Санкт-Петербургский государственный университет

Лекции по алгебре

3 семестр, преподаватель Демченко О. В.

Записали Костин П.А. и Щукин И.В.[1]

[1] Данный документ неидеальный, прошу сообщать о найденных недочетах вконтакте (можно присылать скрины неточностей с указанием билетов)

Содержание

1 Теория групп

2019-09-17

Опр (группа)

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. $(\mathbb{Z}, \cdot)$ - не группа
3. $(R, +)$ - группа кольца
4. $(R^*, \cdot)$
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. $(g^{-1})^{-1} = g$

Опр

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

Теорема (св-ва степени)

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

Опр

$g \in G$, $n \in N$ - порядок g ($\operatorname{ord} g = n$), 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. $(\mathbb{Z}/_6\mathbb{Z}, +)$

   $\operatorname{ord}(\overline{1}) = 6$

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

Утв

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

Док-во

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

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

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

Опр

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

Опр

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

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

G - кон. группа, $a \in G$, $\operatorname{ord} a = m$, $H = \{a^n : n \in \mathbb{Z}\}$, тогда $|H| = m$

Док-во

$\{a^0 = e, a_1, ..., a^{m-1}\}$ - подмножество H
Докажем, что все остальные элементы тоже здесь есть
$n \in \mathbb{Z} \Rightarrow n = mq + r$, $0 \leqslant m - 1$
$a^n = a^{mq+r} = (a^m)^q a^r = a^r$
$a^k = a^l$, $0 \leqslant k \leqslant l \leqslant m - 1$, умножим на a^{-k}
$e = a^{l-k}$ $o \leqslant l - k \leqslant m - 1$ m - наименьшее $\mathbb{N}$ такое что $a^m = e$
$l - k = 0 \Rightarrow l = k$
Докажем, что $|H| = m$
$\Rightarrow |G| \vdots m = \operatorname{ord} a$, т.о. в группе порядок эл-та - делитель порядка группы

Напоминание

Следствие **(теорема Эйлера)**

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

Док-во

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

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 - 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 $\equiv$ $\exists g \in G : \operatorname{ord} g = n$)

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 φ - изоморфизм

Примеры

1. $D_3 \to S_3$

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

Опр

Две группы называются изоморфными, если между ними существует изоморфизм

Утв

Изоморфизм - отношение эквивалентности

Док-во

т.к. композиция изоморфизмов - изоморфизм $G \xrightarrow{e} H \xrightarrow{\psi} H$
$(\psi \circ \varphi)(g_1g_2) = \psi(\varphi(g_1g_2) = \psi(\varphi(g_1)\varphi(g_2)) = \psi(\varphi(g_1))\psi(\varphi(g_2)) = (\psi \circ \varphi)(g_1) \circ (\psi \circ \varphi)(g_2)$
Рефлексивность - тождественное отображение - изоморфизм
Транзитивность: $G \underset{\varphi}{\rightarrow} H$, $H \underset{\varphi^{-1}}{\rightarrow} G$

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 $\varphi(g^kg^l) \underline{= \varphi(g^k) + \varphi(g^l}) = \overline{k} + \overline{l}$
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 $\varphi(g^ng^k) = \varphi(g^n) - \varphi(g^k) = n + k$

2019-09-17

Утв

$|G| = p$, p - простое $\Rightarrow G \cong \mathbb{Z}/p\mathbb{Z}$

Док-во

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

Утв

H, G - группы, $\varphi : G \to H$ - изоморфизм $\Rightarrow n = \operatorname{ord} g = \operatorname{ord} \varphi(g)$

Док-во

Пусть $g^n = e,\ \varphi(g^n) = \varphi(e) \overset{?}{=} e$

$$\varphi(e)^2 = \varphi(e^2) = \varphi(e)$$

Теперь докажем, что меньшего нет

$$\varphi(g)^m = e,\ m \in \mathbb{N} \overset{?}{\Rightarrow} m \geqslant n$$

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

Опр

$H < G$, тогда H - нормльная подгруппа, если $\forall h \in H, g \in G \Rightarrow g^{-1}hg \in H$ - сопряжение элемента h с помощью элемента g, обозначается: $H \triangleleft G$

Замечание

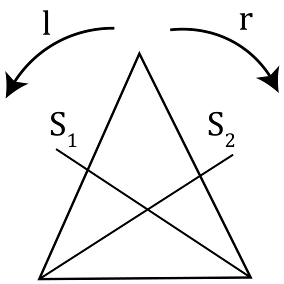
Элементы подгруппы при сопряжении переходят в элементы подгруппы

Замечание

Подгруппа любой коммунитативной группы нормальна

Пример

D_3 - 6 элементов, 3 поворота и 3 симметрии



$\{e, l, r\}$ - нормальная
$\{e, s_1\}$ - не нормальная

Утв

$H \triangleleft G \Leftrightarrow$ разбиение на Л и П кдассы смежности по Н совпадают

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

Док-во

Берем произвольный элемент из левого и правого и докажем, что совпадают. Берем слева:

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

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

Теперь справа:

$$g \in G, \quad h \in H, \quad g^{-1}hg = h_1$$

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

Опр (умножение классов смежности)

$$H \triangleleft G$$

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

Док-во (корректнтости)

Хотим проверить, что

$$\widetilde{g}_1H = g_1H, \quad \widetilde{g}_2H = g_2H \stackrel{?}{\Rightarrow} \widetilde{g}_1\widetilde{g}_2H = g_1g_2H$$

Аналогично прошлому доказательству

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

$$\widetilde{g}_1\widetilde{g}_2h = g_1h_1g_2h_2h = g_1g_2\underset{=h_3}{(g_2^{-1}h_1g_2)}h_2h$$

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

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

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

$$\widetilde{g}_1\widetilde{g}_2H = g_1h_1g_2h_2h = g_1g_2\underset{=h_3}{(g_2^{-1}h_1g_2)}h_2h$$

Осталось доказать, что получается группа

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

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

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

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

G/H

Была эквивалентность: $a \sim b \Leftrightarrow a - b \vdots h$

$G = \mathbb{Z}$

$H = h\mathbb{Z}, \quad g_1g_2^{-1} \in H$ - мульт. запись , $\quad g_1 - g_2 \in n\mathbb{Z}$ - адд. запись

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

Аддитивная группа кольца класса вычетов - это то же самое, что фактор группа группы $\mathbb{Z}$ по подгруппе $n\mathbb{Z}$

Опр

Как в произвольной группе найти подгруппу?

$[g, h] = ghg^{-1}h^{-1}$, $g, h \in G$ - коммутатор элементов $h, g \in G$

Коммутант - множество проззведений всех возможных коммунтаторов

Обозначается $K(G) = \{[g_1, h_1]...[g_n, h_n],\ g_1, h_1 \in G\}$

Док-во (коммутант - подгруппа)

$K(G) < G$

Нейтральный элемент: $[e, e] = e$

Обратный элемент? $[g_1, h_1]...[g_n, h_n]$

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

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

Значит это подгруппа

Нормальная ли? $g^{-1}[g_1, h_1]...[g_n, h_n]g$

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

Нужно доказать, что сопряжение коммутатора лежит в коммутанте

$$g^{-1}g_1h_1g_1^{-1}h_1^{-1}g = \underbrace{g^{-1}g_1h_1g_1^{-1}h_1^{-1}}_{=[g^{-1}g_1, h_1]}\underbrace{h_1g^{-1}h_1^{-1}g}_{=[h_1, g^{-1}]}$$

Утв

Фактор-группа $(G/K(G))$ по коммутанту - коммутативна

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

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

Док-во

Нужно построить изоморфизм $[a]_{mn} \mapsto ([a]_n, [a]_m)$

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

Теперь нужно проверить биекцию

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

Инъективность:

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

На языке сравнений:

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

На самом деле достаточно было проверить одно

Опр

$$\varphi : G \to H \text{ - гомоморфизм, если } \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$$

$$\text{изоморфизм} = \text{гомоморфизм} + \text{биективность}$$

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

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

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

$(a^{-1}ga)(a^{-1}g_1a) = a^{-1}g_1ga$

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

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

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

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

Утв

Ker - нормальная подгруппа G

Док-во

$$\operatorname{Ker} f \lhd G?$$

$$g \in G \qquad a \in \operatorname{Ker} f$$

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

Утв (основная теорема о гомоморфизме)

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

Док-во

Докажем, что это корректное отображение:

$$\operatorname{Ker} f = K$$

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

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

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

Докажем, что φ - 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

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

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

Напоминание

$$\mathrm{SL}_N(K) \text{ - квадратные матрицы с } \det = 1$$

Опр

$$\det : \mathrm{GL}_n(K) \to K^*$$

Но это отображение - сюръекция, а значит:

$$\mathrm{GL}_n(K)/_{\mathrm{SL}_n(K)} \cong K^*$$

$$\mathrm{SL}_n(K) = \{A \in M_n(K) : |A| = 1\}$$

Пример (1)

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

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

Пример (2)

$$G \times H \to G$$

$$(g_1 h) \to g$$

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

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

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

Пример (1)

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

$$G = \mathrm{GL}_n(K)$$

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

$$E_v = v$$

Пример (2)

M = {количество раскрасок вершин квадрата в два цвета}

$$G = D_4$$

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

$$M = G$$

$$gm = gm$$

Опр

$$m \in M$$

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

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

Утв

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

Док-во

Доказательство того, что стабилизатор - подгруппа:

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

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

(симм.) $em = m, \quad e \in G$

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

Утв

$|\text{Orb } m| \cdot |\text{Stab } m| = |G|$

Док-во

$\text{Stab } m = H$

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

$gH \to gm$

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)

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

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

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

$$\sum_{g\in G}|M^g| = |\{(g,m) \in G \times M : gm = m\}| =$$

$$= \sum_{m\in M}|Stab\ m| = |G|\sum_{m\in M}\frac{1}{|Orb\ m|} = |G| \cdot \text{Кол-во орбит}$$

2 Евклидовы и унитарные пр-ва

Опр

$$V \text{ - в.п. над } \mathbb{R}$$

Введем отображение

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

$$(u, v)$$

Свойства этого отображения

1. Симметричность

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

2. Линейность

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

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

3. $(u, v) \geqslant 0 \qquad \forall u \in V$

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

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

Напоминание

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

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

(Сумма элементов главной диагонали)

Примеры

1. Школьные вектора
2. $\mathbb{R}^n$

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

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

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

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

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

(См. след в напоминании)

Опр

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

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

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

Свойства (матрицы Грама)

1. Матрица невырожд
2. e, f - базисы

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

3. $\Gamma_e = \{a_i j\}$

$$u = \sum \lambda_i e_i$$

$$v = \sum \mu_j e_j$$

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

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

Док-во

1. $\urcorner\, |\Gamma_e| = 0 \Rightarrow \exists \lambda_i \in \mathbb{R}$ 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. $\urcorner M_{e \to f} = \{a_{ik}\} \qquad f_k = \sum a_{ik} e_i$

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

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

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

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

Опр

V - в.п. над $\mathbb{R}$

$V \to \mathbb{R}_{\geqslant 0}$

$v \to \|v\|$ - норма

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

2. Нер-во треугольника

$$\|u+v\| \leqslant \|u\| + \|v\|$$

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

Если такое отобр. существует, то оно называется нормой

Утв

(u, v) - ск. пр-ве

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

Пример

$\mathbb{R}^n$

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

$\|x\| = \sum\limits_i |x_i|$

Теорема (Нер-во Коши - Буняковского)

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

Док-во

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

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

$\|u + v\| \leqslant \|u\| + \|v\|$

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

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

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

Утв (Теорема Пифагора)

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

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

Множество всех векторов, которые ортогональны всем векторам из U
Такое мн-во называется ортогональным дополнением

Утв

$U^{\perp}$ - под-пр V

Док-во

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

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

$\lambda \in \mathbb{R}$

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

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

$e_1, ..., e_n$ - базис U дополняем до базиса V

$e_1, ..., e_n, f_1, ..., f_n$ - базис V

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

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

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

это матрица

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

$\Gamma_e x + C_y = 0$

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

$(x, y) \to y$

$\Gamma_e x + C_y = 0$

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

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

2019-10-15

<u>Свойство</u>

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

<u>Док-во</u>

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

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

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

<u>Опр</u>

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

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

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

u называется ортогональной проекцией

Обозначение: $\mathrm{pr}_U\, v \overset{\text{def}}{=} u$

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

<u>Свойства</u> (орт. проекции)

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

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

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

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

2. $\|v - \mathrm{pr}_U\, v\| \leqslant \|v - u\| \quad \forall u \in U$

$$\|v - u\|^2 = \|\underset{\in U^\perp}{v - \mathrm{pr}_U}\, v\|^2 + \|\mathrm{pr}_U \underset{\in U}{v - u}\|^2$$

Опр

$e_1, ..., e_n$ - базис V

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

$$(e_i, e_j) = \delta_{i,j} = \left[\begin{array}{l} 0, i \neq j \\ 1, i = j \end{array}\right.$$

Алгоритм

Процесс ортоганализации Грамма-Шмидта:

$e_1, ..., e_n$ - базис

Хотим ортонормированный $f_1, ..., f_n :< f_1, ..., f_k >=< e_1, ...e_k > \quad \forall 1 \leqslant k \leqslant n$:
Строим по индуции:
Б.И. k=1:

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

И.П. $k - 1 \to k$:

$$f_k = e_k + \sum_{i=0}^{k-1} \lambda_i f_i$$

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

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

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

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

Утв

Если $e_1, ..., e_n$ - ОНБ U

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

Док-во

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

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

Пример

$$\mathbb{R}^n$$

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

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

Пример

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

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

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

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

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

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

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

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

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

Утв

$L \in \mathscr{L}(V)$ (пр-во лин. функционалов)

Следуюшие утверждения равносильны:

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

Док-во

$2 \to 1$

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

$3 \to 2$

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

$$\|L_v\|^2 = (L_v, L_v) = [L_v]_e^T \Gamma_e [L_v]_e = [L_v]_e^T [L_v]_e =$$

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

$1 \to 3$

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

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

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

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

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

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

2019-10-22

Опр (унитарного пространства)

U - в.п. над $\mathbb{C}$

$$U \times U \to ()$$

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

Пример

R^n	C^n
(x,y) $= \sum x_i y_i$	(x,y) $= \sum x_i \overline{y_i}$

$e_1, ..., e_n$ - базис

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

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

$\Gamma_f = M_{e\to f}^T \Gamma_e \overline{M}_{e\to f}$

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

$$\|tu+v\|^2 = t^2\|u\| + t(\underbrace{(u,\ v) + (v,\ u)}_{=2\operatorname{Re}(u,v)}) + \|v\|^2$$

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

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

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

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

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

Доказали КБШ

Опр

V - в.п. над K

$$V^* = \mathscr{L}(V,\ K)$$

Пример

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

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

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

Док-во

$e_1, ..., e_n$ - ОНБ V

$$v = \sum \lambda_i e_i$$

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

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

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

Опр

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

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

Свойства

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

Утв

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

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

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

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

$$u \to w_u$$

Утверждается, что отображение линейно

Док-во

$$\left.\begin{array}{c}(\text{Lv, u}) = (\text{v, w}_u) \\ (\text{Lv, u'}) = (\text{v, w}_{u'})\end{array}\right| \begin{array}{c}(\text{Lv, u+u'}) = (\text{Lv, u}) + (\text{Lv, u'}) = \\ = (\text{u w}_u) + (v,\ w_{u'}) = (v,\ w_u + w_{u'}) = (v,\ w_{u+u'})\end{array}$$

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

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

Опр

L^* - эрмитов сопряженный оператор

Свойства

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

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

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

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

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

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

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

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

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

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

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

<u>Опр</u>

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

A - унитаная, если $A^*A = E$

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

<u>Док-во</u> (что это группа по умножению)

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

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

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

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

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

$L \in \mathscr{L}(V)$

Следующие условия равносильны:

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

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

Док-во

$(4 \Rightarrow 2)$:

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

$(2 \Rightarrow 4)$:

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

По заклинанию $L^*L = \mathrm{id}_V$

Утв

1. $|\det L| = 1$
2. Если L - унитарный, $Lv = \lambda v \underset{v \neq 0}{\Rightarrow} |\lambda| = 1$
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:

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

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

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

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

Делим на λ и туда переносится $\overline{\lambda}$

2019-3-29

Опр

L - орт. оператор на плоскости, $\det L = 1$, тогда L - поворот

e - ортнорм. базис, $[L]_e = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{cases} a^2 + c^2 = 1 \\ b^2 + d^2 = 1 \\ ab + cd = 0 \\ ad - bc = 1 \end{cases}$$

$$a = \cos\varphi, \quad c = \sin\varphi$$

$$b = \sin\varphi, \quad d = \cos\psi$$

$$\underbrace{\cos\varphi\sin\psi + \sin\varphi\cos\psi}_{=\sin(\varphi+\psi)} = 0$$

$$\underbrace{\cos\varphi\cos\psi - \sin\varphi\sin\psi}_{=\cos(\varphi+\psi)} = 0$$

$$\Rightarrow \varphi + \psi = 0$$

$$\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$$

Опр

Если e - ортогональный оператор на пл-ти, $\det L = -1$
S - какая-то осевая симметрия
Тогда:

1. $L = S \circ R_\psi$
2. $L = R_\varphi \circ S$

Рассмотрим $S^{-1} \circ L$ - ортогональный оператор с определителем 1, значит по предыдущему определению $S^{-1} \circ L = R_\varphi$

Утв (теорема Эйлера)

В трехмерном пространстве с определителем 1 является поворотом относительно некоторой оси

Следствие: берем две прямые. Поворачиваем сначала относительно одной, потом относительно другой. И их композицией будет повврот

Док-во (теоремы Эйлера)

L - орт. оператор в пр-ве

$$\det L = 1$$

$$\chi_L(t) \in \mathbb{R}[x], \quad \deg \chi_i = 3$$

$\lambda_1, \lambda_2, \lambda_3$ - корни

$$|\lambda_1| = |\lambda_2| = |\lambda_3| = 1$$

Два варианта:

1. $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$
2. $\lambda_1 \in \mathbb{R}$, $\lambda_2 = \overline{\lambda_3}$

В 1 случае одно из λ равно 1, пусть λ_1
Во 2 случае $\lambda_1 = 1$ т.к. $\lambda_1\lambda_2\lambda_3 = \lambda_1\overline{\lambda_2}\lambda_3 = \lambda_1|\underbrace{\lambda_3}_{=1}|^2 = \lambda_1$
С.в. остается неподвижным при повороте. Ось тоже. Значит собственный вектор при повороте и есть ось
Осталось д-ть, что ортогональное дополнение есть вращение. Тогда докажем, что наш исходный оператор - вращение относительно оси

$$\exists Lv = v$$

$$v^\perp$$

Докажем, что эта плоскость - инвариантное подпространство. Нужно доказать:

$$(u, v) = 0 \to (Lu, v) = 0$$

То есть резульат будет тоже из ортогонального дополнения

$$(Lu, v) = (Lu, Lv) = (u, v) = 0 \text{ ч.т.д.}$$

Так как инвариантное подпространство, можем сузить L. Оно является плоскостью. Т.к. L - орт. оператор, значит он сохраняет расстояние. Т.к. S тоже сохраняет расстояние, значит L является ортоганальным оператором на плоскости. Осталось убедиться, что модуль равен 1. Если исходный оператор сохраняет расстояние, то и его сужение сохраняет ориентацию. Другой способ: построим матрицу L в базисе: V, {два ортогональных вектора на плоскости}, матрица L будет такой:

$$[L] = \begin{pmatrix} 1 & 0 & 0 \\ 0 & ? & ? \\ 0 & ? & ? \end{pmatrix}$$

Вместо ? будет матрица сужения. Мы должны доказать, что это матрица поворота. Определитель большой матрицы равен определителю маленькой, но т.к. большая 1, то и он 1.

По предыдущим рассуждениям - это повrот. То есть у нас есть пространство с осью, на которую оператор действует тождественно, а на другое он действует как повrот.

Утв

Если L - ортогональный оператор в пре-ве с определитем -1 равен композиции повrота, относительно оси и симметрии, то это поворот.

Док-во

Аналогично

Теорема

Унитарный оператор имеет ортонормированный базис из с.в.

Док-во

Индукция по размерности пр-ва.
Пусть одномерное пр-во ($n = 1$) - очевидно, т.к. оператор-вектор v

$$Lv = u, \quad \|u\| = \|v\| \Rightarrow u = \lambda v, \quad |\lambda| = 1$$

Значит $Lv = \lambda v$ - подходит, когда ортонормируем
v - с.в. L с каким-то λ

$$Lv = \lambda v$$

$$< v >^{\perp}$$

Хотим доказать, что подпространство инвариантно относительно действия L:

$$(v,\ u) = 0 \Rightarrow (v,\ Lu) = 0$$

$$(v,\ Lu) = (L^* v,\ u) \overset{(*)}{=} (\overline{\lambda} v,\ u) = \overline{\lambda}(v, u) = 0$$

($*$) т.к. мы доказывали, что у собственного оператора. Если v - вектор унитарного оператора с с.ч. λ
Раз исходный оператор унитарный, то сужение тоже унитарно. Значит мы можем применить индукционное предположение у сужению. На этом ортогональном дополнении у оператора есть базис ортогональных векторов. Добавим к нему отнонормированный вектор v. Очевидно, получим ортонормированный базис из собственных векторов всего пр-ва

Переформулируем на языке матриц

Теорема

U - унитарная матрица, тогда:

$$U = MDM^{-1}, \quad D = \begin{pmatrix} \lambda_1 & ... & 0 \\ 0 & ... & 0 \\ 0 & ... & \lambda_k \end{pmatrix}, \quad |\lambda_i| = 1, \quad M \text{ - унитарная}$$

Док-во

$$\mathbb{C}^n \quad Lz = Uz \qquad [L]_e = U$$

$$e \text{ - есть базис } \mathbb{C}^n$$

$$[L^*L]_e = [L^*]_e[L]_e = [L]_e^*[L]_e = U^*U = E$$

($*$) Из какого-то рассуждения получается
$\Rightarrow$ L - унитарный оператор
По теореме, которую доказали ранее, f - ортонормированный базис $\mathbb{C}^n$ из с.в. L

$$D = [L]_f = M_{e\to f}^{-1}\underbrace{[L]_e}_{=U}M_{e\to f}$$

($*$) У D - на диагонали с.ч., по модулю равные 1
Хотим д-ть: у нас есть два ОНБ, тогда матрица перехода между ними будет унитарна

$$M_{e\to f} = \{a_{ij}\}$$

$$f_j = \sum a_{ij}e_i$$

$$\delta_{jk} = (f_j,\ f_k) = \left(\sum_i a_{ij}e_{ij},\ \sum_l a_{ij}\overline{a}_{lk}e_l\right) = \sum_{i,l} a_{ij}\overline{a}_{lk}(e_i,\ e_l)\sum a_{ij}\overline{a}_{ik}$$

Опр

$A \in M_n(\mathbb{C})$ - эрмитова, если $A^* = A$
$L \in \mathscr{L}(V)$ - самосопряженный, если $L^* = L$

Свойства

1. L - самосопряженный, тогда $[L]_e$ - эрмитова, если e - ортонормированный

$$[L]_e^* = [L^*]_e = [L]_e$$

2. L - самосопряженный, тогда с.ч.$\in \mathbb{R}$

$$\exists Lv = \lambda v, \quad v \neq 0$$

$$\lambda(u,\ v) = (Lv,\ v) = (v,\ Lv) = (v,\ \lambda v) = \overline{\lambda}(v,\ v)$$

3. $Lv = \lambda v \quad Lu = \mu u \qquad \lambda \neq \mu \Rightarrow (u,\ v) = 0$

$$\lambda(v,\ u) = (Lv,\ u) = (v,\ Lu) = (v,\ \mu u) = \mu(v,\ u)$$

2019-10-29

Теорема

L - самосопр. $\Rightarrow \exists e_1, ..., e_n$ - ортнорм. базис из с.в. L

$Lv = \lambda v$

$(u, v) = 0 \overset{?}{\Rightarrow} (Lu, v) = 0$

$(Lu, v) = (u, L^* v) = (u, Lv) = (u, \lambda v) = \lambda(u, v) = 0$

Тут мы должны задать вопрос.

Опр

A - эрмитова матрица

$\Rightarrow M$ - унитарная

D - $\underset{\in\mathbb{R}}{\text{диагональная}}$ $: A = MDM^{-1}$

Теорема

A - эрмитов матрица

Тогда условия равносильны

1. $\underset{x\neq 0}{\forall x \in \mathbb{C}^n} \quad \underset{\in\mathbb{R}}{x^* A x} > 0 \qquad (x^* A x)^* = x^* A^* x = x^* A x$
2. Все с.ч. $A > 0$
3. Все гл. миноры $A > 0$ (критерий Сильвестра)
4. $\exists P$ - обратимое: $A = P^* P$

Если хотя бы одно из них выполняется, то матрица A - положительно опред.

Док-во

$4 \to 1$

$A = P^* P$

$x^* A x = x^* P^* P x = (Px)^*(Px) = < Px, Px >$

$< a, b > = \sum a_i \overline{b}_i$ Стандартное эрмитово скал. произв. в $\mathbb{C}$

$2 \to 4$

$A = MDM^{-1} \quad M$ - унит $\quad D$ - диаг. $(\in \mathbb{R})$

$$D^{\frac{1}{2}} = \begin{pmatrix} \sqrt{d_1} & ... & 0 \\ & \ddots & \\ 0 & ... & \sqrt{d_n} \end{pmatrix} \qquad A = (D^{\frac{1}{2}}M^*)^*(D^{\frac{1}{2}}M^*)$$

M - унитар $\Rightarrow MD^{\frac{1}{2}}D^{\frac{1}{2}}M^* = MDM^{-1} = A$

$1 \to 2$

$Ax = \lambda x$

$x^* \underset{>0}{A} x = x^*\lambda x = \lambda x^* x = \lambda < \underset{>0}{x, x} >$

$1 \to 3$

Нужно доказать, что все главные миноры больше 0

$$A = \begin{pmatrix} A' & B \\ C & D \end{pmatrix}$$

$$\begin{pmatrix} x' \\ 0 \end{pmatrix}^* \begin{pmatrix} A' & B \\ C & D \end{pmatrix} \begin{pmatrix} x' \\ 0 \end{pmatrix} = x'^* A' x' > 0 \quad \forall x' \neq 0$$

$\Rightarrow A'$ уд первому условию, а еще 4 условию

$A' = P * P$

$$\det A' = \det P^* \cdot \det P = \overline{\det P} \cdot \det P = |\det P|^2 > 0 \qquad \text{т.к. P обратим}$$

$3 \to 2$

Индукция по размеру A
Когда матрица 1×1 очев.
Инд. переход : $n \to n + 1$
Пусть λ - с.ч A , $\quad \lambda < 0 \Rightarrow \exists \mu < 0$

$$Ax = \lambda x \qquad Ay = \mu y, \quad < x, y >= 0$$

Если λ и μ различные.
Если с.ч. различны, то им соотв. ортогон. с.в $\Rightarrow$ у эрмит. матр. ортогон с.в соотв. различным с.ч .

У эрмитовой матрицы существует онб из с.в - столбцов. В этом базисе будет два вектора, лежащие в одном подпр-ве.

Что такое собственное под-во?

Если λ и μ совпадают, то есть два неколл. с.в., мы можем их ортогонализировать

$$\exists \alpha, \beta \in \mathbb{C} : \underbrace{\alpha x + \beta y}_{=u} = (u', 0)$$

$$A = \begin{pmatrix} A' & * \\ * & * \end{pmatrix}$$

$u'^* A' u' = u^* A u = |\alpha|^2 x^* A x + |\beta|^2 y^* A y =$ подставили u которое сверху

$$= |\alpha|^2 \underset{<0}{\lambda} \cdot \|x\|^2 + |\beta|^2 \underset{<0}{\mu} \|y\|^2 < 0$$

$$u'^* A' u' < 0$$

Если бы для матрицы A' выполнялось 3 условие, то должно было бы выполняться 2 условие, а 1 не выполняется, это значит, что 3 условие не вып. Все главные миноры A' - это в частности главные миноры A. А 3 выполняется для A. Мы получили противоречие.

Замечание

Все то же самое, можно доказать для симм. матрицы.
Пусть след. усл равносильны... для симм. матрицы над $\mathbb{R}$
Только тут будет P над $\mathbb{R}$

КАЖЕТСЯ, ТУТ ЧТО-ТО НЕ ТАК, ЭТО УЖЕ БЫЛО

Теорема

A - эрмит. матрица

тогда след. условия равносильны

1. $\forall x \in \mathbb{C}^n \qquad \underset{\in \mathbb{R}}{x^* A x} \geqslant 0$
2. Все с.ч. $A \geqslant 0$
3. Все гл. миноры $A \geqslant 0$
4. $\exists P : \qquad A = P^* P$

Такая матрица называется положительно полуопред.

Док-во

Доказать дома

Опр (Singular value decompostition SVD)

$$A \in M_{m,n}(\mathbb{C}) \Rightarrow \exists \underset{m\times m}{U}, \underset{n\times n}{V} \text{ - унитарные}, \quad S \in M_{m,n}(\mathbb{R})$$

S - диаг. насколько это возможно для прямоуг. матрицы, с неотр числами на диаг.

$$A = USV^*$$

Поворот, растяжение, поворот

Док-во

$$m \leqslant n$$

$$A^*A \text{ - эрмитова} \qquad (A^*A)^* = A^*A \text{ - proof}$$

$$x^*A^*Ax = (Ax)^*(Ax) \geqslant 0$$

Значит эта матрица положительно полуопред.

$$\exists V \text{ - унитарная:} \quad V^*A^*AV = D' \text{ - диаг} \quad V \in \mathrm{GL}_n(\mathbb{C})$$

т.к. эта матрица положительно полуопред., то у этой матрицы на диаг будут стоять неотр. с.ч. Переставим с.ч так, что сначала идут положительные, а потом нули

$$D' = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix} \qquad D \in M_k(\mathbb{R}) \quad m \geqslant n \geqslant k$$

$$V = (\underset{k \text{ столб}}{V_1} \quad \underset{n-k \text{ столб.}}{V_2}) \quad V_1 \in M_{n,k}(\mathbb{C}) \quad V_2 \in M_{n,n-k}(\mathbb{C})$$

$$D' = \begin{pmatrix} v_1^* \\ v_2^* \end{pmatrix} A^*A \begin{pmatrix} V_1 & V_2 \end{pmatrix} = \begin{pmatrix} V_1^*A^*AV_1 & V_1^*A^*AV_2 \\ V_2^*A^*AV_1 & V_2^*A^*AV_2 \end{pmatrix} = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$$

$$\Rightarrow \begin{matrix} V_1^*A^*AV_1 = D \\ V_2^*A^*AV_2 = 0 \Rightarrow AV_2 = 0 \end{matrix}$$

$$\begin{pmatrix} V_1^* \\ V_2^* \end{pmatrix} \begin{pmatrix} V_1 & V_2 \end{pmatrix} = \begin{pmatrix} V_1^*V_1 & V_1^*V_2 \\ V_2^*V_1 & V_2^*V_2 \end{pmatrix} = \begin{pmatrix} E_k & 0 \\ 0 & E_{n-k} \end{pmatrix}$$

$$\Rightarrow \begin{matrix} V_1^*V_1 = E_k \\ V_2^*V_2 = E_{n-k} \end{matrix} \qquad \begin{pmatrix} V_1 & V_2 \end{pmatrix} \begin{pmatrix} V_1^* \\ V_2^* \end{pmatrix} = V_1V_1^* + V_2V_2^* = E_n$$

$$U_1 \overset{\text{det}}{=} AV_1D^{-\frac{1}{2}} \in M_{m,k}(\mathbb{C})$$

$$U_1D^{\frac{1}{2}}V_1^* = AV_1D^{-\frac{1}{2}}D^{\frac{1}{2}}V_1^* = A - AV_2V_2^* = A$$

2019-11-05 Продолжение док-ва:

Док-во

$$U_1^*U_1 \overset{def}{=} D^{-\frac{1}{2}} \underbrace{V_1^*A^*AV_1}_{=D} D^{-\frac{1}{2}} = E_k$$

Осталось из U_1 и V$_1$.$\Rightarrow$ U_1 содержит k ортогональных столбцов. Раз они ортогональны, можно дополнить до ортогонального базиса в $\mathbb{C}^n$ и получаем:

$$U = (U_1U_2) \in M_n(\mathbb{C})$$

Эта матрица ортонормирована из-за ортог. столбцов.

$$S := \begin{pmatrix} \begin{pmatrix} D^{\frac{1}{2}} & 0 \\ 0 & 0 \end{pmatrix} \\ 0 \end{pmatrix} \in M_{m_1 n}(\mathbb{C})$$

$$(U_1U_2)S(V_1V_2)^* = U_1F^{\frac{1}{2}}V_1^* = A$$

Матрица S нужного размера. Матрица U_1 - квадратная и унитарная. С V_1 тоже все ок

Замечание

Такая же теорема верна в $\mathbb{R}$. Только если тут унитарные матрицы, то там ортоганальные

2.25 Квадратичные формы над $\mathbb{R}$

Опр

$$x = (x_1, ..., x_n), \text{ тогда:}$$

$$S(x) = \sum_{i \geqslant j} a_{ij}x_ix_j \text{ - квадратичная форма}$$

Замечание

$$S(x) = \sum_{b_{ij}=b_{ji}} a_{ij}x_ix_j$$

$$b_{ij} = \begin{bmatrix} a_{ij}, & i = j \\ \frac{a_{ij}}{2}, & i > j \\ \frac{a_{ji}}{2}, & j > i \end{bmatrix}$$

$B = (b_{ij})$ - матрица соответствующая

$S(x) = x^T Bx$

$x = My$

$S(x) = y^T M^T BMy$

Опр

S - положительно определена, если:

1. $\forall x \quad S(x) \geqslant 0$
2. $S(x) = 0 \Rightarrow x = 0$

Замечание

Эквивалентно тому, что матрица S - положительно определена. В частности это значит, что верен критерий Сильвестра

Опр

$$S(x) = a_1 x^2 + ... + a_n x_n^2 \text{ - канонический вид}$$

Теорема

Любую матрицу можно привести к каноническому виду с помощью элементарного преопразования

Док-во

Любая самосопряженная матрица представляется в виде: унитарная матрица * диагональная * унитарная сопряженная к первой. В $\mathbb{R}$ формулируется так: любая симметрическая матрица: ортогональная * симметричная * ортоганальная в минус 1. То есть получили то что нам нужно

2.26 Применение сингулярного разложения

$Ax = b$

У A столбцов мало, строк много

Хотим решить приближенно, то есть чтобы $\|Ax - b\| \to \min$

Опр

x, который минимизирует разность называется решением методом наименьших квадратов (МНК)

Теорема

$A \in M_{n,m}(\mathbb{R})$

1. x^* - решение МНК $\Leftrightarrow A^TAx^* = A^Tb$
2. $A^TA \in \mathrm{GL}_n(\mathbb{R}) \Leftrightarrow \operatorname{rk} A = m$

Док-во

1. x^* - решением МНК $\overset{\text{Лада записала}}{\Leftrightarrow}$

   Ax^* - проекция b на линейную оболочку столбцов A

   $$Ax^* = \operatorname{pr}_L v$$

   $$b - \operatorname{pr}_L b \perp L \Rightarrow A^T(b - \operatorname{pr}_L b) = 0$$

   Почему $v \perp L \Rightarrow A^T v = 0$?
   $\forall e$: $\underbrace{(Ae, v)}_{=(e, A^Tv)} = 0$
   Какой вектор ортогонален произвольному? Только нулевой. Мы в док-ве воспользовались $(Ax, y) = (x, A^Ty)$ (просто расписать)

   $$A^Tb = A^TAx^*$$

   $$A^TAx^* = A^Tb$$

   $$A^T(Ax^* - b) = 0 \ \Rightarrow \ Ax^* - b \perp L \text{ (аналогично)}$$

   $$\Rightarrow b = \underset{\in L}{Ax^*} - (\in \in L^{\perp}Ax^* - b)$$

2. $Ax = 0 \Leftrightarrow A^TAx = 0$. В $(\Rightarrow)$ - очевидно.
   Пусть $A^TAx = 0 \Rightarrow x^TA^TAx = 0 \Rightarrow (Ax)^*Ax \Leftrightarrow Ax = 0$
   Будем говорить в этом случае (немного некорректно), что x лежит в ядре матрицы A. Теперь к пункту 2.

   $(\Rightarrow)$:

   $$A^TA \in \mathrm{GL}_n(\mathbb{R}) \Rightarrow \operatorname{Ker} A^TA = \{0\} \Rightarrow \operatorname{Ker} A = \{0\}$$

   Значит Ax - не имеет решения кроме нулевого. Но это ЛК столбцов матрицы. Значит столбцы матрицы A - ЛН. Значит она имеет полный ранг. Ч.т.д.

   $(\Leftarrow)$:
   Ранг равен m $\Rightarrow$ столбцы ЛН $\Rightarrow Ax = 0 \Rightarrow x = 0$
   Но знаем, что ядро у матриц в $Ax = 0 \Leftrightarrow A^TAx = 0$ равны нулю $\Rightarrow A^TA$ - обратимо

Теорема

$$A = UDV^T \qquad A \in M_{n,m}(\mathbb{R}) \qquad D \in M_{n,m}(\mathbb{R})$$

Док-во

D - как бы диагональна. А все диагональные элементы вещ. неотриц. числа, приведем её так:

$$D = \begin{pmatrix} \lambda_1 & 0 & 0 & 0 \\ 0 & \vdots & 0 & 0 \\ 0 & 0 & \lambda_k & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$D^+ = \begin{pmatrix} \lambda_1^{-1} & 0 & 0 & 0 \\ 0 & \vdots & 0 & 0 \\ 0 & 0 & \lambda_k^{-1} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \qquad D^+ \in M_{m,n}(\mathbb{R})$$

$$A^+ = VD^+U^T$$

x^* - решение МНК $Ax = b \Leftrightarrow x^* = A^*b$

$$A^TAx^* = A^Tb$$

$$A^TAA^+b \stackrel{?}{=} A^+b$$

$$VD^T\cancel{U^T}UDV^T\cancel{V}D^+U^Tb \stackrel{?}{=} VD^TU^Tb$$

$$V\underbrace{D^TDD^+}_{=D^T}U^Tb$$

Опр

$$\|A\| \stackrel{\text{def}}{=} \sup_{x \neq 0} \frac{\|Ax\|}{\|x\|} = \sup_{\|y\|=1} \|Ay\|$$

Свойства

1. $\|\lambda A\| = |\lambda| \, \|A\|$

2. $\|A + B\| \geqslant \|A\| + \|B\|$

$$\sup_{\|y\|=1} \|(A+B)y\| \leqslant \sup_{\|z_1\|=1} \|Az_1\| + \sup_{\|z_2\|=1} \|Bz_2\|$$

Пусть sup достигается в z_1, z_2

$$\|Az_1\| \geqslant \|Ay\|$$

$$\|Az_2\| \geqslant \|Ay\|$$

Подробное док-во: (убидили д-ть)

$$\sup_{\|y\|=1} \|(A+B)y\| = M$$

$$\sup_{\|z_1\|=1} \|Az_1\| = m_1$$

$$\sup_{\|z_2\|=1} \|Az_2\| = m_2$$

$M \leqslant m_1 + m_2$

$$\forall z : \|z\| = 1 \qquad \|Az\| \leqslant m_1$$

$$\|Bz\| \leqslant m_2 \Rightarrow \|(A+B)z\| \leqslant \|Az\| + \|Bz\| \leqslant m_1 + m_2$$

3. $\|UA\| = \|AV\|\|A\|,$ если U,V - ортогон. матрицы (очевидно)

$$\|UA\| = \sup_{\|y\|=1} \|UAy\| = \sup_{\|y\|=1} \|Ay\| = \|A\|$$

4. $\|A\| = \sigma_1(A)$ - наибольшее сингулярное число. Как его получить? Взяли сингулярное разложение $A = UDV^T$. На диагонали D выбираем наибольшее сингулярное число

2019-11-12

Док-во

$$D = \begin{pmatrix} \sigma_1 & & 0 \\ & \ddots & \\ 0 & & \sigma_k \end{pmatrix}$$

$$A = UDV^T$$

$$\|A\| = \|D\| = \sup_{x \neq 0} \frac{\|D_x\|}{\|x\|} = \sup_{x \neq 0} \frac{\sqrt{(\sigma_1 x_1)^2 + (\sigma_2 x_2)^2 + ... + (\sigma_k x_k)^2}}{\sqrt{x_1^2 + ... + x_n^2}}$$

Задача

Необходимо сжать изображение. Мы хотим сделать так, чтобы фотография занимала меньше места на компьютере. Формально, мы ищем матрицу, которая близка к исходной.

Док-во

$$A \in M_{m,n}(\mathbb{R}) \qquad m \geqslant n$$

$$\hat{A} \in M_{m,n}(\mathbb{R}) \qquad \|A - \hat{A}\| \to \min \qquad \operatorname{rk} \hat{A} \leqslant r$$

Мы можем измерить объем информации рангом матрицы и хранить ЛНЗ строки и линейные комбинации

$$A = UDV^T$$

$$U = (U_1 U_2)$$

$$V = (V_1 V_2)$$

$$U_1 \in M_{m,r}(\mathbb{R})$$

$$V_1 \in M_{n,r}(\mathbb{R})$$

$$D = \begin{pmatrix} D_1 & 0 \\ 0 & D_2 \end{pmatrix} \qquad D_1 \in M_r(\mathbb{R})$$

$$\hat{A} = U_1 D_1 V_1^T$$

$$\hat{A} = U \begin{pmatrix} D_1 & 0 \\ 0 & 0 \end{pmatrix} V^T$$

$$\|A - \hat{A}\| = \|U \begin{pmatrix} 0 & 0 \\ 0 & D_2 \end{pmatrix} V^T\| = \|\begin{pmatrix} 0 & 0 \\ 0 & D_2 \end{pmatrix}\| = \sigma_{r+1}$$

$$B \in M_{m,n}(\mathbb{R}) \overset{?}{\Rightarrow} \|A - B\| \geqslant \sigma_{r+1}$$

$$\operatorname{rk} B = r$$

$$\operatorname{rk} B = r \ \Rightarrow \ B = XY^T, \qquad X \in M_{m,r}(\mathbb{R}) \quad Y \in M_{n,r}(\mathbb{R})$$

Матрица Y образована из ЛНЗ строк из B. Каждая строка B записывается как ЛК этих строчек. X - матрица коэфф.

$$\mathcal{Y} \text{ - линейная оболочка столбцов } Y \quad (\text{в } \mathbb{R}^n)$$

$$\dim \mathcal{Y} \leqslant r$$

Можно взять орт. дополнение

$$\Rightarrow \dim \mathcal{Y}^\perp \geqslant n - r$$

$$\hat{\mathcal{V}} \text{ - линейнвя оболочка первых } r+1 \text{ столбцов } V \qquad (\text{ в } \mathbb{R}^n)$$

$$\dim \hat{\mathcal{V}} = r + 1$$

У них есть нетрив. пересеч. по формуле размерностей подрв-в

$$\Rightarrow \exists\, w \in \hat{\mathcal{V}} \cap \mathcal{Y}^\perp \qquad w \neq 0$$

$$\|w\| = 1$$

$$w \in \mathcal{Y}^\perp \ \Rightarrow \ Y_w^T = 0$$

$$w \in \hat{\mathcal{V}} \ \Rightarrow \ w = V \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_{r+1} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

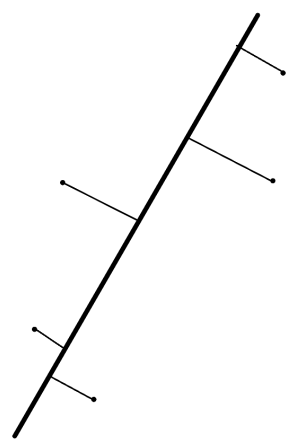
$$\|A-B\|^2 \geqslant \|(A-B)w\|^2 = \|Aw\|^2 = \|UDV^TV \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_{r+1} \\ 0 \\ \vdots \\ 0 \end{pmatrix}\|^2 = \|D \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_{r+1} \\ 0 \\ \vdots \\ 0 \end{pmatrix}\|^2$$

$$= \sigma_1^2 \gamma_1^2 + ... + \sigma_{r+1}^2 \gamma_{r+1}^2 \geqslant \sigma_{r+1}^2$$

$$1 = \|w\| = \|V \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_{r+1} \\ 0 \\ \vdots \\ 0 \end{pmatrix}\| = \| \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_{r+1} \\ 0 \\ \vdots \\ 0 \end{pmatrix}\| = \sqrt{\gamma_1^2 + ... + \gamma_{r+1}^2}$$

Задача

В n - мерном пр-ве есть набор точек и нам нужно найти подпр-во заданной размерности, которое приближает этот набор точек. Что значит приближает? Это наилучшая аппроксимакция этих точек. Берем точки и их проекции. Складываем расстояния в квадрате для каждой точки.



прямая, которая аппроксимирует точки

Дисперсия - сумма квадратов отклонений от среднего значения (центр массы)

$$x_1, ..., x_m \in \mathbb{R}^n$$

$$\dim L = k \qquad L = \underset{\text{ортнорм}}{< u_1, ..., u_k >}$$

$$\mathrm{pr}_L\, x = \sum_{i=1}^{k} (u_i, x) u_i = \begin{pmatrix} u_1 & ... & u_k \end{pmatrix} \begin{pmatrix} (u_1, x) \\ \vdots \\ (u_k, x) \end{pmatrix}$$

$$U = (\begin{pmatrix} u_1 & \dots & u_k \end{pmatrix}) \in M_{n,k}(\mathbb{R}) =$$

$$= \begin{pmatrix} u_1 & \dots & u_k \end{pmatrix} \begin{pmatrix} u_1^T \\ \vdots \\ u_k^T \end{pmatrix} x = UU^T x$$

$$U^T U = I_k$$

$$\min \sum_{i=1}^{m} \|(I_n - UU^T)(x_i - u_0)\|^2$$

$$U \in M_{n,k}(\mathbb{R})$$

$$U^T U = I_k$$

$$u_0 \in \mathbb{R}^n$$

Любое подпр-во проходит через ноль, но мы хотим избавиться от этого ограничения. Мы можем перенести наше под-прво. u_0 - вектор сдвига. Или мы сдвигаем все точки на u_0.

Док-во (решение)

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \in M_{m,n}(\mathbb{R})$$

$$\overline{x} = \frac{1}{m} \sum_{i=1}^{m} x_i \text{ - центр масс}$$

$$\widetilde{X} = X - \begin{pmatrix} \overline{x} \\ \vdots \\ \overline{x} \end{pmatrix} \text{ центрированная матрица } \quad \in M_{m,n}(\mathbb{R})$$

$$\widetilde{X}^T \widetilde{X} \in M_n(\mathbb{R})$$

У этой матрицы есть система из онорм с.в. А соотв. с.ч. вещ. неотр.
Упорядочим с.в. по величине с.ч.
Берем первые k с.в., где k - размер нужного подпр-ва
Нужно взять $u_0 = \overline{x}$

Теорема

Такая задача о минимизации имеет след. решение. Взять $u_0 = \overline{x}$
Взять в качестве U матрицу, сост из первых k веторов матрицы $\widetilde{X}^T \widetilde{X}$, упорядоч. по собс. числу

Лемма

$$\frac{1}{m}\sum_{k=1}^{m}\|y_i - b\|^2 = \frac{1}{m}\sum_{i=1}^{m}\|y_1 - \overline{y}\|^2 + \|\overline{y} - b\|^2$$

$$\overline{y} = \frac{1}{m}\sum_{i=1}^{m} y_i$$

Док-во

$$\frac{1}{m}\sum\|y_1 - b\|^2 = \frac{1}{m}\sum\|(y_1 - \overline{y}) + (\overline{y} - b)\|^2 = \frac{1}{m}\sum\|y_1 - \overline{y}\|^2 + \|\overline{y} - b\|^2 +$$

$$+\frac{2}{m}\sum_{i=1}^{m}(y_1 - \overline{y}, \overline{y} - b) =$$

$$= \frac{1}{m}\sum\|y_1 - \overline{y}\|^2 + \|\overline{y} - b\|^2 + \frac{2}{m}(\underset{=0}{\sum_{i=1}^{m}(y_i - \overline{y})},\ \overline{y} - b)$$

2019-11-19

Док-во (теоремы)

Минимизация в $u_0 = \widetilde{x}$, задача свелась к:

$$\min_{U^T U = I_n} \sum_{i=1}^{m} \|(I - UU^T)(x_i - \overline{x})\|^2$$

$$\sum_{i=1}^{m} \|(I - UU^T)(x_i - \overline{x})\|^2 \overset{1}{=} \sum_{i=1}^{m} \|x_i - \overline{x}\|^2 - \sum_{i=1}^{m} \|U^T(x_i - \overline{x})\|^2 \overset{2}{=}$$

$$= \sum_{i=1}^{m} \|x_i - \overline{x}\| - \operatorname{Tr}(U^T \widetilde{X}^T \widetilde{X} U)$$

Откуда взялись равенства? Объясним первое:

$$\|(I - UU^T)(x_i - \overline{x})\|^2 = \|x_i - \overline{x}\|^2 - 2\underbrace{(x_i - \overline{x},\ UU^T(x_i - \overline{x}))}_{(*)} + \|UU^T(x_i - \overline{x})\|^2$$

т.к. было: $(U^T a,\ b) = (a,\ Ub)$

$$\Rightarrow (*) = (U^T(x_i - \overline{x}),\ U^T(x_i - \overline{x})) \overset{\text{U -трансп.}}{=} (U^T(x_i - \overline{x}),\ U^T UU^T(x_i - \overline{x})) \overset{\text{лемма}}{=}$$

$$= \|UU^T(x_i - \overline{x})\|^2$$

Замечание: посмотрев на первое равенство, понимаем, что задача эквивалентна задаче про максимизации, которая стоит с минусом, а его можно записать как $\|UU^T(x_i - \overline{x})\|^2$.

Это и есть дисперсия (т.е. второй способ формулировки задачи: мы ищем пр-во, дисперсия проекций на которую максимальна)

Теперь объясним второй переход:

$$\sum_{i=1}^{m} \|U^T(x_i - \overline{x})\|^2 \overset{?}{=} \operatorname{Tr}(U^T \widetilde{X}^T \widetilde{X} U)$$

$$x_i - \overline{x} = \begin{pmatrix} x_{i1} \\ \vdots \\ x_{in} \end{pmatrix} \qquad \widetilde{X} = \begin{pmatrix} x_{11} & \dots & x_{1n} \\ \vdots & & \vdots \\ x_{n1} & \dots & x_{nn} \end{pmatrix}$$

$$U^T = \{u_{\alpha\beta}\}$$

$$U^T \widetilde{X} = \begin{pmatrix} \sum_\beta u_{1\beta} x_{i\beta} \\ \vdots \\ \sum_\beta u_{k\beta} x_{i\beta} \end{pmatrix}$$

$$\text{ЛЧ (в ?)} = \sum_{\alpha=1}^{k} \sum_{i=1}^{m} (\sum_{\beta=1}^{n} u_{\alpha\beta} x_{i\beta})^2$$

Обозначим $U^T \widetilde{X}^T = A$, хотим найти $\operatorname{Tr} AA^T$, который равен сумме квадратов элементов этой матрицы:

$$A = \{a_{ij}\} \qquad (AA^T)_{ik} = \sum_j a_{ij} a_{kj} \Rightarrow \operatorname{Tr} AA^T = \sum_i \sum_j a_{ij} a_{ij}$$

То есть ПЧ = ЛЧ

Задача свелась к:

$$\max_{U^T U = I} Tr(U^T \widetilde{X}^T \widetilde{X} U)$$

Лемма

D - диагональная матрица, с упорядоченными по убыванию с.ч.:

$$D = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

$$\lambda_1 \geqslant ... \geqslant \lambda_n$$

Докажем, что $\max\limits_{\substack{W \in M_{n,k}(\mathbb{R}) \\ W^T W = I}} \operatorname{Tr}(W^T D W)$ при $W = \begin{pmatrix} I_k \\ 0 \end{pmatrix}$

Док-во

$$W^T = \{w_{ij}\} \qquad c_j = \sum_{i=1}^{k} w_{ij}^2$$

$$\operatorname{Tr}(W^T D W) = \sum_{i,j} \lambda_j W_{ij}^2 = \sum_{j=1}^{n} \lambda_j$$

Что мы знаем про c_j?

1. $\sum\limits_{j=1}^{n} c_j \overset{\text{т.к. столбцы ортонорм.}(W^TW=I)}{=} k$
   (сумма квадратов по строчкам равна сумме квадратов по столбцам, но все они равны 1, а их k штук)

2. $0 \leqslant c_j \leqslant 1$
   (у матрицы W столбцы ОНБ вектора, любой набор ОН может дополнен до ОНБ, тогда матрица будет ортоганальной, но у нее ОН строчки, в частности сумма квадратов элементов 1, значит у недополненной $\leqslant 1$)

Задача свелась к тому, чтобы д-ть:

$$\sum_{j=1}^{n} \lambda_j \leqslant \sum_{j=1}^{k} \lambda_j$$

(в качестве c_j взять первые k единиц, остальные 0)

$$\lambda_1 + ... + \lambda_k - \lambda_1 c_1 - ... - \lambda_n c_n \overset{\text{по } 1}{=}$$

$$= \lambda_1 + ... + \lambda_k - \lambda_1 c_1 - ... - \lambda_k c_k - \lambda_{k+1}(k - c_1 - ... - c_k - c_{k+2} - ... - c_n) -$$

$$-\lambda_{k+2} c_{k+2} - ... - \lambda_n c_n =$$

$$= (\lambda_1 - \lambda_{k+1})(1 - c_1) + ...(\lambda_k - \lambda_{k+1})(1 - c_n) + (\lambda_{k+1} - \lambda_{k+2}) c_{k+2} + ...(\lambda_{k+1} - \lambda_n) c_n \geqslant 0$$

$$\widetilde{X}^T \widetilde{X} = S^T D S, \quad S \in Q_n(\mathbb{R}), \quad \text{D - диаг}$$

$$\max_{\substack{W \in M_{n,k}(\mathbb{R}) \\ W^TW = I}} \operatorname{Tr}(U^T \widetilde{X}^T \widetilde{X} U) = \operatorname{Tr}(()^T D())$$

<u>Док-во</u> (продолжение д-ва теоремы)

$$\widetilde{X}^T \widetilde{X} = (S^T D S) S^T \underset{\text{на i}}{\begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}} = S^T D \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} = S^T \begin{pmatrix} 0 \\ \vdots \\ \sigma_i \\ \vdots \\ 0 \end{pmatrix} = \sigma_i S^T \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$$

$$(S^T D S) S^T \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \text{ - с.в. с с.ч. } \sigma_i\text{. U состоит их таких столбцов}$$

Такое решение называется методом главных компонент (PCA)

2019-11-19

3 Конечные поля

Кольцом R будем называть ассоциативное коммутативное кольцо с 1

Опр

$I \subset R$ - идеал, если:

1. $\forall a, b \in I \quad a + b \in I$
2. $\forall a \in I,\ r \in R \quad ra \in I$

Пример

Четные числа - идеал кольца целых чисел

Замечание

Идеал - аддитивная группа кольца

Идеал - подгруппа аддитивной группы

Опр (конструкция)

$$a_1, ..., a_n \in R$$

$$(a_1, ..., a_n) = \{r_1 a_1 + ... + r_n a_n, \quad r_i \in R$$

Утв

Это множество является идеалом

Пример

Четные числа - идеал (2)

Опр

Идеал, порожденный одним элементом называется главным идеалом

$$(a) = \{ra, \quad r \in R\}$$

Свойства

1. $a \vdots b \Leftrightarrow (a) \subset (b)$
2. $a \sim b \Leftrightarrow (a) = (b)$ (ассоциировано)

Док-во (1)

($\Leftarrow$):

$$a \,\vdots\, b \;\Rightarrow\; a = bc$$

$$ra = rcb$$

($\Rightarrow$):

$$(a) \subset (b) \;\Rightarrow\; a \in (b)$$

$$\Rightarrow a = bc \;\Rightarrow\; a \,\vdots\, b$$

Теорема

Любой идеал $\mathbb{Z}$ (и $K[x]$) - главный

Док-во (для $\mathbb{Z}$)

I - идеал в $\mathbb{Z}$
Пусть a - минимальный положительный элемент этого идеала

$$b \in I$$

Поделим b на a с остатком:

$$b = aq + c, \quad 0 \leqslant c < a$$

$$a \in I \;\Rightarrow\; aq \in I$$

$$b \in I \;\Rightarrow\; b - aq \in I \;\Rightarrow\; c \in I$$

Значит $c \in I$ и $0 \leqslant c < a \;\Rightarrow\; c = 0$
Значит любой элемент делитсянацело на a
Доказали, что $I \subset (a)$
Но $a \in I \;\Rightarrow\; ar \in R$, доказали

Док-во (для $K[x]$)

Как доказать для кольца многочленов?
Вместо минимального положительного возьмем многочлен минимальной степени, который лежит в идеале. Дальше также. Берем любой, делим на мн-н минимальной степени. Степень остатка меньше степени исходного мн-на

Теорема

В $\mathbb{Z}$ (в $R[x]$)

$$(a, b) = (\text{НОД}(a, b)) \qquad \text{НОД}(a, b) =: d$$

Док-во ($\mathbb{Z}$)

$(a, b) \subset (\text{НОД}(a, b))$:

$$ra + sb = xd \in (d)$$

Возьмем xd

По теореме о линейном представлении: $t_1 a + t_2 b = d$

$$\Rightarrow xd = (t_1 x)a + (t_2 x)b \in (a, b)$$

Док-во (в $\boldsymbol{R[x]}$)

Аналогично

Опр

$I \subset R$ Идеал является подгруппой аддитивной группы кольца, которая коммунитативна.

Профакторизуем: $R/_I$ (фактор-группа по сложению)
Сложение такое же.
Умножение: $\overline{a} \cdot \overline{b} \overset{def}{=} \overline{ab}$

$$\left.\begin{array}{l} \overline{a} = \overline{a'} \\ \overline{b} = \overline{b'} \end{array}\right| \overset{?}{\Rightarrow} \overline{ab} = \overline{a'b'}$$

$$\begin{array}{lll} a - a' \in I & a' = a + s, & s \in I \\ b - b' \in I & b' = b + t, & t \in I \end{array}$$

Перемножим равенства:

$$a'b' - ab = at + sb + st \overset{\text{т.к. каждый} \in I}{\in} I$$

Утв

$R/_I$ - кольцо (ком., асс., с 1)

Замечание

Достаточно д-ть:

1. $(\overline{a}\overline{b})\overline{c} = \overline{a}(\overline{b}\overline{c})$
2. $\overline{a}\overline{b} = \overline{b}\overline{a}$
3. $\overline{1}\overline{a} = \overline{a}$
4. $\overline{a}(\overline{b} + \overline{c}) = \overline{a}\overline{b} + \overline{ac}$

Док-во

Докажем коомунитативность:

$$\overline{a} \cdot \overline{b} = \overline{ab} = \overline{ba} = \overline{b} \cdot \overline{a}$$

(остальные аналогично)

У нас полочилось новое кольцо, которое мы будем называвать фактор-кольцом ($\mathbb{R}/_{I}$) по идеалу I

Напоминание

$$\mathbb{Z}/_{p\mathbb{Z}}$$

Утв

$k[x]/_{(f)}$ - поле (f - непр.)