

# Содержание

<b>1</b>	<b>Теория групп</b>	<b>2</b>
	Простейшие св-ва групп . . . . .	2
	Теорема Лагранжа . . . . .	4
	Циклическая группа . . . . .	5
	Изоморфные группы . . . . .	6
	Нормальная подгруппа . . . . .	8
	Гомоморфизм . . . . .	11
	1.1 Действие группы на множестве . . . . .	14
<b>2</b>	<b>Евклидовы и унитарные пр-ва</b>	<b>17</b>

# 1 Теория групп

2019-09-17

## Опр

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

$$1. (g_1 g_2) g_3 = g_1 (g_2 g_3) \quad \forall g_1, g_2, g_3 \in G$$

$$2. \exists e \in G : eg = ge = g \quad \forall g \in G$$

$$3. \forall g \in G \quad \exists \tilde{g} \in G : g\tilde{g} = g\tilde{g} = e$$

$$4. g_1 g_2 = g_2 g_1 \quad \forall g_1, g_2 \in G$$

## Примеры

$$1. (\mathbb{Z}, +) - \text{группа}$$

$$2. (\mathbb{Z}, \bullet) - \text{не группа}$$

$$3. (R, +) - \text{группа кольца}$$

$$4. (R^*, \bullet)$$

$$5. \text{Группа самосовмещения } D_n, \text{ например } D_4 - \text{квадрат, композиция} \\ - \text{группа, } |D_n| = 2n$$

$$6. GL_n(K) = \{A \in M_n(K) : |A| \neq 0\}, \text{ умножение} - \text{группа}$$

$$7. \mathbb{Z}n\mathbb{Z} - \text{частный случай п.3,4}$$

## Теорема (простейшие св-ва групп)

$$1. e - \text{единственный, } e, e' - \text{нейтральные: } e = ee' = e'$$

$$2. \tilde{g} - \text{единственный}$$

$$\text{Пусть } \tilde{g}, \hat{g} - \text{обратные, тогда } \tilde{g}g = g\tilde{g} = e = \hat{g}g = g\hat{g}$$

$$\hat{g} = e\hat{g} = (\tilde{g}g)\hat{g} = \tilde{g}(g\hat{g}) = \tilde{g}e = \tilde{g}$$

$$3. (ab)^{-1} = b^{-1}a^{-1}$$

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

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

$$4. (g^{-1})^{-1} = g$$

Опр

$$g \in G \quad n \in \mathbb{Z}, \text{ тогда } g = \begin{cases} \overbrace{g \dots g}^n, & n > 0 \\ e, & n = 0 \\ \underbrace{g^{-1} \dots g^{-1}}_n, & n < 0 \end{cases}$$

Теорема (св-ва)

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

Опр

$g \in G, n \in \mathbb{N}$  - порядок  $g$  ( $\text{ord} g = n$ ), если:

1.  $g^n = e$
2.  $g^m = e \rightarrow m \geq n$

Примеры

1.  $D_4 \text{ ord(поворот } 90^\circ) = 4$   
 $D_4 \text{ ord(поворот } 180^\circ) = 2$
2.  $(\mathbb{Z}/6\mathbb{Z}, +) \text{ ord}(\bar{1}) = 6$   
 $\text{ord}(\bar{2}) = 3$

Утв

$$g^m = e \quad \text{ord}(g) = n \rightarrow m : n \quad (n > 0)$$

Док-во

$$m = nq + r, 0 \leq r < n \quad e = g^m = g^{nq+r} = (g^n)^q g^r = g^r \rightarrow r = 0$$

Опр

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

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

Примеры

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

2.  $D_4$ 3.  $SL_n(K) = \{A \in M_n(K) : |A| = 1\}, SL_n(K) < GL_n(K)$ 

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)  $g_1 = g_2 h \xrightarrow{*h^{-1}} g_2 = g_1 h^{-1}$
2. (рефлексивность)  $g = ge$
3. (транзитивность)  $g_1 = g_2 h, g_2 = g_3 h \rightarrow g_1 = g_3(h_2 h_1)$ , где  $h_2 h_1 \in H$

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

$[g] = gH = \{gh, h \in H\}$  (левый класс смежности)  
 $gh \sim g \rightarrow gh \in [g]$   
 $g_1 \in [g] \rightarrow g_1 \sim g \rightarrow g_1 = gh$

**Утв** $[e] = H$ 

Установим биекцию:

$[g] = gh \leftarrow H$   
 $gh \leftarrow h$

Очевидно, сюръекция, почему инъекция?  $gh_1 = gh_2 \xrightarrow{*g^{-1}} h_1 = h_2$ **Теорема (Лагранжа)** $H < G, |G| < \infty$ , тогда  $|G| : |H|$  (уже доказали!)

2019-09-10

Следствие (теорема Эйлера)

Напоминание

 $n, a \in \mathbb{N}, (a, n) = 1$ , тогда  $a^{\varphi(n)} \equiv 1 \pmod{n}$ Док-воРассмотрим  $G = (\mathbb{Z}/n\mathbb{Z})^*$   $|G| = \varphi(n)$  $\bar{a} \in G, \text{ord } \bar{a} = k$  $\varphi(n) : k \Rightarrow \varphi(n) = kl$  $\bar{a} = \bar{1}$  $\bar{a}^{\varphi(n)} = \bar{1}$ Опр $G$  - циклическая группа, если  $\exists g \in G : \forall g' \in G : \exists k \in \mathbb{Z} : g' = g^k$ Такой  $g$  называется образующимОпр $\mathbb{Z}$  (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  $(g, h) * (g', h') \stackrel{\text{def}}{=} (g *_G g', h *_H h')$ 

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  $\Leftrightarrow \exists g \in G : \text{ord } g = n$ )

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

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

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

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

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

### Опр

Две группы называются изоморфными, если между ними существует изоморфизм

### Утв

Изоморфизм - отношение эквивалентности

### Док-во

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

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

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)  $G = \{..., g^{-1}, e, g, g^2, ...\}$  (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 заикликивается через каждые  $k-l$  элементов), построим отображение в  $\mathbb{Z}$ .

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

2019-09-17

УТВ

$$|G| = p, \text{ простое}$$

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

$$\text{ord } g = p$$

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

УТВ

$$H, G - \text{ группы, } g \in G$$

$$\varphi : G \rightarrow H - \text{ изоморфизм}$$

$$\Rightarrow \text{ord } g = \text{ord } \varphi(g)$$

$$\text{ord } g = n \quad g^n = e$$

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

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

$$m \in \mathbb{N}$$

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

Опр

$$H < G$$

$$H - \text{ нормальная подгруппа, если } \forall h \in H, g \in G$$

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

рисунок 1

$$H \triangleleft G$$

УТВ

$$H \triangleleft G \Leftrightarrow - \text{ разбиение на л. и п. классы смежности по } H \text{ совпадают}$$

$$\forall g \quad gH = Hg$$



Док-во

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

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

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

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

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

$$H \triangleleft G$$

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

$$\tilde{g}_1H = g_1H$$

$$\tilde{g}_2H = g_2H \stackrel{?}{\Rightarrow} \tilde{g}_1\tilde{g}_2H = g_1g_2H$$

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

$$\tilde{g}_1\tilde{g}_2h = g_1h_1g_2h_2h = g_1g_2(\underbrace{g_2^{-1}h_1g_2}_{=h_3})h_2h$$

$$\tilde{g}_1H = g_1H \Rightarrow \tilde{g}_1 = g_1h_1$$

$$\tilde{g}_2H = g_2H \Rightarrow \tilde{g}_2 = g_2h_2$$

$$eH = H$$

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

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

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

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

$$G/H$$

$$a \sim b \Leftrightarrow a - b \in H$$

$$G = \mathbb{Z}$$

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

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

Пример

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

$g, h \in G$

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

Док-во

Коммутант - подгруппа

$$K(G) < G$$

$$[e, e] = e$$

$$[g_1, h_1] \dots [g_n, h_n]$$

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

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

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

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

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

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

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

УТВ

$$G/K(G) \text{ - КОММ}$$

Док-во

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

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

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

УТВ

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

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

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

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

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

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

Опр

$\varphi : G \rightarrow H$  - гомоморфизм

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

изоморфизм = гомоморфизм + биективность

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

Примеры

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

$$z \rightarrow |z|$$

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

$$A \rightarrow \det A$$

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

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

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

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

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

../../template/template

2019-09-24

### Напоминание

$G/K(G)$  - коммутативна

### УТВ

$H \triangleleft G \quad G/H$  - комм

$$\forall g_1, g_2 \in G \quad (g_1 H)(g_2 H) = (g_2 H)(g_1 H)$$

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

### Свойства (гомоморфизма)

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

$$1. f(e_G) = e_H \quad f(e) = f(e \cdot e) = f(e) \cdot f(e)$$

$$2. f(a^{-1}) = f(a)^{-1}$$

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

3. Композиция гомоморфизмов

### Опр

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

$$\text{Ker } f = \{g \in G : f(g) = e\} \subset G$$

$$\text{Im } f = \{f(g) : g \in G\} \subset H$$

### УТВ

$\text{Ker}$  и  $\text{Im}$  - подгруппы  $G$

### Док-во

$$1. f(g_1) = f(g_2) = e \Rightarrow f(g_1 g_2) = f(g_1) f(g_2) = e \cdot e = e$$

$$2. f(e) = e$$

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

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

$$2. e = f(e)$$

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

УТВ

$Ker$  - нормальная подгруппа  $G$

Док-во

$$Ker f \triangleleft G?$$

$$g \in G \quad a \in Ker f$$

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

УТВ (основная теорема о гомоморфизме)

$$G/Ker f \cong Im f$$

Док-во

Докажем, что это корректное отображение:

$$Ker f = K$$

$$\varphi(gK) \stackrel{def}{=} f(g) \quad \varphi : G/Ker f \rightarrow Im f$$

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

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

Докажем, что  $\varphi$  - гомоморфизм:

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

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

Докажем, что это биекция. Что сюръекция - очевидно

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

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

Напоминание

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

Опр

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

Но это отображение - сюръекция, а значит:

$$GL_n(K)/SL_n(K) \cong K^*$$

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

Пример (1)

$$S_n \rightarrow \{\pm 1\}$$

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

Пример (2)

$$G \times H \rightarrow G$$

$$(g_1 h) \rightarrow g$$

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

**1.1 Действие группы на множестве**Опр

$M$  - множество

$G$  - группа

$$G \times M \rightarrow M$$

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

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

$$2. \ em = m \quad \forall m \in M$$

Если задано такое отображение, то говорим, что группа  $G$  действует на множестве  $M$

Пример (1)

$$A = k^n \quad (A, v) \rightarrow A_v$$

$$G = GL_n(K)$$

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

$$E_v = v$$

Пример (2)

$M = \{\text{количество раскрасок вершин квадрата в два цвета}\}$

$$G = D_4$$

$$\begin{array}{cccc} \cdot & \text{ч} & \text{ч} & \text{б} \\ \text{б} & \text{ч} & \text{ч} & \text{ч} \end{array} =$$

$$M = G$$

$$gm = gm$$

Опр

$$m \in M$$

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

$$\text{Orb } m = \{gm, g \in G\} - \text{орбита}$$

УТВ

$$\text{Stab } m < G$$

Док-во

Доказательство того, что стабилизатор - подгруппа:

$$1. \quad g_1, g_2 \in \text{Stab } m$$

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

$$2. \quad e \cdot m = m$$

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

$$gm = m$$

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

УТВ

$$m_1, m_2 \in M$$

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

$\Rightarrow \sim$  - отношение эквив

Док-во

$$(\text{рефл.}) \quad gm_1 = m_2 \Rightarrow g^{-1}m_2 = m_1 \quad g^{-1} \in G$$

$$(\text{симм.}) \quad em = m, \quad e \in G$$

$$(\text{тран.}) \quad \left. \begin{array}{l} gm_1 = m_2 \\ g'm_2 = m_3 \end{array} \right| \Rightarrow (g'g)m_1 = g'(gm_1) = g'm_2 = m_3$$

УТВ

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

Док-во

$$Stab \ m = H$$

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

$$gH \rightarrow gm$$

Хотим доказать, что это корректно

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

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

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

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 (Бернсайд)

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

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



../../template/template

2019-10-01

### Напоминание

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

$$M^g = \{m \in M : gm = m^2\}$$

### Док-во

$$\begin{aligned} \sum_{g \in G} |M^g| &= |\{(g, m) \in G \times M : gm = m\}| = \\ &= \sum_{m \in M} |\text{Stab } m| = |G| \sum_{m \in M} \frac{1}{|\text{Orb } m|} = |G| \cdot \text{Кол-во орбит} \end{aligned}$$

## 2 Евклидовы и унитарные пр-ва

### Опр

$V$  - в.п. над  $\mathbb{R}$

Введем отображение

$$V \times V \rightarrow \mathbb{R}$$

$$(u, v)$$

Свойства этого отображения

1. Симметричность

$$(u, v) = (v, u) \quad \forall u, v \in V$$

2. Линейность

$$(\lambda u, v) = \lambda(u, v) \quad \lambda \in \mathbb{R} \quad u, v \in V$$

$$(u + u', v) = (u, v) + (u', v) \quad u, u', v \in V$$

3.  $(u, v) \geq 0 \quad \forall u \in V$

$$(u, u) = 0 \Leftrightarrow u = 0$$

Такое пр-во  $V$  с введенным на нем таким отображением мы называем Евклидовым пр-вом, а отображение скалярным.

### Напоминание

$C = \{c_{ij}\}_{i,j=1}^n$  - квадр. матрица

$$Tr C = \sum_{i=1}^n c_{ii} \text{ - след (Trace)}$$

(Сумма элементов главной диагонали)

### Примеры

1. Школьные вектора

2.  $\mathbb{R}^n$

$$((a_1, \dots, a_n), (b_1, \dots, b_n)) = \sum_{i=1}^n a_i b_i$$

3.  $V = \mathbb{R}[x]_n$  конечномерное пр-во

$$(f, g) = \int_a^b f g dx$$

4.  $V = M_n(\mathbb{R})$

$$(A, B) = Tr AB^T$$

(См. след в напоминании)

### Опр

$e = \{e_1, \dots, e_n\}$  - базис  $V$

$$a_{ij} = (e_i, e_j)$$

$\Gamma_e = \{a_{ij}\}_{i,j=1}^n$  - матрица Грама

### Свойства (матрицы Грама)

1. Матрица невырожд

2.  $e, f$  - базисы

$$\Gamma_f = M_{e \rightarrow f}^T \Gamma_e M_{e \rightarrow f}$$

$$3. \Gamma_e = \{a_{ij}\}$$

$$u = \sum \lambda_i e_i$$

$$v = \sum \mu_j e_j$$

$$(u, v) = \left( \sum \lambda_i e_i, \sum \mu_j e_j \right) = \sum_{i,j} \lambda_i \mu_j (e_i, e_j)$$

$$(u, v) = [u]_e^T \Gamma_e [v]_e$$

### Док-во

$$1. \quad \neg |\Gamma_e| = 0 \Rightarrow \exists \lambda_i \in \mathbb{R} \text{ не все } 0 :$$

$$\sum \lambda_i (e_i, e_j) = 0 \quad \forall j$$

$$\left( \sum \lambda_i e_i, e_j \right) = 0 \quad \forall j$$

$$\left( \sum_i \lambda_i e_i, \sum_j \lambda_j e_j \right) = 0 \Leftrightarrow \sum \lambda_i e_i = 0$$

противоречие

$$2. \quad \neg M_{e \rightarrow f} = \{a_{ik}\} \quad f_k = \sum a_{ik} e_i$$

$$f_l = \sum a_{jl} e_j$$

$$(f_k, f_l) = \sum_{i,j} a_{ik} a_{jl} (e_i, e_j)$$

$$a_{ik} (e_i, e_j) a_{jl}$$

$$\text{Напоминание: } X, Y - \text{матр} \quad X \times Y = Z \quad z_{ij} = \sum x_{is} y_{sj}$$

### Опр

$V$  - в.п. над  $\mathbb{R}$

$$V \rightarrow \mathbb{R}_{\geq 0}$$

$v \rightarrow \|v\|$  - норма

$$1. \quad \|\lambda v\| = |\lambda| \|v\| \quad \forall \lambda \in \mathbb{R} \quad v \in V$$

2. Нер-во треугольника

$$\|u + v\| \leq \|u\| + \|v\|$$

$$3. \|u\| = 0 \Leftrightarrow u = 0$$

Если такое отображ. существует, то оно называется нормой

### УТВ

$(u, v)$  - ск. пр-ве

$$\Rightarrow \|u\| = \sqrt{(u, u)}$$

### Пример

$\mathbb{R}^n$

$$\|x\| = \max |x_i|$$

$$\|x\| = \sum_i |x_i|$$

### Теорема (Нер-во Коши - Буняковского)

$$|(u, v)| \leq \|u\| \cdot \|v\|$$

### Док-во

$$\varphi(t) = \|u + tv\|^2 = (u + tv, u + tv) = \|u\|^2 + 2(u, v)t + t^2\|v\|^2$$

$$D = 4(u, v)^2 - 4\|u\|^2\|v\|^2 \leq 0$$

$$\|u + v\| \leq \|u\| + \|v\|$$

$$(u + v, u + v) \leq \|u\|^2 + \|v\|^2 + 2\|u\|\|v\|$$

$$(u + v, u + v) = \|u\|^2 + \|v\|^2 + 2(u, v)$$

$$2(u, v) \leq 2\|u\|\|v\|$$

### УТВ (Теорема Пифагора)

$$\text{Если } u \perp v \Rightarrow \|u + v\|^2 = \|u\|^2 + \|v\|^2$$

### Док-во

$$\|u + v\|^2 = \|u\|^2 + \|v\|^2 + 2(u, v)$$

Опр (Ортогональное дополнение)

$V$  - евкл. пр-во

$$U \subset V \quad U^\perp = \{v \in V : (v, u) = 0 \quad \forall u \in U\}$$

Множество всех векторов, которые ортогональны всем векторам из  $U$

Такое мн-во называется ортогональным дополнением

УТВ

$U^\perp$  - под-пр  $V$

Док-во

$$\begin{aligned} (v, u) = 0 \quad \forall u \\ (v', u) = 0 \quad \forall u \end{aligned} \Rightarrow (v + v', u) = 0 \quad \forall u$$

$$(v, u) = 0 \quad \forall u$$

$$\lambda \in \mathbb{R}$$

$$(\lambda v, u) = 0 \quad \forall u$$

Тогда  $U^\perp$  дей-во линейное под-прво  $V$

Свойства

$$V = U \oplus U^\perp$$

$$u \in U \cap U^\perp$$

$$u \in U \quad u \in U^\perp$$

$$(u, u) = 0$$

Док-во

$e_1, \dots, e_n$  - базис  $U$  дополняем до базиса  $V$

$e_1, \dots, e_n, f_1, \dots, f_n$  - базис  $V$

$$v \in U^\perp \quad v = \sum \lambda_i e_i + \sum \mu_j f_j$$

$$v \in U^\perp \Leftrightarrow (v, e_k) = 0 \quad \forall 1 \leq k \leq n$$

$$(v, e_k) = \sum \lambda_i (e_i, e_k) + \sum \mu_j (f_j, e_k) = 0 \quad \forall 1 \leq k \leq n$$

это матрица

$$\frac{\begin{array}{c|c|c} & \mathfrak{n} & \mathfrak{m} \\ \hline \mathfrak{n} & \Gamma_e & C \end{array}}{\begin{array}{c|c|c} & \mathfrak{n} & \mathfrak{m} \\ \hline \mathfrak{n} & \Gamma_e & C \end{array}} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$$\Gamma_e x + C_y = 0$$

$\{(x, y) \in \mathbb{R}^n \times \mathbb{R}^m : \Gamma_e x + C_y = 0\}$  - размерность этого  $m$

$$(x, y) \rightarrow y$$

$$\Gamma_e x + C_y = 0$$

$$x = -\Gamma_e^{-1} e_y$$

$$\dim U + \dim U^\perp = \dim V$$

../../template/template

2019-10-15

### Свойство

$$(U^\perp)^\perp = U$$

### Док-во

$$\left. \begin{array}{l} \dim U^\perp + \dim U = \dim V \\ \dim(U^\perp)^\perp + \dim U^\perp = \dim V \end{array} \right| \Rightarrow \dim(U^\perp)^\perp = \dim U$$

$$U \subset (U^\perp)^\perp$$

$$(U^\perp)^\perp = \{v \in V\}$$

### Опр

$$U < V, \quad v \in V$$

$$U \oplus U^\perp = V$$

$$\Rightarrow \exists! u \in U, w \in U^\perp : v = u + w$$

и называется ортогональной проекцией

$$\text{Обозначение: } \operatorname{pr}_U v \stackrel{\text{def}}{=} u$$

$$v = \operatorname{pr}_U v + w \Rightarrow (v, u) = (\operatorname{pr}_U v, u)$$

### Свойства (орт. проекции)

$$1. \operatorname{pr}_U(v + v') = \operatorname{pr}_U v + \operatorname{pr}_U v'$$

$$v = u + w, \quad u \in U, w \in U^\perp$$

$$v' = u' + w', \quad u \in U, w' \in U^\perp$$

$$v + v' = \underbrace{(u + u')}_{\in U} + \underbrace{(w + w')}_{\in U^\perp}$$

$$2. \|v - \operatorname{pr}_U v\| \leq \|v - u\| \quad \forall u \in U$$

$$\|v - u\|^2 = \|v - \underbrace{\operatorname{pr}_U v}_{\in U^\perp}\|^2 + \|\underbrace{\operatorname{pr}_U v - u}_{\in U}\|^2$$

## Опр

$e_1, \dots, e_n$  - базис  $V$

Базис называется ортогональным, если  $(e_i, e_j) = 0 \quad \forall i \neq j$  - ортогональный базис

$$(e_i, e_j) = \delta_{i,j} = \begin{cases} 0, i \neq j \\ 1, i = j \end{cases}$$

Процесс ортогонализации Грамма-Шмидта:

$e_1, \dots, e_n$  - базис

Хотим ортонормированный  $f_1, \dots, f_n : \langle f_1, \dots, f_k \rangle = \langle e_1, \dots, e_k \rangle \quad \forall 1 \leq k \leq n$ :

Строим по индукции:

Б.И.  $k=1$ :

$$f_1 = \frac{1}{\|e_1\|} e_1$$

И.П.  $k-1 \rightarrow k$ :

$$f_k = e_k + \sum_{i=1}^{k-1} \lambda_i f_i$$

$$(f_k, f_j) \stackrel{?}{=} 0 \quad 1 \leq j \leq k-1$$

$$(f_k, f_j) = (e_k, f_j) + \sum_{i=1}^{k-1} \lambda_i (f_i, f_j) \stackrel{= \lambda_j}{=}$$

$$\lambda_j = -(e_k, f_j) \quad \forall 1 \leq j \leq k-1$$

Ортонормируем  $f_k$ , чтобы  $(f_k, f_k) = 1$

## УТВ

Если  $e_1, \dots, e_n$  - ОНБ  $U$

$$\text{pr}_U v = \sum_{i=1}^n (v, e_i) e_i$$

## Док-во

Хотим доказать  $v - \sum_{i=1}^n (v, e_i) e_i \in U^\perp$

Достаточно доказать, что вектор ортогонален любому

$$(v - \sum_{i=1}^n (v, e_i) e_i) e_j = (v, e_i) - \sum_{i=1}^n (v, e_i) (e_i, e_j)$$

$1 \leq j \leq n$



Пример

$$\mathbb{R}^n$$

$$(x; y) = \sum x_i y_i$$

$$e_i = (0, 0, \dots, \underset{i}{1}, \dots, 0)$$

Пример

$$T_n = \left\{ a_0 + \sum_{k=1}^n a_k \cos kx + \sum_{k=1}^n b_k \sin kx \right\}$$

$$(f; g) = \int_0^{2\pi} f g dx$$

$$\left\{ \frac{1}{\sqrt{2\pi}}, \frac{1}{\sqrt{\pi}} \cos kx_{k=1, \dots, n}, \frac{1}{\sqrt{\pi}} \sin kx_{k=1, \dots, n} \right\}$$

$$\begin{aligned} \text{pr}_{T_n} f = \frac{1}{2\pi} \int_0^{2\pi} f(x) dx + \frac{1}{\pi} \sum_{k=1}^n \left( \int_0^{2\pi} f(x) \cos(kx) dx \right) \cdot \cos kx + \\ \frac{1}{\pi} \sum_{k=1}^n \left( \int_0^{2\pi} f(x) \sin(kx) dx \right) \cdot \sin kx \end{aligned}$$

Опр

$A \in M_n(K)$  назыв. ортогональной, если

$$A^T A = E$$

$O_n(K)$  - множество орт. матриц

УТВ

$O_n(K)$  - группа по умножению

Док-во

$$\left. \begin{array}{l} A^T A = E \\ B^T B = E \end{array} \right| \Rightarrow (AB)^T AB = B^T \underbrace{A^T A}_E B = B^T B = E$$

$$A^T A = E \Rightarrow A^{-1} = A^T$$

$$(A^{-1})^T A^{-1} \stackrel{?}{=} E$$

$$(A^T)^T A^{-1} = A A^{-1} = E$$

УТВ

$$L \in L(V)$$

1.  $(L_v, L_{v'}) = (v, v') \quad \forall v, v' \in V$
2.  $\|L_v\| = \|v\| \quad \forall v \in V$
3.  $[L]_e \in O_n(\mathbb{R})$ , если  $e$  - ортонорм. базис

Док-во

$$2 \rightarrow 1$$

$$(v, v') = \frac{1}{2}(\|v + v'\|^2 - \|v\|^2 - \|v'\|^2)$$

$$3 \rightarrow 2$$

$$[L_v]_e = [L]_e[v]_e$$

$$\begin{aligned} \|L_v\|^2 &= (L_v, L_v) = [L_v]_e^T \Gamma_e [L_v]_e = [L_v]_e^T [L_v]_e = \\ &= [v]_e^T \underbrace{[L]_e^t [L]_e}_{=E} [v]_e = [v]_e^T [v]_e = [v]_e^T \Gamma_e [v]_e = (v, v) = \|v\|^2 \end{aligned}$$

$$1 \rightarrow 3$$

$$\mathcal{E}_i^T [L]_e^T [L]_e \mathcal{E}_j$$

$$\mathcal{E}_i = (0, \dots, \underset{i}{1}, \dots, 0)$$

$$\mathcal{E}_i^T A \mathcal{E}_j = a_{ij}$$

$$\mathcal{E}_i = [e_i]_e$$

$$\mathcal{E}_j = [e_j]_e$$

$$[e_i]^T [L]_e^T [L]_e [e_j]_e = [L_{e_i}]_j^T [L_{e_j}]_e = [L_{e_i}]_e^T \Gamma_e [L_{e_j}]_e = (L_{e_i}, L_{e_j}) = (e_i, e_j) = \delta_{ij}$$

Опр (унитарного пространства)

$U$  - в.п. над  $\mathbb{C}$

$$U \times U \rightarrow ()$$

1.  $(u + v, w) = (u, w) + (v, w) \quad \forall u, v, w \in U$   
 $(\lambda v, w) = \lambda(v, w) \quad \forall \lambda \in \mathbb{C}, \quad v, w \in U$
2.  $(u, v) = \overline{(v, u)}$
3.  $(u, u) \geq 0$
4.  $(u, u) = 0 \Rightarrow u = 0$

Пример

$$\mathbb{R}^n | \mathbb{C}^n$$

$$(x, y) = \sum x_i y_i | (x, y) = \sum x_i \overline{y_i}$$

f

$e_1, \dots, e_n$  - базис

$\Gamma_e = \{(e_i, e_j)\}_{i,j}$  - матрица грамма

$$(u, v) = [u]_e^T \Gamma_e \overline{[v]_e}$$

$$\Gamma_f = M_{e \rightarrow f}^T \Gamma_e \overline{M_{e \rightarrow f}}$$

$$|(u, v)| < \|u\| \cdot \|v\|, \quad \|u\| = \sqrt{(u, u)}$$

$$\|tu + v\|^2 = t^2 \|u\|^2 + t((u, v) + (v, u)) + \|v\|^2$$

$$\quad \quad \quad = 2 \operatorname{Re}(u, v)$$

$$\operatorname{Re}(u, v) \leq \|u\|^2 \|v\|^2$$

$$(u, v) = |(u, v)| \cdot |z| \Rightarrow |z| = 0$$

$$\operatorname{Re}\left(\frac{1}{z}u, v\right) \leq \left\|\frac{1}{z}u\right\|^2 \|v\|^2 =$$

$$\text{Напоминание: } \|\lambda u\| = \sqrt{(\lambda u, \lambda u)} = \sqrt{\lambda \bar{\lambda} (u, u)} = |\lambda| \|u\|$$

$$= \|u\| \|v\|$$

$$\operatorname{Re} \frac{1}{z} (u, v) = \operatorname{Re} |(u, v)| = |(u, v)|$$

Доказали КБШ

**Опр**

$V$  - в.п. над  $K$

$$V^* = L(V, k)$$

**Пример**

$v \in V$  - евклидово пр-во (унитарное)

$$\varphi_v(w) = (w, v) \quad \varphi_v : V \rightarrow \mathbb{R}(\mathbb{C})$$

Хотим доказать:  $\varphi \in V^* \Rightarrow \exists! v \in V : \varphi = \varphi_v$

**Док-во**

$e_1, \dots, e_n$  - ОНБ  $V$

$$v = \sum \lambda_i e_i$$

Нужно  $\forall w \in V \quad (w, v) = \varphi(w)$ , т.к.  $\varphi$  - линейный функционал

$$\Leftrightarrow \forall j \quad (e_j, v) = \varphi(e_j)$$

$$(e_j, \sum \lambda_i e_i) = \sum_i \bar{\lambda}_i (e_j, e_i)$$

**Опр**

$$A \in M_n(\mathbb{C})$$

$A^* = \bar{A}^T$  - сопряженная матрица

**Свойства**

1.  $A^{**} = A$
2.  $(\lambda A)^* = \bar{\lambda} A^*$
3.  $(A + B)^* = A^* + B^*$
4.  $(AB)^* = B^* A^*$
5.  $(A^{-1})^* = (A^*)^{-1}$

### УТВ

$V$  - унитарное пр-во,  $L \in L(V)$ ,  $u \in V$

$$\varphi_n(v) = (Lv, u) \in V^*$$

$$\Rightarrow (Lv, u) = (v, w_u)$$

$$\exists! w_u \in V : (v, u) = (v, w_u)$$

$$u \rightarrow w_u$$

Утверждается, что отображение линейно

### Док-во

$$(Lv, u) = (v, w_u) | (Lv, u + u') = (Lv, u) + (Lv, u') =$$

$$(Lv, u') = (v, w_{u'}) | = (u, w_u) + (v, w_{u'}) = (v, w_u + w_{u'}) = (v, w_{u+u'})$$

$$(Lv, \lambda u) = \bar{\lambda}(Lv, u) = \bar{\lambda}(v, w_u) = (v, \lambda w_u)_{=w_{\lambda u}}$$

$$L * u = w_u \quad (Lv, u) = (v, L * u)$$

### Опр

$L^*$  - эрмитов сопряженный оператор

### Свойства

$$1. L^{**} = L$$

$$(L^*v, u) = (v, L^{**}u)$$

$$(L^*v, u) = \overline{(u, L^*v)} = \overline{(Lu, v)} = (v, Lu)$$

$$\Rightarrow L^{**}u = Lu \quad \forall u \in V$$

Почему так?  $(v, w) = (v, w') \quad \forall v \Rightarrow w = w'$

$$(v, w - w') = 0$$

$$v = w - w'$$

$$\|w - w'\|^2 = 0$$

$$\Rightarrow w - w' = 0$$

$$2. (\lambda L)^* = \bar{\lambda} L^*$$

$$(\lambda L)v, u) = (v, (\lambda L)^*u)$$

$$(\lambda L)v, u) = (\lambda \cdot Lv, u) = \lambda(Lv, u) = \lambda(v, L^*u) = (v, \bar{\lambda}L^*u)$$

3.  $(L + L')^* = L^* + L'^*$  аналогично

4.  $(LNv, u) = (v, (LN)^*u)$

$(LNv, u) = (v, N^*L^*u)$  и то же, что делали раньше

5.  $[L]_e^* = [L^*]_e$ , если  $e$  - ОНБ

$$Le_i = \sum a_{li}e_l \quad [L]_e = \{a_{ij}\}$$

$$Le_j = \sum b_{kj}e_k \quad [L]_e = \{b_{kj}\}$$

$$(Le_i, e_j) = (e_i, L^*e_j) \\ = a_{ij} \qquad \qquad \qquad = \bar{b}_{ij}$$

### Опр

$$A \in M_n(\mathbb{C})$$

$A$  - унитарная, если  $A^*A = E$

$$U_n = \{A \in M_n(\mathbb{C}) : (\text{то что сверху})\}$$

### Док-во (что это группа по умножению)

$$\left. \begin{array}{l} A^*A = R \\ B^*B = E \end{array} \right| \Rightarrow (AB)^*AB = B^* \underbrace{A^*A}_{=E} B = E$$

$$(A^{-1})^*A^{-1} \stackrel{?}{=} E$$

$$\Leftrightarrow (A^{-1})^* = A$$

$$\Leftrightarrow (A^*)^{-1} = (A^{-1})^{-1}$$

Докажем, что любая унитарная матрица обратима и модуль определителя равен единице

$$A^*A = E$$

$$\overline{\det A} \cdot \det A = 1$$

$$|\det A|^2 = 1$$

### УТВ

$$L \in L(V)$$

Следующие условия равносильны:

1.  $\|Lv\| = \|v\| \quad \forall v$
2.  $(Lv, Lu) = (v, u) \quad \forall v, u$
3.  $[L]_e \in U_n, \quad e - \text{ортонорм.}$
4.  $L^*L = \text{id}_V$

И оператор, удовлетворяющий этим условиям называется "унитарным" (в евклидовом случае называется "ортогональным")

### Док-во

(4  $\Rightarrow$  2):

$$(v, L^*Lu) = (Lv, Lu) \\ =_{(v,u)}$$

(2  $\Rightarrow$  4):

$$(v, L^*Lu) = (Lv, Lu) = (v, u)$$

По заклинию  $L^*L = \text{id}_V$

### УТВ

1.  $|\det L| = 1$
2. Если  $L$  - унитарный,  $Lv = \lambda v \xRightarrow{v \neq 0} |\lambda| = 1$
3.  $Lv = \lambda v \quad Lu = \mu u \quad \lambda \neq \mu \Rightarrow (u, v) = 0$

### Док-во

1 и 2:

$$\|v\| = \|Lv\| = \|\lambda v\| = |\lambda| \|v\|$$

3:

$$(u, L^*v) = (u, \bar{\lambda}v) = \lambda(u, v)$$

$$(u, L^*v) = (Lu, v) = (\mu u, v) = \mu(u, v)$$

Хотим доказать:  $Lv = \lambda v \Rightarrow L^*v = \bar{\lambda}v$

$$v = L^*Lv = L^*(\lambda v) = \lambda L^*v$$

Делим на  $\lambda$  и туда переносится  $\bar{\lambda}$