Оглавление

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. $ac = bc \overset{\exists c^{-1}}{\Rightarrow} (ac)c^{-1} = (bc)c^{-1} \overset{\text{ассоц.}}{\Rightarrow} a(cc^{-1}) = b(cc^{-1}) \Rightarrow ae = be \Rightarrow a = b$ 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. $G(\mathbb{R},+)$ $H(\mathbb{R}_+^*,\cdot)$ $f(x)=2^x$ - изоморфизм:

$$f(x+y)=2^{x+y}$$
$$f(x)f(y)=2^x\cdot 2^y$$

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. $a \vdots c, b \vdots c \Rightarrow a+b \vdots c, a-b \vdots c$

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

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

2. $\forall k : a \vdots b \Rightarrow ak \vdots b$
3. $a \vdots b \wedge b \vdots c \Rightarrow a \vdots c$
4. $a \vdots b \Rightarrow |a| \geq |b| \vee a = 0$

Доказательство. $a = bc \Rightarrow \begin{bmatrix} c=0, \text{значит } a=0 \\ c\neq 0, \text{значит } |c|\geq 1 \end{bmatrix}$

значит, $|a| = |c||b| \geq |b|$ Q.E.D. □

5. $\forall a : a \vdots 1$
6. $\forall a : 0 \vdots a$

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

Обозначается как: $(a_1, a_2, \ldots, a_k)$

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

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

Теорема 1. Если не все числа $a_1, a_2, \ldots, a_k$ равны нулю, но НОД существует.

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

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

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

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

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

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

0.3 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

Преположим, 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 $a = bq_1 + r_1 = bq_2 + r_2$;

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

$b(q_1 - q_2) = r_2 - r_1 \Rightarrow (r_2 - r_1) \vdots b \Rightarrow \left[\begin{array}{c} r_2 - r_1 = 0 \\ |r_2 - r_1| \geq b - \text{противоречие: } r_1; r_2 \leq b - 1 \end{array}\right.$

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 $a \vdots b$ - 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. $22 = 3 \cdot 6 + 4 : (22, 6) \to (6, 4)$
2. $6 = 1 \cdot 4 + 2 : (22, 6) \to (4, 2)$
3. $4 = 2 \cdot 2$ - конец, ответ: 2

Замечание. (Запись с формулами:)

$$
\begin{array}{lll}
a = bq_0 + r_1 & & 0 \le r_1 < b \\
b = r_1 q_1 + r_2 & & 0 \le r_2 < r_1 \\
r_1 = r_2 q_2 + r_3 & & 0 \le r_3 < r_2 \\
\vdots & \vdots & \vdots \\
r_{k-2} = r_{k-1} q_{k-1} + r_k & & 0 \le r_k < r_{k-1} \\
\vdots & \vdots & \vdots \\
r_{n-2} = r_{n-1} q_{n-1} + r_n & & 0 \le r_n < r_{n-1} \\
r_{n-1} = r_n q_n, \text{ ответ: } r_n & &
\end{array}
$$