ЯКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ МАТЕМАТИКИ И ИНФОРМАТИКИ
КАФЕДРА АЛГЕБРЫ И ГЕОМЕТРИИ

Шамаев Э.И.

лекции по курсу

ЧИСЛОВЫЕ СИСТЕМЫ

$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

Якутск — 2007

Содержание

Введение

История

Умение оперировать натуральными числами — поразительная особенность человеческого мышления[1]. Остальные числовые системы: *арифметики целых чисел, рациональных чисел, действительных чисел* появились из натуральных чисел.

Естественное стремление людей количественно описывать часть целого в налогообложении, учете, распределении и торговли с древнейших времен дали нам понятие дроби. Археологические находки указывают на то, что дробными числами пользовались уже в древнем Шумере, Аккаде, Вавилоне и Египте. В гораздо более позднее время появилось понятие нуля[2] и отрицательного числа. Видимо, история появления рациональных чисел также начинается с доисторических времен — некоторые культуры, не умея считать дальше 100, уже имели представление о половине[3].

История появления вещественных чисел нам известна не намного лучше. Источники указывают, что существование чисел отличных от рациональных было известно пифагорейской школе в Древней Греции. С другой стороны, умение работать с длинами отрезов, т.е. действительными величинами, было почти у всех древних цивилизаций.

Теории современной математики носят дедуктивный характер, т.е. выводятся из некоторого набора начальных очевидных суждений, называемых *аксиомами.*

Знание аксиом натуральных чисел не означает знание ответа на вопрос «что такое число?», а дает нам возможность упорядочить математические знания о натуральных числах.

Современные аксиомы числовых систем были построены в короткий период с 1853 по 1861 г. В 1853 году Гамильтон построил теорию рациональных чисел, комплексных чисел и кватернионов. Теория вещественных чисел были построена Дедкиндом и Ка́нтором в 1857 г. на основе теории рациональных чисел. Несколько лет спустя Пеано построил аксиомы натуральных чисел.

Лекции мы начнем с определений фундаментальных понятий математики — множеств, отображений, групп, колец и полей. Затем ознакомимся с аксиомами Пеано натуральных чисел, и будем постепенно строить целые, рациональные, действительные и комплексные числа.

Множества

Множество определяется своими элементами[4]. Если x является элементом множества A, то пишем $x \in A$, иначе $x \notin A$. Множество не содержащее элементов называется *пустым* и обозначается через $\varnothing$. Множество A, состоящее только из элементов $1, a, -100$, обозначается через $\{1, a, -100\}$. Множество B называется *подмножеством* A, если из для каждого $x \in B$ элемент $x \in A$. Обозначается это отношение через $B \subseteq A$. Множества A и B называются *равными,* если $A \subseteq B$ и $B \subseteq A$. Если $A \subseteq B$ и $A \neq B$, то A называется *собственным подмножеством* B, что обозначается $A \subset B$.

Если число элементов множества конечно, то множество называется *конечной*, иначе множество называется *бесконечной.* Число элементов конечного множества A обозначается через $|A|$.

Примеры всех числовых систем.

$\mathbb{N} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \ldots\}$ — множество натуральных чисел;

$\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$ — множество целых чисел;

$\mathbb{Q} = \left\{\frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{N}\right\}$ — множество рациональных чисел;

$\mathbb{R}$ — множество вещественных чисел; $\mathbb{C}$ — множество комплексных чисел;

ясно, что $\varnothing \subset \{2, 4, 5\} \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, и $\{2, 4, 6\} \subseteq \{2, 4, 6, 8, 2008\}$, но $\{2, 4, 6\} \nsubseteq \{0, 2, 4\}$.

---

[1] здесь уместно спросить: «Умел ли Маугли считать?», «Есть ли у инопланетян натуральные числа?»

[2] древние греки и римляне не знали ноль, понятие нуля в средневековую Европу пришло из Индии

[3] ни в одной из мне известных языков слова «два» и «половина» не похожи!

[4] понятие множества не имеет математического определения, это базовое понятие

Операции над множествами

Объединением множеств A и B называется новое множество состоящее из всех элементов A и B, других элементов нет. Пересечением множеств A и B называется новое множество, состоящее из общих элементов A и B, других элементов нет. Разностью множеств A и B называется новое множество состоящее только из элементов A, которые не принадлежат B. Приведем обозначения и более строгие определения операций.

Объединение $A \cup B = \{x \mid x \in A \text{ или } x \in B\}$.
Пересечение $A \cap B = \{x \mid x \in A \text{ и } x \in B\}$.
Разность $A \backslash B = \{x \mid x \in A \text{ и } x \notin B\}$.

Примеры. Пусть $A = \{1, 2, 3\}$ и $B = \{3, 4\}$. Тогда $A \cup B = \{1, 2, 3, 4\}$, $A \cap B = \{3\}$, $A \backslash B = \{1, 2\}$.
Задачи.

1.1 Постройте произвольное множество из ста одного элемента.

1.2 Пусть $A = \{2, 3, 8, 15\}$ и $B = \{1, 4, 5, 15\}$. Постройте $A \cup B$ и $A \cap B$.

1.3 На рис. 1 даны диагараммы Венна. Выразите с помощью операций над множествами A, B и C выделенные подмножества.

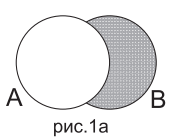

рис.1а

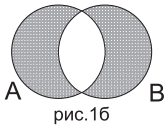

рис.1б

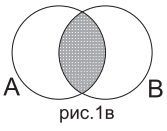

рис.1в

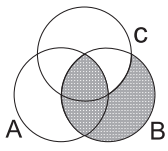

рис.1г

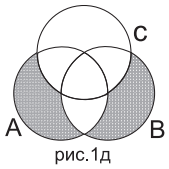

рис.1д

1.4 Постройте $\mathbb{N} \cup \mathbb{Z}$, $\mathbb{N} \cap \mathbb{Z}$. Если $A \subseteq B$, то чему равно $A \cap B$ и $A \cup B$?

1.5 Пусть $2\mathbb{Z} = \{2, 4, 6, 8, \ldots\}$ и $3\mathbb{Z} = \{3, 6, 9, 12, \ldots\}$. Постройте $2\mathbb{Z} \cup 3\mathbb{Z}$.

1.6 Про множество $A \subseteq \mathbb{Z}$ известно, что если $a \in A$, то $a + 3 \in A$ и $a - 6 \in A$, также известно, что $3 \in A$ и $1, 2 \notin A$. Найдите множество A.

1.7 Пусть $A = \{2, 4, 6, \ldots, 298, 300\}$, $B = \{3, 6, 9, \ldots, 297, 300\}$, $C = \{6, 12, 18, \ldots, 294, 300\}$. Вычислите $|A|$, $|B|$, $|C|$ и найдите $\big|\{a \in \mathbb{N} \mid a \leqslant 300 \text{ и } (2|a \text{ или } 3|a)\}\big|$.

1.8 Найдите $\big|\{a \in \mathbb{N} \mid a \leqslant 300 \text{ и } (2 \nmid a \text{ или } 3 \nmid a)\}\big|$.

1.9 Постройте множество всех простых чисел.

Упорядоченные n-ки

Упорядоченные n-ки $(a_1, a_2, \ldots, a_n)$ и $(b_1, b_2, \ldots, b_n)$ *равны,* если и только если $a_1 = b_1$, $a_2 = b_2$, $\ldots$, $a_n = b_n$. *Декартовым (прямым) произведением* множеств A и B называется множество упорядоченных двоек $\{(a, b) \mid a \in A \text{ и } b \in B\}$. Это множество обозначается через $A \times B$. Декартово произведение одного и того же множества A на себя n раз обозначают как A^n.

Примеры.

Если $A = \{1, 2, 3\}$ и $B = \{3, 4\}$, то $A \times B = \{(1, 3), (1, 4), (2, 3), (2, 4), (3, 3), (3, 4)\}$.

В театре «Малый» номера рядов перенумерованы числами множества $\{1, 2\}$, а места в каждом ряду — числами $\{1, 2, 3, 4\}$. Тогда множество мест в билетах театра — декартово произведение —

$$\{1, 2\} \times \{1, 2, 3, 4\} = \begin{matrix} \big\{(1,1), & (1,2), & (1,3), & (1,4), \\ (2,1), & (2,2), & (2,3), & (2,4), \big\}. \end{matrix}$$

Декартов квадрат множества координат точек на прямой равен множеству координат точек на плоскости $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$.

Задачи.

1.10 Пусть $A = \{1, 2\}$ и $B = \{a, b, c\}$. Постройте $A \times B$.

1.11 В самолете ТУ-154 номера рядов перенумерованы числами множества $\{1, 2, \ldots, 25\}$, а места в каждом ряду — буквами $\{a, b, c, d, e, f\}$. Найдите множество мест в этом самолете.

1.12 Постройте множество всевозможных трехзначных чисел.

1.13 Для всех конечных множеств A и B докажите равенство $|A| \times |B| = |A \times B|$.

1.14 Постройте множества A и B такие, что $|A \times B| = 15$.

1.15 Постройте множества A и B такие, что $|A \times B| = 7$.

Отображения

Дадим два определения отображению.

Определение 1. *Некоторое правило f, сопоставляющее части элементов A по одному элементу из множества B, называется отображением из A в B.*

Определение 2. *Отображением из A в B называется подмножество $f \subset A \times B$, удовлетворяющее условию: если (a,b) и $(a,b') \in f$, то $b = b'$.*

Вместо $(a,b) \in f$ всегда пишут $f(a) = b$, а само отображение обозначают как $f : A \to B$.

Множество $A' = \{x \in A \mid f(x) = y \text{ для некоторого } y \in B\}$ называется *множеством (областью) определения* отображения f. Множество $B' = \{y \in B \mid f(x) = y \text{ для некоторого } x \in A\}$ называется *множеством значений* отображения f.

Функциями[5] называются отображения произвольного множества в $\mathbb{R}$, т.е. $f : A \to \mathbb{R}$.

Задачи.

2.1 Постройте отображение из $\{1,2,3,4\}$ в $\{A,B,C,D,E\}$.

2.2 Постройте пример отображения $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.

2.3 Покажите, что отображение из $\mathbb{Z} \times \mathbb{Z}$ в $\mathbb{Z}$, заданное $f(a,b) = a + b$ является отображением.

2.4 Существует некоторое соответствие между множеством номеров паспорта РФ и множеством российских граждан. Постройте отображение между двумя этими множествами, зная, что у некоторых граждан могут быть два паспорта (гражданин потерял, восстановил новый и нашел старый).

Отображение $f : A \to B$ называется *всюду определенным*[6], если для каждого $a \in A$ определен $f(a) \in B$. Отображение $f : A \to B$ называется *«на»*, если для каждого $b \in B$ существует $a \in A$ такой, что $f(a) = b$. И наконец, отображение $f : A \to B$ называется *взаимно-однозначным*, если из $a_1 \neq a_2$ следует $f(a_1) \neq f(a_2)$.

Всюду определенное и взаимно-однозначное отображение f из A на B называется *биекцией.*

Дадим эквивалентное определение. Отображение, сопоставляющее каждому элемент A ровно один элемент B, с множеством значений совпадающим с B, называется биекцией.

Ясно, что существование биекции между конечными множествами A и B означает $|A| = |B|$. Этим очевидным, но важным свойством мы воспользуемся при определении равномощных множеств. Также биекция используется при определении изоморфизмов.

Примеры. Биекция множества $\{1,2,\ldots,n\}$ на себя называется подстановкой. Логарифм $\ln x$ — биекция $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$ на $\mathbb{R}$. Тангенс $\operatorname{tg} x$ — биекция $\left(-\frac{\pi}{2}; \frac{\pi}{2}\right)$ на $\mathbb{R}$. Арктангенс $\operatorname{arctg} x$ — биекция $\mathbb{R}$ на $\left(-\frac{\pi}{2}; \frac{\pi}{2}\right)$.

Задачи.

2.5 Постройте пример биекции между множествами $\{1,2,3,4\}$ и $\{A,B,C,D\}$.

2.6 Докажите, что $f(x) = 2x$ — биекция $\mathbb{Z}$ на $2\mathbb{Z} = \{2a \mid a \in \mathbb{Z}\}$.

2.7 Докажите, что строго монотонная функция всюду определенная на $\mathbb{R}$ является биекцией.

2.8 Покажите, что $f(x) = (b-a)x + a$ — биекция $(0;1)$ на $(a;b)$.

2.9 Докажите, то если σ и τ — подстановки, то функция $\pi(x) = \sigma(\tau(x))$ является подстановкой.

2.10 Пусть $f : X \to Y$, $g : Y \to Z$ — биекции. Покажите, что функция, называемая их суперпозицией, $h(x) = g(f(x))$ является биекций из X на Y. Суперпозицию $g(f(x))$ обозначают $g \circ f$.

2.11 Покажите, что построение биекции между множеством натуральных чисел $\mathbb{N}$ и произвольным множеством A эквиалентно задаче нумерации элементов A.

2.12 Если $f : \mathbb{N} \to A$ — биекция, то докажите существование биекции $g : \mathbb{N} \to A \cup \{1,2,\ldots 100\}$.

2.13 Пусть $f : \mathbb{N} \to A$ — биекция и B — конечное подмножество A. Докажите существование биекции $g : \mathbb{N} \to A \backslash B$.

2.14 В языке филоматенфинити алфавит имеет 20 букв и существуют сколь угодно длинные слова. Постройте биекцию из $\mathbb{N}$ на множество слов этого языка.

2.15 Постройте биекцию из $\mathbb{N}$ на $\mathbb{Z}$.

2.16 Постройте биекцию из $\mathbb{N}$ на $\mathbb{Q}$.

2.17 Постройте биекцию между $[0;1]$ на $[0;10]$.

[5] в школе изучают функции, определенные на множестве действительных чисел

[6] очень часто отображение определяют как всюду определенные отображения

Глава 1

Алгебраические системы

Алгебраические операции

Рассмотрим множество M. Отображение

$$f : M \times M \to M$$

называется *двухместной (бинарной) операцией* на множестве M. Результат операции $f(a, b)$ над a и b обычно обозначается через afb.

Примеры. Хорошо известные двухместные операции: сумма двух чисел, произведение двух чисел, разность двух чисел. Заметим, что на множестве натуральных чисел операция вычитания не всегда определена.

На множестве W матриц вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ определим операции «$+$» и «$\cdot$»:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -b-d & a+c \end{pmatrix};$$
$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix}.$$

Отображение $f : M \to M$ называется *одноместной (унарной) операцией* на множестве M. Примеры: $\sqrt{x}$, x^{-1}, и т.д. Отображение $f : M^n \to M$ называется *n-местной операцией*.

Задачи.

3.1 Проверьте, что операции «$+$» и «$\cdot$» на W верно определены.

3.2 Покажите, что операция вычитания «$-$» на полугруппе $\mathbb{N}$ не является всюду определенной.

3.3 Покажите, что операция x^y на кольце $\mathbb{Z}$ не является всюду определенной операцией.

Алгебраические отношения

Подмножество $f \subseteq M \times M$ называется бинарным (двухместным) *отношением* на множестве M. Если $(a, b) \in f$, то обычно пишут afb.

Примеры. Алгебраические отношения: $2 < 5$, $\quad 1 \leqslant 3$, $\quad a \sim b$.

Алгебраические и числовые системы

Множество с определенными на нем операциями и/или отношениями называется *алгебраической системой*. Алгебраические системы натуральных, целых, рациональных, действительных, комплексных чисел называются *числовыми*.

3.4 Приведите примеры алгебраических систем.

3.5 Постройте биекцию между комплексными числами $\mathbb{C}$ и множеством матриц W.

3.6 Постройте биекцию между действительными числами $\mathbb{R}$ и множеством векторов на прямой.

Группы

Определение 3. *Множество G с двухместной операцией $\circ$ называется группой $\langle G, \circ \rangle$ если*

1. *$a \circ (b \circ c) = (a \circ b) \circ c$ для всех $a, b, c \in G$;*
2. *существует $e \in G$ такой, что $a \circ e = e \circ a = a$ для всех $a \in G$;*
3. *для любого $a \in G$ существует $b \in G$ такой, что $a \circ b = b \circ a = e$.*

Приведенные аксиомы называются *ассоциативности, существования нейтрального элемента, существования обратного элемента*. Элемент e называется *нейтральным* элементом G. Элемент b, такой, что $ab = e$, называется *обратным* элемента a. Если в группе $\langle G, \circ \rangle$ для любых двух элементов a и b справедливо равенство $ab = ba$, то группа называется *коммутативной* или *абелевой*.

Множество G с ассоциативной двухместной операцией $\circ$ называется полугруппой $\langle G, \circ \rangle$.

Лемма 1. *В любой группе существует единственный нейтральный элемент.*

Доказательство. Пусть элементы e и $e' \in G$ нейтральные элементы группы G. Тогда $e \circ e'$ равен, с одной стороны e, с другой стороны e'. Поэтому $e = e'$. Лемма доказана.

Лемма 2. *Каждый элемент группы имеет единственный обратный элемент.*

Доказательство. Пусть элементы b и $b' \in G$ обратные элементы $a \in G$. Тогда $b \circ (a \circ b')$ равен, с одной стороны b, с другой стороны, по свойству ассоциативности, $(b \circ a) \circ b' = b'$. Поэтому $b = b'$. Лемма доказана.

Лемма 3. *В группе $\langle G, \circ \rangle$ для любых $a, c \in G$ решение уравнения $a \circ x = c$ относительно $x \in G$ существует и единственно.*

Доказательство. Покажем существование решения. Пусть b — обратный элемент a. Тогда $x = b \circ c$ является решением уравнения. Осталось показать единственность решения. Пусть x и x' являются решениями уравнения. Тогда $a \circ x = a \circ x'$. Умножим равенство на b справа. Тогда $x = x'$. Лемма доказана.

Аддитивные группы — группы, где имеются следующие обозначения: 0 — нейтральный элемент, $-a$ — обратный элемент a, «$+$» — операция группы. *В мультипликативной* группе приняты обозначения: 1 — нейтральный элемент, a^{-1} — обратный, «$\cdot$» — операция группы.

Определение 4. *Группы $\langle G, \circ \rangle$ и $\langle G', \cdot \rangle$ называются изоморфными, если существует биекция $f : G \to G'$ такая, что для всех $a, b \in G$ верно равенство*

$$f(a \circ b) = f(a) \cdot f(b).$$

Такое отображение f называется изоморфизмом.

Примеры. Алгебраические системы $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{Q} \backslash \{0\}, \cdot \rangle$, $\langle \mathbb{R}^+, \cdot \rangle$, $\langle \mathbb{R}, + \rangle$ — группы.

Алгебраические системы $\langle \mathbb{N}, + \rangle$, $\langle \mathbb{Z}, \cdot \rangle$, $\langle \mathbb{Q}, \cdot \rangle$, $\langle \mathbb{R}, \cdot \rangle$ — полугруппы, но не группы.

Задачи.

4.1 Докажите утверждения из примеров.

4.2 Докажите, что функция $\ln : \mathbb{R}^+ \to \mathbb{R}$ является изоморфизмом групп $\langle \mathbb{R}^+, \cdot \rangle$ и $\langle \mathbb{R}, + \rangle$.

4.3 Показать, что группы $\langle \mathbb{Z}, + \rangle$ и $\langle 2\mathbb{Z}, + \rangle$ изоморфны.

4.4 Докажите, что при изоморфизме групп нейтральный элемент отображается на нейтральный.

4.5 Пусть $\langle G, \cdot \rangle$ — группа и $a, b, c \in G$. Докажите, что решение уравнения $axb = c$ существует и единственно.

4.6 Пусть $g : G \to G'$ — изоморфизм. Пусть e — нейтральный элемент G. Докажите, что элементы, отображающиеся в нейтральный $\{a \mid g(a) = e\}$, образуют группу.

Кольца

Определение 5. *Пусть алгебраическая система $\langle K, +, \cdot \rangle$ является абелевой группой относительно сложения «+», полугруппой относительно «·», и «·» дистрибутивно относительно «+»:*

$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ для каждого } a, b, c \in K.$$

Тогда $\langle K, +, \cdot \rangle$ называется кольцом.

Если в кольце $\langle K, +, \cdot \rangle$ для любых двух элементов a и b справедливо равенство $a \cdot b = b \cdot a$, то кольцо называется *коммутативной.* Кольцо, содержащая единицу, называется *кольцом с единицей.*

Определение 6. *Пусть $\langle K, +, \cdot \rangle$, $\langle L, +, \cdot \rangle$ — кольца такие, что $L \subseteq K$. Тогда L называется подкольцом K.*

Приведем критерий того, что подмножество кольца является подкольцом.

Лемма 4 (Критерий подкольца)**.** *Пусть $\langle K, +, \cdot \rangle$ — кольцо и $L \subseteq K$.*
Тогда следующие два условия на L эквивалентны
1) для любых $a, b \in L$

$$a + b,\ -b,\ a \cdot b \in L$$

2) L является подкольцом K.

Примеры.
Кольца: $\langle \mathbb{Z}, +, \cdot \rangle$, $\langle \mathbb{Q}, +, \cdot \rangle$, $\langle \mathbb{R}, +, \cdot \rangle$, $\langle \mathbb{C}, +, \cdot \rangle$.
Задачи.
5.1 Докажите лемму — критерий подкольца.
5.2 Покажите, что $\langle \mathbb{Z}, +, \cdot \rangle$ подкольцо $\langle \mathbb{Q}, +, \cdot \rangle$.
5.3 Покажите, что $\langle \mathbb{Q}, +, \cdot \rangle$ подкольцо $\langle \mathbb{R}, +, \cdot \rangle$.
5.4 Найдите хотя бы одно подкольцо кольца $\langle \mathbb{Z}, +, \cdot \rangle$.
5.5 Покажите, почему $\langle \mathbb{N}, +, \cdot \rangle$ не является кольцом.

Поля

Коммутативное кольцо с единицей $1 \neq 0$, в котором каждый элемент $a \neq 0$ обратим, называется *полем.* Дадим эквивалентное определение.

Определение 7. *Пусть алгебраическая система $\langle P, +, \cdot \rangle$ — абелева группа, $\langle P \backslash \{0\}, \cdot \rangle$ — коммутативная группа и умножение «·» дистрибутивно относительно «+». Тогда $\langle P, +, \cdot \rangle$ называется полем.*

Если подмножество H поля $\langle P, +, \cdot \rangle$ является полем относительно операций «+» и «·», то $\langle H, +, \cdot \rangle$ называется *подполем.*

Определение 8. *Биекция между алгебраическими системами (группами, кольцами, полями), сохраняющая операции, называется изоморфизмом.*

Примеры.
Поля: $\langle \mathbb{Q}, +, \cdot \rangle$, $\langle \mathbb{R}, +, \cdot \rangle$, $\langle \mathbb{C}, +, \cdot \rangle$.
Задачи.
6.1 Докажите, что определения поля эквивалентны.
6.2 Покажите, что $\langle \mathbb{Q}, +, \cdot \rangle$ подполе $\langle \mathbb{R}, +, \cdot \rangle$.
6.3 Покажите, что $\langle \mathbb{R}, +, \cdot \rangle$ подполе $\langle \mathbb{C}, +, \cdot \rangle$.
6.4 Существует ли подполе у поля $\langle \mathbb{Q}, +, \cdot \rangle$?

Минимальные группы, кольца и поля

Определение 9. *Минимальной группой, содержащей полугруппу H, называется группа M со следующим свойством: если H собственное подмножество группы X, то M подгруппа X.*

Сравните следующее «определения». Минимальной целым, большим числа H, называется число M со следующим свойством: если $H < X$, то $M \leqslant X$. Следующим по росту после Васи является студент A про которого можно сказать следующее: если Вася ниже, скажем, B, то A не выше B.

Определение 10. *Минимальным кольцом, содержащим полукольцо H, называется кольцо M со следующим свойством: если H собственное подмножество произвольного кольца X, то M подкольцо X.*

Определение 11. *Минимальным полем, содержащим кольцо H, называется поле M со следующим свойством: если H собственного подмножество произвольного поля X, то M подполе X.*

Теперь мы можем определить целые и рациональные числа на основе понятия натуральных чисел.

Определение 12. *Минимальное кольцо, содержащее полукольцо натуральных чисел называется кольцом целых чисел $\langle \mathbb{Z}, +, \cdot \rangle$.*

Определение 13. *Минимальное поле, содержащее кольцо целых чисел, называется полем рациональных чисел $\langle \mathbb{Q}, +, \cdot \rangle$.*

Глава 2

Натуральные числа $\mathbb{N}$

Определение 14. *Множеством натуральных чисел называется множество* $\mathbb{N}$, *где определено бинарное отношение* N *и выполнены аксиомы:*

A1 *существует* $1 \in \mathbb{N}$ *такое, что для всех* $m \in \mathbb{N}$ *элемент* $(m, 1) \notin N$;
A2 *для всех* $m \in \mathbb{N}$ *существует единственный* $n \in \mathbb{N}$ *такой, что* $(m, n) \in N$;
A3 *если* $(m, n) \in N$ *и* $(k, n) \in N$, *то* $m = k$;
A4 *пусть* $M \subseteq \mathbb{N}$ *такой, что* $1 \in M$ *и из* $(m, n) \in N$ *следует* $n \in M$. *Тогда* $M = \mathbb{N}$.

Отношение $(m, n) \in N$ читается как «за m непосредственно следует n» или «n предшествует m». Аксиома A1: существует начальное число, не предшествующ

Последняя аксиома называется *аксиомой математической индукции* или просто *аксиомой индукции.*

Вторая часть второй аксиомы означает, что бинарное отношение N является всюду определенным отображением из $\mathbb{N}$ в $\mathbb{N}$. Третья аксиома означает, что N является взаимно однозначным отображением.

Лемма 5. *Любое число, кроме 1, имеет предшествующее число.*

Доказательство. Пусть M — множество, содержащее 1 и все числа, имеющие хотя бы одно предшествующее число. Докажем лемму, используя математическую индукцию. База индукции: $1 \in M$. Шаг индукции: если $n \in M$, то $n + 1$ также принадлежит M. Лемма доказана.

Из леммы 5 следует, что N имеет множество значений $\mathbb{N}\backslash\{1\}$, т.е.

$$N : \mathbb{N}\backslash\{1\} \to \mathbb{N}$$

является биекцией.

Элемент следующий за 1 обозначается через 2. Далее последовательно следуют натуральные числа 3, 4, 5, 6, 7, 8, 9, 10, ... Древние римляне обозначали натуральные числа иначе: I, II, III, IV, V, VI, VII, VIII, IX, ...

Задачи. С помощью индукции докажите леммы:

Лемма 6. *Если числа, непосредственно следующие за данными числами, различны, то и данные числа различны.*

Лемма 7. *Если данные числа различны, то непосредственно следующие за ними числа различны.*

Лемма 8. *Любое число отлично от непосредственно следующего за ним числа, т.е. для натуральных* n *справедливо* $n \neq n + 1$.

Независимость аксиом

Ответим на вопрос: «не является ли одна из аксиом теоремой, вытекающей из остальных аксиом?»

Независимость аксиомы A_1. Допустим обратное — пусть аксиома A_1 является следствием аксиом A_2, A_3 и A_4. Тогда из того, что эти аксиомы выполнены, должна следовать истинность аксиомы A_1. Противоречие со следующим примером.

Пусть $\mathbb{N} = \{1, 2, 3\}$ и $N = \{(1, 2), (2, 3), (3, 1)\}$. Непосредственная проверка показывает, что аксиомы A_2, A_3 и A_4 выполнены и A_1 не выполнена.

Примеры опровергающие какие-либо ложные утверждения называются *контрпримерами.*

Пример. Пример числа 9 опровергает неверное утверждение о том, что все нечетные числа являются простыми.

Приведем контрпримеры, доказывающие независимость аксиом.

Независимость аксиомы A_2. Пусть

$$\mathbb{N} = \{1, 2, 3, 3', 4, 4', \ldots\}, \quad N = \{(1,2), (2,3), (3,4), \ldots\} \cup \{(2,3'), (3',4'), \ldots\}.$$

Для этой системы аксиомы A_1, A_3, A_4 выполнены, но A_2 не выполнена.

Независимость аксиомы A_3. Пусть

$$\mathbb{N} = \{1, 2, 3, 4\}, \quad N = \{(1,2), (2,3), (3,4), (4,2)\}.$$

Аксиомы A_1, A_2, A_4 выполнены, но аксиома A_3 не выполнена.

Независимость аксиомы A_4. Пусть

$$\mathbb{N} = \{1, 2, 3, 4, \ldots\} \cup \{1', 2', 3', 4', \ldots\}$$

и $N = \{(1,2), (2,3), (3,4), (4,5), \ldots\} \cup \{(1',2'), (2',3'), (3',4'), (4',5'), \ldots\}$. Этот пример показывает независимость аксиомы A_4.

Математическая индукция

Из аксиомы индукции A_4 следует, что если некоторое утверждение доказано для 1 и $n+1$ в предположении, что утверждение верно при n, то это утверждение верно для каждого натурального числа.

Пример. Доказать для всех $n \in \mathbb{N}$ равенство $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$.

Доказательство. `База индукции.` *Для $n = 1$ утверждение верно.*

`Индукционное предположение.` *Предположим, что данное равенство выполнено для $n = k$ слагаемых.*

`Шаг индукции.` *Проверим равенство при $n = k + 1$:*

$$1 + 2 + \ldots + k + (k+1) =^{?} \frac{(k+1)(k+2)}{2}.$$

Левая часть по индукционному предположению равна

$$1 + 2 + \ldots + k + (k+1) = \frac{k(k+1)}{2} + (k+1).$$

Вычисляя последнюю сумму, находим, что проверяемое равенство верно.

Утверждение доказано.

Задачи. Докажите следующие тождества для каждого $n \in \mathbb{N}$:

1.1 $1 + 3 + \ldots + (2n-1) = n^2$

1.2 $1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$

1.3 $1^3 + 2^3 + \ldots + n^3 = (1 + 2 + \ldots + n)^2$.

Докажите справедливость следующих утверждений для всех $n \in \mathbb{N}$:

1.4 Справедливо неравенство $2^n > n$.

1.5 $10^n + 18n - 1$ кратно 27.

1.6 $11^{n+2} + 12^{2n+1}$ кратно 133.

1.7 Банк имеет неограниченное количество трех- и пятирублевых купюр. Докажите, что он может выдать ими без сдачи любое число рублей, начиная с восьми.

Сложения натуральных чисел

Из аксиомы A_2 следует, что отношение N на множестве натуральных чисел $\mathbb{N}$ является отображением. Далее вместо $(m,n) \in N$ пишем $m' = n$.

Определение 15. *Сложением двух натуральных чисел называется бинарная операция $+$ на $\mathbb{N}$, удовлетворяющая следующим двум условиям:*

S1 $\forall m \in \mathbb{N} \quad (m+1 = m')$;

S2 $\forall m,n \in \mathbb{N} \quad (m+n' = (m+n)')$.

Теорема 1. *Операция сложения натуральных чисел существует и единственна.*

Доказательство. Покажем, что *существует* операция сложения со свойствами S_1 и S_2. Другими словами, покажем существования отображения $f(m,n) : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ такого, что

$$\forall m \in \mathbb{N} \ \big(f(m,1) = m'\big) \ \text{ и } \ \forall m,n \in \mathbb{N} \ \big(f(m,n') = (f(m,n))'\big).$$

Построим это отображение, используя вспомогательные функции g_n.

`База индукции.` Пусть функция $g_1(m) = m'$.

`Шаг индукции.` Далее построим $g_{n'}$, используя g_n. Примем

$$g_{n'}(m) = g_n(m').$$

Таким образом, по аксиоме индукции мы построили функцию $g_n : \mathbb{N} \to \mathbb{N}$ для каждого $n \in \mathbb{N}$.

Теперь, принимая $f(m,n) = g_n(m)$ со свойствами S_1 и S_2, видим, что сложение натуральных чисел существует.

Докажем *единственность* отображения $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ со свойствами S_1 и S_2. Пусть существует отображение $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ с теми же свойствами.

Используя математическую индукцию, докажем, что эти функции совпадают. Базу индукцию составляют равенства $f(m,1) = h(m,1) = m'$, справедливые для всех $m \in \mathbb{N}$. Шаг индукции следует из равенств $h(m,n') = (h(m,n))' = (f(m,n))' = f(m,n')$.

Таким образом для всех $m,n \in \mathbb{N}$ выполнено $f(m,n) = h(m,n)$. Теорема доказана.

Предложение 1. *Сложение натуральных чисел ассоциативно.*

$$\forall\, k,m,n \in \mathbb{N} \quad (k+m)+n = k+(m+n).$$

Доказательство. Докажем индукцией по n.

При $n = 1$ утверждение верно, поскольку справедливы равенства $(k+m)+1 = (k+m)' = k+m' = k+(m+1)$, где первое и третье равенства следуют из S_1, второе равенство следует из S_2.

Из S_2 следуют равенства

$$\begin{aligned} ((k+m)+n)' &= (k+m)+n'; \\ (k+(m+n))' &= k+(m+n)' = k+(m+n'). \end{aligned}$$

Левые выражения равны по индукционному предположению. Предложение доказано.

Предложение 2. *Сложение натуральных чисел коммутативно.*

$$\forall\, m,n \in \mathbb{N} \quad m+n = n+m$$

Приведем схему доказательства. Индукцией по m докажем, что $m+1 = 1+m$. Здесь важно показать, что

$$m'+1 = (m+1)+1 = (1+m)+1 = 1+(m+1) = 1+m',$$

используя ассоциативность сложения. Затем при фиксированном m индукцией по n показать, что $m+n = n+m$.

Из предложений 1 и 2 следует, что множество натуральных чисел с операцией сложения составляют коммутативную полугруппу.

Задачи.

2.1 Докажите, что $2+2 = 4$ и $3+2 = 5$.

2.2 Докажите следующие леммы:

Лемма 9. *Для любых* $n,\ k \in \mathbb{N}$ *справедливо* $n + k \neq k$.

Лемма 10. *Для любых* $n,\ k \in \mathbb{N}$ *выполнено одно из трех утверждений:*
1) $n = k$;
2) существует $m \in \mathbb{N}$ *такой, что* $n + m = k$;
3) существует $m \in \mathbb{N}$ *такой, что* $k + m = n$.

2.3 Покажите, что множество натуральных чисел $\mathbb{N}$ с операцией сложения не является группой.

Умножение натуральных чисел

Определение 16. *Умножением двух натуральных чисел называется двухместная операция* $\cdot$, *удовлетворяющая условиям*
P1 $\forall m \in \mathbb{N} \quad (m \cdot 1 = m)$;
P2 $\forall m, n \in \mathbb{N} \quad (m \cdot n' = m \cdot n + m)$.

Пример.
Равенство $2 \cdot 2 = 4$ следует из равенств

$$2 \cdot 1' = 2 \cdot 1 + 2 = 2 + 2 = 4.$$

Теорема 2. *Операция умножение натуральных чисел существует и определена единственным образом.*

Предложение 3. *Умножение натуральных чисел дистрибутивно (при умножении справа) по сложению:*

$$\forall m, n, k \in \mathbb{N} \quad (m + n)k = mk + nk.$$

Доказательство. `База индукции`. При $k = 1$ предложение очевидно.
`Шаг индукции`. Проверим равенство $(m+n)k' =^{?} mk' + nk'$. По аксиоме P_2 левая и правая части равны $(m + n)k + (m + n)$ и $mk + m + nk + n$. Из коммутативности сложения и индукционного предположения следует, что

$$(m + n)k' = mk' + nk'.$$

Таким образом, предложение доказано.

Предложение 4. *Умножение натуральных чисел коммутативно:*

$$\forall m, n \in \mathbb{N} \quad m \cdot n = n \cdot m.$$

Доказательство. Докажем индукцией по n.
`База индукции`. При $n = 1$ предложение доказывается индукцией по m.
`Шаг индукции`. Проверим равенство $m \cdot n' =^{?} n' \cdot m$. Докажем это индукцией по m :

`База индукции`. База индукции следует из равенств

$$1 \cdot n' = 1 \cdot n + 1 = n + 1 = n' = n' \cdot 1.$$

`Шаг индукции`. Шаг индукции следует из равенств

$$m' \cdot n' = m' \cdot n + m' = (n + 1) \cdot m' = n' \cdot m'.$$

Здесь мы воспользовались предыдущим предложением о дистрибутивности.
Таким образом, предложение доказано.

Предложение 5. *Умножение натуральных чисел ассоциативно:*

$$\forall m, n, k \in \mathbb{N} \quad (mn)k = m(nk).$$

Доказательство. Докажем индукцией по k.

`База индукции.` Следует из равенств $(mn) \cdot 1 = mn = m(n \cdot 1)$.

`Шаг индукции.` Проверим равенство $(mn) \cdot k' =^? m(n \cdot k')$. Справедливы

$$(mn) \cdot k' = (mn) \cdot k + mn = m \cdot (nk) + m \cdot n = m \cdot (nk + n) = m \cdot (nk').$$

Таким образом, предложение доказано.

Задачи.

3.1 Докажите, что $3 \cdot 2 = 6$, $2 \cdot 2 = 4$.

3.2 Докажите, что $2 \cdot (2 + 1) = 6$, $(2 + 2) \cdot 2 = 8$.

3.3 Докажите, что уравнение $2 \cdot x = 3$ не имеет решений.

3.4 Докажите, что $m \cdot n = 1$ если, и только если $n = 1$ и $m = 1$.

Вычитание натуральных чисел

Определение 17. *Вычитанием двух натуральных чисел называется двухместная операция $-$ такая, что $a - b = c$ тогда и только тогда, когда $a = b + c$.*

Пример. Из $2 + 2 = 4$ следует, что $4 - 2 = 2$.

Заметим, что разность $a - b$ двух чисел определена не для всех $a, b \in \mathbb{N}$.

Характеризация множества натуральных чисел $\mathbb{N}$

Определение 18. *Пусть алгебраическая система $\langle K, +, \cdot \rangle$ является абелевой полугруппой относительно сложения «+», полугруппой относительно «·» и «·» дистрибутивно относительно «+»:*

$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ для каждого } a, b, c \in K.$$

Тогда $\langle K, +, \cdot \rangle$ называется полукольцом.

Ассоциативность и коммутативность сложения показаны в предложениях 1 и 2. Ассоциативность и дистрибутивность умножения показаны в предложениях 3, 4 и 5. Отсюда следует, что верна следующая

Теорема 3. *Множество натуральных чисел $\langle \mathbb{N}, +, \cdot \rangle$ с операцией сложения и умножения образует полукольцо.*

Справедлива

Теорема 4. *Коммутативные полукольца, удовлетворяющие аксиомам A_1, A_2, A_3, S_1, S_2, P_1 и P_2 изоморфны.*

Идея доказательства. Пусть $\langle P_1, +_1, \cdot_1 \rangle$ и $\langle P_2, +_2, \cdot_2 \rangle$ — полукольца, удовлетворяющие аксиомам A_1, A_2, A_3, S_1, S_2, P_1 и P_2. Отношения на P_1 и P_2, определяющие порядок следования, обозначим $'$ и $''$, т.е.

$$1' = 2,\ 2' = 3,\ 3' = 4, \ldots \text{ и } I'' = II,\ II'' = III,\ III'' = IV, \ldots$$

Построим биекцию φ между этими множествами натуральных чисел.

Пусть $\varphi(1) = I$ и $\varphi(a') = \varphi(a)'$. Индукцией по a можно показать, что это отображение является всюду определеной и взаимно однозначным отображением P_1 на P_2.

Далее индукцией по b нужно показать, что

$$\begin{aligned} \varphi(a +_1 b) &= \varphi(a) +_2 \varphi(b) \\ \varphi(a \cdot_1 b) &= \varphi(a) \cdot_2 \varphi(b) \end{aligned}$$

для всех $a \in \mathbb{N}$.

Задачи.

5.1 Являются ли $\langle \mathbb{N}, -, \cdot \rangle$ и $\langle \mathbb{Z}, -, \cdot \rangle$ полукольцами?

5.2 Являются ли $\langle \mathbb{Z}, +, \cdot \rangle$ и $\langle \mathbb{Q}, +, \cdot \rangle$ полукольцами?

5.3 Пусть $2\mathbb{N} = \{2a \mid a \in \mathbb{N}\}$. Будет ли $\langle 2\mathbb{N}, +, \cdot \rangle$ полукольцом?

5.4 Постройте изоморфизм полугрупп $\langle \mathbb{N}, + \rangle$ и $\langle 2\mathbb{N}, + \rangle$

Порядок на множестве натуральных чисел

Если для натуральных чисел m и n существует натуральное число k такое, что $m = n+k$, то говорят, что m *больше* n. Это отношение обозначается как $m > n$ или $n < m$ и обладает свойствами:

Лемма 11. *Если* $k > m$, $m > n$, *то* $k > n$.

Лемма 12. *Для любых двух натуральных чисел* m *и* n *верно одно из трех отношений* $m = n$, $m > n$ *или* $n > m$.

Доказательство. Докажем индукцией по n утверждение равносильное лемме: для каждого $n \in \mathbb{N}$ объединение множеств $A_n = \{m \mid n > m\}$, $\{n\}$ и $B_n = \{m \mid m > n\}$ равно множеству всех натуральных чисел.

`База индукции`. Пусть $n = 1$. Тогда любое число $m \neq 1$ по лемме 5 имеет предшествующее число k, что равносильно равенствам $k' = k + 1 = m$. Из коммутативности сложения следует, что $m = 1 + k$ для $k \in \mathbb{N}$. Это означает $m > 1$ для всех $m \in \mathbb{N}$, кроме единицы.

`Шаг индукции`. Используя лемму 11, легко разобрать, что

$$A_{n+1} = A_n \cup \{n\} \quad \text{и} \quad B_{n+1} = B_n \backslash \{n+1\}.$$

Тогда $A_{n+1} \cup \{n+1\} \cup B_{n+1} = \mathbb{N}$. Лемма доказана.

Лемма 13. *Неравенство* $m > n$ *равносильно, каждому из неравенств*

$$m + k > n + k \qquad \textit{и} \qquad mk > nk$$

для любого $k \in \mathbb{N}$.

Лемма 14. *Из неравенства* $m > n$ *и* $a > b$ *следует*

$$am > bn.$$

Лемма 15. *Число 1 является наименьшим среди натуральных чисел, или другими словами, для любого* $n \in \mathbb{N}$ *справедливо неравенство* $n \geqslant 1$.

Лемма 16 (аксиома Архимеда)**.** *Для любых* m *и* n *существует число* k *такое, что* $mk > n$.

Доказательство. Достаточно взять k равным $n + 1$. Поскольку $m \geqslant 1$, то по лемме 14 справедливо неравенство $(n + 1)m \geqslant n \cdot 1 = n$.

Лемма 17. *Не существуют такие числа, что* $n + 1 > m > n$.

Лемма 18. *Любое непустое множество натуральных чисел содержит наименьшее число.*

Задачи.

6.1 Покажите, что $3 > 1$.
6.2 Покажите, что $nm > m$ для всех $m, n \in \mathbb{N}$.
6.3 Покажите, что $n^2 + m^2 > 2nm$ для всех $m, n \in \mathbb{N}$.
6.4 Докажите, что $2^n > n^2$ для всех натуральных $n > 4$.
6.5 Восстановите пропущенные доказательства лемм.

Основная теорема арифметики

Натуральное число $p > 1$ называется *простым,* если p не имеет делителей, отличных от 1 и p.

Теорема 5 (Основная теорема арифметики)**.** *Для каждого натурального числа* $n > 1$ *существует единственное разложение на простые множители:*

$$n = p_1^{a_1} p_2^{a_2} \cdot \ldots \cdot p_k^{a_k},$$

где $p_1, p_2, ..., p_k$ *— простые числа,* $a_1, a_2, ..., a_k$ *— натуральные числа.*

Задачи (не обязательны для решения).

7.1 На какую цифру заканчивается число 777^{777}?
7.2 Найдите все решения уравнения $4x + 2y = 2007$.
7.3 Может ли разность чисел вида $n^2 + 2n$ равняться 2006?
7.4 Разложите 2009 на простые сомножители.

Глава 3

Целые числа $\mathbb{Z}$

Минимальным кольцом, содержащим полукольцо H, называется кольцо M со следующим свойством: если H подмножество X, то M подкольцо X.

Определение 19. *Минимальное кольцо, содержащее полукольцо натуральных чисел называется кольцом целых чисел* $\langle \mathbb{Z}, +, \cdot \rangle$.

Замечание. Здесь «$\mathbb{Z}$ содержит $\mathbb{N}$» имеет смысл «$\mathbb{Z}$ содержит полукольцо изоморфное $\mathbb{N}$». Это естественно, поскольку мы не различаем изоморфные алгебраические системы.

Теорема 6. *Кольцо натуральных чисел состоит из элементов* $\mathbb{N} \cup \{0\} \cup \mathbb{N}^-$, *где* $\mathbb{N}^-$ *— некоторое множество, биективное* $\mathbb{N}$.

Определение 20. *Разностью двух целых чисел m и n называется число x такое, что $x + n = m$. Число x обозначается через $m - n$.*

Существование кольца целых чисел

В этом параграфе построим кольцо изоморфное обычному кольцу целых чисел. Для этого рассмотрим $\bar{\mathbb{Z}} = \{(a, b) \mid a, b \in \mathbb{N}\}$. Будем считать, что (a, b) и $(c, d) \in \bar{\mathbb{Z}}$ эквивалентны только в случае

$$(a, b) \sim (c, d) \;\Leftrightarrow\; a + d = c + b.$$

Замечание. Далее будет показано, что двойке (a, b) соответствует $a - b \in \mathbb{Z}$.

Ясно, что **1** всегда $(a, b) \sim (a, b)$;
2 если $(a, b) \sim (c, d)$, то $(c, d) \sim (a, b)$;
3 если $(a, b) \sim (c, d)$ и $(c, d) \sim (e, f)$, то $(a, b) \sim (e, f)$.

Отношения, обладающие тремя свойствами 1, 2, и 3 называются *отношениями эквивалентности*. Такие отношения разбивают $\bar{\mathbb{Z}}$ на непересекающиеся *классы эквивалентности*. Множество классов эквивалентности обозначают через $\bar{\mathbb{Z}}/_\sim$.

Пример. Двухместное отношение А $\sim$ В — «А и В учатся в одной учебной группе» на множестве S студентов ИМИ ЯГУ является отношением эквивалентности. Классы эквивалентности — учебные группы, множество $S/_\sim$ — множество учебных групп.

Класс эквивалентности, содержащий (a, b), обозначается через $\overline{(a, b)}$.

Пример. Если Иван А. из группы МПО-97, то $\overline{\text{Иван А.}}$ = МПО-97.

Определим на $\bar{\mathbb{Z}}/_\sim$ операции сложения и умножения:

$$\begin{aligned} \overline{(a, b)} + \overline{(c, d)} &= \overline{(a + c, b + d)}; \\ \overline{(a, b)} \cdot \overline{(c, d)} &= \overline{(ac + bd, ad + bc)}. \end{aligned}$$

Если $A, B, C, D \in \bar{\mathbb{Z}}/_\sim$, $A \sim C$ и $B \sim D$, то

$$A + B \sim C + D \;\text{ и }\; A \cdot B \sim C \cdot D.$$

Отсюда следует корректность определения сложения и умножения классов эквивалентности $\bar{\mathbb{Z}}/_\sim$.

Теперь покажем, что $\langle \bar{\mathbb{Z}}/_\sim, +, \cdot \rangle$ — кольцо. Для этого проверим аксиомы кольца.

1) Сложение очевидно ассоциативно.
2) Нулевой элемент $\overline{(1, 1)} \in \bar{\mathbb{Z}}/_\sim$ существует.
3) Обратным элементом $\overline{(a, b)}$ является $\overline{(b, a)} \in \bar{\mathbb{Z}}/_\sim$.
4) Сложение очевидно коммутативно.

5) Произведение ассоциативно.

6) Произведение дистрибутивно по сложению.

Выделим множество $\bar{\mathbb{N}} = \{(a+1,1) \mid a \in \mathbb{N}\} \subseteq \bar{\mathbb{Z}}$. Очевидно, $\bar{\mathbb{N}}/_\sim$ является полугруппой, изоморфной $\mathbb{N}$.

Покажем, что $\bar{\mathbb{Z}}/_\sim$ является минимальным кольцом, содержащим $\mathbb{N}$.

Обозначим минимальное кольцо, содержащее $\bar{\mathbb{N}}$, через $\mathbb{M}$.

Поскольку $\mathbb{M}$ минимальное кольцо, то $\mathbb{M} \subset \bar{\mathbb{Z}}/_\sim$.

Рассмотрим произвольный $\overline{(a,b)} \in \bar{\mathbb{Z}}/_\sim$ равный $\overline{(a+2,b+2)}$. Тогда $\overline{(a+1,1)}$ и $\overline{(b+1,1)} \in \bar{\mathbb{N}} \subseteq \mathbb{M}$. Обратный $\overline{(1,b+1)}$ к элементу $\overline{(b+1,1)}$ должен принадлежать $\mathbb{M}$. Теперь сумма $\overline{(a+1,1)} + \overline{(1,b+1)} = \overline{(a+2,b+2)}$ также принадлежит $\mathbb{M}$. Следовательно, $\bar{\mathbb{Z}}/_\sim \subseteq \mathbb{M}$.

Таким образом, мы построили кольцо целых чисел $\bar{\mathbb{Z}}/_\sim$.

Мы представили произвольное целое число $\overline{(a,b)}$ в виде разности двух натуральных чисел $\overline{(a+1,1)} + \overline{(1,b+1)}$. Следовательно, верна следующая

Лемма 19. *Каждое целое число можно представить в виде разности двух натуральных.*

Класс $\overline{(a+1,1)}$ обозначают через a, $\overline{(1,a+1)}$ через $-a$, $\overline{(1,1)} - 0$.

Задачи (не обязательные для решения).

8.1 Какой элемент $\bar{\mathbb{Z}}/_\sim$ соответствует -1 и 0?

8.2 Пусть на $\mathbb{Z}$ задано отношение эквивалентности: $a \sim b \Leftrightarrow n|(a-b)$ для некоторого целого n. Найти $|\mathbb{Z}/_\sim|$. Доказать, что $\langle \mathbb{Z}/_\sim, +, \cdot \rangle$ является кольцом.

Свойства целых чисел

Лемма 20. *Для каждого $a \in \mathbb{Z}$ выполнены равенства*

$$a \cdot 0 = 0 \cdot a = 0.$$

Доказательство. Из свойства нуля следует равенство $a \cdot 0 = a \cdot (0+0)$. Согласно дистрибутивности произведения относительно сложения $a \cdot (0+0) = a \cdot 0 + a \cdot 0$. В правую и левую части равенства $a \cdot 0 = a \cdot 0 + a \cdot 0$ прибавим обратный элемент $a \cdot 0$. Отсюда следует равенство $a \cdot 0 = 0$. Лемма доказана.

Лемма 21. *Для всех $a, b \in \mathbb{Z}$ выполнены равенства*

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

Доказательство. Рассмотрим сумму $(-a) \cdot b + a \cdot b$. Согласно закону дистрибутивности эта сумма равна нулю. Следовательно, $(-a) \cdot b$ является обратным к $a \cdot b$.

По дистрибутивности сумма $a \cdot (-b) + a \cdot b = 0$. Следовательно, $a \cdot (-b)$ является обратным к $a \cdot b$. Лемма доказана.

Лемма 22. *Для любого $a \in \mathbb{N}$ произведение $(-1) \cdot a$ равно обратному $-a$:*

$$(-1) \cdot a = -a.$$

Доказательство. Умножим произвольное целое $\overline{(n,m)} \in \bar{\mathbb{Z}}/_\sim$ на $\overline{(1,2)}$. Результат $\overline{(n,m)} \cdot \overline{(1,2)} = \overline{(n+2m, m+2n)}$. Очевидно, $\overline{(n+2m, m+2n)}$ является обратным элементом к $\overline{(m,n)}$. Лемма доказана.

Лемма 23. *Для всех $a, b, c \in \mathbb{Z}$ выполнены равенства*

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

Доказательство. Следует из дистрибутивности умножения относительно сложения и предыдущих лемм:

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

Лемма доказана.

Лемма 24. *Умножение целых чисел коммутативно.*

Доказательство. По лемме 19 всякое целое число можно представить в виде разности натуральных чисел $x = a - b$, $y = c - d$.

$$\begin{aligned} x \cdot y &= (a-b)\cdot(c-d) = a\cdot c - b\cdot c + b\cdot d - a\cdot d \\ &= ca - cb + db - da = c(a-b) + d(b-a) = (c-d)(a-b) \\ &= y \cdot x. \end{aligned}$$

Лемма доказан.

Лемма 25. *Квадрат ненулевого целого числа $n \in \mathbb{Z}$ является натуральным числом.*

Доказательство.

Квадрат произвольного целого числа $(\overline{n,m}) \in \bar{\mathbb{Z}}/_\sim$ равен $(\overline{n^2+m^2, 2nm})$. Из неравенства Коши $n^2 + m^2 > 2nm$ следует, что квадрат произвольного целого числа является натуральным числом. Лемма доказана.

Пример. В кольце матриц умножение не является коммутативным:

$$\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 1\\ 2 & 2\end{pmatrix} = \begin{pmatrix}3 & 3\\ 1 & 1\end{pmatrix}, \quad \begin{pmatrix}1 & 1\\ 2 & 2\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}2 & 1\\ 4 & 2\end{pmatrix}.$$

Лемма 26. *Если произведение двух целых чисел равно нулю, то хотя бы одно из этих чисел равно нулю.*

Доказательство. Докажем утверждение от обратного. Предположим противное: пусть существуют ненулевые целые числа a и b такие, что $a \cdot b = 0$. Рассмотрим квадрат этого произведения $c = (a \cdot b)^2 = (a \cdot b) \cdot (a \cdot b)$. Используя коммутативность умножения получаем, что $c = (a \cdot b) \cdot (b \cdot a)$. Ассоциативность позволяет изменит порядок произведения следующим образом: $c = a^2 \cdot b^2$. Поскольку по лемме 25 квадраты $a^2, b^2 \in \mathbb{N}$, то $c \in \mathbb{N}$. Следовательно, с одной стороны $a \cdot b = 0$, с другой стороны $(a \cdot b)^2 = c \neq 0$.

Противоречие. Лемма доказана.

Задачи (не обязательные для решения).

8.1 Покажите, что для любого $a \in \mathbb{Z}$ справедливо $0 - a = -a$.

8.2 Покажите, что для любого $a, b \in \mathbb{Z}$ справедливо $(-a)(-b) = ab$.

8.3 Уравнения вида

$$\alpha_1 a_1 + \alpha_2 a_2 + \ldots \alpha_n a_n, \quad \alpha_1, \ldots \alpha_n \in \mathbb{Z},$$

которые нужно разрешить относительно $a_1, \ldots, a_n \in \mathbb{Z}$, называются *диофантовыми*. Найти все решения диофантова уравнения $2a + 3b = 1$.

Порядок в кольце целых чисел.

Определение 21. *Если $a - b \in \mathbb{N}$, то a больше b или, иначе говоря, b меньше a. Это отношение обозначается через $a > b$ и $b < a$.*

Лемма 27. *Для всех a, b целых чисел верно одно из следующих утверждений: либо $a > b$, либо $b > a$, либо $a = b$.*

Доказательство. Рассмотрим $a-b$. Поскольку $a-b$ является целым числом, то либо $a-b \in \mathbb{N}^+$, либо $a - b \in \mathbb{N}^-$, либо $a - b = 0$. Лемма доказана.

9.1 Покажите, что $2 + (-3) = -1$.

9.2 Покажите, что $-1(2) = -2$.

9.3 Покажите, что $7 \cdot 2 = 14$.

9.4 Покажите, что для любого $a, b \in \mathbb{Z}$ справедливо $a^2 + b^2 > 2ab$.

9.5 Покажите, что для любого $x \in \mathbb{Z}$ и $n \in \mathbb{N}$ справедливо

$$(1 + a)^n > 1 + na.$$

Глава 4

Рациональные числа $\mathbb{Q}$

Минимальным полем, содержащим кольцо K, называется поле P со свойством: если K подкольцо произвольного поля F, то P подполе F.

Определение 22. *Минимальное поле, содержащее кольцо целых чисел, называется полем рациональных чисел* $\langle \mathbb{Q}, +, \cdot \rangle$.

Замечание. Здесь «$\mathbb{Q}$ содержит $\mathbb{Z}$» имеет смысл «$\mathbb{Q}$ содержит кольцо изоморфное $\mathbb{Z}$». Это естественно, поскольку мы не различаем изоморфные алгебраические системы.

Существование поля рациональных чисел

Построим поле $\bar{\mathbb{Q}}$, изоморфное полю рациональных чисел. Пусть множество

$$T = \mathbb{Z} \times \mathbb{N} = \{(a, b) \,|\, a \in \mathbb{Z}, b \in \mathbb{N}\}.$$

Считаем, что $(a, b) \in T$ и $(c, d) \in T$ *эквивалентными, т.е.* $(a, b) \sim (c, d)$, если $ad = bc$.
Замечание. Далее будет показано, что двойке (a, b) соответствует $a/b \in \mathbb{Q}$.

Ясно, что **1** всегда $(a, b) \sim (a, b)$;
2 если $(a, b) \sim (c, d)$, то $(c, d) \sim (a, b)$;
3 если $(a, b) \sim (c, d)$ и $(c, d) \sim (e, f)$, то $(a, b) \sim (e, f)$.

Таким образом, отношение $\sim$ является *отношениями эквивалентности*. Следовательно, $\sim$ разбивает T на непересекающиеся классы. Класс, содержащий (a, b), будем обозначать как $(\overline{a, b})$.
Пример. $(\overline{4, 3}) = (\overline{8, 6})$, поскольку $(4, 3) \sim (8, 6)$.

Полученное множество классов $T/_\sim$. обозначим через $\bar{\mathbb{Q}}$.

Определение 23. *Введем операцию сложения на множестве* $\bar{\mathbb{Q}}$:

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

Лемма 28. $\langle \bar{\mathbb{Q}}, + \rangle$ — *коммутативная группа.*

Доказательство. Операция сложения «+» на $\bar{\mathbb{Q}}$ определена с помощью всюду определенных операций, поэтому «+» является всюду определенной операцией.

Проверим аксиомы группы для $\langle \bar{\mathbb{Q}}, + \rangle$.

Ассоциативность. Проверим равенство выражений

$$\big((\overline{a, b}) + (\overline{c, d})\big) + (\overline{e, f}) = (\overline{ad + bc, bd}) + (\overline{e, f})$$

и

$$(\overline{a, b}) + \big((\overline{c, d}) + (\overline{e, f})\big) = (\overline{a, b}) + (\overline{cf + de, df}).$$

Непосредственная проверка показывает, что оба выражения равны

$$(\overline{adf + bcf + bde, bdf}).$$

Существование нейтрального элемента. Элемент $(\overline{0, 1})$ является нулевым. Рассмотрим сложение $(\overline{0, 1})$ с произвольным рациональным $(\overline{a, b})$:

$$(\overline{a, b}) + (\overline{0, 1}) = (\overline{0, 1}) + (\overline{a, b}) = (\overline{a, b}).$$

Существование обратного элемента. Для элемента $(\overline{a,b})$ обратным является $(\overline{-a,b})$. Рассмотрим их сложение:

$$(\overline{a,b}) + (\overline{-a,b}) = (\overline{-a,b}) + (\overline{a,b}) = (\overline{0,b}) = (\overline{0,1}).$$

Коммутативность. Очевидно.
Лемма доказана.

Определение 24. *Введем операцию умножения на множестве* $\bar{\mathbb{Q}}$:

$$(\overline{a,b}) \cdot (\overline{c,d}) = (\overline{ac,bd}).$$

Лемма 29. $\langle \bar{\mathbb{Q}}, \cdot \rangle$ — *коммутативная группа.*

Доказательство. **Ассоциативность.** Справедливы равенства:

$$\begin{aligned} \big((\overline{a,b}) \cdot (\overline{c,d})\big) \cdot (\overline{e,f}) &= (\overline{ac,bd}) \cdot (\overline{e,f}) = (\overline{ace,bdf}) \\ &= (\overline{a,b}) \cdot (\overline{ce,df}) = (\overline{a,b}) \cdot \big((\overline{c,d}) \cdot (\overline{e,f})\big). \end{aligned}$$

Существование единичного элемента. Единичность элемента $(\overline{1,1})$ следует из следующего равенства

$$(\overline{a,b}) \cdot (\overline{1,1}) = (\overline{a,b}).$$

Существование обратного элемента. Для произвольного $(\overline{a,b}) \neq (\overline{0,1})$ элемент

$$\begin{cases} (\overline{b,a}) \text{ при } a > 0, \\ (\overline{-b,-a}) \text{ при } a < 0 \end{cases}$$

является обратным к $(\overline{a,b})$.
Коммутативность.

$$(\overline{a,b}) \cdot (\overline{c,d}) = (\overline{ac,bd}) = (\overline{c,d}) \cdot (\overline{a,b}).$$

Лемма доказана.
Из леммы 28 и 29 следует справедливость следующей

Теорема 7. $\langle \bar{\mathbb{Q}}, +, \cdot \rangle$ — *коммутативное поле.*

Теорема 8. $\langle \bar{\mathbb{Q}}, +, \cdot \rangle$ — *поле рациональных чисел.*

Доказательство. $\mathbb{Z}$ **является подкольцом** $\overline{\mathbb{Q}}$. Рассмотрим $\overline{\mathbb{Z}} \cong \mathbb{Z} \times \{1\}/_{\sim} = \{(\overline{a,1}) \,|\, a \in \mathbb{Z}\}$. Легко проверить, что взятие обратного, сложение и произведение элементов $\overline{\mathbb{Z}}$ дает элемент $\overline{\mathbb{Z}}$:

$$(\overline{a,1}) + (\overline{b,1}) = (\overline{a+b,1}), \quad (\overline{a,1}) \cdot (\overline{b,1}) = (\overline{ab,1}), \quad -(\overline{a,1}) = (\overline{-a,1}),$$

Таким образом, $\overline{\mathbb{Z}}$ является подкольцом $\overline{\mathbb{Q}}$.
Покажем, что имеет место изоморфизм $\overline{\mathbb{Z}} \cong \mathbb{Z}$. Пусть отображение $f : \overline{\mathbb{Z}} \to \mathbb{Z}$ задано по правилу $f\big((\overline{a,1})\big) = a$.
1. Отображение f всюду определено, поскольку для каждого элемента $(\overline{a,1}) \in \overline{\mathbb{Z}}$ существует элемент $a \in \mathbb{Z}$ такой, что $f\big((\overline{a,1})\big) = a$.
2. Отображение f является отображением на $\mathbb{Z}$, поскольку для каждого элемента $a \in \mathbb{Z}$ существует элемент $(a,1) \in \overline{\mathbb{Z}}$ такой, что $f\big((a,1)\big) = a$.
3. Из равенства $f\big((\overline{a,1})\big) = f\big((\overline{b,1})\big)$ следует, что $a = b$, поэтому отображение f взаимнооднозначно.
Таким образом, f является биекцией, задающей изоморфизм $\overline{\mathbb{Z}} \cong \mathbb{Z}$.
$\overline{\mathbb{Q}}$ **является минимальным полем, содержащим** $\mathbb{Z}$. Минимальное поле, содержащее $\mathbb{Z}$, обозначим через $\mathbb{Q}$. Ясно, что $\mathbb{Q} \subset \overline{\mathbb{Q}}$.
В поле с каждым ненулевым элементом $\mathbb{Q}$ содержит и обратный элемент. Поэтому обратные элементы $(1,a)$ чисел вида $(a,1) \in \overline{\mathbb{Z}}$ содержатся в $\mathbb{Q}$. Тогда в $\mathbb{Q}$ содержатся все элементы вида (b,a) как произведения чисел вида $(1,a)$ и $(b,1)$. Следовательно, $\overline{\mathbb{Q}} \subset \mathbb{Q}$.
Таким образом, $\mathbb{Q} = \overline{\mathbb{Q}}$ — минимальное поле, содержащее $\mathbb{Z}$.
Теорема доказана.

Поле рациональных чисел

Далее вместо (a, b) всегда пишем $\frac{a}{b}$. Из теоремы 8 следует

Теорема 9. *Поле рациональных чисел состоит из элементов*

$$\left\{\frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{N}\right\},$$

где операции «+» и «·» определены следующим образом

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Задачи.

10.1 Покажите, что $(10^{10}, 5^5) \sim (10^5 \cdot 2^5, 1)$.

10.2 Покажите, что $(\overline{1,2}) = (\overline{3,6})$.

10.3 Вычислите $(\overline{1,2}) + (\overline{3,7})$, $(\overline{1,5}) \cdot (\overline{2,3})$, $(\overline{2,3}) \cdot (\overline{2,5})$,

10.4 Решите уравнение $\big((\overline{x,y}) + (\overline{2,5})\big) \cdot (\overline{5,11}) = (\overline{1,2})$.

Упорядоченное поле рациональных чисел

Определение 25. *Если $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ и $ad < bc$, то $\frac{a}{b}$ больше $\frac{c}{d}$ или, иначе говоря, $\frac{c}{d}$ меньше $\frac{a}{b}$. Это отношение обозначается через*

$$\frac{a}{b} > \frac{c}{d}, \quad \frac{c}{d} < \frac{a}{b}.$$

Лемма 30. *Для всех $\frac{a}{b}$ и $\frac{c}{d}$ рациональных чисел верно одно из следующих утверждений: либо $\frac{a}{b} > \frac{c}{d}$, либо $\frac{a}{b} < \frac{a}{b}$, либо $\frac{a}{b} = \frac{c}{d}$.*

Доказательство. Рассмотрим ad, $bc \in \mathbb{Z}$. По лемме об упорядочивании целых чисел верно одно из утверждений либо $ad > bc$, либо $ad < bc$, либо $ad = bc$. Каждый из этих утверждений равносильно с одним из утверждений леммы. Лемма доказана.

Лемма 31 (Аксиома Архимеда)**.** *Для любого рационального числа $\frac{a}{b}$ существует натуральное, число, большее чем $\frac{a}{b}$.*

Доказательство. Сравним натуральное число $|a| + 1$ с рациональным числом $\frac{a}{b}$. Поскольку

$$b(|a| + 1) > |a| + 1 > a,$$

то лемма верна.

Существование не рациональных чисел.

Лемма 32. *Если $a^2 = 2$, то $a \notin \mathbb{Q}$.*

Доказательство. Допустим, что верно обратное утверждение: *существует несократимая дробь $\frac{a}{b} \in \mathbb{Q}$ такая, что $\left(\frac{a}{b}\right)^2 = 2$.* Последнее равенство равносильно уравнению $a^2 = 2b^2$. Несложно увидеть, что a^2 является четным числом. Это означает, что a также является четным числом. Пусть $a = 2u$. Тогда исследуемое уравнение равносильно уравнению $2u^2 = b^2$. Это означает, что b является четным. Противоречие с нашим допущением о том, что $\frac{a}{b}$ является несократимой дробью. Лемма доказана.

Задачи.

11.1 Покажите, что число $\sqrt{3}$ не является рациональным числом.

11.2 Докажите, что между числам $(\overline{1,2})$ и $(\overline{1,1})$ существует бесконечное число рациональных чисел.

Глава 5

Действительные числа $\mathbb{R}$

Определение 26. *Разбиением $A|A'$ множества рациональных чисел называется пара непустых множеств $A, A' \subseteq \mathbb{Q}$ таких, что $A \cup A' = \mathbb{Q}$ и $A \cap A' = \varnothing$. Разбиение $A|A'$ множества рациональных чисел называется сечением, если для любых $a \in A$ и $a' \in A'$ выполнено неравенство $a < a'$.*

Множество A называется нижним классом сечения, а A' — верхним классом сечения.

Лемма 33. *Не существуют сечения $A|A'$ такие, что A имеет наибольший элемент и A' содержит наименьший элемент.*

Доказательство. Докажем от обратного. Допустим A имеет наибольший элемент a, а A' имеет наименьший элемент a'. Тогда число $\frac{a+a'}{2}$ является рациональным числом и не содержится ни в A, ни в A', поскольку больше наибольшего $a < \frac{a+a'}{2}$ и меньше наименьшего $\frac{a+a'}{2} < a'$. Противоречие с тем, что $A|A'$ является сечением. Лемма доказана.

Таким образом сечения могут быть только трех типов:

а) $\{x \in \mathbb{Q} \,|\, x < a\}|\{x \in \mathbb{Q} \,|\, a \leqslant x\}$ для некоторого $a \in \mathbb{Q}$;

б) $\{x \in \mathbb{Q} \,|\, x \leqslant a\}|\{x \in \mathbb{Q} \,|\, a < x\}$ для некоторого $a \in \mathbb{Q}$;

в) $A|A'$, где A не имеет максимальный элемент, а A' — минимальный.

Пример. Сечение типа в):

$$\mathbb{Q}^- \cup \{0\} \cup \{x \in \mathbb{Q}^+ \,|\, x^2 \leqslant 2\}|\{x \in \mathbb{Q}^+ \,|\, 2 < x^2\}.$$

Определение 27. *Множество всех сечений рациональных чисел называются множеством действительных чисел. Сечения типа* в) *называются иррациональными числами.*

Множество действительных чисел обозначается как $\mathbb{R}$. Считаем, что рациональному числу a сопоставлено сечение типа б).

Два действительных числа $\alpha = A|A'$ и $\beta = B|B'$ считаются равными, если $A = B$ и $A' = B'$.

Упорядочение вещественных чисел

Определение 28. *Если $\alpha = A|A'$, $\beta = B|B'$ — сечения и $A \subset B$, то β больше α или, иначе говоря, α меньше β. Это отношение обозначается через $\alpha < \beta$ и $\beta > \alpha$.*

Лемма 34. *Для всех α и β действительных чисел верно одно из следующих утверждений: либо $\alpha > \beta$, либо $\alpha < \beta$, либо $\alpha = \beta$.*

Доказательство. Пусть $\alpha = A|A'$ и $\beta = B|B'$. Возможны случаи: либо $A \supseteq B$, либо $A \subseteq B$, либо $A = B$. Лемма доказана.

Лемма 35. *Из $\alpha > \beta$ и $\beta > \gamma$ следует $\alpha > \gamma$.*

Доказательство. Пусть $\alpha = A|A'$, $\beta = B|B'$ и $\gamma = C|C'$. Неравенства $\alpha > \beta$ и $\beta > \gamma$ означают $A \supset B$ и $B \supset C$. Следовательно, справедливо $A \supset C$, что означает $\alpha > \gamma$. Лемма доказана.

Сумма действительных чисел

Определение 29. *Суммой действительных чисел $\alpha = A|A'$, $\beta = B|B'$ называется число $\gamma = C|C'$ такое, что*

$$C = \{a + b \,|\, a \in A, b \in B\}.$$

Число γ обозначается как $\alpha + \beta$.

Лемма 36. *Сложение действительных чисел является коммутативной операцией.*

Доказательство. Утверждение леммы следует из равенств

$$A|A' + B|B' = \{a + b \,|\, a \in A, b \in B\}|\{a + b \,|\, a' \in A', b' \in B'\}$$

$$= \{b + a \,|\, b \in B, a \in A\} \,|\, \{b + a \,|\, b' \in B', a' \in A'\} = B|B' + A|A'.$$

Лемма доказана.

Следующая лемма является очевидной

Лемма 37. *Сложение действительных чисел является ассоциативной операцией.*

Лемма 38. *Для любого $\alpha \in \mathbb{R}$*

$$\alpha + 0 = \alpha.$$

Доказательство. Число 0 задается сечением $\mathbb{Q}^- \cup \{0\}|Q^+$. Пусть $\alpha = A|A'$. Лемма следует из следующих равенств

$$A|A' + \mathbb{Q}^- \cup \{0\}|Q^+ = \left\{a + b \,|\, a \in A, b \in \mathbb{Q}^- \cup \{0\}\right\} \,|\, \ldots = A|A'.$$

Последнее равенство можно установить следующими рассуждениями.

Если $c \in \{a + b \,|\, a \in A, b \in \mathbb{Q}^- \cup \{0\}\}$, то $c = a + b$ для некоторых $a \in A$ и $b \leqslant 0$; следовательно, $c \leqslant a \in A$; то $c \in A$.

Если $c \in A$ то $c = c + 0$ следовательно, $c \in \{a + b \,|\, a \in A, b \in \mathbb{Q}^- \cup \{0\}\}$.

Таким образом, $\{a + b \,|\, a \in A, b \in \mathbb{Q}^- \cup \{0\}\} = A$.

Лемма доказана.

Лемма 39. *Для любого $\alpha \in \mathbb{R}$ существует $\beta \in \mathbb{R}$ такой, что*

$$\alpha + \beta = 0.$$

Доказательство. Введем обозначение $-A = \{-a \,|\, a \in A\}$. Естественно, тогда $-A' = \{-a \,|\, a \in A'\}$.

Если $\alpha = A|A'$, то пусть $\beta = -A'| - A$ и

$$C \,|\, C' = \alpha + \beta.$$

Тогда

$$C = \{a + b \,|\, a \in A, b \in -A'\} = \{a - b \,|\, a \in A, b \in A'\}.$$

Из неравенства $a < b$ для $a \in A$ и $b \in A'$ следует, что $a - b \in \mathbb{Q}^-$ и $C \subseteq \mathbb{Q}^-$. Покажем, что верно и обратное включение.

Произведение действительных чисел

Определение 30. *Произведением действительных чисел $\alpha = A|A'$, $\beta = B|B'$ называется число $\gamma = C|C'$ такое, что*

$$C = \{ab \,|\, a \in A, b \in B\}.$$

Число γ обозначается как $\alpha \cdot \beta$ или $\alpha\beta$.

Лемма 40. *Произведение действительных чисел является коммутативной операцией.*

Доказательство. Утверждение леммы следует из равенств

$$A|A' \cdot B|B' = \{ab \,|\, a \in A, b \in B\}|\{a'b' \,|\, a' \in A', b' \in B'\}$$

$$= \{ba \,|\, b \in B, a \in A\} \,|\, \{b'a' \,|\, b' \in B', a' \in A'\} = B|B' \cdot A|A'.$$

Лемма доказана.

Лемма 41. *Произведение действительных чисел является ассоциативной операцией.*

Доказательство. Утверждение леммы следует из равенств

$$A|A' + B|B' = \{a + b \,|\, a \in A, b \in B\}|\{a' + b' \,|\, a' \in A', b' \in B'\}$$

$$= \{b + a \,|\, b \in B, a \in A\} \,|\, \{b' + a' \,|\, b' \in B', a' \in A'\} = B|B' + A|A'.$$

Лемма доказана.

Лемма 42. *Для каждого* $\alpha \in \mathbb{R}$

$$\alpha \cdot 1 = \alpha.$$

Доказательство. Число 1 задается сечением $\{b \,|\, b \leqslant 1\}|\{b' \,|\, b' > 1\}$. Пусть $\alpha = A|A'$. Лемма следует из следующих равенств

$$A|A' \cdot \{b \,|\, b \leqslant 1\}|\{b' \,|\, b' > 1\} = A|A'.$$

Последнее равенство можно установить следующими рассуждениями.

Лемма доказана.

Лемма 43. *Для каждого* $\alpha \in \mathbb{R}$ *существует* $\beta \in \mathbb{R}$ *такой, что*

$$\alpha\beta = 1.$$

Доказательство. Введем обозначение $-A = \{-a \,|\, a \in A\}$. Естественно, тогда $-A' = \{-a \,|\, a \in A'\}$.

Если $\alpha = A|A'$, то пусть $\beta = -A'| - A$ и

$$C \,|\, C' = \alpha + \beta.$$

Тогда

$$C = \{a + b \,|\, a \in A, b \in -A'\} = \{a - b \,|\, a \in A, b \in A'\}.$$

Из неравенства $a < b$ для $a \in A$ и $b \in A'$ следует, что $a - b \in \mathbb{Q}^-$ и $C \subseteq \mathbb{Q}^-$. Покажем, что верно и обратное включение.

Лемма доказана.

Из лемм 36 - 43 следует

Теорема 10. $\langle \mathbb{R}, +, \cdot \rangle$ *— поле действительных чисел.*

Глава 6

Комплексные числа $\mathbb{C}$

Литература

1. С. Феферман *Числовые системы.* М.:Наука, 1971.

3. *Энциклопедия элементарной математики. т 1. Арифметика.*/ под. ред. П.С. Александрова, А.И. Маркушевича, А.Я. Хинчина. М.: Гос.издат. технико-теоретической лит-ры, 1951.

4. И.В. Арнольд *Теоретическая арифметика.* М.: Гос. уч.пед. изд-во, 1938.

5. И.Я. Депман *История арифметики.* М.: Просвещение, 1965.

6. F. Lemmermeyer *Numbers and Curves.* Berlin: Springer-Verlag, 2001.

7. P. Wolff *Breakthroughs in mathematics.* New York: Plume Books, 1970.