

# Алгебра. Глава 0. Основные понятия.

Д. В. Карпов

2023

## Кольцо и поле

• Пусть  $K$  — множество, элементы которого мы будем называть *числами*. На множестве  $K$  определены две операции  $+$  :  $K \times K \rightarrow K$  и  $\cdot$  :  $K \times K \rightarrow K$ .

1) Ассоциативность  $+$   $\forall a, b, c \in K \quad (a + b) + c = a + (b + c)$ .

2) Коммутативность  $+$   $\forall a, b \in K \quad a + b = b + a$ .

3) Ноль  $\exists 0 \in K : a + 0 = a$ .

4) Обратный элемент по  $+$   $\forall a \in K \exists (-a) \in K : a + (-a) = 0$ .

5) Дистрибутивность

$\forall a, b, c \in K \quad (a + b)c = ac + bc$  и  $a(b + c) = ab + ac$ .

6) Ассоциативность  $\cdot$   $\forall a, b, c \in K \quad (ab)c = a(bc)$ .

7) Коммутативность  $\cdot$   $\forall a, b \in K \quad ab = ba$ .

8) Единица  $\cdot$   $\exists 1 \in K : a \cdot 1 = 1 \cdot a = a$ .

9) Обратный элемент по  $\cdot$

$\forall a \in K \setminus \{0\} \exists (a)^{-1} \in K : a \cdot (a)^{-1} = (a)^{-1} \cdot a = 1$ .

• Выполнено 1 – 6:  $K$  — *кольцо*.

• Выполнено 1 – 7:  $K$  — *коммутативное кольцо*.

• Выполнено 1 – 6 и 8:  $K$  — *кольцо с 1*.

• Выполнено 1 – 6, 8 и 9:  $K$  — *тело*.

• Выполнено 1 – 9:  $K$  — *поле*.

## Свойство 1

*Ноль в кольце  $K$  единственен.*

**Доказательство.** Пусть есть два нуля:  $0_1$  и  $0_2$ . Тогда:

$$0_1 = 0_1 + 0_2 = 0_2 + 0_1 = 0_2.$$



## Свойство 2

*Для любого  $a \in K$ , обратный элемент по  $+$  единственен.*

**Доказательство.** Пусть есть два обратных элемента по  $+$  для  $a \in K$ :  $b_1$  и  $b_2$ . Тогда:

$$b_1 = b_1 + 0 = b_1 + (a + b_2) = (b_1 + a) + b_2 = 0 + b_2 = b_2.$$



## Свойство 3

$\forall a \in K \quad -(-a) = a.$

**Доказательство.**  $a = a + ((-a) + (-(-a))) =$   
 $= (a + (-a)) + (-(-a)) = (-(-a)).$



## Свойство 4

*В кольце не более одной единицы.*

**Доказательство.** Пусть есть две единицы:  $1_1$  и  $1_2$ . Тогда:

$$1_1 = 1_1 \cdot 1_2 = 1_2.$$



## Определение

Пусть  $K$  — кольцо с 1. Элемент  $a \in K$  **обратимый**, если существует  $a^{-1} \in K$ .

- В поле все ненулевые элементы обратимы.

## Свойство 5

*Пусть  $K$  — кольцо с 1. Тогда для любого  $a \in K$  существует не более чем один обратный элемент по  $\cdot$ .*

**Доказательство.** Пусть есть два обратных элемента по  $\cdot$  для  $a \in K$ :  $b_1$  и  $b_2$ . Тогда:

$$b_1 = b_1 \cdot 1 = b_1 \cdot (a \cdot b_2) = (b_1 \cdot a) \cdot b_2 = 1 \cdot b_2 = b_2.$$



## Свойство 6

*Пусть  $K$  — кольцо с 1. Тогда для любого обратимого  $a \in K$  выполнено  $(a^{-1})^{-1} = a$ .*

**Доказательство.**  $a = a \cdot 1 = a \cdot (a^{-1} \cdot (a^{-1})^{-1}) =$   
 $= (a \cdot a^{-1}) \cdot (a^{-1})^{-1} = 1 \cdot (a^{-1})^{-1} = (a^{-1})^{-1}.$



## Свойство 7

$$-0 = 0.$$

**Доказательство.** Следует из  $0 + 0 = 0$ . □

## Свойство 8

Если  $K$  — кольцо с 1, то  $1^{-1} = 1$ .

**Доказательство.** Следует из  $1 \cdot 1 = 1$ . □

## Определение

- **Вычитание** — это прибавление обратного элемента по  $+$  :

$$a - b := a + (-b).$$

- **Деление** на обратимый элемент  $b$  — это умножение на  $b^{-1}$  :

$$\frac{a}{b} := a \cdot b^{-1}.$$

## Определение

- Пусть  $K \subset L$ , причем оба они — кольца с одними и теми же операциями  $+$  и  $\cdot$ . Тогда  $K$  — **подкольцо**  $L$ , а  $L$  — **надкольцо**  $K$ .
- Пусть  $K \subset L$ , причем оба они — поля с одними и теми же операциями  $+$  и  $\cdot$ . Тогда  $K$  — **подполе**  $L$ , а  $L$  — **надполе**  $K$ .

## Лемма 1

Пусть  $L$  — кольцо,  $K \subset L$ . Пусть выполнены следующие условия:

1° *Замкнутость по  $+$*   $\forall a, b \in K \quad a + b \in K$ .

2° *Замкнутость по  $\cdot$*   $\forall a, b \in K \quad a \cdot b \in K$ .

3° *Существование обратного элемента по  $+$*   
 $\forall a \in K \quad \exists -a \in K$ .

Тогда  $K$  — кольцо, а значит, подкольцо  $L$ . Если  $L$  — коммутативно, то  $K$  тоже.

**Доказательство.** • Условия 1° и 2° означают, что  $+$  и  $\cdot$  корректно определены в  $K$ .

• Ассоциативность и коммутативность  $+$ , ассоциативность  $\cdot$ , коммутативность  $\cdot$  (если есть) наследуются из  $L$ .

Рассмотрим любой элемент  $a \in K$ . Тогда  $-a \in K$ , а значит  $a - a = 0 \in K$ . □

## Лемма 2

Пусть  $L$  — поле,  $K \subset L$ . Пусть выполнены следующие условия:

1° *Замкнутость по  $+$*   $\forall a, b \in K \quad a + b \in K$ .

2° *Замкнутость по  $\cdot$*   $\forall a, b \in K \quad a \cdot b \in K$ .

3° *Существование обратного элемента по  $+$*   
 $\forall a \in K \quad \exists -a \in K$ .

4° *Существование обратного элемента по  $\cdot$*   
 $\forall a \in K, a \neq 0, \quad \exists (a)^{-1} \in K$ .

Тогда  $K$  — поле, а значит, подполе  $L$ .

**Доказательство.** • По Лемме 1,  $K$  — коммутативное подкольцо  $L$ .

• Остается проверить существование 1 в  $K$ .

Рассмотрим любой ненулевой элемент  $a \in K$ . Тогда  $a^{-1} \in K$ , а значит,  $a \cdot a^{-1} = 1 \in K$ . □



# Гомоморфизм

## Определение

• Пусть  $K, L$  — кольца. Отображение  $f : K \rightarrow L$  называется **гомоморфизмом**, если  $\forall a, b \in K$ :

$$f(a + b) = f(a) + f(b) \quad \text{и} \quad f(ab) = f(a)f(b).$$

**Ядро** гомоморфизма  $f$  — это  $\text{Ker}(f) = \{x \in K : f(x) = 0\}$ .

**Образ** гомоморфизма  $f$  — это  $\text{Im}(f) = \{y \in L : \exists x \in K : f(x) = y\}$ .

## Свойство 1

Если  $f : K \rightarrow L$  гомоморфизм, то  $f(0_K) = 0_L$ .

**Доказательство.**  $f(0_K) = f(0_K + 0_K) = f(0_K) + f(0_K)$ . Вычитая из левой и правой частей  $f(0_K)$ , получаем  $f(0_K) = 0_L$ .  $\square$

## Свойство 2

Если  $f : K \rightarrow L$  гомоморфизм, то  $f(-a) = -f(a)$ .

**Доказательство.**  $0_L = f(0_K) = f(a + (-a)) = f(a) + f(-a)$ . Вычитая из левой и правой частей  $f(a)$ , получаем  $-f(a) = f(-a)$ .  $\square$

### Лемма 3

Пусть  $K, L$  — кольца,  $f : K \rightarrow L$  — гомоморфизм колец.

Тогда:

- 1)  $\text{Ker}(f)$  — подкольцо  $K$ .
- 2)  $\text{Im}(f)$  — подкольцо  $L$ .

**Доказательство.** Достаточно проверить условия из Леммы 1.

1) • Пусть  $a, b \in \text{Ker}(f)$ . Тогда

$f(a + b) = f(a) + f(b) = 0 + 0 = 0$ , следовательно,  
 $a + b \in \text{Ker}(f)$ .

•  $f(ab) = f(a)f(b) = 0 \cdot 0 = 0$ , следовательно,  
 $ab \in \text{Ker}(f)$ .

•  $f(-a) = -f(a) = -0_L = 0_L$ .

2) • Пусть  $y, y' \in \text{Im}(f)$ , а  $x, x' \in K$  таковы, что  $f(x) = y$   
и  $f(x') = y'$ .

• Тогда  $y + y' = f(x) + f(x') = f(x + x') \in \text{Im}(f)$  и  
 $y \cdot y' = f(x) \cdot f(x') \in \text{Im}(f)$ .

•  $-y = -f(x) = f(-x) \in \text{Im}(f)$ .

## Типы гомоморфизмов

- Пусть  $f : K \rightarrow L$  — гомоморфизм колец.
- Если  $f$  — инъекция, то  $f$  — **мономорфизм**.
- Если  $f$  — сюръекция (то есть,  $\text{Im}(f) = L$ ), то  $f$  — **эпиморфизм**.
- Если  $f$  — биекция, то  $f$  — **изоморфизм**.
- Изоморфизм = мономорфизм + эпиморфизм.

### Лемма 4

Пусть  $f : K \rightarrow L$  — гомоморфизм колец. Тогда  $f$  — мономорфизм, если и только если  $\text{Ker}(f) = \{0\}$ .

**Доказательство.**  $\Rightarrow$  • Если  $f$  — мономорфизм, то  $f$  — инъекция.

• Пусть  $a \in \text{Ker}(f)$ . Из  $f(a) = 0 = f(0)$  следует, что  $a = 0$  (так как  $f$  — инъекция).

$\Leftarrow$  • Пусть  $f(a) = f(b)$ . Тогда  $f(a - b) = f(a) - f(b) = 0$ .

• Значит,  $a - b \in \text{Ker}(f) = \{0\}$ , откуда  $a = b$ . Таким образом,  $f$  — инъекция, а значит, мономорфизм.

## Лемма 5

Пусть  $f : K \rightarrow L$  — изоморфизм колец. Тогда и  $f^{-1} : L \rightarrow K$  — изоморфизм колец.

**Доказательство.** • Достаточно доказать, что  $f^{-1}$  — гомоморфизм (так как отображение, обратное к биекции — биекция).

- Рассмотрим любые  $a, b \in L$ .
- Пусть  $w = f^{-1}(a + b) - f^{-1}(a) - f^{-1}(b)$ . Так как  $f$  — гомоморфизм, имеем

$$f(w) = f(f^{-1}(a + b)) - f(f^{-1}(a)) - f(f^{-1}(b)) = a + b - a - b = 0.$$

- Из  $f(w) = 0 = f(0)$  и того, что  $f$  — биекция, следует  $w = 0$ .
- Следовательно,  $f^{-1}(a + b) = f^{-1}(a) + f^{-1}(b)$ .
- Пусть  $z = f^{-1}(ab) - f^{-1}(a)f^{-1}(b)$ . Так как  $f$  — гомоморфизм, имеем

$$f(z) = f(f^{-1}(ab)) - f(f^{-1}(a)) \cdot f(f^{-1}(b)) = ab - ab = 0.$$

- Из  $f(z) = 0 = f(0)$  и того, что  $f$  — биекция, следует  $z = 0$ .
- Следовательно,  $f^{-1}(ab) = f^{-1}(a) \cdot f^{-1}(b)$ .

## Определение

Если существует изоморфизм  $f : K \rightarrow L$ , то говорят, что эти кольца **изоморфны**. Обозначение:  $K \simeq L$ .

## Теорема 0

$\simeq$  — отношение эквивалентности на множестве всех колец.

**Доказательство.** • Рефлексивность очевидна: тождественное отображение  $\text{id} : K \rightarrow K$  (заданное формулой  $\text{id}(x) = x$  для всех  $x \in K$ ) очевидно, является изоморфизмом.

• Симметричность доказана в Лемме 5.  
• Докажем транзитивность. Пусть  $K, L, M$  — кольца,  $K \simeq L$  и  $L \simeq M$ .

• Тогда существуют изоморфизмы  $f : K \rightarrow L$  и  $g : L \rightarrow M$ .

Докажем, что их композиция  $g \cdot f : K \rightarrow M$  (заданная правилом  $gf(a) := g(f(a))$ ) также является изоморфизмом.

• Композиция биекций  $g$  и  $f$ , очевидно, является биекцией.

• Проверим, что  $gf$  — гомоморфизм колец:

$$gf(a + b) = g(f(a + b)) = g(f(a) + f(b)) = g(f(a)) + g(f(b)) = gf(a) + gf(b);$$

$$gf(ab) = g(f(ab)) = g(f(a) \cdot f(b)) = g(f(a)) \cdot g(f(b)) = gf(a) \cdot gf(b).$$

# Идеал

## Определение

Пусть  $K$  — коммутативное кольцо. Множество  $I \subset K$  — *идеал* в  $K$ , если  $I$  — подкольцо  $K$  и выполнено следующее условие:

$$\forall x \in K \text{ и } \forall a \in I \quad ax \in I.$$

- В любом кольце  $K$  есть два “неинтересных” идеала: это  $\{0\}$  и  $K$ .

## Лемма 6

Пусть  $K$  — коммутативное кольцо,  $I \subset K$ . Пусть выполнены следующие условия:

1° *Замкнутость по  $+$*   $\forall a, b \in I \quad a + b \in I$ .

2° *Замкнутость по  $-$*   $\forall a \in I \quad \exists(-a) \in I$ .

3° *Замкнутость по  $\cdot$  на элементы  $K$*   $\forall x \in K \text{ и } \forall a \in I \quad ax \in I$

Тогда  $I$  — идеал в  $K$ .

**Доказательство.** • По Лемме 1,  $I$  — подкольцо  $K$ .

- Теперь по условию 3° несложно понять, что  $I$  — идеал.  $\square$

## Лемма 7

Пусть  $K$  — коммутативное кольцо,  $\varphi : K \rightarrow L$  — гомоморфизм колец. Тогда  $\ker(\varphi)$  — идеал в  $K$ .

**Доказательство.** • По Лемме 3,  $\ker(\varphi)$  — подкольцо  $K$ .

• Пусть  $a \in \ker(\varphi)$  и  $x \in K$ . Тогда  $\varphi(ax) = \varphi(a) \cdot \varphi(x) = 0 \cdot \varphi(x) = 0$ , а значит,  $ax \in \ker(\varphi)$

• По Лемме 6,  $\ker(\varphi)$  — идеал в  $K$ . □

## Лемма 8

Пусть  $K$  — коммутативное кольцо с 1,  $I$  — идеал в  $K$ , а  $x \in I$  — обратимый элемент кольца  $K$ . Тогда  $I = K$ .

**Доказательство.** • Так как  $x^{-1} \in K$  и  $x \in I$ , мы имеем  $1 = x \cdot x^{-1} \in I$ .

•  $\forall y \in K$  имеем  $y = y \cdot 1 \in I$ . Значит,  $I = K$ . □

## Следствие 1

Пусть  $K$  — поле, а  $I$  — идеал в  $K$ . Тогда  $I = K$  или  $I = \{0\}$ .

**Доказательство.** • Предположим, что  $I \neq \{0\}$ . Тогда  $\exists a \in I$ ,  $a \neq 0$ . Так как  $a$  — обратимый элемент (как все ненулевые элементы поля),  $I = K$  по Лемме 8. □

## Следствие 2

Пусть  $K$  — поле,  $L$  — кольцо, а  $f : K \rightarrow L$  — гомоморфизм колец. Тогда либо  $\text{Im}(f) = \{0\}$ , либо  $f$  — мономорфизм.

**Доказательство.** • По Лемме 7  $\ker(f)$  — идеал в поле  $K$ .

- Тогда по Следствию 1 либо  $\ker(f) = K$ , либо  $\ker(f) = \{0\}$ .
- Если  $\ker(f) = K$ , то  $\text{Im}(f) = \{0\}$ .
- Если  $\ker(f) = \{0\}$ , то  $f$  — мономорфизм. □

## Определение

Пусть  $K$  — коммутативное кольцо,  $M \subset K$ . Тогда

$\langle M \rangle := \{m_1x_1 + \dots + m_sx_s : m_1, \dots, m_s \in M, x_1, \dots, x_s \in K\}$  —

*идеал, порожденный множеством  $M$*  (здесь количество элементов  $s$  не фиксировано и может быть любым натуральным числом).

- Идеал, порожденный  $M$  — множество всех линейных комбинаций элементов из  $M$ .

**Определение.** Пусть  $K$  — коммутативное кольцо.

1) Пусть  $m \in K$ . Тогда  $mK = \{mx : x \in K\}$  — *главный идеал*.

2) Если все идеалы в кольце  $K$  — главные, то  $K$  — *кольцо главных идеалов*.



## Лемма 9

Пусть  $K$  — коммутативное кольцо,  $M \subset K$ . Тогда  $\langle M \rangle$  — идеал в  $K$ .

**Доказательство.** • Нужно проверить условия из Леммы 6.

- Пусть  $a, b \in \langle M \rangle$ . Тогда существуют такие  $m_1, \dots, m_s \in M$ ,  $a_1, \dots, a_s, b_1, \dots, b_s \in K$ , что  $a = a_1 m_1 + \dots + a_s m_s$  и  $b = b_1 m_1 + \dots + b_s m_s$  (можно считать, что  $a$  и  $b$  — линейные комбинации одних и тех же элементов  $M$ , при необходимости добавив слагаемые с нулевыми коэффициентами).
- $-a = (-a_1)m_1 + \dots + (-a_s)m_s \in \langle M \rangle$ .
- Тогда  $a + b = (a_1 + b_1)m_1 + \dots + (a_s + b_s)m_s \in \langle M \rangle$ .
- Для любого  $x \in K$ ,  $ax = (a_1 x)m_1 + \dots + (a_s x)m_s \in \langle M \rangle$ .
- Условия Леммы 6 проверены, а значит,  $\langle M \rangle$  — идеал в  $K$ . □

## Сравнение по модулю идеала

- Пусть  $K$  — коммутативное кольцо,  $I$  — идеал в  $K$ .

### Определение

Пусть  $a, b \in K$ . Тогда  $a \equiv_I b$  (или, что то же самое,  $a \equiv b \pmod{I}$ ), если и только если  $a - b \in I$ .

### Лемма 10

$\equiv_I$  — отношение эквивалентности (то есть, рефлексивно, симметрично и транзитивно).

**Доказательство.** •  $a \equiv_I a$ , так как  $a - a = 0 \in I$ .

• Если  $a \equiv_I b$ , то  $a - b \in I$ . Значит,  $b - a \in I$ , откуда  $b \equiv_I a$ .

• Если  $a \equiv_I b$  и  $b \equiv_I c$ , то  $a - b, b - c \in I$ . Значит,  $a - c = (a - b) + (b - c) \in I$ , откуда  $a \equiv_I c$ . □

### Определение

**Вычет** по модулю идеала  $I$  — это класс эквивалентности по  $\equiv_I$ .

- Различные вычеты не пересекаются. Кольцо  $K$  разбито на вычеты.

## Факторкольцо

- Для  $a \in K$  вычит, состоящий из элементов кольца, сравнимых с  $a$ , как правило, будем обозначать через  $\bar{a}$ .
- Из определения следует, что  $\bar{a} = a + I = \{a + x : x \in I\}$ .

### Определение

- Пусть  $K$  — коммутативное кольцо,  $I$  — идеал в  $K$ .

**Факторкольцо**  $K/I := \{\bar{a} : a \in K\}$ .

- $\bar{a} + \bar{b} := \overline{a + b}$ ;       $\bar{a} \cdot \bar{b} := \overline{ab}$ .

### Лемма 11

$+$  и  $\cdot$  в  $K/I$  определены корректно.

**Доказательство.** • Пусть  $a \equiv_I a'$ , то есть,  $\bar{a} = \bar{a}'$ . Это означает, что  $a - a' \in I$ . Докажем, что от замены  $a$  на  $a'$  результат  $+$  и  $\cdot$  не изменится:

$$\bar{a} + \bar{b} = \bar{a}' + \bar{b} \iff a + b \equiv_I a' + b \iff a + b - (a' + b) = a - a' \in I;$$

$$\bar{a} \cdot \bar{b} = \bar{a}' \cdot \bar{b} \iff ab \equiv_I a'b \iff$$

$$ab - (a'b) = (a - a')b \in I \iff a - a' \in I. \quad \square$$

## Теорема 1

- $K/I$  с определенными выше  $+$  и  $\cdot$  — коммутативное кольцо.
- Если  $K$  — кольцо с 1, то  $K/I$  — тоже. Если при этом  $a \in K$  — обратимый элемент в  $K$ , то  $\bar{a}$  — обратимый в  $K/I$ .

**Доказательство.** • Так как  $\bar{a} + \bar{b} = \overline{a + b}$ , из ассоциативности и коммутативности  $+$  в  $K$  следует ассоциативность и коммутативность  $+$  в  $K/I$ .

• Так как  $\bar{a} \cdot \bar{b} = \overline{ab}$ , из ассоциативности и коммутативности умножения в  $K$  следует ассоциативность и коммутативность умножения в  $K/I$ .

• **Дистрибутивность:**

$$\bar{a}(\bar{b} + \bar{c}) = \overline{a(b + c)} = \overline{ab + ac} = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}.$$

• **Ноль** — это  $\bar{0}$ .

• **Обратный по сложению:**  $-\bar{a} := \overline{-a}$ .

• **Единица:** если  $1 \in K$ , то  $\bar{1}$  — единица в  $K/I$ .

• Если  $a \in K$  — обратимый, то  $(\bar{a})^{-1} := \overline{a^{-1}}$  — обратный в  $K/I$ .



## Теорема о гомоморфизме колец

### Теорема 2

Пусть  $K, L$  — коммутативные кольца,  $f : K \rightarrow L$  — гомоморфизм. Тогда  $K/\text{Ker}(f) \simeq \text{Im}(f)$ . Более того, отображение  $\bar{f} : K/\text{Ker}(f) \rightarrow \text{Im}(f)$ , заданное формулой  $\bar{f}(\bar{x}) := f(x)$ , является изоморфизмом колец.

**Доказательство.** • Докажем корректность определения  $\bar{f}$ .

Пусть  $\bar{x} = \bar{y}$ . Тогда  $x - y \in \text{Ker}(f)$ , а значит,  
 $f(x) = f(y) + f(x - y) = f(y) + 0 = f(y)$ .

• Теперь ясно, что  $\bar{f}$  — гомоморфизм:

$$\begin{aligned}\bar{f}(\bar{x} + \bar{y}) &= \bar{f}(\overline{x + y}) = f(x + y) = f(x) + f(y) = \bar{f}(\bar{x}) + \bar{f}(\bar{y}); \\ \bar{f}(\bar{x} \cdot \bar{y}) &= \bar{f}(\overline{x \cdot y}) = f(xy) = f(x)f(y) = \bar{f}(\bar{x}) \cdot \bar{f}(\bar{y}).\end{aligned}$$

• Очевидно,  $\bar{f}$  — сюръекция:  $\forall y \in \text{Im}(f) \exists x \in K$  такой, что  $y = f(x)$ . Тогда и  $y = \bar{f}(\bar{x})$ .

• Пусть  $\bar{a} \in \text{Ker}(\bar{f})$ . Тогда  $0 = \bar{f}(\bar{a}) = f(a)$ , а значит,  $a \in \text{Ker}(f)$ , откуда следует  $\bar{a} = \bar{0}$ . Следовательно,  $\text{Ker}(\bar{f}) = \{\bar{0}\}$ .

• Таким образом,  $\bar{f}$  — изоморфизм, а значит,  $K/\text{Ker}(f) \simeq \text{Im}(f)$ .

## Поле частных

- Пусть  $K$  — коммутативное кольцо **без делителей нуля** (то есть, если  $a, b \in K$  и  $ab = 0$ , то  $a = 0$  или  $b = 0$ ).
- Обозначим через  $M$  множество всех **дробей**  $\frac{a}{b}$ , где  $a, b \in K$ ,  $b \neq 0$ .
- Пусть  $\frac{a}{b} \sim \frac{c}{d} \iff ad = bc$ .

### Свойство 1

$$\frac{0}{b} \sim \frac{c}{d} \iff c = 0.$$

**Доказательство.**  $\Leftarrow$ . Если  $c = 0$ , то  $0 \cdot d = 0 = b \cdot 0$ .

$\Rightarrow$ .  $\frac{0}{b} \sim \frac{c}{d} \Rightarrow 0 = 0 \cdot d = bc$ . Так как по определению  $b \neq 0$ , а делителей 0 в  $K$  нет,  $c = 0$ .  $\square$

### Свойство 2

$$\frac{a}{a} \sim \frac{c}{d} \iff c = d.$$

**Доказательство.** Очевидно,  $a \neq 0$ . Следовательно,  $\frac{a}{a} \sim \frac{c}{d} \iff ad = ac \iff a(d - c) = 0 \iff d - c = 0 \iff c = d$ .  $\square$

### Свойство 3

**Сокращение дроби.**  $\frac{a}{b} \sim \frac{ac}{bc}$  при  $c \neq 0$ .

**Доказательство.**  $abc - bac = 0$ .

## Лемма 12

$\sim$  — отношение эквивалентности.

Доказательство. • Рефлексивность очевидна.

• Симметричность.

$$\frac{a}{b} \sim \frac{c}{d} \iff ad = bc \iff cb = da \iff \frac{c}{d} \sim \frac{a}{b}.$$

• Транзитивность. Если  $\frac{a}{b} \sim \frac{c}{d}$  и  $\frac{c}{d} \sim \frac{e}{f}$ , то  $ad = bc$  и  $cf = de$ .

• Если хотя бы одно из  $a, c, e$  равно 0, то по Свойству 1 равны и два других. Тогда  $\frac{a}{b} \sim \frac{e}{f}$ .

• Пусть  $0 \notin \{a, c, e\}$ . Тогда перемножим полученные равенства и сократим на  $cd \neq 0$ :

$$adcf = bcde \Rightarrow af = be \Rightarrow \frac{a}{b} \sim \frac{e}{f}.$$



## Определение

**Поле частных**  $F$  коммутативного кольца  $K$  без делителей нуля состоит из классов эквивалентности дробей. Мы будем обозначать класс эквивалентности дроби  $\frac{a}{b}$  в точности так же, как саму эту дробь.

**Сложение:**  $\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}$ .

**Умножение:**  $\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$ .

## Свойство 4

$$\frac{a}{d} + \frac{c}{d} = \frac{a+c}{d}.$$

**Доказательство.**  $\frac{a}{d} + \frac{c}{d} = \frac{ad+cd}{d^2} = \frac{a+c}{d}$  по Свойству 3.



## Лемма 13

Сложение и умножение в поле частных определены корректно, то есть, результат не зависит от замены дроби на эквивалентную

**Доказательство.** • Достаточно доказать, что при замене первой дроби  $\frac{a}{b}$  на эквивалентную дробь  $\frac{a'}{b'}$  результат сложения и умножения не изменится. Отметим, что  $ab' = a'b$ .

• **Сложение** (мы можем сократить на  $d^2$ , так как  $d \neq 0$ ):

$$\begin{aligned}\frac{a}{b} + \frac{c}{d} &= \frac{ad + bc}{bd} \sim \frac{a'}{b'} + \frac{c}{d} = \frac{a'd + b'c}{b'd} \iff \\ (ad + bc)b'd &= (a'd + b'c)bd \iff adb'd + bcb'd = a'dbd + b'cbd \\ &\iff ab'd^2 = a'bd^2 \iff ab' = a'b.\end{aligned}$$

• **Умножение.** Если  $c = 0$ , утверждение следует из Свойства 1. Иначе можно сокращать на  $cd$ :

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \sim \frac{a'}{b'} \cdot \frac{c}{d} = \frac{a'c}{b'd} \iff acb'd = a'cbd \iff ab' = a'b.$$

## Теорема 3

Поле частных  $F$  коммутативного кольца  $K$  без делителей нуля — поле.

**Доказательство.** Коммутативность сложения и умножения очевидно следуют из аналогичных свойств в  $K$ .

**Ассоциативность сложения.**

$$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{ad + bc}{bd} + \frac{e}{f} = \frac{adf + bcf + bde}{bdf}.$$

В каждом из слагаемых три сомножителя, один числитель и два знаменателя других дробей. Легко понять, что при другом порядке сложения будет то же самое.

**Ноль.** Дроби вида  $\frac{0}{b}$  ( $b \in K, b \neq 0$ ) образуют класс эквивалентности по Свойству 1. Несложно проверить, что это класс и будет 0 в поле частных:  $\frac{0}{b} + \frac{c}{d} = \frac{bc}{bd} = \frac{c}{d}$ .

**Обратный элемент по +.** Положим  $-\left(\frac{a}{b}\right) := \frac{-a}{b}$ .

Проверка:  $\frac{-a}{b} + \frac{a}{b} = \frac{0}{b^2} = 0$ .

Ассоциативность умножения.

$$\left(\frac{a}{b} \cdot \frac{c}{d}\right) \cdot \frac{e}{f} = \frac{ac}{bd} \cdot \frac{e}{f} = \frac{ace}{bdf}.$$

Легко понять, что при другом порядке умножения будет то же самое.

Дистрибутивность.

$$\left(\frac{a}{b} + \frac{c}{d}\right) \cdot \frac{e}{f} = \frac{ad + bc}{bd} \cdot \frac{e}{f} = \frac{ade + bce}{bdf} = \frac{ade}{bdf} + \frac{bce}{bdf} = \frac{ae}{bf} + \frac{ce}{df}$$

(последний переход верен по Свойству 3).

**Единица.** В качестве 1 подойдет класс эквивалентности дробей вида  $\frac{a}{a}$ , где  $a \neq 0$ .

**Обратный элемент по умножению.** Для дроби  $\frac{a}{b}$ , где  $a \neq 0$  положим  $\left(\frac{a}{b}\right)^{-1} := \frac{b}{a}$ .

Проверка:  $\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = 1$  по определению. □

## Лемма 14

Пусть  $K$  — коммутативное кольцо с 1 без делителей 0, а  $F$  — его поле частных. Тогда отображение  $\varphi : K \rightarrow F$ , заданное формулой  $\varphi(a) = \frac{a}{1}$  — мономорфизм колец.

**Доказательство.** • Проверим, что  $\varphi$  — гомоморфизм колец. Пусть  $a, b \in K$ .

- $\varphi(a) + \varphi(b) = \frac{a}{1} + \frac{b}{1} = \frac{a \cdot 1 + b \cdot 1}{1 \cdot 1} = \frac{a+b}{1} = \varphi(a+b)$ .
- $\varphi(a)\varphi(b) = \frac{a}{1} \cdot \frac{b}{1} = \frac{ab}{1 \cdot 1} = \varphi(ab)$ .
- Пусть  $a \in \text{Ker}(\varphi)$ . Тогда  $0 = \varphi(a) = \frac{a}{1} \iff a = 0$ . □
- Далее мы будем отождествлять число  $a \in K$  с дробью  $\frac{a}{1} \in F$  и считать, что  $K \subset F$ .

## Определение

Пусть  $K$  — поле.

• Положим  $\underline{k} := \underbrace{1 + 1 + \cdots + 1}_k$  для  $k \in \mathbb{N}$  и

$\underline{k} := -\underbrace{(1 + 1 + \cdots + 1)}_{-k}$  для отрицательных  $k \in \mathbb{Z}$ , а

также  $\underline{0} = 0$ .

• Если существует такие  $k \in \mathbb{N}$ , что  $\underline{k} = 0$ , то **характеристика поля**  $\text{char}(K)$  равна наименьшему из таких чисел.

• Если же таких натуральных чисел нет, то считается, что  $\text{char}(K) = 0$ .

- Несложно проверить, что  $\underline{a} + \underline{b} = \underline{a + b}$ .
- Раскрыв скобки по дистрибутивности, можно убедиться в том, что  $\underline{a} \cdot \underline{b} = \underline{ab}$ .

### Лемма 15

Пусть  $K$  — поле и  $\text{char}(K) = p \neq 0$ . Тогда  $p \in \mathbb{P}$ .

**Доказательство.** • Пусть  $p = ab$ , где  $1 < a < p$  и  $1 < b < p$ .

- Тогда  $\underline{a} \cdot \underline{b} = \underline{ab} = \underline{p} = 0$ .
- Так как  $K$  — поле, отсюда следует, что хотя бы одно из чисел  $\underline{a}$  и  $\underline{b}$  равно 0, что противоречит определению характеристики поля. □

## Теорема 4

Пусть  $K$  — поле.

1) Если  $\text{char}(K) = p \in \mathbb{P}$ , то отображение  $\varphi : \mathbb{Z}/p\mathbb{Z} \rightarrow K$ , заданное формулой  $\varphi(\bar{m}) = \underline{m}$  (для  $m \in \mathbb{Z}$ ) — мономорфизм полей. В частности,  $K$  имеет подполе, изоморфное  $\mathbb{Z}/p\mathbb{Z}$ .

2) Если  $\text{char}(K) = 0$ , то отображение  $\varphi : \mathbb{Q} \rightarrow K$ , заданное формулой  $\varphi\left(\frac{a}{b}\right) = \frac{\underline{a}}{\underline{b}}$  (для  $a, b \in \mathbb{Z}, b \neq 0$ ) — мономорфизм полей. В частности,  $K$  имеет подполе, изоморфное  $\mathbb{Q}$ .

**Доказательство.** 1) Отображение  $\psi : \mathbb{Z} \rightarrow K$ , заданное формулой  $\psi(m) := \underline{m}$ , очевидно, является гомоморфизмом колец.

- $\ker(\psi) = \{m \in \mathbb{Z} : \underline{m} = 0\}$  — идеал в  $\mathbb{Z}$ . НУО,  $\ker(\psi) = q\mathbb{Z}$ .
- Тогда  $\underline{m} = 0 \iff m \vdots q$ , то есть,  $\text{char}(K) = q$ . Значит,  $q = p$  и  $\ker(\psi) = p\mathbb{Z}$ .
- По Теореме 2 (о гомоморфизме колец), отображение  $\bar{\psi} : \mathbb{Z}/p\mathbb{Z} \rightarrow K$ , заданное формулой  $\bar{\psi}(\bar{m}) = \underline{m}$  — изоморфизм между  $\mathbb{Z}/p\mathbb{Z}$  и  $\text{Im}(\psi)$  — подполем  $K$ .

2) • В этом случае  $\forall m \in \mathbb{N} \underline{m} \neq 0$ , то есть,  $\text{char}(K) = 0$ .

• Определим отображение  $\varphi : \mathbb{Q} \rightarrow K$  формулой

$$\varphi\left(\frac{a}{b}\right) := \frac{\underline{a}}{\underline{b}} \quad (\text{при } b \neq 0).$$

• Проверим **корректность**. Пусть  $\frac{a}{b} = \frac{c}{d} \iff ad = bc$   
(здесь  $b, d \neq 0$ ).

• Тогда по дистрибутивности в поле  $K$  имеем

$$\underline{a} \cdot \underline{d} = \underline{b} \cdot \underline{c} \iff \frac{\underline{a}}{\underline{b}} = \frac{\underline{c}}{\underline{d}}.$$

• Проверим, что  $\varphi$  — **гомоморфизм**:

$$\bullet \varphi\left(\frac{a}{b}\right) \cdot \varphi\left(\frac{c}{d}\right) = \frac{\underline{a}}{\underline{b}} \cdot \frac{\underline{c}}{\underline{d}} = \frac{\underline{a \cdot c}}{\underline{b \cdot d}} = \varphi\left(\frac{ac}{bd}\right) = \varphi\left(\frac{a}{b} \cdot \frac{c}{d}\right).$$

$$\bullet \varphi\left(\frac{a}{b}\right) + \varphi\left(\frac{c}{d}\right) = \frac{\underline{a}}{\underline{b}} + \frac{\underline{c}}{\underline{d}} = \frac{\underline{a \cdot d + b \cdot c}}{\underline{b \cdot d}} = \varphi\left(\frac{ad+bc}{bd}\right) = \varphi\left(\frac{a}{b} + \frac{c}{d}\right).$$

• Так как  $\mathbb{Q}$  — поле и  $\varphi$  принимает не только нулевые значения,  $\ker(\varphi) = \{0\}$ .

• Значит,  $\text{Im}(\varphi)$  — подполе  $K$ , изоморфное  $\mathbb{Q}$ . □

### Следствие 3

*Все поля из  $p \in \mathbb{P}$  элементов изоморфны  $\mathbb{Z}/p\mathbb{Z}$ .*

• Будем применять при  $p \in \mathbb{P}$  обозначение  $\mathbb{F}_p$  для поля из  $p$  элементов (изоморфного  $\mathbb{Z}/p\mathbb{Z}$ ).



Материалы курса можно найти вот здесь:

`logic.pdmi.ras.ru/~dvk/ITMO/Algebra`