УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
«Брестский государственный университет имени А.С. Пушкина»
Кафедра алгебры, геометрии и математического моделирования

О.В. Матысик
Д.В. Грицук

ЧИСЛОВЫЕ СИСТЕМЫ

Курс лекций для студентов специальности
1-02 05 01 «Математика и информатика»
физико-математического факультета

Брест, 2015

Авторы:

Матысик Олег Викторович — заведующий кафедрой прикладной математики и технологий программирования Учреждения образования «Брестский государственный университет имени А.С. Пушкина», кандидат физико-математических наук, доцент

Грицук Дмитрий Владимирович — старший преподаватель кафедры алгебры, геометрии и математического моделирования Учреждения образования «Брестский государственный университет имени А.С. Пушкина», кандидат физико-математических наук

Редактор:

Грицук Дмитрий Владимирович — старший преподаватель кафедры алгебры, геометрии и математического моделирования Учреждения образования «Брестский государственный университет имени А.С. Пушкина», кандидат физико-математических наук

Рецензенты:

Парфомук Сергей Иванович — заведующий кафедрой информатики иприкладной математики Учреждения образования «Брестский государственный технический университет», кандидат технических, доцент

Будько Александр Евгеньевич — проректор по научной работе и экономике Учреждения образования «Брестский государственный университет имени А.С. Пушкина», кандидат физико-математических наук, доцент

Курс лекций написан в соответствии с действующей типовой программой по дисциплине «Числовые системы» и ставит своей целью облегчить самостоятельную работу студентов с теоретическим материалом при подготовке к лекциям, практическим занятиям и к экзамену.

Предназначен для студентов специальности 1-02 05 01 «Математика и информатика» физико-математического факультета.

СОДЕРЖАНИЕ

Кафедра АГиММ

Кафедра АГиММ

ТЕСТ

Предисловие

Настоящий курс лекций предназначен для студентов отделений 1-02 05 01 «Математика и информатика» физико-математического факультета. Он написан в соответствии с действующей типовой программой по курсу «Числовые системы», утверждённой учебно-методическим объединением высших учебных заведений Республики Беларусь. В курсе лекций излагается теоретический материал, содержащий вопросы аксиоматического построения теорий натуральных, целых, рациональных, действительных и комплексных чисел. Электронное пособие ставит своей целью облегчить самостоятельную работу студентов с теоретическим материалом при подготовке к лекциям, практическим занятиям и к экзамену.

Авторы

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

РАЗДЕЛ 1
АКСИОМАТИЧЕСКИЕ ТЕОРИИ

1.1 Аксиоматическая теория

Определение 1.1. *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:

$$w_1, ..., w_k;\ w_i \in W;\ i = 1, ..., k;\ k \geq 1 \tag{1.1}$$

такая, что выполняются следующие условия:

1) каждое высказывание 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 (1.1) с указанными выше свойствами называется *доказательством* или ıвыводом 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.

1.2 Схема построения неформальной аксиоматической теории

При построении аксиоматической теории обычно исходят из некоторой достаточно развитой интуитивной теории и предполагают известной интуитивную систему классической логики.

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 дан-

ная теория. Аналогичное замечание можно сделать и относительно терминов, используемых в данной теории.

Определение 1.2. *Упорядоченную пару множеств* $\langle S_0, T_0 \rangle$ *называют* формулировкой *данной аксиоматической теории.*

1.3 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. Пусть 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.

Тогда такую систему объектов второй теории называют *интерпретацией* данной теории.

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

1.4 Свойства аксиоматических теорий

Аксиоматическую теорию называют *непротиворечивой*, если для любого высказываниям 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. Исчисление высказываний непротиворечиво.

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

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

У нас нет средств для решения проблемы полноты содержательной аксиоматической теории. Да таких средств и не существует, поскольку в содержательной аксиоматической теорий 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 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.

Если непротиворечива теория, формулировкой которой служит пара $\langle S_0, T_0' \rangle$, где $T_0' \Leftrightarrow (T_0 \setminus \{A_1\}) \cup \{\overline{A}_1\}$, 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.

РАЗДЕЛ 2
СИСТЕМА НАТУРАЛЬНЫХ ЧИСЕЛ

2.1 Аксиомы множества натуральных чисел

Рассмотрим множество N натуральных чисел как множество элементов (символов). Один из элементов множества обозначим символом 1(единица).

Будем считать, что множество N обладает следующими свойствами:

A_1. Каждому $a \in N$ соответствует единственное натуральное число, которое назовем *следующим за* a числом и обозначим a', т.е.

$$(\forall a, b \in N)\ a = b \Rightarrow a' = b'.$$

A_2. Существует натуральное число 1, которое не следует ни за каким натуральным числом, т.е. $(\forall a \in N)\ a' \neq 1$.

A_3. Любое натуральное число следует не более чем за одним натуральным числом, т.е.

$$(\forall a, b \in N)\ a' = b' \Rightarrow a = b.$$

A_4. **(Аксиома индукции)** Если множество M натуральных чисел содержит единицу и вместе с каждым, содержащимся в нем числом a содержит и следующее за ним число a', то $M = N$, т.е.

$$(1 \in M) \wedge ((\forall a \in N)\ a \in M \Rightarrow a' \in M) \Rightarrow M = N.$$

Замечание. Аксиома 4 лежит в основе метода математической индукции.

A_5. $(\forall a \in N)\ a + 1 = a'$.

A_6. $(\forall a, b \in N)\ a + b' = (a + b)'$.

A_7. $(\forall a \in N)\ a \cdot 1 = a$.

A_8. $(\forall a, b \in N)\ a \cdot b' = a \cdot b + a$.

Аксиомы A_1–A_8 были впервые сформулированы в 1801 году итальянским учёным Пеано и получили название *аксиом Пеано*.

Рассмотрим некоторые теоремы, вытекающие непосредственно из аксиом Пеано.

Теорема 2.1. *Если два натуральных числа, следующие за двумя данными натуральными числами различны, то и данные числа различны, т.е.*

$$(\forall a, b \in N)\ a' \neq b' \Rightarrow a \neq b.$$

Доказательство. Теорема равносильна аксиоме A_1. ⊠

Теорема 2.2. *Если два натуральных числа различны, то и следующие за ними числа различны, т.е.*

$$(\forall a, b \in N)\ a \neq b \Rightarrow a' \neq b'.$$

Доказательство. Теорема справедлива, так как она контрпозиционна аксиоме A_3. ⊠

Теорема 2.3. *Ни одно натуральное число не совпадает со следующим за ним натуральным числом, т.е.*

$$(\forall a \in N)\ a' \neq a.$$

Доказательство. Для доказательства воспользуемся аксиомой индукции. Пусть M множество натуральных чисел, каждое из которых не равно следующему за ним натуральному числу, т.е.

$$M = \{a \in N |\ a' \neq a\}.$$

Заметим, что $1 \in M$, так как $1' \neq 1$ по аксиоме A_2.

Пусть $a \in M$. Тогда $a' \neq a$ и по теореме 2.2 имеем $(a')' \neq a'$. Следовательно, $a' \in M$.

Таким образом множество M удовлетворяет всем условиям аксиомы индукции A_4. А это значает, что $M = N$, т.е. для любого $a \in N$ имеем, что $a' \neq a$. ⊠

Теорема 2.4. *Любое натуральное число, отличное от 1, следует только за одним натуральным числом.*

Доказательство. Рассмотрим множество M, которое содержит 1, а также всякое натуральное число, которое следует хотя бы за одним натуральным числом. Пусть $a \in M$, тогда и $a' \in M$, как число, следующее за a. Тогда по аксиоме индукции $M = N$, т.е. всякое натуральное число, отличное от 1, следует хотя бы за одним натуральным числом. Учитывая аксиому A_1, имеем единственность такого числа. ⊠

Теорема 2.5. **(О законности доказательства индукции)** *Пусть некоторое утверждение $T(n)$ о натуральных числах верно при $n = 1$, и в предположении, что $T(a)$ верно, доказано $T(a')$, тогда для любого $n \in N$ верно $T(n)$.*

Доказательство. Построим множество, состоящее из натуральных чисел, при которых истинно высказывание $T(n)$:

$$M = \{m \in N |\ T(m) \equiv 1\}.$$

Так как по условию $T(1) \equiv 1$, $1 \in M$. А так как $T(a) \equiv 1$ и $T(a') \equiv 1$, то $a \in M$ и $a' \in M$. Значит, если натуральное число $a \in M$, то и $a' \in M$. Тогда по аксиоме индукции $M = N$. $\boxtimes$

2.2 Сложение натуральных чисел

Определим операцию сложения на множестве натуральных чисел исходя только из аксиом Пеано.

Определение 2.1. *Бинарной алгебраической операцией на некотором множестве M называется отображение прямого произведения $M \times M$ в M.*

Определение 2.2. *Бинарной алгебраической операцией сложения на множестве N называется отображение $+ : N^2 \to N$, ставящее в соответствие любой паре натуральных чисел $(a, b) \in N^2$ натуральное число $(a + b) \in N$, и удовлетворяющее аксиомам A_5 и A_6 системы Пеано, т.е.*

1) $(\forall a \in N)\ a + 1 = a'$;
2) $(\forall a, b \in N)\ a + b' = (a + b)'$.

Теорема 2.6. *Алгебраическая операция сложения на N, удовлетворяющая аксиомам A_5 и A_6 системы Пеано, существует и единственна.*

Доказательство. Докажем сначала единственность операции сложения на множестве N.

Предположим, что $\langle + \rangle$ и $\langle \oplus \rangle$ — две операции сложения, удовлетворяющие аксиомам A_5 и A_6: $\langle + \rangle$ и $\langle \oplus \rangle$. Докажем, что

$$(\forall a, b \in N)\ a + b = a \oplus b.$$

Пусть M — это множество натуральных чисел b, для которых верно $a + b = a \oplus b$ при любом натуральном числе a, т.е.

$$M = \{b \in N |\ (\forall a \in N)\ a + b = a \oplus b\}$$

Так как для обеих операций выполняется аксиома A_5, то $a + 1 = a'$, $a \oplus 1 = a'$. Поэтому $1 \in M$.

Предположим, что $k \in M$, т.е. $a + k = a \oplus k$. Докажем, что в этом случае и $k' \in M$.

Для операции $\langle + \rangle$ выполняется аксиома A_6, поэтому $a + k' = (a + k)'$. Так как по предположению индукции $a + k = a \oplus k$, то по аксиоме A_1 $(a + k)' = (a \oplus k)'$. Но для операции $\langle \oplus \rangle$ тоже выполняется аксиома A_6, поэтому $(a \oplus k)' = a + k'$. Следовательно, $k' \in M$. По принципу математической индукции $M = N$. Единственность доказана.

Чтобы доказать существование операции $\langle + \rangle$, сначала докажем, что она существует для пар вида $(1, b)$. Для того, чтобы доказать существование $1 + b$, введём дополнительную математическую конструкцию $1 + b = b'$ (введём новую аксиому, но назовём её конструкцией).

I. $\underline{1 + b = b'}$.

Воспользуемся аксиомой индукции. Пусть

$$M = \{b \in N |\ \exists (1 + b)\}.$$

По аксиоме A_5 $1 + 1 = 1'$, поэтому $1 \in M$.

Предположим, что $k \in M$, т.е. $1+k = k'$ верно. Покажем, что $k' \in M$. Применяем последовательно аксиому A_6 и конструкцию I:

$$1 + k' = (1 + k)' = (k')'.$$

Следовательно, если существует сумма $1 + k$, то существует и сумма $1 + k'$, так как сумма $1 + k'$, полученная по конструкции, совпадает с суммой $(1 + k)'$, полученной по системе аксиом. По аксиоме индукции $M = N$, т.е суммма $1 + b$ сущесвтует при любом $b \in N$.

II. $a' + b = (a + b)'$. По первому шагу мы доказали, что существует сумма $a + b$, при $a = 1$.

Построим множество

$$M = \{a \in N |\ (\forall b \in N)\ \exists (k + b)\}.$$

По первому шагу имеем, что $1 \in M$. Допустим, что $k \in M$, т.е. существует сумма $k + b$, где $k + 1 = k'$, $k + b' = (k + b)'$.

Докажем, что $k' \in M$, т.е. что существует сумма $k' + b$ такая, что $k' + 1 = (k')'$ и $k' + b' = (k' + b)'$. По аксиоме A_5 имеем $k' + 1 = (k')'$, а $k' + b' = (k + b')'$ по конструкции II. Но для k сумма $k + b$ существует при любом натуральном числе b, в том числе и для b'. По аксиоме A_6 имеем $k + (b')' = (k + b')'$. Применяя конструкцию II, а затем аксиому A_6 получим $(k + b')' = (k' + b)'$.

Следовательно, $k' + b$ существует. Поэтому $k' \in M$. Тогда по аксиоме A_4 $M = N$. $\boxtimes$

Пользуясь определением 2.2, можно составить таблицу сложения натуральных чисел:

$1+1=1'=2$ (2 — обозначение числа $1'$),

$2+1=2'=3$,

$3+1=3'=4$,

$2+2=2+1'=(2+1)'=3'=4$,

$3+2=3+1'=(3+1)'=4'=5$ и т.д.

Замечание. Символы 2, 3, 4, 5, ... являются обозначениями соответствующих чисел $1'$, $2'$, $3'$, $4'$, ...

2.2.1 Свойства сложения на множестве натуральных чисел

Теорема 2.7. *Сложение натуральных чисел ассоциативно, т.е.*

$$(\forall a,b,c\in N)\ (a+b)+c=a+(b+c). \tag{2.1}$$

Доказательство. Пусть M — подмножество натуральных чисел, для которых выполняется равенство (2.1) при любых $a,b\in N$.

Заметим, что $1\in M$, так как

$$(a+b)+1 \overset{df\,2.2}{=} (a+b)' \overset{df\,2.2}{=} a+b'=a+(b+1).$$

Пусть натуральное число $k\in M$, т.е. верно

$$(a+b)+k=a+(b+k) \tag{2.2}$$

для любых $a, b \in N$ и фиксированного $k \in N$.

Докажем, что $k' \in M$.

Рассуждая следующим образом, получим

$$(a+b)+k' \overset{A_6}{=} ((a+b)+k)' \overset{(2.2)}{=} (a+(b+k))' \overset{A_6}{=} a+(b+c)' \overset{A_6}{=} a+(b+c').$$

Таким образом, доказано, что выполняются все условия аксиомы индукции. Поэтому $M = N$, т.е. равенство (2.1) верно для любых натуральных чисел a, b и c. $\boxtimes$

Теорема 2.8. *Сложение натуральных чисел коммутативно, т.е.*

$$(\forall a, b \in N)\ a+b = b+a. \tag{2.3}$$

Доказательство. Предварительно докажем, что

$$(\forall a \in N)\ a+1 = 1+a. \tag{2.4}$$

Пусть M — множество натуральных чисел, для каждого из которых верно равенство (2.4). Очевидно, что $1 \in M$.

Предположим, что $a \in M$, т.е. для некоторого фиксированного a верно равенство (2.4).

Докажем, что $a' \in M$, т.е. верно равенство $a'+1 = 1+a'$. Действительно,

$$a'+1 \overset{A_5}{=} (a+1)+1 \overset{(2.4)}{=} (1+a)+1 \overset{\text{T.2.7}}{=} 1+(a+1) \overset{A_5}{=} 1+a'.$$

Таким образом, по аксиоме индукции $M = N$, т.е. равенство (2.4) верно для любого $a \in N$.

Докажем равенство (2.3) для любых $a, b \in N$. Рассмотрим множество T таких натуральных чисел b, для которых верно равенство (2.3) при любом $a \in N$.

В силу доказанного выше $1 \in T$. Пусть $b \in T$, т.е. верно равенство (2.3) при фиксированном $b \in N$ и любом натуральном числе a. Докажем, что и $b' \in T$.

Действительно:

$$a + b' \overset{df2.2}{=} (a + b)' \overset{\text{т.к. } b \in T}{=} (b + a)' \overset{df2.2}{=} b + a' = b + (a + 1) \overset{(2.4)}{=}$$

$$= b + (1 + a) \overset{\text{Т.2.7}}{=} (b + 1) + a \overset{A_5}{=} b' + a.$$

Следовательно, по аксиоме A_4 равенство (2.3) верно для любых натуральных чисел a и b. $\boxtimes$

2.3 Умножение натуральных чисел

Определение 2.3. *Бинарной алгебраической операцией умножения на множестве N называется отображение $\cdot : N^2 \to N$, ставящее в соответствие каждой паре $(a, b) \in N^2$ натуральное число $a \cdot b \in N$, и удовлетворяющее аксиомам A_7 и A_8 системы Пеано, т.е.*

1) $(\forall a \in N)\ a \cdot 1 = a;$

2) $(\forall a, b \in N)\ a \cdot b' = ab + a.$

Замечание. Далее вместо $m \cdot n$ будем писать mn.

Теорема 2.9. *Алгебраическая операция умножения на N, удовлетворяющая аксиомам A_7 и A_8 системы Пеано, существует и единственна.*

Доказательство. Аналогично как для сложения.

Составим таблицу умножения натуральных чисел:

$1 \cdot 1 = 1, \quad 2 \cdot 2 = 2 \cdot 1' = 2 \cdot 1 + 2 = 2 + 2 = 4,$

$2 \cdot 1 = 2, \quad 3 \cdot 2 = 3 \cdot 1' = 3 \cdot 1 + 3 = 3 + 3 = 6$ и т.д.

Замечание. При построении таблицы умножения использованы условия 1-2 определения 2.3 и таблица сложения натуральных чисел.

2.3.1 Свойства умножения на множестве натуральных чисел

Теорема 2.10. *Умножение на множестве натуральных чисел N дистрибутивно справа относительно сложения, т.е.*

$$(\forall a, b, \in N)\ (a+b)c = ac + bc. \tag{2.5}$$

Доказательство. Зафиксируем натуральные числа a, b и обозначим через M подмножество натуральных чисел, для которых выполняется равенство (2.5):

$$M = \{c \in N | (a+b)c = ac + bc\}.$$

Так как $(a+b)\cdot 1 = a+b = a\cdot 1 + b\cdot 1$, то $1 \in M$.

Предположим, что некоторое натуральное число c принадлежит множеству M, т.е. для некоторого $c \in N$ справедливо

$$(a+b)c = ac + bc. \tag{2.6}$$

Покажем, что c' также принадлежит множеству M. Для этого рассмотрим $(a+b)c' \overset{df}{=} (a+b)c + (a+b) \overset{(2.6)}{=} ac + bc + a + b$. Применяя теорему 2.8 и определение 2.3 получим $ac + bc + a + b = ac' + bc'$. Следовательно, $c' \in M$. Тогда по аксиоме индукции A_4 равенство (2.5) выполняется для любых $a, b, c \in N$. $\boxtimes$

Теорема 2.11. *Умножение на множестве N коммутативно, т.е.*

$$(\forall a, b \in N)\ ab = ba. \tag{2.7}$$

Доказательство. Докажем справедливость (2.7) при $b = 1$. Рассмотрим подмножество $M = \{a \in N |\ a \cdot 1 = 1 \cdot a\}$. Очевидно, что $1 \in M$. Пусть некоторое натуральное число a принадлежит множеству M. Докажем, что $a' \in M$. Рассмотрим

$$a' \cdot 1 \overset{A_7}{=} (a+1) \cdot 1 \overset{\text{T.2.10}}{=} a \cdot 1 + 1 = 1 \cdot a + 1 = 1 \cdot a' \overset{A_7}{=} a'.$$

Следовательно, $a' \in M$, и по аксиоме индукции $M = N$.

Теперь докажем, что (2.7) верно для любого натурального числа b. Рассмотрим множество T, состоящее из наутарльных чисел b, для которых выполняется (2.7) при любом $a \in N$, т.е.

$$T = \{b \in N |\ (\forall a \in N)\ ab = ba\}.$$

Из доказанного выше следует, что $1 \in T$. Пусть $b \in T$, т.е. $ab = ba$. Рассмотрим

$$ab' \overset{A_8}{=} ab + a = ba + a \overset{\text{T.2.10}}{=} (b+1)a = b'a.$$

Поэтому $b' \in T$. По аксиоме индукции $T = N$. ⊠

Теорема 2.12. *Умножение на N дистрибутивно слева относительно сложения, т.е.*

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

Доказательсвто. Для любых натуральных чисел a, b и c по теореме 2.11 имеем $c(a+b) = (a+b)c$. Тогда $(a+b)c = a \cdot c + bc$ по теореме 2.10. Так как умножение на N коммутативно, то $ac + bc = ca + cb$. $\boxtimes$

Теорема 2.13. *Умножение на N ассоциативно, т.е.*

$$(\forall a, b, \in N)\ (ab)c = a(bc).$$

Доказательство. Рассмотрим множество

$$M = \{c \in N |\ (\forall a, b \in N)\ (ab)c = a(bc)\}.$$

Так как $(ab) \cdot 1 \overset{A_7}{=} ab \overset{A_7}{=} a(b \cdot 1)$, то $1 \in M$.

Пусть некоторое натуральное число $c \in M$, т.е. выполнятеся равенство $(ab)c = a(bc)$. Рассмотрим

$$(ab)c' \overset{A_8}{=} (ab)c + ab = a(bc) + ab \overset{\text{Т.2.12}}{=} a(bc + b) \overset{A_8}{=} a(bc').$$

Следовательно, $c' \in M$. Поэтому по аксиоме индукции $M = N$. $\boxtimes$

2.4 Порядок во множестве натуральных чисел

Теорема 2.14. *Для любого натурального числа a, $a \neq 1$ существует натуральное число n, такое что $a = 1 + n$, т.е.*

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

Доказательство. Рассмотрим множество

$$M = \{1\} \cup \{a \in N |\ (\exists n \in N)\ a = 1 + n\}.$$

Очевидно, что $1 \in M$. Если $a \in N$, то $a' = a + 1 = 1 + a \in M$. По аксиоме индукции $M = N$. ⊠

Теорема 2.15. *Сумма натуральных чисел не равна ни одному из слагаемых этой суммы, т.е.*

$$(\forall a, b \in N)\ a + b \neq b. \tag{2.8}$$

Доказательство Рассмотрим M_b — подмножество натуральных чисел N, для которого выполняется условие (2.10) при любом $a \in N$. Очевидно, что $1 \in M_b$, так как для любого $a \in N$ по аксиоме A_2 имеем, что $a + 1 \neq 1$. Пусть некоторое натуральное число b принадлежит множеству M_b т.е. (2.10) верно для любого $a \in N$ и фиксированного b. Докажем, что $b' \in M_b$.

Действительно, так как $a + b \neq b$, $a \in N$, $b \in N$, b — фиксированное, то по теореме 2.2 $(a + b)' \neq b'$, но $(a + b)' = a + b'$. Следовательно, $a + b' \neq b'$. Таким образом, $b' \in M_b$. По аксиоме индукции $M = N$. ⊠

Определение 2.4. *Будем говорить, что натуральное число a больше натурального числа b, и записывать $a > b$, если существует натуральное число n такое, что a, b, n связаны равенством $a = b + n$.*

Если b меньше a, то будем записывать $b < a$.

Если $a > b$ или $a = b$, то будем говорить, что «a не меньше b» ($a \geq b$), если $a < b$ или $a = b$, то будем говорить, что «a не больше b» ($a \leq b$).

Теорема 2.16. **(Закон трихотомии для «>»)** *Для любых натуральных чисел a и b имеет место только один из трех случаев:*

1) $a = b$,
2) $a > b$,
3) $a < b$ $(b > a)$.

Доказательство. Покажем, что для любых натуральных чисел a и b невозможны одновременно два из трех указанных случаев.

Действительно, пусть для $a, b \in N$ имеют место случаи 1 и 2. Тогда по определению понятия «больше» 2.4 $a = b + n$, $n \in N$, учитывая первый пункт, получим равенство $b = b + n$, которое противоречит теореме 2.15. Отсюда следует, что случаи 1 и 2 несовместимы.

Аналогично доказывается, что несовместимы случаи 1 и 3.

Допустим, что совместимы 2) и 3), т.е. $a > b$ и $b > a$. Тогда по определению понятия «больше» 2.4 верны равенства $a = b + n$ и $b = a + k$, где $n, k \in N$. Подставив второе равенство в первое получим

$$a = (a + k) + n = a + (k + n) = a + m, \text{ где } m = k + n \in N.$$

Это равенство противоречит теореме 2.15.

Мы доказали, что для любых $a, b \in N$ не возможны одновременно два из трех указанных случаев.

Докажем, что для любых $a, b \in N$ имеет место только один из трех случаев.

Пусть M – множество таких натуральных чисел b, для которых имеет место только один из трех случаев при любом $a \in N$.

Покажем, что $1 \in M$, т.е. для 1 и любого $a \in N$ имеет место только один из трех случаев. Действительно, если $a = 1$, то имеет место случай 1. Если $a \neq 1$, то $a = c' = c + 1$ $(c \in N)$ и по определению понятия «больше» $a > 1$, т.е. для a и 1 имеет место случай 2.

Пусть натуральное число $b \in M$, т.е. для любого $a \in N$ и фиксированного b имеет место только один из трех случаев. Докажем, что $b' \in M$ т.е. для любого $a \in N$ и b' выполняется один из трех случаев:

$$1)\ a = b',\ 2)\ a > b',\ 3)\ a < b'.$$

Рассмотрим каждый из трех случаев для любого $a \in N$ и фиксированного $b \in M$.

1) Пусть $a = b$. Тогда по аксиоме A_1 имеем $b' = a' = a + 1$, т.е. $b' > a$ по определению понятия «больше» 2.4.

2) Пусть $a > b$. Тогда по определению 2.4 $a = b + n$, $n \in N$. Если $n = 1$, то $a = b + 1 = b'$ т.е. выполняется первый случай. Если $n \neq 1$, то

$n = c'$, где $c \in N$. Поэтому $a = b + c' = (b + c)' = (c + b)' = c + b' = b' + c$ и по определению 2.4 $a > b'$.

3) Пусть $b > a$. Тогда по определению понятия «больше» 2.4 $b = a + n$, где $n \in N$. По аксиоме A_6 имеем $b' = (a + n)' = a + n'$ $(b' \in N)$. Следовательно, по определению 2.4 $b' > a$, т.е. для b' и a выполняется случай 3.

Таким образом, показано, что если для любого $a \in N$ и фиксированного $b \in M$ выполняется один из трех случаев, то и для любого $a \in N$ и $b' \in M$ также выполняется один из трех случаев. А тогда по аксиоме математической индукции $M = N$, т.е. для любых $a, b \in N$ имеет место один из трех случаев. ☒

Теорема 2.17. (Транзитивность) *Для любых натуральных чисел $a, b, c \in N$, если $a > b$ и $b > c$, то $a > c$.*

Доказательство. Если $a > b$ и $b > c$, то по определению понятия «больше» 2.4 $a = b + n$ и $b = c + m$, где $m, n \in N$. Тогда

$$a = (c + m) + n = c + (m + n) = c + k, \text{ где } k = m + n \in N,$$

и по определению $a > c$. ☒

Следствие 2.1. $(\forall a, b, c \in N)\ a < b \wedge b < c \Rightarrow a < c$.

Теорема 2.18. *Отношение «меньше» («больше») на множестве натуральных чисел N является отношением строгого линейного порядка.*

Доказательство. Так как отношение $<$ на множестве N обладает свойствами антисимметричности, транзитивности и связности. $\boxtimes$

Таким образом, множество N является упорядоченным.

2.4.1 Свойства неравенств на N

Теорема 2.19. (Связность) $(\forall a, b \in N)\ a \neq b \Rightarrow a > b \vee b > a.$

Теорема 2.20. (Антирефлексивность) $(\forall a \in N)\ \rceil(a > a).$

Доказательство.Предположим обратное, т.е. предположим, что существет натуральное число $a \in N$ такое, что $a > a$. Тогда по определению понятия «больше» 2.4 существует натуральное число $n \in N$, что $a = a + n$. А это противоречит теореме 2.15. Поэтому предположение не верно. ⊠

Теорема 2.21. (Асимметричность) $(\forall a, b \in N)\ a > b \Rightarrow \rceil(b > a).$

Теорема 2.22. (Монотонность относительно сложения и умножения) 1. $(\forall a, b, c \in N)\ a > b \Rightarrow a + c > b + c.$

2. $(\forall a, b, c \in N)\ a > b \Rightarrow ac > bc.$

Теорема 2.23. *Любое натуральное число — положительно, т.е.*

$$(\forall a, b \in N)\ a + b > a.$$

Теорема 2.24. (Правила сложения и умножения неравенств одного смысла)

1. *Если* $a \geq b \wedge c \geq d$, *то* $a + c \geq b + d$ *и* $ac \geq bd.$
2. *Если* $a \leq b \wedge c \leq d$, *то* $a + c \leq b + d$ *и* $ac \leq bd.$

Замечание. Теоремы 2.19–2.24 легко выводятся из теорем 2.15 и 2.16, а также из свойств сложения и умножения.

Теорема 2.25. *Среди всех натуральных чисел 1 является наименьшим, т.е.* $(\forall a \in N)\ 1 \leq a$.

Доказательство. Так как $a \neq 1$, то по аксиоме A_3 из системы аксиом Пеано, натуральное число a следует только за одним натуральным числом, т.е. $a = c' = c+1 = 1+c$. Следовательно, $a > 1$. Отсюда следует, что N ограничено снизу. ⊠

Теорема 2.26. **(Дискретность)** *Для любого натурального числа a не существует такого $b \in N$, что $a < b < a+1$.*

Доказательство. Докажем, что если $a < b$, то $b \geq a+1$. Действительно, если $a < b$, то $b > a$. По определению понятия «больше» 2.4 $b = a+n$, где $n \in N$. Так как $n \geq 1$, то $b \geq a+1$. ⊠

Теорема 2.27. **(Архимедовость)** *Для любых натуральных чисел a и b существует натуральное число n такое, что $nb > a$.*

Доказательство. Каким бы ни было натуральное число a, существует натуральное число $n > a$. Таким, в частности, является число $n = a+1$. Поэтому $nb > ab$. Но $ab \geq a$, поскольку $b \geq 1$. Следовательно, $nb > a$. ⊠

Замечание. В геометрии аналогичное утверждение для любых двух отрезков a и b называется *аксиомой Архимеда*.

Теорема 2.28. **(Бесконечность)** *Множество всех натуральных чисел N бесконечно.*

Доказательство. Множество всех натуральных чисел N бесконечно, т.к. отображение $f(n) = n + 1$ для любого натурального числа n отображает взаимнооднозначно множество $N = \{1, 2, 3, ...\}$ на его собственное подмножество $N_1 = \{2, 3, ...\}$, т.е. множество N равномощно множеству $N \setminus \{1\}$. $\boxtimes$

Множество натуральных чисел, расположенных так, что первым является число 1 и справа от каждого натурального числа n стоит следующее за ним натуральное число $n + 1$ называется *натуральным рядом*.

Заметим, что в силу аксиомы индукции в натуральном ряду содержатся все натуральные числа.

2.5 Вычитание и деление натуральных чисел

Определение 2.5. *Вычитанием натуральных чисел называется отображение, сопоставляющее паре натуральных чисел a и b число $(a-b)$, называемое их разностью, такое что $(a-b)+b=a$.*

Замечание. Вычитание является операцией обратной сложению.

Теорема 2.29. (Критерий существования разности двух натуральных чисел) *Разность двух натуральных чисел a и b существует тогда и только тогда, когда $a>b$. Если разность существует, то она единственна.*

Доказательство. Так как $a>b$, то существует $k\in N$ такое, что $a=b+k$. Тогда по определению разности двух натуральных чисел $k=a-b$.

Наоборот: из $k=a-b$ следует $a=b+k$, откуда $a>b$.

Докажем единственность. Предположим оборатное. Пусть $a-b=n$ и $a-b=m$. Тогда по определению разности $a=b+n$ и $a=b+m$, т.е. a имеет разное значение. Получили противоречие. $\boxtimes$

Замечание. Из теоремы 2.29 следует, что вычитание натуральных чисел не всегда выполнимо, т.е. операция «вычитание» на N неопределена.

Определение 2.6. *Делением натуральных чисел a и b называется операция, обратная умножению, т.е. отображение, которое сопоставляет паре натуральных чисел a и b число $a : b$ (или $\frac{a}{b}$), называемое их частным, такое что $(a : b) \cdot b = a$, где a — делимое, b — делитель, $\frac{a}{b}$ – частное.*

Теорема 2.30. (Необходимое условие существования частного) *Частное двух натуральных чисел a и b существует только тогда, когда a делится на b, т.е. a кратно b.*

Доказательство. Пусть a делится на b, тогда существует натуральное число n такое, что $n = a : b$. Тогда по определению операции «деление» $n \cdot b = a$, т.е. a кратно b. $\boxtimes$

Замечание. Верно и тверждение, обратное теореме 2.30.

Замечание. Из теоремы 2.30 следует, что бинарная операция «деление» на множестве натуральных чисел не является алгебраической, т.е. неопределена.

Таким образом, построено множество N натуральных чисел, на котором определены бинарные алгебраические операции «сложение», «умножение» и отношение строгого линейного порядка, т.е. построена система натуральных чисел.

Заметим, что это одна из бесконечного множества моделей систем натуральных чисел. Но можно доказать, что все они изоморфны и поэтому можно утверждать, что с точностью до изоморфизма существует единственная система натуральных чисел.

2.6 Независимость аксиомы математической индукции от остальных аксиом

Чтобы доказать независимость какой-то аксиомы от системы аксиом, достаточно построить модель системы аксиом, включающей все аксиомы данной теории, кроме выделенной аксиомы, т.е. такую модель, в которой верны все аксиомы теории, кроме выделенной (выделенная аксиома не верна).

Интерпретация I_1

Рассмотрим множество упорядоченных пар

$$N^{(1)} = \{(a, b) |\ a \in N, b \in \{0, 1\}\}.$$

За единицу примем пару $(1, 1)$. Сложение и умножение в $N^{(1)}$ определим следующим образом:

$$(a, x) \oplus (b, y) = \begin{cases} (a + b, 0), & \text{если } x = y \\ (a + b, 1), & \text{если } x \neq y \end{cases};$$

$$(a, x) \odot (b, y) = (ab, xy).$$

Легко проверить, что для интерпретации I_1 выполняются аксиомы $A_1 - A_3$ и $A_5 - A_8$ содержательной теории натуральных чисел. Покажем, что аксиома A_4 (аксиома математической индукции) не выполняется.

Обозначим через

$$M = \{(2a, 0) |\ a \in N\} \cup \{(2a - 1, 1) |\ a \in N\}.$$

Имеем $(1, 1) \in M$, $M \subset N^{(1)}$ и $M \neq N^{(1)}$. Следовательно, M — собственное подмножество $N^{(1)}$.

1) $(1, 1) \in M$,

2) Пусть $\alpha \in M$. Покажем, что $\alpha' \in M$.

Т.к. $\alpha \in M$, то α — либо пара $(2a, 0)$, либо $(2a-1, 1)$. Если $\alpha = (2a, 0)$, то $\alpha' = (2a + 1, 1)$. Значит, $\alpha' \in M$. Если $\alpha = (2a - 1, 1)$, то

$$\alpha' = \alpha + 1 = (2a - 1, 1) \oplus (1, 1) = (2a, 0), \text{ т.е. } \alpha' \in M.$$

Условия аксиомы A_4 выполняются, но заключение $M = N^{(1)}$ не выполняется, так как M является собственным подмножеством множества $N^{(1)}$.

Следовательно, аксиома A_4 не является следствием остальных аксиом Пеано, т.е. доказана её независимость.

Покажем, что без аксиомы A_4 системы Пеано нельзя обосновать теорию неравенств в I_1. Предположим, что в интерпретации I_1 определено транзитивное, антирефлексивное, связное и монотонное относительно общих операций бинарное отношение $>$.

Рассмотрим две пары $(0, 1)$ и $(1, 1)$.

Возможны два случая:

1. $(1, 0) > (1, 1)$;

2. $(1,1) > (1,0)$.

Рассмотрим первый случай. Тогда имеет место неравенство

$$(1,0) > (1,1). \tag{2.9}$$

Прибавим к неравенству 2.9 пару $(1,0)$:

$$(1,0) \oplus (1,0) > (1,1) \oplus (1,0),$$

т.е. $(2,0) > (2,1)$. Затем прибавим к 2.9 пару $(1,1)$, получим:

$$(1,0) \oplus (1,1) > (1,1) \oplus (1,1),$$

т.е. $(2,1) > (2,0)$. Из того, что $(2,0) > (2,1)$ и $(2,1) > (2,0)$ получаем $(2,0) > (2,0)$, а это противоречит антирефлексивности.

Следовательно, без аксиомы математической индукции нельзя построить теорию неравенств во множестве N.

Интерпретация I_2

Рассмотрим множество:

$$N^{(2)} = \left\{ \frac{a+1}{2} | \ a \in N \right\}.$$

Единица в этой модели — обычная единица $1 = \dfrac{1+1}{2}$.

Определим сложение в $N^{(2)}$:

$$(\forall \alpha, \beta \in N^{(2)})\ \alpha \oplus \beta = \alpha + \beta \text{ — обычное сложение.}$$

Умножение здесь вводится сложнее:

$$(\forall \alpha, \beta \in N^{(2)})\ \alpha \odot \beta = \frac{[2\alpha\beta]}{2}, \text{ где } [c] \text{ — целая часть числа } c.$$

Например, если $\alpha = \frac{1}{2}$, $\beta = \frac{3}{2}$, то $\alpha \odot \beta = \frac{\left[2 \cdot \frac{1}{2} \cdot \frac{3}{2}\right]}{2} = \frac{\left[\frac{3}{2}\right]}{2} = \frac{1}{2}$.

Под α' будем понимать $\alpha' = \alpha + 1$ (здесь $\langle + \rangle$ — обычное сложение).

Легко проверить, что все аксиомы Пеано, кроме аксиомы A_4, верны на модели $N^{(2)}$. Покажем, что IV-ая аксиома не верна.

В самом деле, пусть $M = N \neq N^{(2)}$, $M \subset N^{(2)}$. Имеем $1 \in M$. Кроме того, для любого $\alpha \in N^{(2)}$, если $\alpha \in M$, то $\alpha \in N$. Поэтому $\alpha + 1 \in N$ и, следовательно, $\alpha \oplus 1 \in M$. Значит для M выполняются все условия аксиомы индукции, но $M \neq N^{(2)}$, так как $N^{(2)}$, кроме N, содержит и другие числа.

Следовательно, на этой модели аксиома A_4 не верна.

Покажем, что в интерпретации I_2 не выполняется ассоциативный закон:

$$\frac{3}{2}\odot\left(\frac{3}{2}\odot 2\right)=\frac{3}{2}\odot\frac{\left[2\cdot\frac{3}{2}\cdot 2\right]}{2}=\frac{3}{2}\odot 3=\frac{\left[2\cdot\frac{3}{2}\cdot 3\right]}{2}=\frac{9}{2},$$

с другой стороны,

$$\left(\frac{3}{2}\odot\frac{3}{2}\right)\odot 2=\frac{\left[2\cdot\frac{3}{2}\cdot\frac{3}{2}\right]}{2}\odot 2=2\odot 2=\frac{[2\cdot 2\cdot 2]}{2}=4,\ \text{а}\ \frac{9}{2}\neq 4.$$

Покажем, что здесь и дистрибутивный закон тоже не выполняется:

$$\left(\frac{3}{2}\odot\frac{3}{2}\right)\odot\frac{3}{2}=3\odot\frac{3}{2}=\frac{\left[2\cdot 3\cdot\frac{3}{2}\right]}{2}=\frac{9}{2},$$

$$\frac{3}{2}\odot\frac{3}{2}\oplus\frac{3}{2}\odot\frac{3}{2}=\frac{\left[2\cdot\frac{3}{2}\cdot\frac{3}{2}\right]}{2}\oplus\frac{\left[2\cdot\frac{3}{2}\cdot\frac{3}{2}\right]}{2}=2\oplus 2=4,\ \text{а}\ \frac{9}{2}\neq 4.$$

Интерпретация I_3

За множество $N^{(3)}$ примем множество пар целых чисел

$$N^{(3)} = \{(n, x) |\ n \in N \wedge x \in \{0, 1\}\}.$$

За единицу примем пару $(1, 0)$. Сложение и умножение определим следующим образом:

$$(\forall (n, x), (m, y) \in N^{(3)})\ (n, x) \oplus (m, y) \begin{cases} (n + m, x), & \text{если } xy = 0 \\ (m, 1), & \text{если } xy = 1 \end{cases};$$

$$(\forall (n, x), (m, y) \in N^{(3)})\ (n, x) \odot (m, y) \begin{cases} (nm, y), & \text{если } x = 0 \\ (n, 1), & \text{если } x = 1 \end{cases}.$$

Можно показать, что на I_3 выполняются все аксиомы системы натуральных чисел, кроме аксиомы индукции. Кроме этого, не выполняется ассоциативность сложения, дистрибутивность умножения относительно сложения.

Замечание. Из моделей $N^{(1)}$–$N^{(3)}$ следует, что известные свойства арифметических действий не могут быть обоснованы без аксиомы индукции.

Интерпретация I_4

Рассмотрим множество

$$N^{(4)} = \left\{ \frac{a}{b} \middle| \; a, b \in N \wedge a > b \right\}.$$

За единицу примем число $\frac{1}{1}$. Сложение и умножение определим следующим образом: $\alpha \oplus \beta = \alpha + \beta$; $\alpha \odot \beta = \alpha \cdot \beta$.

На этой интерпретации выполняются все аксиомы системы натуральных чисел, кроме аксиомы индукции. Кроме этого $\langle N^{(4)}, \oplus, \odot \rangle$ является полукольцом. Примечательным является и тот факт, что на $N^{(4)}$ нет простых чисел. Пусть $\alpha \in N^{(4)}$, $\alpha \neq 1$. Тогда $\alpha = \frac{a}{b}$; $a > b$. Известно, что существует натуральное число $x \in N$ такое, что $(a-b)x > b$. 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.

Интерпретация I_5

Пусть

$$N^{(5)} = \{(a, b) | \; a, b \in N \wedge a \leq b\}.$$

Операции сложения и умножения на $N^{(5)}$ определим следующим образом:

$$(a,b) \oplus (c,d) = (a+c, b+d);$$

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

На $N^{(5)}$ выполняются все аксиомы системы натуральных чисел, кроме аксиомы индукции. В $N^{(5)}$ есть простые числа. Например, $(17,19)$, $(2,5)$, $(3,7)$.

Рассмотрим пару $(6,35) = (2,7) \odot (3,5) = (3,7) \odot (2,5)$. Поэтому на $N^{(5)}$ нет однозначности разложения на простые множители.

Замечание. Из существования $N^{(4)}$ и $N^{(5)}$ следует, что теорию делимости нельзя обосновать без аксиомы индукции.

Таким образом, аксиома индукции играет огромную роль в теории натуральных чисел.

Если нужно доказать, что для любого $n \in N$ верно $T(n)$, то

1) сначала проверяем, что $T(1)$ верно;

2) $(\forall m \in N)\ T(m) \Rightarrow T(m')$, т.е. если из предположения истинности $T(m)$ следует истинность $T(m')$, то $T(n)$ верно для любого $n \in N$.

2.7 Категоричность аксиоматической теории натуральных чисел

Теорема 2.31. *Аксиоматическая теория натуральных чисел категорична.*

Доказательство. В предположении, что аксиоматическая теория натуральных чисел непротиворечива, докажем, что любые её две модели изоморфны.

Пусть $\langle N_1, +, \cdot, 1_1\rangle$ и $\langle N_2, \oplus, \odot, 1_2\rangle$ две модели нашей теории. Любой элемент из N_1 снабжаем индексом 1, а любой элемент из N_2 — индексом 2

Построим изоморфное отображение одной системы на другую. Докажем, что существует взаимнооднозначное соответствие $\varphi : N_1 \to N_2$, обладающее свойствами:

а) $\varphi(1_1) = 1_2$;

б) $(\forall x_1 \in N_1)\ \varphi(x_1 + 1_1) = \varphi(x_1) \oplus 1_2$, $\varphi(x_1 \cdot 1_1) = \varphi(x_1) \odot 1_2$.

(Здесь $\varphi(x_1) = x_2$, $\varphi(x_1 + 1_1) = x_2 \oplus 1_2$, т.е. $\varphi(x_1') = x_2'$).

Покажем, что φ — инъекция, т.е.

$$(\forall x_1, y_1 \in N_1)\ x_1 \neq y_1 \Rightarrow \varphi(x_1) \neq \varphi(y_1). \tag{2.10}$$

Проверим (2.10) при $y_1 = 1_1$. Если $x_1 \neq 1_1$, то существует $z_1 \in N_1$, такое что $x_1 = z_1 = 1_1$. Тогда

$$\varphi(y_1) = \varphi(1_1) = 1_2,\ \ \varphi(x_1) = \varphi(z_1 + 1_1) = \varphi(z_1) \oplus 1_2.$$

Следовательно, получим $\varphi(z_1) \oplus 1_2 \neq 1_2 \Rightarrow \varphi(x_1) \neq \varphi(y_1)$.

Предположим, что для некоторого $y_1 \in N_1$ условие (2.10) выполняется. Рассмотрим $x_1 \neq y_1 + 1_1$. Требуется доказать, что $\varphi(x_1) \neq \varphi(y_1 + 1_1)$. Предположим противное, т.е. что

$$\varphi(x_1) = \varphi(y_1 + 1_1). \tag{2.11}$$

Но $\varphi(y_1 + 1_1) = \varphi(y_1) \oplus 1_2$. Поэтому $\varphi(x_1) = \varphi(y_1) \oplus 1_2 \neq 1_2$ и, значит, $x_1 \neq 1_1$. Таким образом, существует $z_1 \in N_1$, что $x_1 = z_1 + 1_1$. Но тогда получим $\varphi(x_1) = \varphi(z_1 + 1_1) = \varphi(z_1) \oplus 1_2$. В силу (2.11)

$$\varphi(z_1) \oplus 1_2 = \varphi(y_1) \oplus 1_2.$$

По аксиоме A_3 следует $\varphi(z_1) = \varphi(y_1)$ и по предположению $z_1 = y_1$. А это противоречит условию, так как $x_1 = z_1 + 1_1 = y_1 + 1_1$, а мы выбирали $x_1 \neq y_1 + 1_1$.

По аксиоме A_4 инъекция доказана для отображения φ.

Покажем, что φ — сюръективное отображение N_1 на N_2, т.е. что любой элемент из N_2 имеет хотя бы один праобраз в N_1.

Прежде всего имеем, что $1_2 = \varphi(1_1)$. Значит, 1_2 имеет прообраз в N_1. Предположим, что любой элемент $x_2 \in N_2$ имеет праобраз в N_1, т.е. $x_2 = \varphi(x_1)$ и рассмотрим $x_2 \oplus 1_2 = \varphi(x_1) \oplus 1_2 = \varphi(x_1 + 1_1)$. Значит, $x_2 \oplus 1_2$ имеет прообразом число $(x_1 + 1_1) \in N_1$. По аксиоме A_4 доказана сюръекция φ.

Следовательно, отображение φ взаимнооднозначно.

Осталось показать, что $(\forall x_1, y_1 \in N_1)$
1) $\varphi(x_1 + y_1) = \varphi(x_1) \oplus \varphi(y_1)$,
2) $\varphi(x_1 \cdot y_1) = \varphi(x_1) \odot \varphi(y_1)$.

Докажем по индукции первое равенство. При $y_1 = 1_1$ имеем

$$\varphi(x_1 + 1_1) = \varphi(x_1) \oplus 1_2 = \varphi(x_1) \oplus \varphi(1_1),$$

т.е. при $y_1 = 1_1$ первое равенство верено.

Предположим, что 1 верно при y_1, т.е. $\varphi(x_1 + y_1) = \varphi(x_1) \oplus \varphi(y_1)$. Рассмотрим при $y_1 + 1_1$, т.е.

$$\varphi(x_1 + (y_1 + 1_1)) = \varphi((x_1 + y_1) + 1_1) = \varphi(x_1 + y_1) \oplus 1_2.$$

По предположению получаем

$$\varphi(x_1+y_1)\oplus 1_2 = (\varphi(x_1)\oplus\varphi(y_1))\oplus 1_2 = \varphi(x_1)\oplus(\varphi(y_1)\oplus 1_2) = \varphi(x_1)\oplus\varphi(y_1+1_1).$$

По индукции первое равенство доказано.

Аналогично доказывается и второе равенство.

Следовательно, $N_1 \cong N_2$. Значит, аксиоматическая теория натуральных чисел категорична, поскольку любые её модели изоморфны. $\boxtimes$

2.8 Непротиворечивость арифметики

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 году К.Гёдель доказал, что непротиворечивость формальной аксиоматической теории натуральных чисел не может быть обоснована средствами этой же теории (вторая теорема Гёделя). Гёдель показал, что формальная арифметика некатегорична. На первый взгляд этот результат противоречит теореме 2.31.

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 определённые 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 Гёделя 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 надёжных.

В 1936 году Г.Генцен получил доказательство непротиворечивости формальной арифметики с помощью средств другой формальной теории.

Непротиворечивость аксиоматических теорий других числовых систем доказывается построением модели в рамках теории непротиворечивость которой известна или в рамках теории, которая предположительно непротиворечива. В каждом случае исходят из некоторого бесконечного множества объектов непротиворечивой теории и средствами интуитивной теории множеств завершают построения соотвествующей модели. Такой подход к обоснованию числовых систем был разработан в 18 веке. В теории множеств обнаружен ряд пардоксов, которые до сих пор являются неопределенными. Поэтому остается вопрос о тех или иных способах рассуждений в математике.

Непротиворечивость, полнота систем аксиом и другие вопросы обоснования математики, арифметики тесно связаны с проблемами теории доказательств, теории алгоритмов, разрешением которых занимается математическая логика.

На основе рассмотернной теории, базирующейся на аксиоме постро-

ения чисел, можно продолжить построение арифметики натуральных чисел, т.е. вывести всевозможные предложения выражающие свойства натуральных чисел. Например, можно дать определение суммы n натуральных чисел и получить реккурентные формулы сложения чисел, а также доказать, что сумма не зависит от расстановки скобок и от порядка слагаемых; можно доказать ряд свойств прямых и обратных арифметических действий.

Теория является непротиворечивой, если из нее невозможно вывести одновременно истиность и ложность одного и того же предложения. Если же теория противоречива, то в ней невозможно отличить истинное от ложного (в ней можно доказать все, что угодно). Гарантией непротиворечивости аксиоматической теориии натуральных чисел является многовековая практика, показавшая отсутсвие противоречий этой теории, правильное отражение ею действительного соотношения реального мира.

Пример 1.

$$35 + 10 - 45 = 42 + 12 - 54;$$
$$5(7 + 2 - 9) = 6(7 + 2 - 9);$$
$$5 = 6.$$

Пример 1 показывает, что нельзя сокращать на нуль.

Пример 2.

$$36 - 16 = 45 - 25;$$

$$20\frac{1}{4} - 36 + 16 = 20\frac{1}{4} - 45 + 25;$$

$$\left(4 - \frac{9}{2}\right)^2 = \left(5 - \frac{9}{2}\right)^2;$$

$$4 - \frac{9}{2} = 5 - \frac{9}{2};$$

$$4 = 5.$$

Пример 2 показывает, что избавляясь от квадратов нужно ставить знак модуля.

2.9 Вопросы и задания для самоконтроля

1. Сформулируйте аксиомы системы натуральных чисел.
2. Какое число называется следующим за числом a?
3. Что утверждают аксиомы
   - *a*) A_1;
   - *b*) A_2;
   - *c*) A_3;
   - *d*) A_4;
   - *e*) A_5 и A_6;
   - *g*) A_7 и A_8?
4. Какие из аксиом Пеано не выполняются для следующего множества $\{1, 2, 3, 4, 5, 6, 7\}$?
5. Выполняются ли hyperlinks21аксиомы Пеано для множества

$$\{a^2, a^4, a^{16}, a^{32}, ...\},$$

если роль единицы играет a^2, а отношение «следовать за» понимается как «равно квадрату»?

6. Почему утверждение $a = b \Rightarrow a' = b'$ не доказывается как отдельная теорема?
7. Откуда следует утверждение $a \neq b \Rightarrow a' \neq b'$?
8. Откуда следует утверждение $a' \neq b' \Rightarrow a \neq b$?
9. Воспользовавшись определениями операций сложения и умножения, найдите $3 + 5$, $2 \cdot 4$.

РАЗДЕЛ 3
СИСТЕМА ЦЕЛЫХ ЧИСЕЛ

3.1 Предварительные замечания

На множестве натуральных чисел не определена бинарная операция вычитания. Это и послужило причиной расширения множества натуральных чисел до множества целых чисел.

При расширении системы натуральных чисел до системы целых чисел Z потребуем, чтобы система Z удовлетворяла следующим аксиомам (аксиомам расширения):

A_1. $N \subset Z$;

A_2. Операции сложения и умножения должны быть определены на множестве Z так, чтобы сумма и произведение любых двух натуральных чисел a и b как элементов системы Z совпадали с суммой $a + b$ и произведением $a \cdot b$ этих чисел в системе N.

A_3. Определенные на Z операции сложения и умножения должны обладать теми же свойствами, что и одноименные операции на N, т.е. операции сложения и умножения на Z ассоциативны, коммутативны и связаны законами дистрибутивности.

A_4. На Z выполнимо вычитание.

Замечание. Множество Z, удовлетворяющее аксиомам A_1–A_4, есть упорядоченное коммутативное кольцо, являющееся расширением системы натуральных чисел.

3.2 Аксиоматическое построение кольца целых чисел

Первичные термины в Z:

1) Z — множество, его элементы называются целыми числами;
2) $+$, $\cdot$ — бинарные операции сложения и умножения на Z;
3) 0 — нуль, нейтральный элемент сложения на Z;
4) N — подмножество Z, его элементы называются натуральными числами;
5) $\oplus$, $\odot$ — бинарные операции сложения и умножения на N.

Определение 3.1. *Системой целых чисел называется система* $\langle Z, +, \cdot, 0, \oplus, \odot \rangle$, *удовлетворяющая трем группам аксиом:*

I. Аксиомы кольца:

Z_1. $(\forall a, b \in Z)\ (\exists! c \in Z)\ a + b = c$.
Z_2. $(\forall a, b, c \in Z)\ (a + b) + c = a + (b + c)$.
Z_3. $(\forall a, b \in Z)\ a + b = b + a$.
Z_4. $(\exists 0 \in Z)\ (\forall a \in Z)\ a + 0 = a$.
Z_5. $(\forall a \in Z)\ (\exists! a' \in Z)\ a + a' = 0$.
Z_6. $(\forall a, b \in Z)\ (\exists! p \in Z)\ ab = p$.
Z_7. $(\forall a, b, c \in Z)\ (ab)c = a(bc)$.
Z_8. $(\forall a, b, c \in Z)\ (a + b)c = ac + bc \wedge c(a + b) = ca + cb$.

II. Аксиомы расширения:

Z_9. $\langle N, \oplus, \odot \rangle$ — полукольцо натуральных чисел.
Z_{10}. $N \subset Z$.
Z_{11}. $(\forall a, b \in N)\ a + b = a \oplus b$.
Z_{12}. $(\forall a, b \in N)\ a \cdot b = a \odot b$.

III. Аксиома минимальности:

Z_{13}. Пусть $M \subset Z$ и M содержит в себе множество N $(N \subset M)$ и пусть $(\forall a, b \in M)\ a - b \in M$, тогда $M = Z$.

Следствия из аксиом

Следствие 3.1. *Любой элемент из Z представим в виде разности двух натуральных чисел.*

Доказательство. Обозначим через M подмножество Z всех таких целых чисел, которые представляемы в виде разности натуральных чисел. Имеем

1) $(\forall n \in N)\ n = (n+1) - 1 \in M$. Поэтому $N \subset M$.

2) $(\forall a, b \in M)\ (\exists k, l, m, n \in N)$ такие, что $a = k - l$ и $b = m - n$. Поэтому $a - b = (k - l) - (m - n) = k - l - m + n = (k + n) - (l + m)$ является разностью натуральных чисел и, следовательно, $(a - b) \in M$.

По аксиоме минимальности $M = Z$. ⊠

Следствие 3.2. *Кольцо Z — коммутативное кольцо с единицей.*

Доказательство. Чтобы доказать, что Z является коммутативным кольцом с единицей, нужно доказать, что умножение на Z коммутативно и существует нейтральный элемент по умножению. Возьмем любые $a, b \in Z$. По следствию 3.1 $a = k - l, b = m - n$, где $k, l, m, n \in N$.

Тогда

$$a \cdot b = (k-l)(m-n) \overset{Z_8}{=} (k-l)m - (k-l)n \overset{Z_8}{=}$$

$$= km - lm - kn + ln \overset{Z_3}{=} (km + ln) - (kn + lm).$$

С другой стороны,

$$b \cdot a = (m-n)(k-l) \overset{Z_8}{=} (m-n)k - (m-n)l \overset{Z_8}{=}$$

$$= mk - nk - ml + nl \overset{Z_3}{=} (mk + nl) - (nk + ml).$$

Так как $\langle\cdot\rangle$ на N коммутативно, то коммутативность $\langle\cdot\rangle$ в Z доказана. Так как $1 \in N$, а $N \subset Z$, то $1 \in Z$. $\boxtimes$

Следствие 3.3. *Всякий элемент кольца целых чисел есть либо нуль, либо натуральное число, либо противоположное натуральному числу.*

Доказательство. Доказательство следует из следствия 3.1. Любой элемент $a \in Z$ можно представить в виде разности $a = m - n$, где $m, n \in N$. Если $m = n$, то $a = 0$. Если $m > n$, то $a = m - n \in N$. Если $m < n$, то $a = m - n$ — противоположное натуральному числу. $\boxtimes$

Следствие 3.4. *Кольцо Z можно линейно и строго упорядочить и притом единственным образом. Порядок в кольце целых чисел архимедов и продолжает порядок в полукольце натуральных чисел.*

3.3 Свойства целых чисел

Кольцо Z обладает всеми свойствами произвольного кольца. Операции $\langle + \rangle$ и $\langle \cdot \rangle$ связаны с отношением порядка на Z следующим образом

Теорема 3.1. **(Монотонность сложения и умножения)**
1) $(\forall a, b, \in Z)\ a > b \ \vee\ a = b \ \vee\ a < b \ \Rightarrow\ a + c > b + c \ \vee\ a + c = b + c \ \vee\ a + c < b + c.$
2) $(\forall a, b, \in Z, c > 0)\ a > b \ \vee\ a = b \ \vee\ a < b \ \Rightarrow\ ac > bc \ \vee\ ac = bc \ \vee\ ac < bc.$
3) $(\forall a, b, \in Z, c < 0)\ a > b \ \vee\ a = b \ \vee\ a < b \ \Rightarrow\ ac < bc \ \vee\ ac = bc \ \vee\ ac > bc.$

Определение 3.2. *Областью целостности называется коммутативное кольцо с единицей, не содержащее делителей нуля.*

Теорема 3.2. *Кольцо Z является областью целостности.*

Теорема 3.3. 1. *Кольцо Z является расположенным кольцом, т.е. для любого $a \in Z$ имеет место только одно из соотношений:*

$$a > 0 \text{ или } a = 0 \text{ или } a < 0.$$

2. $(\forall a, b \in Z)\ a > 0, b > 0 \Rightarrow a + b > 0 \wedge ab > 0.$

Теорема 3.4. **(Архимедовость)** *Кольцо Z является архимедовски упорядоченным кольцом, т.е. для любых целых чисел a и $b > 0$ существует натуральное число n такое, что $nb > a$.*

Доказательство.

1) Пусть $a \leq 0$. Так как $b > 0$ и $n > 0$, то $bn > 0$ согласно теореме 3.1. Следовательно, $bn > a$.

2) Пусть $a > 0$. Тогда $a, b \in N$, а для натуральных чисел имеет место теорема Архимеда. ⊠

Замечание. Из теоремы 3.4 следует неограниченность множества Z.

Теорема 3.5. (Дискретность) *Каково бы ни было целое число a, не существует такого целого числа b, что $a < b < a + 1$, т.е.*

$$(\forall a \in Z)\ \overline{|}(\exists b \in Z)\ a < b < a + 1.$$

Доказательство. 1. Если $a > 0$, то a и $a + 1$ натуральные числа. Следовательно, теорема верна (см. теорему 2.26).

2. Зададим взаимно однозначное отображение φ множества $\{0, 1, 2, 3, ...\}$ на множество $\{0, -1, -2, -3, ...\}$, т.е. поставим в соответствие каждому элементу a из первого множества число $-a$ из второго множества и $0 \to 0$.

Если для отрицательных чисел выполняется условие

$$-(a + 1) < -b < -a,$$

то из взаимной однозначности отображения φ следует, что $a < b < a+1$, что невозможно для натуральных чисел a, b, $a + 1$.

А так как нет натуральных чисел, предшествующих 1, то не существует b, такое что $0 < b < 1$.

Значит, в силу заданного отображения φ не существует отрицательного числа $-b$ между -1 и 0. $\boxtimes$

Замечание. Из теоремы 3.5 следует, что множество Z дискретно.

Теорема 3.6. *Произведение целых чисел равно нулю тогда и только тогда, когда хотя бы один из сомножителей равен нулю.*

3.4 Категоричность и непротиворечивость системы аксиом кольца Z

3.4.1 Непротиворечивость аксиоматической теории целых чисел

Теорема 3.7. *Аксиоматическая теория целых чисел непротиворечива.*

Доказательство. Докажем непротиворечивость аксиоматической теории целых чисел, исходя из предположения, что непротиворечива аксиоматическая теория натуральных чисел.

Построим модель, на которой выполняются все аксиомы системы целых чисел. Будем использовать следующий алгоритм доказательства теоремы:

1) построение кольца;

2) включение полукольца натуральных чисел: для этой цели мы покажем, что некоторое полукольцо построенной интерпретации нашей теории изоморфно полукольцу натуральных чисел и, значит, само является таковым;

3) проверка выполнения аксиомы минимальности.

Пусть $N = \langle N, +, \cdot, 1\rangle$ — система натуральных чисел. Рассмотрим множество $P = \{(a, b)|\ a, b \in N\}$. Определим на множестве P бинарные

операции сложения $\oplus$ и умножения $\odot$ следующим образом:

$$(\forall a, b, a', b' \in N)\ (a, b) \oplus (a', b') = (a + a', b + b');$$

$$(\forall a, b, a', b' \in N)\ (a, b) \odot (a', b') = (aa' + bb', ab' + a'b).$$

Известно, что система $\langle P, \oplus, \odot \rangle$ образует коммутативное полукольцо. Однако, эта система не является кольцом.

Введем на множестве P бинарное отношение:

$$(\forall a, b, a', b' \in N)\ (a, b) \sim (a', b') \Leftrightarrow a + b' = a' + b.$$

Это отношение является рефлексивным, симметричным, транзитивным и монотонно относительно обеих операций, определенных в P. Поэтому отношение $\sim$ является отношением эквивалентности.

Кроме этого рассмотрим множество $\overline{P}$ — множество классов эквивалентности множества P относительно рассмотренного отношения. Обозначая класс α, содержащий пару (a, b), символом $\overline{(a, b)}$, мы имеем $\alpha = \overline{(a, b)}$, и если $\beta = \overline{(a', b')}$, то

$$\alpha = \beta \Leftrightarrow (a, b) \sim (a', b').$$

В частности, $\overline{(a, b)} = \overline{(a + c, b + c)}$ для каждого c из N.

Определим бинарные операции сложения и умножения в $\overline{P}$:

$$\overline{(a, b)} + \overline{(a', b')} = \overline{(a, b) \oplus (a', b')};$$

$$\overline{(a,b)} \cdot \overline{(a',b')} = \overline{(a,b) \odot (a',b')}.$$

Соответствие, которое переводит (a,b) в $\overline{(a,b)}$ является гомоморфным отображением системы $\langle P, \oplus, \odot \rangle$ на систему $\langle \overline{P}, +, \cdot \rangle$.

Система $\langle \overline{P}, +, \cdot \rangle$ является коммутативным полукольцом. Докажем, что эта система является кольцом.

Пусть $\alpha = \overline{(a,b)}$ и $\beta = \overline{(a',b')}$ — произвольные классы из $\overline{P}$. Покажем, что в $\overline{P}$ существует класс $\gamma = \overline{(x,y)}$, такой что

$$\alpha + \gamma = \beta. \tag{3.1}$$

Но

$$(\forall x, y \in N)\ \overline{(a,b)} + \overline{(x,y)} = \overline{(a',b')} \Leftrightarrow \overline{(a+x, b+y)} = \overline{(a',b')}.$$

С другой стороны

$$\overline{(a+x, b+y)} = \overline{(a',b')} \Leftrightarrow a + x + b' = a' + b + y.$$

Последнее соотношение выполняется, если $x = a' + b$ и $y = a + b'$. Отсюда следует, что класс $\overline{(a'+b, a+b')}$ является решением уравнения 3.1. Другими словами, $\overline{(a',b')} - \overline{(a,b)} = \overline{(a'+b, a+b')}$.

Выберем в $\overline{P}$ подмножество N_0 следующим образом:

$$(\forall \alpha = \overline{(a,b)} \in \overline{P})\ \alpha \in N_0 \Leftrightarrow a > b.$$

Проверим, что принадлежность $\alpha \in N_0$ не зависит от выбора представителя класса α. В самом деле, если $a = b + n$, то

$$(a, b) \sim (a', b') \Leftrightarrow a' = b' + n.$$

Сопоставим с натуральным числом n класс $\varphi(n) = \overline{(1 + n, 1)}$. Имеем: $\varphi(m) = \varphi(n) \Leftrightarrow m = n$. Далее

$$\varphi(m + n) = \overline{(m + n + 1, 1)} = \overline{(1 + n + 1 + m, 1 + 1)} =$$

$$= \overline{(1 + m, 1)} + \overline{(1 + n, 1)} = \varphi(m) + \varphi(n).$$

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 $\langle N_0, +, \cdot \rangle$.

Докажем, что на построенной интерпретации аксиоматической теории целых чисел выполняется и последняя аксиома — аксиома минимальности.

Рассмотрим некоторое непустое подмножество M множества $\overline{P}$, 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 $\gamma = \overline{(n, m)}$, n и m — какие-нибудь элементы N. Покажем, что класс γ можно представить в виде разности

двух элементов из N_0. Но мы имеем:

$$(n, m) + (m + 1, 1) = (n + m + 1, m + 1);$$

$$(n + m + 1, m + 1) \sim (n + 1, 1).$$

Поэтому

$$\gamma = \overline{(n, m)} = \overline{(n + 1, 1)} - \overline{(m + 1, 1)} \in M.$$

⊠

3.4.2 Категоричность аксиоматической теории целых чисел

Теорема 3.8. *Система аксиом кольца Z является категоричной.*

Доказательство. В предположении, что аксиоматическая теория целых чисел непротиворечива, покажем, что любые 2 модели кольца целых чисел Z изоморфны. Рассмотрим две модели $\langle Z_1, +, \cdot, 0_1, N_1, +, \cdot\rangle$ и $\langle Z_2, \oplus, \odot, 0_2, N_2, \oplus, \odot\rangle$, где $\langle N_1, +, \cdot\rangle$ и $\langle N_2, \oplus, \odot\rangle$ — полукольца натуральных чисел ($N_1 \subset Z_1$, $N_2 \subset Z_2$). Любой элемент множества Z_1 снабдим индексом 1, а элементы множества Z_2 — индексом 2.

Существует изоморфное отображение $\varphi : N_1 \to N_2$ первого полукольца на второе, которое удовлетворяет двум условиям:

1) $(\forall a_1, b_1 \in N_1)\ \varphi(a_1 + b_1) = \varphi(a_1) \oplus \varphi(b_1)$;

2) $(\forall a_1, b_1 \in N_1)\ \varphi(a_1 \cdot b_1) = \varphi(a_1) \odot \varphi(b_1)$.

По следствию 3.1 каждый элемент из Z_1 представим в виде разности элементов из N_1, а каждый элемент из Z_2 — в виде разности элементов из N_2. Этим и воспользуемся для определения изоморфного отображения f первой системы Z_1 на вторую Z_2.

Пусть $c_1 \in Z_1$, тогда существуют $k_1, l_1 \in N_1$ такие, что $c_1 = k_1 - l_1$. Полагаем, что $f(c_1) = \varphi(k_1) \ominus \varphi(l_1)$. Заметим, что $\varphi(k_1) \in N_2$, $\varphi(l_1) \in N_2$, поэтому $f(c_1) = \varphi(k_1) \ominus \varphi(l_1) \in Z_2$.

Если m_1 и n_1 такие элементы из N_1, что $k_1 - l_1 = m_1 - n_1$, то справедливо $k_1 + n_1 = m_1 + l_1$ и

$$\varphi(k_1) \oplus \varphi(n_1) = \varphi(k_1 + n_1) = \varphi(m_1 + l_1) = \varphi(m_1) \oplus \varphi(l_1).$$

Отсюда, $\varphi(k_1) \ominus \varphi(l_1) = \varphi(m_1) \ominus \varphi(n_1)$. Поэтому f является однозначным отображением Z_1 в Z_2.

Для любого $a_2 \in Z_2$ можно найти элементы $k_2, l_2 \in Z_2$ такие, что $a_2 = k_2 - l_2$. А так как φ — однозначное отображение N_1 на N_2, то существуют элементы k_1, l_1 в N_1, что $k_2 = \varphi(k_1)$ и $l_2 = \varphi(l_1)$. Значит, $a_2 = k_2 - l_2 = \varphi(k_1) \ominus \varphi(l_1) = f(k_1 - l_1)$, т.е. для любого элемента $a_2 \in Z_2$ существует элемент $(k_1 - l_1) \in Z_1$, который является прообразом элемента a_2 в Z_1. Следовательно, f — сюръекция.

Покажем, что если образы равны, то равны и прообразы, т.е. для любых $k_1, l_1, m_1, n_1 \in N_1$ из равенства $f(k_1 - l_1) = f(m_1 - n_1)$ следует, что $k_1 - l_1 = m_1 - n_1$. В самом деле,

$$f(k_1 - l_1) = \varphi(k_1) \ominus \varphi(l_1) = f(m_1 - n_1) = \varphi(m_1) \ominus \varphi(n_1).$$

Откуда $\varphi(k_1) \oplus \varphi(n_1) = \varphi(m_1) \oplus \varphi(l_1)$.

Так как φ — изоморфизм N_1 на N_2, то $\varphi(k_1+n_1) = \varphi(m_1+l_1)$ и в силу изоморфизма φ имеем $k_1+n_1 = m_1+l_1$. Следовательно, $k_1-l_1 = m_1-n_1$. Значит, равные образы имеют одинаковые прообразы.

Доказано, что f — взаимнооднозначное соответствие.

Покажем, что

1) $(\forall z_1, \rho_1 \in Z_1)\ f(z_1 + \rho_1) = f(z_1) \oplus f(\rho_1)$;

2) $(\forall z_1, \rho_1 \in Z_1)\ f(z_1 \cdot \rho_1) = f(z_1) \odot f(\rho_1)$.

Докажем первое утверждение. Пусть $z_1 = a_1 - b_1$, $\rho_1 = c_1 - d_1$, где $a_1, b_1, c_1, d_1 \in N_1$.

Найдем

$$f(z_1 + \rho_1) = f((a_1 + c_1) - (b_1 + d_1)) = \varphi(a_1 + c_1) \ominus \varphi(b_1 + d_1) =$$

$$= (\varphi(a_1) \oplus \varphi(c_1)) \ominus (\varphi(b_1) \oplus \varphi(d_1)) = (\varphi(a_1) \ominus \varphi(b_1)) \oplus (\varphi(c_1) \ominus \varphi(d_1)) =$$

$$= f(z_1) \oplus f(\rho_1).$$

Аналогично доказывается и второе утверждение. Следовательно, f является изоморфизмом Z_1 на Z_2. $\boxtimes$

3.5 Вопросы и задания для самоконтроля

1. Сформулируйте аксиомы системы целых чисел.
2. Какую алгебру представляет собой система целых чисел?
3. Из какой аксиомы следует существование противоположного числа для a?
4. Из каких аксиом следует, что Z является расширением N?
5. Как доказать, что кольцо целых чисел можно упорядочить единственным способом и этот порядок является архимедовским, продолжением порядка в N?

РАЗДЕЛ 4
СИСТЕМА РАЦИОНАЛЬНЫХ ЧИСЕЛ

4.1 Введение

Задачи измерения пространственных, временных, физических и других величин приводят к необходимости учитывать такие части соответствующих единиц измерений, из которых единицы измерения целиком могут быть составлены, а также — совокупности таких частей. Например, измерение длины отрезков.

Целые числа не могут обеспечить решение рассмотренных задач. Возникает необходимость введения новых чисел, которые могли бы характеризовать части единицы и совокупности таких частей. С точки зрения арифметической теории такое расширение системы Z делает действие деления выполнимым для любых чисел, кроме деления на нуль.

Представление человека о дробных числах возникло в столь далёкие времена, что проследить по каким-либо источникам процесс возникновения понятия дроби не представляется возможным. Вероятнее всего, появление дробных чисел связано с процессом различных измерений: длины, веса, площади и т.д. У всех народов особое место занимали двоичные дроби, связанные с делением пополам. В древнем Вавилоне пользовались шестидесятеричными дробями, в древнем Египте — дробями, у которых числитель равен единице, тоже замечено и в древней Греции.

Индийцы и арабы записывали дроби, располагая числитель над знаменателем, но без черты. Употребление черты для обозначения дроби встречается в 13 веке в работах Леонардо Пизанского. Однако в качестве общепринятого обозначения дроби черта стала употребляться лишь начиная с 16 века.

Десятичные дроби были предложены к употреблению фламандским инженером и учёным Симоном Стивенсоном в 1584 году.

В начале 17 века в качестве разделительного знака в качестве разделительного знака в десятичных дробях стали использовать запятую или точку.

Окончательное утверждение десятичных дробей следует связать с введением десятичной системы мер и весов: это произошло после Французской буржуазной революции 1789 года.

На территории нашего государства метрическая система введена в 1918 году.

Прежде чем перейти к аксиоматическому построению теории рациональных чисел введем ряд определений и утверждений.

Определение 4.1. *Поле $P(K)$ называется полем частных области целостности K, если выполняются следующие условия*

1) *K — подкольцо поля P,*

2) *всякий элемент из P представим в виде частного двух элементов из K.*

Теорема 4.1. *Для всякой области целостности K существует поле частных. Если P и F два поля частных для области целостности K, то существует изоморфизм поля P на поле F, переводящий каждый элемент K в себя.*

Определение 4.2. *Поле P называется упорядоченным полем, если множество его элементов можно строго и линейно упорядочить, а отношение порядка $<$ удовлетворяет следующим условиям:*

1) $(\forall a, b, c \in P)\ a < b \Rightarrow a + c < b + c$;
2) $(\forall a, b, c, d \in P)\ a < b \wedge c < d \Rightarrow ac < bd$.

Теорема 4.2. *Пусть a и b элементы упорядоченного поля P. Тогда и только тогда $b > a$, когда $(b - a) > 0$.*

Замечание. Если a положительный элемент упорядоченного поля P, то ему противоположный элемент является отрицательным.

Определение 4.3. *Упорядоченное поле P называется Архимедовски упорядоченным полем, если для любых элементов $a > 0$ и $b > 0$ поля P, существует такое $n \in N$, что $na > b$.*

Всякое упорядоченное поле обладает следующими свойствами:

1. $(\forall a, b, c \in P)\ a < b \wedge c < 0 \Rightarrow ac > bc$.
2. $(\forall a, b, c \in P)\ a + c < b + c \Rightarrow a < c$.
3. $(\forall a, b, c \in P)\ ac < bc \wedge c > 0 \Rightarrow a < b$.

4. $(\forall a, b, c \in P)\ ac < bc \wedge c < 0 \Rightarrow a > b$.

5. Поле P является расположенным полем, т.е. выполняется два условия

a) Для любого элемента $a \in P$ либо $a > 0$, либо $a = 0$, либо $a < 0$.

b) $(\forall a, b \in P)\ a > 0 \wedge b > 0 \Rightarrow a + b > 0 \wedge ab > 0$.

6. $(\forall a, b, c, d \in P)\ a < b \wedge c < d \Rightarrow a + c < b + d$.

7. $(\forall a, b, c, d \in P, a > 0, b > 0, c > 0, d > 0)\ a < b \wedge c < d \Rightarrow ac < bd$.

Определение 4.4. *Абсолютной величиной или модулем элемента $a \in P$ называют сам элемент a, если $a > 0$ или $-a$, если $a < 0$ и обозначают $|a|$. Таким образом $|a| = a$, если $a > 0$, и $|a| = -a$, если $a < 0$.*

Свойства модулей элементов упорядоченного поля

1. Модуль суммы конечного числа элементов упорядоченного поля P не превосходит суммы модулей, т.е. $|a_1+a_2+...+a_n| \leq |a_1|+|a_2|+...+|a_n|$.

2. Модуль произведения элементов упорядоченного поля P равен произведению модулей этих элементов, т.е. $|a_1 \cdot a_2 \cdot ... \cdot a_n| = |a_1| \cdot |a_2| \cdot ... \cdot |a_n|$.

3. Сумма квадратов конечного числа элементов упорядоченного поля, среди которых хотя бы один отличен от нуля, является числом положительным, т.е. $a_1^2 + a_2^2 + ... + a_n^2 > 0$.

Следствие 1. $(\forall a \in P)\ a \neq 0 \Rightarrow a^2 > 0$.

Теорема 4.3. *Характеристика всякого упорядоченного поля равна* 0.

4.2 Аксиоматическое построение поля рациональных чисел

Определение 4.5. *Полем рациональных чисел* называется *минимальное поле, которое является расширением кольца целых чисел.*

Первичные термины:

1) Q — множество, его элементы называем рациональными числами;
2) $+$ и $\cdot$ — бинарные операции сложения и умножения на Q;
3) 0 — нуль — нейтральный элемент сложения на Q;
4) Z — подмножество Q, его элементы называются целыми числами;
5) $\oplus$, $\odot$ — бинарные операции сложения и умножения на Z.

Определение 4.6. *Система* $\langle Q, +, \cdot, 0, Z, \oplus, \odot\rangle$ *называется системой рациональных чисел, если она удовлетворяет 15-ти аксиомам, составляющим следующие три группы:*

A:

Q_1. $(\forall a, b \in Q)\ (\exists! c \in Q)\ a + b = c$.
Q_2. $(\forall a, b, c \in Q)\ (a + b) + c = a + (b + c)$.
Q_3. $(\forall a, b \in Q)\ a + b = b + a$.
Q_4. $(\exists 0 \in Q)\ (\forall a \in Q)\ a + 0 = a$.
Q_5. $(\forall a \in Q)\ (\exists a' \in Q)\ a + a' = 0$.
Q_6. $(\forall a, b \in Q)\ (\exists! p \in Q)\ a \cdot b = p$.
Q_7. $(\forall a, b, c \in Q)\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Q_8. $(\forall a, b \in Q)\ a \cdot b = b \cdot a$.
Q_9. $(\forall a, b, c \in Q)\ (a + b) \cdot c = a \cdot c + b \cdot c$.
Q_{10}. $(\forall a, b \in Q, a \neq 0)\ (\exists x \in Q)\ ax = b$.

$\underline{B}$:

Q_{11}. $\langle Z, \oplus, \odot \rangle$ — кольцо целых чисел.
Q_{12}. $Z \subset Q$.
Q_{13}. $(\forall a, b \in Z)\ a + b = a \oplus b$.
Q_{14}. $(\forall a, b \in Z)\ a \cdot b = a \odot b$.

$\underline{C}$:

Q_{15}. (аксиома минимальности): Всякое подмножество M множества Q совпадает с Q, если выполняются два условия

а) $Z \subset M$;

б) $(\forall a, b \in M, b \neq 0)\ \dfrac{b}{a} \in Q$.

Аксиомы Q_1–Q_{15} лежат в основе аксиоматической теории рациональных чисел.

Замечание. Из определения системы рациональных чисел следует, что:

1) в Q содержится нулевой и единичный элементы (обозначаемые символами 0 и 1 соответственно);

2) для произвольного отличного от 0 рационального числа m существует обратное m^{-1}, и, таким образом, в Q выполнима операция деления (обозначаемая символом «:») любого числа m на $n \neq 0$, понимаемая как умножение m на n^{-1}.

4.3 Свойства рациональных чисел

Множество рациональных чисел Q обладает всеми свойствами поля. Кроме того, поле рациональных чисел является полем частных области целостности Z.

Теорема 4.4. *Всякое рациональное число есть частное целых чисел, т.е.*

$$(\forall a \in Q)\ (\exists k, l \in Z, l \neq 0)\ a = \frac{k}{l}.$$

Доказательство. Обозначим через

$$M = \left\{ \frac{a}{b} \in Q |\ a, b \in Z \wedge b \neq 0 \right\}$$

подмножество Q всех таких рациональных чисел, которые представимы в виде частного целых чисел.

Так как любой элемент a из Z можно записать как $a = \frac{a}{1} \in M$, то $Z \subset Q$.

Пусть $r_1 \in M$, $r_2 \in M$ и $r_2 \neq 0$. Тогда $r_1 = \frac{a_1}{a_2}$, $r_2 = \frac{b_1}{b_2}$, где $a_1, a_2, b_1, b_2 \in Z$, $a_2 \neq 0$, $b_2 \neq 0$ и, значит, $\frac{r_1}{r_2} = \frac{a_1 \cdot b_2}{a_2 \cdot b_1} \in M$.

Следовательно, по аксиоме минимальности Q_{15} получаем, что множества M и Q совпадают. ⊠

Замечание. Верно и обратное утверждение: множество дробей образует поле рациональных чисел.

Замечание. Равенство $\frac{m_1}{n_1} = \frac{m_2}{n_2}$ имеет место тогда и только тогда, когда $m_1 n_2 = n_1 m_2$. Отсюда в частности, вытекает основное свойство дроби:

$$(\forall p \in Z, p \neq 0)\ \frac{m}{n} = \frac{mp}{np},$$

на котором основаны сокращения дробей и приведение их к общему знаменателю.

Замечание. Число $\frac{m}{n}$ будет целым лишь при условии, что m делится на n. Простейшим обозначением целого числа будет дробь $\frac{m}{1}$; сохраним за ней также обозначение m. В частности, $\frac{0}{1} = 0$; $\frac{1}{1} = 1$.

Теорема 4.5. *В множестве рациональных чисел выполнима и однозначна операция вычитания.*

Доказательство. Другими словами, нам надо показать, что для любых рациональных чисел $\frac{a}{b}$ и $\frac{c}{d}$ существует единственное рациональное число $\frac{x}{y}$, такое, что $\frac{c}{d} + \frac{x}{y} = \frac{a}{b}$.

Предположим, что существует рациональное число $\frac{x}{y}$, такое, что выполняется равенство $\frac{c}{d}+\frac{x}{y}=\frac{a}{b}$. Тогда $\frac{cy+dx}{dy}=\frac{a}{b}$. рациональные числа $\frac{cy+dx}{dy}$ и $\frac{a}{b}$ равны тогда, когда $(cy+dx)b=ady$, или $cyb+dxb=ady$. Отсюда $x(bd)=y(ad-bc)$. Отсюда, $\frac{x}{y}=\frac{ad-bc}{bd}$.

В самом деле, найденное рациональное число $\frac{x}{y}$ удовлетворяет определению разности рациональных чисел $\frac{a}{b}$ и $\frac{c}{d}$:

$$\frac{c}{d}+\frac{ad-bc}{bd}=\frac{cbd+add-bcd}{dbd}=\frac{add}{bdd}=\frac{a}{b}.$$

Итак, для любых рациональных чисел $\frac{a}{b}$ и $\frac{c}{d}$ существует рациональное число $\frac{ad-bc}{bd}$, такое, что $\frac{c}{d}+\frac{ad-bc}{bd}=\frac{a}{b}$. Это и свидетельствует о выполнимости вычитания в множестве рациональных чисел.

Однозначность следует из однозначности и свойств умножения и вычитания в множестве целых чисел. ⊠

Определение 4.7. *Говорят, что рациональное число* $\frac{m}{n}$ $(m \in Z,$ $n \in N)$ *меньше рационального числа* $\frac{r}{s}$ $(r \in Z, s \in N)$, *если* $ms < rn$.

Замечание. Понятие «меньше» для рациональных чисел определено с помощью понятия «меньше» для целых чисел. Можно проверить, что отношение $<$ на Q является отношением строгого линейного порядка и удовлетворяет двум условиям определения упорядоченного поля, поэтому поле Q является упорядоченным, т.е. является системой рациональных чисел и кроме этого обладает следующими свойствами:

1) Q является архимедовски упорядоченным полем.

2) поле Q является плотным, т.е. между двумя неравными рациональными числами существует хотя бы одно рациональное число.

Теорема 4.6. *Между двумя неравными рациональными числами сущесвует бесконечное множество рациональных чисел.*

Замечание. Множество Q не дискретно. Однако, оно не является непрерывным.

Замечание. Множество Q является счетным. Множество Q не ограничено.

Теорема 4.7. *Поле рациональных чисел можно линейно и строго упорядочить, притом единственным образом. Порядок в поле Q архимедов и продолжает порядок кольца Z.*

Доказательство. Рассмотрим $r = \frac{k}{l}$, где $k, l \in Z$, $l \neq 0$. Будем считать, что r положительно тогда и только тогда, когда оба числа k и l одновременно положительны или одновременно отрицательны. Другими словами r положительно, если $k \cdot l > 0$.

Условимся далее рациональное число r считать меньше, чем рациональное число r_1, а рациональное число $r_1 > r$, если $r_1 - r > 0$.

Введенное таким образом отношение «меньше» является отношением строгого линейного порядка, т.к. оно антирефлексивно, антисимметрично и транзитивно. Следовательно поле рациональных чисел с отношением «меньше» можно линейно упорядочить.

Введенное нами отношение $r < r_1$ удовлетворяет требованиям упорядоченного поля, т.е.

1) $(\forall r, r_1, c \in Q)\ r < r_1 \Rightarrow r + c < r_1 + c$;

2) $(\forall r, r_1, c \in Q)\ r < r_1 \wedge c > 0 \Rightarrow rc < r_1 c$.

Так как $r < r_1$ то по определению это означает, что $r_1 - r > 0$, т.е. $r_1 - r$ положительное число. Тогда $(r_1 + c) - (r + c) > 0$ и, если $c > 0$, то $(r_1 c) - (rc) > 0$. Это означает, что $r + c < r_1 + c$ и, если $c > 0$, то $rc < r_1 c$. $\boxtimes$

4.4 Категоричность и непротиворечивость аксиоматической теории рациональных чисел

4.4.1 Непротиворечивость аксиоматической теории рациональных чисел

Теорема 4.8. *Аксиоматическая теория рациональных чисел непротиворечива.*

Доказательство. Докажем непротиворечивость аксиоматической теории Q относительно непротиворечивости аксиоматической теории целых чисел.

Для докзательства построим модель, на которой будут выполняться все 15 аксиом теории рациональных чисел. План доказательства:

1) построение поля;

2) включение кольца целых чисел: для этой цели покажем, что некоторое подкольцо построенной интерпретации нашей теории изоморфно кольцу целых чисел и, значит, само является таковым;

3) проверка выполнения аксиомы минимальности.

1) Пусть $\langle Z, +, \cdot, 0, N, +, \cdot, 1\rangle$ — какая-либо система целых чисел.

Рассмотрим множество P пар целых чисел (a, n):

$$P = \{(a, n)|\ a \in Z, n \in N\}.$$

Введем на P бинарные операции сложения $\langle\oplus\rangle$ и умножения $\langle\odot\rangle$ следеющим образом

$$(\forall a, a' \in Z, \forall n, n' \in N)\ (a, n) \oplus (a', n') = (an' + a'n, nn'),$$

$$(\forall a, a' \in Z, \forall n, n' \in N)\ (a, n) \odot (a', n') = (aa', nn').$$

Легко показать, что $\langle P, \oplus \rangle$ и $\langle P, \odot \rangle$ — коммутативные полугруппы с нейтральными элементами $(0, 1)$ и $(1, 1)$ соответственно.

Введём на P бинарное отношение $\sim$ следующим образом:

$$(\forall a, a' \in Z)(n, n' \in N)\ (a, n) \sim (a', n') \Leftrightarrow an' = a'n.$$

Легко проверить, что введенное таким образом отношение $\sim$ рефлексивно, симметрично и транзитивно, т.е. является отношением эквивалентности. Также можно проверить, что это отношение монотонно относительно обеих операций. Опредилим во множестве классов эквивалентности $\overline{P}$ операции $\langle + \rangle$ и $\langle \cdot \rangle$:

$$(\forall (a, n), (a', n') \in \overline{P})\ \overline{(a, n)} + \overline{(a', n')} = \overline{(a, n) \oplus (a', n')},$$

$$(\forall (a, n), (a', n') \in \overline{P})\ \overline{(a, n)} \cdot \overline{(a', n')} = \overline{(a, n) \odot (a', n')}.$$

Соответствие f, по которому с парой (a, n) сопоставляется класс эквивалентности $\overline{(a, n)}$, содержащий эту пару, есть гомоморфное отображение системы $\langle P, \oplus, \odot \rangle$ на систему $\langle \overline{P}, +, \cdot \rangle$.

Докажем, что система $\langle \overline{P}, +, \cdot \rangle$ — коммутативное кольцо. Прежде всего заметим, что $(a, n) \oplus (-a, n) = (0, n^2) \sim (0, 1)$.

Проверим дистрибутивность умножения относительно сложения. Имеем

$$((a,m)\oplus(a',n'))\cdot(b,n)=(am'+a'm,mm')\odot(b,n)=(am'b+a'bm,mm'n);$$

$$(a,m)\odot(b,n)\oplus(a',n')\odot(b,n)=(ab,mn)\oplus(a'b+m'n)=$$
$$=(am'bn+a'bmn,mm'n^2).$$

Но

$$(abm'+a'bm,mm'n)\sim(abm'n+a'bmn,mm'n^2).$$

Поэтому

$$(\overline{(a,m)}\oplus\overline{(a',n')})\odot\overline{(b,n)}=\overline{(a,m)}\odot\overline{(b,n)}\oplus\overline{(a',n')}\odot\overline{(b,n)}.$$

Таким образом, система $\langle\overline{P},+,\cdot\rangle$ — коммутативное кольцо. Нетрудно проверить, что класс $\overline{(0,m)}$, где $m\in N$, является нулем этого кольца.

Докажем, что система $\langle\overline{P},+,\cdot\rangle$ — поле.

Пусть $\alpha=\overline{(a,m)}\in\overline{P}$, $\beta=\overline{(a',m')}\in\overline{P}$ и $\alpha\neq0$, т.е. $a\neq0$. Достаточно проверить, что уравнение

$$\alpha\gamma=\beta$$

разрешимо в кольце $\langle\overline{P},+,\cdot,0\rangle$. Но это так, ибо

$$\overline{(a,m)}\cdot\overline{(aa'm,m'a^2)}=\overline{(a^2a'm,mm'a^2)}=\overline{(a',m')}.$$

2) Выделим в $\overline{P}$ подмножество Z_0 такое, что

$$(\forall\alpha=\overline{(a,m)}\in\overline{P})\ \alpha\in Z_0\Leftrightarrow(\exists c\in Z)\ a=cm\wedge c\neq0.$$

Проверим, что принадлежность α к Z_0 не зависит от выбора представителя класса α. В самом деле, если $a = cm$, то

$$(a, m) \sim (a', m') \Leftrightarrow a' = cm'.$$

Сопоставим с целым числом c класс $\varphi(c) \sim \overline{(c, 1)}$. 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, φ — изоморфное отображение кольца целых чисел $\langle Z, +, \cdot \rangle$ на $\langle Z_0, +, \cdot \rangle$. Поэтому, $\langle Z_0, +, \cdot \rangle$ — является кольцом целых чисел, а поле $\langle \overline{P}, +, \cdot \rangle$ — расширение кольца $\langle Z_0, +, \cdot \rangle$.

3) Докажем, что на построенной итерпретации выполняется аксиома минимальности. Пусть M — подмножество множества $\overline{P}$, удовлетворяющее двум условиям:

a) $Z_0 \subset M$;

b) для любых α и β из M, если β не нуль кольца $\langle \overline{P}, +, \cdot \rangle$, то $\dfrac{\alpha}{\beta} \in M$.

Покажем, что в таком случае $M = \overline{P}$. Нам достаточно показать, что любой элемент $\gamma = \overline{(c, m)}$ из $\overline{P}$ принадлежит M. Если $c = 0$, то $\gamma = 0$ и, таким образом, $\gamma \in M$. Пусть $c \neq 0$. Имеем $\overline{(c, m)} \cdot \overline{(m, 1)} = \overline{(cm, m)}$. Следовательно, класс γ есть частное двух классов из Z_0, а поэтому входит в M. $\boxtimes$

4.4.2 Категоричность аксиоматической теории рациональных чисел

Теорема 4.9. *Аксиоматическая теория рациональных чисел категорична.*

Доказательство. В предположении, что аксиоматическая теория рациональных чисел непротиворечива, докажем, что любые две модели, на которых выполняются все 15 аксиом нашей теории, изоморфны.

Пусть $\langle Q_1, +, \cdot, 0_1, Z_1, +, \cdot\rangle$ и $\langle Q_2, \oplus, \odot, 0_2, Z_2, \oplus, \odot\rangle$ — две модели нашей теории. Так как любые кольца целых чисел изоморфны, то существует изоморфное отображение φ кольца $\langle Z_1, +, \cdot\rangle$ на кольцо $\langle Z_2, \oplus, \odot\rangle$. Но по теореме 4.4 любой элемент из Q_1 представим в виде частного элементов из Z_1, а любой элемент из Q_2 — в виде частного элементов из Z_2. Этим воспользуемся для задания изоморфного отображения f первой системы на вторую.

Пусть $q_1 \in Q_1$, тогда существуют $k_1, l_1 \in Z_1$ такие, что $q_1 = \dfrac{k_1}{l_1}$.

Полагаем, что $f(q_1) = \dfrac{\varphi(k_1)}{\varphi(l_1)} \in Q_2$, а $\varphi(k_1), \varphi(l_1) \in Z_2$.

Если элементы m_1 и n_1 из Z_1 обладают свойством, что $\dfrac{k_1}{l_1} = \dfrac{m_1}{n_1}$. Тогда $k_1 n_1 = m_1 l_1$. Кроме этого

$$\varphi(k_1) \odot \varphi(n_1) = \varphi(k_1 n_1) = \varphi(m_1 l_1) = \varphi(m_1) \odot \varphi(l_1).$$

Поэтому $\dfrac{\varphi(k_1)}{\varphi(l_1)} = \dfrac{\varphi(m_1)}{\varphi(n_1)}$.

Покажем, что отображение f является сюръекцией.

Для любого элемента $q_2 \in Q_2$ можно найти такие элементы k_2 и l_2 из Z_2, что $q_2 = \dfrac{k_2}{l_2}$. Отображение φ взаимнооднозначно переводит Z_1 в Z_2, поэтому существуют элементы $k_1, l_1 \in Z_1$ такие, что $k_2 = \varphi(k_1)$, $l_2 = \varphi(l_1)$. Поэтому $q_2 = \dfrac{\varphi(k_1)}{\varphi(l_1)} = f\left(\dfrac{k_1}{l_1}\right) = f(q_1)$, т.е. для элемента $q_2 \in Q_2$ существует элемент $\dfrac{k_1}{l_1} \in Q_1$, являющийся его прообразом. Это означает, что f — сюръекция.

Покажем, что если образы равны, то равны и их прообразы, т.е. если $f(q_1) = f(q_2)$, то $q_1 = q_2$.

Рассмотрим $f(q_1) = f\left(\dfrac{k_1}{l_1}\right) = \dfrac{\varphi(k_1)}{\varphi(l_1)} = f\left(\dfrac{m_1}{n_1}\right) = \dfrac{\varphi(m_1)}{\varphi(n_1)}$.

Имеем $\varphi(k_1) \odot \varphi(n_1) = \varphi(m_1) \odot \varphi(l_1)$. Так как φ — изоморфное отображение Z_1 на Z_2, то $\varphi(k_1 n_1) = \varphi(m_1 l_1) \Rightarrow k_1 n_1 = m_1 l_1$. Следовательно, $\dfrac{k_1}{l_1} = \dfrac{m_1}{n_1}$. Это означает, что равные образы имеют равные прообразы. Значит отображение f является однозначным соответствием.

Покажем, что

1) $(\forall g_1, q_1 \in Q)\ f(g_1 + q_1) = f(g_1) \oplus f(q_1)$;
2) $(\forall g_1, q_1 \in Q)\ f(g_1 \cdot q_1) = f(g_1) \odot f(q_1)$.

Возьмем $g_1 = \dfrac{k_1}{l_1}$ и $q_1 = \dfrac{m_1}{n_1}$.

Имеем

$$f\left(\frac{k_1}{l_1} + \frac{m_1}{n_1}\right) = f\left(\frac{k_1 n_1 + m_1 l_1}{l_1 n_1}\right) = \frac{\varphi(k_1 n_1 + m_1 l_1)}{\varphi(l_1 n_1)} = \frac{\varphi(k_1 n_1) \oplus \varphi(m_1 l_1)}{\varphi(l_1) \odot \varphi(n_1)} =$$

$$= \frac{\varphi(k_1) \odot \varphi(n_1) \oplus \varphi(m_1)\varphi(l_1)}{\varphi(l_1) \odot \varphi(n_1)} = \frac{\varphi(k_1) \odot \varphi(n_1)}{\varphi(l_1) \odot \varphi(n_1)} \oplus \frac{\varphi(m_1)\varphi(l_1)}{\varphi(l_1) \odot \varphi(n_1)} =$$

$$= \frac{\varphi(k_1)}{\varphi(l_1)} \oplus \frac{\varphi(m_1)}{\varphi(n_1)} = f\left(\frac{k_1}{l_1}\right) \oplus f\left(\frac{m_1}{n_1}\right).$$

$$f\left(\frac{k_1}{l_1} \cdot \frac{m_1}{n_1}\right) = f\left(\frac{k_1 \cdot m_1}{l_1 \cdot n_1}\right) = \frac{\varphi(k_1 \cdot m_1)}{\varphi(l_1 \cdot n_1)} = \frac{\varphi(k_1) \odot \varphi(m_1)}{\varphi(l_1) \odot \varphi(n_1)} =$$

$$= \frac{\varphi(k_1)}{\varphi(l_1)} \odot \frac{\varphi(m_1)}{\varphi(n_1)} = f\left(\frac{k_1}{l_1}\right) \odot f\left(\frac{m_1}{n_1}\right).$$

Далее, рассуждая, как при доказательстве теоремы 3.8, получим, что f — изоморфизм одной модели на другую. $\boxtimes$

4.5 Вопросы и задания для самоконтроля

1. Какая алгебра называется системой рациональных чисел?

2. Из каких аксиом следует, что $\langle Q, +, \cdot \rangle$ является полем?

3. Из какой аксиомы вытекает, что уравнение $ax = b$, где $a \neq 0$ имеет единственное решение в Q?

4. Из какой аксиомы следует, что для любого элемента $a \in Q$ существует противоположный элемент?

5. Докажите, что уравнение $x^2 = 2$ не имеет решений в поле рациональных чисел.

6. Докажите, что уравнение $x^2 = p$, где p — простое число, не имеет решений в поле рациональных чисел.

РАЗДЕЛ 5
СИСТЕМА ДЕЙСТВИТЕЛЬНЫХ ЧИСЕЛ

5.1 Введение

Ещё древнегреческие математики обнаружили существование несоизмеримых отрезков (это значит, что один из них не может быть составлен ни из какого целого числа равных между собой частей другого).

Таковыми являются, например, сторона квадрата и его диагональ. Понимание этого, с нашей современной точки зрения, можно расценить как признание существования иррациональных чисел, например $\sqrt{s}$.

Начиная с XV и XVI вв. по мере увеличения интереса к алгебраическим уравнениям математикам всё чаще приходилось иметь дело с выражениями, полученными из исходных чисел при помощи таких операций (извлечение корней), здесь очевидным образом нельзя было приписывать им рациональных значений. По существу это означало введение иррациональных чисел.

Только во второй половине XIX века была определена система вещественных чисел. Построение полной системы определений и рассуждений было выполнено Дедекиндом. Почти в то же самое время другие математики (Мере, Кантор, Вейерштрасс) нашли другие обоснования теории вещественных чисел. Опираясь на другие исходные понятия, каждый из них осуществил построение теории, по существу эквивалентной теории Дедекинда.

5.2 Предварительные замечания

Пусть P— упорядоченное поле.

Определение 5.1. *Элемент $a \in P$ называется предделом бесконечной последовательности $\{a_n\}$ элементов из этого поля P, если для любого $\varepsilon \in P, \varepsilon > 0$ существует такое натуральное число $n_0 \in N$, что для любого натурального числа $n \geq n_0$ выполнятеся $|a_n - a| < \varepsilon$.*

Определение 5.2. *Если бесконечная последовательность $\{a_n\}_n$ элементов упорядоченного поля P имеет предел, то она называется сходящейся.*

Определение 5.3. *Упорядоченное поле P называется полным, если всякая фундаментальная последовательность этого поля сходится в этом поле.*

Определение 5.4. *Бесконечная последовательность $\{a_n\}$ элементов упорядоченного поля P называется фундаментальной, если для любого $\varepsilon \in P, \varepsilon > 0$ существует такое натуральное число $n_0 \in N$, что для любых натуральных числел $n \geq n_0$ и $k \geq n_0$ выполнятеся $|a_n - a_k| < \varepsilon$.*

Определение 5.5. *Системой действительных чисел называется полное архимедово упорядоченное поле.*

В поле рациональных чисел разрешимы уравнения $a+x=b$ и $ax=b$ $(a\neq 0)$. Однако и рациональных чисел недостаточно для решения многих, даже элементарных задач. В частности, их недостаточно для решения квадратных уравнений $x^2=a$, где $a>0$. В самом деле, в поле рациональных чисел Q уравнение $x^2=2$ не имеет решения, т.е. нет такого рационального числа $\frac{p}{q}$, что $\left(\frac{p}{q}\right)^2=2$. Чтобы это доказать, предположим противное. Пусть существует такое рациональное число $\frac{p}{q}$, что $\left(\frac{p}{q}\right)^2=2$. Число $\frac{p}{q}$, очевидно, не может быть целым. Будем считать, что $\frac{p}{q}$ — несократимая дробь, т.е., что числа p и q — взаимно простые (этого всегда можно достичь, сократив дробь на наибольший общий делитель числителя и знаменателя). Из равенства $\left(\frac{p}{q}\right)^2=2$ вытекает, что $p^2=2q^2$ и, следовательно, p — четное число. Пусть $p=2r$, где r — целое число. Тогда имеем $4r^2=2q^2$, $2r^2=q^2$ и поэтому q также должно быть четным числом. Но p и q не могут одновременно быть четными числами, так как они взаимно простые. Таким образом, предположение, что уравнение $x^2=2$ имеет в поле рациональных чисел решение, приводит

к противоречию и поэтому оно неверно.

Рациональных чисел недостаточно также и для решения такой задачи, как измерение величин. Например, длина диагонали квадрата, сторона которого равна единице длины, не может быть выражена никаким рациональным числом $\frac{p}{q}$, так как в противном случае квадрат этой длины $\left(\frac{p}{q}\right)^2$ равнялся бы 2, что, по доказанному выше, невозможно.

Естественно возникает вопрос о дальнейшем расширении запаса чисел, имеющегося в нашем распоряжении, иными словами о расширении поля рациональных чисел Q.

Мы аксиоматически определим поле, которое будет расширением поля Q и в котором любое уравнение вида $x^2 = a$ $(a > 0)$ будет иметь решение. Однако в определении этого поля о разрешимости уравнения $x^2 = a$ $(a > 0)$ ничего говориться не будет; в основу определения будет положено другое требование. Это поле называют полем действительных чисел.

Прежде чем перейти к определению поля действительных чисел, введем понятия, которыми в дальнейшем нам придется пользоваться.

Пусть P — любое упорядоченное множество, а E — некоторое подмножество множества P.

Определение 5.6. *Множество E называется ограниченным снизу,*

если существует такой элемент $p \in P$, что все элементы множества E не меньше p; элемент p в этом случае называется нижней гранью множества E. Множество E называется ограниченным сверху, если существует элемент $p' \in P$ такой, что все элементы множества E не больше p'; элемент p' называется верхней гранью множества E. Множество E называется ограниченным, если оно ограничено одновременно и снизу и сверху.

Примеры. 1. Множество натуральных чисел N ограничено снизу, так как существует, например, число 0, которое меньше любого натурального числа.

2. Множество N, как известно, не ограничено сверху.

3. Множество целых отрицательных чисел ограничено сверху, так как каждое отрицательное число меньше 0, и не ограничено снизу.

4. Множество положительных дробей, в каждой из которых числитель и знаменатель — натуральные числа и числитель меньше знаменателя, ограничено и снизу и сверху: каждая такая дробь больше 0 и меньше 1.

Если элемент p является нижней гранью множества E, то и всякий элемент $p_1 \in P$, меньше p, также будет нижней гранью этого множества. Аналогично, если элемент p' является верхней гранью множества E, то и всякий элемент p'_1 при больше p' также будет верхней гранью множества E.

Таким образом, если множество E некоторых элементов упорядоченного множества P ограничено снизу, то оно может иметь бесконечное множество нижних граней, а если множество E ограничено сверху, то оно может иметь в P бесконечное множество верхних граней.

Определение 5.7. *Элемент $a \in P$ называется точной нижней гранью множества E, если:*

1) *любой элемент x множества E не меньше a, т.е. $x \geq a$;*

2) *не существует в P элемента $a_1 > a$, который обладал бы свойством, что $x \geq a_1$ для любого элемента x множества E.*

Элемент $b \in P$ называют точной верхней гранью множества E, если:

1) *любой элемент x множества E не больше b, т.е. $x < b$;*

2) *не существует в P элемента $b_1 < b$, который обладал бы свойством, что $x \leq b_1$ для всякого элемента x множества E.*

Примеры. 1. Число 0 является точной верхней гранью множества всех отрицательных рациональных чисел и точной нижней гранью множества всех положительных рациональных чисел.

2. Число -1 является точной верхней гранью множества всех целых отрицательных чисел.

3. Число 1 является точной нижней гранью множества всех натуральных чисел.

Точную верхнюю грань множества E обозначают $\sup E$ (читают «супремум E»), а точную нижнюю грань — символом $\inf E$ (читают «инфимум E»). Как видно из приведенных примеров, точная верхняя и точная нижняя грани множества в одних случаях принадлежат множеству, в других — не принадлежат ему.

Очевидно, когда множество E имеет точную верхнюю грань, то оно ограничено сверху, а когда имеет точную нижнюю грань, то ограничено снизу.

5.3 Аксиоматическое построение поля действительных чисел

Определение 5.8. *Полем действительных чисел называется любое упорядоченное поле, в котором каждое ограниченное сверху подмножество его элементов имеет точную верхнюю грань.*

Будем обозначать поле действительных чисел символом R. Элементы поля будем называть действительными числами.

Определение поля действительных чисел сформулировано нами в сжатой форме. На самом же деле оно состоит из аксиом, определяющих поле, аксиом упорядоченности и аксиомы точной верхней грани. Сформулируем определение поля действительных чисел в развернутом виде.

Первичные термины R:

1) R — множество, его элементы называются действительными числами;

2) $+, \cdot$ — бинарные операции сложения и умножения в R;

3) 0 и 1 — нуль и единица, элементы R;

4) $>$ — бинарное отношение в R.

Аксиомы системы $R = \langle R, +, \cdot, 0, 1, > \rangle$ разбиваются на 3 группы и формируются следующим образом:

I. Аксиомы поля:

R_1. $(\forall a, b \in R)(\exists! c \in R)\ a + b = c$
R_2 $(\forall a, b, c \in R)\ (a + b) + c = a + (b + c)$.
R_3. $(\forall a, b \in R)\ a + b = b + a$.
R_4. $(\exists 0 \in R)\ (\forall a \in R)\ a + 0 = a$.
R_5. $(\forall a \in R)(\exists a' \in R)\ a + a' = 0$.
R_6. $(\forall a, b \in R)(\exists! p \in R)\ a \cdot b = p$.
R_7. $(\forall a, b, c \in R)\ (ab)c = a(bc)$.
R_8. $(\forall a, b \in R)\ ab = ba$.
R_9. $(\forall a, b, c \in R)\ (a + b)c = ac + bc$.
R_{10}. $(\exists 1 \in R, 1 \neq 0)\ (\forall a \in R)\ a \cdot 1 = a$.
R_{11}. $(\forall a \in R, a \neq 0)(\exists a' \in R)\ aa' = 1$.

II. Аксиомы упорядоченности поля:

R_{12}. $(\forall a, b \in R)\ a \neq b \Rightarrow a > b \vee b > a$.
R_{13}. $(\forall a \in R)\ \rceil(a > a)$.
R_{14}. $(\forall a, b, c \in R)\ (a > b) \wedge (b > c) \Rightarrow a > c$.
R_{15}. $(\forall a, b, c \in R)\ a > b \Rightarrow a + c > b + c$.
R_{16}. $(\forall a, b, c \in R, c > 0)\ (a > b) \Rightarrow a \cdot c > b \cdot c$.

III. Аксиома точной верхней грани:

R_{17}. Для любой фундаментальной последовательности $\{a_n\}_n$ элементов R сущесвует в R элемент α такой, что $\lim\limits_{n\to\infty} a_n = \alpha$.

5.4 Свойства действительных чисел

Теорема 5.1. (Принцип Архимеда) *Для любых действительных чисел a и b, где $a > 0$, существует такое натуральное число n, что $na > b$.*

Доказательство. Предположим, что в поле действительных чисел R принцип Архимеда не выполняется. Тогда существуют действительные числа $a > 0$ и $b > 0$ такие, что при любом натуральном n справедливо неравенство $na < b$. Таким образом, множество A всех действительных чисел вида na, ограничено сверху, и поэтому, по аксиоме точной верхней грани, оно имеет точную верхнюю грань ε. Так как ε — точная верхняя грань множества $A = \{na\}$, то, по определению точной верхней грани, среди чисел вида na существует число $pa > \varepsilon - a$. Отсюда вытекает, что $(p+1)a > \varepsilon$, а это противоречит тому, что ϵ — точная верхняя грань множества $A = \{na\}$. Следовательно, предположение, что в поле действительных чисел R принцип Архимеда не выполняется, приводит к противоречию, и поэтому оно неправильно.

В частности, если $a = 1$, получаем: для любого $b \in R$ существует такое натуральное n, что $n > b$. Упорядоченное поле, в котором выполняется принцип Архимеда, называют архимедовски упорядоченным. Таким образом, поле действительных чисел R является архимедовски упорядоченным. ⊠

Из теоремы 5.1 вытекает следующее следствие.

Следствие 5.1. *Для любых действительных чисел $a > 0$ и $b > 0$ существует такое натуральной число n, что $\frac{b}{n} = a$.*

Доказательство. В самом деле, существует такое натуральное число n, что $n > \frac{b}{a}$. Умножив это неравенство на $\frac{a}{n}$, получим $\frac{b}{n} < a$. ⊠

Пусть a и b — произвольные числа, причем $a < b$. Совокупность всех действительных чисел x, которые удовлетворяют двойному неравенству $a \leq x \leq b$, называют *отрезком* или *сегментом*, и обозначают символом $[a; b]$. Числа a и b называют соответственно левым и правым концами сегмента. Совокупность всех действительных чисел x, удовлетворяющих неравенствам $a < x < b$, называют *интервалом с левым концом a и правым концом b* и обозначают символом $(a; b)$. Совокупность действительных чисел x, удовлетворяющих неравенствам $a < x \leq b$ и $a \leq x < b$, называют *полуинтервалами*, или *полусегментами*, и обозначают соответственно символами $(a; b]$, $[a; b)$. Отрезки, интервалы и полуинтервалы называют промежутками.

Теорема 5.2. *Каждый интервал $(a; b)$ содержит рациональное число.*

Доказательство. Пусть $h = b - a > 0$. Тогда, в силу следствия из принципа Архимеда, существует натуральное число n такое, что $\frac{1}{n} = h$.

В силу принципа Архимеда, существует такое натуральное число l, что $l \cdot \frac{1}{n} > |a|$. Следовательно, $(-l) \cdot \frac{1}{n} < a < l \cdot \frac{1}{n}$. Среди целых чисел $-l, -(l-1), ..., -1, 0, 1, 2, ..., l$, очевидно, существует такое число m, что $m \cdot \frac{1}{n} \le a < (m+1) \cdot \frac{1}{n}$, т.е. $\frac{m}{n} \le a < \frac{m+1}{n}$. Из неравенств $\frac{m}{n} \le a < \frac{m+1}{n}$ вытекает, что $\frac{m+1}{n} - a \le \frac{m+1}{n} - \frac{m}{n}$ и, следовательно, $\frac{m+1}{n} < b$. Таким образом, $a < \frac{m+1}{n} < b$, т.е. $\frac{m+1}{n} \in (a, b)$. $\boxtimes$

Из теоремы 5.2 вытекает, что в интервале $(a; b)$ содержится бесконечное множество рациональных чисел. В самом деле, применяя изложенные только что рассуждения к интервалам $\left(a; \frac{m+1}{n}\right)$ и $\left(\frac{m+1}{n}, b\right)$, получим новые рациональные числа $\frac{p}{q}$ такое, что $a < \frac{p}{q} < \frac{m+1}{n}$, и $\frac{r}{s}$ такое, что $\frac{m+1}{n} < \frac{r}{s} < b$. Этот процесс можно продолжать неограниченно.

Определение 5.9. *Корнем n-й степени из действительного числа a (n — любое натуральное число) называют такое действительное число b, что $b^n = a$. Корень n-й степени из числа a обозначают символом $\sqrt[n]{a}$. Следовательно, если $b = a^n$, то $b = \sqrt[n]{a}$.*

Теорема 5.3. *Для любого действительного числа $a > 0$ и любого натурального числа n существует одно и только одно такое действительное число $b > 0$, что $b^n = a$, т.е. $-\sqrt[n]{a}$ имеет одно и только одно положительное значение b.*

Положительный действительный корень n-й степени из положительного действительного числа a называют *арифметическим корнем* или *арифметическим значением корня n-й степени* из числа a. Заметим, что когда число n-четное, то кроме арифметического значения b существует также, и притом только одно, отрицательное значение $-b$ корня n-й степени из действительного числа $a > 0$.

Если же n — нечетное, то $\sqrt[n]{a}$ отрицательных значений не имеет. Таким образом, каждое уравнение вида $x^n = a$ $(a > 0)$, в частности и уравнение $x^2 = a$, решается в поле действительных чисел. При n четном оно имеет два решения: $\sqrt[n]{a}$ и $-\sqrt[n]{a}$, а при n нечетном — одно решение $\sqrt[n]{a}$.

Алгоритм извлечения квадратного корня

Пусть нужно извлечь квадратный корень из натурального числа m, причем известно, что корень извлекается.

1. Разобьем число m на грани (справа налево, начиная с последней цифры), включив в каждую грань по две рядом стоящие цифры. При этом следует учесть, что если m состоит из четного числа цифр, то в первой (слева) грани будет две цифры; если же число m состоит из

нечетного числа цифр, то первая грань состоит из одной цифры. Количество граней показывает количество цифр результата.

2. Подбираем наибольшую цифру, такую, что ее квадрат не превосходит числа, находящегося в первой грани; эта цифра — первая цифра результата.

3. Возведем первую цифру результата в квадрат, вычтем полученное число из первой грани, припишем к найденной разности справа вторую грань. Получится некоторое число A. Удвоив имеющуюся часть результата, получим число a. Теперь подберем такую наибольшую цифру x, чтобы произведение числа $\overline{ax}$ (запись $\overline{ax}$ означает $10 \cdot a + x$) на x не превосходило числа A. Цифра x — вторая цифра результата.

4. Произведение числа $\overline{ax}$ на x вычтем из числа A, припишем к найденной разности справа третью грань, получится некоторое число B. Удвоив имеющуюся часть результата, получим число b. Теперь подберем такую наибольшую цифру y, чтобы произведение числа $\overline{by}$ на y не превосходило числа B. Цифра y — третья цифра результата.

Далее повторяем 4-й шаг. Это продолжается до тех пор, пока не используется последняя грань.

Если корень не извлекается, то после последней цифры заданного числа ставят запятую и образуют дальнейшие грани, каждая из которых имеет вид 00. В этом случае процесс извлечения корня бесконечен; он прекращается, когда достигается требуемая точность.

Пример. Вычислить $\sqrt{138384}$.

Решение. Разобьем число на грани: $13'83'84$ — их три, значит, в результате должно получиться трехзначное число. Первая цифра результата 3, так как $3^2 < 13$, тогда как $4^2 > 13$. Вычтя 9 из 13, получим 4. Приписав к 4 следующую грань, получим $A = 483$. Удвоив имеющуюся часть результата, т.е. число 3, получим $a = 6$. Подберем теперь такую наибольшую цифру x, чтобы произведение двузначного числа $\overline{ax}$ на x было меньше числа 483. Такой цифрой будет 7, так как $67 \cdot 7 = 469$ меньше 483, тогда как $68 \cdot 8 = 544$ это больше 483. Итак, вторая цифра результата 7. Вычтя 469 из 483, получим 14. Приписав к этому числу справа последнюю грань, получим $b = 1484$. Удвоив имеющуюся часть результата, т.е. число 37, получим $B = 74$. Подберем теперь такую наибольшую цифру y, чтобы произведение трехзначного числа $\overline{by}$ на y не превосходило 1484. Такой цифрой будет 2, так как $742 \cdot 2 = 1484$. Цифра 2 — последняя цифра результата. В ответе получили 372.

Теорема 5.4. *Каким бы ни было действительное число a, всегда найдется такое целое число m, и притом только одно, что будут выполняться неравенства $m \leq a < m + 1$.*

5.5 Позиционная десятичная запись дейтсвительных чисел

В практике применения действительных чисел, как правило, пользуются записью их в десятичной системе исчисления. Об этой записи и пойдет речь дальше.

Символическую запись $i_p i_{p-1} \ldots i_1 i_0, j_1 j_2 \ldots j_n \ldots$ называют *десятичной записью действительного числа*. Целое неотрицательное число $i_p i_{p-1} \ldots i_1 i_0$ называют *целой частью действительного числа*, а j_1, j_2, ..., j_n, ... называют соответственно *1-м, 2-м, ... k-м десятичным знаком действительного числа*.

Теорема 5.5. *Каждое действительное число a можно записать в виде бесконечной десятичной дроби, не имеющей девятки в периоде.*

Справедлива также и обратная теорема.

Теорема 5.6. *Каждая бесконечная десятичная дробь, которая не имеет девятки в периоде, является записью некоторого действительного числа a.*

Замечание. Бесконечная десятичная дробь с девяткой в периоде также определяет некоторое действительное число.

Выясним теперь, в чем проявляется рациональность или иррациональность действительного числа, если записать его в виде бесконечной десятичной дроби.

Каждое рациональное число записывается в виде либо конечной десятичной дроби, либо десятичной периодической дроби. Но каждую конечную десятичную дробь можно считать дробью периодической с цифрой 0 в периоде. Таким образом, каждое рациональное число записывается в виде периодической десятичной дроби. Каждое иррациональное число записывается в виде бесконечной непериодической дроби.

Под действительными числами подразумевают бесконечные десятичные дроби без девятки в периоде: под рациональными числами подразумевают десятичные периодические дроби, а под иррациональными — бесконечные, непериодические десятичные дроби.

Замечание. Бесконечные десятичные дроби без девятки в периоде можно рассматривать просто как определенные символы, образованные из цифр 0, 1, 2, ..., 9. На множестве всех этих символов можно так определить операции сложения и умножения и отношение строгого линейного порядка, что при этом будут выполняться все аксиомы поля действительных чисел, и, таким образом, на этом множестве будет реализоваться система аксиом поля действительных чисел.

Замечание. Между множеством действительных чисел и множеством всех точек направленной прямой можно установить взаимно однозначное соответствие, изоморфное относительно отношений порядка, заданных в поле действительных чисел и в множестве точек числовой прямой.

Алгоритм обращения бесконечной периодической десятичной дроби в обыкновенную дробь

Бесконечная периодическая дробь равна обыкновенной дроби, в числителе которой разность между всем числом после запятой и чсилом после запятой до периода, а знаменатель состоит из «девяток» и «нулей», причем «девяток» столько, сколько цифр в периоде, а «нулей» столько, сколько цифр после запятой до периода.

Например, обратим в обыкновенную дробь число $0,41(6)$. В числителе обыкновенной дроби запишем разность между всем числом после запятой (416) и числом после запятой до периода дроби (41). В периоде одна цифра, а после запятой до периода две цифры, поэтому знаменатель будет состоять из одной девятки и двух нулей (900):

$$0,41(6) = \frac{416 - 41}{900} = \frac{375}{900} = \frac{5}{12}.$$

5.6 Категоричность и непротиворечивость аксиоматической теории действительных чисел

5.6.1 Непротиворечивость аксиоматической теории действительных чисел

Теорема 5.7. *Аксиоматическая теория действительных чисел непротиворечива.*

Доказательство. Докажем непротиворечивость аксиоматической теории R относительно аксиоматической теории Q.

Построим модель, на которой выполняются все 17 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

$$\{a_n\}_n + \{b_n\}_n = \{a_n + b_n\}_n,$$

$$\{a_n\}_n \cdot \{b_n\}_n = \{a_n \cdot b_n\}_n.$$

Таким образом, на F введены бинарные алгебраические операции сложения и умножения.

Покажем, что F — коммутативное кольцо с единицей.

Сложение на F ассоциативно, т.к. для любых последовательностей $\{a_n\}_n, \{b_n\}_n, \{c_n\}_n \in F$ имеем

$$(\{a_n\}_n + \{b_n\}_n) + \{c_n\}_n = \{a_n + b_n\}_n + \{c_n\}_n = \{a_n + b_n + c_n\}_n =$$

$$= \{a_n\}_n + \{b_n + c_n\}_n = \{a_n\}_n + (\{b_n\}_n + \{c_n\}_n).$$

Аналогично доказывается, что сложение на F коммутативно.

В F есть нуль: им является стационарная последовательность $\{0\}_n$.

Для любой последовательности $\{a_n\}_n \in F$ в F существует противоположный элемент, это последовательность $\{-a_n\}_n$. Действительно,

$$\{a_n\}_n + \{-a_n\}_n = \{a_n - a_n\}_n = \{0\}_n.$$

Значит, F — абелева группа по сложению.

Группа F является группой с сокращением, т.к. для любых последовательностей $\{a_n\}_n, \{b_n\}_n, \{c_n\}_n \in F$ из $\{a_n\}_n + \{c_n\}_n = \{b_n\}_n + \{c_n\}_n$ следует, что $\{a_n + c_n\}_n = \{b_n + c_n\}_n$. А так как Q — группа с сокращением, то $a_n = b_n$, поэтому $\{a_n\}_n = \{b_n\}_n$.

Нетрудно показать, что умножение на F ассоциативно и коммутативно. Следовательно, $\langle F, +, \cdot \rangle$ — абелева полугруппа по умножению.

На F выполняется дистрибутивный закон, так как для любых последовательностей $\{a_n\}_n, \{b_n\}_n, \{c_n\}_n \in F$ имеем

$$(\{a_n\}_n + \{b_n\}_n) \cdot \{c_n\}_n = \{a_n + b_n\}_n \cdot \{c_n\}_n = \{\{a_n + b_n\}_n \cdot c_n\}_n =$$

$$= \{a_n \cdot c_n + b_n \cdot c_n\}_n = \{a_n \cdot c_n\}_n + \{b_n \cdot c_n\}_n = \{a_n\}_n \cdot \{c_n\}_n + \{b_n\}_n \cdot \{c_n\}_n.$$

Значит, $\langle F, +, \cdot \rangle$ — коммутативное кольцо. Единицей в F служит стационарная последовательность $\{1\}_n$.

2. Введём отношение ρ в F следующим образом:

$$\{a_n\}_n \rho \{b_n\}_n \text{ относительно поля } Q, \text{ если } \{a_n - b_n\}_n \to 0.$$

Легко проверить, что ρ рефлексивно, симметрично и транзитивно. Поэтому отношение в ρ является отношением эквивалентности (обозначается $\sim$) и, поэтому, оно разбивает множество F на непустые попарно непересекающиеся классы, объединение которых даёт F.

Будем обозначать класс эквивалентности α, в который входит последовательность $\{a_n\}_n$, символом $\overline{\{a_n\}}_n$, т.е. $\alpha = \overline{\{a_n\}}_n$.

Если $\beta = \overline{\{b_n\}}_n$, то $\alpha = \beta \Leftrightarrow \{a_n\}_n \sim \{b_n\}_n$.

Введём сложение и умножение классов:

$$\overline{\{a_n\}}_n + \overline{\{b_n\}}_n = \overline{\{a_n + b_n\}}_n,$$

$$\overline{\{a_n\}}_n \cdot \overline{\{b_n\}}_n = \overline{\{a_n \cdot b_n\}}_n.$$

Пусть $\varphi : F \to \overline{F}$ — отображение, построенное по закону:

$$(\forall \{a_n\}_n \in F)\ \varphi(\{a_n\}_n) = \overline{\{a_n\}}_n.$$

Покажем, что φ — гомоморфизм F на $\overline{F}$. Для любых последовательностей $\{a_n\}_n, \{b_n\}_n \in F$ имеем

$$\varphi(\{a_n\}_n + \{b_n\}_n) = \varphi(\{a_n + b_n\}_n) = \overline{\{a_n + b_n\}}_n =$$

$$= \overline{\{a_n\}}_n + \overline{\{b_n\}}_n = \varphi(\{a_n\}_n) + \varphi(\{b_n\}_n).$$

Аналогично доказывается,

$$(\forall\{a_n\}_n, \{b_n\}_n \in F)\ \varphi(\{a_n\}_n \cdot \{b_n\}_n) = \varphi(\{a_n\}_n) \cdot \varphi(\{b_n\}_n).$$

Следовательно, φ — гомоморфизм кольца F на множество $\overline{F}$. Поэтому система $\langle \overline{F}, +, \cdot \rangle$ является коммутативным кольцом с единицей.

Итак, построена интерпретация, на которой выполняются первые 10 аксиом нашей теории.

3. Покажем, что $\langle \overline{F}, +, \cdot \rangle$ — 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 $\{0\}_n$, т.е. класс $\overline{\{0\}}_n$, а единица — класс $\overline{\{1\}}_n$.

Пусть класс $\alpha = \overline{\{a_n\}}_n$ не является нулём кольца $\langle \overline{F}, +, \cdot \rangle$. В таком случае последовательности $\{a_n\}_n$ и $\{0\}_n$ не эквивалентны и, следовательно, последовательность $\{a_n\}_n$ не сходится к нулю. Поэтому существует $\varepsilon \in Q$ и подпоследовательность $\{a_{k_n}\}_n$ последовательности $\{a_n\}_n$ такие, что для любого $n \in N$ спарведливо $|a_{k_n}| \geq \varepsilon$.

Известно, что если последовательность сходится по норме к a то и её подпоследовательность тоже сходится по норме к a. А это означает, что $\{a_n\}_n \sim \{a_{k_n}\}_n$ и, следовательно, $\alpha = \overline{\{a_n\}}_n = \overline{\{a_{k_n}\}}_n$. Кроме того, так как $\{a_{k_n}\}_n$ — фундаментальна, то последовательность $\left\{\dfrac{1}{a_{k_n}}\right\}_n$ — тоже,

и, значит, $\left\{\dfrac{1}{a_{k_n}}\right\}_n \in F$.

Пусть $\gamma = \overline{\left\{\dfrac{1}{a_{k_n}}\right\}_n}$. Нетрудно видеть, что

$$\alpha \cdot \gamma = \overline{\{a_{k_n}\}}_n \cdot \overline{\left\{\frac{1}{a_{k_n}}\right\}}_n = \overline{\left\{a_{k_n} \cdot \frac{1}{a_{k_n}}\right\}}_n = \overline{\{1\}}_n.$$

Значит, для любого $\alpha \in \overline{F}$ существует $\gamma \in \overline{F}$, что $\alpha \cdot \gamma = \overline{\{1\}}_n$. Следовательно, система $\langle \overline{F}, +, \cdot \rangle$ — поле.

4. Введем в поле $\langle \overline{F}, +, \cdot \rangle$ линйный порядок. Положительную часть $\overline{F}^+$ определим условием

$$\alpha \in \overline{F}^+ \Leftrightarrow (\exists \varepsilon \in Q^+)\ (\exists n \in N)\ (\forall n \in N)\ n \geq n_0 \Rightarrow a_n \geq \varepsilon.$$

Покажем прежде всего, что принадлежность класса α к $\overline{F}^+$ не заисит от выбора представителя класса. В самом деле, если $\{a_n\}_n \sim \{b_n\}_n$, то существует такое натуральное число n_1, что

$$(\forall n \in N)\ n \geq n_1 \Rightarrow |b_n - a_n| < \frac{1}{2}\varepsilon.$$

Поэтому

$$(\forall n \in N)\ n \geq \max\{n_0, n_1\} \Rightarrow b_n \geq a_n - \frac{1}{2}\varepsilon \geq \frac{1}{2}\varepsilon.$$

Далее, пусть класс α ненулевой. Поэтому либо α, либо $-\alpha$ принадлежит к $\overline{F}^+$. Наконец, совсем не трудно проверить, что

$$(\forall \alpha, \beta \in \overline{F}^+)\ \alpha + \beta \in \overline{F}^+;$$

$$(\forall \alpha, \beta \in \overline{F}^+)\ \alpha \cdot \beta \in \overline{F}^+.$$

Тем самым система $\langle \overline{F}, +, \cdot, \overline{F}^+ \rangle$ — упорядоченное поле. Полезно отметить следующее свойство, вытекающее из определения. Пусть $\alpha, \beta \in \overline{F}$, $\alpha = \overline{\{a_n\}}_n$, $\beta = \overline{\{b_n\}}_n$. Если существует натуральное число n_0 такое, что для любого натурального числа $n \geq n_0$ справедливо $a_n > b_n$, то $\alpha \geq \beta$. Покажем, что введенный порядок архимедов. Пусть $\alpha, \beta \in \overline{F}^+$. Тогда существуют $\varepsilon, c \in Q^+$ такие, что

$$(\exists n_0 \in N)\ (\forall n \in N)\ n \geq n_0 \Rightarrow a_n > \varepsilon \wedge c > b_n.$$

Так как порядок в поле рациональных чисел архимедов, то существует натуральное число k такое, что $k\varepsilon > c$. А в этом случае

$$(\forall n \in n)\ n \geq n_0 \Rightarrow k a_n > b_n,$$

а в силу отмеченного свойства $k\alpha \geq \beta$.

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 $\overline{F}$.

Сначала определим подмножество P множества $\overline{F}$. Элемент α множества $\overline{F}$ отнесем к P в том и только том случае, если класс α содержит стационарную последовательность, т.е. если для некоторого рационального a имеем $\alpha = \overline{\{a\}}_n$. Легко проверить, что отображение $a \to \overline{\{a\}}_n$ является изоморфным отображением поля рациональных чисел на систему $\langle P, +, \cdot \rangle$. Отсюда следует, что система $\langle P, +, \cdot \rangle$ — поле. Заметим, что $\overline{\{a\}}_n \in \overline{F}^{+}$ тогда и только тогда, если a — положительное рациональное число. Поэтому в указанной последовательности элементов одного поля отвечает фундаментальная последовательность элементов второго поля.

Пусть

$$\alpha_1, \alpha_2, ..., \alpha_k, ...; \ \alpha_k = \overline{\{a_k\}}_n - \tag{5.1}$$

какая-нибудь фундаментальная последовательность элементов поля P. В силу сделанного замечания последовательность

$$a_1, a_2, ..., a_k, ... - \tag{5.2}$$

фундаментальная последовательность рациональных чисел. Рассмотрим класс $\alpha = \overline{\{a_n\}}_n$ и докажем, что $\lim\limits_{k\to\infty} \alpha_k = \alpha$. Пусть $\varepsilon = \overline{\{e\}}_n$, где e — положительное рациональное число. Так как последовательность (5.2) фундаментальна, то существует натуральное число n_0 такое, что для

любого $k \geq n_0$

$$(\forall n \in N)\ n \geq n_0 \Rightarrow |a_k - a_n| < e.$$

отсюда следует, что

$$(\forall k \in N)\ k \geq n_0 \Rightarrow |\alpha_k - \alpha| \leq \varepsilon.$$

Другими словами последовательность (5.1) сходится к элемнту множества $\overline{F}$. Этим завершается доказательство теоремы. ⊠

5.6.2 Категоричность аксиоматической теории действительных чисел

Теорема 5.8. *Аксиоматическая теория действительных чисел категорична.*

Доказательство. В предположении, что аксиоматическая теория действительных чисел непротиворечива докажем, что любые две модели на которых выполняются все аксиомы R, являются изоморфными.

Пусть $\langle R, +, \cdot, 0\rangle$ и $\langle R_1, \oplus, \odot, 0\rangle$ — это две модели системы R. Известно, что поле $\langle R, +, \cdot, 0\rangle$ есть расширение поля рациональных чисел $\langle Q, +, \cdot, 0\rangle$, а поле $\langle R_1, \oplus, \odot, 0\rangle$ есть расширение $\langle Q_1, \oplus, \odot, 0\rangle$. По теореме 4.9 существует изоморфное отображение φ поля Q на поле Q_1. Кроме этого отношение $>$ является отношением порядка в Q, поле Q можно единственным образом упорядочить:

$$(\forall a, b \in Q)\ a > b \Leftrightarrow \varphi(a) > \varphi(b).$$

Рассмотрим последовательность $\{a_n\}_n$ элементов поля $\langle Q, +, \cdot, 0\rangle$. Эта последовательность фундаментальна, значит фундаментальной является и последовательность $\{\varphi(a_n)\}_n$.

Пусть α — какое-нибудь число поля $\langle R, +, \cdot, 0\rangle$. Тогда α есть предел некоторой последовательности $\{a_n\}_n$ элементов поля Q. Но эта последовательность фундаментальна, и, следовательно, последовательность $\{\varphi(a_n)\}_n$ фундаментальна и по определению поля действительных чисел сходится к некоторому элементу поля $\langle R_1, \oplus, \odot, 0\rangle$. Обозначим этот элемент через $f(\alpha)$. Покажем, что определенное так отображение f поля $\langle R, +, \cdot, 0\rangle$ в поле $\langle R_1, \oplus, \odot, 0\rangle$ есть взаимнооднозначное отображение множества R на R_1. Так как эквивалентные последовательности элементов поля Q при отображении φ переходят в эквивалентные последовательности элементов поля Q_1. Отсюда следует, что f — однозначное отображение множества R в R_1. 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 Q такие, что $\alpha = \lim\limits_{n\to\infty} a_n$ и $\beta = \lim\limits_{n\to\infty} b_n$. Тогда имеем $f(\alpha) = \lim\limits_{n\to\infty} \varphi(a_n)$ и $f(\beta) = \lim\limits_{n\to\infty} \varphi(b_n)$. Отсюда получим

$$\alpha + \beta = \lim_{n\to\infty} (a_n + b_n)$$

и

$$f(\alpha) \oplus f(\beta) = \lim_{n\to\infty} (\varphi(a_n) \oplus \varphi(b_n)).$$

А потому $f(\alpha) \oplus f(\beta) = f(\alpha + \beta)$, так как $\varphi(a_n) \oplus \varphi(b_n) = \varphi(a_n + b_n)$.

Аналогично получаем

$$\alpha \cdot \beta = \lim_{n\to\infty} (a_n \cdot b_n)$$

и

$$f(\alpha) \odot f(\beta) = \lim_{n\to\infty} (\varphi(a_n) \odot \varphi(b_n)).$$

А потому $f(\alpha) \odot f(\beta) = f(\alpha \cdot \beta)$, так как $\varphi(a_n) \odot \varphi(b_n) = \varphi(a_n \cdot b_n)$.

Таким образом f является изоморфным отображением. $\boxtimes$

5.7 Конечные и бесконечные цепные дроби

Определение 5.10. *Конечной цепной дробью называется выражение вида* $a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + ... + \cfrac{1}{a_n}}}$, *где* $a_i \in N, i = \overline{1,n}$, $a_0 \in Z$, $a_1 \neq 1$, *и обозначается* $\frac{a}{b} = [a_0; a_1, a_2, ..., a_n]$. *Элементы* a_i *называются элементами цепной дроби.*

Определение 5.11. *Отрезок цепной дроби от* a_0 *до* a_k *называется подходящей дробью k-го порядка для данной цепной дроби и обозначается* $A_k = [a_0; a_1, ..., a_k]$, $k \leq n$.

Замечание. Последняя подходящая дробь совпадает со всей дробью.

Теорема 5.9. *Всякое рациональное число* $\frac{a}{b}$ *можно однозначно представить в виде конечной цепной дроби. Причем элементами цепной дроби будут является неполные частные из алгоритма Евклида для чисел* a *и* b.

Доказательство. Пусть $\frac{a}{b} \in Q$, $a \in Z$, $b \in N$. Применим к числам a и b алгоритм Евклида:

$$a = ba_0 + r_1,\ 0 \le r_1 < b;$$

$$b = r_1a_1 + r_2,\ 0 \le r_2 < r_1;$$

$$r_1 = r_2a_2 + r_3,\ 0 \le r_3 < r_2;$$

$$\ldots$$

$$r_{n-2} = r_{n-1}a_{n-1} + r_n,\ 0 \le r_n < r_{n-1};$$

$$r_{n-1} = r_na_n.$$

Заметим, что $a_0 \in Z$, $a_i \in N$ $i = \overline{1,n}$.
Разделим первое равенство на b, второе на r_1 и т.д. Получим

$$\frac{a}{b} = a_0 + \frac{r_1}{b} = a_0 + \frac{1}{\frac{b}{r_1}};$$

$$\frac{b}{r_1} = a_1 + \frac{1}{\frac{r_2}{r_1}};$$

$$\frac{r_1}{r_2} = a_2 + \frac{1}{\frac{r_3}{r_2}};$$

$$\ldots$$

$$\frac{r_{n-2}}{r_{n-1}} = a_{n-1} + \frac{1}{\frac{r_{n-1}}{r_n}};$$

$$\frac{r_{n-1}}{r_n} = a_n.$$

Подставив в первое равенство последовательно все остальные получим

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots + \cfrac{1}{a_n}}}, \text{ где } a_i \in N, i = \overline{1,n}, a_0 \in Z, a_1 \neq 1$$

Единственность такого представления вытекает в силу однозначности деления с отстатком. ⊠

Замечание. Если в определении 5.10 допустить, что $a_n = 1$, то тогда представление рационального числа $\frac{a}{b}$ в виде конечной цепной дроби не единственно. Например, $\frac{11}{2} = 5 + \frac{1}{2}$ и $\frac{11}{2} = 5 + \cfrac{1}{1 + \cfrac{1}{1}}$.

Замечание. Из теоремы 5.9 следует алгоритм представления рационального числа в виде конечной цепной дроби.

Пусть α — произвольное иррациональное число. Алгоритм Евклида уже не применим для разложения α в цепную дробь. Вспоминая однако, что каждое неполное частное в конечной цепной дроби — это целая часть некоторого рационального числа, поступим следующим образом.

Положим $\alpha = [\alpha] + \varepsilon_0$, где $0 < \varepsilon_0 < 1$ (здесь $[r]$ — целая часть действительного числа r). Величину $[\alpha] \in Z$ обозначим через q_0 т.е.

$$\alpha = q_0 + \cfrac{1}{\cfrac{1}{\varepsilon_0}},$$

где $\frac{1}{\varepsilon_0} > 1$. Так как $\frac{1}{\varepsilon_0} = \left[\frac{1}{\varepsilon_0}\right] + \varepsilon_1 = q_1 + \varepsilon_1$, где $0 < \varepsilon_1 < 1$, то

$\alpha = q_0 + \cfrac{1}{q_1 + \cfrac{1}{\cfrac{1}{\varepsilon_1}}}$. Продолжая вычисления, получим, что

$$\alpha = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + ...}} = [q_0; q_1, q_2, ...], \ q_i \neq 0. \tag{5.3}$$

Замечание. Для любого $i \in N$ $q_i \neq 0$, так как в противном случае разложение (5.3) становится конечной цепной дробью, т.е. рациональным числом.

Таким образом, любое иррациональное число раскладывается единственным образом в цепную дробь вида (5.3), которую в дальнейшем будем называть бесконечной цепной дробью.

5.8 Вопросы и задания для самоконтроля

1. Какая последовательность называется
   ограниченной;
   фундаментальной;
   сходящейся?
2. Охарактеризуйте аксиомы группы I?
3. Охарактеризуйте аксиомы группы II?
4. Охарактеризуйте аксиому группы III?
5. Как доказать, что любое действительное число является пределом последовательности рациональных чисел?
6. Докажите, что для любого положительного действительного числа α уравнение $x^2 = \alpha$ имеет решение в поле действительных чисел.
7. Как представить действительное число в виде систематической дроби?
8. Как представить действительно число в виде бесконечной цепной дроби?

РАЗДЕЛ 6
СИСТЕМА КОМПЛЕКСНЫХ ЧИСЕЛ

6.1 Введение

Впервые мнимые величины появились в известном труде«Великое искусство, или об алгебраических правилах» Дж. Кардано (1545 год), который счёл их бесполезными, непригодными к употреблению. Пользу мнимых чисел, в частности, при решении кубического уравнения в так называемом неприводимом случае (когда действительные корни выражаются через кубические корни из мнимых величин) впервые оценил Р. Бомбелли (1572 год). Он же дал некоторые простейшие правила действий с комплексными числами.

Вообще выражения вида $a+b\sqrt{-1}$, $b \neq 0$, появляющиеся при решении квадратных и кубических уравнений, стали называть в 16-17 вв. мнимыми. Однако даже для многих крупных учёных 17 века алгебраическая и геометрическая сущность мнимых величин представлялась неясной и даже загадочной (мистической). И. Ньютон не включал мнимые числа в понятие числа, а Г. Лейбницу принадлежит фраза: «Мнимые числа — это прекрасное и чудесное убежище божественного духа, почти что амфибия бытия с небытиём».

Символ $i = \sqrt{-1}$ предложил Л.Эйлер. Он же высказал в 1751 году мысль об алгебраической замкнутости поля C. К такому же выводу при-

шёл и Д'аламбер, но строгое доказательство этого принадлежит Гауссу (1799 год).

Чисто арифметическая теория комплексных чисел, как пар действительных чисел, была построена У.Гамильтоном (1837 год). Ему же принадлежит и важное обобщение комплексных чисел — кватернионы.

6.2 Аксиоматическое построение поля комплексных чисел

Определение 6.1. *Системой комплексных чисел* называется *минимальное поле, которое является расширением поля действительных чисел, и в котором есть элемент i с условием $i^2 + 1 = 0$.*

Первичные термины.

1) C — множество, его элементы называются комплексными числами;
2) $+$, $\cdot$ — бинарные операции сложения и умножения на C;
3) 0, 1 и i — элементы C;
4) R — подмножество C, его элементы называются действительными числами;
5) $\oplus$, $\odot$ — бинарные операции сложения и умножения на R.

Аксиомы системы C делятся на 4 группы и могут быть сформулированны следующим образом:

A :

C_1. $(\forall a, b \in C)\ (\exists! c \in C)\ a + b = c$.
C_2. $(\forall a, b, c \in C)\ (a + b) + c = a + (b + c)$.
C_3. $(\forall a, b \in C)\ a + b = b + a$.
C_4. $(\exists 0 \in C)\ (\forall a \in C)\ a + 0 = a$.
C_5. $(\forall a \in C)\ (\exists a' \in C)\ a + a' = 0$.

C_6. $(\forall a, b \in C)\ (\exists! p \in C)\ ab = p$.
C_7. $(\forall a, b, c \in C)\ (ab)c = a(bc)$.
C_8. $(\forall a, b \in C)\ ab = ba$.
C_9. $(\forall a, b, c \in C)\ (a + b)c = ac + bc$.
C_{10}. $(\exists 1 \in C, 1 \neq 0)\ (\forall a \in C)\ a \cdot 1 = a$.
C_{11}. $(\forall a \in C, a \neq 0)\ (\exists a' \in C)\ aa' = 1$.

B :

C_{12}. $\langle R, \oplus, \odot, 0, 1\rangle$ — поле действительных чисел.
C_{13}. $R \subset C$.
C_{14}. $(\forall a, b \in R)\ a + b = a \oplus b$.
C_{15}. $(\forall a, b \in C)\ a \cdot b = a \odot b$.

C :

C_{16}. $(\exists i \in C)\ i^2 + 1 = 0$.

D (Аксиома минимальности):

C_{17}. Любое подмножество M множества C совпадает с C, если оно удовлетворяет четырем условиям:

$a)$ $R \subset M$;
$b)$ $i \in M$;
$c)$ $(\forall a, b \in M)\ a + b \in M$;
$d)$ $(\forall a, b \in M)\ a \cdot b \in M$.

6.3 Свойства комплексных чисел

Теорема 6.1. *Всякое комплексное число α можно единственным образом представить в виде $\alpha = a + bi$, $a, b \in R$.*

Доказательство. Возможность представления доказывается в алгебре.

Докажем единственность. Предположим обратное. Пусть $\alpha = a + bi$ и $\alpha = a_1 + b_1 i$, где $a, b, a_1, b_1 \in R$. Поскольку $\langle C, +, \cdot \rangle$ — поле, то из равенства $a + bi = a_1 + b_1 i$ следует, что $(b - b_1)i = a_1 - a$. Если $b \neq b_1$, то $i = \dfrac{a_1 - a}{b - b_1} \in R$. А этого быть не может, так как в любом линейно упорядоченном кольце квадрат любого не равного нулю элемента больше нуля. А $i^2 = -1 < 0$, следовательно $i \notin R$, где R — линейно упорядоченное поле. ⊠

Теорема 6.2. *Поле C нельзя линейно упорядочить.*

Доказательство. Это следует из теоремы, что в линейно упорядоченном кольце сумма квадратов его не равных нулю элементов не равна нулю.

В поле C имеем $i^2 + 1^2 = 0$. Поэтому поле C не является линейно упорядоченным. ⊠

6.4 Действия над комплексными числами

6.4.1 Алгебраическая форма комплексных чисел

Запись $a+bi$ называется *алгебраической формой комплексного числа*, число a — его *комплексной частью*, а bi — *мнимой частью*.

Сложение и умножение комплексных чисел в алгебраической форме выполняется следующим образом:

$$(a+bi)+(c+di)=(a+c)+(b+d)i;$$

$$(a+bi)\cdot(c+di)=(ac-bd)+(ad+bc)i.$$

В частности, при умножении комплексных чисел раскрываются скобки и i^2 заменяется на -1.

Для комплексного числа $z=a+bi$ комплексное число $a-bi$ называется *сопряженным* и обозначается $\overline{z}$. Итак, у сопряженных чисел дейтсвительные части совпадают, а мнимые — взаимно противоположны. Очевидно, что $z=\overline{z}$ тогда и только тогда когда z — действительное число.

При делении комплексных чисел делимое и делитель умножаются на число, сопряженной делителю:

$$\frac{a+bi}{c+di}=\frac{a+bi}{c+di}\cdot\frac{c-di}{c-di}=\frac{ac+bd-(ad-bc)i}{c^2+d^2}=\frac{ac+bd}{c^2+d^2}-\frac{ad-bc}{c^2+d^2}i.$$

Здесь надо считать, что $c+di\neq 0$, то есть $c\neq 0\neq d$.

В поле комплексных чисел разрешимо уравнение $x^2+1=0$. Его решениями являются числа i и $-i$. Поэтому в поле C существует квадратный корень из -1, а именно: $\sqrt{-1}=\pm i$. Отсюда следует, что в поле C существуют квадратные корни из отрицательных действительных чисел:

$$\sqrt{-a}=\sqrt{(-1)a}=\sqrt{-1}\cdot\sqrt{a}=\sqrt{a}.$$

Пусть теперь требуется извлечь квадратный корень из комплексного числа $z=a+bi$. Положим $x+yi=\sqrt{a+bi}$. Возведем обе части этого равенства в квадрат: $x^2-y^2+2xyi=a+bi$. Приравнивая действительные и мнимые части, получаем:

$$\begin{cases} x^2-y^2=a, \\ 2xy=b. \end{cases}$$

Возведем оба уравнения в квадрат:

$$\begin{cases} (x^2-y^2)^2=a^2, \\ 4x^2y^2=b^2. \end{cases} \tag{6.1}$$

Складывая оба уравнения последней системы, получим уравнение

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

Теперь имеем систему:

$$\begin{cases} x^2+y^2=\sqrt{a^2+b^2}, \\ x^2-y^2=a. \end{cases}$$

Складывая оба уравнения, а затем вычитая из первого уравнения второе, получаем: $2x^2 = \sqrt{a^2+b^2}+a$, $2y^2 = \sqrt{a^2+b^2}-a$. Извлекая корни из каждого уравнения, получаем:

$$x = \delta_1\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}},\ x = \delta_2\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}},$$

где $\delta_1 = \pm 1 = \delta_2$. Но из второго уравнения системы (7.4) следует, что $xy = \dfrac{b}{2}$. Поэтому при $b \geq 0$ произведение $\delta_1\delta_2 = 1$, то есть x и y имеют одинаковые знаки, а $b > 0$ произведение $\delta_1\delta_2 = -1$, то есть x и y имеют одинаковые знаки. В общем случае эту запись можно записать, используя функцию «знак» следующм образом: $\delta_2 = \delta_1 \operatorname{sign} b$,

$$\sqrt{a+bi} = \pm\left(\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}} + (\operatorname{sign} b)i\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}}\right).$$

6.4.2 Тригонометрическая форма комплексных чисел

Действительные числа можно изображать точками на числовой оси. Комплексное число $z = a+bi$ задается двумя действительными числами a и b, поэтому естественно изображать комплексные числа точками на плоскости.

На плоскости с заданной на ней прямоугольной декартовой системой

координат xOy выберем полярную систему координат так, чтобы полюс совпадал с точкой O, а полярная ось — с положительной полуосью Ox.

Пусть $a+bi$ — произвольное отличное от 0 комплексное числа и OA соответствующий ему вектор. Если выразить декартовы координаты конца этого вектора через его полярные координаты r и φ, то получим

$$a = r\cos\varphi,\ \ b = r\sin\varphi,$$

где r — длина полярного радиус-вектора OA, φ — угол, отсчитываемый от полярной оси до вектора OA против хода часовой стрелки и измеряемый в радикалах.

Отсюда имеем

$$a + bi = r(\cos\varphi + i\sin\varphi).$$

Запись $z = r(\cos\varphi + i\sin\varphi)$ называется тригонометрической формой комплексного числа.

Неотрицательное число r называется *модулем комплексного числа* z и обозначается $|z|$. Ясно, что

$$|z| = \sqrt{x^2 + y^2}.$$

Угол φ называют *аргументом комплексного числа* z и обозначают через $\arg z$.

Для аргумента φ комплексного числа $z = x + yi$ имеем равенства:

$$\varphi = \begin{cases} \operatorname{arctg}\dfrac{y}{x}, \text{ если } x > 0, \\ \operatorname{arctg}\dfrac{y}{x} + \pi, \text{ если } x < 0, y \geq 0, \\ \operatorname{arctg}\dfrac{y}{x} - \pi, \text{ если } x < 0, y < 0 \\ \operatorname{arctg}\dfrac{\pi}{2}, \text{ если } x = 0, y > 0 \\ \operatorname{arctg}\dfrac{\pi}{2}, \text{ если } x = 0, y < 0 \\ 0, \text{ если } x = 0, y = 0. \end{cases}$$

Теорема 6.3. 1. *При умножении комплексных чисел в тригонометрической форме их модули перемножаются, а аргументы складываются:*

$$|z_1|(\cos\varphi_1 + i\sin\varphi_1) \cdot |z_2|(\cos\varphi_2 + i\sin\varphi_2) =$$

$$= |z_1| \cdot |z_2|(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)).$$

2. *При делении комплексных чисел их модули делятся, а аргументы вычитаются:*

$$\frac{|z_1|(\cos\varphi_1 + i\sin\varphi_1)}{|z_2|(\cos\varphi_2 + i\sin\varphi_2)} = \frac{|z_1|}{|z_2|}(\cos(\varphi_1 - \varphi_2) + i\sin(\varphi_1 - \varphi_2)).$$

Теорема 6.4. (Формула Муавра) *Пусть n — целое число. Тогда*

$$(|z|(\cos\varphi + i\sin\varphi))^n = |z|^n(\cos(n\varphi) + i\sin(n\varphi)).$$

Пусть $n \in N$, $n > 1$.

Определение 6.2. *Корнем n-й степени из комплексного числа z называется такое комплексное число c, что $c^n = z$. Таким образом, если $c = \sqrt[n]{z}$, то $c^n = z$.*

Теорема 6.5. *Пусть z — комплексное число и n — натуральное число, $n > 1$. В поле комплексных чисел корень $\sqrt[n]{z}$ при $z = 0$ имеет единственное значение $\sqrt[n]{z} = 0$, а при $z \neq 0$ — n различных значений. Если $z = |z|(\cos\varphi + i\sin\varphi) \neq 0$, то эти значения находятся по формуле*

$$\sqrt[n]{z} = \sqrt[n]{|z|}\left(\cos\frac{\varphi + 2k\pi}{n} + i\sin\frac{\varphi + 2k\pi}{n}\right),$$

$$\text{где } k = 0, 1, ..., n-1.$$

6.4.3 Показательная форма комплексных чисел

Показательная и тригонометрические функции в области комплексных чисел связаны между собой формулой

$$e^{i\varphi} = \cos\varphi + i\sin\varphi,$$

которая носит название *формулы Эйлера*. Обосновать ее можно с помощью теории степенных рядов.

Пусть комплексное число z в тригонометрической форме имеет вид $z = r(\cos\varphi + i\sin\varphi)$. На основании формулы Эйлера выражение в скобках можно заменить на показательное выражение. В результате

$$z = re^{i\varphi}.$$

Эта запись называется *показательной формой* комплексного числа. Так же, как и в тригонометрической форме, здесь $r = |z|$, $\varphi = \arg z$.

Умножение комплексного числа $z_1 = |z_1|e^{i\varphi_1}$ на комплексное число $z_2 = |z_2|e^{i\varphi_2}$ выглядит следующим образом:

$$z_1 \cdot z_2 = |z_1|e^{i\varphi_1} \cdot |z_2|e^{i\varphi_2} = |z_1| \cdot |z_2|e^{i\varphi_1+i\varphi_2} =$$

$$= |z_1| \cdot |z_2|e^{i(\varphi_1+\varphi_2)}.$$

То есть, чтобы найти произведение комплексных чисел в показательной форме, нужно перемножить их модули и сложить аргументы.

Аналогично можно найти частное от деления комплексного числа $z_1 = |z_1|e^{i\varphi_1}$ на комплексное число $z_2 = |z_2|e^{i\varphi_2} \neq 0$:

$$\frac{z_1}{z_2} = \frac{|z_1|e^{i\varphi_1}}{|z_2|e^{i\varphi_2}} = \frac{|z_1|}{|z_2|}e^{i\varphi_1-i\varphi_2} = \frac{|z_1|}{|z_2|}e^{i(\varphi_1-\varphi_2)}.$$

Отсюда получаем правило: при делении двух комплексных чисел в показательной форме их модули делятся, а аргументы вычитаются.

Для возведения комплексного числа $z = |z|e^{i\varphi}$ в показательной форме в целую степень n, нужно модуль возвести в эту степень, а аргумент увеличить в n раз:

$$z^n = \left(|z|e^{i\varphi}\right)^n = |z|^n e^{in\varphi}.$$

Извлечение корня n-й степени из комплексного числа в показательной форме выполняется по следующему правилу:

$$\sqrt[n]{z} = \sqrt[n]{r} \cdot e^{i\left(\frac{\varphi+2\pi k}{n}\right)}, \text{ где } k = 0, 1, ..., n-1.$$

6.5 Категоричность и непротиворечивость аксиоматической теории комплексных чисел

6.5.1 Непротиворечивость аксиоматической теории комплексных чисел

Теорема 6.6. *Аксиоматическая теория комплексных чисел непротиворечива.*

Доказательство. Докажем непротиворечивость аксиоматической теории комплексных чисел относительно аксиоматической теории действительных чисел.

Построим модель, на которой выполняются все 17 аксиом нашей теории. Пусть $\langle R, +, \cdot, 0, 1\rangle$ — поле действительных чисел.

Рассмотрим множество $P = \{(a, b) |\ a, b \in R\}$ и определим на P бинарные операции $\oplus$ и $\odot$ (сложение и умножение) следующим образом:

$$(\forall a, b, a', b' \in R)\ (a, b) \oplus (a', b') = (a + a', b + b')$$

$$(\forall a, b, a', b' \in R)\ (a, b) \odot (a', b') = (aa' - bb', ab' + a'b).$$

Из курса алгебры известно, что P является полем. Выберем в P подмножество R_0 пар вида: $(a, 0)$.

Построим отображение $\varphi : R \to R_0$, по закону

$$(\forall a \in R)\ \varphi(a) = (a, 0).$$

Легко видеть, что φ — взаимнооднозначное отображение R на R_0. Кроме этого,

$$(\forall a, b \in R)\ \varphi(a+b) = (a+b, 0) = (a,0) \oplus (b,0) = \varphi(a) \oplus \varphi(b),$$

$$(\forall a, b \in R)\ \varphi(ab) = (ab, 0) = (a,0) \odot (b,0) = \varphi(a) \odot \varphi(b).$$

Таким образом, φ — изоморфизм $\langle R, +, \cdot \rangle$ на $\langle R_0, \oplus, \odot \rangle$. Следовательно,

1) $\langle R_0, \oplus, \odot \rangle$ — поле действительных чисел;

2) $\langle P, \oplus, \odot \rangle$ — расширение поля $\langle R_0, \oplus, \odot \rangle$.

Заметим также, что $(1,0)$ и $(0,0)$ — единица и нуль поля $\langle R_0, \oplus, \odot \rangle$. Полагаем $i = (0,1)$. Имеем

$$i^2 \oplus (1,0) = (0,1) \odot (0,1) \oplus (1,0) = (-1,0) \oplus (1,0) = (0,0).$$

Итак, на системе $\langle P, \oplus, \odot, R_0, \oplus, \odot \rangle$ выполняются первые 16 аксиом нашей теории.

Пусть, наконец, $M \subset P$ и M такое, что

a) $R_0 \subset M$;

b) $i \in M$;

c) $(\alpha, \beta \in M)\ \alpha + \beta \in M$;

d) $(\alpha, \beta \in M)\ \alpha \cdot \beta \in M$.

Докажем, что в таком случае любой элемент множества P принадлежит множеству M. В самом деле, имеем для любой пары $(a,b) \in P$ представление $(a,b) = (a,0) \oplus (b,0) \odot (0,1)$. Так как $(a,0), (b,0) \in R_0 \subset M$,

$(0,1) = i \in M$, то $(a,b) \in M$. Следовательно, на P выполняется аксиома минимальности.

Тем самым доказано, что на P выполняются все 17 аксиом нашей теории. $\boxtimes$

6.5.2 Категоричность аксиоматической теории комплексных чисел

Теорема 6.7. *Аксиоматическая теория комплексных чисел категорична.*

Доказательство. Пусть $\langle C', +, \cdot, i', R' \rangle$ и $\langle C'', \oplus, \odot, i'', R'' \rangle$ — две системы комплексных чисел.

Поскольку любые поля действительных чисел изоморфны, то существует взаимнооднозначное отображение φ множества R' на R'' такое, что:

$$1)(\forall a', b' \in R')\ \varphi(a' + b') = \varphi(a') \oplus \varphi(b');$$

$$2)(\forall a', b' \in R')\ \varphi(a' \cdot b') = \varphi(a') \odot \varphi(b').$$

Определим однозначное отображение f множества C' в C'' следующим условием:

$$f : a' + b'i' \to \varphi(a') \oplus \varphi(b') \odot i''.$$

Нетрудно убедиться, что отображение f — взаимно-однозначное отображение C' на C''.

Пусть $\alpha' = a'_1 + a'_2 i'$, $\beta' = b'_1 + b'_2 i'$. 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

$$(\forall \alpha', \beta' \in C')\ f(\alpha') \odot f(\beta') = f(\alpha' \cdot \beta').$$

$\boxtimes$

Замечание 1. В поле C существует только одно подполукольцо, изоморфное полукольцу натуральных чисел.

Замечание 2. В поле C существует только одно подкольцо, изоморфное кольцу целых чисел.

Замечание 3. В поле C имеется только одно поле, изоморфное полю рациональных чисел.

Замечание 4. В поле C имеется бесконечное множество подполей, изоморфных полю действительных чисел.

6.6 Вопросы и задания для самоконтроля

1. Какова необходимость введения комплексных чисел?
2. Охарактеризуйте аксиомы группы A?
3. Охарактеризуйте аксиомы группы B?
4. Охарактеризуйте аксиомы группы C?
5. Охарактеризуйте аксиому группы D?
6. Какая группа аксиом утверждает, что C — поле?
7. Какая группа аксиом утверждает, что C — расширение R?
8. Какая группа аксиом раскрывает свойства i?
9. Как доказать, что любое комплексное число можно единственным образом записать в виде $z = a + bi$, где $a, b \in R$?
10. Из чего следует, что поле C нельзя упорядочить?

РАЗДЕЛ 7
КВАТЕРНИОНЫ

Пусть $\langle A, +, \cdot, 0, P\rangle$ — линейная алгебра над полем P.

Определение 7.1. *Алгебру A называют алгеброй ранга n над полем P, если алгебра $\langle A, +, 0, P\rangle$ — n-мерное векторное пространство над полем P.*

Базисом алгебры A называют базис пространства $\langle A, +, 0, P\rangle$.

Примеры. 1. Всякое поле P есть алгебра с делением ранга 1 над полем P.

2. Поле C есть алгебра с делением ранга 2 над полем R.

Пусть M_2 — это множество матриц второго порядка над полем C, т.е. множество матриц с комплексными элементами, для кооторых сложение $\oplus$ и умножение $\odot$ определены обычным образом. Тогда $\langle M_2, \oplus, \odot\rangle$ — некоммутативное кольцо с делителями нуля.

Рассмотрим множество матриц M_2' с комплексными элементами, причем эти матрицы будут иметь вид $\begin{bmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{bmatrix}$, где $\alpha = a + bi$, $\overline{\alpha} = a - bi$, $\beta = c + di$, $\overline{\beta} = c - di$, $a, b, c, d \in R$.

Определение 7.2. *Кольцо $\langle A, +, \cdot, 0\rangle$ называется телом, если множество A состоит не из одного нуля, и если для любых элементов*

$a, b \in A, a \neq 0$ *существуют элементы* $x, y \in A$, *что верно следующее равенство* $ax = b$ *и* $ya = b$.

Множество $\langle M_2', \oplus, \odot \rangle$ является телом.

Определение 7.3. *Всякую алгебру* K *изоморфную алгебре с делением ранга* 4 *над полем* R *называют алгеброй кватернионов.*

Легко проверить, что любой кватернион $q = \begin{bmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{bmatrix}$ можно представить в виде $q = ai_0 + bi_1 + ci_2 + di_3$, где a, b, c, d — действительные числа, причем

$$i_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, i_1 = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, i_2 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, i_3 = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

Следует заметить, что таблица умножения для 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

Замечание. Легко проверить, что таблица умножения элементов i_0, i_1, i_2, i_3 определяется следующими условиями:

1) i_0 — единица алгебры кватернионов;

2) $i_1 \cdot i_2 = -i_2 \cdot i_1 = i_3$;

3) $i_1^2 = i_2^2 = i_3^2 = -i_0 = -1$.

Поля C, R и тело кватернионов K мы можем рассматривать как алгебры над полем R. Каждая из этих алгебр является алгеброй с делением и имеет конечный ранг. Ранг R равен 1, ранг C равен 2 и ранг K равен 4.

Очень часто кватернионы записывают в виде $q = a + bi + cj + dk$, где a, b, c, d — действительные числа, а i, j, k — мнимые единицы. Причем, $i^2 = j^2 = k^2 = ijk = -1$, $ij = k$ и $ji = -k$.

7.1 Действия над кватернионами

Пусть $q_1 = a_1 + b_1 i + c_1 j + d_1 k$ и $q_2 = a_2 + b_2 i + c_2 j + d_2 k$ два кватерниона.

Сложение кватернионов

Сложение кватернионов выполняется по следующему закону

$$q_1 + q_2 = (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k.$$

Умножение кватернионов

Чтобы описать закон умножения достаточно указать чему равны всевозможные парные произведения чисел i, j и k. Таблица умножения для элементов i, j, k имеет следующий вид

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Замечание. Запомнить эту таблицу помогает рисунок 7.1, на котором кватернионы i, j, k изображены тремя точками окружности, расположенными по направлению движения часовой стрелки. Произведение любых двух чисел из тройки i, j, k равно третьему, если движение от

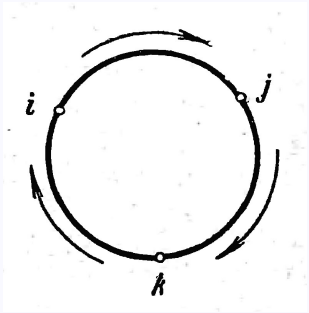

Рис. 7.1:

первого множителя происходит по часовой стрелке, и равно третьему со знаком минус, если движение происходит против часовой стрелки.

Выведем закон умножения кватернионов

$$q_1 \cdot q_2 = a_1a_2 + a_1(b_2i) + a_1(c_2j) + a_1(d_2k) + (b_1i)a_2 + (b_1i)(b_2i) +$$
$$+(b_1i)(c_2j) + (b_1i)(d_2k) + (c_1j)a_2 + (c_1j)(b_2i) + (c_1j)(c_2)j +$$
$$+(c_1j)(d_2k) + (d_1k)a_2 + (d_1k)(b_2i) + (d_1k)(c_2j) + (d_1k)(d_2k).$$

Воспользовавшись таблицей умножения получим

$$q_1q_2 = (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)i +$$
$$+(a_1c_2 + c_1a_2 + d_1b_2 - b_1d_2)j + (a_1d_2 + d_1a_2 + b_1c_2 - C_1b_2)k.$$

Сопряжение кватернионов

Определение 7.4. *Кватернион* $\overline{q} = a - bi - cj - dk$ *называется* *сопряженным* *для кватерниона* $q = a + bi + cj + dk$.

Очевидно, что сумма сопряженных кватернионов есть действительное число. Но и произведение $q\overline{q}$ также является действительным числом, что сразу же следует из формулы для умножения кватеорнионов:

$$q\overline{q} = (a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2. \qquad (7.1)$$

Число $\sqrt{a^2 + b^2 + c^2 + d^2}$ называется *модулем* кватерниона q и обозначается $|q|$. Тогда равенство 7.1 перепишится так:

$$q\overline{q} = |q|^2.$$

Непосредственная проверка показывает, что операция сопряжения обладает такими свойствами:

$$\overline{q_1 + q_2} = \overline{q}_1 + \overline{q}_2 \qquad (7.2)$$

(сопряжение к сумме равно сумме сопряженных) и

$$\overline{q_1 q_2} = \overline{q}_2 \overline{q}_1 \qquad (7.3)$$

(сопряженное к произведению равно произведению сопряженных, вятых в обратном порядке).

Чтобы убедиться в справедливости равенства 7.3, достаточно проверить его для каждого из случаев, когда вместо q_1 и q_2 берутся i, j, k. Например,

$$\overline{ii} = \overline{-1} = -1, \text{ но и } \overline{i}\,\overline{i} = (-i)(-i) = i^2 = -1,$$

$$\overline{ij} = \overline{k} = -k, \text{ но и } \overline{j}\,\overline{i} = (-j)(-i) = ji = -k$$

и т.д.

Деление кватернионов

Прежде, чем ввести деление кватернионов обратим внимание на существенное отличие в самой постановке вопросов о делении кватернионов и делении комплексных чисел. Для комплексных чисел частным от деления z_1 на z_2 является решение уравнения $z_2x = z_1$. Но для кватернионов произведение зависит от порядка сомножителей, поэтому вместо одного уравнения нужно рассмотреть два:

$$q_2x = q_1 \tag{7.4}$$

и

$$xq_2 = q_1. \tag{7.5}$$

Соответственно, решение первого уравнения будем называть *левым частным* от деления q_1 на q_2 и обозначать x_l, а решение второго — *правым частным* x_r (в случае комплексных чисел оба частных совпадают).

Чтобы решить уравнение 7.4 умножим обе части этого уравнения слева сначала на $\overline{q}_2$, а затем на $\dfrac{1}{|q_2|^2}$. Получим

$$x = \frac{1}{|q_2|^2}\overline{q}_2 q_1.$$

Непосредственной подстановкой в уравнение 7.4 убеждаемся, что это выражение действительно является решением. Таким образом

$$x_l = \frac{1}{|q_2|^2}\overline{q}_2 q_1.$$

Аналогично находится x_r:

$$x_r = \frac{1}{|q_2|^2} q_1 \overline{q}_2.$$

В качестве примера найдем левое и правое частные от деления k на $1 + j + k$:

$$x_l = \frac{1}{3}(1 - i - k)k = \frac{1}{3}(k + j + 1),$$

$$x_r = \frac{1}{3}k(1 - i - k) = \frac{1}{3}(k - j - 1).$$

Замечание. Кватернионы — система с делением.

Замечание. Кватернион можно представить как пару комплексных чисел. Например, $q = z + wj$, где $z = a + bi$, $w = c + di$.

Для кватерниона $q = a + bi + cj + dk$ число a называется *скалярной частью*, а $bi + cj + dk$ — *векторной*. Если векторная часть равна 0, то кватернион называется *чисто скалярным*. Если скалярная часть равна 0, то кватернион называется *чисто мнимым*.

Кватернионы можно определить как вещественные матрицы вида

$$\begin{bmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{bmatrix}.$$

При такой записи сопряженному кватерниону соответствует транспонированная матрица.

7.2 Свойства кватернионов

1^0. Четыре базисных кватерниона и четыре противоположных им по знаку образуют по умножению группу кватернионов

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}.$$

Эта группа конечна и ее порядок равен 8.

2^0. Множество кватернионов является кольцом с делением.

3^0. Множество кватернионов образует четырехмерную ассоциативную алгебру с делением над полем R.

Замечание. R, C и K являются единственными конечномерными ассоциативными алгебрами с делением над полем R.

4^0. Умножения кватернионов некоммутативно.

5^0. Умножения кватернионов ассоциативно.

7.3 Теорема Фробениуса

Лемма 7.1. *Пусть* $\{A, +, \cdot, R\}$ — *ассоциативная алгебра с делением конечного ранга* n *над полем действительных чисел* R. *Тогда:*

1) *любой элемент* α *алгебры* A — *корень неприводимого над* R *многочлена первой и второй степени. При этом* $\alpha \notin R$ *тогда и только тогда, когда* α — *корень неприводимого над полем* 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* A *изоморфна алгебре комплексных чисел.*

Лемма 7.2. *Не существует ассоциативных алгебр с делением ранга 3 над полем действительных чисел.*

Лемма 7.3. *Всякая ассоциативная алгебра с делением ранга 4 над полем действительных чисел изоморфна алгебре кватернионов.*

Лемма 7.4. *Над полем действительных чисел нет ассоциативных алгебр с делением конечного ранга* n, *если* $n \geq 5$.

Замечание. Ознакомиться с доказательством теорем 7.1–7.4 можно, например, в [9, с. 171–174].

Из теорем 7.1–7.4 следует

Теорема 7.1. **(Теорема Фробениуса)** *Над полем R действительных чисел любая ассоциативная алгебра A с делением конечного ранга n имеет ранг 1, 2 или 4. При этом:*

1) *если $n = 1$, то алгебра A изоморфна R;*
2) *если $n = 2$, то алгебра A изоморфна C;*
3) *если $n = 4$, то алгебра A изоморфна K.*

7.4 Вопросы и задания для самоконтроля

1. Что называется алгеброй кватернионов?
2. Какова таблица умножения в алгебре кватернионов?
3. Какими свойствами обладает умножение в алгебре кватернионов?
4. Какой кватернион называется сопряженным данному?
5. Какой кватернион называется чисто мнимым?
6. Чему равно произведение сопряженных кватернионов?
7. Что называется модулем кватерниона?
8. Как доказать, что $\overline{q_1 + q_2} = \overline{q}_1 + \overline{q}_2$ и $\overline{q_1 \cdot q_2} = \overline{q}_2 \cdot \overline{q}_1$?
9. Как доказать $|q_1 \cdot q_2|^2 = |q_2|^2 \cdot |q_1|^2$?
10. Как выполняется деление в алгебре кватернионов?
11. Как определить кватернионы с помощью комплексных чисел?
12. В чем состоит теорема Фробениуса?

Литература

1. Драбкина, М. Е. Основания арифметики / М.Е. Драбкина. — Минск, 1962. — 205 с.

2. Завало, С.Т. Алгебра и теория чисел: учеб. пособие: в 2 ч. / С.Т. Завало, В.Н. Костарчук, Б.И. Хацет. — Киев: Высшая школа, 1977. — Ч. 1. — 400 с.

3. Кантор, И.Л. Гиперкомплексные числа / И.Л. Кантор, А.С. Солодовников. — М.: Наука, 1973. — 144 с.

4. Куликов, Л.Я. Алгебра и теория чисел / Л.Я. Куликов. — М.: Высшая школа, 1979. — 559 с.

5. Мальцев, А.И. Алгебраические системы / А.И. Мальцев. — М.: Наука, 1970.

6. Матысик, О.В. Числовые системы: курс лекций / О.В. Матысик, Л.П. Молодова. — Брест: Изд-во БрГУ, 2008. — 48 с.

7. Милованов, М.В. Алгебра и аналитическая геометрия: учеб. пособие: в 2 ч. / М.В. Милованов [и др.]. — Мінск: Вышэйшая школа, 1987. — Ч. 2. — 269 с.

8. Монахов, В.С. Алгебра и теория чисел: практикум: учеб. пособие: в 2 ч. / В.С. Монахов, А.В. Бузланов. — Минск: Изд. центр БГУ, 2007. — Ч. 1. — 264 с.

9. Нечаев, В.И. Числовые системы / В.И. Нечаев. — М.: Просвещение, 1975. — 198 с.

10. Проскуряков, И.В. Числа и многочлены / И.В. Проскуряков. — М.: Просвещение, 1965. — 283 с.

11. Смолин, Ю.Н. Числовые системы: учеб. пособие / Ю.Н. Смолин. — М.: Флинта: Наука, 2009. — 112 с.

12. Феферман, С. Числовые системы / С. Феферман. — М.: Наука, 1971. — 440 с.