Алгебра. Глава 0. Основные понятия.

Д. В. Карпов

2022

Кольцо и поле

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

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

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

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

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

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

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

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

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

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 ноля: 0_1 и 0_2. Тогда:

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

$\square$

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:

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

$\square$

Свойство 3

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

Доказательство. $\quad a = a + ((-a) + (-(-a))) =$

$= (a + (-a)) + (-(-a)) = (-(-a)).$ $\square$

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 $+$ 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} :

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

Подполе и подкольцо

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 $a - a = 0 \in K$. $\square$

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, $a \cdot a^{-1} = 1 \in K$. $\square$

Гомоморфизм

Определение

• Пусть K, L — кольца. Отображение $f : K \to L$ 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 $\mathrm{Ker}(f) = \{x \in K \ : \ f(x) = 0\}$.

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

Свойство 1

Если $f : K \to L$ 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 $f(0_K) = 0_L$. □

Свойство 2

Если $f : K \to L$ 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
$-f(a) = f(-a)$. □

Лемма 3

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

1) $\mathrm{Ker}(f)$ *— подкольцо K.*

2) $\mathrm{Im}(f)$ *— подкольцо L.*

Доказательство. Достаточно проверить условия из Леммы 1.

1) • Пусть $a, b \in \mathrm{Ker}(f)$. Тогда $f(a+b) = f(a) + f(b) = 0 + 0 = 0$, следовательно, $a + b \in \mathrm{Ker}(f)$.

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

• $f(-a) = -f(a) = -0_L = 0_L$.

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

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

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

Типы гомоморфизмов

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

Лемма 4

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

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

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

Лемма 5

Пусть $f : K \to L$ — изоморфизм колец. Тогда и $f^{-1} : L \to K$ — 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 $f : K \to L$, то говорят, что эти кольца изоморфны. Обозначение: $K \simeq L$.

Теорема 0

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

Доказательство. • Рефлексивность очевидна: тождественное отображение $\mathrm{id} : K \to K$ (заданное формулой $\mathrm{id}(x) = x$ 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 измОрфизмы $f : K \to L$ и $g : L \to M$. Докажем, что их композиция $g \cdot f : K \to M$ (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:

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

• В любом кольце K есть два "неинетересных" 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° *$\exists$ обратного элемента по +* $\forall\, a \in I \quad \exists(-a) \in I.$

3° *Замкнутость по $\cdot$ на элементы K* $\forall x \in K$ *и* $\forall a \in I \qquad ax \in I$

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, $\varphi : K \to L$ — 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. $\square$

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, $I = K$. $\square$

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. $\square$

Следствие 2

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

• Если $\ker(f) = \{0\}$, то f — мономорфизм. $\square$

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. $\square$

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

Определение

- Пусть K — коммутативное кольцо, I — идеал в K. *Факторкольцо* $K/I := \{\overline{a} \ : \ a \in K\}$.
- $\overline{a} + \overline{b} := \overline{a + b}; \qquad \overline{a} \cdot \overline{b} := \overline{ab}$.

Лемма 11

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

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

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

$$\overline{a} \cdot \overline{b} = \overline{a'} \cdot \overline{b} \iff ab \equiv_I a'b \iff$$
$$ab - (a'b) = (a - a')b \in I \Leftarrow a - a' \in I. \qquad \square$$

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 $\overline{a}$ — обратимый в K/I.*

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

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

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

• Ноль — это $\overline{0}$.

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

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

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

Теорема о гомоморфизме колец

Теорема 2

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

Доказательство. • Докажем корректность определения $\overline{f}$. Пусть $\overline{x} = \overline{y}$. Тогда $x - y \in \mathrm{Ker}(f)$, а значит, $f(x) = f(y) + f(x - y) = f(y) + 0 = f(y)$.

• Теперь ясно, что $\overline{f}$ — гомоморфизм:
$\overline{f}(\overline{x} + \overline{y}) = \overline{f}(\overline{x + y}) = f(x + y) = f(x) + f(y) = \overline{f}(\overline{x}) + \overline{f}(\overline{y})$;
$\overline{f}(\overline{x} \cdot \overline{y}) = \overline{f}(\overline{x \cdot y}) = f(xy) = f(x)f(y) = \overline{f}(\overline{x}) \cdot \overline{f}(\overline{y})$.

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

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

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

Поле частных

- Пусть K — коммутативное кольцо без делителей ноля (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, $c = 0$. □

Свойство 2

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

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

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 $cd \neq 0$:
$adcf = bcde \Rightarrow af = be \Rightarrow \frac{a}{b} \sim \frac{e}{f}$. $\square$

Определение

Поле частных F коммутативного кольца K без делителей ноля 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 1.

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 $d \neq 0$):

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \sim \frac{a'}{b'} + \frac{c}{d} = \frac{a'd+b'c}{b'd} \iff$$

$$(ad+bc)b'd = (a'd+b'c)bd \iff adb'd+bcb'd = a'dbd+b'cbd$$

$$\iff ab'd^2 = a'bd^2 \iff ab' = a'b.$$

• 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 ноля — 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: $\frac{o}{b}+\frac{c}{d}=\frac{bc}{bd}=\frac{c}{d}$.

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

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. □

Вложение кольца в поле частных

Лемма 14

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

Доказательство. • Проверим, что φ — 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 $a \in \mathrm{Ker}(\varphi)$. 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 $K \subset F$.

Характеристика поля

Определение

Пусть K — поле.

• Положим $\underline{k} := \underbrace{1+1+\dots+1}_{k}$ для $k \in \mathbb{N}$ и $\underline{k} := \underbrace{1+1+\dots+1}_{-k}$ 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 $\mathrm{char}(K)$ равна наименьшему из таких чисел.

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

Лемма 15

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

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

• Из дистрибутивности следует, что $\underline{a} \cdot \underline{b} = \underline{ab} = \underline{p} = 0$.

• 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* $\mathrm{char}(K) = p \in \mathbb{P}$, *то отображение* $\varphi : \mathbb{Z}/p\mathbb{Z} \to K$, *заданное формулой* $\varphi(\overline{m}) = \underline{m}$ *(для* $m \in \mathbb{Z}$*) — мономорфизм полей. В частности,* K *имеет подполе* $\mathbb{Z}/p\mathbb{Z}$.

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

Доказательство. 1) Отображение $\psi : \mathbb{Z} \to K$, 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, $\mathrm{char}(K) = q$. Значит, $q = p$ и $\ker(\psi) = p\mathbb{Z}$.
- По Теореме 2 (о гомоморфизме колец), отображение $\overline{\psi} : \mathbb{Z}/p\mathbb{Z} \to K$, заданное формулой $\overline{\psi}(\overline{m}) = \underline{m}$ — изоморфизм между $\mathbb{Z}/p\mathbb{Z}$ и $\mathrm{Im}(\psi)$ — подполем K.

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

• Определим отображение $\varphi : \mathbb{Q} \to K$ формулой $\varphi(\frac{a}{b}) := \frac{\underline{a}}{\underline{b}}$ (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 φ — гомоморфизм:

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

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

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

Следствие 3

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

Материалы курса можно найти вот здесь:

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