2019-02-17

Следствие (теорема Эйлера)

Напоминание

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

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

Определение

Две группы называются изоморфными, если между ними существует изоморфизм

Утверждение

Изоморфизм - отношение эквивалентности

Док-во

т.к. композиция изоморфизмов - изоморфизм $G \stackrel{e}{\to} H \stackrel{\psi}{\to} H$
$(\psi \circ \varphi)(g_1 g_2) = \psi(\varphi(g_1 g_2) = \psi(\varphi(g_1)\varphi(g_2)) = \psi(\varphi(g_1))\psi(\varphi(g_2)) = (\psi \circ \varphi)(g_1) \circ (\psi \circ \varphi)(g_2)$
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 $\varphi(g^n g^k) = \varphi(g^n) - \varphi(g^k) = n + k$

2019-09-17

Утверждение

$|G| = p$, *простое*

$\Rightarrow G \simeq \mathbb{Z}_{/p\mathbb{Z}} \qquad g \in G, g \neq e$

$ord\ g = p$

$\Rightarrow G = \{e = g^0, g^1, ..., g^{p-1}\}$

Утверждение

H, G - *группы*, $\quad g \in G$

$\varphi : G \to H$ - *изоморфизм*

$\Rightarrow \ ord\ g = \ ord\ \varphi(g)$

$ord\ g = n \qquad g^n = e$

$\varphi(g)^n = \varphi(g^n) = \varphi(e) = e \qquad \varphi(e)^2 = \varphi(e^2) = \varphi(e)$

$\varphi(g)^n \overset{?}{\Rightarrow} e \Rightarrow m \geq n$

$m \in \mathbb{N}$

$\varphi(g^m) = \varphi(g)^m = e = \varphi(e) \quad \Rightarrow g^m = e \Rightarrow m \geq n$

Определение

$H < G$

H - *нормальная подгруппа, если* $\forall h \in H, g \in G$

$g^{-1}hg \in H$ - *сопряжение элемента* h *с помощью элемента* g

рисунок 1

$H \lhd G$

Утверждение

$H \lhd G \Leftrightarrow$ - *разбиение на л. и п. классы смежности по* H *совпадают*

$\forall g \quad gH = Hg$

Док-во

$$\Rightarrow h \in H \qquad gh \in gH$$

$$gh = \underbrace{(g^{-1})^{-1}hg^{-1}}_{\in H} g = h_1 g$$

$$\Leftarrow g \in G, h \in H$$

$$g^{-1}hg = h_1$$

$$hg \in Hg = gH \Rightarrow gh_1, h_1 \in H$$

$$H \lhd G$$

$$g_1H * g_2H \overset{def}{=} g_1g_2H$$

$$\widetilde{g_1}H = g_1H$$

$$\widetilde{g_2}H = g_2H \overset{?}{\Rightarrow} \widetilde{g_1}\widetilde{g_2}H = g_1g_2H$$

$$g_2^{-1}h_1g_2 = h_3 \in H$$

$$\widetilde{g_1}\widetilde{g_2}h = g_1h_1g_2h_2h = g_1g_2(\underbrace{g_2^{-1}h_1g_2}_{=h_3})h_2h$$

$$\widetilde{g_1}H = g_1H \Rightarrow \widetilde{g_1} = g_1h_1$$

$$\widetilde{g_2}H = g_2H \Rightarrow \widetilde{g_2} = g_2h_2$$

$$eH = H$$

$$1) \quad eH * gH = (eg)H = gH$$

$$2) \quad (g_1H * g_2H) * g_3H \overset{?}{=} g_1H * (g_2H * g_3H)$$

$$(g_1g_2)H * g_3H = (g_1g_2)g_3H$$

$$3) \quad gH * g^{-1}H = (gg^{-1})H = eH$$

$$G_{/H}$$

$$a \sim b \Leftrightarrow a - b \,\vdots\, h$$

$$G = \mathbb{Z}$$

$$H = h\mathbb{Z} \quad g_1 - g_2 \in n\mathbb{Z}$$

$$[a] + [b] = [a + b]$$

Пример

$$[g,h] = ghg^{-1}h^{-1} \text{ - } \textit{коммутатор}$$

$$g, h \in G$$

$$K(G) = \{[g_1,h_1],...,[g_n,h_n], g_i, h_i \in G\} \text{ - } \textit{коммутант}$$

Док-во

Коммутант - подгруппа

$$K(G) < G$$

$$[e,e] = e$$

$$[g_1,h_1]...[g_n,h_n]$$

$$[g,h]^{-1} = (ghg^{-1}h^{-1})^{-1} = hgh^{-1}g^{-1} = [h,g]$$

$$([g_1,h_1]...[g_n,h_n])^{-1} = [h_1,g_1]...[g_n,h_n]$$

$$g^{-1}[g_1,h_1]...[g_n,h_n]g =$$

$$= (g^{-1}[g_1,h_1]g)(g^{-1}[g_2,h_2]g)...(g^{-1}[g_n,h_n]g)$$

$$g^{-1}g_1h_1g_1^{-1}h_1^{-1}g =$$

$$= (g^{-1}g_1h_1g_1^{-1}(gh_1^{-1})h_1g^{-1})h_1^{-1}g$$

$$[g^{-1}g_1,h_1] \qquad [h_1,g^{-1}]$$

Утверждение

$$G_{/K(G)} \text{ - } \textit{комм}$$

Док-во

$$g_1, g_2 \in G \qquad g_1K(G)g_2K(G) \stackrel{?}{=} g_2K(G)g_1K(G)$$

$$g_1g_2K(G) = g_1g_2K(G) \qquad g_2K(G)g_1K(G) = g_2g_1K(G)$$

$$[g_1,g_2] = g_1g_2(g_2g_1)^{-1} \in K(G)$$

Утверждение

$$\mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}_{mn},\ \textit{если}\ (m,n) = 1$$

$$[a]_{nm} \to ([a]_n, [a]_m)$$

$$[a]_{nm} = [a']_{mn} \Rightarrow [a]_n = [a']_n, [a']_m = [a']_m$$

$$\forall b, c \in \mathbb{Z}\ \exists x \in \mathbb{Z} : \begin{cases} [x]_n = [b]_n \\ [x]_m = [c]_m \end{cases}$$

$$\begin{matrix} [a]_n = [b]_n \\ [a]_m = [b]_m \end{matrix} \Rightarrow [a]_{mn} = [b]_{mn}$$

$$\begin{matrix} a \equiv b(n) \\ a \equiv b(m) \end{matrix} \Rightarrow a \equiv b(mn)$$

Определение

$$\varphi : G \to H\ \text{-}\ \textit{гомоморфизм}$$

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

изоморфизм = гомоморфизм + биективность

$$\varphi \in Hom(G, H)\ \text{-}\ \textit{множество гомоморфизмов}$$

Примеры

$$1) \quad \mathbb{C}^* \to \mathbb{R}^*$$

$$z \to |z|$$

$$2) \quad GL_n(K) \to K^*$$

$$A \to \det A$$

$$3) \quad S_n \to \{\pm 1\}$$

$$\sigma \to \begin{cases} +1, & \textit{если}\ \sigma\ \text{-}\ \textit{четн.} \\ -1, & \textit{если}\ \sigma\ \text{-}\ \textit{неч.} \end{cases}$$

$$4) \quad a \in G \quad G \to G$$

$$g \to a^{-1} g a$$

$$(a^{-1} g a)(a^{-1} g_1 a) = a^{-1} g_g 1 a$$