n\rangle = \langle am' + a'm, mm'\rangle \odot \langle b, n\rangle =$$
$$= \langle abm' + a'bm, mm'n\rangle;$$
$$\langle a, m\rangle \odot \langle b, n\rangle \oplus \langle a', m'\rangle \odot \langle b, n\rangle = \langle ab, mn\rangle \oplus \langle a'b, m'n\rangle =$$
$$= \langle abm'n + a'bmn, mm'n^2\rangle.$$

Но

$$\langle abm' + a'bm, mm'n\rangle \sim \langle abm'n + a'bmn, mn'n^2\rangle.$$

Поэтому

$$\overline{(\langle a, m\rangle + \langle a', m'\rangle)} \cdot \overline{\langle b, n\rangle} = \overline{\langle a, m\rangle} \cdot \overline{\langle b, n\rangle} + \overline{\langle a', m'\rangle} \cdot \overline{\langle b, n\rangle}.$$

Таким образом, система $\langle \overline{P}; +, \cdot\rangle$ — коммутативное кольцо. Нетрудно видеть, что класс $\theta \rightleftharpoons \overline{\langle 0, m\rangle}$, где $m \in N$, является нулем этого кольца.

1г) Докажем, что система $\langle \overline{P}; +, \cdot, \theta\rangle$ — поле. Пусть $\alpha \rightleftharpoons \overline{\langle a, m\rangle} \in \overline{P}$, $\beta \rightleftharpoons \overline{\langle a', m'\rangle} \in \overline{P}$ и $\alpha \neq 0$, т. е. $a \neq 0$. Нам достаточно проверить, что уравнение

$$\alpha\xi = \beta \tag{6.8.1}$$

разрешимо в кольце $\langle \overline{P}; +, \cdot, \theta\rangle$. Но это так, ибо

$$\overline{\langle a, m\rangle} \cdot \overline{\langle aa'm, m'a^2\rangle} = \overline{\langle a^2a'm, mm'a^2\rangle} = \overline{\langle a', m'\rangle}.$$

2) Выделим в $\overline{P}$ подмножество Z_0 условием:

$$\forall (\alpha \rightleftharpoons \overline{\langle a, m\rangle} \in \overline{P}) \quad \alpha \in Z_0 \overset{\text{Di}}{\Leftrightarrow} \exists (c \in Z) \quad a = cm \wedge c \neq 0.$$

Проверим, что принадлежность α к Z_0 не зависит от выбора представителя класса α. В самом деле, если $a = cm$, то

$$\langle a, m\rangle \sim \langle a', m'\rangle \Leftrightarrow a' = cm'.$$

Сопоставим с целым числом c класс $\varphi(c) \Leftrightarrow \overline{\langle c, 1\rangle}$. Имеем

$$\varphi(c) = \varphi(c') \Leftrightarrow c = c'.$$

Далее, легко показать, что

$$\varphi(c + c') = \varphi(c) + \varphi(c');$$
$$\varphi(c \cdot c') = \varphi(c) \cdot \varphi(c')$$

для любых c и c' из Z. Таким образом, α — изоморфное отображение кольца целых чисел $\langle Z; +, \cdot\rangle$ на $\langle Z_0; +, \cdot\rangle$. Следовательно:

а) система $\langle Z_0; +, \cdot\rangle$ сама является кольцом целых чисел;

б) поле $\langle \bar{P}; +, \cdot, \theta\rangle$ — расширение кольца $\langle Z_0; +, \cdot\rangle$.

3) Докажем, что на построенной интерпретации выполняется аксиома 15 (минимальности). Пусть M — какое угодно подмножество $\bar{P}$, удовлетворяющее двум условиям:

а) оно включает Z_0;

б) для любых α и β из M, если β — не нуль кольца $\langle \bar{P}; +, \cdot, \theta\rangle$, их частное $\frac{\alpha}{\beta}$ принадлежит M.

Покажем, что в таком случае $M = \bar{P}$. Нам достаточно показать, что любой элемент $\gamma = \overline{\langle c, m\rangle}$ из $\bar{P}$ принадлежит M. Если $c = 0$, то $\gamma = \theta$ и, таким образом, $\gamma \in M$. Пусть $c \neq 0$. Имеем

$$\overline{\langle c, m\rangle} \cdot \overline{\langle m, 1\rangle} = \overline{\langle cm, m\rangle}.$$

Итак, класс γ есть частное двух классов из Z_0, а потому входит в M. Теорема доказана.

Вопросы: 6.8.1. Доказать, что всякое минимальное упорядоченное тело изоморфно полю рациональных чисел.

6.8.2. Доказать, что всякое тело характеристики нуль, т. е. тело, в котором все кратные единицы различны, содержит и только одно подполе, изоморфное полю рациональных чисел.

6.8.3. Доказать, что всякое тело характеристики нуль содержит и только одно подкольцо, изоморфное кольцу целых чисел.

6.8.4. Доказать, что всякое тело характеристики нуль содержит и только одно полукольцо, изоморфное полукольцу натуральных чисел.

§ 7. ПОСЛЕДОВАТЕЛЬНОСТИ В НОРМИРОВАННЫХ ПОЛЯХ

7.1. Нормированные поля

Определение 7.1.1. Пусть $\mathbf{A} \rightleftharpoons \langle A;\ +,\ \cdot,\ 0,\ 1\rangle$ — поле, $\mathbf{P} \rightleftharpoons \langle P;\ +,\ \cdot, 0, 1, >\rangle$ — линейно упорядоченное поле; ν — однозначное отображение A в P. Систему $\langle A;\ +,\ \cdot, 0, 1, P;\ +,\ \cdot,\ 0,\ 1, >, \nu\rangle$, короче $\langle \mathbf{A};\ \mathbf{P};\ \nu\rangle$, называют *нормированным полем,* если выполняются 3 следующих условия:

1) $\forall\,(a \in A)\quad \nu(a) \geqslant 0 \wedge \nu(a) = 0 \Leftrightarrow a = 0;$

2) $\forall\,(a, b \in A)\quad \nu(a \cdot b) = \nu(a) \cdot \nu(b);$

3) $\forall\,(a, b \in A)\quad \nu(a + b) \leqslant \nu(a) + \nu(b).$

Вместо того чтобы сказать: система $\langle \mathbf{A};\ \mathbf{P};\ \nu\rangle$ — нормированное поле, говорят также: $\mathbf{A}$ — нормированное относительно линейно упорядоченного поля $\mathbf{P}$ с нормой ν поле.

Примеры: 7.1.1. Пусть $\mathbf{A}$ — любое поле, $\mathbf{P}$ — любое линейно упорядоченное поле. Полагаем:

$$\forall\,(a \in A)\qquad \nu(a) \rightleftharpoons \begin{cases} 1, & \text{если}\quad a \neq 0; \\ 0, & \text{если}\quad a = 0. \end{cases}$$

Нетрудно проверить, что система $\langle \mathbf{A};\ \mathbf{P};\ \nu\rangle$ — нормированное поле. Норму ν, определенную указанным выше способом, называют *тривиальной*. Итак, любое поле можно тривиально нормировать.

7.1.2. Пусть $\mathbf{A}$ — любое линейно упорядоченное поле и $\mathbf{P} \rightleftharpoons \mathbf{A}$. Полагаем

$$\forall\,(a \in A)\quad \nu(a) \rightleftharpoons |a|.$$

Система $\langle \mathbf{A};\ \mathbf{A};\ \nu\rangle$ является нормированным полем. Норму $|a|$ называют *естественной*. Итак: любое линейно упорядоченное поле допускает естественное нормирование.

7.1.3. Пусть Q — поле рациональных чисел, p — простое число и θ — рациональное число с условием $0 < \theta < 1$. Определим функцию ν_p следующим образом. Пусть α — какое-либо не равное нулю рациональное число. Представляем α в виде

$$\alpha = p^n \cdot \frac{a}{b},$$

где a и b — целые, взаимно-простые с p числа и n — целое число. Нетрудно проверить, что число n определяется однозначно.

Полагаем

$$\nu_p(\alpha) \rightleftharpoons \theta^n, \quad \nu_p(0) \rightleftharpoons 0.$$

Пусть теперь $\beta = p^m \cdot \frac{c}{d}$ и $\nu_p(\beta) = \theta^m$. Имеем

$$\alpha \cdot \beta = p^{n+m} \cdot \frac{ac}{bd}, \quad \alpha + \beta = p^n \frac{ad + p^{m-n}bc}{bd}.$$

Отсюда следует, что

$$\forall (\alpha, \beta \in Q) \quad \nu_p(\alpha \cdot \beta) = \nu_p(\alpha) \cdot \nu_p(\beta)$$

и

$$\forall (\alpha, \beta \in Q) \quad \nu_p(\alpha + \beta) \leqslant \max(\nu_p(\alpha), \nu_p(\beta)) \leqslant \nu_p(\alpha) + \nu_p(\beta).$$

Итак, система $\langle \mathbf{Q}; \mathbf{Q}; \nu_p \rangle$ — нормированное поле. Норму ν_p называют *p-адической*. Полезно заметить, что p-адическая норма удовлетворяет условию

$$\forall (\alpha, \beta \in Q) \quad \nu_p(\alpha + \beta) \leqslant \max(\nu_p(\alpha), \nu_p(\beta)). \tag{7.1.1}$$

7.1.4. Пусть $\mathbf{Q}(x)$ — поле рациональных функций над полем рациональных чисел $\mathbf{Q}$, θ — рациональное число, большее единицы. Если $\alpha \in \mathbf{Q}(x)$ и $\alpha \neq 0$, то α можно представить в виде

$$\alpha = \frac{a_0 + a_1 x + \cdots + a_n x^n}{b_0 + b_1 x + \cdots + b_m x^m},$$

где $a_0 + a_1 x + \cdots + a_n x^n$ и $b_0 + b_1 x + \cdots + b_m x^m$ — многочлены над полем $\mathbf{Q}$ степеней $n \geqslant 0$ и $m \geqslant 0$ соответственно. Мы полагаем, что

$$\nu(\alpha) \rightleftharpoons \theta^{n-m}, \quad \nu(0) = 0.$$

Нетрудно убедиться, что система $\langle \mathbf{Q}(x); \mathbf{Q}; \nu \rangle$ — нормированное поле.

Теорема 7.1.1. Если $\langle \mathbf{A}; \mathbf{P}; \nu \rangle$ — нормированное поле, то

1) $\nu(1) = 1$;

2) $\nu(-1) = 1$;

3) $\forall (a \in A) \quad \nu(a) = \nu(-a)$;

4) $\forall (a \in A) \quad a \neq 0 \Rightarrow \nu\left(\frac{1}{a}\right) = \frac{1}{\nu(a)}$;

5) $\forall (a, b \in A) \quad a \neq 0 \Rightarrow \nu\left(\frac{b}{a}\right) = \frac{\nu(b)}{\nu(a)}$;

6) $\forall (a, b \in A) \quad |\nu(a) - \nu(b)| \leqslant \nu(a - b) \leqslant \nu(a) + \nu(b)$;

7) $\forall (a, b \in A) \quad \nu(a) \geqslant \nu(b) - \nu(b - a)$.

Доказательство. Имеем

$$\nu(1) \cdot \nu(1) = \nu(1 \cdot 1) = \nu(1).$$

Так как уравнение второй степени над любым полем имеет не более двух корней, то $\nu(1) = 1$ или $\nu(1) = 0$. Второе исключено.

Далее имеем

$$\nu(-1) \cdot \nu(-1) = \nu(1) = 1.$$

Рассуждая аналогично, получим $\nu(-1) \rightleftharpoons 1$. Остальные утверждения очевидны.

Вопросы: 7.1.1. Пусть $\mathbf{A} \rightleftharpoons \mathbf{Q}$ и $\mathbf{P} \rightleftharpoons \mathbf{R}$. Полагаем $\nu(a) \rightleftharpoons |a|^c$, где $0 < c \leqslant 1$. Показать, что система $\langle \mathbf{Q}; \mathbf{R}; \nu \rangle$ — нормированное поле.

7.1.2. Пусть ν_p — p-адическая норма примера 7.1.3 и a — любое положительное число. Показать, что $\langle \mathbf{Q}; \mathbf{R}; \nu_p^a \rangle$ — нормированное поле.

7.1.3*. Норму ν поля $\mathbf{P}$ относительно поля действительных чисел называют *неархимедовой*, если для любого натурального n $\nu(n * 1) \leqslant \leqslant 1$. Показать, что норма ν поля $\mathbf{P}$ является неархимедовой тогда и только тогда, если

$$\forall (a, b \in P) \quad \nu(a + b) \leqslant \max(\nu(a), \nu(b)).$$

Справедлива теорема **Островского:** пусть $\mathbf{Q}$ — поле рациональных чисел, $\mathbf{R}$ — поле действительных чисел и $\langle \mathbf{Q}; \mathbf{R}; \nu \rangle$ — нормированное поле. Тогда ν либо тривиальная норма, либо норма вопросов 7.1.1 и 7.1.2.

7.2. Последовательности в нормированных полях

Определение 7.2.1. Пусть $\langle \mathbf{A}; \mathbf{P}; \nu \rangle$ — нормированное поле, $\mathbf{P}_1$ — подполе поля $\mathbf{P}$. Последовательность $\{a_n\}_n \rightleftharpoons \{a_n\}_{n=1}^{\infty}$ элементов поля $\mathbf{A}$ называется *ограниченной* относительно поля $\mathbf{P}_1$ по норме ν, если выполняется любое из следующих двух эквивалентных условий:

А. $\exists (c \in P_1^+) \quad \forall (n \in N) \quad \nu(a_n) < c$;

Б. $\exists (c_1 \in P_1^+) \quad \forall (n \in N) \quad \nu(a_n) \leqslant c_1$.

Определение 7.2.2. Пусть $\langle \mathbf{A}; \mathbf{P}; \nu \rangle$ — нормированное поле, $\mathbf{P}_1$ — подполе поля $\mathbf{P}$. Последовательность $\{a_n\}_n \rightleftharpoons \{a_n\}_{n=1}^{\infty}$ элементов поля $\mathbf{A}$ называют *фундаментальной* по норме ν относительно поля $\mathbf{P}_1$, если выполняется любое из следующих шести эквивалентных условий:

А. $\forall (\varepsilon_1 \in P_1^+) \exists (n_1 \in N) \quad \forall (n, k \in N) \quad n \geqslant n_1 \wedge k \geqslant n_1 \Rightarrow$
$\Rightarrow \nu(a_k - a_n) < \varepsilon_1$;

Б. $\forall (\varepsilon_2 \in P_1^+) \exists (n_2 \in N) \quad \forall (n, k \in N) \quad n \geqslant n_2 \wedge k \geqslant n_2 \Rightarrow$
$\Rightarrow \nu(a_k - a_n) \leqslant \varepsilon_2$;

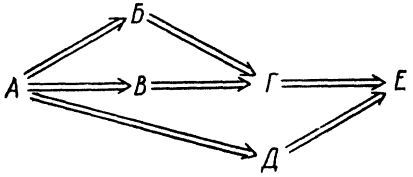
В. $\forall (\varepsilon_3 \in P_1^+) \exists (n_3 \in N) \quad \forall (n, k \in N) \quad n \geqslant n_3 \Rightarrow \nu(a_{n+k} - a_n) < \varepsilon_3$;

Г. $\forall (\varepsilon_4 \in P_1^+)\, \exists (n_4 \in N)\ \ \forall (n, k \in N)\ \ n \geqslant n_4 \Rightarrow \nu (a_{n+k} - a_n) \leqslant \varepsilon_4$;

Д. $\forall (\varepsilon_5 \in P_1^+)\, \exists (n_5 \in N)\ \ \forall (n \in N)\ \ n \geqslant n_5 \Rightarrow \nu (a_n - a_{n_5}) < \varepsilon_5$;

Е. $\forall (\varepsilon_6 \in P_1^+)\, \exists (n_6 \in N)\ \ \forall (n \in N)\ \ n \geqslant n_6 \Rightarrow \nu (a_n - a_{n_6}) \leqslant \varepsilon_6$.

Легко видеть, что



Полагаем $\varepsilon_6 \rightleftharpoons \frac{1}{3}\varepsilon$, $n_1 \rightleftharpoons n_6$. Имеем

$$\forall (n, k \in N)\ \ n \geqslant n_1 \wedge k \geqslant n_1 \Rightarrow \nu (a_k - a_n) \leqslant$$

$$\leqslant \nu (a_k - a_{n_6}) + \nu (a_n - a_{n_6}) \leqslant \frac{1}{3}\varepsilon_1 + \frac{1}{3}\varepsilon_1.$$

Поэтому

$$E \Rightarrow A.$$

Тем самым эквивалентность всех шести условий доказана.

Определение 7.2.3. Пусть $\langle \mathbf{A};\ \mathbf{P};\ \nu \rangle$ — нормированное поле, $\mathbf{P}_1$ — подполе поля $\mathbf{P}$. Последовательность $\{a_n\}_n$ элементов поля $\mathbf{A}$ называется *сходящейся* к элементу a поля $\mathbf{A}$ относительно поля $\mathbf{P}_1$ по норме ν, если выполняется любое из следующих двух эквивалентных условий:

А. $\forall (\varepsilon_1 \in P_1^+)\, \exists (n_1 \in N)\, \forall (n \in N)\ \ n \geqslant n_1 \Rightarrow \nu (a_n - a) < \varepsilon_1$;

Б. $\forall (\varepsilon_2 \in P_1^+)\, \exists (n_2 \in N)\, \forall (n \in N)\ \ n \geqslant n_2 \Rightarrow \nu (a_n - a) \leqslant \varepsilon_2$.

Эквивалентность этих условий проверяется без труда.

Запись

$$\{a_n\}_n \underset{\nu}{\longmapsto} a\ (\mathbf{P}_1)$$

означает, что последовательность $\{a_n\}_n$ сходится к элементу a по норме ν относительно поля $\mathbf{P}_1$.

Если последовательность $\{a_n\}_n$ сходится к элементу a по норме ν относительно поля $\mathbf{P}_1$, то элемент a называют также *пределом последовательности* $\{a_n\}_n$ *по норме* ν относительно поля $\mathbf{P}_1$; если к тому же $a = 0$, то последовательность $\{a_n\}_n$ называют *нулевой по норме* ν относительно поля $\mathbf{P}_1$ последовательностью.

Определение 7.2.4. Пусть $\langle \mathbf{A};\ \mathbf{P};\ \nu \rangle$ — нормированное поле, $\mathbf{P}_1$ — подполе поля $\mathbf{P}$. Последовательности $\{a_n\}_n$ и $\{b_n\}_n$ элементов поля $\mathbf{A}$ называют *эквивалентными по норме* ν относительно поля $\mathbf{P}_1$, если последовательность с общим членом $a_n - b_n$ нулевая по норме ν относительно поля $\mathbf{P}_1$.

Обозначение: $\{a_n\}_n\ \tilde{\nu}\{b_n\}_n\ (\mathbf{P}_1)$.

В случае если за норму принимается абсолютная величина, слова «по норме ν» в терминах, введенных определениями 7.2.2, 7.2.3 и 7.2.4, мы будем опускать. В случае если поле **P** архимедовски упорядочено, выбор подполя $\mathbf{P}_1$ при рассмотрении ограниченной, фундаментальной, сходящейся или эквивалентных последовательностей относительно поля $\mathbf{P}_1$, как это следует из теоремы 5.4.9, не имеет значения. Поэтому слова «относительно поля $\mathbf{P}_1$» в этом случае в терминах, указанных выше, мы иногда будем опускать.

Если поле **P** архимедовски упорядочено и в качестве нормы принята абсолютная величина, то предел последовательности $\{a_n\}_n$ мы будем обозначать также и таким символом: $\lim\limits_{n\to\infty} a_n$.

Пример 7.2.1. Пусть **Q** — поле рациональных чисел; **Q** (x) — поле рациональных функций над полем **Q**. Введем в **Q** (x) тот порядок, который в примере 5.4.3. рассмотрен первым. Полученную систему примем за **P**. Нормирование выберем естественное. Заметим, что поле **Q** — подполе поля **Q** (x) и порядок, индуцированный порядком системы **Q** (x) в поле **Q**, совпадает с обычным отношением «больше» в поле рациональных чисел. Нам известно, что $x > 0$ и $\frac{1}{x} > 0$ в системе **P**. Рассмотрим последовательность $\{n\}_n$, т. е. 1, 2, ..., n, ... Эта последовательность неограниченно возрастает относительно поля **Q**, но ограничена относительно поля **Q** (x). В самом деле,

$$\forall (n \in N) \qquad n < x.$$

Рассмотрим дальше последовательность $\left\{\frac{1}{n}\right\}_n$. Она сходится к нулю относительно поля **Q**, но не сходится к нулю относительно поля **Q** (x). Действительно,

$$\forall (n \in N) \qquad \left|\frac{1}{n} - 0\right| = \frac{1}{n} > \frac{1}{x}.$$

Та же последовательность не является и фундаментальной относительно поля Q (x), так как

$$\forall (n, k \in N) \qquad \left|\frac{1}{n} - \frac{1}{n+k}\right| = \frac{k}{n(n+k)} > \frac{1}{x}.$$

Наконец, стационарная последовательность $\{0\}_n$ и последовательность $\left\{\frac{1}{n}\right\}_n$ эквивалентны относительно поля **Q**, но не эквивалентны относительно поля Q (x).

Пример 7.2.2. Пусть p — простое число. Рассмотрим последовательность $\{p^n\}_n$. Эта последовательность рациональных чисел сходится к нулю по p-адической норме.

Вопросы: 7.2.1. Рассмотрим в поле рациональных чисел естественное нормирование. Пусть $\{a_n\}_n$ — какая-нибудь последовательность. Показать, что сходимость к нулю последовательности $\{a_{n+1} - a_n\}_n$ является необходимым, но не достаточным условием для того, чтобы последовательность $\{a_n\}_n$ была фундаментальна.

7.2.2. Рассмотрим p-адическое нормирование поля рациональных чисел. Показать, что сходимость к нулю последовательности $\{a_{n+1} - a_n\}_n$ является необходимым и достаточным условием для того, чтобы последовательность $\{a_n\}_n$ была фундаментальной по p-адической норме последовательностью.

7.2.3. Назвать какую-нибудь фундаментальную по p-адической норме, но нестационарную последовательность рациональных чисел.

7.2.4. Назвать нестационарную, но сходящуюся и по p-адической и по естественной норме последовательность рациональных чисел.

Определение 7.2.5. Пусть $\mathbf{P} \rightleftharpoons \langle P;\ +,\ \cdot, 0, > \rangle$ — упорядоченное поле; последовательность $\{a_n\}_n$ элементов поля $\mathbf{P}$ называют *возрастающей,* если

$$\forall (n \in N) \qquad a_n \leqslant a_{n+1},$$

и *строго возрастающей,* если

$$\forall (n \in N) \qquad a_n < a_{n+1}.$$

Определение 7.2.6. Пусть M — какое угодно множество, $\{a_n\}_n$ — последовательность элементов множества M и $\{k_n\}_n$ — строго возрастающая последовательность натуральных чисел. Последовательность $\{a_{k_n}\}_n$, т. е. $a_{k_1}, a_{k_2}, \ldots, a_{k_n}, \ldots$, называют *подпоследовательностью* последовательности $\{a_n\}_n$.

Вопрос 7.2.5. Доказать, что

$$\forall (n \in N) \qquad k_n \geqslant n,$$

если $\{k_n\}_n$ — строго возрастающая последовательность натуральных чисел.

7.3. Свойства последовательностей в нормированных полях

В этом разделе рассматривается нормированное поле $\langle \mathbf{A};\ \mathbf{P};\ \nu \rangle$; через $\mathbf{P}_1$ обозначается любое подполе поля $\mathbf{P}$.

Теорема 7.3.1. Всякая стационарная последовательность $\{a_n\}_n$ элементов поля $\mathbf{A}$ сходится к a по норме ν относительно поля $\mathbf{P}_1$.

В самом деле, для любого положительного ε из $\mathbf{P}_1$ имеем

$$\forall (n \in N) \quad \nu(a - a) = \nu(0) = 0 < \varepsilon.$$

Легко доказывается следующая теорема.

Теорема 7.3.2. Всякая подпоследовательность $\{a_{k_n}\}_n$ последовательности $\alpha \rightleftharpoons \{a_n\}_n$ элементов поля $\mathbf{A}$

1) ограничена по норме ν относительно поля $\mathbf{P}_1$, если последовательность α ограничена по норме ν относительно поля $\mathbf{P}_1$;

2) фундаментальна по норме ν относительно поля $\mathbf{P}_1$, если последовательность α фундаментальна по норме ν относительно поля $\mathbf{P}_1$;

3) сходится к элементу a поля $\mathbf{A}$ по норме ν относительно поля $\mathbf{P}_1$, если последовательность α сходится к элементу a по норме ν относительно поля $\mathbf{P}_1$;

4) эквивалентна последовательности α по норме ν относительно поля $\mathbf{P}_1$, если последовательность α фундаментальна по норме ν относительно поля $\mathbf{P}_1$.

Теорема 7.3.3. Всякая сходящаяся по норме ν относительно поля $\mathbf{P}_1$ последовательность элементов поля $\mathbf{A}$ фундаментальна по норме ν относительно поля $\mathbf{P}_1$.

В самом деле, если последовательность $\{a_n\}_n$ сходится к элементу a по норме ν относительно поля $\mathbf{P}_1$, то для любого положительного элемента ε поля $\mathbf{P}_1$ можно найти натуральное n_0 такое, что

$$\forall (n \in N) \quad n \geqslant n_0 \Rightarrow \nu(a_n - a) < \frac{1}{2}\varepsilon.$$

Имеем

$$\forall (n, k \in N) \; n \geqslant n_0 \wedge k \geqslant n_0 \Rightarrow \nu(a_n - a_k) \leqslant \nu(a_n - a) + \nu(a - a_k) < \varepsilon.$$

Теорема 7.3.4. Пусть $\{a_n\}_n$ и $\{b_n\}_n$ — фундаментальные по норме ν относительно поля $\mathbf{P}_1$ последовательности элементов поля $\mathbf{A}$. Тогда фундаментальна по норме ν относительно поля $\mathbf{P}_1$ каждая из последовательностей:

1) $\{a_n + b_n\}_n$;

2) $\{a_n - b_n\}_n$.

Доказательство. Утверждения вытекают из следующих неравенств:

$$\nu(a_n + b_n - a_k - b_k) \leqslant \nu(a_n - a_k) + \nu(b_n - b_k);$$
$$\nu(a_n - b_n - a_k + b_k) \leqslant \nu(a_n - a_k) + \nu(b_n - b_k).$$

Теорема 7.3.5. Пусть $\{a_n\}_n$ и $\{b_n\}_n$ — сходящиеся по норме ν относительно поля $\mathbf{P}_1$ к элементам a и b соответственно последовательности элементов поля $\mathbf{A}$. Тогда последовательности:

1) $\{a_n + b_n\}_n$;

2) $\{a_n - b_n\}_n$ —

сходятся по норме ν относительно поля $\mathbf{P}_1$ к элементам $a + b$ и $a - b$ соответственно.

Доказательство легко получается из рассмотрения следующих неравенств:

$$\nu(a_n + b_n - a - b) \leqslant \nu(a_n - a) + \nu(b_n - b);$$
$$\nu(a_n - b_n - a + b) \leqslant \nu(a_n - a) + \nu(b_n - b).$$

Теорема 7.3.6. Если последовательность $\{a_n\}_n$ нулевая по норме ν относительно поля $\mathbf{P}_1$, а последовательность $\{b_n\}_n$ ограничена по норме ν относительно поля $\mathbf{P}_1$, то последовательность $\{a_n b_n\}_n$ нулевая по норме ν относительно поля $\mathbf{P}_1$.

Доказательство. В самом деле, имеем

$$\nu(a_n \cdot b_n) = \nu(a_n) \cdot \nu(b_n).$$

Теорема 7.3.7. Пусть $\{a_n\}_n$, $\{b_n\}_n$ и $\{c_n\}_n$ — последовательности элементов поля **A**. Тогда:

1) $\{a_n\}_n \underset{\nu}{\sim} \{a_n\}_n$ $(\mathbf{P}_1)$;

2) $\{a_n\}_n \underset{\nu}{\sim} \{b_n\}_n$ $(\mathbf{P}_1) \Rightarrow \{b_n\}_n \underset{\nu}{\sim} \{a_n\}_n$ $(\mathbf{P}_1)$;

3) $\{a_n\}_n \underset{\nu}{\sim} \{b_n\}_n$ $(\mathbf{P}_1) \wedge \{b_n\}_n \underset{\nu}{\sim} \{c_n\}_n (\mathbf{P}_1) \Rightarrow \{a_n\}_n \underset{\nu}{\sim} \{c_n\}_n$ $(\mathbf{P}_1)$;

4) $\{a_n\}_n \underset{\nu}{\sim} \{b_n\}_n$ $(\mathbf{P}_1) \Rightarrow \{a_n + c_n\}_n \underset{\nu}{\sim} \{b_n + c_n\}_n$ $(\mathbf{P}_1)$.

Если последовательность $\{c_n\}_n$ ограничена по норме ν относительно поля $\mathbf{P}_1$, то

5) $\{a_n\}_n \underset{\nu}{\sim} \{b_n\}_n$ $(\mathbf{P}_1) \Rightarrow \{a_n c_n\}_n \underset{\nu}{\sim} \{b_n c_n\}_n$ $(\mathbf{P}_1)$.

Справедливость теоремы легко выводится из теорем 7.3.1, 7.3.5 и 7.3.6.

Теорема 7.3.8. Пусть $\{a_n\}_n$ и $\{b_n\}_n$ — эквивалентные по норме ν относительно поля $\mathbf{P}_1$ последовательности элементов поля **A**. Тогда:

1) одна из них фундаментальна по норме ν относительно поля $\mathbf{P}_1$, если и только если тем же свойством обладает вторая;

2) одна из них сходится к элементу a поля **A** по норме ν относительно поля $\mathbf{P}_1$, если и только если тем же свойством обладает вторая.

Доказательство теоремы нетрудно получить из рассмотрения неравенств:

$$\nu(a_n - a_k) \leqslant \nu(a_n - b_n) + \nu(b_n - b_k) + \nu(b_k - a_k);$$
$$\nu(a_n - a) \leqslant \nu(a_n - b_n) + \nu(b_n - a).$$

Теорема 7.3.9. Пусть $\alpha \rightleftharpoons \{a_n\}_n$ — последовательность элементов поля **A**, $\beta \rightleftharpoons \{\nu(a_n)\}_n$. Тогда:

1) если последовательность α фундаментальна по норме ν относительно поля $\mathbf{P}_1$, то и последовательность β фундаментальна относительно поля $\mathbf{P}_1$;

2) если последовательность α сходится к элементу a по норме ν относительно поля $\mathbf{P}_1$, то и последовательность β сходится к элементу $\nu(a)$ относительно поля $\mathbf{P}_1$;

3) последовательность α нулевая по норме ν относительно поля $\mathbf{P}_1$, если и только если последовательность β нулевая относительно поля $\mathbf{P}_1$.

Доказательство легко получается из следующих соотношений:

$$|\nu(a_n) - \nu(a_k)| \leqslant \nu(a_n - a_k);$$
$$|\nu(a_n) - \nu(a)| \leqslant \nu(a_n - a);$$
$$|\nu(a_n)| = \nu(a_n).$$

Теорема 7.3.10. Если последовательность $\alpha \rightleftharpoons \{a_n\}_n$ элементов поля **A** не сходится к нулю по норме ν относительно поля $\mathbf{P}_1$, то существует такой положительный элемент ε в поле $\mathbf{P}_1$ и такая подпоследовательность $\{a_{k_n}\}_n$ последовательности α, что

$$\forall (n \in N) \quad \nu(a_{k_n}) \geqslant \varepsilon.$$

Доказательство. В самом деле, если последовательность α не сходится к нулю по норме ν относительно поля $\mathbf{P}_1$, то это значит, что для некоторого положительного элемента ε поля $\mathbf{P}_1$, каково бы ни было натуральное число n', существует натуральное число $n'' > n'$ такое, что

$$\nu(a_{n''}) \geqslant \varepsilon.$$

Теорема 7.3.11. Если последовательность $\alpha \rightleftharpoons \{a_n\}_n$ фундаментальна по норме ν относительно поля $\mathbf{P}_1$ и не сходится к нулю по норме ν относительно поля $\mathbf{P}_1$, то существует такой положительный элемент ε в поле $\mathbf{P}_1$ и такое натуральное число n_0, что

$$\forall (n \in N) \quad n \geqslant n_0 \Rightarrow \nu(a_n) \geqslant \varepsilon \wedge \nu(a_{n+1} - a_n) < \varepsilon.$$

Доказательство. По теореме 7.3.10 можно указать такой положительный элемент ε_0 в поле $\mathbf{P}_1$ и подпоследовательность $\beta \rightleftharpoons \{a_{k_n}\}_n$, что

$$\forall (n \in N) \quad \nu(a_{k_n}) \geqslant \varepsilon_0. \tag{7.3.1}$$

С другой стороны, по теореме 7.3.2. последовательность α и ее подпоследовательность β эквивалентны по норме ν относительно поля $\mathbf{P}_1$. Отсюда следует, что существует такое натуральное число n_0, что

$$\forall (n \in N)\, n \geqslant n_0 \Rightarrow \nu(a_{k_n} - a_n) < \frac{1}{2}\varepsilon_0 \wedge \nu(a_{n+1} - a_n) < \frac{1}{2}\varepsilon_0.$$

Поэтому в силу (7.3.1) имеем

$$\forall (n \in N) \quad n \geqslant n_0 \Rightarrow \nu(a_n) \geqslant \nu(a_{k_n}) - \nu(a_n - a_{k_n}) > \frac{1}{2}\varepsilon_0 = \varepsilon.$$

В формулировках теорем 7.3.12—7.3.17 упорядоченное поле **P** нельзя заменить на любое его подполе.

Теорема 7.3.12. Всякая сходящаяся по норме ν относительно поля **P** последовательность $\{a_n\}_n$ элементов поля **P** имеет не более одного предела.

Доказательство. Пусть a и b — пределы последовательности α по норме ν относительно поля **P**. Если $a \neq b$, то $\nu(a-b) > 0$. Полагаем $\varepsilon \rightleftharpoons \frac{1}{2}\nu(a-b)$ и выбираем натуральные числа n_1 и n_2 так, что

$$\forall (n \in N) \quad n \geqslant n_1 \wedge n \geqslant n_2 \Rightarrow \nu(a_n - a) < \varepsilon \wedge \nu(a_n - b) < \varepsilon.$$

Отсюда получим противоречие:

$$\forall (n \in N) \quad n \geqslant \max(n_1, n_2) \Rightarrow \nu(a-b) \leqslant \nu(a-a_n) + \nu(a_n - b) < \\ < 2\varepsilon = \nu(a-b).$$

Теорема 7.3.13. Последовательность $\{a_n\}_n$ элементов поля **A** ограничена по норме ν относительно поля **P** тогда и только тогда, если выполняется любое из следующих соотношений:

1) $\exists (c_1 \in P^+) \quad \exists (n_1 \in N) \quad \forall (n \geqslant n_1) \quad \nu(a_n) \leqslant c_1$;

2) $\exists (c_2 \in P^+) \quad \exists (n_2 \in N) \quad \forall (n \geqslant n_2) \quad \nu(a_n) < c_2$.

Доказательство. Из 1) следует, что

$$\forall (n \in N) \quad \nu(a_n) \leqslant \sum_{n=1}^{n_1} \nu(a_n) + c_1,$$

но

$$\sum_{n=1}^{n_1} \nu(a_n) + c_1 \in P.$$

Теорема 7.3.14. Всякая фундаментальная по норме ν относительно поля **P** последовательность $\{a_n\}_n$ ограничена по норме ν относительно поля **P**.

Доказательство. В самом деле, для, например, $\varepsilon = 1$ можно найти натуральное число n_0 такое, что

$$\forall (n \in N) \quad n \geqslant n_0 \Rightarrow \nu(a_n - a_{n_0}) < 1.$$

Наше утверждение следует из теоремы 7.3.13 и неравенства

$$\nu(a_n) \leqslant \nu(a_n - a_{n_0}) + \nu(a_{n_0}).$$

Теорема 7.3.15. Пусть $\{a_n\}_n$ и $\{b_n\}_n$ — эквивалентные по норме ν относительно поля **P** последовательности элементов поля **A**. Тогда:

1) одна из них ограничена по норме ν относительно поля **P**, если и только если тем же свойством обладает вторая;

2) если одна из них ограничена по норме ν относительно поля **P**, то для любого натурального k последовательности $\{a_n^k\}_n$ и $\{b_n^k\}_n$ эквивалентны по норме ν относительно поля **P**.

Доказательство теоремы легко следует из теоремы 7.3.13 и неравенств:

$$\nu(a_n) \leqslant \nu(a_n - b_n) + \nu(b_n);$$
$$\nu(a_n^k - b_n^k) \leqslant \nu(a_n^{k-1})\,\nu(a_n - b_n) + \nu(b_n) \cdot \nu(a_n^{k-1} - b_n^{k-1}).$$

Теорема 7.3.16. Пусть $\alpha \leftrightharpoons \{a_n\}_n$ и $\beta \leftrightharpoons \{b_n\}_n$ — фундаментальные по норме ν относительно поля **P** последовательности элементов поля **A**. Тогда:

1) последовательность $\{a_n b_n\}_n$ фундаментальна по норме ν относительно поля **P**;

2) если последовательность β не нулевая по норме ν относительно поля **P** и $\forall (n \in N)\ b_n \neq 0$, то последовательность $\left\{\frac{a_n}{b_n}\right\}_n$ фундаментальна по норме ν относительно поля **P**.

Доказательство. Первое утверждение легко следует из теоремы 7.3.14 и неравенства

$$\nu(a_n b_n - a_k b_k) \leqslant \nu(a_n)\,\nu(b_n - b_k) + \nu(a_n - a_k)\,\nu(b_k).$$

Второе утверждение следует из теорем 7.3.11, 7.3.14 и неравенства

$$\nu\left(\frac{a_n}{b_n}-\frac{a_k}{b_k}\right)\leqslant\frac{1}{\nu(b_n)}\nu(a_n-a_k)+\frac{\nu(a_k)}{\nu(b_n)\,\nu(b_k)}\nu(b_n-b_k).$$

Теорема 7.3.17. Пусть $\alpha\leftrightarrows\{a_n\}_n$ и $\beta\leftrightarrows\{b_n\}_n$ — сходящиеся по норме ν относительно поля $\mathbf{P}$ к элементам a и b соответственно последовательности элементов поля $\mathbf{P}$. Тогда:

1) последовательность $\{a_nb_n\}_n$ сходится к ab по норме ν относительно поля $\mathbf{P}$;

2) если $b\neq0$ и $\forall\,(n\in N)\,b_n\neq0$, то последовательность $\left\{\frac{a_n}{b_n}\right\}_n$ сходится к $\frac{a}{b}$ по норме ν относительно поля $\mathbf{P}$.

Доказательство теоремы легко получается из неравенств:

$$\nu(a_nb_n-ab)\leqslant\nu(a_n)\,\nu(b_n-b)+\nu(a_n-a)\,\nu(b);$$

$$\nu\left(\frac{a_n}{b_n}-\frac{a}{b}\right)\leqslant\frac{1}{\nu(b_n)}\nu(a_n-a)+\frac{\nu(a)}{\nu(b_n)\,\nu(b)}\nu(b_n-b).$$

Вопросы: 7.3.1. Пусть θ_1 и θ_2 — рациональные числа; $0<\theta_1<1$, $0<\theta_2<1$; p — простое число; ν_p' и ν_p'' — p-адические нормы примера 7.1.3, определяемые для неравного нулю числа α условиями:

$$\nu_p'(\alpha)=\theta_1^n;\quad\nu_p''(\alpha)=\theta_2^n,$$

если

$$\alpha=p^n\cdot\frac{a}{b};\quad a,b\in Z;\quad(a,p)=(b,p)=1.$$

Доказать, что последовательность рациональных чисел нулевая по норме ν_p' тогда и только тогда, если она нулевая по норме ν_p''.

7.3.2. В системе примера 7.2.1 рассматриваются последовательности:

$$\alpha\leftrightarrows\{a_n\}_n;\quad\beta\leftrightarrows\{b_n\}_n;\quad\beta'\leftrightarrows\{b_n'\}_n;\quad\gamma\leftrightarrows\{c_n\}_n;\quad\delta\leftrightarrows\{d_n\}_n$$

с общими членами вида:

$$a_n\leftrightarrows0;\quad b_n\leftrightarrows\frac{1}{n};\quad c_n\leftrightarrows x+\frac{1}{n};\quad d_n\leftrightarrows1-\frac{1}{n};$$

$$b_n'\leftrightarrows\begin{cases}x, & \text{если}\quad n=1,2;\\ b_n, & \text{если}\quad n\geqslant3.\end{cases}$$

Проверить, что:

1) каждая из последовательностей α, β, β', γ, δ фундаментальна относительно поля $\mathbf{Q}$;

2) последовательности α, β и δ ограничены относительно поля $\mathbf{Q}$, последовательности β', γ не ограничены относительно поля $\mathbf{Q}$;

3) последовательность β относительно поля $\mathbf{Q}$ сходится к любому элементу поля $\mathbf{Q}$ (x) вида $\frac{r}{x}$, где $r\in\mathbf{Q}$;

4) последовательность с общим членом b_nc_n не является фундаментальной относительно поля **Q**;

5) последовательности β и γ сходятся относительно поля **Q**, но последовательность с общим членом b_nc_n не сходится относительно поля **Q**.

6) последовательности α и β эквивалентны относительно поля Q, но последовательности с общими членами a_nc_n и b_nc_n неэквивалентны относительно поля **Q**;

7) последовательность δ сходится к 1 относительно поля **Q**, ее каждый член меньше $1 - \frac{1}{x}$, но

$$1 > 1 - \frac{1}{x};$$

8) последовательность β сходится к $\frac{1}{x}$ относительно поля **Q**, но последовательность с общим членом $\frac{1}{b_n}$ не сходится к x относительно поля **Q**.

7.4. Последовательности элементов линейно упорядоченного поля

Мы будем здесь предполагать, что $\mathbf{A} \rightleftharpoons \langle A;\ +,\ \cdot,\ 0,1, > \rangle$ и $\mathbf{P} \rightleftharpoons \langle P;\ +,\ \cdot,\ 0,\ 1,\ > \rangle$ — линейно упорядоченные поля, причем **P** — расширение системы **A**, $\nu(a) = |a|$ — абсолютная величина элемента a, $\mathbf{P}_1$, как и прежде, подполе поля **P**.

Теорема 7.4.1. Пусть $\{a_n\}_n$ — фундаментальная относительно поля $\mathbf{P}_1$ и не нулевая относительно поля $\mathbf{P}_1$ последовательность элементов поля **A**. Тогда существует в поле $\mathbf{P}_1$ такой положительный элемент ε и натуральное число n_0, что

$$\forall (n \in N) \quad n \geqslant n_0 \Rightarrow |a_n| \geqslant \varepsilon;$$

при этом либо

$$a_n \geqslant \varepsilon > 0,$$

либо

$$-a_n \geqslant \varepsilon > 0.$$

Доказательство. В самом деле, по теореме 7.3.11

$$\exists (\varepsilon \in P_1^+)\ \exists (n_0 \in N)\ \ \forall (n \in N) \quad n \geqslant n_0 \Rightarrow |a_n| \geqslant \varepsilon \wedge |a_{n+1} - a_n| < \varepsilon.$$

Предположение, что числа a_n и a_{n+1} разных знаков, сразу приводит к противоречию, так как

$$|a_{n+1} - a_n| = |a_{n+1}| + |a_n| \geqslant 2\varepsilon > \varepsilon.$$

Легко доказывается

Теорема 7.4.2. Если возрастающая последовательность $\{a_n\}_n$ положительных элементов поля **A** не ограничена относительно поля $\mathbf{P}_1$, то последовательность $\left\{\frac{1}{a_n}\right\}_n$ нулевая относительно поля $\mathbf{P}_1$.

В следующих теоремах поле **P** нельзя заменить на любое его подполе.

Теорема 7.4.3. Если последовательность $\{a_n\}_n$ элементов поля **A** сходится относительно поля **P** к элементу a того же поля, $c \in P$ и

$$\forall (n \in N) \quad a_n \leqslant c,$$

то $a \leqslant c$.

Доказательство. В самом деле, если $a > c$, то, полагая $\varepsilon \rightleftharpoons a - c$, мы для всех натуральных n, начиная с некоторого, в противоречие с предположением получим

$$a_n \geqslant a - |a_n - a| > a - (a - c) = c.$$

Теорема 7.4.4. Если последовательность $\alpha \rightleftharpoons \{a_n\}_n$ элементов поля **A** строго возрастает, не ограничена относительно поля **P**, то для любого элемента γ поля **A** с условием $\gamma \geqslant a_1$ существует и только одно натуральное число c такое, что

$$a_c \leqslant \gamma < a_{c+1}.$$

Доказательство. Так как последовательность α не ограничена относительно поля **P**, то $(A \subset P)$ существует натуральное число n' такое, что

$$a_{n'} > \gamma.$$

Пусть M — множество тех натуральных чисел n (индексов членов последовательности α), для которых $a_n \leqslant \gamma$. Множество M ограничено сверху числом n' и непусто, так как $1 \in M$. Поэтому M имеет наибольший элемент c. Таким образом,

$$a_c \leqslant \gamma < a_{c+1}.$$

Легко проверить, что только одно натуральное число c удовлетворяет этому условию.

7.5. Последовательности элементов архимедовски линейно упорядоченного поля

Мы будет предполагать, что $\mathbf{A} \rightleftharpoons \langle A; +, \cdot, 0, 1, > \rangle$, $\mathbf{P} \rightleftharpoons \langle P; +, \cdot, 0, 1, > \rangle$ — архимедовски линейно упорядоченные поля, **A** — подполе поля **P** и $\nu(a) = |a|$ — абсолютная величина элемента $a \in A$. В этих предположениях, как мы в свое время заметили, выбор подполя $\mathbf{P}_1$ поля **P** не имеет значения. В качестве поля $\mathbf{P}_1$ можно всегда выбирать поле рациональных чисел **Q**, которое в наших предположениях является подполем поля **A**, а следовательно, и поля **P**. Поскольку поле рациональных чисел допускает только одно линейное и строгое упорядочивание, всякий порядок в **P** является продолжением порядка в **Q**.

Теорема 7.5.1. Пусть k — любое натуральное число. Тогда последовательность $\{n^k\}_n$ строго и неограниченно возрастает (относительно любого архимедовски упорядоченного поля).

Доказательство. В самом деле, $n^k \geqslant n$.

Теорема 7.5.2. Пусть q — любое не равное единице натуральное число; тогда последовательность $\{q^n\}_n$ строго и неограниченно возрастает.

Доказательство. В самом деле, $q^n \geqslant n$.

Теорема 7.5.3. Пусть γ — любое рациональное большее единицы число; тогда последовательность $\{\gamma^n\}_n$ строго и неограниченно возрастает.

Доказательство. Удобно записать γ в виде $\gamma = 1 + \alpha$, где $\alpha > 0$. Тогда $\gamma^n \geqslant 1 + n\alpha$ для любого натурального n. Это следует из неравенства

$$(1 + n\alpha)(1 + \alpha) > 1 + (n + 1)\alpha.$$

Дальше можно воспользоваться тем, что порядок в поле **Q** архимедов.

Теорема 7.5.4. Если последовательность $\{a_n\}_n$ элементов поля **A** возрастает и ограничена относительно архимедовски линейно упорядоченного поля **P**, то она фундаментальна относительно архимедовски линейно упорядоченного поля **P**.

Доказательство. В поле **P** можно указать такой элемент c, что

$$\forall (n \in N) \quad a_n \leqslant c.$$

Предположим, что последовательность $\{a_n\}_n$ не фундаментальна относительно поля **P**. Тогда существует такой положительный элемент ε_0 в поле **P**, что для любого натурального числа n_0 можно найти натуральное n_1 такое, что

$$n_1 > n_0 \wedge |a_{n_1} - a_{n_0}| = a_{n_1} - a_{n_0} \geqslant \varepsilon_0.$$

По n_1 мы выбираем n_2, так, что $a_{n_2} - a_{n_1} \geqslant \varepsilon_0$. Так продолжаем дальше:

$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$

$$a_{n_k} - a_{n_{k-1}} \geqslant \varepsilon_0.$$

Складывая полученные неравенства, найдем, что

$$a_{n_k} \geqslant a_{n_0} + k \cdot \varepsilon_0.$$

Так как поле **P** архимедовски упорядочено, можно найти натуральное k_0 такое, что

$$k_0 \varepsilon_0 > c + |a_{n_0}|.$$

Отсюда имеем:

$$\forall (k \in N) \quad k \geqslant k_0 \Rightarrow a_{n_k} \geqslant a_{n_0} + k\varepsilon_0 > c.$$

Теорема 7.5.5. Пусть k — натуральное число, γ — любой положительный элемент архимедовски линейно упорядоченного поля **A**. Тогда можно найти фундаментальную последовательность $\{a_n\}_n$ элементов поля **A** такую, что последовательность $\{a_n^k\}_n$ сходится к γ относительно архимедовски линейно упорядоченного поля **P**.

Доказательство. Мы ограничимся рассмотрением случая, когда $\gamma \geqslant 1$. Так как $1^k \leqslant \gamma$, то в силу теорем 7.5.1. и 7.4.4. существует натуральное число a_1 такое, что

$$a_1^k \leqslant \gamma < (a_1 + 1)^k.$$

Пусть для некоторого натурального n и $a_n \in A$ верны соотношения:

$$a_n^k \leqslant \gamma < \left(a_n + \frac{1}{2^{n-1}}\right)^k.$$

Выберем a_{n+1} следующим образом:

$$a_{n+1} \rightleftharpoons \begin{cases} a_n, & \text{если } \gamma < \left(a_n + \frac{1}{2^n}\right)^k; \\ a_n + \frac{1}{2^n}, & \text{если } \gamma \geqslant \left(a_n + \frac{1}{2^n}\right)^k. \end{cases}$$

Построенная нами последовательность $\{a_n\}_n$ элементов поля **A** удовлетворяет условию:

$$\forall (n \in N) \quad a_n^k \leqslant \gamma < \left(a_n + \frac{1}{2^{n-1}}\right)^k,$$

при этом

$$\forall (n \in N) \quad 1 \leqslant a_n \leqslant a_{n+1} \leqslant a_n + \frac{1}{2^n}.$$

Итак, последовательность $\{a_n\}_n$ возрастает и ограничена сверху, так как

$$a_n \leqslant a_n^k \leqslant \gamma.$$

Следовательно, по теореме 7.5.4 последовательность $\{a_n\}_n$ фундаментальна относительно поля **P**. Но последовательности $\{a_n\}_n$ и $\left\{a_n + \frac{1}{2^{n-1}}\right\}_n$ эквивалентны относительно поля **P**, так как $\left\{\frac{1}{2^{n-1}}\right\}_n \to 0$ (**P**). Поэтому в силу теоремы 7.3.15 и последовательности $\{a_n^k\}_n$ и $\left\{\left(a_n + \frac{1}{2^{n-1}}\right)^k\right\}_n$ эквивалентны относительно поля **P**. А потому, каков бы ни был положительный элемент ε из **P**, можно найти натуральное n_0 такое, что

$$\forall (n \in N) \quad n \geqslant n_0 \Rightarrow \left| a_n^k - \left(a_n + \frac{1}{2^{n-1}}\right)^k \right| < \varepsilon,$$

но

$$|a_n^k - \gamma| < \left| a_n^k - \left(a_n + \frac{1}{2^{n-1}}\right)^k \right|.$$

Теорема 7.5.6. Пусть $\mathbf{A}_1$ — подполе поля **A**. Для любой последовательности элементов $\{a_n\}_n$ архимедовски линейно упорядоченного поля **A** можно в поле $\mathbf{A}_1$ указать эквивалентную ей относительно архимедовски линейно упорядоченного поля **P** последовательность элементов поля $\mathbf{A}_1$.

Доказательство. Поскольку всякое упорядоченное поле — расширение поля рациональных чисел, то без ограничения общности можно предполагать, что $\mathbf{A}_1$ есть поле рациональных чисел. По теореме 7.4.2 последовательность $\left\{\frac{1}{n}\right\}_n$ сходится к нулю. По теореме 5.4.9 для каждого натурального n можно найти рациональное число b_n такое, что

$$a_n < b_n < a_n + \frac{1}{n}.$$

Этим все доказано.

Вопросы: 7.5.1. Пусть $\mathbf{A} = \mathbf{P} \rightleftharpoons \langle P; +, \cdot, 0, 1, > \rangle$ — архимедовски линейно упорядоченное тело. Доказать, что для любого $\gamma > 1$ из P можно найти элемент $r \in P$ такой, что

$$1 < r < r^2 < \gamma.$$

7.5.2. Пусть $\mathbf{A} = \mathbf{P} \rightleftharpoons \langle P; +, \cdot, 0, 1, > \rangle$ — архимедовски линейно упорядоченное тело. Пусть γ и r — такие элементы P, что $1 < r < \gamma$. Доказать, что существует натуральное n с условием

$$r^n \leqslant \gamma < r^{n+1}.$$

7.5.3*. Доказать, что архимедовски линейно упорядоченное тело $\mathbf{T} \rightleftharpoons \langle T; +, \cdot, 0, 1 \rangle$ коммутативно.

7.5.4. Пусть $\mathbf{Q}$ — поле рациональных чисел, $\mathbf{R}$ — система действительных чисел, p — простое число, $\langle \mathbf{Q}; \mathbf{R}; \nu \rangle$ — нормированное поле. Доказать, что последовательность $\{p^n\}_n$ сходится к нулю по норме ν относительно $\mathbf{Q}$ тогда и только тогда, если ν — p-адическая норма поля $\mathbf{Q}$ или норма вопроса 7.1.2.

§ 8. СИСТЕМА ДЕЙСТВИТЕЛЬНЫХ ЧИСЕЛ

8.1. Первичные термины и аксиомы теории действительных чисел

Мы исходим из определения: *системой действительных чисел* называется линейно и архимедовски упорядоченное поле, всякая фундаментальная последовательность элементов которого сходится.

В качестве первичных мы принимаем следующие термины:

а) R — множество, его элементы называются действительными числами;

б) $+$ и $\cdot$ — сложение и умножение — бинарные операции на R;

в) 0 и 1 — нуль и единица — элементы R;

г) $>$ — бинарное отношение в R.

Аксиомы системы $\mathbf{R} \Leftrightarrows \langle R; +, \cdot, 0, 1, > \rangle$ разбиваются на 3 группы и формулируются следующим образом:

А

R_{I}. $\forall (a, b \in R) \quad \exists! (c \in R) \quad a + b = c$;

R_{II}. $\forall (a, b, c \in R) \quad (a + b) + c = a + (b + c)$;

R_{III}. $\forall (a, b \in R) \quad a + b = b + a$;

R_{IV}. $0 \in R \wedge \forall (a \in R) \quad a + 0 = a$;

R_{V}. $\forall (a \in R) \exists (a' \in R) \quad a + a' = 0$;

R_{VI}. $\forall (a, b \in R) \quad \exists! (p \in R) \quad a \cdot b = p$;

R_{VII}. $\forall (a, b, c \in R) \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$;

R_{VIII}. $\forall (a, b \in R) \quad a \cdot b = b \cdot a$;

R_{IX}. $\forall (a, b, c \in R) \quad (a + b) \cdot c = a \cdot c + b \cdot c$;

R_{X}. $1 \in R \wedge 1 \neq 0 \wedge \forall (a \in R) \quad a \cdot 1 = a$;

R_{XI}. $\forall (a \in R) \quad \exists (a' \in R) \quad a \neq 0 \Rightarrow a \cdot a' = 1$.

Б

R_{XII}. $\forall (a, b \in R) \quad a \neq b \Rightarrow a > b \vee b > a$;

R_{XIII}. $\forall (a \in R) \quad \neg a > a$;

R_{XIV}. $\forall (a, b, c \in R) \quad a > b \wedge b > c \Rightarrow a > c$;

R_{XV}. $\forall (a, b, c \in R) \quad a > b \Rightarrow a + c > b + c$;

R_{XVI}. $\forall (a, b, c \in R) \quad a > b \wedge c > 0 \Rightarrow a \cdot c > b \cdot c$;

R_{XVII}. $\forall (a, b \in R) \quad a > 0 \wedge b > 0 \Rightarrow \exists (n \in N) \quad n * a > b$.

В

R_{XVIII}. Для любой фундаментальной последовательности $\{a_n\}_n$ элементов R существует в R элемент α такой, что $\lim\limits_{n\to\infty} a_n = \alpha$.

8.2. Свойства действительных чисел

Заметим прежде всего, что в силу теоремы 6.2.3 система действительных чисел имеет подполе, изоморфное полю рациональных чисел. А так как на любом поле, изоморфном полю рациональных чисел, все аксиомы аксиоматической теории рациональных чисел, очевидно, выполняются, то мы можем отсюда сделать вывод, что поле действительных чисел является расширением поля рациональных чисел.

Теорема 8.2.1. Всякое действительное число есть предел последовательности рациональных чисел.

Доказательство. Пусть r — какое-нибудь действительное число. По теореме 7.5.6 для стационарной последовательности $\{r\}_n$ действительных чисел можно указать эквивалентную ей последовательность $\{a_n\}_n$ рациональных чисел. Отсюда сразу следует, что $\lim\limits_{n\to\infty} a_n = r$.

Теорема 8.2.2 (о существовании корня любой натуральной степени из положительного числа).

$$\forall (\alpha \in R) \quad \forall (k \in N) \quad \alpha > 0 \Rightarrow \exists! (\beta \in R) \quad \beta^k = \alpha \wedge \beta > 0.$$

Другими словами, каковы бы ни были натуральное число k и действительное α, если $\alpha > 0$, то существует и только одно положительное действительное число β такое, что

$$\beta^k = \alpha. \tag{8.2.1}$$

Доказательство. По теореме 7.5.5 существует такая фундаментальная последовательность $\{a_n\}_n$ действительных чисел, что

$$\lim_{n\to\infty} a_n^k = \alpha.$$

Но по аксиоме R_{XVIII} существует действительное число β такое, что

$$\lim_{n\to\infty} a_n = \beta.$$

Из теорем 7.3.17 и 7.3.12 мы выводим наше утверждение.

Теорема 8.2.3. Поле $\langle R; +, \cdot, 0\rangle$ можно линейно и строго упорядочить не более чем одним способом.

Доказательство. Пусть R^+ и R^{++} — положительные части поля действительных чисел. Если $\alpha \in R^+$, то по теореме 8.2.2 можно

найти действительное число β такое, что $\alpha = \beta^2$. Заметим, что $\beta \neq 0$, а потому $\alpha = \beta^2 \in R^{++}$ в силу теоремы 5.4.4. Итак, $R^+ \subset R^{++}$ и, следовательно, $R^+ = R^{++}$ по теореме 5.4.12.

Теорема 8.2.4 (о двойной последовательности). Пусть $\{a_n\}_n$ и $\{b_n\}_n$ — последовательности действительных чисел, удовлетворяющие условиям:

1) $\forall (n \in N) \quad a_n \leqslant b_n$;

2) $\forall (n \in N) \quad a_n \leqslant a_{n+1} \wedge b_{n+1} \leqslant b_n$;

3) $\lim\limits_{n\to\infty} (a_n - b_n) = 0$.

Тогда существует и только одно действительное число γ такое, что

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n = \gamma$$

и

$$\forall (n \in N) \quad a_n \leqslant \gamma \leqslant b_n.$$

Доказательство. По теореме 7.5.4 последовательность $\{a_n\}_n$ фундаментальна; по аксиоме R_{XVIII} она имеет предел γ. По теореме 7.3.8 тот же предел имеет и последовательность $\{b_n\}_n$. Последнее утверждение теоремы легко следует из теоремы 7.4.3.

Теорема 8.2.5 (*всякое сечение имеет рубеж*). Пусть множество R разбито на 2 класса A и B так, что:

1) $A \neq \varnothing \wedge B \neq \varnothing$;

2) $R = A \cup B$;

3) $A \cap B = \varnothing$;

4) $\forall (\alpha \in A) \quad \forall (\beta \in B) \quad \alpha < \beta$.

Тогда существует действительное число γ такое, что либо $\gamma \in A$ и тогда $\forall (\alpha \in A)\ \alpha \leqslant \gamma$, либо $\gamma \in B$ и тогда $\forall (\beta \in B)\ \gamma \leqslant \beta$.

Доказательство. Построим двойную в смысле теоремы 8.2.4 последовательность. За a_1 и b_1 примем любые элементы классов A и B соответственно. Предположим, что члены $a_1, \ldots, a_n$; $b_1, \ldots, b_n$ выбраны, причем:

1) $a_1 \leqslant \cdots \leqslant a_n; \quad b_n \leqslant \cdots \leqslant b_1$;

2) $a_1, \ldots, a_n \in A; \quad b_1, \ldots, b_n \in B$.

Следующую пару членов a_{n+1} и b_{n+1} выбираем так:

$$a_{n+1} = \begin{cases} a_n, & \text{если } \dfrac{a_n + b_n}{2} \in B; \\ \dfrac{a_n + b_n}{2}, & \text{если } \dfrac{a_n + b_n}{2} \in A; \end{cases}$$

$$b_{n+1} = \begin{cases} \dfrac{a_n + b_n}{2}, & \text{если } \dfrac{a_n + b_n}{2} \in B; \\ b_n, & \text{если } \dfrac{a_n + b_n}{2} \in A. \end{cases}$$

Таким образом, двойная последовательность $\{\langle a_n, b_n\rangle\}_n$ нами построена. Нетрудно видеть, что к ней применима теорема 8.2.4. Поэтому существует действительное число γ такое, что

$$\forall (n \in N) \quad a_n \leqslant \gamma \leqslant b_n.$$

Покажем, что если $\gamma \in A$, то $\forall (\alpha \in A)\ \alpha \leqslant \gamma$. Допустим, что $\gamma < \alpha$ для некоторого α из A. В таком случае, $b_n - a_n \geqslant \alpha - \gamma > 0$. А это невозможно.

Вопросы: 8.2.1*. Доказать, что всякое архимедовски линейно упорядоченное поле изоморфно отображается в поле действительных чисел.

8.2.2. Показать, что если подполе **P** поля действительных чисел можно неархимедовски линейно упорядочить, то множество P содержит трансцендентные числа.

8.2.3. Пусть **R** — поле действительных чисел, **Q** — поле рациональных чисел, θ — действительное число. Показать, что число θ трансцендентно в том и только в том случае, если простое расширение $\mathbf{Q}(\theta)$ поля рациональных чисел можно неархимедовски упорядочить.

8.2.4*. Пусть $\mathbf{R} \rightleftharpoons \langle R;\ +,\ \cdot,\ 0\rangle$ и $\mathbf{Q} \rightleftharpoons \langle Q;\ +, \cdot,\ 0\rangle$ — поля действительных и рациональных чисел соответственно и **Q** — подполе поля **R**. Доказать, пользуясь теоремой Цермело, что поле **R** имеет *линейный базис* над **Q**, другими словами, существует вполне упорядоченное множество **B** и отображение Ω множества B в R:

$$\Omega : \beta \mapsto \omega_\beta$$

с условием, что для любого действительного числа α можно найти и только одно такое отображение a множества B в Q

$$a : \beta \mapsto a_\beta,$$

что:

1) $a_\beta = 0$ для всех β из B, кроме, быть может, конечного подмножества;

$$2)\ \alpha = \sum_{\beta \in B} a_\beta \cdot \omega_\beta. \tag{8.2.2}$$

8.2.5. Пусть $\mathbf{R} \rightleftharpoons \langle R;\ +,\ \cdot,\ 0, >\rangle$ — система действительных чисел, **Q** — поле рациональных чисел. Пусть $\langle \mathbf{B};\ \Omega\rangle$ — линейный базис поля $\langle R;\ +,\ \cdot, 0\rangle$ над полем рациональных чисел **Q**; $\alpha,\ \gamma \in R$ и

$$\alpha = \sum_{\beta \in B} a_\beta \omega_\beta, \quad \gamma = \sum_{\beta \in B} c_\beta \omega_\beta$$

их представления в форме (8.2.2). Определим в множестве R бинарное отношение $\succ$ следующим лексикографическим условием:

$$\alpha \succ \gamma \rightleftharpoons a_1 > c_1 \vee (a_1 = c_1 \wedge a_2 > c_2) \vee \cdots$$

в трансфинитном смысле. Показать, что $\langle R; +, \succ\rangle$ — линейно и строго упорядоченная группа.

8.2.6. Пусть $\succ$ — бинарное отношение в R, определяемое соглашением

$$\alpha \succ \beta \Leftrightarrow (\alpha \geqslant 0 \wedge \beta < 0) \vee (\alpha > 0 \wedge \beta = 0) \vee (\alpha \cdot \beta > 0 \wedge |\alpha| > |\beta|).$$

Показать, что оно обладает следующими свойствами:

1) $\forall (a, b \in R) \quad a \succ b \Rightarrow a \neq b$;

2) $\forall (a, b \in R) \quad a \succ b \wedge b \succ 0 \Rightarrow a \succ 0$;

3) $\forall (a, b, c \in R) \quad a \neq b \Rightarrow a \succ b \vee b \succ a$;

4) $\forall (a, b, c \in R) \quad a \succ b \wedge c \succ 0 \Rightarrow ac \succ bc$.

8.2.7*. Показать, что линейный порядок $\succ$ в поле действительных чисел определяется и притом однозначно следующими условиями:

1) $\forall (a, b \in R) \quad a \succ b \Rightarrow a \neq b$;

2) $\forall (a, b \in R) \quad a \succ b \wedge b \succ 0 \Rightarrow a \succ 0$;

3) $\forall (a, b, c \in R) \quad a \succ b \Rightarrow a + c \succ b + c$;

4) $\forall (a, b \in R) \quad a \neq b \Rightarrow a \succ b \vee b \succ a$;

5) $\forall (a, b, c \in R) \quad a \succ b \wedge c \succ 0 \Rightarrow ac \succ bc$.

8.2.9*. Показать, что множество линейных и строгих порядков в аддитивной группе действительных чисел бесконечно.

Пусть $\mathbf{A} \leftrightarrows \langle A; +, \cdot \rangle$ — подполе поля $\mathbf{P} \leftrightarrows \langle P; +, \cdot \rangle$, $B \subset P$. Символом $\mathbf{A}(B)$ обозначают минимальное подполе поля $\mathbf{P}$, содержащее множество $A \cup B$. Вполне упорядоченное множество $\langle B; \succ \rangle$ называют *базисом поля* $\mathbf{P}$ относительно поля $\mathbf{A}$, если $\mathbf{P} = \mathbf{A}(B)$ и $\mathbf{P} \neq \mathbf{A}(B_1)$ для любого собственного подмножества B_1 множества B. Вполне упорядоченное множество $\langle B; \succ \rangle$ называют *базисом трансцендентности поля* $\mathbf{P}$ относительно поля $\mathbf{A}$, если каждый элемент P — корень некоторого многочлена степени выше нулевой над полем $\mathbf{A}(B)$ и никакое собственное подмножество множества B не обладает таким свойством.

8.2.10. Пользуясь теоремой Цермело, доказать, что любое поле имеет базис относительно каждого подполя.

8.2.11. Пользуясь теоремой Цермело, доказать, что любое поле имеет базис трансцендентности относительно каждого подполя.

Определение 8.2.1. Единственное положительное число, удовлетворяющее уравнению (8.2.1), называют *корнем* k-*й степени* из числа α и обозначают символом $\alpha^{\frac{1}{k}}$.

Вопрос 8.2.12. Пусть α — положительное действительное число, $n, m \in N$; $c \in Z$. Доказать, что:

1) $(\alpha^c)^{\frac{1}{n}} = (\alpha^{cm})^{\frac{1}{nm}} = (\alpha^{\frac{1}{nm}})^{cm}$;

2) $(\alpha^{\frac{1}{n}})^{\frac{1}{m}} = \alpha^{\frac{1}{nm}}$.

Определение 8.2.2 *(рациональная степень)*. Пусть α — положительное действительное число, $c \in Z$, $n \in N$. Полагаем

$$\alpha^{\frac{c}{n}} \rightleftharpoons (\alpha^c)^{\frac{1}{n}}.$$

Вопросы: 8.2.13. Пусть α и β — положительные действительные числа, r, $q \in Q$. Доказать, что:

1) $\alpha^r > 0$;
2) $\alpha^r \cdot \alpha^q = \alpha^{r+q}$;
3) $(\alpha^r)^q = \alpha^{rq}$;
4) $(\alpha\beta)^r = \alpha^r \cdot \beta^r$.

8.2.14*. Пусть α и β — положительные действительные числа; $r \in Q$, $r > 0$. Доказать, что

$$\alpha > \beta \Leftrightarrow \alpha^r > \beta^r.$$

8.2.15*. Пусть α —положительное действительное число, $\alpha > 1$, r, $q \in Q$. Доказать, что

$$r > q \Leftrightarrow \alpha^r > \alpha^q.$$

8.2.16*. Пусть a, b, c_1 и c_2 — действительные числа, $a > 0$, $b > 0$, $n \in N$. Пусть далее:

$$0 < c_1 < a^n < c_2;$$

$$0 < c_1 < b^n < c_2.$$

Доказать, что:

1) $a^n - b^n < (a - b)\, n c_2^{\frac{n-1}{n}}$;

2) $a - b < \dfrac{a^n - b^n}{n c_1^{\frac{n-1}{n}}}$.

8.2.17*. Пусть $\{a_n\}_n$ — последовательность положительных действительных чисел, r — положительное рациональное число. Доказать, что последовательность $\{a_n\}_n$ нулевая тогда и только тогда, если последовательность $\{a_n^r\}_n$ нулевая.

8.2.18*. Пусть $\{a_n\}_n$—ненулевая последовательность действительных положительных чисел; $r \in Q$. Доказать, что последовательность $\{a_n\}_n$ фундаментальна тогда и только тогда, если последовательность $\{a_n^r\}_n$ фундаментальна.

8.2.19. Пусть a — положительное действительное число, c_1, c_2, $r \in Q$. Доказать, что

$$c_1 < r < c_2 \Rightarrow |a^r - a^{c_1}| \leqslant |a^{c_1} - a^{c_2}|.$$

8.2.20*. Пусть $\{a_n\}_n$ — ненулевая последовательность положительных действительных чисел, α — положительное действительное число, $r \in Q$, $r \neq 0$. Доказать, что

$$\{a_n\}_n \mapsto \alpha \Leftrightarrow \{a_n^r\}_n \mapsto \alpha^r.$$

8.2.21. Пусть $\{a_n\}_n$ — последовательность положительных действительных чисел, $\{b_n\}_n$ — фундаментальная последовательность рациональных чисел. Доказать, что если последовательность $\{a_n\}_n$ сходится к 1, то и последовательность $\{a_n^{b_n}\}_n$ сходится к тому же пределу.

8.2.22. Пусть $\{b_n\}_n$ — неограниченно возрастающая последовательность рациональных чисел, $c \in R$, $c > 1$. Доказать, что последовательность $\{c^{b_n}\}_n$ неограниченно возрастает.

8.2.23*. Пусть $\{b_n\}_n$ — нулевая последовательность рациональных чисел, $c \in R$, $c > 0$. Доказать, что последовательность $\{c^{b_n}\}_n$ сходится к 1.

8.2.24. Пусть a — положительное действительное число, c_1, c_2, b — рациональные числа. Доказать, что

$$c_1 \leqslant b \leqslant c_2 \Rightarrow \min(a^{c_1}, a^{-c_2}) \leqslant a^b \leqslant \max(a^{c_2}, a^{-c_1}).$$

8.2.25. Пусть $\{a_n\}_n$ — ненулевая фундаментальная последовательность положительных действительных чисел, $\{b_n\}_n$ — нулевая последовательность рациональных чисел. Доказать, что

$$\{a_n^{b_n}\}_n \mapsto 1.$$

8.2.26. Пусть $\{a_n\}_n$ — ненулевая фундаментальная последовательность положительных действительных чисел, $\{b_n\}_n$ — фундаментальная последовательность рациональных чисел. Доказать, что последовательность $\{a_n^{b_n}\}_n$ фундаментальна.

8.2.27. Доказать, что если $\{a_n\}_n$ и $\{b_n\}_n$ — эквивалентные ненулевые последовательности действительных чисел и $\forall\, (n \in N) b_n \neq 0$, то последовательность $\left\{\frac{a_n}{b_n}\right\}_n$ сходится к 1.

8.2.28. Доказать, что если $\{a_n\}_n$ — ограниченная и ненулевая последовательность действительных положительных чисел, $\{b_n\}_n$ — ограниченная последовательность рациональных чисел, то последовательность $\{a_n^{b_n}\}_n$ ограничена.

8.2.29. Пусть $\{a_n\}_n$ и $\{b_n\}_n$ — эквивалентные ненулевые фундаментальные последовательности положительных действительных чисел, $\{c_n\}_n$ и $\{d_n\}_n$ — эквивалентные последовательности рациональных чисел. Доказать, что:

последовательности $\{a_n^{c_n}\}_n$ и $\{b_n^{d_n}\}_n$ эквивалентны, а каждая из них фундаментальна.

Определение 8.2.3 *(вещественная степень).* Пусть α и β — действительные числа, $\alpha > 0$, $\{a_n\}_n$ — последовательность положительных рациональных чисел, сходящаяся к числу α, и $\{b_n\}_n$ — последовательность рациональных чисел, сходящаяся к β. Полагаем

$$\alpha^\beta \rightleftharpoons \lim_{n\to\infty} a_n^{b_n}.$$

Вопрос 8.2.30. Пусть α, β, r и q — действительные числа, $\alpha > 0$, $\beta > 0$. Доказать, что:

1) $\alpha^r > 0$;
2) $\alpha^r \cdot \alpha^q = \alpha^{r+q}$;
3) $(\alpha^r)^q = \alpha^{rq}$;
4) $(\alpha\beta)^r = \alpha^r \cdot \beta^r$.

8.3. Систематические дроби как аппарат для представления действительных чисел

Обозначения: $\mathbf{R} \rightleftharpoons \langle R;\ +,\ \cdot,\ 0,\ 1\rangle$ — система *действительных* чисел, $\mathbf{Z} \rightleftharpoons \langle Z;\ +,\ \cdot,\ N,\ +,\ \cdot\rangle$ — система *целых* чисел и $\mathbf{N} \rightleftharpoons \langle N;\ +,\ \cdot, 1\rangle$ — система *натуральных* чисел.

Мы предполагаем, что поле действительных чисел — расширение кольца целых, кольцо целых — расширение полукольца натуральных чисел.

Определение 8.3.1. Пусть $\{a_n\}_n$ — последовательность действительных чисел и пусть $S_n \rightleftharpoons \sum\limits_{x=0}^{n} a_x$ для каждого натурального n. Выражение

$$\sum_{x=0}^{\infty} a_x \tag{8.3.1}$$

называют *рядом*. Если последовательность $\{S_n\}_n$ сходится к действительному числу α, то α называют *суммой ряда* (8.3.1) и употребляют запись

$$\sum_{x=0}^{\infty} a_x = \alpha.$$

Теорема 8.3.1. Пусть q — целое $\geqslant 2$. Тогда

$$\sum_{x=0}^{\infty} q^{-x} = \frac{q}{q-1}.$$

Доказательство. Имеем

$$S_n = 1 + \frac{1}{q} + \cdots + \frac{1}{q^n} = \frac{q}{q-1} - \frac{q}{q^{n+1}(q-1)}.$$

Теорема 8.3.2. Пусть q — целое $\geqslant 2$ и $\{a_n\}_n$ — последовательность целых с условием $0 \leqslant a_n \leqslant q-1$. Тогда ряд

$$\sum_{n=0}^{\infty} a_n q^{-n} \tag{8.3.2}$$

сходится. Его сумма α удовлетворяет условию

$$a_0 \leqslant \alpha \leqslant a_0 + 1.$$

При этом равенство $\alpha = a_0 + 1$ возможно только в случае, если

$$\forall\, (n \in N) \quad a_n = q-1.$$

Доказательство. В самом деле, последовательность $\{S_n\}_n$, где $S_n \rightleftharpoons \sum_{x=0}^{n} a_x$, ограничена суммой ряда

$$a_0 + \sum_{n=1}^{\infty} (q-1)\, q^{-n} = a_0 + 1.$$

Теорема 8.3.3. Пусть q — целое $\geqslant 2$. Каждое действительное число α можно представить и притом единственным способом в виде

$$\alpha = \pm q^n \sum_{x=0}^{\infty} a_x q^{-x}, \tag{8.3.3}$$

где:

1) если $\alpha \geqslant 0$, то перед правой частью равенства (8.3.3) выбирается знак $+$; если $\alpha < 0$, то знак $-$;

2) если $\alpha = 0$, то $n = 0 \wedge \forall (x \in Z)\ x \geqslant 0 \Rightarrow a_x = 0$;

3) если $\alpha \neq 0$, то n и все a_x — целые;

$$a_0 > 0 \wedge \forall (x \in Z) \quad x \geqslant 0 \Rightarrow 0 \leqslant a_x \leqslant q-1 \wedge$$
$$\wedge\ \neg\, \exists (n_0 \in N) \quad \forall (x \in N) \quad x \geqslant n_0 \Rightarrow a_x = q-1.$$

Доказательство. Предположим, что $\alpha > 0$ и число α представлено в форме (8.3.3). Из теоремы 8.3.2 следует, что

$$1 \leqslant a_0 \leqslant \sum_{x=0}^{\infty} a_x q^{-x} < a_0 + 1 \leqslant q.$$

Поэтому

$$q^n \leqslant \alpha < q^{n+1}. \tag{8.3.4}$$

Этим условием по теореме 7.4.4 число n определяется однозначно. Но тогда

$$a_0 \leqslant q^{-n}\alpha < a_0 + 1, \tag{8.3.5}$$

и, следовательно, число a_0 определяется однозначно. Далее заметим, что

$$q^m\left(q^{-n}\alpha - \sum_{x=0}^{m-1} a_x q^{-x}\right) = \sum_{x=m}^{\infty} a_x q^{-x+m}$$

и, таким образом,

$$a_m \leqslant q^m\left(q^{-n}\alpha - \sum_{x=0}^{m-1} a_x q^{-x}\right) < a_m + 1. \tag{8.3.6}$$

Итак, коль $a_0, \ldots, a_{m-1}$ определены, то и a_m определяется однозначно. Пусть теперь целые числа n; $a_0, a_1, \ldots$ определены указанным выше способом, т. е. n из условия 8.3.4, числа $a_0, a_1, \ldots$ из условия 8.3.5 и 8.3.6. Тогда имеем

$$a_m q^{-m+n} \leqslant \alpha - q^n \sum_{x=0}^{m-1} a_x q^{-x} < (a_m + 1)\, q^{-m+n},$$

следовательно,

$$\alpha = q^n \sum_{x=0}^{\infty} a_x q^{-x}.$$

Наконец, заметим, что

$$\neg\, \exists\, (n_0 \in N) \quad \forall\, (x \in N) \quad x \geqslant n_0 \Rightarrow a_x = q - 1.$$

Вопросы: **8.3.1***. Доказать, что мощность множества всех действительных чисел интервала (0, 1) равна мощности множества всех подмножеств множества натуральных чисел N.

8.3.2. Доказать, что множество натуральных чисел N и множество всех его подмножеств не равномощны.

Множество, равномощные множеству всех действительных чисел интервала (0, 1), называют *континуальным* (мощности *континуум*).

8.3.3. Доказать, что множество всех действительных чисел — континуальное.

8.3.4. Доказать, что множество всех последовательностей действительных чисел континуальное.

8.4. Категоричность аксиоматической теории действительных чисел

Теорема 8.4.1. Пусть $\langle R;\ +, \cdot, 0, > \rangle$ и $\langle R_1;\ \oplus, \odot, \theta, >_1 \rangle$ — две модели аксиоматической теории действительных чисел. Тогда существует изоморфное отображение одной модели на вторую.

Доказательство. По теореме 6.6.3 поле $\langle R;\ +,\ \cdot,\ 0 \rangle$ есть расширение поля рациональных чисел $\mathbf{Q} \rightleftharpoons \langle Q;\ +,\ \cdot,\ 0 \rangle$, поле $\langle R_1;\ \oplus,\ \odot,\ \theta \rangle$ есть расширение поля рациональных чисел $\mathbf{Q}_1 \rightleftharpoons \langle Q_1;\ \oplus, \odot, \theta \rangle$. По теореме 6.7.1 существует изоморфное отображение φ поля $\mathbf{Q}$ на поле $\mathbf{Q}_1$. По теореме 5.3.2 бинарное отношение в Q_1, наведенное отношением $>$ в Q, есть порядок. Но по теореме 6.6.2 поле рациональных чисел можно упорядочить только одним способом. Из этого следует, что

$$\forall\, (a, b \in Q) \quad a > b \Leftrightarrow \varphi(a) >_1 \varphi(b).$$

Отсюда также следует, что если последовательность $\{a_n\}_n$ элементов поля $\langle Q;\ +,\ \cdot, > \rangle$ фундаментальна, то и последовательность $\{\varphi(a_n)\}_n$ фундаментальна.

Пусть α — какое-нибудь число поля $\langle R;\ +,\ \cdot,\ 0 \rangle$. Тогда α есть предел стационарной последовательности $\{\alpha\}_n$, а следовательно, в силу теорем 7.5.6 и 7.3.8 и предел некоторой последовательности $\{a_n\}_n$ элементов поля $\langle Q;\ +,\ \cdot,\ 0 \rangle$. Но по теореме 7.3.3 эта последовательность фундаментальна, и, следовательно, последовательность $\{\varphi(a_n)\}_n$ фундаментальна и по определению поля действительных чисел сходится к некоторому элементу поля $\langle R_1;\ \oplus,\ \odot,\ \theta \rangle$. Обозначим этот элемент через $\Phi(\alpha)$. Покажем, что определенное так отображение Φ поля $\langle R;\ +,\ \cdot,\ 0 \rangle$ в поле $\langle R_1;\ \oplus,\ \odot,\ \theta \rangle$ есть

взаимно-однозначное отображение множества R на R_1. Заметим прежде всего, что эквивалентные последовательности элементов поля $\mathbf{Q}$ при отображении φ переходят в эквивалентные последовательности элементов поля $\mathbf{Q}_1$. Отсюда следует, что Φ — однозначное отображение множества R в R_1. Столь же нетрудно доказать, что разным элементам множества R отвечают различные элементы множества R_1 и что для каждого элемента из R_1 в R имеется прообраз.

Пусть α и β — какие-либо элементы множества R, $\{a_n\}_n$ и $\{b_n\}_n$ — последовательности элементов поля $\mathbf{Q}$ такие, что

$$\alpha = \lim_{n\to\infty} a_n; \qquad \beta = \lim_{n\to\infty} b_n.$$

Тогда имеем

$$\Phi(\alpha) = \lim_{n\to\infty} \varphi(a_n); \qquad \Phi(\beta) = \lim_{n\to\infty} \varphi(b_n).$$

Отсюда получим

$$\alpha + \beta = \lim_{n\to\infty} (a_n + b_n)$$

и

$$\Phi(\alpha) \oplus \Phi(\beta) = \lim_{n\to\infty} (\varphi(a_n) \oplus \varphi(b_n)).$$

А потому

$$\Phi(\alpha) \oplus \Phi(\beta) = \Phi(\alpha + \beta),$$

так как

$$\varphi(a_n) \oplus \varphi(b_n) = \varphi(a_n + b_n).$$

Аналогично можно показать, что

$$\Phi(\alpha) \odot \Phi(\beta) = \Phi(\alpha \cdot \beta).$$

Наконец, из теорем 5.3.2 и 8.2.3 следует, что

$$\alpha > \beta \Leftrightarrow \alpha \succ \beta.$$

Тем самым изоморфизм двух систем доказан.

Вопрос 8.4.1. Доказать, что поле действительных чисел $\mathbf{R} \rightleftarrows \langle R; +, \cdot, 0\rangle$ не имеет никакого автоморфизма (т. е. изоморфизма $\mathbf{R} \cong \mathbf{R}$), кроме тождественного.

8.5. Непротиворечивость аксиоматической теории действительных чисел

Теорема 8.5.1. Аксиоматическая теория действительных чисел непротиворечива относительно аксиоматической теории рациональных чисел.

Доказательство. Мы построим модель, на которой выполняются все 18 аксиом нашей теории.

1) Пусть F — множество всех фундаментальных последовательностей рациональных чисел. Если $\{a_n\}_n \in F$ и $\{b_n\}_n \in F$, то полагаем:

$$\{a_n\}_n + \{b_n\}_n \rightleftharpoons \{a_n + b_n\}_n;$$
$$\{a_n\}_n \cdot \{b_n\}_n \rightleftharpoons \{a_n \cdot b_n\}_n.$$

В силу теорем 7.3.4 и 7.3.16 введенные отношения — бинарные алгебраические операции на F. Без труда проверяется, что система $\langle F; +, \cdot \rangle$ — коммутативное кольцо с единицей.

2) В силу теоремы 7.3.7 бинарное отношение, введенное определением 7.2.4, является отношением эквивалентности во множестве всех последовательностей рациональных чисел. Условимся обозначать класс эквивалентности α, в который входит последовательность $\{a_n\}_n$, символом $\{\overline{a_n}\}_n$. Таким образом,

$$\alpha \rightleftharpoons \{\overline{a_n}\}_n.$$

Далее, если $\beta \rightleftharpoons \{\overline{b_n}\}_n$, то

$$\alpha = \beta \Leftrightarrow \{a_n\}_n \sim \{b_n\}_n.$$

В силу той же теоремы 7.3.7 это отношение эквивалентности во множестве фундаментальных последовательностей рациональных чисел монотонно относительно сложения и умножения.

Поэтому тернарные отношения, определяемые равенствами,

$$\overline{\{a_n\}_n} + \overline{\{b_n\}_n} \rightleftharpoons \overline{\{a_n + b_n\}_n};$$
$$\overline{\{a_n\}_n} \cdot \overline{\{b_n\}_n} \rightleftharpoons \overline{\{a_n \cdot b_n\}_n},$$

бинарные алгебраические операции на множестве $\overline{F}$ классов эквивалентных последовательностей рациональных чисел. Из теорем 2.9.3, 2.8.2 и 2.8.3 следует, что система $\langle \overline{F}; +, \cdot \rangle$ — коммутативное кольцо с единицей. Таким образом построена интерпретация, на которой первые 10 аксиом нашей теории выполнены.

3) Покажем, что система $\langle \overline{F}; +, \cdot \rangle$ — поле. Так как при гомоморфизме колец нуль переходит в нуль, а единица в единицу, то нуль кольца $\langle \overline{F}; +, \cdot \rangle$ — это класс, содержащий стационарную последовательность $\{0\}_n$, а единица — класс, содержащий стационарную последовательность $\{1\}_n$. Пусть класс $\alpha \rightleftharpoons \{\overline{a_n}\}_n$ не является нулем кольца $\langle \overline{F}; +, \cdot \rangle$. В таком случае последовательности $\{a_n\}_n$ и $\{0\}_n$ неэквивалентны, и, следовательно, последовательность $\{a_n\}_n$ не сходится к нулю. Но тогда по теореме 7.3.10 существуют рациональное число ε и подпоследовательность последовательности $\{a_n\}_n$ такие, что

$$\forall (n \in N) \quad |a_{k_n}| \geqslant \varepsilon.$$

В силу теоремы 7.3.2 $\alpha = \overline{\{a_{k_n}\}_n}$, а в силу теоремы 7.3.16 последовательность $\left\{\frac{1}{a_{k_n}}\right\}$ фундаментальна. Пусть $\gamma \rightleftharpoons \overline{\left\{\frac{1}{a_{k_n}}\right\}_n}$.

Нетрудно видеть, что $\alpha \cdot \gamma = \{1\}_n$. Таким образом, система $\langle \overline{F}; +, \cdot \rangle$ — поле.

4) Введем в поле $\langle \overline{F};\ +,\ \cdot \rangle$ линейный порядок. Положительную часть $\overline{F}^+$ определим условием

$$\alpha \in \overline{F}^+ \Leftrightarrow \exists\,(\varepsilon \in Q^+)\,\exists\,(n_0 \in N)\ \forall\,(n \in N)\quad n \geqslant n_0 \Rightarrow a_n \geqslant \varepsilon.$$

Покажем прежде всего, что принадлежность класса α к $\overline{F}^+$ не зависит от выбора представителя класса. В самом деле, если $\{a_n\}_n \sim \{b_n\}_n$, то существует такое натуральное число n_1, что

$$\forall\,(n \in N)\quad n \geqslant n_1 \Rightarrow |b_n - a_n| < \frac{1}{2}\varepsilon.$$

Поэтому

$$\forall\,(n \in N)\quad n \geqslant \max(n_0, n_1) \Rightarrow b_n > a_n - \frac{1}{2}\varepsilon \geqslant \frac{1}{2}\varepsilon.$$

Далее, пусть класс α ненулевой. В силу теоремы 7.4.1 либо α, либо $-\alpha$ принадлежит к $\overline{F}^+$. Наконец, совсем нетрудно проверить, что

$$\forall\,(\alpha, \beta \in \overline{F}^+)\quad \alpha + \beta \in \overline{F}^+;$$

$$\forall\,(\alpha, \beta \in \overline{F}^+)\quad \alpha \cdot \beta \in \overline{F}^+.$$

Тем самым система $\langle \overline{F};\ +,\ \cdot,\ \overline{F}^+\rangle$ — упорядоченное поле. Полезно отметить следующее свойство, вытекающее из определения. Пусть $\alpha, \beta \in \overline{F}$,

$$\alpha \rightleftharpoons \overline{\{a_n\}_n},\quad \beta \rightleftharpoons \overline{\{b_n\}_n}.$$

Если $\exists\ (n_0 \in N)\ \forall\ (n \in N)\ n \geqslant n_0 \Rightarrow a_n > b_n$, то $\alpha \geqslant \beta$. Покажем, что введенный порядок архимедов. Пусть $\alpha, \beta \in \overline{F}^+$. Тогда

$$\exists\,(\varepsilon \in Q^+) \wedge \exists\,(c \in Q^+)$$

такие, что

$$\exists\,(n_0 \in N)\ \forall\,(n \in N)\quad n \geqslant n_0 \Rightarrow a_n > \varepsilon \wedge c > b_n.$$

Так как порядок в поле рациональных чисел архимедов, то существует натуральное k такое, что

$$k \cdot \varepsilon > c.$$

А в таком случае

$$\forall\,(n \in N)\quad n \geqslant n_0 \Rightarrow k \cdot a_n > b_n,$$

и в силу отмеченного свойства

$$k \cdot \alpha \geqslant \beta.$$

Итак, в построенной интерпретации нашей теории выполнены первые пятнадцать аксиом.

5) Докажем, что любая фундаментальная последовательность элементов нашей системы сходится. Для этого выберем некоторое подполе упорядоченного поля $\langle \overline{F};\ +,\ \cdot, \overline{F}^+\rangle$ и докажем, что любая фундаментальная последовательность выбранного подполя сходится в $\overline{F}$. Из теорем 7.3.8 и 7.5.6 и будет следовать наше утверждение. Сначала определим подмножество P множества $\overline{F}$. Элемент α мно-

жества $\overline{F}$ отнесем к P в том и только том случае, если класс α содержит стационарную последовательность, т. е. если для некоторого рационального a

$$\alpha = \overline{\{a\}}_n.$$

Легко проверить, что отображение

$$a \mapsto \overline{\{a\}}_n$$

является изоморфным отображением поля рациональных чисел на систему $\mathbf{P} \rightleftharpoons \langle P;\ +,\ \cdot \rangle$. Отсюда следует, что система $\mathbf{P}$ — поле. Заметим, что $\overline{\{a\}}_n \in \overline{F}^+$ тогда и только тогда, если a — положительное рациональное число. Поэтому в указанном отображении фундаментальной последовательности элементов одного поля отвечает фундаментальная последовательность элементов второго поля.

Пусть

$$\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_k,\ \ldots;\qquad \alpha_k \rightleftharpoons \overline{\{a_k\}}_n — \tag{8.5.1}$$

какая-нибудь фундаментальная последовательность элементов поля $\mathbf{P}$. В силу сделанного замечания последовательность

$$a_1,\ a_2,\ \ldots,\ a_k,\ \ldots — \tag{8.5.2}$$

фундаментальная последовательность рациональных чисел. Рассмотрим класс $\alpha \rightleftharpoons \overline{\{a_n\}}_n$ и докажем, что $\lim\limits_{k\to\infty} \alpha_k = \alpha$. Пусть $\varepsilon \rightleftharpoons \overline{\{e\}}_n$, где e — положительное рациональное число. Так как последовательность (8.5.2) фундаментальна, то существует натуральное число n_0 такое, что для любого $k \geqslant n_0$

$$\forall\, (n \in N)\ n \geqslant n_0 \Rightarrow |a_k - a_n| < e.$$

Отсюда следует, что

$$\forall\, (k \in N)\ k \geqslant n_0 \Rightarrow |\alpha_k - \alpha| \leqslant \varepsilon.$$

Другими словами, последовательность (8.5.1) сходится к элементу множества $\overline{F}$. Этим завершается доказательство теоремы.

8.6. Система p-адических чисел

Тот же путь, который в связи с естественным нормированием поля рациональных чисел приводит к понятию действительного числа, в связи с p-адическим нормированием приводит к понятию p-адического числа. Систему p-адических чисел можно определить как минимальное нормированное расширение поля рациональных чисел, в котором всякая фундаментальная по p-адической норме ν_p последовательность рациональных чисел сходится по норме ν_p. Отдельные части этой фразы требуют дополнительных пояснений, но, вместо того чтобы давать такие пояснения, мы попытаемся дать достаточно подробную схему построения аксиоматической теории p-адических чисел.

Первичные термины.

а) Q, R и Q_p — *множества;* их элементы называются *рациональными, действительными* и *p-адическими числами* соответственно.

б) $+$ и $\cdot$ — *тернарные* отношения в них (для большей четности следовало бы пользоваться набором из трех пар символов).

в) $>$ — *бинарные* отношения в Q и в R (для большей четкости следовало бы пользоваться двумя символами).

г) 0, e, $p * e$ — *элементы* Q, p — *простое число.*

д) ν и ϑ — *отображения* $\mathbf{Q}$ и $\mathbf{Q}_p$ соответственно в R.

Аксиомы.

1. $\mathbf{R} \rightleftharpoons \langle R;\ +,\ \cdot,\ 0,\ 1,\ > \rangle$ — система действительных чисел.

2. $\mathbf{Q} \rightleftharpoons \langle Q;\ +,\ \cdot,\ 0,\ e \rangle$ — поле рациональных чисел и $p * e$ — простой элемент поля $\mathbf{Q}$.

3. $\langle \mathbf{Q};\ \mathbf{R};\ \nu \rangle$ — нормированное поле, в котором последовательность $\{p^n * e\}_n$ нулевая по норме ν, т. е. ν является p-адической нормой.

4. $\mathbf{Q}_p \rightleftharpoons \langle Q_p;\ +,\ \cdot \rangle$ — поле.

5. $\langle \mathbf{Q}_p;\ \mathbf{R};\ \vartheta \rangle$ — нормированное поле.

6. Поле $\mathbf{Q}_p$ — расширение поля $\mathbf{Q}$.

7. Норма ϑ — продолжение нормы ν, т. е. $\forall\,(a \in Q)\ \nu\,(a) = \vartheta\,(a)$.

8. Всякая фундаментальная по норме ν последовательность элементов Q сходится по норме ϑ к элементу из $\mathbf{Q}_p$.

9. *Аксиома минимальности.* Пусть M — подмножество Q_p такое, что всякая фундаментальная по норме ν последовательность элементов Q сходится по норме ϑ к элементу из M; тогда $M = Q_p$.

Вопросы: 8.6.1. Доказать, что каждое p-адическое число — предел по норме ϑ последовательности рациональных чисел.

8.6.2. Доказать, что для любых α из Q_p и ε из Q^+ существует в Q элемент a такой, что

$$\vartheta\,(\alpha - a) < \varepsilon.$$

8.6.3. Доказать, что для любой последовательности p-адических чисел существует эквивалентная ей по норме ϑ последовательность рациональных чисел.

8.6.4. Доказать, что любая фундаментальная по норме ϑ последовательность p-адических чисел сходится по норме ϑ в Q_p.

8.6.5. Доказать, что каждое отличное от нуля p-адическое число α может быть представлено и притом единственным способом в виде

$$\alpha = p^n \sum_{x=0}^{\infty} a_x p^x, \qquad (8.6.1)$$

где n и a_x — целые; $\forall\,(x \in Z)\ x \geqslant 0 \Rightarrow 0 \leqslant a_x \leqslant p - 1,\ a_0 \neq 0$.

8.6.6. Найти представление -1 в форме (8.6.1).

8.6.7. Решить в поле $\mathbf{Q}_5$ уравнение $x^2 + 1 = 0$.

8.6.8. Доказать, что не существует изоморфного отображения поля $\mathbf{Q}_p$ в поле $\langle R;\ +\ ,\ \cdot \rangle$.

8.6.9. Пусть p и q — различные простые. Доказать, что не существует изоморфного отображения $\mathbf{Q}_p$ на $\mathbf{Q}_q$.

8.6.10. Доказать, что для любых двух систем p-адических чисел $\langle \mathbf{Q}_p; \mathbf{R}; \vartheta \rangle$ и $\langle \mathbf{Q}'_p; \mathbf{R}'; \vartheta' \rangle$ можно найти изоморфное отображение φ поля $\mathbf{Q}_p$ на поле $\mathbf{Q}'_p$, которое любую нулевую по норме ϑ последовательность элементов поля $\mathbf{Q}_p$ переводит в нулевую по норме ϑ' последовательность элементов поля $\mathbf{Q}'_p$ (категоричность).

8.6.11. Доказать, что множество всех p-адических чисел континуальное.

8.6.12. Доказать, что базис трансцендентности поля p-адических чисел относительно поля рациональных чисел — континуальное множество.

Теорема 8.6.1. Аксиоматическая теория p-адических чисел непротиворечива.

Доказательство. В предположении, что аксиоматические теории рациональных и действительных чисел непротиворечивы, мы докажем непротиворечивость аксиоматической теории p-адических чисел. Для этой цели мы построим модель, на которой выполняются все аксиомы нашей теории.

План доказательства:

1) Построение поля $\mathbf{Q}_p$.

2) Включение поля $\mathbf{Q}$ рациональных чисел.

3) Определение нормы ϑ в поле $\mathbf{Q}_p$.

4) Проверка сходимости фундаментальной по норме ν последовательности элементов поля $\mathbf{Q}$ в поле $\mathbf{Q}_p$.

5) Проверка выполнения аксиомы минимальности.

Пусть $\mathbf{R} \rightleftharpoons \langle R; +, \cdot, > \rangle$ — какая-либо система действительных чисел и $\mathbf{Q}^* \rightleftharpoons \langle Q^*; +, \cdot, 1 \rangle$ — ее подполе — поле рациональных чисел, p — простое число и ν_p — p-адическая норма в поле $\mathbf{Q}$.

1а) Выбором системы $\mathbf{R}$ мы обеспечили выполнение первой аксиомы. Далее рассуждаем так. Рассмотрим множество F фундаментальных по норме ν_p последовательностей поля $\mathbf{Q}^*$. Определим на множестве F два тернарных отношения $\oplus$ и $\odot$ и бинарное отношение $\sim$ следующим образом:

$$\{a_n\}_n \oplus \{b_n\}_n \rightleftharpoons \{a_n + b_n\}_n;$$

$$\{a_n\}_n \odot \{b_n\}_n \rightleftharpoons \{a_n \cdot b_n\}_n;$$

$$\{a_n\}_n \sim \{b_n\}_n \overset{\text{Df}}{\Leftrightarrow} \{a_n - b_n\}_n \underset{\nu_p}{\to} 0.$$

Легко проверить, что система $\langle F; \oplus, \odot \rangle$ — коммутативное кольцо, а отношение $\sim$ — отношение эквивалентности на F. Пусть $Q_p \rightleftharpoons \overline{F}$ — множество классов эквивалентности множества F. В силу того что отношение эквивалентности на F монотонно относительно обеих операций $\oplus$ и $\odot$, тернарные отношения на $\overline{F}$, определяемые условиями:

$$\overline{\{a_n\}_n} + \overline{\{b_n\}_n} \rightleftharpoons \overline{\{a_n\}_n \oplus \{b_n\}_n},$$

$$\overline{\{a_n\}_n} \cdot \overline{\{b_n\}_n} \rightleftharpoons \overline{\{a_n\}_n \odot \{b_n\}_n},$$

суть бинарные алгебраические операции на $\overline{F}$.

1б) Можно показать, что система $\langle F;\ +,\ \cdot\rangle$ — коммутативное кольцо, нулем которого является класс θ, содержащий все нулевые по норме ν_p последовательности элементов Q^*.

1в) Нетрудно доказать, что система $\mathbf{Q}_p \rightleftharpoons \langle \bar{F};\ +,\ \cdot\rangle$ — поле (аксиома 4).

2) Выделим в множестве $\bar{F}$ подмножество Q тех классов α, каждый из которых содержит стационарную последовательность элементов Q^*; другими словами,

$$\alpha \in Q \overset{\text{Df}}{\Leftrightarrow} \exists (a \in Q^*)\quad \alpha = \overline{\{a\}}_n.$$

Рассмотрим отображение φ множества Q^* на Q, определяемое условием

$$\varphi\colon a \mapsto \overline{\{a\}}_n.$$

Легко проверить, что φ — изоморфное отображение поля $\mathbf{Q}^*$ на систему $\mathbf{Q} \rightleftharpoons \langle Q;\ +,\ \cdot\rangle$. Отсюда следует, что система $\mathbf{Q}$ — поле и, более того, является полем рациональных чисел, а поле $\mathbf{Q}_p$ — расширение поля $\mathbf{Q}$. Единицей поля $\mathbf{Q}$ является элемент $e \rightleftharpoons \overline{\{1\}}_n$. Нетрудно усмотреть, что $p * e$ — простой элемент поля $\mathbf{Q}$. Таким образом, аксиомы 2 и 6 выполняются.

3а) Пусть $\alpha \rightleftharpoons \overline{\{a\}}_n$ — какой-нибудь элемент $\mathbf{Q}$. Определим отображение ν поля $\mathbf{Q}$ в систему $\mathbf{R}$ условием

$$\nu(\alpha) \rightleftharpoons \nu_p(a).$$

Легко проверить, что ν — норма поля $\mathbf{Q}$ и что последовательность $\{p^n * e\}_n$ — нулевая по норме ν. Таким образом, аксиома 3 выполнена.

3б) В силу теоремы 7.3.9 если последовательность $\{a_n\}_n$ элементов Q^* фундаментальна по норме ν_p, то и последовательность $\{\nu_p(a_n)\}_n$ фундаментальна и, следовательно, сходится в R. Далее, если последовательности $\{a_n\}_n$ и $\{b_n\}_n$ из F эквивалентны по норме ν_p, то и последовательности $\{\nu_p(a_n)\}_n$ и $\{\nu_p(b_n)\}_n$ эквивалентны. Из этих замечаний следует, что отображение ϑ множества Q_p в R, определяемое условием

$$\vartheta\colon \alpha \rightleftharpoons \overline{\{a_n\}}_n \mapsto \lim_{h\to\infty} \nu_p(a_n),\ —$$

однозначное отображение множества Q_p в R. Без труда проверяется выполнение аксиом 5 и 7.

4) Рассуждая как при доказательстве теоремы 8.5.1, нетрудно убедиться в том, что любая фундаментальная по норме ν последовательность элементов поля $\mathbf{Q}$ сходится по норме ϑ к элементу поля $\mathbf{Q}_p$.

5) Пусть $\alpha \rightleftharpoons \overline{\{a_n\}}_n$ — произвольный элемент Q_p. Рассуждая как при доказательстве теоремы 8.5.1, мы покажем, что последовательность $\alpha_1, \ldots, \alpha_k, \ldots, \alpha_k \rightleftharpoons \overline{\{a_k\}}_n$ элементов Q сходится по норме ϑ к α. Отсюда следует, что и аксиома 9 выполняется.

Тем самым построение поля p-адических чисел завершено.

8.7. Конечные и бесконечные цепные дроби

Буквой n в этом разделе мы будем обозначать целое число, буквой ω — неотрицательное целое число k или символ ∞. В последнем случае условимся, что

$$\omega + 1 \rightleftharpoons \omega$$

и $n < \omega$ для любого целого числа n.

Определение 8.7.1. Пусть $a \rightleftharpoons \{a_n\}_{n=0}^{\omega}$ — конечная или бесконечная последовательность целых чисел, все члены которой, кроме, быть может, a_0,— натуральные числа. Выражение

$$a_0 + \cfrac{1}{a_1 + \cfrac{\ddots}{\ddots + \cfrac{1}{a_k}}}$$

в случае, если $\omega \rightleftharpoons k$, или

$$a_0 + \cfrac{1}{a_1 + \cfrac{\ddots}{\ddots + \cfrac{1}{a_n + \ddots}}}$$

в случае, если $\omega \rightleftharpoons \infty$, называют *цепной дробью последовательности* a или цепной дробью порядка ω. Любой член последовательности a называют *элементом* или *неполным частным* этой цепной дроби. Для каждого неотрицательного целого n, если $n < \omega + 1$, конечную цепную дробь

$$\delta_n = [a_0;\ a_1,\ \ldots,\ a_n] \rightleftharpoons a_0 + \cfrac{1}{a_1 + \cfrac{\ddots}{\ddots + \cfrac{1}{a_n}}}$$

называют ее *подходящей дробью порядка* n (определение 4.8.3).

Определение 8.7.2. Пусть $a \rightleftharpoons \{a_n\}_{n=0}^{\omega}$ — последовательность целых чисел, все члены которой, кроме, быть может, a_0,— натуральные числа. *Подходящей функцией порядка* n цепной дроби последовательности a называют функцию $\delta_n(x)$, удовлетворяющую условиям:

1) $\delta_0(x) \rightleftharpoons x$;

2) $\forall (n \in Z) \quad 0 \leqslant n < \omega \Rightarrow \delta_{n+1} \rightleftharpoons \delta_n(a_n + \frac{1}{x})$.

Функция $\delta_n(x)$ определена для всех положительных значений переменного x. Легко видеть, что:

1) $\delta_n(a_n) = \delta_n$;
2) $\delta_1(x) = a_0 + \frac{1}{x}$.

Определение 8.7.3. Пусть $a \rightleftharpoons \{a_n\}_{n=0}^{\omega}$ — последовательность целых чисел, все члены которой, начиная с a_1,— натуральные числа. Полагаем:

1) $P_{-2} \rightleftharpoons 0, \quad P_{-1} \rightleftharpoons 1,$
   $Q_{-2} \rightleftharpoons 1, \quad Q_{-1} \rightleftharpoons 0;$
2) $\forall (n \in Z) \quad 0 \leqslant n < \omega + 1.$

$$\left.\begin{aligned} P_n &= a_n P_{n-1} + P_{n-2}; \\ Q_n &= a_n Q_{n-1} + Q_{n-2}. \end{aligned}\right\} \qquad (8.7.1)$$

Легко видеть, что $(0 < \omega)$:

$$P_0 = a_0, \quad P_1 = a_1 a_0 + 1;$$
$$Q_0 = 1, \quad Q_1 = a_1.$$

Числа P_n называют *числителями*, а Q_n — *знаменателями* подходящих дробей.

Из определения 8.7.3 следует теорема:

Теорема 8.7.1. Если $0 \leqslant n < \omega$, то

$$Q_{n+1} \geqslant Q_n + Q_{n-1};$$

Следствие 1. Если $0 \leqslant n < \omega$, то

$$Q_{n+1} \geqslant Q_n \geqslant 1.$$

Следствие 2. Если $1 \leqslant n < \omega$, то

$$Q_{n+1} > Q_n.$$

Следствие 3. Если $\omega \rightleftharpoons \infty$, то

$$\lim_{n \to \infty} Q_n = \infty.$$

Индукцией по n из формул (8.7.1) легко выводится:

Теорема 8.7.2. Если $0 \leqslant n < \omega + 1$, то

$$Q_n P_{n-1} - Q_{n-1} P_n = (-1)^n;$$

Следствие 1. Если $0 \leqslant n < \omega + 1$, то

$$(P_n, Q_n) = 1,$$

т. е. для всех допустимых значений n целые числа P_n и Q_n **взаимно просты.**

Следствие 2. Если $0 \leqslant n < \omega + 1$, то

$$(Q_n, Q_{n-1}) = 1,$$

Теорема 8.7.3. Если $0 \leqslant n < \omega + 1$, то

$$\delta_n(x) = \frac{xP_{n-1} + P_{n-2}}{xQ_{n-1} + Q_{n-2}}, \tag{8.7.2}$$

Доказательство. Имеем

$$\delta_0(x) = x = \frac{x \cdot 1 + 0}{x \cdot 0 + 1} = \frac{xP_{-1} + P_{-2}}{xQ_{-1} + Q_{-2}}.$$

Предположим, что для некоторого n с условием $0 \leqslant n < \omega$ равенство (8.7.2) верно. Имеем

$$\delta_{n+1}(x) = \delta_n\left(a_n + \frac{1}{x}\right) = \frac{\left(a_n + \frac{1}{x}\right)P_{n-1} + P_{n-2}}{\left(a_n + \frac{1}{x}\right)Q_{n-1} + Q_{n-2}}.$$

Поэтому

$$\delta_{n+1}(x) = \frac{x(a_nP_{n-1} + P_{n-2}) + P_{n-1}}{x(a_nQ_{n-1} + Q_{n-2}) + Q_{n-1}}.$$

Отсюда в силу (8.7.1) получаем

$$\delta_{n+1}(x) = \frac{xP_n + P_{n-1}}{xQ_n + Q_{n-1}}.$$

Теорема 8.7.4. Если $0 \leqslant n < \omega$, то

$$\delta_n = \frac{P_n}{Q_n}.$$

Доказательство. Имеем

$$\delta_0 = a_0 = \frac{a_0}{1} = \frac{P_0}{Q_0}.$$

Пусть $1 \leqslant n < \omega + 1$. Имеем

$$\delta_n = \delta_n(a_n).$$

Воспользовавшись доказанной теоремой, получаем

$$\delta_n = \frac{a_nP_{n-1} + P_{n-2}}{a_nQ_{n-1} + Q_{n-2}} = \frac{P_n}{Q_n}.$$

Из теорем 8.7.3, 8.7.4 и 8.7.2 легко следует теорема.

Теорема 8.7.5. Если $1 \leqslant n < \omega + 1$, то

$$\delta_n(x) - \delta_{n-1} = \frac{(-1)^{n-1}}{Q_{n-1}(xQ_{n-1} + Q_{n-2})}. \tag{8.7.3}$$

Теорема 8.7.6. Если $1 \leqslant n < \omega + 1$, то

$$\delta_n - \delta_{n-1} = \frac{(-1)^{n-1}}{Q_nQ_{n-1}}.$$

Доказательство. Полагая в тождестве (8.7.3) $x = a_n$ и замечая, что

$$Q_n = a_n Q_{n-1} + Q_{n-2},$$

мы немедленно убеждаемся в справедливости нашего утверждения.

Легко видеть, что функция $\delta_n(x)$ дифференцируема для каждого $x > 0$ и, более того, из теоремы 8.7.3 без труда выводится:

Теорема 8.7.7. Если $0 \leqslant n < \omega + 1$, то

$$\frac{d}{dx}\delta_n(x) = \frac{(-1)^n}{(xQ_{n-1} + Q_{n-2})^2}.$$

Теорема 8.7.8. Если $0 < n < n+1 < \omega$ и n нечетно, то

$$\delta_{n-1} < \delta_{n+1} < \delta_{n+2} < \delta_n.$$

Доказательство. Легко видеть, что

$$\delta_n = \delta_n(a_n);$$

$$\delta_{n+1} = \delta_n\left(a_n + \frac{1}{a_{n+1}}\right);$$

$$\delta_{n+2} = \delta_n\left(a_n + \frac{1}{a_{n+1} + \dfrac{1}{a_{n+2}}}\right);$$

$$\delta_{n-1} = \lim_{x\to\infty} \delta_n(x).$$

С другой стороны,

$$a_n < a_n + \frac{1}{a_{n+1} + \dfrac{1}{a_{n+2}}} < a_n + \frac{1}{a_{n+1}} < \infty.$$

Отсюда и из теоремы 8.7.7 сразу следует наше утверждение.

Следствие 1. Последовательность подходящих дробей данной цепной дроби четного порядка возрастает, а последовательность подходящих дробей нечетного порядка убывает; любая подходящая дробь четного порядка меньше каждой подходящей дроби нечетного порядка.

Следствие 2. Если $0 \leqslant n < \omega + 1$, то $\delta_n \geqslant a_0$; при этом $\delta_n = a_0$ только в случае, если $n = 0$.

Из доказанной теоремы и теоремы 8.7.6 следует теорема.

Теорема 8.7.9. Для каждой бесконечной цепной дроби существует предел последовательности ее подходящих дробей.

Определение 8.7.4. Пусть $a \rightleftharpoons \{a_n\}_{n=0}^{\omega}$ — последовательность целых чисел, все члены которой, начиная с a_1, положительны. *Значением цепной дроби* последовательности a называют ее подходящую дробь порядка ω, если $\omega < \infty$, и предел последовательности ее подходящих дробей в случае, если $\omega \rightleftharpoons \infty$. *Полным частным порядка n цепной дроби* последовательности a, если $n < \omega + 1$, называют значение цепной дроби последовательности $\{a_x\}_{x=n}^{\omega}$, т. е.

значение цепной дроби

$$a_n + \cfrac{1}{a_{n+1} + \ddots + \cfrac{1}{a_k}},$$

если $\omega \rightleftharpoons k$, или цепной дроби

$$a_n + \cfrac{1}{a_{n+1} + \ddots + \cfrac{1}{a_m + \ddots}},$$

если $\omega \rightleftharpoons \infty$.

Символом α_n для каждого n мы обозначаем дальше полное частное цепной дроби последовательности a.

Итак, α_0 — значение цепной дроби последовательности a.

Подобно тому как значение конечной цепной дроби

$$a_0 + \cfrac{1}{a_1 + \ddots + \cfrac{1}{a_k}}$$

мы обозначаем символом $[a_0; a_1, \ldots, a_k]$, так и значение бесконечной цепной дроби последовательности $\{a_n\}_{n=0}^{\infty}$ мы будем обозначать выражением $[a_0; a_1, \ldots, a_n, \ldots]$.

Теорема 8.7.10. Если $0 \leqslant n < \omega + 1$, то

$$\alpha_n \geqslant a_n \tag{8.7.4}$$

и равенство возможно только в случае, если $\omega = n$.

Доказательство. Легко видеть, что наше утверждение достаточно доказать для $n = 0$. Если данная цепная дробь конечна и имеет порядок $\omega = k$, то $\alpha_0 = \delta_k$. Вместе с тем $a_0 = \delta_0$. Но по доказанному (теорема 8.7.8, следствие 1) для любого n, если $0 \leqslant n < \omega + 1$,

$$\delta_n \geqslant \delta_0$$

и равенство возможно только в случае, если $n = 0$. Если данная дробь бесконечна, то

$$\alpha_0 = \lim_{n \to \infty} \delta_n.$$

Отсюда легко следует наше утверждение и в этом случае.

Теорема 8.7.11. Если $0 \leqslant n < \omega + 1$, то

$$\alpha_0 = \frac{\alpha_n P_{n-1} + P_{n-2}}{\alpha_n Q_{n-1} + Q_{n-2}} = \delta_n(\alpha_n). \tag{8.7.5}$$

Доказательство. Подходящую дробь порядка m цепной дроби последовательности $\{a_x\}_{x=n}^{\omega}$ условимся обозначать символом σ_m. Итак, имеем:

$$\sigma_m = [a_n;\ a_{n+1},\ \ldots,\ a_{n+m}].$$

Нетрудно заметить, что

$$\delta_{n+m} = [a_0;\ \ldots,\ a_{n+m}] = [a_0;\ \ldots,\ a_{n-1},\ [a_n;\ a_{n+1},\ \ldots,\ a_{n+m}]] =$$
$$= \delta_n(\sigma_m).$$

Отсюда и из теоремы 8.7.3 получаем:

$$\delta_{n+m} = \frac{\sigma_m P_{n-1} + P_{n-2}}{\sigma_m Q_{n-1} + Q_{n-2}}. \tag{8.7.6}$$

Пусть сначала $\omega \rightleftharpoons k < \infty$. Тогда выбираем m так, что $n + m = k$. При этом условии $\delta_{n+m} = \alpha_0$ и $\sigma_m = \alpha_n$, что доказывает теорему. Пусть теперь $\omega \rightleftharpoons \infty$. Имеем:

$$\alpha_0 = \lim_{n\to\infty} \delta_n;$$

$$\alpha_n = \lim_{m\to\infty} \sigma_m.$$

Отсюда и из равенства (8.7.6) следует справедливость нашего утверждения и в этом случае.

Следствие 1. Если $\omega > 0$, то

$$\alpha_0 = a_0 + \frac{1}{\alpha_1}.$$

Следствие 2. Если $\omega > n$, то

$$\alpha_n = a_n + \frac{1}{\alpha_{n+1}}.$$

Следствие 3. Если $0 \leqslant n < \omega + 1$, то

$$\alpha_n = \frac{P_{n-2} - \alpha_0 Q_{n-2}}{\alpha_0 Q_{n-1} - P_{n-1}}.$$

Теорема 8.7.12. Если $1 \leqslant n < \omega + 1$, то

$$\alpha_0 - \delta_{n-1} = \frac{(-1)^{n-1}}{Q_{n-1}(\alpha_n Q_{n-1} + Q_{n-2})}.$$

Следствие 1. Если $0 \leqslant n < \omega$, то

$$\alpha_0 - \delta_n = \frac{(-1)^n}{Q_n(\alpha_{n+1} Q_n + Q_{n-1})}.$$

Следствие 2. Если $0 \leqslant n < \omega$, то

$$\alpha_0 > \delta_n$$

при n четном и

$$\alpha_0 < \delta_n$$

при n нечетном.

Определение 8.7.5. Пусть $a \leftrightarrows \{a_n\}_{n=0}^{\omega}$ — последовательность целых чисел, все члены которой, начиная с a_1, положительны. *Последовательность* a будем называть *канонической,* если $\omega \leftrightarrows \infty$, или $\omega \leftrightarrows 0$, или если $1 \leqslant \omega \leftrightarrows k < \infty$ и $a_k \geqslant 2$. *Цепную дробь* канонической последовательности будем называть *канонической.*

Теорема 8.7.13. Для канонической цепной дроби, если $0 \leqslant n < \omega + 1$, то

$$a_n = [\alpha_n],$$

т. е. неполное частное a_n равно целой части ее полного частного.

Доказательство. Наше утверждение очевидно, если $\omega \leftrightarrows n$. Пусть $\omega > n$. По доказанному (теорема 8.7.11, следствие 2)

$$\alpha_n = a_n + \frac{1}{\alpha_{n+1}}.$$

Если $\omega > n + 1$, то в силу теоремы 8.7.10

$$\alpha_{n+1} > a_{n+1} \geqslant 1.$$

Если $\omega = n + 1$, то

$$\alpha_{n+1} = a_{n+1},$$

что $\geqslant 2$, так как цепная дробь каноническая. Итак, если $0 \leqslant n < \omega$, то $\alpha_{n+1} > 1$. Это и доказывает наше утверждение.

Теорема 8.7.14 Пусть $a \leftrightarrows \{a_n\}_{n=0}^{\omega}$, $b \leftrightarrows \{b_n\}_{n=0}^{\omega'}$ — канонические последовательности целых чисел. Значения α_0 и β_0 цепных дробей последовательностей a и b соответственно равны тогда и только тогда, если последовательности a и b одного порядка и если равны их соответствующие члены.

Доказательство. Предположим, что

$$\alpha_0 = \beta_0,$$

и докажем, что

$$a_n = b_n,$$

если $0 \leqslant n < \omega + 1$.

В силу теоремы 8.7.13 нам достаточно показать, что

$$\forall (n \in Z) \quad 0 \leqslant n < \omega + 1 \Rightarrow \alpha_n = \beta_n.$$

Символами α_n и β_n мы обозначаем полные частные порядки n цепных дробей последовательностей a и b соответственно.

Пусть для некоторого целого n $(n < \infty)$

$$\alpha_n = \beta_n.$$

Но в силу теоремы 8.7.13

$$a_n = [\alpha_n], \quad b_n = [\beta_n].$$

Итак, $a_n = b_n$. Но

$$\alpha_n = a_n + \frac{1}{\alpha_{n+1}}, \quad \beta_n = b_n + \frac{1}{\beta_{n+1}}.$$

Отсюда следует, что

$$\alpha_{n+1} = \beta_{n+1}.$$

Обратное утверждение теоремы очевидно.

Теорема 8.7.15 (представление действительных чисел цепными дробями). Для любого действительного числа r существует и только одна каноническая цепная дробь, значение которой равно r. Порядок этой дроби конечен, если число r рациональное, и бесконечен в противном случае.

Доказательство. Единственность требуемого представления следует из теоремы 8.7.14. Существование. Полагаем

$$a_0 \rightleftharpoons [r].$$

Если r не целое, то полагаем

$$r = a_0 + \frac{1}{r_1},$$

где $r_1 > 1$. Полагаем

$$a_1 \rightleftharpoons [r_1].$$

Если r_1 не целое, то полагаем

$$r_1 = a_1 + \frac{1}{r_2},$$

где $r_2 > 1$. Так, продолжая дальше, мы получим последовательность $a \rightleftharpoons \{a_x\}_{x=0}^{\omega}$ целых чисел. Заметим, что все члены этой последовательности, начиная с a_1, положительны. Если эта последовательность конечна, т. е. если $\omega \rightleftharpoons k < \infty$, то

$$a_k = [r_k] = r_k > 1$$

и потому $a_k \geqslant 2$. Поэтому полученная последовательность каноническая. Докажем, что ее значение равно числу r. Для каждой подходящей функции порядка $n < \omega$ цепной дроби последовательности a

$$\delta_n\left(a_n + \frac{1}{x}\right) = \delta_{n+1}(x).$$

Поэтому

$$\delta_n(r_n) = \delta_n\left(a_n + \frac{1}{r_{n+1}}\right) = \delta_{n+1}(r_{n+1}).$$

Но

$$r = a_0 + \frac{1}{r_1} = \delta_1(r_1).$$

Отсюда следует, что

$$r = \delta_n(r_n), \tag{8.7.7}$$

если $0 \leqslant n < \omega + 1$. Пусть $\omega \rightleftharpoons k < \infty$. В таком случае

$$r = \delta_k(r_k) = \delta_k(a_k) = \delta_k = \alpha_0.$$

Пусть $\omega \leftrightarrows \infty$. Из теоремы 8.7.5 и тождества (8.7.7) следует, что

$$|r - \delta_{n-1}| = \frac{1}{Q_{n-1}(r_n Q_{n-1} + Q_{n-2})} \leqslant \frac{1}{Q_n Q_{n+1}}.$$

Замечая, что

$$\lim_{n\to\infty} \delta_{n-1} = \alpha_0;$$

$$\lim_{n\to\infty} Q_n = \infty,$$

мы получим, что $r = \alpha_0$ и в этом случае. Покажем теперь, что последовательность a конечна в том и только в том случае, если число r рационально. Если $\omega \leftrightarrows k < \infty$, то

$$r = \delta_k = \frac{P_k}{Q_k}$$

и, следовательно, число r рационально. Предположим, что $r = \frac{a}{b}$, где a — целое, а b — натуральное число. По теореме о делении с остатком (вопрос 6.2.4) можно найти частное (неполное) q и остаток b_1 такие, что:

1) $a = bq + b_1$;

2) $0 \leqslant b_1 < b$.

Отсюда следует, что

$$r = \frac{a}{b} = q + \frac{b_1}{b}.$$

Если $b_1 > 0$, то $0 < \frac{b_1}{b} < 1$. Поэтому

$$a_0 = [r] = q$$

и

$$r_1 = \frac{b}{b_1}.$$

Продолжая дальше, мы находим, что

$$b = b_1 q_1 + b_2,$$

где $q_1 \geqslant 1$, $0 \leqslant b_2 < b_1$.

Поэтому, если $b_2 \neq 0$, то

$$a_1 = [r_1] = q_1$$

и

$$r_2 = \frac{b_1}{b_2}.$$

Так как последовательность

$$b,\ b_1,\ b_2,\ \ldots$$

неотрицательных целых чисел строго убывает, то она конечна. А отсюда сразу следует, что и последовательность $a_0, a_1, \ldots$ конечна.

Вопрос 8.7.1. Пусть $a = \{a_n\}_{n=0}^{\infty}$ — последовательность целых чисел и $\beta = \{\beta_n\}_{n=0}^{\infty}$ — последовательность действительных чисел с условием, что $\beta_n > 0$ для каждого $n \geqslant 1$. Доказать, что если

$$\beta_n = a_n + \frac{1}{\beta_{n+1}}$$

для всех $n \geqslant 0$, то a — каноническая последовательность и значение цепной дроби этой последовательности равно β_0.

Определение 8.7.6. Цепную дробь канонической последовательности называют *периодической,* если все члены данной последовательности, начиная с некоторого, периодически повторяются.

Теорема 8.7.16. Для того чтобы цепная дробь канонической последовательности $a \rightleftharpoons \{a_n\}_{n=0}^{\infty}$ была периодической, необходимо и достаточно, чтобы

$$\alpha_n = \alpha_m$$

для каких-нибудь неотрицательных целых и различных чисел n и m.

Доказательство. Предположим, что

$$\alpha_n = \alpha_m,$$

где $0 \leqslant n < m$. Докажем, что для любого неотрицательного целого x

$$a_{n+x} = a_{m+x}$$

и

$$\alpha_{n+x+1} = \alpha_{m+x+1}.$$

В самом деле, если

$$\alpha_{n+x} = \alpha_{m+x},$$

то

$$a_{n+x} = [\alpha_{n+x}] = [\alpha_{m+x}] = a_{m+x},$$

а в силу следствия 2 из теоремы 8.7.11 отсюда следует, что

$$\alpha_{n+x+1} = \alpha_{m+x+1}.$$

Теорема 8.7.17 (*Лагранжа* о квадратичной иррациональности). Если действительное число r — иррациональный корень многочлена второй степени с целыми коэффициентами, то каноническая цепная дробь, значение которой равно r, периодична.

Доказательство. Без ограничения общности можно предположить, что число r — корень уравнения с четным коэффициентом при первой степени неизвестного. Таким образом, существуют целые A_0, B_0, C_0 такие, что

$$A_0 r^2 + 2B_0 r + C_0 = 0.$$

Так как $r \in R$, то

$$d \rightleftharpoons B_0^2 - A_0 C_0 > 0.$$

Пусть r — значение канонической цепной дроби последовательности $a \rightleftharpoons \{a_x\}_{x=0}^{\omega}$. Так как число r — иррационально, то $\omega \rightleftharpoons \infty$.

Символом α_n, как и прежде, обозначаем полное частное цепной дроби последовательности a. Определим три последовательности целых чисел $\{A_n\}_{n=0}^{\infty}$, $\{B_n\}_{n=0}^{\infty}$ и $\{C_n\}_{n=0}^{\infty}$ при помощи следующих рекуррентных соотношений:

$$\left.\begin{aligned} A_{n+1} &= A_n a_n^2 + 2B_n a_n + C_n; \\ B_{n+1} &= A_n a_n + B_n; \\ C_{n+1} &= A_n. \end{aligned}\right\} \tag{8.7.8}$$

Докажем, что для любого неотрицательного целого n

$$A_n \alpha_n^2 + 2B_n \alpha_n + C_n = 0 \tag{8.7.9}$$

и

$$B_n^2 - A_n C_n = d. \tag{8.7.10}$$

Для $n = 0$ равенства (8.7.9) и (8.7.10) выполняются в силу предположения, так как $\alpha_0 = r$. Пусть для некоторого неотрицательного целого n оба равенства верны. Имеем (теорема 8.7.11, следствие 2)

$$\alpha_n = a_n + \frac{1}{\alpha_{n+1}}.$$

Поэтому из равенства (8.7.9) мы получим

$$A_n\left(a_n + \frac{1}{\alpha_{n+1}}\right)^2 + 2B_n\left(a_n + \frac{1}{\alpha_{n+1}}\right) + C_n = 0.$$

Отсюда следует, что

$$(A_n a_n^2 + 2B_n a_n + C_n)\,\alpha_{n+1}^2 + 2\,(A_n a_n + B_n)\,\alpha_{n+1} + A_n = 0,$$

т. е.

$$A_{n+1}\alpha_{n+1}^2 + 2B_{n+1}\alpha_{n+1} + C_{n+1} = 0.$$

Далее нетрудно проверить, что

$$(A_n a_n + B_n)^2 - (A_n a_n^2 + 2B_n a_n + C_n)\,A_n = B_n^2 - A_n C_n.$$

Этим доказывается второе утверждение.

Пусть

$$M \rightleftharpoons \{n \mid A_n \cdot A_{n-1} < 0\}.$$

Докажем, что множество M бесконечно. В самом деле, в противном случае все члены последовательности $\{A_n\}_n$, начиная с некоторого, одного знака. Без ограничения общности можно предположить, что все члены этой последовательности, начиная с некоторого, положительны. А тогда в силу равенства (8.7.8) и все члены последовательностей целых чисел $\{B_n\}_{n=0}^{\infty}$ и $\{C_n\}_{n=0}^{\infty}$, начиная с некоторого, положительны. Но в таком случае для таких натуральных n

$$A_n \alpha_n^2 + 2B_n \alpha_n + C_n > 0.$$

Пусть $n \in M$. Тогда $A_n \cdot C_n < 0$, и мы имеем:

$$d = B_n^2 - A_n C_n = |B_n|^2 + |A_n| \cdot |C_n|. \tag{8.7.11}$$

Но числа A_n, B_n и C_n целые, поэтому из равенства (8.7.11) мы получим, что

$$|A_n| \leqslant d, \quad |B_n| \leqslant d, \quad |C_n| \leqslant d.$$

Отсюда следует, что множество

$$\{\langle A_n, B_n, C_n\rangle \mid n \in M\}$$

конечно. А потому и конечно множество

$$\{t \mid t \in R, \ A_n t^2 + B_n t + C_n = 0, \quad n \in M\}.$$

Но множество M бесконечно. Поэтому в нем можно найти числа n и m такие, что

$$\alpha_n = \alpha_m, \quad n < m,$$

что в силу теоремы 8.7.16 и доказывает наше утверждение.

Теорема 8.7.18. Если r — значение периодической цепной дроби, то r — квадратичная иррациональность, т. е. r— иррациональный корень уравнения второй степени с целыми коэффициентами.

Доказательство. Пусть $a \leftrightarrows \{a_n\}_{n=0}^{\infty}$ — периодическая каноническая последовательность целых чисел, значение цепной дроби которой равно r. По теореме 8.7.16 для некоторых неотрицательных целых и различных n и m $(n < m)$

$$\alpha_n = \alpha_m.$$

Поэтому в силу следствия 3 теоремы 8.7.11 получим равенство

$$\frac{P_{n-2} - rQ_{n-2}}{rQ_{n-1} - P_{n-1}} = \frac{P_{m-2} - rQ_{m-2}}{rQ_{m-1} - P_{m-1}}.$$

Отсюда легко следует, что число r — корень квадратного трехчлена с целыми коэффициентами и со старшим коэффициентом, равным

$$Q_{n-1}Q_{m-2} - Q_{n-2}Q_{m-1}.$$

Этот коэффициент не равен нулю. В противном случае

$$Q_{n-1}Q_{m-2} = Q_{n-2}Q_{m-1}.$$

Но числа Q_{m-1} и Q_{m-2} взаимно-просты. Следовательно, Q_{m-1}— делитель Q_{n-1}. А это не может быть, так как $Q_{m-1} > Q_{n-1}$.

Итак, r — корень уравнения второй степени с целыми коэффициентами. При этом r — иррациональное действительное число, так как последовательность a бесконечна.

Теорема 8.7.19 (*Эйлера*). Пусть $a \leftrightarrows \{a_n\}_{n=0}^{\infty}$ — последовательность целых чисел, члены которой определяются следующими рекуррентными соотношениями:

1) $a_0 = 2$;

2) если $n \geqslant 1$, то

$$a_{3n-2} = 1, \quad a_{3n-1} = 2n, \quad a_{3n} = 1.$$

Тогда значение цепной дроби последовательности a равно e.

Доказательство. Ряд

$$f_n(x) = \sum_{s=0}^{\infty} u_s$$

с общим членом

$$u_s = \frac{(n+s)!}{s!\,(2n+2s)!}\,x^{2s}, \quad x \in R$$

абсолютно сходится, так как

$$\lim_{s\to\infty} \frac{u_{s+1}}{u_s} = 0.$$

Легко проверить, что

$$\frac{n!}{(2n)!} - (4n+2)\frac{(n+1)!}{(2n+2)!} = 0$$

и при $s \geqslant 1$

$$\frac{(n+s)!}{s!\,(2n+2s)!} - (4n+2)\frac{(n+s+1)!}{s!\,(2n+2s+2)!} = 4\,\frac{(n+s+1)!}{(s-1)!\,(2n+2s+2)!}.$$

Отсюда следует тождество

$$f_n(x) - (4n+2)\,f_{n+1}(x) = 4x^2 f_{n+2}(x).$$

Таким образом,

$$\frac{f_n(x)}{f_{n+1}(x)} = 4n + 2 + \frac{1}{\dfrac{f_{n+1}(x)}{4x^2 f_{n+2}(x)}}.$$

Полагая

$$x \rightleftarrows \frac{1}{2}, \quad \beta_n \rightleftarrows \frac{f_n\left(\frac{1}{2}\right)}{f_{n+1}\left(\frac{1}{2}\right)},$$

мы получим

$$\beta_n = 4n + 2 + \frac{1}{\beta_{n+1}}.$$

Отсюда следует (вопрос 8.7.1), что β_0 — значение цепной дроби последовательности $b = \{b_n\}_{n=0}^{\infty}$, где $b_n = 4n + 2$. Далее имеем:

$$f_0\left(\frac{1}{2}\right) = \sum_{s=0}^{\infty} \frac{1}{(2s)!}\left(\frac{1}{2}\right)^{2s} = \frac{1}{2}\,(e^{\frac{1}{2}} + e^{-\frac{1}{2}});$$

$$f_1\left(\frac{1}{2}\right) = \sum_{s=0}^{\infty} \frac{(s+1)}{(2s+1)!\,(2s+2)}\left(\frac{1}{2}\right)^{2s} = \sum_{s=0}^{\infty} \frac{1}{(2s+1)!}\left(\frac{1}{2}\right)^{2s+1} =$$

$$= \frac{1}{2}\,(e^{\frac{1}{2}} - e^{-\frac{1}{2}}),$$

Итак,

$$\beta_0 = \frac{f_0\left(\frac{1}{2}\right)}{f_1\left(\frac{1}{2}\right)} = \frac{e^{\frac{1}{2}} + e^{-\frac{1}{2}}}{e^{\frac{1}{2}} - e^{-\frac{1}{2}}} = \frac{e+1}{e-1} -$$

значение цепной дроби последовательности b.

Пусть $\sigma_n = \frac{R_n}{S_n}$ — подходящая дробь порядка n последовательности b. В таком случае для всех $n \geqslant 0$

$$R_n = (4n+2)\,R_{n-1} + R_{n-2},$$
$$S_n = (4n+2)\,S_{n-1} + S_{n-2};$$

при этом

$$R_{-2} = 0, \quad R_{-1} = 1,$$
$$S_{-2} = 1, \quad S_{-1} = 0.$$

Пусть, как всегда, α_n и $\delta_n = \frac{P_n}{Q_n}$ — полное частное и подходящая дробь порядка n последовательности a. Докажем, что для всех $n \geqslant 0$:

$$\left.\begin{aligned} P_{3n+1} &= R_n + S_n, \\ Q_{3n+1} &= R_n - S_n. \end{aligned}\right\} \tag{8.7.12}$$

В справедливости этих равенств при $n = 0$ и $n = 1$ легко убедиться непосредственно. Далее, имеем:

$$P_{3n+1} = P_{3n} + P_{3n-1},$$
$$P_{3n} = P_{3n-1} + P_{3n-2},$$
$$P_{3n-1} = 2nP_{3n-2} + P_{3n-3},$$
$$P_{3n-2} = P_{3n-3} + P_{3n-4},$$
$$P_{3n-3} = P_{3n-4} + P_{3n-5}.$$

Умножая эти равенства соответственно на 1, 1, 2, —1, 1 и складывая, получим

$$P_{3n+1} = (4n+2)\,P_{3n-1} + P_{3n-5}.$$

Аналогично

$$Q_{3n+1} = (4n+2)\,Q_{3n-1} + Q_{3n-5}.$$

Отсюда легко следует тождество (8.7.12). Таким образом,

$$\frac{P_{3n+1}}{Q_{3n+1}} = \frac{\frac{R_n}{S_n} + 1}{\frac{R_n}{S_n} - 1}. \tag{8.7.13}$$

Переходя к пределу при $n \to \infty$, получим

$$\alpha_0 = \frac{\frac{e+1}{e-1}+1}{\frac{e+1}{e-1}-1} = \frac{2e}{2} = e.$$

Итак,

$$e = [2;\ 1, 2, 1, 1, 4, 1, 1, 6, 1, \ldots].$$

Примеры: 8.7.1. Пусть $r = \sqrt{3}$. Имеем:

$$a_0 = [\sqrt{3}] = 1, \quad \sqrt{3} = 1 + \frac{1}{\alpha_1},$$

$$\alpha_1 = \frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2};$$

$$a_1 = [\alpha_1] = 1, \quad \frac{\sqrt{3}+1}{2} = 1 + \frac{1}{\alpha_2},$$

$$\alpha_2 = \frac{2}{\sqrt{3}-1} = \sqrt{3}+1;$$

$$a_2 = [\alpha_2] = 2, \quad \sqrt{3}+1 = 2 + \frac{1}{\alpha_3},$$

$$\alpha_3 = \frac{1}{\sqrt{3}-1} = \alpha_1.$$

Таким образом,

$$\sqrt{3} = [1;\ 1, 2, 1, 2, 1, 2, \ldots].$$

8.7.2. Первые 8 элементов разложения числа π в цепную дробь таковы:

$$\pi = [3;\ 7, 15, 1, 292, 1, 1, 2, \ldots].$$

В следующих теоремах идет речь о приближениях действительных чисел рациональными. Из теорем 8.7.10 и 8.7.12 (следствие 2) легко выводятся следующие две теоремы.

Теорема 8.7.20. Если $0 \leqslant n < \omega$, то

$$|\alpha_0 - \delta_n| \leqslant \frac{1}{Q_n Q_{n+1}};$$

при этом равенство возможно только в случае, если $\omega \leftrightarrows n+1$.

Теорема 8.7.21. Если $0 \leqslant n < \omega + 1$, то

$$|\alpha_0 - \delta_n| < \frac{1}{Q_n^2}.$$

Теорема 8.7.22. Пусть α_0 — значение канонической цепной дроби последовательности $a = \{a_n\}_{n=0}^{\omega}$. Если $1 \leqslant n < \omega + 1$, то

$$|\alpha_0 - \delta_n| < |\alpha_0 - \delta_{n-1}|.$$

Доказательство. Если $\omega = n$, то $\alpha_0 - \delta_n = 0 < |\alpha_0 - \delta_{n-1}|$. Пусть $1 \leqslant n < \omega$. В силу теоремы 8.7.11 (следствие 3) имеем

$$\alpha_{n+1} = \frac{P_{n-1} - \alpha_0 Q_{n-1}}{\alpha_0 Q_n - P_n}.$$

Отсюда получим, что

$$\frac{\left|\alpha_0 - \frac{P_{n-1}}{Q_{n-1}}\right|}{\left|\alpha_0 - \frac{P_n}{Q_n}\right|} = \alpha_{n+1} \cdot \frac{Q_n}{Q_{n-1}} \geqslant \alpha_{n+1} > 1.$$

Теорема 8.7.23 (о наилучшем приближении). Пусть $a \in Z, b \in N$, $1 \leqslant n < \omega + 1$. Если $\delta_n \neq \frac{a}{b}$ и $\left|\frac{a}{b} - \alpha_0\right| \leqslant |\alpha - \delta_n|$, то

$$b > Q_n.$$

Доказательство. Если

$$\left|\frac{a}{b} - \alpha_0\right| \leqslant |\alpha_0 - \delta_n|,$$

то

$$\left|\frac{a}{b} - \alpha_0\right| < |\alpha_0 - \delta_{n-1}|.$$

А так как числа $\alpha_0 - \delta_n$ и $\alpha_0 - \delta_{n-1}$ в силу теоремы 8.7.12 разных знаков и $\delta_n \neq \frac{a}{b}$, то

$$\frac{a}{b} \in [\delta_n, \delta_{n-1}].$$

Отсюда следует, что

$$|\delta_n - \delta_{n-1}| = \left|\delta_n - \frac{a}{b} + \frac{a}{b} - \delta_{n-1}\right| = \left|\delta_n - \frac{a}{b}\right| + \left|\frac{a}{b} - \delta_{n-1}\right|.$$

В силу теоремы 8.7.6

$$|\delta_n - \delta_{n-1}| = \frac{1}{Q_n Q_{n+1}}.$$

Числа $bP_n - aQ_n$ и $aQ_{n-1} - bP_{n-1}$ — целые и не равные нулю. Поэтому имеем

$$\frac{1}{Q_n Q_{n+1}} = \frac{|bP_n - aQ_n|}{bQ_n} + \frac{|aQ_{n-1} - bP_{n-1}|}{bQ_{n-1}} \geqslant \frac{1}{bQ_n} + \frac{1}{bQ_{n-1}}.$$

Отсюда получим, что

$$b \geqslant Q_n + Q_{n-1} > Q_n.$$

Теорема 8.7.24 (*Дирихле*). Пусть $\tau \geqslant 1$ — действительное число. Для любого действительного числа α существует целое a и натуральное число b такие, что $0 < b \leqslant \tau$ и

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b\tau}.$$

Доказательство. Разлагая число α в цепную дробь, мы найдем каноническую последовательность $a = \{a_n\}_{n=0}^{\omega}$, значение цепной дроби которой равно α. Так как $Q_0 = 1$ и последовательность целых чисел $\{a_x\}_{x=0}^{\infty}$ строго возрастает, то либо существует неотрицательное целое n такое, что

$$Q_n \leqslant \tau < Q_{n+1},$$

либо $Q_n \leqslant \tau$ для всех чисел $n < \omega + 1$. В первом случае

$$\left|\alpha - \frac{P_n}{Q_n}\right| = |\alpha - \delta_n| \leqslant \frac{1}{Q_n Q_{n+1}} < \frac{1}{Q_n \tau}.$$

Во втором случае $\omega \rightleftharpoons b < \infty$ и мы имеем

$$\left|\alpha - \frac{P_k}{Q_k}\right| = 0 < \frac{1}{Q_k \tau}.$$

Теорема 8.7.25 (*Лиувилля*). Пусть α — действительный корень многочлена с целыми коэффициентами степени $n \geqslant 1$. Существует положительное число c такое, что для любых целого a и натурального b, если $\alpha \neq \frac{a}{b}$, выполняется неравенство

$$\left|\alpha - \frac{a}{b}\right| > \frac{c}{b^n}.$$

Доказательство. Пусть $f(x)$ — многочлен наименьшей степени n с целыми коэффициентами и корнем α. Имеем

$$f(x) = (x - \alpha) f_1(x),$$

где $f_1(x)$ — многочлен с действительными коэффициентами. Легко видеть, что

$$f_1\left(\frac{a}{b}\right) \neq 0.$$

Поэтому имеем

$$\left|\frac{a}{b} - \alpha\right| = \frac{\left|f\left(\frac{a}{b}\right)\right|}{\left|f_1\left(\frac{a}{b}\right)\right|} = \frac{\left|b^n f\left(\frac{a}{b}\right)\right|}{b^n \left|f_1\left(\frac{a}{b}\right)\right|}.$$

Так как числитель $\left|b^n f\left(\frac{a}{b}\right)\right|$ — число целое и не равное нулю, то

$$\left|\frac{a}{b} - \alpha\right| \geqslant \frac{1}{b^n \left|f_1\left(\frac{a}{b}\right)\right|}.$$

Рассмотрим отрезок $[\alpha - 1, \alpha + 1]$. Функция $f_1(x)$ непрерывна на этом отрезке, и потому можно найти положительное число M такое, что

$$|f_1(x)| < M$$

для всех x данного отрезка. Отсюда следует, что если

$$\frac{a}{b} \in [\alpha - 1, \alpha + 1], \quad \text{то} \quad \left|\frac{a}{b} - \alpha\right| > \frac{1}{b^n M}.$$

Если же

$$\frac{a}{b} \notin [\alpha - 1,\ \alpha + 1], \text{ то } \left|\frac{a}{b} - \alpha\right| > 1 \geqslant \frac{1}{b^n}.$$

Выбирая в качестве c наименьшее из чисел 1 и $\frac{1}{M}$, мы убеждаемся в справедливости теоремы для выбранного n. Общий случай отсюда немедленно следует.

Теорема 8.7.26 (конструкция трансцендентных чисел). Пусть $a \leftrightharpoons \{a_n\}_{n=0}^{\infty}$ — каноническая последовательность, элементы которой выбираются из условий:

1) a_0 — любое целое;

2) если $a_0, \ldots, a_n$ выбраны, то за a_{n+1} принимаем целое такое, что

$$a_{n+1} > Q_n^n.$$

Тогда значение α_0 цепной дроби последовательности a трансцендентно.

Доказательство. Предположим, что это не так. Тогда α — корень некоторого многочлена с целыми коэффициентами степени $n \geqslant 1$. В силу теоремы 8.7.24 существует положительное число c такое, что

$$\left|\frac{a}{b} - \alpha\right| > \frac{c}{b}, \tag{8.7.14}$$

каково бы ни было рациональное число $\frac{a}{b}$ $(b > 0)$.

С другой стороны, если $\frac{P_s}{Q_s}$ — подходящая дробь разложения числа α в цепную дробь, то

$$\left|\alpha - \frac{P_s}{Q_s}\right| < \frac{1}{Q_s Q_{s+1}}.$$

Так как

$$Q_{s+1} = a_{s+1}Q_s + Q_{s-1} > Q_s^{s+1},$$

то, выбирая $s > n$ и $Q_s > \frac{1}{c}$, мы получим

$$\frac{c}{Q_s^n} > \frac{1}{Q_s^{n+1}} > \frac{1}{Q_s^{s+1}} > \left|\alpha - \frac{P_s}{Q_s}\right|$$

в противоречии с неравенством (8.7.14).

Вопросы: **8.7.2***. Пусть $f(x)$ — многочлен с рациональными коэффициентами степени $m \geqslant 0$; $I \leftrightharpoons \int_0^1 f(x) \sin \pi x dx$, n и k — натуральные числа. Доказать, что:

1) $I = \frac{1}{\pi}(f(0) + f(1)) - \frac{1}{\pi^3}(f^{II}(0) + f^{II}(1)) +$

$+ \frac{1}{\pi^5}(f^{IV}(0) + f^{IV}(1)) - \cdots;$

2) из предположения, что $\pi = \frac{a}{b}$, где a и b — натуральные числа, следует равенство

$$a^{m+1} I = b a^m (f(0) + f(1)) - b^3 a^{m-2} (f^{II}(0) + f^{II}(1)) + \cdots \quad (8.7.15)$$

Пусть, в частности, $f(x) \rightleftharpoons \frac{x^n (1-x)^n}{n!}$. Доказать далее, что:

3) $f^{(k)}(0)$ и $f^{(k)}(1)$ — целые числа;

4) $0 < I < \frac{1}{n!}$;

5) равенство (8.7.15) неверно для всех достаточно больших n.

8.7.3*. Доказать, что число π иррационально.

8.7.4*. Пусть $f(x)$ — многочлен с рациональными коэффициентами степени $m \geqslant 0$; n и k — неотрицательные целые;

$$I_k \rightleftharpoons e^k \int_0^k f(x) e^{-x} dx;$$

$$F(x) \rightleftharpoons f(x) + f'(x) + \cdots + f^{(m)}(x).$$

Доказать, что:

1) $I_k = F(0) e^k - F(k)$;

2) из предположения, что существуют целые числа $c_0, c_1, \ldots, c_n$ такие, что $c_0 \neq 0$ и $c_0 + c_1 e + \ldots + c_n e^n = 0$, следует равенство

$$\sum_{k=0}^{n} c_k F(k) = -\sum_{k=0}^{n} c_k I_k. \quad (8.7.16)$$

Пусть, в частности, $f(x) \rightleftharpoons \frac{1}{(p-1)!} x^{p-1} (x-1)^p \cdot \ldots \cdot (x-n)^p$, где p — простое $> n$. Доказать далее, что:

3) $F(k)$ — целое число, кратное p при $k \geqslant 1$ и не делящееся на p при $k = 0$;

4) $|I_k| \leqslant e^k \frac{n^{np+p-1}}{(p-1)!}$;

5) равенство (8.7.16) неверно для всех достаточно больших p.

8.7.5*. Доказать, что число e трансцендентно (теорема *Эрмита*).

8.7.6*. Пусть $b_0 = 1$, $a_0 \geqslant 0$,

$$\{a_n\}_{n=1}^{\omega}, \quad \{b_n\}_{n=0}^{\omega} \quad (8.7.17)$$

конечные $(1 \leqslant \omega < \infty)$ или бесконечные $(\omega \rightleftharpoons \infty)$ последовательности действительных чисел. Целые значения n, удовлетворяющие условию $0 \leqslant n < \omega + 1$, в дальнейшем называются допустимыми. Выражение

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{a_3 + \ddots}}} \quad (8.7.18)$$

называют *общей цепной дробью,* а члены последовательностей (8.7.16) — ее *элементами.* Элементы a_n и b_n называют соответственно *числителями* и *знаменателями* цепной дроби (8.7.18). Пусть далее $\{P_n\}_{n=0}^{\omega}$ и $\{Q_n\}_{n=0}^{\omega}$ — последовательности чисел, удовлетворяющие для всех допустимых значений n рекуррентным уравнениям:

$$P_n = a_n P_{n-1} + b_n Q_{n-2};$$
$$Q_n = a_n Q_{n-1} + b_n Q_{n-2}$$

с начальными условиями

$$P_{-2} = 0, \quad P_{-1} = 1;$$
$$Q_{-2} = 1, \quad Q_{-1} = 0.$$

Каково бы ни было действительное число α, если все числители b_n данной цепной дроби (8.7.18) отличны от нуля, число α_n, определяемое для допустимых значений n из условий $\alpha = \alpha_0$ и $\alpha_{n-1} = a_{n-1} + \frac{b_n}{\alpha_n}$ при $n \geqslant 1$, называют *полным частным* разложения α в данную цепную дробь.

Если $Q_n \neq 0$ для какого-нибудь значения n, то число $\delta_n \rightleftharpoons \frac{P_n}{Q_n}$ называют *подходящей дробью порядка n* данной цепной дроби (8.7.18).

Если цепная дробь (8.7.18) бесконечна, $Q_n \neq 0$ для всех допустимых значений n и последовательность

$$\{\delta_n\}_n^{\infty} \tag{8.7.19}$$

сходится, то данную цепную дробь называют *сходящейся,* а предел последовательности (8.7.19) — ее *значением.*

Если все элементы цепной дроби (8.7.18) положительны, то равенство

$$\delta_n(x) = \frac{xP_{n-1} + b_n P_{n-2}}{xQ_{n-1} + b_n Q_{n-2}}$$

для каждого положительного x определяет действительное число $\delta_n(x)$. Функцию $\delta_n(x)$ называют *подходящей функцией* цепной дроби (8.7.18).

Доказать, что:

1) для всех допустимых значений n

$$P_n Q_{n-1} - P_{n-1} Q_n = (-1)^n b_0 \cdot \ \cdots \ \cdot b_n;$$

2) для всех допустимых значений n, начиная с 1,

$$P_n Q_{n-2} - P_{n-2} Q_n = (-1)^n b_0 \cdot \ \cdots \ \cdot b_{n-1} a_n;$$

3) значение сходящейся цепной дроби не изменится, если для каждого допустимого значения n, начиная с 1, ее соответствующие

элементы a_n и b_n умножить на какое-нибудь не равное нулю число k_n;

4) если $a_n \geqslant |b_n| + 1$ для каждого допустимого значения n, то

$$Q_n - Q_{n-1} \geqslant |b_0 \cdot \cdots \cdot b_n|;$$

5) бесконечная цепная дробь (8.7.18) сходится, если $a_n \geqslant |b_n| + 1$ для каждого допустимого значения n;

6) для любой цепной дроби с положительными элементами ее подходящие функции для всех допустимых значений n удовлетворяют рекуррентному уравнению

$$\delta_n(x) = \delta_{n-1}\left(a_{n-1} + \frac{b_n}{x}\right)$$

с начальным условием $\delta_0(x) = x$;

7) для любой цепной дроби с положительными элементами и для каждого допустимого значения n

$$\frac{d}{dx}\delta_n(x) = \frac{(-1)^n b_0 \cdot \cdots \cdot b_n}{(xQ_{n-1} + b_n Q_{n-2})^2};$$

8) если цепная дробь с положительными элементами сходится, то для каждой пары соседних подходящих дробей ее значение больше одной из них и меньше второй;

9) если все элементы данной цепной дроби положительны, то для каждого допустимого значения n, начиная с 2, отображение

$$x \mapsto \frac{xP_{n-1} + b_n P_{n-2}}{xQ_{n-1} + b_n Q_{n-2}}$$

есть взаимно-однозначное отображение множества положительных чисел на интервал с концами δ_{n-1} и δ_{n-2};

10) сходящаяся цепная дробь с положительными элементами сходится к числу α тогда и только тогда, если все полные частные разложения α в данную цепную дробь положительны;

11) если цепная дробь (8.7.18) бесконечна и ее элементы — натуральные числа, удовлетворяющие для каждого допустимого значения n условию $a_n > b_n$, то данная цепная дробь сходится и ее значение иррационально;

12) если все знаменатели бесконечной цепной дроби (8.7.18) положительны, а все ее числители равны 1, то данная цепная дробь сходится тогда и только тогда, если ряд $\sum_{n=0}^{\infty} a_n$ расходится.

§ 9. СИСТЕМА КОМПЛЕКСНЫХ ЧИСЕЛ, КВАТЕРНИОНЫ И ТЕОРЕМА ФРОБЕНИУСА

9.1. Первичные термины и аксиомы теории комплексных чисел

Под системой комплексных чисел понимают минимальное поле, которое является расширением поля действительных чисел и в котором есть элемент i с условием $i^2 + 1 = 0$. В качестве первичных принимают следующие термины:

а) C — множество, его элементы называются *комплексными числами;*

б) $+$, $\cdot$ — сложение и умножение — бинарные операции на C;

в) 0, 1 и i — элементы C;

г) R — подмножество C, его элементы называются действительными числами;

д) $\oplus$ и $\odot$ — сложение и умножение — бинарные операции на R.

Аксиомы разделяются на четыре группы и могут быть сформулированы так:

А

C_I. $\forall (a, b \in C) \exists ! (c \in C) \quad a + b = c$;

C_{II}. $\forall (a, b, c \in C) \quad (a + b) + c = a + (b + c)$;

C_{III}. $\forall (a, b \in C) \quad a + b = b + a$;

C_{IV}. $0 \in C \wedge \forall (a \in C) \quad a + 0 = a$;

C_V. $\forall (a \in C) \exists (a' \in C) \quad a + a' = 0$;

C_{VI}. $\forall (a, b \in C) \exists ! (p \in C) \quad a \cdot b = p$;

C_{VII}. $\forall (a, b, c \in C) \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$;

C_{VIII}. $\forall (a, b \in C) \quad a \cdot b = b \cdot a$;

C_{IX}. $\forall (a, b, c \in C) \quad (a + b) \cdot c = a \cdot c + b \cdot c$;

C_X. $1 \in C \wedge 1 \neq 0 \wedge \forall (a \in C) \quad a \cdot 1 = a$;

C_{XI}. $\forall (a \in C) \quad a \neq 0 \Rightarrow \exists (a' \in C) \quad a \cdot a' = 1$.

Б

C_{XII}. $\langle R;\ \oplus,\ \odot,\ 0,\ 1\rangle$ — поле действительных чисел;

C_{XIII}. $R \subset C$;

C_{XIV}. $\forall\,(a, b \in R)\quad a + b = a \oplus b$;

C_{XV}. $\forall\,(a, b \in R)\quad a \cdot b = a \odot b$.

В

C_{XVI} $\quad i \in C \wedge i^2 + 1 = 0$.

Г

C_{XVII} (аксиома минимальности). Любое подмножество M множества C совпадает с C, если оно удовлетворяет следующим четырем условиям:

а) $R \subset M$;

б) $i \in M$;

в) $\forall\,(a,\ b \in M)\quad a + b \in M$;

г) $\forall\,(a,\ b \in M)\quad a \cdot b \in M$.

9.2. Свойства комплексных чисел

Мы предполагаем, что $C \leftrightarrows \langle \mathbf{C};\ +,\ \cdot,\ 0,\ 1,\ i,\ \mathbf{R}\rangle$ — система комплексных чисел. Таким образом, для этой системы выполнены все названные в разделе 9.1 аксиомы. Далее можно повторить замечание о знаках операций, сделанное в разделе 6.2.

Теорема 9.2.1. Всякое комплексное число α можно представить и только одним способом в виде

$$\alpha = a + bi, \quad a \in R, \quad b \in R.$$

Доказательство. Предположим сначала, что

$$a + bi = a_1 + b_1 i$$

для некоторых действительных чисел a, b, a_1, b_1. Поскольку $\langle C; +,\ \cdot\rangle$ — поле, то $(b - b_1)\, i = a_1 - a$. Если $b \neq b_1$, то

$$i = \frac{a_1 - a}{b - b_1} \in R.$$

А это не может быть в силу теоремы 5.4.4. Возможность представления легко следует из аксиомы минимальности.

Теорема 9.2.2. Поле комплексных чисел нельзя линейно упорядочить.

Следует из теоремы 5.4.5, так как $i^2 + 1^2 = 0$.

Теорема 9.2.3. Аддитивную группу комплексных чисел можно линейно и строго упорядочить. См. вопрос 8.2.5.

Следующие две теоремы известны из курса алгебры.

Теорема 9.2.4. Любой многочлен степени $n > 0$ над полем комплексных чисел можно разложить в произведение многочленов первой степени с комплексными коэффициентами. Другими словами, поле комплексных чисел *алгебраически замкнуто*.

Теорема 9.2.5. Любой многочлен степени $n > 0$ над полем действительных чисел можно разложить в произведение неприводимых над полем действительных чисел сомножителей первой и второй степени.

Вопросы: 9.2.1*. Показать, что поле комплексных чисел можно нетривиально нормировать относительно поля действительных чисел.

9.2.2*. Показать, что множество линейных и строгих порядков в аддитивной группе комплексных чисел бесконечно.

9.3. Категоричность аксиоматической теории комплексных чисел

Теорема 9.3.1. Пусть $\mathbf{C}' \rightleftharpoons \langle C'; +, \cdot, i', \mathbf{R}'\rangle$ и $\mathbf{C}'' \rightleftharpoons \langle C''; \oplus, \odot, i'', \mathbf{R}''\rangle$—системы комплексных чисел. Тогда существует изоморфное отображение f системы $\mathbf{C}'$ на $\mathbf{C}''$.

Доказательство. Прежде всего условливаемся в целях краткости пользоваться одинаковыми знаками операций в $\mathbf{C}'$ и $\mathbf{R}'$, а также в $\mathbf{C}''$ и $\mathbf{R}''$. Далее, условливаемся элементы из C' снабжать одним штрихом: α', β', i', ..., а элементы из C'' двумя: α'', β'', i'', ... Поскольку любые поля действительных чисел по теореме 8.4.1 изоморфны, существует взаимно-однозначное отображение φ множества R' на R'' такое, что:

1) $\forall (a', b' \in R') \quad \varphi(a' + b') = \varphi(a') \oplus \varphi(b')$;
2) $\forall (a', b' \in R') \quad \varphi(a' \cdot b') = \varphi(a') \odot \varphi(b')$.

Определим однозначное отображение f множества C' в C'' следующим условием:

$$f: a' + b'i' \mapsto \varphi(a') \oplus \varphi(b') \odot i''.$$

Нетрудно убедиться в том, что f — взаимно-однозначное отображение C' на C''.

Пусть $\alpha' \rightleftharpoons a_1' + a_2'i'$, $\beta' \rightleftharpoons b_1' + b_2'i'$. Имеем:

$$f(\alpha') \oplus f(\beta') = (\varphi(a_1') \oplus \varphi(a_2') \odot i'') \oplus (\varphi(b_1') \oplus \varphi(b_2') \odot i'') =$$
$$= (\varphi(a_1') \oplus \varphi(b_1')) \oplus (\varphi(a_2') \oplus \varphi(b_2')) \odot i'' =$$
$$= \varphi(a_1' + b_1') \oplus \varphi(a_2' + b_2') \odot i'' =$$
$$= f(a_1' + b_1') + (a_2' + b_2')\, i') = f(\alpha' + \beta').$$

Аналогично проверяется и условие

$$\forall (\alpha', \beta' \in C') \quad f(\alpha') \odot f(\beta') = f(\alpha' \cdot \beta').$$

Вопросы: 9.3.1. Доказать, что в поле комплексных чисел имеется:

а) только одно подполукольцо, изоморфное полукольцу натуральных чисел;

б) только одно подкольцо, изоморфное кольцу целых чисел;

в) только одно поле, изоморфное полю рациональных чисел;

г) три поля, изоморфных полю вопроса 2.6.23.

9.3.2. Доказать, что в поле комплексных чисел имеется:

а) только один, отличный от тождественного, автоморфизм, оставляющий действительные числа на месте;

б) бесконечно много автоморфизмов.

9.3.3. Доказать, что в поле комплексных чисел имеется бесконечно много подполей, изоморфных полю действительных чисел.

9.4. Непротиворечивость аксиоматической теории комплексных чисел

Теорема 9.4.1. Аксиоматическая теория комплексных чисел непротиворечива относительно аксиоматической теории действительных чисел.

Доказательство. Мы укажем модель данной теории. Пусть $\langle R;\ +,\ \cdot,\ 0,\ 1\rangle$ — поле действительных чисел. Рассмотрим множество P пар $\langle a,\ b\rangle$ действительных чисел и определим на P бинарные операции $\oplus$ и $\odot$ (сложение и умножение) следующими условиями:

$$\forall\,(a,\ b,\ a',\ b' \in R)\quad \langle a,\ b\rangle \oplus \langle a',\ b'\rangle \rightleftharpoons \langle a + a',\ b + b'\rangle;$$

$$\forall\,(a,\ b,\ a',\ b' \in R)\quad \langle a,\ b\rangle \odot \langle a',\ b'\rangle \rightleftharpoons \langle aa' - bb',\ ab' + a'b\rangle.$$

Нам известно (вопрос 2.6.19), что $\langle P;\ \oplus,\ \odot\rangle$ — поле. Выберем в P подмножество R_0 пар вида $\langle a,\ 0\rangle$. Сопоставим с каждым действительным числом a пару $\varphi\,(a) \rightleftharpoons \langle a,\ 0\rangle$. Легко видеть, что φ — взаимно-однозначное отображение R на R_0. Далее, имеем:

$$\forall\,(a,\ b \in R)\quad \varphi\,(a) \oplus \varphi\,(b) = \langle a,\ 0\rangle \oplus \langle b,\ 0\rangle =$$
$$= \langle a + b,\ 0\rangle = \varphi\,(a + b);$$

$$\forall\,(a,\ b \in R)\quad \varphi\,(a) \odot \varphi\,(b) = \langle a,\ 0\rangle \odot \langle b,\ 0\rangle =$$
$$= \langle a \cdot b,\ 0\rangle = \varphi\,(a \cdot b).$$

Таким образом, φ — изоморфное отображение $\langle R;\ +,\ \cdot\rangle$ на $\langle R_0;\ \oplus,\ \odot\rangle$. Следовательно:

а) $\langle R_0;\ \oplus,\ \odot\rangle$ — поле действительных чисел;

б) поле $\langle P;\ \oplus,\ \odot\rangle$ — расширение поля $\langle R_0;\ \oplus,\ \odot\rangle$.

Заметим также, что $\langle 1,\ 0\rangle$ и $\langle 0{,}0\rangle$ — единица и нуль поля $\langle R_0;\ \oplus,\ \odot\rangle$. Полагаем $i \rightleftharpoons \langle 0,\ 1\rangle$. Имеем

$$i^2 \oplus \langle 1,\ 0\rangle = \langle 0,\ 1\rangle \odot \langle 0,\ 1\rangle \oplus \langle 1,\ 0\rangle = \langle -1,\ 0\rangle \oplus \langle 1,\ 0\rangle = \langle 0,\ 0\rangle.$$

Итак, на системе $\langle P;\ \oplus,\ \odot,\ R_0,\ \oplus,\ \odot\rangle$ выполняются первые 15 аксиом нашей теории. Пусть, наконец, M — подмножество P такое, что:

а) $R_0 \subset M$;

б) $i \in M$;

в) $\forall\,(\alpha,\ \beta \in M)\quad \alpha + \beta \in M$;

г) $\forall\,(\alpha,\ \beta \in M)\quad \alpha \cdot \beta \in M$.

Докажем, что в таком случае любой элемент множества P принадлежит множеству M. В самом деле, имеем

$$\langle a, b\rangle = \langle a, 0\rangle \oplus \langle b, 0\rangle \odot \langle 0, 1\rangle.$$

Теорема доказана.

Вопросы: 9.4.1. Доказать непротиворечивость аксиоматической теории комплексных чисел, рассматривая ее интерпретацию, в которой множества C_0, R_0, операции на них $\oplus$, $\odot$ и элементы e, θ, i определены соглашениями:

$$C_0 \rightleftharpoons \{\langle a, b\rangle \mid a, b \in R\}, \quad R_0 \rightleftharpoons \{\langle a, 0\rangle \mid a \in R\};$$

$$\langle a, b\rangle \oplus \langle a', b'\rangle \rightleftharpoons \langle a + a', b + b'\rangle;$$

$$\langle a, b\rangle \odot \langle a', b'\rangle \rightleftharpoons \langle aa' - bb', ab' + a'b - bb'\rangle;$$

$$e \rightleftharpoons \langle 1, 0\rangle, \quad \theta \rightleftharpoons \langle 0, 0\rangle, \quad i \rightleftharpoons \left\langle \frac{1}{3}\sqrt{3}, \frac{2}{3}\sqrt{3}\right\rangle.$$

9.4.2. Пусть T — множество троек действительных чисел, на котором операции $\oplus$, $\odot$ и бинарное отношение $\sim$ определены соглашениями:

$$\langle a_1, a_2, a_3\rangle \oplus \langle b_1, b_2, b_3\rangle \rightleftharpoons \langle a_1 + b_1, a_2 + b_2, a_3 + b_3\rangle;$$

$$\langle a_1, a_2, a_3\rangle \odot \langle b_1, b_2, b_3\rangle \rightleftharpoons$$

$$\rightleftharpoons \langle a_0b_0 + 2a_2b_3 + 2a_3b_2, a_1b_2 + a_2b_1 + 2a_3b_3, a_1b_3 + a_2b_2 + a_3b_1\rangle;$$

$$\langle a_1, a_2, a_3\rangle \sim \langle b_1, b_2, b_3\rangle \overset{\text{Df}}{\Leftrightarrow} a_1 - b_1 = (a_3 - b_3)\sqrt[3]{4} \wedge a_2 - b_2 =$$

$$= (a_3 - b_3)\sqrt[3]{2}.$$

Доказать, что:

1) алгебра $\mathbf{T} \rightleftharpoons \langle T; \oplus, \odot\rangle$ — коммутативное кольцо;

2) отношение $\sim$ — отношение эквивалентности, монотонное относительно обеих операций;

3) факторкольцо $T/_{\sim}$ — поле, изоморфное полю комплексных чисел.

9.4.3. Воспользовавшись результатом вопроса 9.4.2, найти модель для аксиоматической теории комплексных чисел.

9.5. Алгебры конечного ранга

Определение 9.5.1. Пусть $\mathbf{A} \rightleftharpoons \langle A; +, \cdot, \theta, \mathbf{P}\rangle$ — линейная алгебра над полем $\mathbf{P}$. Алгебру $\mathbf{A}$ называют *алгеброй ранга n* над полем $\mathbf{P}$, если алгебра $\langle A; +, \theta; \mathbf{P}\rangle$ — n-мерное векторное пространство над полем $\mathbf{P}$. *Базисом алгебры* $\mathbf{A}$ называют базис пространства $\langle A; +, \theta; \mathbf{P}\rangle$.

Примеры: 9.5.1. Всякое поле $\mathbf{P}$ — алгебра с делением ранга 1 над полем $\mathbf{P}$.

Более точно под этим понимается следующее: пусть $\mathbf{P} \rightleftharpoons \langle P; +, \cdot, 0\rangle$ — поле и пусть для каждого a из P оператор ω_k умноже-

ния на элемент k из P определен соглашением $\omega_k a \rightleftharpoons k \cdot a$. Тогда алгебра $\langle P;\ +,\ \cdot,\ 0,\ \{\omega_k \mid k \in P\}\rangle$ — линейная алгебра с делением ранга 1 над полем **P**.

9.5.2. Поле комплексных чисел — алгебра с делением ранга 2 над полем действительных чисел.

9.5.3. Поле примера 2.6.23 — алгебра с делением ранга 3 над полем действительных чисел.

9.5.4. Алгебра примера 2.7.3 — алгебра конечного ранга n^2 над полем **Q**.

9.5.5. Рассмотрим тело вопроса 2.6.21. Определим для элементов этого тела умножение на действительные числа, как в примере 2.7.2. В результате мы получим алгебру **K** с делением ранга 4 над полем действительных чисел. Всякую алгебру, изоморфную алгебре **K**, называют *алгеброй кватернионов*. Легко видеть, что всякий кватернион $q \rightleftharpoons \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}$ можно представить в виде

$$q = ai_0 + bi_1 + ci_2 + di_3,$$

где

$$a,\ b,\ c,\ d \in R;\quad i_0 \rightleftharpoons \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ i_1 \rightleftharpoons \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ i_2 \rightleftharpoons \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

$$i_3 \rightleftharpoons \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Следует заметить, что таблица умножения элементов i_0, i_1, i_2, i_3 имеет вид:

	i_0	i_1	i_2	i_3
i_0	i_0	i_1	i_2	i_3
i_1	i_1	$-i_0$	i_3	$-i_2$
i_2	i_2	$-i_3$	$-i_0$	i_1
i_3	i_3	i_2	$-i_1$	i_0

	b
a	$\rightarrow ab$

Легко проверить, что таблица умножения элементов i_0, i_1, i_2, i_3 определяется условиями:

1) i_0 — единица алгебры **K**;
2) $i_1 \cdot i_2 = -i_2 \cdot i_1 = i_3$;
3) $i_1^2 = i_2^2 = -i_0$.

Теорема 9.5.1. Если **A** — алгебра ранга n над полем **P**, то любые $k > n$ элементов алгебры **A** линейно зависимы над полем **P**.

Доказательство. Пусть $\langle e_1, \ldots, e_n\rangle$ — базис алгебры **A** над полем **P**; $\alpha_1, \ldots, \alpha_k$ — элементы **A**. Тогда в поле **P** можно найти элементы a_{ij}, $1 \leqslant i \leqslant k$, $1 \leqslant j \leqslant n$ такие, что:

$$\alpha_1 = a_{11}e_1 + \cdots + a_{1n}e_n;$$
$$\alpha_2 = a_{21}e_1 + \cdots + a_{2n}e_n;$$
$$\cdots\cdots\cdots\cdots$$
$$\alpha_k = a_{k1}e_1 + \cdots + a_{kn}e_n.$$

Поскольку в матрице

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{k1} & \dots & a_{kn} \end{pmatrix}$$

число строк больше числа столбцов, то утверждение теоремы сразу следует из известной теоремы линейной алгебры.

В дальнейшем мы, как правило, будем рассматривать ассоциативные алгебры с делением. Всякая такая алгебра **A** над полем **P** содержит поле, изоморфное **P** (вопрос 2.7.3). В связи с этим будем дальше предполагать, что само поле **P** является подполем алгебры **A**. Нетрудно заметить, что такое предположение в худшем случае равносильно изменению обозначений унарных алгебраических операций алгебры **A**.

Теорема 9.5.2. Пусть **A** — алгебра ранга n над полем **P**. Тогда любой элемент α алгебры **A** — корень многочлена степени не выше n над полем **P**.

Доказательство. В самом деле, по теореме 9.5.1 элементы

$$1, \alpha, \dots, \alpha^n$$

линейно зависимы над полем **P**. Отсюда прямо следует утверждение теоремы.

Теорема 9.5.3. Над полем **C** комплексных чисел нет других алгебр с делением конечного ранга, кроме самого поля **C**.

Доказательство. Пусть **A** — алгебра с делением ранга n над полем комплексных чисел **C**. Докажем, что любой ее элемент α принадлежит **C**. По теореме 9.5.2 элемент α — корень многочлена $f(x) \rightleftharpoons a_0 + a_1x + \dots + a_nx^n$ над полем **C**. По теореме 9.2.4 многочлен $f(x)$ можно разложить в произведение

$$f(x) = \varphi_1(x) \cdot \dots \cdot \varphi_s(x), \quad 1 \leqslant s \leqslant n \qquad (9.5.1)$$

линейных над **C** сомножителей. Заменяя в равенстве (9.5.1) x на α, что возможно (вопрос 2.6.13), получим

$$\varphi_1(\alpha) \cdot \dots \cdot \varphi_s(\alpha) = 0.$$

Так как алгебра **A** делителей нуля не имеет, то хотя бы один из сомножителей равен нулю. Отсюда и следует наше утверждение.

Вопросы: 9.5.1. Пусть **P** — подполе поля **A** и пусть каждый элемент поля **A** — корень неприводимого над полем **P** многочлена. Доказать, что всякое изоморфное отображение поля **P** в поле комплексных чисел **C** можно продолжить до изоморфизма поля **A** в поле **P**.

9.5.2. Пусть поле **A** — расширение поля рациональных чисел **Q** и пусть базис трансцендентности поля **A** относительно поля **Q** — континуальное множество. Доказать, что существует изоморфное отображение поля **A** в поле комплексных чисел.

9.5.3. Доказать, что для всякого поля $\mathbf{Q}_p$ p-адических чисел существует изоморфное отображение поля $\mathbf{Q}_p$ в поле комплексных чисел.

9.6. Алгебры над полем действительных чисел

Теорема 9.6.1. Пусть $\langle A; +, \cdot, \mathbf{R}\rangle$ — ассоциативная алгебра с делением конечного ранга n над полем действительных чисел $\mathbf{R}$. Тогда:

1) любой элемент α алгебры $\mathbf{A}$ — корень неприводимого над $\mathbf{R}$ многочлена первой или второй степени. При этом $\alpha \notin R$ тогда и только тогда, если α — корень неприводимого над полем $\mathbf{R}$ многочлена второй степени и, более того, если существуют такие действительные числа a и a', причем $a \neq 0$, что

$$(a\alpha + a')^2 = -1;$$

2) если $n = 2$, то алгебра $\mathbf{A}$ изоморфна алгебре комплексных чисел.

Доказательство. Известно, что (теорема 9.2.5) всякий многочлен с действительными коэффициентами степени выше нулевой разлагается в произведение неприводимых над полем $\mathbf{R}$ многочленов первой и второй степени. Отсюда, рассуждая как при доказательстве теоремы 9.5.3, получим:

а) любой элемент алгебры $\mathbf{A}$ — корень многочлена первой или второй степени над полем $\mathbf{R}$;

б) корнями приводимого многочлена над полем $\mathbf{R}$ могут быть только действительные числа.

Пусть теперь $\alpha \in A$, но $\alpha \notin R$. Из доказанного следует, что можно найти такие действительные числа p и q, что

$$\alpha^2 + p\alpha + q = 0 \qquad (9.6.1)$$

и

$$p^2 - 4q < 0.$$

Поэтому в силу теоремы 8.2.2 существует действительное число b такое, что

$$4q - p^2 = b^{-2}.$$

Умножая обе части равенства (9.6.1) на $4b^2$, мы без особых затруднений получим

$$(2b\alpha + bp)^2 + 1 = 0.$$

Пусть теперь ранг алгебры $\mathbf{A}$ над полем $\mathbf{R}$ равен 2. Тогда найдется элемент $\alpha \in A$ такой, что $\alpha \notin R$. Элементы 1, α линейно независимы над полем $\mathbf{R}$. Легко заметить, что для любых действительных чисел a и a', если только $a \neq 0$, элементы 1 и $\tau = a\alpha + a'$ также линейно независимы над $\mathbf{R}$. Числа a и a' выберем так, что

$$\tau^2 = (a\alpha + a')^2 = -1.$$

Элементы 1, τ образуют базис алгебры $\mathbf{A}$. Следовательно, любой элемент γ из A однозначно представим в виде

$$\gamma = x + y\tau, \quad x \in R, \quad y \in R.$$

Нетрудно проверить, что соответствие

$$x + y\tau \mapsto x + yi$$

является изоморфным отображением алгебры **A** на алгебру комплексных чисел.

Теорема 9.6.2. Не существует ассоциативных алгебр с делением ранга 3 над полем действительных чисел.

Доказательство. Пусть $\mathbf{A} \leftrightarrows \langle A;\ +,\ \cdot,\ \mathbf{R}\rangle$ — алгебра ранга $n \geqslant 3$ над полем действительных чисел. Тогда, рассуждая как при доказательстве теоремы 9.6.1, найдем линейно независимые над **R** элементы 1, α, β такие, что

$$\alpha^2 = \beta^2 = -1.$$

Докажем, что в таком случае элементы 1, α, β, $\alpha \cdot \beta$ линейно независимы над полем **R**. Таким образом, мы получим, что $n \geqslant 4$.

Предположим, что элементы 1, α, β, $\alpha \cdot \beta$ линейно зависимы над полем **R**. Тогда существуют действительные числа a, b, c такие, что

$$\alpha \cdot \beta = a + b\alpha + c\beta.$$

Умножая слева обе части этого равенства на α, получим

$$\alpha^2\beta = a\alpha + b\alpha^2 + c\alpha\beta.$$

Иначе

$$-\beta = a\alpha - b + c(a + b\alpha + c\beta).$$

Совершая несложные преобразования, найдем

$$ca - b + (a + bc)\alpha + (1 + c^2)\beta = 0.$$

Но

$$ca - b \in R, \quad a + bc \in R, \quad 1 + c^2 \in R.$$

Поэтому

$$ca - b = 0, \quad a + bc = 0, \quad 1 + c^2 = 0.$$

Последнее равенство, как известно, ни для какого действительного числа c выполняться не может. Отсюда следует, что элементы 1, α, β, $\alpha \cdot \beta$ линейно независимы над **R** и $n \geqslant 4$.

Теорема 9.6.3. Пусть **A** — ассоциативная алгебра с делением ранга $n \geqslant 4$ над полем **R** действительных чисел и ее элементы 1, α, β линейно независимы над этим полем, $\alpha^2 = \beta^2 = -1$. Тогда $\alpha\beta + \beta\alpha \in R$.

Доказательство. Из условия теоремы следует, что $\alpha + \beta \notin R$ и $\alpha - \beta \notin R$. По теореме 9.6.1 можно найти действительные числа p, q, p', q' такие, что:

$$\left.\begin{aligned}(\alpha + \beta)^2 &= p(\alpha + \beta) + q;\\ (\alpha - \beta)^2 &= p'(\alpha - \beta) + q'.\end{aligned}\right\} \qquad (9.6.2)$$

С другой стороны:

$$(\alpha + \beta)^2 = (\alpha + \beta)(\alpha + \beta) = \alpha^2 + \beta\alpha + \alpha\beta + \beta^2 = -2 + \beta\alpha + \alpha\beta;$$
$$(\alpha - \beta)^2 = (\alpha - \beta)(\alpha - \beta) = \alpha^2 - \beta\alpha - \alpha\beta + \beta^2 = -2 - \beta\alpha - \alpha\beta.$$

Поэтому, складывая почленно равенства (9.6.2), находим

$$-4 = (p + p')\alpha + (p - p')\beta + q + q'.$$

Отсюда в силу линейной независимости над полем $\mathbf{R}$ кортежа $\langle 1, \alpha, \beta\rangle$ получаем:

$$p + p' = 0, \quad p - p' = 0,$$

и, следовательно, $p = p' = 0$. Обратимся вновь к равенствам (9.6.2). Легко проверить теперь, что $2(\beta\alpha + \alpha\beta) = q - q'$. А это и доказывает наше утверждение.

Теорема 9.6.4. Всякая ассоциативная алгебра с делением ранга 4 над полем действительных чисел изоморфна алгебре кватернионов.

Доказательство. Пусть $\mathbf{A} \rightleftharpoons \langle A; +, \cdot, \mathbf{R}\rangle$ — ассоциативная алгебра ранга 4 над полем действительных чисел $\mathbf{R} \rightleftharpoons \langle R; +, \cdot, 0, 1\rangle$. Мы докажем, что алгебра имеет базис, состоящий из элементов $1, i, j, k$ таких, что

$$i^2 = j^2 = -1, \quad ij = -ji = k.$$

Рассуждая как при доказательстве теоремы 9.6.1, мы найдем линейно независимые над полем $\mathbf{R}$ элементы $1, \alpha, \beta$ такие, что $\alpha^2 = \beta^2 = -1$. Полагаем $i = \alpha$, $j = x\alpha + y\beta$, где x, y — действительные числа, которые подберем так, чтобы выполнялись условия:

1) элементы $1, i, j$ линейно независимы над полем $\mathbf{R}$;

2) $ij + ji = 0$;

3) $i^2 = j^2 = -1$.

Первое условие, очевидно, выполняется для любого действительного числа y, если $y \neq 0$. Далее заметим, что $\alpha\beta + \beta\alpha \in R$ в силу теоремы 9.6.3. Полагаем

$$a \rightleftharpoons \frac{1}{2}(\alpha\beta + \beta\alpha).$$

Элемент a — действительное число. Имеем

$$ij + ji = \alpha(x\alpha + y\beta) + (x\alpha + y\beta)\alpha = 2x\alpha^2 + y(\alpha\beta + \beta\alpha) =$$
$$= -2x + 2ay = 2(ay - x).$$

Таким образом, второе условие выполняется, если $x = ay$.

Выбором y попробуем обеспечить выполнение последнего условия. Мы имеем

$$(a\alpha + \beta)^2 = (a\alpha + \beta)(a\alpha + \beta) = a^2\alpha^2 + a(\alpha\beta + \beta\alpha) + \beta^2 =$$
$$= -a^2 + 2a^2 - 1 = a^2 - 1.$$

Так как элементы $1, \alpha, \beta$ линейно независимы над полем $\mathbf{R}$, то $a\alpha + \beta \notin R$, а поэтому $a^2 - 1 < 0$ в силу теоремы 9.6.1. По теореме 8.2.2 можно найти действительное число y такое, что

$$y^2(a^2 - 1) = -1.$$

В итоге получим

$$j^2 = (ay\alpha + y\beta)^2 = y^2(a^2 - 1) = -1.$$

Этим завершается доказательство теоремы.

Теорема 9.6.5. Над полем действительных чисел нет ассоциативных алгебр с делением конечного ранга n, если $n \geqslant 5$.

Доказательство. Пусть $\mathbf{A}$ — ассоциативная алгебра с делением над полем $\mathbf{R}$ действительных чисел конечного ранга n и $n \geqslant 5$. Рассуждая как при доказательстве теоремы 9.6.4, мы найдем элементы i, j, k такие, что:

1) элементы 1, i, j, k линейно независимы над $\mathbf{R}$;

2) $i^2 = j^2 = -1$, $ij = -ji = k$.

Так как ранг n больше 4, то в алгебре имеется еще по крайней мере один элемент l такой, что элементы 1, i, j, k, l линейно независимы над $\mathbf{R}$. Очевидно, можно предположить, что $l^2 = -1$. Поэтому по теореме 9.6.3 существуют действительные числа a, b, c такие, что:

$$il + li = a;$$
$$jl + lj = b;$$
$$kl + lk = c.$$

Имеем

$$lk = lij = (a - il)j = aj - ilj = aj - i(b - jl) =$$
$$= aj - bi + ijl = aj - bi + kl.$$

Но $kl = c - lk$. Поэтому

$$lk = aj - bi + c - lk.$$

Отсюда получаем

$$2lk = aj - bi + c.$$

Умножая справа обе части равенства на k, находим

$$-2l = ai + bj + ck,$$

что противоречит предположению о линейной независимости над полем $\mathbf{R}$ элементов 1, i, j, k, l.

Поля действительных и комплексных чисел и тело кватернионов мы можем рассматривать как алгебры над полем действительных чисел. Каждая из них алгебра с делением и имеет конечный ранг. Пусть $\mathbf{R}$, $\mathbf{C}$ и $\mathbf{K}$ эти алгебры. Ранги алгебр $\mathbf{R}$, $\mathbf{C}$, $\mathbf{K}$ соответственно равны 1, 2 и 4.

Из теорем 9.6.1, 9.6.2, 9.6.4 и 9.6.5 следует

Теорема Фробениуса. Над полем $\mathbf{R}$ действительных чисел любая ассоциативная алгебра $\mathbf{A}$ с делением конечного ранга n имеет ранг 1, 2 или 4. При этом:

1) если $n = 1$, то алгебра $\mathbf{A}$ изоморфна $\mathbf{R}$;

2) если $n = 2$, то алгебра $\mathbf{A}$ изоморфна $\mathbf{C}$;

3) если $n = 4$, то алгебра $\mathbf{A}$ изоморфна $\mathbf{K}$.

Вопросы: **9.7.1.** Доказать, что формулы:

1) $(a+b)^2 = a^2 + 2ab + b^2$;
2) $a^2 - b^2 = (a+b)(a-b)$

для элементов алгебры кватернионов не верны.

9.7.2. Доказать, что теорема о том, что всякий многочлен степени n (в частности $n = 2$) имеет не более n корней, не верна в алгебре кватернионов.

9.7.3. Пусть $q \rightleftharpoons a + bi + cj + dk$ — кватернион. Обозначим через q^* кватернион вида

$$q^* = a - bi - cj - dk.$$

Показать, что:

1) $(q_1 \cdot q_2)^* = q_2^* \cdot q_1^*$;

2) $q \cdot q^* = q^* \cdot q = a^2 + b^2 + c^2 + d^2$.

9.7.4. Для любых кватернионов q_1 и q_2 доказать тождество

$$(q_1 \cdot q_1^*) \cdot (q_2 \cdot q_2^*) = (q_1 \cdot q_2) \cdot (q_1 \cdot q_2)^*$$

и вывести отсюда, что произведение суммы квадратов четырех целых чисел на сумму квадратов четырех целых чисел, есть сумма квадратов четырех целых чисел (*тождество Эйлера*).

9.7.5. Доказать, что

$$q_1 q_2 + (q_1 q_2)^* = q_2 q_1 + (q_2 q_1)^*$$

для любых кватернионов q_1 и q_2.

9.7.6. Пусть $\mathbf{K} \rightleftharpoons \langle K;\ +,\ \cdot,\ 0,\ \mathbf{R}\rangle$ — алгебра кватернионов. На множестве K^2 определим две бинарные операции и для каждого действительного числа a оператор условиями:

1) $\langle \alpha_1, \beta_1\rangle + \langle \alpha_2, \beta_2\rangle \rightleftharpoons \langle \alpha_1 + \alpha_2,\ \beta_1 + \beta_2\rangle$;

2) $\langle \alpha_1, \beta_1\rangle \cdot \langle \alpha_2, \beta_2\rangle \rightleftharpoons \langle \alpha_1\alpha_2 - \beta_2^*\beta_1,\ \beta_2\alpha_1 + \beta_1\alpha_2^*\rangle$;

3) $a \cdot \langle \alpha, \beta\rangle \rightleftharpoons \langle a\alpha, a\beta\rangle$.

Пусть далее:

4) $U \rightleftharpoons K^2$;

5) $\forall\, (\alpha, \beta \in K)\quad \langle \overline{\alpha, \beta}\rangle \rightleftharpoons \langle \alpha^*, -\beta\rangle$;

6) $\forall\, (\xi \in U)\quad \nu(\xi) \rightleftharpoons \xi \cdot \overline{\xi}$.

Доказать, что алгебра $\mathbf{U} \rightleftharpoons \langle U;\ +,\ \cdot,\ \mathbf{R}\rangle$:

1) линейна;
2) $\forall\, (\alpha, \beta) \in K\quad \langle \alpha, \beta\rangle = \langle \alpha, 0\rangle + \langle \beta, 0\rangle \cdot \langle 0, 1\rangle$;
3) конечного ранга 8;
4) альтернативна;
5) отображение $\alpha \mapsto \langle \alpha, 0\rangle$ является изоморфным отображением алгебры кватернионов в алгебру $\mathbf{U}$;

6) $\forall (\xi, \eta \in U)\quad \overline{\xi} \cdot (\xi \cdot \eta) = (\eta \cdot \xi) \cdot \overline{\xi} = \nu(\xi)\eta$;

7) с делением.

Алгебру вопроса 9.7.6 и любую, ей изоморфную, называют *алгеброй Кэли*. Элементы этой алгебры называют *числами Кэли*.

9.7.7. Доказать, что для любых элементов ξ и η алгебры Кэли

$$\nu(\xi \cdot \eta) = \nu(\xi) \cdot \nu(\eta).$$

Верна следующая

Теорема. Любая альтернативная линейная алгебра с делением конечной размерности над полем действительных чисел имеет ранг 1, 2, 4 или 8. В первом случае она изоморфна полю действительных чисел, во втором — алгебре комплексных чисел, в третьем — алгебре кватернионов, в четвертом — алгебре Кэли.

УКАЗАНИЯ И РЕШЕНИЯ

2.3.4. Рассмотреть отображение

$$\langle a, b\rangle \mapsto \frac{1}{2}(a+b-1)(a+b-2)+2.$$

2.3.11. 1) Воспользоваться свойством 1.3.17.
2) $A = S \cup (A \setminus S)$.

2.3.13. Из 2.3.11 и 2.3.12 следует существование взаимно-однозначного отображения множества A на подмножество θ (B) этого множества.

2.6.7. Определение 2.5.2.

2.6.13. Пусть сначала $f(x) \rightleftharpoons ax^k$ и $g(x) \rightleftharpoons bx^l$. Имеем:

$$[f(x)\cdot g(x)]_{x=\alpha} = [ax^k \cdot bx^l]_{x=\alpha} = [abx^{k+l}]_{x=\alpha} = ab\alpha^{k+l};$$

$$[f(x)]_{x=\alpha}\cdot[g(x)]_{x=\alpha} = [ax^k]_{x=\alpha}\cdot[bx^l]_{x=\alpha} = a\alpha^k \cdot b\alpha^l = ab\alpha^{k+l}.$$

Далее, следует проверить, что из (2.6.1) и

$$[f(x)\cdot h(x)]_{x=\alpha} = [f(x)]_{x=\alpha}\cdot[h(x)]_{x=\alpha}$$

следует

$$[f(x)\cdot(g(x)+h(x))]_{x=\alpha} = [f(x)]_{x=\alpha}\cdot[g(x)+h(x)]_{x=\alpha}.$$

2.6.21. Прежде всего нужно доказать, что $\langle M_2'; \oplus, \odot\rangle$ — кольцо с единицей. Это легко сделать, если воспользоваться результатами вопросов 2.6.1 и 2.6.9. Далее через q^* обозначим матрицу

$$q^* \rightleftharpoons \begin{pmatrix} \bar{\alpha} & -\beta \\ \bar{\beta} & \alpha \end{pmatrix}.$$

Рассматривая произведение qq^*, легко убедиться в том, что всякая отличная от нуля матрица q имеет обратный элемент.

2.8.6. Ввести в рассмотрение множество P' всех элементов $x\varepsilon$ таких, что $x \in P$. Пусть 0 — нуль поля P, θ — нуль алгебры A. Если $x \neq 0$, то $\exists(y \in P)\ y\cdot x = 1$. Поэтому из $\theta = x\varepsilon$ следует

$$\theta = y\theta = yx\cdot\varepsilon = 1\cdot\varepsilon = \varepsilon,$$

чего нет в кольце с единицей. Окончание доказательства несложно.

2.10.1. Воспользоваться результатом вопроса 2.9.4.

3.5.2. Из аксиом A_I, A_{II}, A_{III} следует, что для любой пары элементов d, d' множества G существуют элементы e, f, g такие, что $ed = d$, $ef = d'$, $dg = f$. Поэтому $f = dg = (ed)\,g$ и $d' = ef = e\,(dg)$. Из аксиомы A_{IV} следует $f = d'$. Тем самым доказано существование левой единицы. Аналогично рассуждая, находим, что для любой пары элементов d, d' из G в G существуют элементы x, y, z такие, что $xd = e$, $xy = d'$, $dz = y$.

Поэтому имеем $z = ez = (xd) \cdot z$ и $d' = xy = x\,(dz)$. В силу аксиомы A_{IV} находим, что $z = d'$. Итак,

$$\forall\,(d, d' \in G) \quad \exists\,(y \in G) \quad d \cdot d' = y.$$

4.6.19. Сначала докажем, что

$$\forall\,(a \in N) \quad a > 1 \Leftrightarrow a \neq 1.$$

Из $a > 1$ в силу антирефлексивности следует, что $a \neq 1$. Обозначим через M множество $\{a \mid a = 1 \vee a > 1\}$. Легко доказывается, что $M = N$. Затем без труда устанавливается, что $\forall\,(a \in N)\ a + 1 > a$. Далее введем множество условием

$$M_1 \Leftrightarrow \{a \mid \forall\,(n \in N) \quad n > a \Rightarrow \exists\,(x \in N) \quad n = a + x\}$$

и доказываем, что $M_1 = N$. Таким образом,

$$\forall\,(a, b \in N) \quad b > a \quad \Rightarrow \exists\,(x \in N) \quad b = a + x.$$

Пусть теперь $b = a + x$, тогда $a \neq b$ и, следовательно, $a > b$ либо $b > a$. В первом случае, по доказанному,

$$\exists\,(y \in N) \quad a = b + x,$$

в противоречии с теоремой 4.5.3.

4.6.20. Первое утверждение доказывается при помощи рассуждений, сходных с теми, которые проводятся при доказательстве утверждения вопроса 4.6.19. Чтобы доказать, что ни одно из условий не является лишним, достаточно привести примеры четырех бинарных отношений на множестве натуральных чисел, каждое из которых не удовлетворяет последовательно одному из указанных условий и удовлетворяет трем остальным. Такими отношениями будут:

1) $a > b \Leftrightarrow a \not> b$;

2) $a > b \Leftrightarrow a \neq b$;

3) $a > b \Leftrightarrow (b = 1 \wedge a \neq 1) \vee (b \neq 1 \wedge a > b + 1)$;

4) $a > b \Leftrightarrow a > b + 1$.

4.7.2. Пусть A — множество четных, B — нечетных натуральных чисел. Тогда $N = A \cup B$ и $A \cap B = \varnothing$. Равенство $\mathfrak{a}_0 \cdot \mathfrak{a}_0 = \mathfrak{a}_0$ следует из 2.3.4.

4.8.5. Обозначим через M множество тех натуральных n, для которых утверждение вопроса 4.8.5 верно. Легко видеть, что $1 \in M$. Предположим, что $n \in M$, и докажем, что $n + 1 \in M$. Пусть S — взаимно-однозначное отображение отрезка $[1, n + 1]$ на себя.

Если $S(n+1) = n+1$, то имеем

$$\sum_{x=1}^{n+1} a_{S(x)} = \sum_{x=1}^{h} a_{S(x)} + a_{n+1}.$$

А дальше следует воспользоваться тем, что S индуцирует взаимно-однозначное отображение отрезка $[1, n]$ на себя. Пусть теперь $S(n+1) = b \neq n+1$ и $S(k) = n+1$. Из вопроса 4.8.2 и коммутативности сложения следует, что

$$\sum_{x=1}^{n+1} a_{S(x)} = \sum_{x=1}^{k-1} a_{S(x)} + a_{S(k)} + \sum_{x=k+1}^{n} a_{S(x)} + a_{S(n+1)} =$$

$$= \sum_{x=1}^{k-1} a_{S(x)} + a_{S(n+1)} + \sum_{x=k+1}^{n} a_{S(x)} + a_{S(k)}.$$

Введя новое взаимно-однозначное отображение t отрезка $[1, n+1]$ на себя условием

$$t_x \rightleftharpoons \begin{cases} S(x), & \text{если } x \neq k; \quad \wedge x = n+1; \\ e = S(n+1), & \text{если } x = k; \\ n+1 = S(k), & \text{если } x = n+1, \end{cases}$$

легко закончить рассуждение.

4.8.9. Прежде всего заметим, что отношение S легко определяется через первичные термины нашей теории:

$$Sa \rightleftharpoons a + 1.$$

Таким образом, перечень первичных терминов второй теории содержится в совокупности терминов первой. Легко видеть также, что все аксиомы второй теории являются теоремами первой. Они просто переходят в ее аксиомы. Нам остается показать, что первичные термины первой теории выразимы через термины второй, а аксиомы первой теории являются теоремами второй.

Для этой цели определим во второй теории два тернарных отношения: $\oplus$ — сумма — и $\odot$ — произведение — так, чтобы выполнялись следующие условия:

$$\forall (a \in A) \quad \exists ! (c \in A) \quad c \in a \oplus 1; \tag{I}$$

$$\forall (a, b \in A) \quad a \oplus Sb = S(a + b); \tag{II}$$

$$\forall (a \in A) \quad a \odot 1 = a; \tag{III}$$

$$\forall (a, b \in A) \quad a \odot Sb = a \odot b \oplus a. \tag{IV}$$

При фиксированном a каждое из вводимых нами тернарных отношений бинарное. Чтобы ввести искомые тернарные отношения, введем для каждого a бинарные отношения с теми же условиями. Иначе говоря, покажем, что для каждого a из A можно ввести бинарное отношение $\oplus$, удовлетворяющее условиям:

$$\exists ! (c \in A) \quad c \in a \oplus 1; \tag{V}$$

$$\forall (b \in A) \quad a \oplus Sb = S(a \oplus b). \tag{VI}$$

Пусть сначала $a = 1$. Полагаем

$$\forall (b \in A) \quad 1 \oplus b = Sb.$$

Имеем:

1) $1 \oplus 1 = S\ 1$.

В силу аксиомы A_{II} — условие (V) выполнено.

2) $\forall (b \in A) \quad 1 \oplus Sb = SSb$.

Таким образом, условие (VI) для введенного нами бинарного отношения также выполнено.

Пусть для какого-нибудь $a \in A$ определено бинарное отношение $\oplus$, и притом так, что условия (V) и (VI) выполнены. Полагаем

$$Sa \oplus b = S(a \oplus b). \tag{VII}$$

Имеем:

1) $Sa \oplus 1 = S(a \oplus 1)$.

В силу предположения индукции и аксиомы A_{II} условие (V) для Sa выполнено.

2) $\forall (b \in A) \quad Sa \oplus Sb = S(a \oplus Sb)$

в силу равенства (VII). Далее, в силу равенства (VI) получим

$$S(a \oplus Sb) = SS(a \oplus b).$$

Далее вновь применяется равенство (VII):

$$SS(a \oplus b) = S(Sa \oplus b).$$

Окончательно имеем

$$\forall (b \in A) \quad Sa \oplus Sb = S(Sa \oplus b).$$

Таким образом, условие (VI) для Sa выполняется. По аксиоме A_{IV} для любого a из A с каждым b из A можно сопоставить элемент $a \oplus b$ так, что будут выполняться условия (V) и (VI). А это определяет тернарное отношение $\oplus$, удовлетворяющее условиям (I) и (II).

Аналогично можно определить тернарное отношение $\odot$ — умножение, удовлетворяющее условиям (III) и (IV). Нетрудно видеть, что аксиомы первой теории после введения этих отношений становятся теоремами второй теории. Тем самым показана эквивалентность формулировок обеих аксиоматических теорий.

4.8.10. Докажем, что в наших предположениях для каждого натурального z существует и только одна функция c_z

$$c_z: \quad A \times [1, z] \to B,$$

которая удовлетворяет условиям:

$$\left.\begin{array}{l} \forall (x \in A) \quad c_z(x, 1) = a(z); \\ \forall (x \in A)\, \forall (y \in N)\ 1 \leqslant y < z \Rightarrow c_z(x, y+1) = b(x, y, c_z(x,y)). \end{array}\right\} \tag{VIII}$$

Пусть M — множество тех натуральных z, для которых функция c_z с условиями (VIII) существует. Легко доказать, что $M = N$.

Пусть c_z и c'_z — функции, удовлетворяющие условиям (VIII), и M — объединение множества

$$M_1 \rightleftharpoons \{n \mid n \in N \wedge n > z\}$$

и множества

$$M_2 \rightleftharpoons \{n \mid n \in N, \quad \forall (x \in A)\, c_z(x_1 n) = c'_z(x, n)\}.$$

Легко доказывается, что $M = N$. Далее заметим, что

$$\forall (x \in A) \forall (z, z' \in N) \forall (y \in N)\, y \leqslant \min(z, z') \Rightarrow$$
$$\Rightarrow c_z(x, y) = c_{z'}(x, y).$$

Полагаем

$$\forall (x \in A) \forall (y \in N) \forall (z \in N)\, z \geqslant y \Rightarrow c(x, y) \rightleftharpoons c_z(x, y).$$

Нетрудно проверить, что функция c удовлетворяет условиям (4.8.2), а также, что этими условиями функция c определяется однозначно.

4.8.12. Пусть $k \in N_0$ и

$$M = \{x \mid x \in N_0 \wedge 0 \leqslant x \leqslant k\}.$$

Индукцией по n можно доказать, что для каждого натурального $n \leqslant k + 1$ существует частичная на множестве $M \times M$ функция, значения которой определены для всех пар $\langle x, y\rangle$ таких, что

$$0 \leqslant x \leqslant y < x + n \wedge 0 \leqslant x \leqslant y \leqslant k,$$

и которая удовлетворяет следующим условиям:

$$\forall (x \in M) \quad f_\alpha^{(n)}(x) = a_x;$$
$$\forall (x, y \in M) \quad 0 \leqslant x < y \leqslant x + n \Rightarrow$$
$$\Rightarrow f_\alpha^{(n)}(x, y) = a_x + \frac{1}{f_\alpha^{(n)}(x + 1, y)}.$$

4.9.1. Рассмотреть интерпретации:

1) $N^{(1)} \rightleftharpoons E = \varnothing$;

2) $N^{(2)} \rightleftharpoons E = \{1\}$; $1 \oplus 1 = \varnothing$; $1 \odot 1 = 1$;

3) $N^{(3)} \rightleftharpoons \{1, 2\}$; $E \rightleftharpoons \{1\}$;

$$\forall (a, b \in N^{(3)}) \quad a \oplus b \rightleftharpoons 2;$$
$$\forall (a, b \in N^{(3)})\, a \odot b \rightleftharpoons \begin{cases} 1, \text{ если } b = 1, \\ 2, \text{ в противном случае;} \end{cases}$$

4) $N^{(4)} \rightleftharpoons N$; $E \rightleftharpoons \{1\}$;

$$\forall (a, b \in N^{(4)}) \quad a \oplus b \rightleftharpoons \begin{cases} a + 1, \text{ если } b = 1, \\ \varnothing, \text{ в противном случае;} \end{cases}$$

$$\forall (a, b \in N^{(4)}) \quad a \odot b = \begin{cases} a \cdot b, \text{ если } a = 1 \text{ или } b = 1, \\ \varnothing, \text{ в противном случае;} \end{cases}$$

5) $N^{(5)} \rightleftharpoons N$; $E \rightleftharpoons \{1\}$;

$$\forall (a, b \in N^{(5)}) \quad a \oplus b \rightleftharpoons a + b; \quad a \odot b \rightleftharpoons \varnothing;$$

6) $N^{(6)} \rightleftharpoons N$; $E \rightleftharpoons \{1\}$;

$$\forall (a, b \in N^{(6)}) \quad a \oplus b \rightleftharpoons a + b;$$

$$\forall (a, b \in N^{(6)}) \quad a \odot b \rightleftharpoons \begin{cases} 1, & \text{если } b = 1, \\ \varnothing, & \text{если } b \neq 1. \end{cases}$$

5.1.5. 24; 6; 6.

5.1.8. Определение 5.1.3.

5.1.12. Следует из линейности порядка $\succ$.

5.1.13. Если a — наименьший элемент множества $A \setminus B$ и

$$\forall (x \in B)\, \forall (y \in A \setminus B)\ y \succ x,$$

то B — интервал, отделенный элементом a.

5.1.14. Пусть a — наименьший элемент множества

$$M \rightleftharpoons \{x \mid x \in A \wedge \varphi(x) < x\}$$

и $b = \varphi(a)$. Тогда $b < a$. Из свойств отображения φ следует, что $\varphi(b) < \varphi(a) = b$.

5.1.15. Следует из 5.1.14.

5.1.19. Пусть β и γ — какие-нибудь элементы множества $W(\alpha)$ и $\alpha \rightleftharpoons \mathbf{A}$, $\beta \rightleftharpoons \mathbf{B}$, $\gamma \rightleftharpoons \mathbf{C}$. Тогда системы $\mathbf{B}$ и $\mathbf{C}$ соответственно изоморфны некоторым интервалам $\mathbf{P}_a \rightleftharpoons \langle P_a; \leqslant \rangle$ и $\mathbf{P}_b \rightleftharpoons \langle P_b; \leqslant \rangle$ вполне упорядоченного множества $\mathbf{A}$. Если $b < c$, то интервал $\mathbf{P}_b$ изоморфно отображается на некоторый интервал системы $\mathbf{P}_c$. Поэтому $\beta < \gamma$. Отсюда и из вопроса 5.1.18 следует: система $\langle W(\alpha); \leqslant \rangle$ — линейно упорядоченное множество. Сопоставляя с элементом b множества A порядковое число $\beta \rightleftharpoons \overline{\mathbf{P}}_b$, легко убедиться в том, что определенное так соответствие — изоморфное отображение системы $\mathbf{A}$ на систему $\langle W(\alpha); \leqslant \rangle$. Отсюда следует, что система $\mathbf{W}(\alpha) \rightleftharpoons \langle W(\alpha); \leqslant \rangle$ — вполне упорядоченное множество и что $\alpha = \mathbf{W}(\alpha)$.

5.1.20. Пусть $\mathbf{A} \rightleftharpoons \langle W(\alpha); \leqslant \rangle$, $\mathbf{B} \rightleftharpoons \langle W(\beta); \leqslant \rangle$ и $C \rightleftharpoons A \cap B$. Система $\mathbf{C} \rightleftharpoons \langle C; \leqslant \rangle$ — вполне упорядоченное множество. Пусть $\gamma \rightleftharpoons \mathbf{C}$. Если $C \subset A$ и $C \subset B$, то $\mathbf{C}$ — интервал каждой из систем $\mathbf{A}$ и $\mathbf{B}$ и поэтому $\gamma \in C$, чего не может быть.

5.1.25. Имеем

$$\mathfrak{a} \leqslant \mathfrak{b} + \mathfrak{a} \leqslant \mathfrak{a} + \mathfrak{a} \leqslant 2\mathfrak{a} \leqslant \mathfrak{a}_0 \cdot \mathfrak{a}.$$

Поэтому достаточно доказать равенство

$$\mathfrak{a}_0 \cdot \mathfrak{a} = \mathfrak{a}.$$

Это равенство можно вывести, если воспользоваться результатами вопросов 5.1.23 и 5.1.24.

5.1.27. Имеем

$$\mathfrak{a} \leqslant \mathfrak{b}\mathfrak{a} \leqslant \mathfrak{a}^2.$$

Поэтому достаточно доказать, что $a^2 = a$. Последнее равенство можно вывести, если воспользоваться результатами вопросов 5.1.23 и 5.1.25.

5.2.4. Из соотношений $a + a \succ a$ и $b + b \succ b$ следует, что

$$a + b + a + b \succ a + b, \quad a + a + b + b \succ a + b + b \quad \text{и}$$

$$a + b + b \succ a + b.$$

Если $a + b + a + b = a + b$, то в силу антисимметричности отношения порядка, мы получим, что $a + b + b = a + b$. А это влечет $b + b = b$.

5.2.5. Если a и b положительны, то по теореме 5.2.4 $a + b \succ b$ и $a + b \succ a$. Отсюда следует, что

$$a + b + a + b \succ a + b \text{ и } a + b + a + b \neq a + b.$$

5.2.7. См. пример 5.2.5.

5.2.9. Показать, что множество автоморфизмов мультипликативной полугруппы натуральных чисел бесконечно.

5.4.1. Показать, что $(a + b\sqrt{2}) \cdot b\sqrt{2} > 0$ в любом порядке этого поля, если только $a^2 - 2b^2 < 0$.

6.2.10. Сначала доказывается, что из указанных пяти условий следует монотонность порядка $\succ$ относительно сложения. Затем, что

$$\forall (a, b \in Z) \forall (n \in N) \quad a = b + n \Rightarrow a \succ b$$

и

$$\forall (a, b \in Z) \quad a \neq b \Rightarrow a \succ b \vee b \succ a.$$

Чтобы доказать, что ни одно из пяти условий не является лишним, достаточно найти примеры таких пяти бинарных отношений в кольце целых чисел, каждое из которых не удовлетворяет последовательно одному из указанных отношений и удовлетворяет всем остальным. Такими отношениями будут:

1) $a \succ b \Leftrightarrow a \geqslant b$;
2) $a \succ b \Leftrightarrow a \neq b$;
3) $a \succ b \Leftrightarrow a > b \wedge 1 > a$;
4) $a \succ b \Leftrightarrow a > b \wedge b \geqslant 0$;
5) $a \succ b \Leftrightarrow a > b + 1$.

6.6.9. Сначала показать, что этими условиями определяется строгий и линейный порядок в аддитивной группе рациональных чисел. Затем рассмотреть бинарные отношения в поле рациональных чисел, определяемые ниже:

1) $a \succ b \Leftrightarrow a \geqslant b$;
2) $a \succ b \Leftrightarrow a \neq b$;
3) $a \succ b \Leftrightarrow (a > b \wedge (a) = (b)) \vee ((a) > (b))$*;
4) $a \succ b \Leftrightarrow a > b \wedge a, b \in N$;
5) $a \succ b \Leftrightarrow b > a$.

---

* (X) — дробная доля X, т. е. $(X) = X - [X]$.

7.1.3. Воспользоваться леммой: если α, β, γ — любые положительные числа и $\gamma^n \leqslant \alpha n + \beta$ для каждого натурального n, то $\gamma \leqslant 1$.

7.5.3. Легко проверить, что достаточно доказать следующее:

$$\forall\, (x,\ y \in T) \qquad x > 1 \wedge y > 1 \Rightarrow xy = yx.$$

Предположим, что

$$x > 1,\ y > 1,\ xy > yx$$

для каких-либо элементов x и y тела **T**. В таком случае

$$xyx^{-1}y^{-1} > 1.$$

Далее найдем элемент $r \in T$ такой, что

$$1 < r < x,\ r < y,\ r^2 < xyx^{-1}y^{-1}.$$

Наконец, находим натуральные n и m такие, что

$$r^n \leqslant x < r^{n+1},\ r^m \leqslant y < r^{m+1}$$

(вопрос 7.5.2). Отсюда имеем

$$xy < r^{n+m+2},\ x^{-1} < r^{-n},\ y^{-1} < r^{-m},$$

и поэтому

$$xyx^{-1}y^{-1} < r^2.$$

8.2.1. С каждым элементом α архимедовски упорядоченного поля сопоставить сходящуюся к α последовательность рациональных чисел этого поля.

8.2.4. Введем, пользуясь теоремой Цермело, в R полный порядок, а затем удалим из R каждое число, которое линейно с коэффициентами из Q выражается через конечное множество предшествующих (в этом порядке). Далее нетрудно показать, что оставшиеся элементы образуют искомый базис.

8.2.7. На первую часть вопроса ответить нетрудно. Далее, достаточно рассмотреть пять бинарных отношений в поле, определяемых следующим образом:

1) $a \succ b \Leftrightarrow a \geqslant b$;
2) $a \succ b \Leftrightarrow a \neq b$;
3) отношение вопроса 8.2.6;
4) $a \succ b \Leftrightarrow a > b$ (a, b — целые числа);
5) отношение вопроса 8.2.5.

8.2.9. Вопрос 8.2.5.

8.2.14. а) $r \in N$. Теорема 5.2.2. б) $\frac{1}{r} \in N$. Определение 8.2.1.

8.2.15. а) $q = 0$; 8.2.14.

8.2.16. $a^n - b^n = (a - b)\ (a^{n-1} + a^{n-2}\, b + \ldots + b^{n-1})$.

8.2.17. 8.2.14.

8.2.18. 8.2.16.

8.2.20. а) $r \in N$; 8.2.18.

8.2.21. 8.2.19 и 8.2.20.

8.2.23. а) $c > 1$,

$$1 < c^{b_n} < 1 + \varepsilon \Leftrightarrow 1 < c < (1 + \varepsilon)^{\frac{1}{b_n}}.$$

8.3.1. С каждым подмножеством $M \subset N$ сопоставим последовательность $\{a_n\}_{n=1}^{\infty}$ целых чисел, определяемую из условий:

$$a_n = \begin{cases} 1, & \text{если } n \in M; \\ 0, & \text{если } n \notin M, \end{cases}$$

и двоичную дробь

$$0,\ a_1,\ a_2,\ \ldots,\ a_n,\ \ldots,$$

т. е. ряд

$$\sum_{n=1}^{\infty} a_n 2^{-n}.$$

8.7.2. 1) Выражение для I находится путем повторного применения правила интегрирования по частям.

2) Следует из 1).

3) Если $k \geqslant n$, то $f^{(k)}(x)$ — многочлен с целыми коэффициентами и $f^{(k)}(0)$, $f^{(k)}(1)$ — целые числа. Если $0 \leqslant k \leqslant n-1$, то $f^{(k)}(0) = f^{(k)}(1) = 0$.

4) Если $0 < x < 1$, то $0 < f(x) < 1$.

5) Из 2), 3) и 4) следует, что существует целое положительное и сколь угодно малое число.

8.7.3. Следует из 8.7.2.

8.7.4. 1) Выражение для I_k находится путем повторного применения правила интегрирования по частям.

2) Следует из 1).

3) Если $k \geqslant p$, то $f^{(k)}(x)$ — многочлен с целыми, кратными p коэффициентами и $f^{(k)}(x)$ — целое, кратное p число при любом целом x. Для каждого целого x от 1 до n многочлен f и его первые $p-1$ производные обращаются в нуль. Если $x = 0$, то многочлен f и его первые $p-2$ производные также обращаются в нуль. Но число

$$f^{(p-1)}(0) = (n!)^p$$

не делится на p, если $p > n$.

4) Если $0 \leqslant x \leqslant n$, то $|f(x)| \leqslant \dfrac{n^{np+p-1}}{(p-1)!}$.

5) Из 2), 3) и 4) следует, что существует не равное нулю целое и сколь угодно малое число.

8.7.5. Следует из 8.7.4.

8.7.6. 1), 2), 4) и 6) доказываются индукцией по n. 3) Очевидно.

5) Для каждого допустимого значения n, начиная с 1, полагаем:

$$c_n = |b_n|;$$

$$Q_n^1 = 1 + c_1 + c_1c_2 + \ldots + c_1c_2 \cdot \ldots \cdot c_n;$$

$$S_n = \frac{c_1}{Q_1^1} + \frac{c_1c_2}{Q_1^1Q_2^1} + \ldots + \frac{c_1c_2 \cdot \ldots \cdot c_n}{Q_{n-1}^1Q_n^1}.$$

Так как $S_n \leqslant S_{n+1}$ и $S_n = 1 - \frac{1}{Q_n^1} < 1$, то последовательность $\{S_n\}_{n=1}^{\infty}$ сходится. Из 1) и 4) при $n \geqslant 1$ находим, что

$$\delta_n - \delta_0 = \frac{b_1}{Q_1} - \frac{b_1 b_2}{Q_1 Q_2} + \ldots + (-1)^{n-1} \frac{b_1 b_2 \cdot \ldots \cdot b_n}{Q_{n-1} Q_n}$$

и что

$$\left| (-1)^{i-1} \frac{b_1 \cdot \ldots \cdot b_i}{Q_{i-1} Q_i} \right| \leqslant \frac{c_1 \cdot \ldots \cdot c_i}{Q'_{i-1} Q'_i}$$

для каждого натурального i от 1 до n. Отсюда легко следует сходимость последовательности $\{\delta_n\}_{n=0}^{\infty}$.

7) Проверяется непосредственно.

8) Следует из 1) и 2).

9) Из уравнения

$$y = \frac{xP_{n-1} + b_n P_{n-2}}{xQ_{n-1} + b_n Q_{n-2}}$$

и 7) следует, что для каждого положительного x и $n \geqslant 2$ число y принадлежит интервалу с концами δ_{n-1} и δ_{n-2}. Взаимно-однозначность названного отображения проверяется без труда.

10) Из 8), 9) и 6) следует, что если цепная дробь с положительными элементами сходится к числу α, то число α принадлежит интервалу с концами δ_{n-1} и δ_{n-2}. Но тогда $\alpha_n > 0$ в силу 6) и 9). Наоборот, если все полные частные разложения числа α в данную цепную дробь положительны, то число α в силу 9) принадлежит интервалу с концами δ_{n-1} и δ_{n-2} и, следовательно, последовательность $\{\delta_n\}_{n=0}^{\infty}$ сходится к числу α.

11) В силу 5) данная цепная дробь сходится к некоторому числу α. В силу 9) это число положительно. Предположим теперь, что число α рационально. Тогда из равенства

$$\alpha_{n-1} = a_{n-1} + \frac{1}{\alpha_n},$$

верного для любого натурального n, следует, что при каждом натуральном n число $\alpha_{n-1} - a_{n-1}$ положительно и рационально. Обозначая для каждого неотрицательного целого n через A_n и B_n натуральные и взаимно-простые числа такие, что $\alpha_n - a_n = \frac{A_n}{B_n}$, мы получим

$$\frac{A_{n-1}}{B_{n-1}} = \frac{b_n}{a_n + \frac{A_n}{B_n}}.$$

Но $a_n > b_n$, поэтому $B_{n-1} > A_{n-1}$. Далее имеем

$$\frac{A_{n-1}}{B_{n-1}} = \frac{b_n B_n}{a_n B_n + A_n}.$$

Так как числа A_{n-1} и B_{n-1} взаимно-просты, то для некоторого натурального числа c:

$$cA_{n-1} = b_nB_n;$$

$$cB_{n-1} = a_nB_n + A_n.$$

Из этих равенств легко следует, что числа c и B_n взаимно-просты. Поэтому число b_n кратно c и $A_{n-1} \geqslant B_n$. Итак, для каждого натурального n

$$B_{n-1} > A_{n-1} \geqslant B_n.$$

Поэтому последовательность $\{B_n\}_{n=0}^{\infty}$ натуральных чисел строго убывает, что заведомо невозможно.

12) Из 1) и 2) следует, что цепная дробь (8.7.18) с положительными элементами сходится тогда и только тогда, если

$$\lim \frac{1}{Q_nQ_{n-1}} = 0.$$

Так как $Q_0 = 1$, $Q_1 = a_1$, то из равенства $Q_n = a_nQ_{n-1} + Q_{n-2}$ легко следует, что любой знаменатель подходящей дроби четного порядка не меньше 1, а нечетного порядка — не меньше a_1. Следовательно, каково бы ни было натуральное число k,

$$Q_{2k} \geqslant a_1a_{2k} + Q_{2k-2};$$

$$Q_{2k+1} \geqslant a_{2k+1} + Q_{2k-1}.$$

Применяя эти неравенства повторно, мы получим:

$$Q_{2k} \geqslant a_1(a_2 + a_4 + \ldots + a_{2k});$$

$$Q_{2k+1} \geqslant a_1 + a_3 + \ldots + a_{2k+1}.$$

Поэтому, если ряд $\sum_{n=0}^{\infty} a_n$ расходится, то

$$\lim_{k\to\infty} \frac{1}{Q_{2k}Q_{2k+1}} = 0.$$

Из равенства $Q_n = a_nQ_{n-1} + Q_{n-2}$ индукцией по n легко выводится неравенство

$$Q_n < (1 + a_1)(1 + a_2) \cdot \ldots \cdot (1 + a_n).$$

Но $1 + x < e^x$ для каждого положительного x. Поэтому

$$Q_n < e^{\sum_{i=0}^{n} a_i}.$$

Следовательно, если ряд $\sum_{n=0}^{\infty} a_n$ сходится, то последовательность $\{Q_n\}_{n=0}^{\infty}$ ограничена и последовательность $\left\{\frac{1}{Q_nQ_{n-1}}\right\}_n$ к нулю не сходится.

9.2.1. Модуль комплексного числа.

9.2.2. Вопрос 8.2.9.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

УКАЗАТЕЛЬ ОБОЗНАЧЕНИЙ

$\wedge$	конъюнкция 5
$\vee$	дизъюнкция 5
$\neg$	отрицание 5
$\Rightarrow$	импликация 5
$\Leftrightarrow$	эквиваленция 5
$\forall$	квантор общности 5
$\exists$	квантор существования 5
$\exists!$	квантор существования и единственности 5
$a \in A$	a — элемент множества A 5
$=$	равно 6
$\rightleftarrows$	равно по определению 6
$\varnothing$	пустое множество 6
$A \subset B$	множество A — подмножество множества B 6
$A \cup B$	объединение множеств A и B 6
$\bigcup_{\mu \in M} A_\mu$	объединение всех множеств A_μ таких, что $\mu \in M$ 6
$A \cap B$	пересечение множеств A и B 6
$\bigcap_{\mu \in M} A_\mu$	пересечение всех множеств A_μ таких, что $\mu \in M$ 6
$A \setminus B$	разность множеств A и B 6
$\{a\}$	множество, состоящее из одного элемента a 6
$\{a, b, c\}$	множество, состоящее из элементов a, b и c 6
$\{x\|\ldots\}$	множество, содержащее те и только те элементы x, которые обладают свойством... 6
$\langle a, b\rangle$	пара элементов a и b 9
$\langle a, b, c\rangle$	тройка (кортеж) из элементов a, b и c 9
$A \times B$	произведение множеств A и B 10
$A \times B \times C$	произведение множеств A, B и C 10
A^0, A^1, A^2, A^3	нулевая, первая, вторая и третья степени множества A 10
$\omega a_1 \ldots a_n$	множество всех x таких, что для кортежа $\langle a_1 \ldots a_n, x\rangle$ выполняется $(n+1)$-членное отношение ω 11
$a \omega b$	для элементов a и b выполняется отношение ω, если ω — бинарное отношение 11
$a \omega b$	множество всех x таких, что для кортежа $\langle a, b, x\rangle$ выполняется отношение ω, если ω—тернарное отношение 11
$\frac{b}{a}$	частное элементов b и a 14
$b - a$	разность элементов b и a 14
$-a$	противоположный элементу a элемент 15

a^{-1}	обратный элементу a элемент 15
ω^{-1}	отношение, обратное отношению ω 16
ωa, $\omega\,(a)$	множество всех образов элемента a в бинарном отношении ω 16
$\omega^{-1}\,a$	множество всех прообразов элемента a в бинарном отношении ω 16
ωA, $\omega\,(A)$	множество всех образов всех элементов из множества A в бинарном отношении ω 16
$\omega\colon A \to B$	ω — функция из A в B 16
$\omega\colon a \mapsto b$	b — образ элемента a, a — прообраз элемента b в однозначном отображении ω 16
B^A	множество всех функций из A в B 16
$(a)_m$	класс целых чисел, сравнимых с a по модулю m 17
$\omega\colon A \cong B$	ω — взаимно-однозначное отображение множества A на множество B 17
$A \cong B$	множества A и B равномощны 17
$\overline{A}$	кардинальное число множества A 19
$\langle A; \{\rho_\beta \mid \beta \in B\}\rangle$	алгебраическая система, состоящая из множества A и множества отношений $\{\rho_\beta \mid \beta \in B\}$ в нем 21
$\lvert f(x)\rvert_x = \alpha$	значение многочлена $f(x)$ при значении неизвестного x, равном элементу α 29
$\langle A; +, \theta; \mathbf{P}\rangle$	векторное пространство над полем $\mathbf{P}$ 31
$\langle A; +, \cdot, \theta; \mathbf{P}\rangle$	линейная алгебра над полем $\mathbf{P}$ 33
$f\colon \mathbf{A} \cong \mathbf{B}$	f—изоморфное отображение системы $\mathbf{A}$ на систему $\mathbf{B}$ 35
$\mathbf{A} \cong \mathbf{B}$	системы $\mathbf{A}$ и $\mathbf{B}$ изоморфны 35
$\sim$	отношение эквивалентности 38
ωx, $(x)_\omega$, $\overline{x}$	класс эквивалентности элемента x относительно отношения ω 38
A/ω	фактормножество множества A относительно отношения эквивалентности ω в нем 38
N	множество натуральных чисел, натуральный ряд 52
$A + B$	множество всех натуральных чисел, каждое из которых есть сумма слагаемых, первого из A и второго из B 52
$A \cdot B$	множество всех натуральных чисел, каждое из которых есть произведение сомножителей, первого из A и второго из B 52
2, 3, 4, 5, 6, 7, 8, 9	натуральные числа 56
$>$, $<$, $\geqslant$, $\leqslant$	отношения «больше», «меньше», «больше или равно», «меньше или равно» в N 57
$a > b > c$	a больше b и b больше c 57
$[a, b]$	отрезок натурального ряда с концами a и b 57
N_0	расширенный ряд натуральных чисел 62
$\mathfrak{a}_0$	мощность счетного множества 62
$\{a_n\}_{n=1}^{k}$	конечная последовательность 63
$\{a_n\}_{n=1}^{\infty}$	бесконечная последовательность 63

$\sum_{x=1}^{k} a_x$	сумма k первых членов последовательности 64
$k * a$	k-кратное элемента a 64
$a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_k}}}$	цепная дробь последовательности $\{a_x\}_{x=0}^{k}$ 67
$a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n + \ddots}}}$	цепная дробь последовательности $\{a_x\}_{x=0}^{\infty}$ 67
$[a_0, \ldots, a_n]$	подходящая дробь порядка n последовательности $\{a_x\}_{x=0}^{\omega}$ 68
$\mathbf{A}[x]$	кольцо, полученное путем присоединения к кольцу **A** элемента x 76
$\mathbf{A}[x, y]$	кольцо, полученное путем присоединения к кольцу **A** элементов x и y 76
$\mathbf{A}(x)$ $(A(x, y))$	тело, полученное путем присоединения к телу **A** элемента x (элементов x и y) 76
$\mathbf{P}[a]$ $(\mathbf{P}[a, b])$	линейная алгебра, полученная путем присоединения к полю **P** элемента a (элементов a и b) 76
$\succ$	отношение порядка 78
PM	множество всех подмножеств множества M 79
P_a	интервал, отделенный элементом a 80
$\bar{\mathbf{A}}$	порядковое число вполне упорядоченного множества **A** 83
$W(\alpha)$	множество порядковых чисел, строго меньших порядкового числа α 83
$\Omega(\mathfrak{a})$	множество кардинальных чисел, строго меньших кардинального числа $\mathfrak{a}$ 84
$\lvert a \rvert$	абсолютная величина элемента a 91
A^+	положительная часть кольца $\langle A; +, \cdot, 0\rangle$ 92
Z	множество целых чисел 95
$\langle Z; +, \cdot, 0, N, \oplus, \odot\rangle$	система целых чисел 95
$\langle Z; +, \cdot, 0\rangle$	кольцо целых чисел 96
$\langle Z; +, 0\rangle$	аддитивная группа целых чисел 96
$\langle Z; \cdot\rangle$	мультипликативная полугруппа целых чисел 96
$[\alpha]$	целая часть элемента α архимедовски линейно упорядоченного поля 98
Q	множество рациональных чисел 103
$\langle Q; +, \cdot, 0, Z, \oplus, \odot\rangle$	система рациональных чисел 103
$\langle Q; +, 0\rangle$	аддитивная группа рациональных чисел 103
$\langle Q; \cdot\rangle$	мультипликативная полугруппа рациональных чисел 103

$\langle Q \setminus \{0\}; \cdot \rangle$	мультипликативная группа рациональных чисел 103
$\langle \mathbf{A}; \mathbf{P}; \nu \rangle$	нормированное поле 110
ν_p	p-адическая норма 111
$\{a_n\}_n$	последовательность $\{a_n\}_{n=1}^{\infty}$ 112
$\{a_n\}_n \xrightarrow[\nu]{} a\ (\mathbf{P}_1)$	последовательность $\{a_n\}_n$ сходится к элементу a по норме ν относительно поля $\mathbf{P}_1$ 113
$\{a_n\}_n \underset{\nu}{\sim} \{b_n\}_n\ (\mathbf{P}_1)$	последовательности $\{a_n\}_n$ и $\{b_n\}_n$ эквивалентны по норме ν относительно поля $\mathbf{P}_1$ 113
$\lim\limits_{n\to\infty} a_n$	предел последовательности архимедовски упорядоченного поля 114
$\alpha^{\frac{1}{k}}$	корень k-й степени из положительного числа 130
$\alpha^{\frac{c}{n}}$	рациональная степень 131
α^{β}	вещественная степень 133
$\sum\limits_{x=0}^{\infty} a_x$	ряд, сумма ряда 133
$\{a_n\}_n + \{b_n\}_n$	сумма последовательностей $\{a_n\}_n$ и $\{b_n\}_n$ 137
$\{a_n\}_n \cdot \{b_n\}_n$	произведение последовательностей $\{a_n\}_n$ и $\{b_n\}_n$ 137
$\overline{\{a_n\}_n}$	класс эквивалентных последовательностей 137
$\delta_n(x)$	подходящая функция 143
$P_n,\ Q_n$	числители и знаменатели подходящих дробей 144
α_n	полное частное 147
$[a_0; a_1, \ldots, a_n, \ldots]$	значение бесконечной цепной дроби последовательности $\{a_x\}_{x=0}^{\infty}$ 147
(α)	дробная доля числа α 183

ЛИТЕРАТУРА

1. Биркгоф Г. Теория структур. М., «Иностранная литература», 1952.
2. Боревич З. И., Шафаревич И. Р. Теория чисел, изд. 2. М., «Наука», 1972.
3. Бурбаки Н. Алгебра. Алгебраические структуры, линейная и полилинейная алгебра. М., Физматгиз, 1962.
4. Бурбаки Н. Теория множеств. М., «Мир», 1965.
5. Бухштаб А. А. Теория чисел, изд. 2. М., «Просвещение», 1966.
6. Ван-дер-Варден Б. Л. Современная алгебра. Ч. 1. М., ГТТИ, 1947.
7. Ван-Хао и Мак-Нотон Р. Аксиоматические системы теории множеств. М., «Иностранная литература», 1963.
8. Гейтинг А. Интуиционизм. М., «Мир», 1965.
9. Гонин Е. Г. Теоретическая арифметика. М., Учпедгиз, 1959.
10. Гудстейн Р. Л. Математическая логика. М., «Иностранная литература», 1961.
11. Жегалкин И. Трансфинитные числа. М., 1907.
12. Клини С. К. Введение в математику. М., «Иностранная литература», 1957.
13. Кокорин А. И., Копытов В. М. Линейно упорядоченные группы. М., «Наука», 1972.
14. Коэн П. Д. Теория множеств и континуум — гипотеза. М., «Мир», 1969.
15. Куратовский К., Мостовский А. Теория множеств. М., «Мир», 1970.
16. Курош А. Г. Курс высшей алгебры, изд. 10. М., «Наука», 1971.
17. Курош А. Г. Лекции по общей алгебре, изд. 2. М., «Наука», 1973.
18. Курош А. Г. Теория групп, изд. 3. М., «Наука», 1972.
19. Кушнер Б. А. Лекции по конструктивному математическому анализу. М., «Наука», 1973.
20. Ленг С. Введение в теорию диофантовых приближений. М., «Мир», 1970.
21. Мальцев А. И. Алгебраические системы. М., «Наука», 1970.
22. Мальцев А. И. Основы линейной алгебры, изд. 3. М., «Наука», 1970.
23. Марков А. А. О логике конструктивной математики. М., «Знание», 1972.
24. Марков А. А. Избранные труды. М., ГТТИ, 1948.

25. Мендельсон Э. Введение в математическую логику. М., «Наука», 1971.

26. Нагель Э., Ньюмен Дж. Р. Теорема Геделя. М., «Знание», 1970.

27. Новиков П. С. Элементы математической логики, изд. 2. М., «Наука», 1973.

28. Расева Е., Сикорский Р. Математика, метаматематики. М., «Наука», 1972.

29. Столл Р. Р. Множества. Логика. Аксиоматические теории. М., «Просвещение», 1968.

30. Фор Р., Кофман А., Дени-Папен М. Современная математика. М., «Мир», 1966.

31. Френкель А., Бар-Хиллел И. Основания теории множеств. М., «Мир», 1966.

32. Фукс Л. Частично упорядоченные алгебраические системы. М., «Мир», 1965.

33. Хинчин А. Я. Цепные дроби, изд. 3. М., Физматгиз, 1961.

34. Черч А. Введение в математическую логику. Т. 1. М., «Иностранная литература», 1960.

35. Энциклопедия элементарной математики. Кн. 1. М., ГТТИ, 1951.

36. Проблемы Гильберта. — Сб. под ред. П. С. Александрова. М., «Наука», 1969.

37. Генцен Г. Новое изложение доказательства непротиворечивости для чистой теории чисел. — Сб.: Математическая теория логического вывода. М., «Наука», 1967, с. 154—190.

38. Линник Ю. В. Кватернионы и числа Кэли. Т. 4, вып. 5 (33). М., «Успехи математических наук», 1949, с. 49—98.

39. Линник Ю. В. и Малышев А. В. Приложения арифметики кватернионов к теории тернарных квадратичных форм и к разложению чисел на кубы. Т. 8, вып. 5 (57). М., «Успехи математических наук», 1953, с. 3—71.

40. Молодший В. Н. К вопросу об истолковании роли аксиомы индукции в арифметике натуральных чисел. — «Математика в школе», 1954, № 3, с. 1—5.

СОДЕРЖАНИЕ

Василий Ильич Нечаев

ЧИСЛОВЫЕ СИСТЕМЫ

Редактор *В. С. Капустина*
Художник переплета *Е. Т. Яковлев*
Художественный редактор *Е. Н. Карасик*
Технический редактор *Л. Я. Медведев*
Корректор *Н. И. Котельникова*

Сдано в набор 23/XII 1974 г. Подписано к печати 22/VII 1975 г. 60×90¹/₁₆. Бумага типогр. № 3. Печ. л. 12,5. Уч.-изд. л. 10,71. Тираж 75 тыс. экз.

Ордена Трудового Красного Знамени издательство «Просвещение» Государственного комитета Совета Министров РСФСР по делам издательств, полиграфии и книжной торговли. Москва, 3-й проезд Марьиной рощи, 41.

Головное предприятие республиканского производственного объединения «Полиграфкнига» Госкомиздата УССР, Киев, ул. Довженко, 3.
Зак. 4—3071.

Цена без переплета 30 коп., переплет 10 коп.