Алгебра 3

Igor Engel

1

X - множество, на котором задана бинарная операция $(\cdot) : X \times X \mapsto X$
$(\cdot)$ - ассоциативна, если $\forall a, b, c \in X \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$
$(\cdot)$ - коммутотивна, если $\forall a, b \in X \quad a \cdot b = b \cdot a$
У $(\cdot)$ есть нейтральный элемент, если $\exists 1 \in X \quad \forall x \in X \quad 1 \cdot X$
$x \in X$ обратим, если $\exists x^{-1} \in X \quad x \cdot x^{-1} = x^{-1} \cdot x = 1$. x^{-1} называется обратным к x.
$x^n = \underbrace{x \cdot x \cdot \ldots \cdot x}_{n}$
Нейтральный элемент единственнен.

Определение 1.1. Пара $\langle X, \cdot \rangle$ называется моноидом, если:

- $\cdot$ - ассоциативна
- Сещуствует нейтральный элемент

Лемма 1.1.1. Если X - моноид, а $x, y \in X$ - обратимые элементы, и $x \cdot y$ - обратимо, то $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$.

Доказательство. Рассмотрим произведение

$$(x \cdot y) \cdot y^{-1} \cdot x^{-1}.$$

$$x \cdot y \cdot y^{-1} \cdot x^{-1} = x \cdot 1 \cdot x^{-1} = 1.$$

□

Лемма 1.1.2. Если X - моноид, то обраиный элемент единственнен

Лемма 1.1.3. Если x обратим, $x^{-1^{-1}} = x$

Определение 1.2. $\langle G, \cdot \rangle$ называется группой, если:
$\langle G, \cdot \rangle$ - моноид
Любой $g \in G$ обратим

- X - множество. Рассмотрим $S_X = \{f : X \mapsto X \mid f\text{- обратима}\}$. Тогда $\langle S_X, \circ \rangle$ - группа

Определение 1.3. $\langle G, \cdot\rangle$ - абелева группа, если:
$\langle G, \cdot\rangle$ - группа
$(\cdot)$ - коммутативна
Примеры:

- $\left\langle Z_{/n}, \cdot\right\rangle$
- $\langle\mathbb{Z}|\mathbb{Q}|\mathbb{R}, +\rangle$

Определение 1.4. Пусть G - группа.
$H \subset G$.
H - подгруппа G, если:

1. $\forall a, b \in H \quad a \cdot b \in H$
2. $\forall a \in H \quad a^{-1} \in H$
3. $1 \in H$

Примеры:

- Плоскость $\mathbb{R}^2$, $S_{\mathbb{R}^2} = \{f : \mathbb{R}^2 \mapsto \mathbb{R}^2 \mid f\text{- биекция}\}$. Подгруппа: $\mathrm{Isom}_{\mathbb{R}^2} = \{f \in S_{\mathbb{R}^2} \mid \forall\langle x, y\rangle \in \mathbb{R}^2 \quad \|f(x) - f(y)\| = \|x - y\|\}$.

- Рассмотрим подгруппу внутри $\mathrm{Ison}_{\mathbb{R}^2}$. $H = \{f \in \mathrm{Ison}_{\mathbb{R}^2} \mid f(x_0) = x_0\}$

Определение 1.5. Если $X = \{1, \ldots, n\}$, то S_X называется группой перестановок и обазначатеся S_n.
Если $n \geq 3$, то группа перестановок неабелева.

Определение 1.6. Пусть G_1, G_2 - группы. Рассмотрим группу $G_1 \times G_2$. Операция этой группы:

$$\langle g_1, g_2\rangle \cdot \langle h_1, h_2\rangle = \langle g_1 h_1, g_2 h_2\rangle .$$

Нейтральный элемент:

$$\langle 1_1, 1_2\rangle .$$

Обратный к $\langle g_1, g_2\rangle$:

$$\left\langle g_1^{-1}, g_2^{-1}\right\rangle .$$

Определение 1.7. Пусть G - группа. $x \in \mathbb{G}$.
Определим x^n, $n \in \mathbb{Z}$:

$$x^n = \begin{cases} x^n, & n > 0 \\ 1, & n = 0 \\ \left(x^{-1}\right)^{|n|}, & n < 0 \end{cases}$$

$$x^{n+m} = x^n x^m.$$

$$(x^n)^m = x^{nm}.$$

Определение 1.8. Набор $\langle R, +, \cdot \rangle$ - кльцо, если:

- $< R, + >$ - абелева группа

- $\forall a, b, c \in R \quad (a + b) \cdot c = c \cdot (a + b) = a \cdot c + b \cdot c$

Кольцо R - ассцоиативное, если $(\cdot)$ - ассоциативна Кольцо R - коммутативное, если $(\cdot)$ - коммутативно Кольцо R - кольцо с единицей, если у $(\cdot)$ существует нейтральный элемент.

Лемма 1.8.1. Если R - кольцо, то:

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

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

$$(-1) \cdot a = a \cdot (-1) = -a, \text{ если } R \text{ - кольцо с единицей.}$$

Доказательство.

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0 \implies a \cdot 0 = 0.$$

$$a \cdot (b + (-b)) = a \cdot 0 = 0.$$

$$a \cdot (b + (-b)) = a \cdot b + a \cdot -b = 0 \implies a \cdot (-b) = -(a \cdot b).$$

$\square$

Лемма 1.8.2. Если R - коммутатвное кольцо и $b \in R$ обратим, то $\frac{a}{b} = a \cdot b^{-1}$.

Определение 1.9. R - коммутативное ассоциативное кольцо является полем, если:

$$\forall r \in R \setminus \{0\} \quad r \text{ - обратимо.}$$

Примеры:

- $\langle \mathbb{Q} | \mathbb{R}, +, \cdot \rangle$

- $\left\langle \mathbb{Z}_{/p}, +, \cdot \right\rangle$, если $p \in \mathbb{P}$