

Алгебра и теория чисел

Курс Жукова И. Б.

осень 2021 г.

Оглавление

Оглавление	i
I Алгебраические структуры	1
1 Множества	3
1.1 Нотация	3
1.2 Операции на множествах	4
1.3 Отображение	4
1.4 Композиция	6
1.5 Тожественное отображение	7
2 Группы	9
2.1 Введение	9
2.2 Определение группы	10
2.3 Подгруппы	11
2.4 Таблицы Кэли	12

Часть I

Алгебраические структуры

ГЛАВА 1

Множества

1.1. Нотация

Стандартная запись

$$A' = \{1, 3, 5, 7\}$$

$$A = \{1, 3, 5, \dots, 99\}$$

Общий вид

$$B = \{2, 4, 6, \dots\} = \{2n : n \in \mathbb{N}\}$$

Стандартные числовые множества

$$\mathbb{N} = \{1, 2, 3, \dots\}$$

$$\mathbb{Z} = \{\dots, -1, 0, 1, 2, \dots\}$$

$$\mathbb{Q} = \left\{ \frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0 \right\}$$

$$\mathbb{R}, \mathbb{C}$$

Подмножества

$$A' \subset A \subset \mathbb{N}, A' \not\subset B$$

$$C = \{1, 2, 3\}$$

$$\emptyset, \{1\}, \{2\}, \{3\}$$

$$\{1, 2\}, \{1, 3\}, \{2, 3\}$$

$$\{1, 2, 3\} = C$$

Предикат для подмножеств: $\{n \in \mathbb{N} : n < 5\} = \{1, 2, 3, 4\}$

1.2. Операции на множествах

$$\oplus \Leftrightarrow \triangle$$

Пусть A, B — множества

$$A \cap B = \{a \in A \wedge a \in B\}$$

$$A \cup B = \{a : a \in A \vee a \in B\}$$

$$A \setminus B = \{a \in A \wedge a \notin B\}$$

$$A \triangle B = (A \setminus B) \cup (B \setminus A)$$

$$A \times B = \{(a, b) : a \in A, b \in B\}$$

$$A = \{1, 2, 3\} \quad B = \{-1, 1\}$$

$$A \times B = \{(1, -1), (1, 1), (2, -1), (2, 1), (3, -1), (3, 1)\}$$

$$\bigcap_{i=1}^n A_i \quad \bigcup_{i=1}^n A_i$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

1.3. Отображение

A, B — множества

Определение 1. Задать отображение A в B , значит для каждого $a \in A$ задать некоторый элемент B (т.н. образ элемента A)

$$A = \{1, 2, 3, 4\}$$

$$B = \mathbb{R}$$

a	$f(a)$
1	$\sqrt{2}$
2	0
3	7^5
4	0

$$\begin{aligned} f : \mathbb{R} &\rightarrow \mathbb{R} \\ f(a) &= a - 3 \end{aligned}$$

$$\begin{aligned} f : \mathbb{R} &\rightarrow \mathbb{R} \\ a &\mapsto a - 3 \end{aligned}$$

a	$f(a)$
1	-2
2	-1
3	0
4	1

$$\begin{aligned} f : \mathbb{R} &\rightarrow \mathbb{Z} \\ a &\mapsto \begin{cases} 1, & a > 0 \\ 0, & a = 0 \\ -1, & a < 0 \end{cases} \end{aligned}$$

$$\begin{aligned} \varphi : \mathbb{N} &\rightarrow \mathbb{N} \\ n &\mapsto |\{m \in \mathbb{N} : m \leq n \text{ \& } (m, n) = 1\}| \end{aligned}$$

$|M| = \#M = \text{Card } M$ — мощность множества
 2^M — множество всех подмножеств M , его мощность $|2^M| = 2^{|M|}$

Свойства

$f : A \rightarrow B$ называется инъекцией, если $\forall a_1, a_2 \in A : a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$

отображение называется сюръекцией, если $\forall b \in B, \exists a \in A : f(a) = b$

отображение называется биекцией, если оно одновременно инъекция и сюръекция

$$\begin{aligned} f : A &\rightarrow B \\ b \in B &\text{ полный прообраз } b \text{ относительно } f : \\ f^{-1}(b) &= \{a \in A : f(a) = b\} \end{aligned}$$

$$\begin{array}{ll} \mathbb{R} \rightarrow \mathbb{R} & \\ f : x \mapsto x^2 & f^{-1}(4) = \{-2, 2\} \\ & f^{-1}(0) = \{0\} \\ & f^{-1}(-3) = \emptyset \end{array}$$

$$\begin{array}{l} f - \text{инъекция} \Leftrightarrow \forall b \in B : |f^{-1}(b)| \leq 1 \\ f - \text{сюръекция} \Leftrightarrow \forall b \in B : |f^{-1}(b)| \geq 1 \\ f - \text{биекция} \Leftrightarrow \forall b \in B : |f^{-1}(b)| = 1 \end{array}$$

Сужение отображения

$$\begin{array}{lll} f : A \rightarrow B & A' \subset A & f : \mathbb{R} \rightarrow \mathbb{R} \\ f|_{A'} : A' \rightarrow B & & x \mapsto x^2 \\ a \mapsto f(a) & & f|_{\mathbb{R}_{\geq 0}} : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R} \end{array}$$

Образ подмножества

$$\begin{array}{ll} f : A \rightarrow B & \\ M \subset A & f(M) = \{f(m) : m \in M\} \\ & f(A) = \text{Im} A \end{array}$$

1.4. Композиция

$$\begin{array}{l} f : A \rightarrow B \quad g : B \rightarrow C \\ g \circ f : A \rightarrow C \\ a \mapsto g(f(a)) \end{array}$$

— композиция f и g

$$\begin{aligned}
f, g : \mathbb{R} &\rightarrow \mathbb{R} \\
f(x) &= x + 1 \\
g(x) &= 2x \\
g \circ f : \mathbb{R} &\rightarrow \mathbb{R} & f \circ g : \mathbb{R} &\rightarrow \mathbb{R} \\
x \mapsto 2x + 2 & & x \mapsto 2x + 1
\end{aligned}$$

1.5. Тожественное отображение

Пусть M – множество

$$\begin{aligned}
\text{id}_M : M &\rightarrow M \\
m &\mapsto m
\end{aligned}$$

Пусть $f : X \rightarrow Y$, тогда отображение $g : Y \rightarrow X$ называется обратным, если $g \circ f = \text{id}_X$, $f \circ g = \text{id}_Y$

Теорема 1. У $f : X \rightarrow Y$ есть обратное $\Leftrightarrow f$ – биекция

Доказательство.

$$\begin{aligned}
&\Rightarrow g : Y \rightarrow X & g \circ f &= \text{id}_X \\
& & f \circ g &= \text{id}_Y \\
&y \in Y & f^{-1}(y) &= \{x\} \\
&g(y) := x \\
\\
&(g \circ f)(x) = g(f(x)) = x & f^{-1}(f(x)) &= \{x\} \\
&(f \circ g)(y) = f(g(y)) = y \\
\\
&\Leftarrow g \circ f = \text{id}_X & f \circ g &= \text{id}_Y \\
&\Downarrow \Uparrow & \Downarrow \Uparrow \\
&f - \text{инъекция} & f - \text{сюръекция} \\
&f(x_1) = f(x_2) & y \in Y \Rightarrow \\
\Rightarrow g(f(x_1)) = g(f(x_2)) & \exists x \in X : f(x) = y \\
\Rightarrow x_1 = x_2 & f(g(y)) = y
\end{aligned}$$

■

ГЛАВА 2

Группы

2.1. Введение

Определение 2. Бинарная операция на множестве M – отображение из $M \times M \rightarrow M$

Примеры

1. $+, -, \cdot$ на \mathbb{Z}
2. $+$ на векторном пространстве
3. $M = X^X = \{f : X \rightarrow X\}$
 $(f, g) \mapsto f \circ g$
 $M \times M \mapsto M$

Свойства

Есть операция $M \times M \rightarrow M$, обозначим ее $(a, b) \mapsto a * b$

1. Если $\forall a, b \in M : a * b = b * a$, то $*$ коммутативна
2. $*$ ассоциативна, если $\forall a, b, c \in M : (a * b) * c = a * (b * c)$
3. $e \in M$ называется левым нейтральным, если $\forall a \in M : e * a = a$ В вычитании целых чисел ноль
 $e \in M$ называется правым нейтральным, если $\forall a \in M : a * e = a$
 $e \in M$ называется нейтральным, если он и левый, и правый нейтрален справа
нейтральный

Лемма 1. Пусть $*$ – операция, e_L, e_R – нейтральные слева и справа относительно $*$, тогда $e_L = e_R$.

Доказательство.

$$e_R = e_L \cdot e_R = e_L$$

■

Обратное к a обозначается a^{-1}

4. Пусть e нейтральный относительно $*$, $a \in M$. Элемент $b \in M$ называется обратным к a , если $b * a = a * b = e$
 Если $b * a = e \Rightarrow b$ обратный слева
 Если $a * b = e \Rightarrow b$ обратный справа

Лемма 2. Если $*$ ассоциативна и у a есть левый и правый обратный, тогда они равны. $b * a = e, a * c = e$

Доказательство.

$$\begin{aligned}(b * a) * c &= b * (c * a) \\ e * c &= b * e \\ c &= b\end{aligned}$$

■

Если $*$ – ассоциативная операция, $m \in \mathbb{Z}$:

$$a^m = \begin{cases} a_1 * a_2 * \dots * a_m & m > 0 \\ e & m = 0 \\ a_1^{-1} * a_2^{-1} * \dots * a_{-m}^{-1} & m < 0 \end{cases}$$

$$a^m * a^n = a^{m+n} \quad (a^m)^n = a^{mn}$$

2.2. Определение группы

Определение 3. Группой называется множества G с операцией $*$, такие что:

1. $*$ ассоциативна
2. У $*$ есть нейтральный элемент
3. У любого $g \in G$ есть обратный

Группа G называется абелевой (коммутативной), если $*$ коммутативна

Примеры1–4 абелевы
группы

1. $(\mathbb{Z}, +)$
2. $(\mathbb{Q}, +), (\mathbb{R}, +)$
3. $(\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot)$
4. $(\{1, -1\}, \cdot)$
5. (X^X, \cdot) – не группа, при $|X| > 1$
6. $(S(X), \cdot)$, что $S(x) = \{f : x \rightarrow x : x \text{ - биекция}\}$ – группа, не абелева при $|X| = 2$

2.3. Подгруппы

Пример. $(\mathbb{Z}, +)$ – группа, $2\mathbb{Z} = \{2n : n \in \mathbb{Z}\}$ – подгруппа

Определение 4. G – группа, $H \subset G$ называется подгруппой, если:

1. H замкнуто относительно умножения, т.е. $\forall h_1, h_2 \in H : h_1 h_2 \in H$
2. $e \in H$
3. H замкнуто относительно обратного, т.е. $\forall h \in H : h^{-1} \in H$

Примеры $\subset \Leftrightarrow <$

- $2\mathbb{Z} < \mathbb{Z}$
- $\{0\} < \mathbb{Z}$
- $\mathbb{Z} \in \mathbb{Q}$
- $(\{-1, 1\}, \cdot) < \mathbb{Q}^*$
- $\{2^n : n \in \mathbb{Z}\} < \mathbb{Q}^*$
- Группы самосовмещений (симметрий) фигур, Π – плоскость, $S(\Pi)$, $T(\Pi) < S(\Pi)$ – перемещения плоскости (движения)

Законы сокращения

Лемма 3. Пусть G - группа, $g, h_1, h_2 \in G$

$$1. gh_1 = gh_2 \Rightarrow h_1 = h_2$$

$$2. h_1g = h_2g \Rightarrow h_1 = h_2$$

Доказательство.

$$g^{-1}gh_1 = g^{-1}gh_2 \Rightarrow h_1 = h_2$$

■

2.4. Таблицы Кэли

Дана группа $G = \{g_1, g_2, \dots, g_n\}$:

	g_1	g_2	\dots	g_n
g_1	g_1g_1	g_1g_2	\dots	g_1g_n
g_2	g_2g_1	g_2g_2	\dots	g_2g_n
\vdots	\dots	\dots	\dots	\dots
g_n	\dots	\dots	\dots	\dots

Дана группа $\mathbb{Z}^* = (\{\pm 1\}, \cdot)$:

	1	-1
1	1	-1
-1	-1	1

Таблица Кэли является латинским квадратом

Дана группа самосовмещений правильного прямоугольника:

\square	e	S_1	S_2	R_π
e	e	S_1	S_2	R_π
S_1	S_1	e	R_π	S_2
S_2	S_2	R_π	e	S_1
R_π	R_π	S_2	S_1	e

Группа абелева, т.к. симметрична относительно диагонали

Рассмотрим $\mathbb{Z}^* \times \mathbb{Z}^* = \{(1, 1), (1, -1), (-1, 1), (-1, -1)\}$. Операции будем производить покомпонентно: $(a, b)(a', b') = (aa', bb')$.

	e	$(1, -1)$	$(-1, 1)$	$(-1, -1)$
e	e	$(1, -1)$	$(-1, 1)$	$(-1, -1)$
$(1, -1)$	$(1, -1)$	e	$(-1, -1)$	$(-1, 1)$
$(-1, 1)$	$(-1, 1)$	$(-1, -1)$	e	$(1, -1)$
$(-1, -1)$	$(-1, -1)$	$(-1, 1)$	$(1, -1)$	e

Последние 2 группы изоморфны (если заменить все элементы, например, буквами, то они и их таблицы Кэли будут идентичны)

Теория групп изучает группы с точностью до изоморфизма

Аксиома 1. Любые группы третьего порядка изоморфны.

С группами порядка 4 это уже не выполняется