# 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

**Теорема (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. $(g^{-1})^{-1} = g$

**<u>Опр</u>**

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

**<u>Теорема</u> (св-ва)**

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

**<u>Опр</u>**

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

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

**<u>Примеры</u>**

1. $D_4$ ord(поворот $90°$) $= 4$

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

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

**<u>Утв</u>**

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

**<u>Док-во</u>**

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

**<u>Опр</u>**

$H \subset G$ 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. $g \in H \to g^{-1} \in H$

**<u>Примеры</u>**

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, сюръекция, почему инъекция? $gh_1 = gh_2 \overset{*g^{-1}}{\to} h_1 = h$

**Теорема (Лагранжа)**

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

2019-09-10

**Следствие (теорема Эйлера)**

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

**Док-во**

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

**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 - коммунитативна

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

**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**

$\varphi : G \to H$ - 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. $D_3 \to S_3$
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: $G \underset{\varphi}{\to} H$, $H \underset{\varphi^{-1}}{\to} G$

**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 $\varphi(g^k g^l) = \varphi(g^k) + \varphi(g^l) = \overline{k} + \overline{l}$

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

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

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

$m \in \mathbb{N}$

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

**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**

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

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

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

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

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

$$H \lhd G$$

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

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

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

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

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

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

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

$$eH = H$$

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

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

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

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

$$G_{/H}$$

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

$$G = \mathbb{Z}$$

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

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

**Пример**

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

$g, h \in G$

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

$G_{/K(G)}$ - 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**

$\mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}_{mn}$, 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

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

**Примеры**

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

$z \to |z|$

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

$A \to \det A$

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

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

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

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

$(a^{-1}ga)(a^{-1}g_1a) = a^{-1}g_g1a$

../../../template/template
2019-09-24

**Напоминание**

$$G/K(G) \text{ - коммутативна}$$

**Утв**

$$H \triangleleft G \quad G/_H \text{ - комм}$$

$$\forall g_1, g_2 \in G \quad (g_1H)(g_2H) = (g_2H)(g_1H)$$
$$[g_1, g_2] = g_1^{-1}g_2^{-1}g_1g_2 \in H \Rightarrow K(G) \subset H$$

**Свойства (гомоморфизма)**

$$f \in \operatorname{Hom}(G, H)$$

1. $f(e_G) = e_H \qquad f(e) = f(e \cdot e) = f(e) \cdot f(e)$
2. $f(a^{-1}) = f(a)^{-1}$

$$f(a)f(a^{-1}) = f(aa^{-1}) = f(e) = e$$

3. Композиция гомоморфизмов

**Опр**

$$f \in \operatorname{Hom}(G, H)$$

$$Kerf = \{g \in G : \ f(g) = e\} \subset G$$
$$\operatorname{Im} f = \{f(g) : \ g \in G\} \subset H$$

**Утв**

$Ker$ и Im - подгруппы G

**Док-во**

1. $f(g_1) = f(g_2) = e \Rightarrow f(g_1g_2) = f(g_1)f(g_2) = e \cdot e = e$
2. $f(e) = e$
3. $f(g) = e \Rightarrow f(g^{-1}) = f(g)^{-1} = e^{-1} = e$

1. $f(g_1) \cdot f(g_2) = f(g_1g_2)$

2. $e = f(e)$

3. $f(g)^{-1} = f(g^{-1})$

**<u>Утв</u>**

$Ker$ - нормальная подгруппа G

**<u>Док-во</u>**

$$Kerf \triangleleft G?$$

$$g \in G \qquad a \in Kerf$$

$$f(g^{-1}ag) = f(g)^{-1} \underbrace{f(a)}_{=e} f(g) = e$$

**<u>Утв</u> (основная теорема о гомоморфизме)**

$$G/_{Kerf} \cong \operatorname{Im} f$$

**<u>Док-во</u>**

$$Kerf = K$$

$$\varphi(gK) \stackrel{def}{=} f(g) \qquad \varphi : G/_{Kerf} \to \operatorname{Im} f$$

$$gK = g'K \stackrel{?}{\Rightarrow} f(g) = f(g')$$

$$g' = g \cdot a, \quad a \in K \qquad f(g') = f(g) \cdot \underbrace{f(a)}_{=e} = f(g)$$

$$f(g_1)f(g_2) = \varphi(g_1K)\varphi(g_2K) \stackrel{?}{=} \varphi(g_1Kg_2K) = \varphi((g_1g_2)K) = f(g_1g_2)$$

$$\varphi(g_1K) = \varphi(g_2K) \stackrel{?}{\Rightarrow} g_1K = g_2K$$

$$f(g_1) = f(g_2) \qquad \Rightarrow g_1g_2^{-1} \in K$$

$$\underbrace{f(g1)f(g_2)^{-1}}_{=f(g_1)f(g_2^{-1})} = e$$

**<u>Напоминание</u>**

$SL_N(K)$ - квадратные матрицы с $\det = 1$

**Опр**

$$\det : GL_n(K) \to K^*$$

$$GL_n(K)/_{SL_n(K)} \cong K^*$$

$$SL_n(K) = \{A \in M_n(K) : |A| = 1\}$$

**Пример (1)**

$$S_n \to \{\pm 1\}$$

$$S_n/_{A_n} \cong \{\pm 1\}(\cong \mathbb{Z}/_{2\mathbb{Z}})$$

**Пример (2)**

$$G \times H \to G$$

$$(g_1 h) \to g$$

$$G \times H/_{e \times H} \cong G$$

## 1.1 Действие группы на множестве

**Опр**

$M$ - множество

$G$ - группа

$$G \times M \to M$$

$$(g, m) \to gm$$

1. $g_1(g_2 m) = (g_1 g_2)m \quad \forall g_1 g_2 \in G, \quad m \in M$
2. $em = m \quad \forall m \in M$

**Пример (1)**

$$A = k^n \qquad (A, v) \to A_v$$

$$G = GL_n(K)$$

$$A(B_v) = (AB)_v$$

$$E_v = v$$

**Пример (2)**

M = {количество раскрасок вершин квадрата в два цвета}

$$G = D_4$$

$$\cdot \begin{matrix} ч & ч \\ б & ч \end{matrix} = \begin{matrix} ч & б \\ ч & ч \end{matrix}$$

$$M = G$$

$$gm = gm$$

**Опр**

$$m \in M$$

$Stab\ m = \{g \in G : gm = m\}$ - стабилизация

$Orb\ m = \{gm,\ g \in G\}$ - орбита

**Утв**

$$Stab\ m < G$$

**Док-во**

1. $g_1, g_2 \in Stab\ m$

$$(g_1 g_2)m = g_1(\underbrace{g_2 m}_{=m}) = g_1 m = m$$

2. $e \cdot m = m$

3. $gm = m \overset{?}{\Rightarrow} g^{-1}m = m$

$$gm = m$$

$$\underbrace{g^{-1}gm}_{=(g^{-1}g)m=em=m} = g^{-1}m$$

**Утв**

$$m_1, m_2 \in M$$

$m_1 \sim m_2$, если $\exists g \in G : gm_1 = m_2$

$\Rightarrow \sim$ - отношение эквив

**Док-во**

$$gm_1 = m_2 \Rightarrow g^{-1}m_2 = m_1 \quad g^{-1} \in G$$

$$em = m, \quad e \in G$$

$$\left.\begin{matrix} gm_1 = m_2 \\ g'm_2 = m_3 \end{matrix}\right| \Rightarrow (g'g)m_1 = g'(gm_1) = g'm_2 = m_3$$

**Утв**

$$|Orb\ m| \cdot |Stab\ m| = |G|$$

**Док-во**

$$Stab\ m = H$$

$$\{gH,\ g \in G\} \to Orb\ m$$

$$gH \to gm$$

Хотим доказать, что это корректно

$$gH = g'H \overset{?}{\Rightarrow} gm = g'm$$

$$g' = ga, \quad g \in H$$

$$g'm = (ga)m = g(am) = gm$$

Хотим доказать биективность. Сюръективность - очев. Инъективность:

$$gm = g'm \Rightarrow gH = g'H$$

$$m = em = (g^{-1}g')m = g^{-1}(gm) = g^{-1}(g'm) = (g^{-1}g')m$$

$$\Rightarrow g^{-1}g' \in H \Rightarrow gH = g'H$$

**Лемма (Бернсайда)**

$$\text{Кол-во орбит } = \frac{1}{|G|}\sum_{g \in G} |M^g|$$

$$M^g = \{m \in M : gm = m\}$$