Оглавление

Глава 1

Кольца и поля

1.1. Факторкольцо

Напоминание. A – кольцо, A/I – множество классов вычетов

Продолжаем доказательство:

Доказательство. A/I – абелева группа (по т. о факторгруппе)
Нужно доказать, что $(\overline{x}+\overline{y})\overline{z} = \overline{xz}+\overline{yz}$
Выберем $x \in \overline{x}, \quad y \in \overline{y}, \quad z \in \overline{z}$

$$(\overline{x}+\overline{y})\overline{z} = \overline{xz}+\overline{yz} \quad \Longleftarrow \quad \overline{(x+y)z} = \overline{xz+yz}$$

Остальное – аналогично
Если A – кольцо с единицей, то $\overline{1}$ – единица в A/I □

Теорема 1 (факторкольцо по простому идеалу). A – коммутативное ассоциативное кольцо, I – идеал. Следующие условия равносильны:

1. I – простой
2. $\frac{A}{I}$ – область целостности

Доказательство. Пусть $X \in A/I, \quad x \in X$
Тогда $X = 0 \iff \overline{x} = \overline{0} \iff x \underset{I}{\equiv} 0 \iff x - 0 \in I \iff x \in I$

- (1) $\Longrightarrow$ (2)
  Пусть $X, Y \in A/I, \qquad XY = \overline{0}$
  Пусть $x \in X, \quad y \in Y \implies \overline{xy} = \overline{0} \implies xy \in I \xRightarrow[I \text{ простой}]{} \left[\begin{array}{l} x \in I \implies X = \overline{0} \\ y \in I \implies Y = \overline{0} \end{array}\right.$
- (2) $\Longrightarrow$ (1)
  Пусть $xy \in I \implies \overline{xy} = \overline{0} \implies \overline{x}\cdot\overline{y} = \overline{0} \xRightarrow[\text{обл. цел.}]{} \left[\begin{array}{l} \overline{x} = 0 \implies x \in I \\ \overline{y} = 0 \implies y \in I \end{array}\right.$

□

Теорема 2 (факторкольцо по максимальному идеалу). A – коммутативное ассоциативное кольцо с единицей, I – идеал. Следующие условия равносильны:

1. I – максимальный
2. A/I – поле

Доказательство.

- (1) $\Longrightarrow$ (2)
  A/I – коммутативное ассоциативное кольцо с единицей

Осталось доказать, что $\forall X \in {}^{A}\!/_{I},\ X \neq \overline{0} \quad \exists X^{-1}$

$$\overline{0} = I \implies X \neq I$$

Пусть $x \in X \implies x \in I$
Пусть $J := \langle x, I \rangle$ (он существует, это обсуждалось в прошлый раз)

$$J \supset I,\ J \neq I \xrightarrow[I \text{ – макс.}]{} J = A \implies A \in J$$

$$1 \in \langle I, x \rangle \implies 1 = \underbrace{a_1 s_1 + \ldots + a_k s_k}_{\in I} + bx \text{ для некоторых } s_i \in I, \quad a_i, b \in A$$

$$\implies 1 \equiv bx \pmod{I} \implies \overline{1} = \overline{b} \cdot \overline{x} = \overline{b}X \implies \overline{b} = X^{-1}$$

- (2) $\implies$ (1)
Пусть J – идеал, $I \subset J,\ I \neq J$
Докажем, что $J = A$:
Пусть $x \in J \setminus I$

$$\overline{x} \in {}^{A}\!/_{I}, \qquad \overline{x} \neq \overline{0} \quad \implies \exists Y : \overline{x}Y = \overline{1}$$

Пусть $\overline{y} \in Y \implies \overline{x} \cdot \overline{y} = \overline{1} \implies xy - 1 \in I$

$$\left.\begin{array}{l} x \in J \\ xy - 1 \in I \end{array}\right\} \implies 1 = \underbrace{xy}_{\in J} - \underbrace{(xy-1)}_{\in I} \in J \implies J = A$$

□

Замечание. Поле является областью целостности $\implies$ в кольце с единицей максимальный идеал является простым

Теорема 3 (факторкольцо кольца многочленов). K – поле, $A = K[x]$, $P(x) \in A$, $I = \langle P(x) \rangle$ (это не условие, а обозначение – известно, что все идеалы такие), $B = {}^{A}\!/_{I}$
Тогда равносильны условия:

1. P неприводим $\iff {}^{A}\!/_{I}$ – поле

Доказательство. Правая часть равносильна тому, что I максимальный

- $\implies$
Пусть $I \in J, \quad Q(x)$ – такой, что $J = \langle Q(x) \rangle$

$$\langle P(x) \rangle \subset \langle Q(x) \rangle \implies P(x) \vdots Q(x) \xrightarrow[P \text{ неприводимый}]{}$$

$$\implies \left[\begin{array}{l} Q(x) = cP(x), \quad c \in K, \quad c \neq 0 \implies J = I \\ Q(x) = c, \quad c \in K, \quad c \neq 0 \implies J = A \end{array}\right. \implies I \text{ max}$$

- $\impliedby$
Пусть P приводим

$$\implies \exists Q(x) : \quad P(x) \vdots Q(x), \qquad Q(x) \neq cP(x), \quad Q(x) \neq c$$

$$\implies \langle P(x) \rangle \subsetneq \langle Q(x) \rangle \subsetneq A \implies I \text{ не max}$$

□

1.2. Гомоморфизм колец

Определение 1. $(A, +_A, \cdot_A)$, $(B, +_B, \cdot_B)$ – кольца

Отображение $f : A \to B$ называется гомоморфизмом, если

$$f(x +_A y) = f(x) +_B f(y)$$

$$f(x \cdot_A y) = f(a) \cdot_B f(y)$$

Определение 2. Отображение $f : A \to B$ называется изоморфизмом, если f – гомоморфизм и биекция

Определение 3. Если существует изоморфизм из A в B, то A и B называются изоморфными

Обозначение. $A \simeq B$

Все тривиальные свойства верны: про обратный, про композицию, про отношение "эквивалентности" (настоящей эквивалентности здесь нет – нет множества всех колец)

Определение 4. A, B – цольцо, $f : A \to B$ – гомоморфизм
Ядро: $\{ x \in A \mid f(x) = 0 \}$

Обозначение. $\ker f$

Образ: $\{ f(x) \mid x \in A \}$

Обозначение. $\operatorname{Im} A$

Свойства. A, B – коммутативные, $f : A \to B$ - гомоморфизм

1. $f(0) = 0$

   Доказательство. Следует из аналогичного свойства для гомоморфизма групп □

   Замечание. Коммутативность здесь не нужна

   Замечание. Для единицы не верно

2. $\ker f$ – идеал

   Доказательство. $\ker f \neq 0$, т. к. $0_A \in \ker f$

   - $x, y \in \ker f \implies f(x+y) = \underbrace{f(x)}_{0} + \underbrace{f(y)}_{0} = 0 + 0 = 0$
   - $\underbrace{f(0)}_{0} = f\big(x + (-x)\big) = \underbrace{f(x)}_{0} + f(x) \implies f(-x) = 0$
   - $a \in A \qquad f(ax) = f(a)f(x) = f(a) \cdot 0 = 0$

   □

3. $\operatorname{Im} f$ – подкольцо B

   Доказательство. $\operatorname{Im} f \subset B$
   Нужно преверить, что $\operatorname{Im} f$ замкнут относительно операции
   Для сложения – можно сослаться на группы
   Для умножения:

   $$x, y \in \operatorname{Im} f \implies a, b \in A : \quad f(a) = x, \quad f(b) = y$$
   $$\implies xy = f(a)f(b) = f(ab) \in \operatorname{Im} f$$

   □

Теорема 4 (о гомомрфизме колец). A, B – коммутативные ассоциативные кольца
$f : A \to B$ – гомоморфизм
Тогда $A/\ker f \simeq \operatorname{Im} f$

Доказательство. Определим $\varphi : A/\ker f \to \operatorname{Im} f$
Пусть $X \in A/\ker f, \quad x \in X$

Положим $\varphi(X) \coloneqq f(x)$

$$x \in X \implies X = \overline{x} \implies \varphi(\overline{x}) = f(x)$$

- Корректность:
  Пусть $x, x' \in X$
  Проверим, что $f(x') = f(x)$

$$\overline{x} = \overline{x'} \implies x \underset{\ker f}{\equiv} x' \implies x - x' \in \ker f \implies f(x) = f\big(x' + (x - x')\big) = f(x') + \underbrace{f(x - x')}_{0 \ (x - x' \in \ker f)}$$

- Гомоморфизм:

$$X, Y \in A/_{\ker f}, \qquad x \in, \quad y \in Y$$

$$X = \overline{x}, \quad Y = \overline{y}, \qquad X + Y = \overline{x + y}, \quad XY = \overline{xy}$$

$$\varphi(X + Y) = \varphi(\overline{x + y}) = f(x + y) \underset{f \text{ гомомрф.}}{=\!=\!=\!=\!=} f(x) + f(y) = \varphi(\overline{x}) + \varphi(\overline{y}) = \varphi(\overline{x} + \overline{y})$$

  Для умножения – то же самое

- Сюръективность:
  Пусть $b \in \operatorname{Im} f$

$$\implies \exists\, x \in A: \quad f(x) = b \implies \varphi(\overline{x}) = b$$

- Инъективность:
  Пусть $\varphi(X) = \varphi(Y), \quad x \in X, \ y \in Y$

$$\implies f(x) = f(y) \implies f(x - y) = 0 \implies x - y \in \ker f \implies \overline{x} \underset{\ker f}{\equiv} y \implies \overline{x} = \overline{y} \implies X = Y$$

□

1.3. Классификация простых полей

Определение 5. A – кольцо
Характеристикой A называется называется наименьшее $n \in \mathbb{N}$ такое, что

$$\underbrace{a + a + \ldots + a}_{n} = 0 \quad \forall a \in A$$

Если такого n не существует, то характеристика равна нулю

Определение 6. $\operatorname{char} A$

Примеры. $\mathbb{R}, \mathbb{Z}, \mathbb{Q}$ – $\operatorname{char} = 0$
$\operatorname{char}(\mathbb{Z}_2) = 2$

Свойство. Если A кольцо с единицей, то $\operatorname{char} A$ – ниаменьшее $n \in \mathbb{N}$ такое, что

$$\underbrace{1 + 1 + \ldots + 1}_{n} = 0$$

Доказательство. Нужно доказать, что

$$\underbrace{a + a + \ldots + a}_{n} = 0 \quad \forall a \in A \qquad \iff \qquad \underbrace{1 + 1 + \ldots + 1}_{n} = 0$$

- $\implies$
  Подставим $a = 1$
- $\impliedby$

$$a + a + \ldots + a = a(1 + \ldots + 1) = a \cdot 0 = 0$$

□

Свойство. A – поле
Тогда $\operatorname{char} A = 0$ или $\operatorname{char} A \in \mathbb{P}$

Доказательство. Пусть **это не так** и $\operatorname{char} A$ – составное

$$\operatorname{char} A = n = mk, \qquad 1 < m, \quad k < n$$

$$0 = \underbrace{1 + \ldots + 1}_{n} = (\underbrace{1 + \ldots + 1}_{m})(\underbrace{1 + \ldots + 1}_{k}) \implies \left[\begin{array}{l} \underbrace{1 + \ldots + 1}_{m} = 0 \\ \underbrace{1 + \ldots + 1}_{k} = 0 \end{array}\right.$$

Получили противоречие с минимальностью n □

Примечание. Достаточно области целостности с единицей

Определение 7. L – поле, $K \subset L$, K является полем с теми же операциями
Тогда K называется подполем L
L называется расширением K

Примеры.

1. $\mathbb{R}$ – подполе $\mathbb{C}$
2. $\mathbb{R}(x)$ – расширение $\mathbb{R}$

Определение 8. Поле K называется простым, если оно не содержит подполей, отличных от K (считаем, что поле не может состоять из одного элемента, т. е. $0 \neq 1$)