

---

2019-09-10

### Следствие

$G$  - кон. группа,  $a \in G$ ,  $\text{ord } a = m$ ,  $H = \{a^n : n \in \mathbb{Z}\}$ , тогда  $|H| = m$

### Док-во

$\{a^0 = e, a^1, \dots, a^{m-1}\}$  - подмножество  $H$

Докажем, что все остальные элементы тоже здесь есть

$$n \in \mathbb{Z} \Rightarrow n = mq + r, 0 \leq m - 1$$

$$a^n = a^{mq+r} = (a^m)^q a^r = a^r$$

$$a^k = a^l, 0 \leq k \leq l \leq m - 1, \text{ умножим на } a^{-k}$$

$$e = a^{l-k} \text{ } 0 \leq l - k \leq m - 1 \text{ m - наименьшее } \mathbb{N} \text{ такое что } a^m = e$$

$$l - k = 0 \Rightarrow l = k$$

Докажем, что  $|H| = m$

$\Rightarrow |G| : m = \text{ord } a$ , т.о. в группе порядок эл-та - делитель порядка группы

Напоминание

### Следствие (теорема Эйлера)

$n, a \in \mathbb{N}$ ,  $(a, n) = 1$ , тогда  $a^{\varphi(n)} \equiv 1 \pmod{n}$

### Док-во

Рассмотрим  $G = (\mathbb{Z}/n\mathbb{Z})^*$   $|G| = \varphi(n)$

$$\bar{a} \in G, \text{ord } \bar{a} = k$$

$$\varphi(n) : k \Rightarrow \varphi(n) = kl$$

$$\bar{a} = \bar{1}$$

$$\bar{a}^{\varphi(n)} = \bar{1}$$

### Опр

$G$  - циклическая группа, если  $\exists g \in G : \forall g' \in G : \exists k \in \mathbb{Z} : g' = g^k$

Такой  $g$  называется образующим

### Опр

$\mathbb{Z}$  (образующий - единица и минус единица)

### Замечание

Любая циклическая группа - коммутативна

### Док-во

$$g'g'' = g''g' = g^k g^l = g^l g^k$$

Пусть  $G, H$  - группы, рассмотрим  $G \times H = \{(g, h) : g \in G, h \in H\}$

Введем операцию  $(g, h) * (g', h') \stackrel{def}{=} (g *_G g', h *_H h')$

Докажем, что это группа.

Доказательство ассоциативности:  $((g, h)(g', h'))(g'', h'') \stackrel{?}{=} (g, h)((g', h')(g'', h''))$

$$(gg', hh')(g'', h'') \stackrel{?}{=} (g, h)(g'g'', h'h'')$$

$$((gg')g'', (hh')h'') \stackrel{?}{=} (g(g'g''), h(h'h'')) - \text{очевидно}$$

Нейтральный элемент:

$$\text{Рассмотрим } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1})\}$$

## Опр

Конечная группа порядка  $n$  является циклической тогда и только тогда, когда она содержит элемент порядка  $n$  ( $|G| = n$ ,  $G$  - циклическая  $\equiv \exists g \in G : \text{ord } g = n$ )

Рассмотрим  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$  - циклическая

$$((\bar{1}, \bar{1}), (\bar{0}, \bar{2}), (\bar{1}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{2}))$$

Рассмотрим  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$  - не циклическая

## Опр

$\varphi : G \rightarrow H$  - биекция и  $\varphi(g_1, g_2) = \varphi(g_1)\varphi(g_2) \quad \forall g_1, g_2 \in G$ , тогда  $\varphi$  - изоморфизм

## Примеры

$$1. D_3 \rightarrow S_3$$

$$2. U_n = \{z \in \mathbb{C} : z^n = 1\} \leftarrow \mathbb{Z}/n\mathbb{Z}$$

$$\left(\frac{2\pi a}{n} + i \sin \frac{2\pi a}{n} = \varphi \bar{a} \bar{a}\right)$$

$$\bar{a} = \bar{b} \rightarrow \varphi(\bar{a}) = \varphi(\bar{b})$$

$$\varphi(\bar{a} + \bar{b}) \stackrel{?}{=} \varphi(\bar{a})\varphi(\bar{b})$$

$$\cos \frac{2\pi(a+b)}{n} + i \sin \frac{2\pi(a+b)}{n} = \left(\cos \frac{2\pi a}{n} + i \sin \frac{2\pi a}{n}\right)$$

## Опр

Две группы называются изоморфными, если между ними существует изоморфизм

## Утв

Изоморфизм - отношение эквивалентности

## Док-во

т.к. композиция изоморфизмов - изоморфизм  $G \xrightarrow{\epsilon} H \xrightarrow{\psi} H$

$$(\psi \circ \varphi)(g_1 g_2) = \psi(\varphi(g_1 g_2)) = \psi(\varphi(g_1)\varphi(g_2)) = \psi(\varphi(g_1))\psi(\varphi(g_2)) = (\psi \circ$$

$$\varphi(g_1) \circ (\psi \circ \varphi)(g_2)$$

Рефлексивность - тождественное отображение - изоморфизм

Транзитивность:  $G \xrightarrow{\varphi} H, H \xrightarrow{\varphi^{-1}} G$

## Теорема

$G$  - циклическая группа

$$1) |G| = n \Rightarrow G \cong \mathbb{Z}/n\mathbb{Z}$$

$$2) |G| = \infty \Rightarrow G \cong \mathbb{Z}$$

## Док-во

1)  $g$  - обр.  $G$ , значит  $G = \{e, g, g^2, \dots, g^{n-1}\}$  (среди них нет одинаковых), построим изоморфизм в  $\mathbb{Z}/n\mathbb{Z}$ :  $\varphi(g^k) = \bar{k}$

Проверим, что  $\varphi(g^k g^l) = \varphi(g^k) + \varphi(g^l) = \bar{k} + \bar{l}$

Левая часть:  $\varphi(g^{k+l}) = \overline{(k+l)} \bmod n = \bar{k} + \bar{l}$

2)  $G = \{\dots, g^{-1}, e, g, g^2, \dots\}$  (тоже нет совпадающих элементов, иначе  $g^k = g^l$ , при  $k > l$ , тогда  $g^{k-l} = e$ , но тогда конечное число элементов, потому что оно заикликивается через каждые  $k-l$  элементов), построим отображение в  $\mathbb{Z}$ .

$\varphi(g^n) = n$  -, очевидно, биекция. И нужно доказать, что  $\varphi(g^n g^k) = \varphi(g^n) + \varphi(g^k) = n + k$