

Оглавление

0.1	Группы	1
0.2	Кольца и поля	2
1	Теория чисел	4
1.1	Алгоритм Евклида	4

Лекция 3: Группы, кольца, поля и теория чисел

22.09.2023

0.1 Группы

- Пример.**
1. $\mathbb{R}^* = (\mathbb{R} \setminus \{0\}, \cdot)$ - абелева группа
аналогично с $\mathbb{Q}^*, \mathbb{Q}_+^*, \mathbb{R}_+^*$
 2. $(\mathbb{R}, +)$ - абелева
 3. пусть X - множество, G - множество биекций $X \Rightarrow X$, \circ - композиция, тогда G - группа
 4. Группа движений плоскости, операция - \circ
 5. пусть X - множество, тогда $(2^X, \triangle)$ - группа (доказать)

Свойство. (сокращение), G - группа, $a, b, c \in G$

1. если $ac = bc \Rightarrow a = b$
2. если $ca = cb \Rightarrow a = b$

Доказательство. $ac = bc \xRightarrow{\exists c^{-1}} (ac)c^{-1} = (bc)c^{-1} \xRightarrow{\text{ассоц.}} a(cc^{-1}) = b(cc^{-1}) \Rightarrow ae = be \Rightarrow a = b$ Q.E.D. □

Определение 1. Группы G и H - изоморфны, если \exists биекция из G в H , т.ч. $\forall x, y \in G : f(x \cdot y) = f(x) * f(y)$ где \cdot - операция G , $*$ - операция H

Обозначение. $G \cong H$, f - изоморфизм

Пример. $G(\mathbb{R}, +) \cong H(\mathbb{R}_+^*, \cdot)$ $f(x) = 2^x$ - изоморфизм:

$$\begin{aligned} f(x+y) &= 2^{x+y} \\ f(x)f(y) &= 2^x \cdot 2^y \end{aligned}$$

0.2 Кольца и поля

Замечание. в теории чисел все числа по умолчанию целые

Определение 2. число a делится на b , если: $\exists c : a = bc$

Свойство. 1. $a : c, b : c \Rightarrow a + b : c, a - b : c$

Доказательство. $a : c \Rightarrow a = kc \wedge b : c \Rightarrow b = mc$

$$a = kc \wedge b = mc \Rightarrow \begin{cases} a + b = (m + k)c : c \\ a - b = (m - k)c : c \end{cases} \quad \text{Q.E.D.} \quad \square$$

2. $\forall k : a : b \Rightarrow ak : b$

3. $a : b \wedge b : c \Rightarrow a : c$

4. $a : b \Rightarrow |a| \geq |b| \vee a = 0$

Доказательство. $a = bc \Rightarrow \begin{cases} c = 0, \text{ значит } a = 0 \\ c \neq 0, \text{ значит } |c| \geq 1 \end{cases}$
значит, $|a| = |c||b| \geq |b|$ Q.E.D. \square

5. $\forall a : a : 1$

6. $\forall a : 0 : a$

Определение 3. НОД (a_1, a_2, \dots, a_k) - наибольшее число, на которое делятся a_1, a_2, \dots, a_k

Обозначается как: (a_1, a_2, \dots, a_k)

Определение 4. НОК (a_1, a_2, \dots, a_k) - наименьшее число, которое делится на a_1, a_2, \dots, a_k

Обозначается как: $[a_1, a_2, \dots, a_k]$

Теорема 1. Если не все числа a_1, a_2, \dots, a_k равны нулю, то НОД существует.

Доказательство. Пусть A - множество всех общих делителей, тогда $1 \in A \Rightarrow A \neq \emptyset$

A ограничено сверху, т.к. $\forall \text{ делитель } \leq |a_i|$, где a_i - любое ненулевое

число, значит, в множестве A есть наибольший элемент Q.E.D. \square

Теорема 2. Если все числа a_1, a_2, \dots, a_k не равны нулю, но НОК существует.

Доказательство. Пусть A - множество всех общих кратных, тогда $a_1, a_2, \dots, a_k \in A \Rightarrow A \neq \emptyset$

A ограничено снизу числом 0, значит, в множестве A есть наименьший элемент Q.E.D. \square

Глава 1

Теория чисел

1.1 Алгоритм Евклида

Теорема 3. (деление с остатком) Пусть $b \in \mathbb{N}, a \in \mathbb{Z}$, тогда $\exists! q, r$:

$$\begin{cases} a = bq + r, \\ 0 \leq r \leq b - 1 \end{cases}$$

Доказательство. 1. Пусть $A = \{a - bx : x \in \mathbb{Z}\}$

Среди элементов A есть хотя бы один неотрицательный:

- . если $a \geq 0$, то $a \in A$
- . если $a < 0$, то $a - ab = a(1 - b) \in A$

Пусть r - наименьший неотрицательный элемент в A . Проверим, что он подходит.

$r = a - bx \Rightarrow a = bx + r$, x можно взять в качестве q

Предположим, что $r \geq b$, тогда:

$r - b = a - b(x + 1) \in A \Rightarrow r$ - не наименьший элемент в $A \Rightarrow r \leq b - 1$

2. Докажем единственностью Пусть $a = bq_1 + r_1 = bq_2 + r_2$;

$0 \leq r_1, r_2 \leq b - 1$

$b(q_1 - q_2) = r_2 - r_1 \Rightarrow (r_2 - r_1) : b \Rightarrow \begin{cases} r_2 - r_1 = 0 \\ |r_2 - r_1| \geq b \end{cases}$ - противоречие: $r_1, r_2 \leq b - 1$

Значит, $r_1 = r_2 \Rightarrow q_1 = q_2$ Q.E.D.

□

Определение 5. (Алгоритм Евклида) даны числа $a, b \in \mathbb{N}, a \geq b$

1. если $a : b$ - конец алгоритма, результат = b
2. если же не делится, то алгоритм применяется к паре (b, r) , где r - остаток от деления a на b

Пример. $a = 22$, $b = 6$

$$1. \ 22 = 3 \cdot 6 + 4 : (22, 6) \rightarrow (6, 4)$$

$$2. \ 6 = 1 \cdot 4 + 2 : (22, 6) \rightarrow (4, 2)$$

$$3. \ 4 = 2 \cdot 2 - \text{конец, ответ: } 2$$

Замечание. (Запись с формулами:)

$$a = bq_0 + r_1 \quad 0 \leq r_1 < b$$

$$b = r_1q_1 + r_2 \quad 0 \leq r_2 < r_1$$

$$r_1 = r_2q_2 + r_3 \quad 0 \leq r_3 < r_2$$

$$\vdots \quad \vdots \quad \vdots$$

$$r_{k-2} = r_{k-1}q_{k-1} + r_k \quad 0 \leq r_k < r_{k-1}$$

$$\vdots \quad \vdots \quad \vdots$$

$$r_{n-2} = r_{n-1}q_{n-1} + r_n \quad 0 \leq r_n < r_{n-1}$$

$$r_{n-1} = r_nq_n, \text{ ОТВЕТ: } r_n$$