Содержание

1 Теория групп

2019-09-17

Опр

G - *мн-во*, $*: G * G \to G,\ (g_1, g_2) \to (g_1 * g_2)\ (g_1 g_2)$

1. $(g_1 g_2) g_3 = g_1 (g_2 g_3) \quad \forall g_1, g_2, g_3 \in G$
2. $\exists e \in G : eg = ge = g \quad \forall g \in G$
3. $\forall g \in G \quad \exists \widetilde{g} \in G : g\widetilde{g} = g\widetilde{g} = e$
4. $g_1 g_2 = g_2 g_1 \quad \forall g_1, g_2 \in G$

Примеры

1. $(\mathbb{Z}, +)$ - *группа*
2. $(\mathbb{Z}, \bullet)$ - *не группа*
3. $(R, +)$ - *группа кольца*
4. $(R^*, \bullet)$
5. *Группа самосовмещения* D_n, *например* D_4 - *квадрат, композиция - группа,* $|D_n| = 2n$
6. $GL_n(K) = \{A \in M_n(K) : |A| \neq 0\}$, *умножение - группа*
7. $\mathbb{Z}n\mathbb{Z}$ - *частный случай п.3,4*

Теор (простейшие св-ва групп)

1. e - *единственный,* e, e' - *нейтральные:* $e = ee' = e'$
2. $\widetilde{g}$ - *единственный*

   Пусть $\widetilde{g}, \hat{g}$ - *обратные, тогда* $\widetilde{g}g = g\widetilde{g} = e = \hat{g}g = g\hat{g}$

   $\hat{g} = e\hat{g} = (\widetilde{g}g)\hat{g} = \widetilde{g}(g\hat{g}) = \widetilde{g}e = \widetilde{g}$
3. $(ab)^{-1} = b^{-1}a^{-1}$

   Это верно, если $(ab)(b^{-1}a^{-1}) = (b^{-1}a^{-1})(ab) = e$, *докажем первое:*

   $(ab)(b^{-1}a^{-1}) = ((ab)b^{-1})a^{-1} = (a(bb^{-1}))a^{-1} = (ae)a^{-1} = aa^{-1} = e$
4. $(g^{-1})^{-1} = g$

Опр

$g \in G \quad n \in \mathbb{Z}$, *тогда* $g = \left[\begin{array}{l} \overbrace{g...g}^{n}, \quad n > 0 \\ e, \quad n = 0 \\ \underbrace{g^{-1}...g^{-1}}_{n}, \quad n < 0 \end{array}\right.$

Теор (св-ва)

1. $g^{n+m} = g^n g^m$
2. $(g^n)^m = g^{nm}$

Опр

$g \in G$, $n \in N$ - *порядок* g ($ord g = n$), *если:*

1. $g^n = e$
2. $g^m = e \to m \geqslant n$

Примеры

1. D_4 *ord(поворот* $90°) = 4$

   D_4 *ord(поворот* $180°) = 2$
2. $(\mathbb{Z}/6\mathbb{Z}, +)$ $ord(\overline{1}) = 6$

   $ord(\overline{2}) = 3$

Утв

$g^m = e \quad ord(g) = n \to m \,\vdots\, n$ *(n>0)*

Док-во

$m = nq + r$, $0 \leqslant r < n$ $e = g^m = g^{nq+r} = (g^n)^q g^r = g^r \to r = 0$

Опр

$H \subset G$ *называется подгруппой* G $(H < G)$ *(и сама является группой), если:*

1. $g_1, g_2 \in H \to g_1 g_2 \in H$
2. $e \in H$
3. $g \in H \to g^{-1} \in H$

Примеры

1. $n\mathbb{Z} < \mathbb{Z}$
2. D_4

3. $SL_n(K) = \{A \in M_n(K) : \quad |A| = 1\}$, $SL_n(K) < GL_n(K)$

Мультипликативная запись	Аддитивная запись
$g_1 g_2$	$g_1 + g_2$
e	0
g^{-1}	$-g$
g^n	ng

Опр

$H < G$, $g_1, g_2 \in G$, тогда $g_1 \sim g_2$, если:

1. $g_1 = g_2 h$, $h \in H$ *(левое)*

2. $g_2 = h g_1$, $h \in H$ *(правое)*

Док-во (эквивалентность)

1. *(симметричность)* $g_1 = g_2 h \overset{*h^{-1}}{\to} g_2 = g_1 h^{-1}$

2. *(рефлексивность)* $g = ge$

3. *(транзитивнось)* $g_1 = g_2 h$, $g_2 = g_3 h \to g_1 = g_3(h_2 h_1)$, *где* $h_2 h_1 \in H$

Опр

$[a] = \{b : ab\}$*классы эквивалентности*

Опр

$[g] = gH = \{gh, h \in H\}$ *(левый класс смежности)*

$gh \sim g \to gh \in [g]$

$g_1 \in [g] \to g_1 \sim g \to g_1 = gh$

Утв

$[e] = H$

Установим биекцию:

$[g] = gh \leftarrow H$

$gh \leftarrow h$

Очевидно, сюрьекция, почему иньекция? $gh_1 = gh_2 \overset{*g^{-1}}{\to} h_1 = h$

Теор (Лагранжа)

$H < G$, $|G| < \infty$, *тогда* $|G| \vdots |H|$ *(уже доказали!)*

2019-09-10

След (теорема Эйлера)

Напоминание

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

Док-во

Рассмотрим $G = (\mathbb{Z}/n\mathbb{Z})* \ |G| = \varphi(n)$
$\overline{a} \in G$, $ord\overline{a} = k$
$\varphi(n) \vdots k \Rightarrow \varphi(n) = kl$
$\overline{a} = \overline{1}$
$\overline{a}^{\varphi(n)} = \overline{1}$

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)*

Замеч

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 $(g, h) * (g', h') \overset{def}{=} (g *_G g', h *_H h')$
Докажем, что это группа.
Доказательство ассоциативности: $((g, h)(g', h'))(g'', h'') \overset{?}{=} (g, h)((g', h')(g'', h'')$
$(gg', hh')(g'', h'') \overset{?}{=} (g, h)(g'g'', h'h'')$
$((gg')g'', (hh')h'') \overset{?}{=} (g(g', g''), h(h'h'')$ - очевидно
Нейтральный элемент:
Рассмотрим $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1})\}$

Опр

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

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

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* φ *- изоморфизм*

Примеры

1. $D_3 \to S_3$

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

Опр

Две группы называются изоморфными, если между ними существует изоморфизм

Утв

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: $G \underset{\varphi}{\to} H$, $H \underset{\varphi^{-1}}{\to} G$

Теор

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

Утв

$|G| = p$, *простое*

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

$ord\ g = p$

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

Утв

H, G - *группы*, $\quad g \in G$

$\varphi : G \to H$ - *изоморфизм*

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

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

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

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

$m \in \mathbb{N}$

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

Опр

$H < G$

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

$H \lhd G$

Утв

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

$\forall g \quad gH = Hg$

Док-во

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

$gh = \underbrace{(g^{-1})^{-1}hg^{-1}}_{\in H}g = h_1g$

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

$g^{-1}hg = h_1$

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

$H \lhd G$

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

$\widetilde{g_1}H = g_1H$

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

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

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

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

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

$eH = H$

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

$$K(G) < G$$

$$[e,e] = e$$
$$[g_1,h_1]...[g_n,h_n]$$
$$[g,h]^{-1} = (ghg^{-1}h^{-1})^{-1} = hgh^{-1}g^{-1} = [h,g]$$
$$([g_1,h_1]...[g_n,h_n])^{-1} = [h_1,g_1]...[g_n,h_n]$$
$$g^{-1}[g_1,h_1]...[g_n,h_n]g =$$
$$= (g^{-1}[g_1,h_1]g)(g^{-1}[g_2,h_2]g)...(g^{-1}[g_n,h_n]g)$$
$$g^{-1}g_1h_1g_1^{-1}h_1^{-1}g =$$
$$= (g^{-1}g_1h_1g_1^{-1}(gh_1^{-1})h_1g^{-1})h_1^{-1}g$$
$$[g^{-1}g_1,h_1] \qquad [h_1,g^{-1}]$$

Утв

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

Док-во

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

$$g_1g_2K(G) = g_1g_2K(G) \qquad g_2K(G)g_1K(G) = g_2g_1K(G)$$
$$[g_1,g_2] = g_1g_2(g_2g_1)^{-1} \in K(G)$$

Утв

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

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

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

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

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

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

Опр

$\varphi : G \to H$ - *гомоморфизм*

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

изоморфизм = гомоморфизм + биективность

$\varphi \in Hom(G, H)$ - *множество гомоморфизмов*

Примеры

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

$$z \to |z|$$

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

$$A \to \det A$$

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

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

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

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

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