Следствие **(теорема Эйлера)**

Напоминание

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

Док-во

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

$\overline{a} \in G$, $ord\overline{a} = k$

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

$\overline{a} = \overline{1}$

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

Определение

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

Такой g *называется образующим*

Определение

$\mathbb{Z}$ *(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: $((g, h)(g', h'))(g'', h'') \stackrel{?}{=} (g, h)((g', h')(g'', h'')$

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

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

Нейтральный элемент:

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

Определение

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

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

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

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

Определение

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

Примеры

1. $D_3 \to S_3$
2. $U_n = \{z \in \mathbb{C} : z^n = 1\} \leftarrow \mathbb{Z}/n\mathbb{Z}$
   $(\frac{2\pi a}{n} + i \sin \frac{2\pi a}{n} = \varphi \overline{a a})$
   $\overline{a} = \overline{b} \to \varphi(\overline{a}) = \varphi(\overline{b})$
   $\varphi(\overline{a} + \overline{b}) \stackrel{?}{=} \varphi(\overline{a})\varphi(\overline{b})$
   $\cos \frac{2\pi(a+b)}{n} + i \sin \frac{2\pi(a+b)}{n} = (\cos \frac{2\pi a}{n} + i \sin \frac{2\pi a}{n})$

Определение

Две группы называются изоморфными, если между ними существует изоморфизм

Утверждение

Изоморфизм - отношение эквивалентности

Док-во

т.к. композиция изоморфизмов - изоморфизм $G \xrightarrow{e} H \xrightarrow{\psi} H$
$(\psi \circ \varphi)(g_1 g_2) = \psi(\varphi(g_1 g_2) = \psi(\varphi(g_1)\varphi(g_2)) = \psi(\varphi(g_1))\psi(\varphi(g_2)) = (\psi \circ \varphi)(g_1) \circ (\psi \circ \varphi)(g_2)$
Рефлексивность - тождественное отображение - изоморфизм
Транзитивность: $G \underset{\varphi}{\to} H$, $H \underset{\varphi^{-1}}{\to} G$

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 $G = \{e, g, g^2, ..., g^{n-1}\}$ (среди них нет одинаковых), построим изоморфизм в $\mathbb{Z}/n\mathbb{Z}$: $\varphi(g^k) = \overline{k}$
Проверим, что $\varphi(g^k g^l) \underline{= \varphi(g^k) + \varphi(g^l)} = \overline{k} + \overline{l}$
Левая часть: $\varphi(g^{k+l} = \overline{(k+l) \mod n} = \overline{k} + \overline{l}$
2) $G = \{..., g^{-1}, e, g, g^2, ...\}$ (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 зацикливается через каждые $k - l$ элементов), построим отображение в $\mathbb{Z}$.
$\varphi(g^n) = n$ -, очевидно, биекция. И нужно доказать, что $\varphi(g^n g^k) = \varphi(g^n) - \varphi(g^k) = n + k$