Алгебра и теория чисел

Курс Жукова И. Б.

осень 2021 г.

Оглавление

Часть I

Алгебраические структуры

ГЛАВА 1

Множества

1.1. Нотация

Стандартная запись

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

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

Общий вид

$$B = \{2, 4, 6, ...0\} = \{2n : n \in \mathbb{N}\}$$

Стандартные числовые множества

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

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

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

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

Подмножества

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

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

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

$$f : \mathbb{R} \to \mathbb{R} \qquad f : \mathbb{R} \to \mathbb{R}$$
$$f(a) = a - 3 \qquad a \mapsto a - 3$$

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

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

$$\varphi : \mathbb{N} \to \mathbb{N}$$
$$n \mapsto |\{m \in \mathbb{N} : m \leqslant n \,\&\, (m, n) = 1\}|$$

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

Свойства

$f : A \to B$ 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

$$f : A \to B$$
$b \in B$ полный прообраз b относительно f :
$$f^{-1}(b) = \{a \in A : f(a) = b\}$$

$$\begin{array}{r} \mathbb{R} \to \mathbb{R} \\ f : x \mapsto x^2 \end{array} \qquad \begin{array}{r} f^{-1}(4) = \{-2, 2\} \\ f^{-1}(0) = \{0\} \\ f^{-1}(-3) = \varnothing \end{array}$$

f – инъекция $\Leftrightarrow \forall b \in B : |f^{-1}(b)| \leqslant 1$
f – сюръекция $\Leftrightarrow \forall b \in B : |f^{-1}(b)| \geqslant 1$
f – биекция $\Leftrightarrow \forall b \in B : |f^{-1}(b)| = 1$

Сужение отображения

$$\begin{array}{r} f : A \to B \\ f|_{A'} : A' \to B \\ a \mapsto f(a) \end{array} \qquad A' \subset A \qquad \begin{array}{r} f : \mathbb{R} \to \mathbb{R} \\ x \mapsto x^2 \\ f|_{\mathbb{R}_{\geqslant 0}} : \mathbb{R}_{\geqslant 0} \to \mathbb{R} \end{array}$$

Образ подмножества

$$\begin{array}{r} f : A \to B \\ M \subset A \end{array} \qquad \begin{array}{r} f(M) = \{f(m) : m \in M\} \\ f(A) = \mathrm{Im} A \end{array}$$

1.4. Композиция

$$f : A \to B \quad g : B \to C$$
$$g \circ f : A \to C$$
$$a \mapsto g(f(a))$$

— композиция f и g

$$f, g : \mathbb{R} \to \mathbb{R}$$
$$f(x) = x + 1$$
$$g(x) = 2x$$
$$g \circ f : \mathbb{R} \to \mathbb{R} \qquad f \circ g : \mathbb{R} \to \mathbb{R}$$
$$x \mapsto 2x + 2 \qquad x \mapsto 2x + 1$$

1.5. Тождественное отображение

Пусть M – множество

$$\mathrm{id}_M : M \to M$$
$$m \mapsto m$$

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

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

Доказательство.

$$\Longrightarrow g : Y \to X \qquad g \circ f = \mathrm{id}_X$$
$$f \circ g = \mathrm{id}_Y$$
$$y \in Y \qquad f^{-1}(y) = \{x\}$$
$$g(y) := x$$

$$(g \circ f)(x) = g(f(x)) = x \qquad f^{-1}(f(x)) = \{x\}$$
$$(f \circ g)(y) = f(g(y)) = y$$

$$\Longleftarrow g \circ f = \mathrm{id}_X \qquad f \circ g = \mathrm{id}_Y$$
$$\Downarrow \Uparrow \qquad \Downarrow \Uparrow$$
$$f \text{ – инъекция} \qquad f \text{ – сюръекция}$$
$$f(x_1) = f(x_2) \qquad y \in Y \Rightarrow$$
$$\Rightarrow g(f(x_1)) = g(f(x_2)) \qquad \exists x \in X : f(x) = y$$
$$\Rightarrow x_1 = x_2 \qquad f(g(y)) = y$$

■

ГЛАВА 2

Группы

2.1. Введение

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

Примеры

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

Свойства

Есть операция $M \times M \to M$, 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 $\forall a \in M : e * a = a$
   $e \in M$ называется правым нейтральным, если $\forall a \in M : a * e = a$
   $e \in M$ называется нейтральный, если он и левый, и правый нейтральный

В вычитании целых чисел ноль нейтрален справа

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 если левый и правый обратный, тогда они равны. $b * a = e, a * c = e$*

Доказательство.

$$(b * a) * c = b * (c * a)$$
$$e * c = b * e$$
$$c = b$$

■

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

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

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

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

Примеры

1–4 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 $S(x) = \{f : x \to x : x$ - 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. $h_1 g = h_2 g \Rightarrow h_1 = h_2$

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	$\cdots$	g_n
g_1	g_1g_1	g_1g_2	$\cdots$	g_1g_n
g_2	g_2g_1	g_2g_2	$\cdots$	g_2g_n
$\vdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
g_n	$\cdots$	$\cdots$	$\cdots$	$\cdots$

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 изомфорфизма

Аксиома 1. Любые группы третьего порядка изоморфны.

С группами порядка 4 это уже не выполняется

ГЛАВА 3

Отношения на множестве

Определение 5. Отношения на множестве M – это подмножество в $M \times M$

Пример. $\leqslant$ на $\{1,2,3\}$ – $\{(1,1),(1,2),(1,3),(2,2),(2,3),(3,3)\}$

Определение 6. R на M называется рефлексивным, если

$$\forall m \in M : (m,n) \in R$$

Определение 7. R на M называется симметричным, если

$$\forall m,n \in M : (m,n) \in R \implies (n,m) \in R$$

Определение 8. R на M называется антисимметричным, если

$$\forall m,n \in M : (m,n) \in R, (n,m) \in R \implies m = n$$

Определение 9. R на M называется транзитивным, если

$$\forall a,b \in M : (a,b) \in R, (b,c) \in R \implies (a,c) \in R$$

Определение 10. R называется отношением эквивалентности, если оно рефлексивно, симметрично и транзитивно.

Пусть R – отношения эквивалентности на M, $a \in M$. Класс $[a] = \{b \in M : bRa\}$

Будем использовать запись $(a,b) \in R = aRb$

Лемма 4.

$$\forall m,n \in M : [m] = [n] \text{ или } [m] \cap [n] = \varnothing$$

Доказательство.

$$[m] \cap [n] \neq \varnothing$$
$$\exists l \in [m] \cap [n]$$
$$\Longrightarrow lRm, lRn \Longrightarrow mRl \Longrightarrow mRn$$
$$a \in [m] \Longrightarrow aRm \Longrightarrow aRn \Longrightarrow a \in [n]$$

Таким образом $[m] \subset [n]$. Аналогично $[n] \subset [m] \Longrightarrow [m] = [m]$

■

Теорема 2. *Пусть R отношение эквивалентности на множестве M, тогда $M = \bigcup_{i \in I} C_i$, т.ч. $C_i \cap C_j = \varnothing (i \neq j)$ и $mRn \Leftrightarrow m, n \in C_i$ для некоторого i.*

Доказательство.

$$C_i\text{– всевозможные } [m] \in R$$
$$M = \bigcup_{m \in M} [m] \text{ т.к. } m \in [m]$$
$$a, b \in [m] \Longrightarrow \begin{cases} aRm \\ bRm \end{cases} \Longrightarrow aRb$$
$$\left.\begin{array}{l} a \in [m] \\ b \in [n] \\ aRb \end{array}\right\} \Longrightarrow [m] = [n]$$
$$\left.\begin{array}{l} bRn \\ aRb \end{array}\right\} \Longrightarrow aRn \Longrightarrow a \in [m] \cap [n] \Longrightarrow [m] \cap [n] \neq \varnothing \Longrightarrow [m] = [n]$$

■

Определение 11. Если $\sim$ – отношение эквивалентности на M, то множество классов эквивалентности: $M/\sim$ – фактормножество M относительно $\sim$

Часть II

Основы теории чисел

ГЛАВА 4

Делимость

$a \mid b$ или $b \vdots a$ читается как a делит b или b делится на a, если $\exists q \in \mathbb{Z} : b = aq$

Пример. Делители $4 : -4, -2, -1, 1, 2, 4$
Делители 0: все элементы $\mathbb{Z}$

4.1. Свойства

1. Рефлексивность
2. $\left.\begin{matrix} a \mid b \\ b \mid a \end{matrix}\right\} \implies a = \pm b$
3. Транзитивность
4. $a \mid b \implies \forall c \in Z : a \mid bc$
5. $a \mid b, a \mid c \implies a \mid (b \pm c)$
6. $a \mid b \implies \forall k \in \mathbb{Z} : ka \mid kb \qquad b = aq \implies kb = kaq \implies ka \mid kb$
7. $ka \mid kb, k \neq 0 \implies a \mid b \qquad kb = kaq \Leftrightarrow k(b - aq) = 0 \implies b - aq = 0 \implies b = aq$

Теорема 3 (О делении с остатком)**.** $\forall a \in \mathbb{Z} \forall b \in \mathbb{N} \exists! q, r \in \mathbb{Z}$

1. $a = bq + r$

2. $0 \leqslant r < b$

Доказательство. Выберем q, т.ч. $a - bq \geqslant 0$ наименьшая возможная разность

$$r = a - bq$$
$$r = a - bq \implies a = bq + r$$
$$r \geqslant 0$$
предположим, что $r \geqslant b$
$$a - bq - b = r - b \geqslant 0 \implies a - b(q+1) < a - bq$$
противоречие с выбором q

Пусть $a = bq_1 + r_1 = bq_2 + r_2$

$$0 \leqslant r_1, r_2 < b$$
$$b(q_1 - q_2) = r_2 - r_1$$
$$-(b-1) \leqslant r_2 - r_1 \leqslant 0 - 1$$
$$b \mid b(q_1 - q_2) \implies q_1 - q_2 = 0 \implies r_2 - r_1 = 0$$

■

ГЛАВА 5

Простые числа

Определение 12. $p \in \mathbb{Z}$ называется простым, если $p \neq 0, \pm 1$ и $\{a : a \mid p\} = \{\pm 1, \pm p\}$. Простые числа могут быть отрицательными.

$$\mathbb{Z} = \{0, \pm 1\} \cup \{\text{простые}\} \cup \{\text{составные}\}$$

Утверждение 1. *Пусть $a > 1$, тогда наименьший натуральный делитель a, отличный от 1 – простое число.*

Доказательство. p – наименьший натуральный делитель n. Если p составное, то $\exists q : 1 < q < p, q \mid p$

$$\left.\begin{array}{l} q \mid p \\ p \mid n \end{array}\right\} \implies q \mid n, q < p \qquad \perp$$

■

Следствие 1. *Любое целое число, кроме ± 1 делится на простое*

Следствие 2. *Наименьший натуральный делитель, $\neq 1$, составного числа n не больше $\sqrt{n}$.*

Доказательство. p – наименьший натуральный делитель n, $\neq 1$.

$$n = pb$$

Предположим, что $p > \sqrt{n}$, n – составное $\implies b \neq 1 \implies b \geqslant p > \sqrt{n}$

$$n = pb > \sqrt{n}\sqrt{n} = n \qquad \perp$$

■

Теорема 4 (Эвклида)**.** *Простых бесконечно много.*

Доказательство. Пусть это не так, $p_1, p_2, ..., p_k$ – все положительные простые.

$$n = p_1 p_2 ... p_k + 1$$
$$n > 1 \implies \text{составное}$$
$$\implies \exists \text{ простое } p \mid n, p > 0$$
$$\implies p \in \{p_1, ..., p_k\} \implies p \mid (n-1)$$
$$\left.\begin{array}{l} p \mid n \\ p \mid (n-1) \end{array}\right\} \implies p \mid 1 \implies p = \pm 1 \qquad \bot$$

■

ГЛАВА 6

Наибольший общий делитель

$a_1, ..., a_n \in \mathbb{Z}$ не все 0, $d \geqslant 0$ называется наибольшим общим делителем $a_1, ..., a_n$ если:

1. $d \mid a_1, ..., d \mid a_n$
2. $\forall d' \geqslant 0 : d' \mid a_1, ..., d' \mid a_n \implies d' \mid d$

Определение 13. НОД существует и единственный

Доказательство.

$$I = \{a_1c_1 + ... + a_nc_n : c_1, ..., c_n \in \mathbb{Z}\}$$

d – наименьший положительный элемент I

$$c_i \neq 0 \implies c_i \cdot 1 > 0 \text{ или } c_i \cdot (-1) > 0$$

Доказать: d – НОД $a_1, ..., a_n$

Предположим, что $d \nmid a_j$

$$a_j = dq + r, 0 < r < d$$
$$r = a_j - dq = a_j - (a_1c_1 + ... + a_nc_n)q =$$
$$= a_1(-c_1)q + ... + a_j(1 - c_1q) + a_n(-c_nq) \in I \qquad \perp$$

Пусть $d' \mid a_1, ..., d' \mid a_n \implies d' \mid a_1c_1, ..., d' \mid a_nc_n \implies d' \mid (a_1c_1 + ... + a_nc_n) \implies d' \mid d$

Единственность. Пусть d_1, d_2 – НОД $a_1, ..., a_n \implies d_2 \mid d_1$, аналогично $d_1 \mid d_2 \implies d_1 = d_2$ ■