Алгебра 4

Igor Engel

1 Кольца (продолжение)

Определение 1.1. Рассмотрим множество X и кольцо R.

$$R^X = \{f : X \mapsto R\}.$$

Введём операции:

$$(f+g)(x) = f(x) + g(x).$$

$$(f \cdot g)(x) = f(x) \cdot g(x).$$

Принцип: Если свойство верно для R, то верно и для R^X
Значит, $\langle R, + \rangle$ и $\langle R, \cdot \rangle$ наследуют свойства R.

Определение 1.2. Пусть R_1, R_2 - кольца.

$$\langle a, b \rangle + \langle c, d \rangle = \langle a + c, b + d \rangle .$$

$$\langle a, b \rangle \cdot \langle c, d \rangle = \langle a \cdot c, b \cdot d \rangle .$$

Тогда $\langle R_1 \times R_2, + \rangle$ и $\langle R_1 \times R_2, \cdot \rangle$ наследуют свойства R_1 и R_2

Определение 1.3. R - кольцо.
Кольцо верхних треугольных матриц с коэффициэнтами из R, размера 2×2:

$$R^3 = \{\langle a, b, c \rangle \mid a, b, c \in R\}.$$

$$\langle a, b, c \rangle + \left\langle a', b', c' \right\rangle = \left\langle a + a', b + b', c + c' \right\rangle .$$

$$\langle a, b, c \rangle \cdot \left\langle a', b', c' \right\rangle = \left\langle aa', ab' + bc', cc' \right\rangle .$$

Докажем ассоциативность:

$$\langle a, b, c \rangle + \left\langle a', b', c' \right\rangle) \cdot \left\langle a'', b'', c'' \right\rangle .$$

Рассмотрим центральный элемент:

$$\left\langle a + a', b + b', c + c' \right\rangle \cdot \left\langle a'', b'', c'' \right\rangle = \left\langle \_, (a + a)'b'' + (b + b')c'', \_ \right\rangle .$$

$$\langle a, b, c \rangle \cdot \left\langle a'', b'', c'' \right\rangle + \left\langle a', b', c' \right\rangle \cdot \left\langle a'', b'', c'' \right\rangle .$$

$$\left\langle \_, ab'' + bc'', \_ \right\rangle + \left\langle \_, a'b'' + b'c'', \_ \right\rangle = \left\langle \_, (a+a')b'' + (b+b')c'', \_ \right\rangle.$$

Докажем отсутствие коммутативности:
Пусть $1 \in R$.

$$\langle 1,0,0\rangle \cdot \langle 0,1,1\rangle = \langle 0, 1\cdot 1 + 0\cdot 1, 0\rangle = \langle 0,1,0\rangle.$$
$$\langle 0,1,1\rangle \cdot \langle 1,0,0\rangle = \langle 0, 0\cdot 0 + 1\cdot 0, 0\rangle = \langle 0,0,0\rangle.$$

Определение 1.4. Пусть $\langle R, +, \cdot\rangle$ - кольцо. Тогда $\langle S, +, \cdot\rangle$, $S \subset R$ называется подкольцом, если:

1. $\langle S, +\rangle$ - подгруппа R
2. $$\forall a, b \in S \quad a \cdot b \in S.$$
3. Если $1 \in R$, то $1 \in S$

Если $\langle S, +, \cdot\rangle$ - подкольцо, то:

1. $\langle S, +, \cdot\rangle$ - кольцо
2. $\langle S, +, \cdot\rangle$ наследует свойства R, за исключением обратных элементов.

Пример 1.1. Возьмём $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \subset \mathbb{R}$.

$$(a + b\sqrt{2}) + \left(a' + b'\sqrt{2}\right) = \left(a + a'\right) + \left(b + b'\right)\sqrt{2}.$$
$$(a + b\sqrt{2}) \cdot (a' + b'\sqrt{2}) = \left(aa' + 2bb'\right) + \left(ab' + ba'\right)\sqrt{2}.$$
$$1 + 0\sqrt{2} = 1.$$

Определение 1.5 (Кольцо многочленов)**.** Пусть R - кольцо.

$$R[x] = \{a_0 + a_1 x + \ldots + a_n x^n \mid a_i \in R\}.$$

$$R[[x]] = \{a_0 + a_1 x + \ldots + a_n x^n + \ldots \mid a_i \in R\} = \{f : \mathbb{N} \mapsto R\}.$$
$$R[x] \subset R[[x]].$$
$$R[x] = \{f : \mathbb{N} \mapsto R \mid \exists N > 0 \quad \forall n > N \quad f(n) = 0\}.$$
$$(f + g)(n) = f(n) + g(n).$$
$$(f \cdot g)(n) = \sum_{i+j=n} f(i) \cdot b(j).$$

$R[[x]]$ - кольцо, $R[x]$ - его подкольцо.
Оба кольца наследуют свойства R.

Определение 1.6. Пусть $\langle R, +, \cdot \rangle$ - ассоциативное кольцо с единицей.
x называется обратимым, если он обратим относительно $\cdot$

$$\exists x^{-1} \in R \quad x \cdot x^{-1} = x^{-1} \cdot x = 1.$$

Теорема 1.1.

$$R^* = \{a \in R \mid a \text{ - обратим}\}.$$

R^* - подкольцо R.

$$(a \cdot b)(b^{-1}a^{-1}).$$

$$a^{-1} \in R \impliedby a^{-1}(a^{-1})^{-1} = 1.$$

Определение 1.7. R - поле, если R - ассоциативное коммутативное кольцо с единицей, и $R^* = R \setminus \{0\}$.

Пример 1.2.

$$\mathbb{Z}^* = \{-1, 1\}.$$

Пример 1.3.

$$\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}.$$

$$\mathbb{R}^* = \mathbb{R} \setminus \{0\}.$$

Пример 1.4.

$$(\mathbb{Z}/n)^* = \{a \in \mathbb{Z}/n \mid (a, n) = 1\}.$$

$$(\mathbb{Z}/n)^* = \mathbb{Z} \setminus \{0\} \iff n \in \mathbb{P}.$$

Пример 1.5.

$$(R^X)^* = \{f(x) \in R^X \mid \forall x \in X \quad f(x) \in R^*\}.$$

Пример 1.6.

$$(R_1 \times R_2)^* = \{\langle a, b \rangle \in R_1 \times R_2 \mid a \in R_1^* \wedge b \in R_2^*\}.$$

$$(R_1 \times R_2)^* = R_1^* \times R_2^*.$$

Пример 1.7. Если R - ассоциативное коммутативное кольцо с единицей.

$$(R[[x]])^* = \{f(x) \in R[[x]] \mid f(0) \in R^*\}.$$

В дальнейшем, если не указано иное: кольцо = ассоциативное коммутативное кольцо с единицей.

2 Группы

2.1 Гомоморфизмы групп

Определение 2.1. Пусть $\langle g_1, \cdot\rangle$, $\langle g_2, \times\rangle$ - группы $f : g_1 \mapsto g_2$ - гомоморфизм g_1, g_2, если:

$$\forall a, b \in g_1 \quad f(a \cdot b) = f(a) \times f(b).$$

Лемма 2.1.1. Если $f : g_1 \mapsto g_2$ - гомоморфизм, то:

$$f(1) = 1.$$

$$f(x^{-1}) = (f(x))^{-1}.$$

$$f(x^n) = f(x)^n, n \in \mathbb{Z}.$$

Доказательство.

$$f(1) = f(1 \cdot 1) = f(1) \times f(1) = 1 = 1 \times 1.$$

$$f(1) = f(xx^{-1}) = f(x) \times f(x^{-1}) = 1 \implies f(x^{-1}) = f(x)^{-1}.$$

Если $n > 0$:

$$f(x^n) = f(\underbrace{x \cdot x \cdot \ldots \cdot x}_{n}) = \underbrace{f(x) \times f(x) \times \ldots f(x)}_{n} = f(x)^n.$$

Если $n = 0$:

$$f(x^0) = f(1) = 1 = f(x)^0.$$

□

Определение 2.2. $f : g_1 \mapsto g_2$ - гомоморфизм.
f - мономорфизм, если f инъективная
f - эпиморфизм, если f сюръективна
f - изоморфизм, если f мономорфизм и эпиморфизм.

Определение 2.3. Если $f : g_1 \mapsto g_2$ - гомоморфизм, то

$$\ker f = \{x \in g_1 \mid f(x) = 1\}.$$

Теорема 2.1. $\ker f$ - подгруппа g_1
f - мономорфизм, тогда и только тогда $\ker f = \{1\}$

Доказательство. Пусть $a, b \in \ker f$.
Тогда $f(a) = f(b) = 1$, $f(a)f(b) = 1$
Докажем что $f(x) = f(y) \implies x = y$:
Рассмотрим $f(xy^{-1} = f(x) \times f(y)^{-1} = 1 \implies xy^{-1} = 1 \implies x = y$ □

Теорема 2.2. Если $f : g_1 \mapsto g_2$ - изоморфизм, то $f^{-1} : g_2 \mapsto g_1$ - изоморфизм.

Доказательство.

$$f^{-1}(a \times b) = f^{-1}(a) \cdot f(b).$$

$$f^{-1}(f(q) \times f(v)) = q \cdot v.$$

$$f^{-1}(f(q \cdot v)) = q \cdot v.$$

$\square$