



Санкт-Петербургский государственный университет

Лекции по алгебре

3 семестр, преподаватель Демченко О. В.
Записали Костин П.А. и Шукин И.В.¹

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

Содержание

1	Теория групп	4
1.1	Простейшие св-ва групп	4
1.2	Теорема Лагранжа	7
1.3	Циклическая группа	7
1.4	Изоморфные группы	8
1.5	Теорема о циклических группах	9
1.6	Сопряжение элемента	10
1.7	О классах смежности	11
1.8	Про коммутанты	12
1.9	Гомоморфизм	13
1.10	Свойства гомоморфизма	15
1.11	Основная теорема о гомоморфизме	16
1.12	Действие группы на множестве	17
1.13	Stab и Orb	18
1.14	Лемма Бернсайда	19
2	Евклидовы и унитарные пр-ва	20
2.1	Скалярное умножение	20
2.2	Матрица Грама	21
2.3	Норма	22
2.4	Нер-во Коши - Буняковского	23
2.5	Ортогональное дополнение	24
2.6	Ортогональная проекция	26
2.7	Ортогональный базис	26
2.8	Ортогональная матрица	28
2.9	О линейных функционалах	29
2.10	Унитарные пространства	30
2.11	Сопряжение?	30
2.12	Сопряженная матрица	31
2.13	Эрмитов сопряженный оператор	32
2.14	33
2.15	Унитарный оператор	33
2.16	Поворот	35
2.17	Теорема Эйлера	35
2.19	Про композицию поворотов	37
2.20	Теорема. Унитарный оператор имеет ОНБ из с.в.	37
2.21	Теорема про унитарную матрицу	38
2.22	Эрмитова матрица и самосопряженный оператор	38
2.23	Теорема про самосопряженный оператор	40

2.23	Теорема про эрмитову матрицу	40
2.24	Singular value decomposition	42
2.25	Квадратичные формы над \mathbb{R}	44
2.26	Применение сингулярного разложения	45
2.27	Норма	47
2.31	Лемма для теоремы о минимизации	55
3	Конечные поля	57

1 Теория групп

2019-09-17

Опр (группа)

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

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

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

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

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

Примеры

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

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

$$3. (R, +) - \text{группа кольца}$$

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

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

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

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

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

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

Теорема (св-ва степени)

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. $g^m = e \Rightarrow m \geq n$

Порядок может быть бесконечным

Примеры

1. $D_4 \quad \text{ord}(\text{поворот } 90^\circ) = 4$

$$D_4 \quad \text{ord}(\text{поворот } 180^\circ) = 2$$

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

$$m = nq + r, \quad 0 \leq r < n$$

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

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

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

$$2. D_4$$

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

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

Док-во (эквивалентность)

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

Опр

$[a] = \{b : a \sim b\}$ 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? $gh_1 = gh_2 \xrightarrow{*g^{-1}} h_1 = h$

Теорема (Лагранжа)

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

2019-09-10

Следствие

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

Док-во

$\{a^0 = e, a^1, \dots, a^{m-1}\}$ - подмножество H

Докажем, что все остальные элементы тоже здесь есть

$$n \in \mathbb{Z} \Rightarrow n = mq + r, \quad 0 \leq r < m$$

$$a^n = a^{mq+r} = (a^m)^q a^r = a^r$$

$$a^k = a^l, \quad 0 \leq k < l < m, \text{ умножим на } a^{-k}$$

$$e = a^{l-k}, \quad 0 < l-k < m \text{ и } m \text{ - наименьшее } \mathbb{N} \text{ такое что } a^m = e$$

$$l-k = 0 \Rightarrow l = k$$

Докажем, что $|H| = m$

$\Rightarrow |G| : m = \text{ord } a$, т.о. в группе порядок эл-та - делитель порядка группы

Напоминание (теорема Эйлера)

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

Док-во

Рассмотрим $G = (\mathbb{Z}/n\mathbb{Z}, *)$ $|G| = \varphi(n)$

$$\bar{a} \in G, \text{ord } \bar{a} = k$$

$$\varphi(n) : k \Rightarrow \varphi(n) = kl$$

$$\bar{a} = \bar{1}$$

$$\bar{a}^{\varphi(n)} = \bar{1}$$

Опр

G - циклическая группа, если $\exists g \in G : \forall g' \in G : \exists k \in \mathbb{Z} : g' = g^k$

Такой g называется 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 $(g, h) * (g', h') \stackrel{def}{=} (g *_G g', h *_H h')$

Докажем, что это группа.

Доказательство ассоциативности: $((g, h)(g', h'))(g'', h'') \stackrel{?}{=} (g, h)((g', h')(g'', h''))$

$(gg', hh')(g'', h'') \stackrel{?}{=} (g, h)(g'g'', h'h'')$

$((gg')g'', (hh')h'') \stackrel{?}{=} (g(g'g''), h(h'h''))$ - очевидно

Нейтральный элемент:

Рассмотрим $\mathbb{Z}/_2\mathbb{Z} \times \mathbb{Z}/_2\mathbb{Z} = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1})\}$

Опр

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

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 φ - изоморфизм

Примеры

$$1. D_3 \rightarrow S_3$$

$$2. U_n = \{z \in \mathbb{C} : z^n = 1\} \leftarrow \mathbb{Z}/_n\mathbb{Z}$$

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

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

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

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

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) $G = \{\dots, g^{-1}, e, g, g^2, \dots\}$ (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 закликивается 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

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

Док-во

$$\begin{aligned} g \in G, g \neq e, \text{ord } g = p \\ \Rightarrow G = \{e = g^0, g, \dots, g^{p-1}\} \end{aligned}$$

УТВ

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

Док-во

$$\text{Пусть } g^n = e, \quad \varphi(g^n) = \varphi(e) \stackrel{?}{=} e$$

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

Теперь докажем, что меньшего нет

$$\varphi(g)^m = e, \quad m \in \mathbb{N} \stackrel{?}{\Rightarrow} m \geq n$$

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

Опр

$H < G$, тогда H - нормальная 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

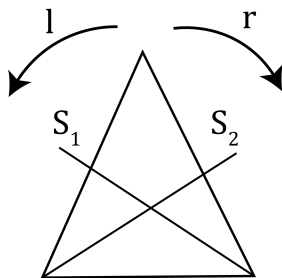
Элементы подгруппы при сопряжении переходят в элементы подгруппы

Замечание

Подгруппа любой коммутативной 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 клЗассы 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 (корректности)

Хотим проверить, что

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

Аналогично прошлому доказательству

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

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

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

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

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

$$\tilde{g}_1\tilde{g}_2H = g_1h_1g_2h_2h = g_1g_2(\underbrace{g_2^{-1}h_1g_2}_{=h_3})h_2h$$

Осталось доказать, что получается группа

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

$$2) \text{ Ассоциативность } (g_1H + g_2H) * g_3H \stackrel{?}{=} g_1H * (g_2H * g_3H) \\ (g_1g_2)H * g_3H = (g_1g_2)g_3H$$

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

$$G/H$$

Была эквивалентность: $a \sim b \Leftrightarrow a - b \in H$

$$G = \mathbb{Z}$$

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

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

Коммутант - множество произведений всех возможных коммутаторов

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

Док-во (коммутант - подгруппа)

$$K(G) < G$$

Нейтральный элемент: $[e, e] = e$

Обратный элемент? $[g_1, h_1] \dots [g_n, h_n]$

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

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

Значит это подгруппа

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

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

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

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

$$g_1 g_2 K(G) = g_1 g_2 K(G) \quad g_2 K(G) g_1 K(G) = g_2 g_1 K(G)$$

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

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

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

Инъективность:

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

На самом деле достаточно было проверить одно

Опр

$\varphi : G \rightarrow H$ - гомоморфизм, если $\varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2)$

изоморфизм = гомоморфизм + биекция

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

Примеры

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

$$z \rightarrow |z|$$

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

$$A \rightarrow \det A$$

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

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

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

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

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

2019-09-24

Напоминание $G/K(G)$ - коммутативнаУТВ $H \triangleleft G \quad G/H$ - 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

Ker и 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

$\text{Ker } f$ - нормальная подгруппа G

Док-во

$$\text{Ker } f \triangleleft G?$$

$$g \in G \quad a \in \text{Ker } f$$

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

УТВ (основная теорема о гомоморфизме)

$$G/\text{Ker } f \cong \text{Im } f$$

Док-во

Докажем, что это корректное отображение:

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

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

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

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

Докажем, что 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

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

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

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)

$$G \times H \rightarrow G$$

$$(g_1 h) \rightarrow g$$

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

1.12 Действие группы на множествеОпр

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)

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

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

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

$$E_v = v$$

Пример (2)

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

$$G = D_4$$

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

$$M = G$$

$$gm = gm$$

Опр

$$m \in M$$

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

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

УТВ

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

Док-во

Доказательство того, что стабилизатор - подгруппа:

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

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

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

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

$$gm = m$$

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

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

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

Док-во

$$\text{Stab } m = H$$

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

$$gH \rightarrow gm$$

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)

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

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

2019-10-01

Напоминание

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

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

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-ваОпр

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

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

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

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

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

противоречие

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

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

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

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

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

Опр

V - в.п. над \mathbb{R}

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

$v \rightarrow \|v\|$ - норма

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

2. Нер-во треугольника

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

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

Если такое отобр. существует, то оно называется нормой

УТВ

(u, v) - ск. произв.

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

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

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

$$\Gamma_e x + C_y = 0$$

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

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

$$\Gamma_e x + C_y = 0$$

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

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

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

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

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

Свойства (орт. проекции)

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

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

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

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

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

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

Опр

e_1, \dots, e_n - базис V

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

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

Алгоритм

Процесс ортогонализации Грамма-Шмидта:

e_1, \dots, e_n - базис

Хотим ортонормированный f_1, \dots, f_n :

$$(f_1, \dots, f_k) = (e_1, \dots, e_k) \quad \forall 1 \leq k \leq n :$$

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

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

Пример

$$\mathbb{R}^n$$

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

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

Пример

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

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

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

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

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

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

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

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

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

УТВ

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

Следующие утверждения равносильны:

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

$$2 \rightarrow 1$$

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

$$3 \rightarrow 2$$

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

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

$$1 \rightarrow 3$$

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

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

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

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

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

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

2019-10-22

Опр (унитарного пространства)

U - в.п. над \mathbb{C}

$(\cdot, \cdot) : U \times U \rightarrow \mathbb{C}$ - эрмитово скал. произведение

$$1. (u + v, w) = (u, w) + (v, w) \quad \forall u, v, w \in U$$

$$(\lambda v, w) = \lambda(v, w) \quad \forall \lambda \in \mathbb{C}, \quad v, w \in U$$

$$2. (u, v) = \overline{(v, u)}$$

$$3. (u, u) \geq 0$$

$$4. (u, u) = 0 \Rightarrow u = 0$$

$(U, (\cdot, \cdot))$ - унитарное пространство

Пример

$$(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^n x_i y_i \quad \Bigg| \quad (\mathbf{x}, \mathbf{y}) = \sum_{i=1}^n x_i \overline{y_i}$$

e_1, \dots, e_n - базис

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

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

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

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

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

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

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

$$(u, v) = |(u, v)| \cdot z \Rightarrow |z| = 1$$

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

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

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

Доказали КБШ

Опр

V - в.п. над K

$V^* = \mathcal{L}(V, K)$ - двойственное пр-во

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. φ - 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

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

$A^* = \bar{A}^T$ - эрмитово-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, $L \in \mathcal{L}(V)$, $u \in V$

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

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

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

$$u \rightarrow w_u$$

Утверждается, что отображение линейно

Док-во

$$\begin{aligned} (Lv, u) = (v, w_u) \quad \Bigg| \quad (Lv, u+u') &= (Lv, u) + (Lv, u') = \\ (Lv, u') &= (v, w_{u'}) \quad \Bigg| = (u, w_u) + (v, w_{u'}) = (v, w_u + w_{u'}) = (v, w_{u+u'}) \end{aligned}$$

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

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

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

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

$$v = w - w'$$

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

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

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

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

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

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

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

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

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

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)

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

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

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

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

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

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

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

$(4 \Rightarrow 2)$:

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

$(2 \Rightarrow 4)$:

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

$$L^*L = \text{id}_V$$

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 λ и туда переносится $\bar{\lambda}$

2019-3-29

Опр

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

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

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

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

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

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

$$\cos \varphi \sin \psi + \sin \varphi \cos \psi = 0$$

$$= \sin(\varphi + \psi)$$

$$\cos \varphi \cos \psi - \sin \varphi \sin \psi = 0$$

$$= \cos(\varphi + \psi)$$

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

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

Опр

Если L - 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 ортогональное отображение с определителем 1 является поворотом относительно некоторой оси

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

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. $\lambda_1 \lambda_2 \lambda_3 = \lambda_1 \overline{\lambda_2} \lambda_3 = \lambda_1 \underbrace{|\lambda_3|^2}_{=1} = \lambda_1$

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:

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

То есть результат 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 ортогональным 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 поворот. То есть у нас есть пространство с осью, на которую оператор действует тождественно, а на другое он действует как поворот.

УТВ

Если L - ортогональный оператор в пр-ве с определителем -1 равен композиции поворота, 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

$$Lv = \lambda v$$

$$\langle v, v \rangle = 1$$

Хотим доказать, что подпространство инвариантно относительно действия L :

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

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

(*) 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 к сужению. На этом ортогональном дополнении у оператора есть базис ортогональных векторов. Добавим к нему ортонормированный вектор v . Очевидно, получим ортонормированный базис из собственных векторов всего пр-ва

Переформулируем на языке матриц

Теорема

U - унитарная матрица, тогда:

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

Док-во

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

e - 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

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

(*) 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

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

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

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

Опр

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

$L \in \mathcal{L}(V)$ - 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. $Lv = \lambda v \quad Lu = \mu u \quad \lambda \neq \mu \Rightarrow (u, v) = 0$

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

2019-10-29

Теорема

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

$$Lv = \lambda v$$

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

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

Тут мы должны задать вопрос.

Опр

A - эрмитова матрица

$\Rightarrow M$ - унитарная

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

Теорема

A - эрмитова матрица

Тогда условия равносильны

1. $\forall x \in \mathbb{C}^n \quad x^*Ax > 0 \quad (x^*Ax)^* = x^*A^*x = x^*Ax$
 $x \neq 0$ $\in \mathbb{R}$
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

$$4 \rightarrow 1$$

$$A = P^*P$$

$$x^*Ax = x^*P^*Px = (Px)^*(Px) = \langle Px, Px \rangle$$

$$\langle a, b \rangle = \sum a_i \bar{b}_i \quad \text{Стандартное эрмитово скал. произв. в } \mathbb{C}$$

$$2 \rightarrow 4$$

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

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

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

$$1 \rightarrow 2$$

$$Ax = \lambda x$$

$$x^*_{>0} Ax = x^* \lambda x = \lambda x^* x = \lambda < x, x >_{>0}$$

$$1 \rightarrow 3$$

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

$$A' = P * P$$

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

$$3 \rightarrow 2$$

Индукция по размеру A

Когда матрица 1×1 очев.

Инд. переход : $n \rightarrow n + 1$

Пусть λ - с.ч A , $\lambda < 0 \Rightarrow \exists \mu < 0$

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

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

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

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

$$\begin{aligned} u'^* A' u' &= u^* A u = |\alpha|^2 x^* A x + |\beta|^2 y^* A y = \quad \text{подставили } u, \text{ которое сверху} \\ &= |\alpha|^2 \underset{<0}{\lambda} \cdot \|x\|^2 + |\beta|^2 \underset{<0}{\mu} \|y\|^2 < 0 \end{aligned}$$

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

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}

Теорема

A - эрмит. матрица

тогда след. условия равносильны

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

Такая матрица называется положительно полуопред.

Док-во

Доказать дома

Опр (Singular value decomposition SVD)

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

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

$$A = USV^*$$

Поворот, растяжение, поворот

Док-во

$$m \leq n$$

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

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

Значит эта матрица положительно полуопред.

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

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

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

$$V = \begin{pmatrix} V_1 & V_2 \end{pmatrix} \quad \begin{matrix} V_1 \in M_{n,k}(\mathbb{C}) \\ k \text{ столб} \end{matrix} \quad \begin{matrix} V_2 \in M_{n,n-k}(\mathbb{C}) \\ n-k \text{ столб} \end{matrix}$$

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

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

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

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

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

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

2019-11-05 Продолжение док-ва:

Док-во

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

Осталось из U_1 и V_1 сделать прямоуг. матрицы $\Rightarrow U_1$ содержит k ортогональных столбцов. Раз они ортогональны, можно дополнить до ортогонального базиса в \mathbb{C}^n и получаем:

$$U = (U_1 U_2) \in M_n(\mathbb{C})$$

Эта матрица ортонормирована из-за ортог. столбцов.

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

$$(U_1 U_2) S (V_1 V_2)^* = U_1 F^{\frac{1}{2}} V_1^* = A$$

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 ортогональные

2.25 Квадратичные формы над \mathbb{R}

Опр

$x = (x_1, \dots, x_n)$, тогда:

$$S(x) = \sum_{i \geq j} a_{ij} x_i x_j - \text{квадратичная форма}$$

Замечание

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

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

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

$$S(x) = x^T Bx$$

$$x = My$$

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

Опр

S - положительно определена, если:

$$1. \forall x \quad S(x) \geq 0$$

$$2. S(x) = 0 \Rightarrow x = 0$$

Замечание

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

Опр

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

Теорема

Любую матрицу можно привести к каноническому виду с помощью элементарного преобразования

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 * ортогональная 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 $\|Ax - b\| \rightarrow \min$

Опр

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

Теорема

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

1. x^* - решение МНК $\Leftrightarrow A^T A x^* = A^T b$
2. $A^T A \in GL_n(\mathbb{R}) \Leftrightarrow \text{rk } A = m$

Док-во

1. x^* - решением МНК \Leftrightarrow

Ax^* - проекция b на линейную оболочку столбцов A

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

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

Почему $v \perp L \Rightarrow A^T v = 0$?

$$\forall e: (Ae, v) = 0 \\ = (e, A^T v)$$

Какой вектор ортогонален произвольному? Только нулевой. Мы в док-ве воспользовались $(Ax, y) = (x, A^T y)$ (просто расписать)

$$A^T b = A^T Ax^*$$

$$A^T Ax^* = A^T b$$

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

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

2. $Ax = 0 \Leftrightarrow A^T Ax = 0$. В (\Rightarrow) - очевидно.

$$\text{Пусть } A^T Ax = 0 \Rightarrow x^T A^T Ax = 0 \Rightarrow (Ax)^* Ax \Leftrightarrow Ax = 0$$

Будем говорить в этом случае (немного некорректно), что x лежит в ядре матрицы A . Теперь к пункту 2.

(\Rightarrow) :

$$A^T A \in GL_n(\mathbb{R}) \Rightarrow \text{Ker } A^T A = \{0\} \Rightarrow \text{Ker } A = \{0\}$$

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) :

$$\text{Ранг равен } m \Rightarrow \text{столбцы ЛН} \Rightarrow Ax = 0 \Rightarrow x = 0$$

Но знаем, что ядро у матриц в $Ax = 0 \Leftrightarrow A^T Ax = 0$ равны нулю $\Rightarrow A^T A$ - обратимо

Теорема

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

Док-во

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

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

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

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

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

$$A^T Ax^* = A^T b$$

$$A^T AA^+b \stackrel{?}{=} A^+b$$

$$VD^T \cancel{U^T} U D V^T \cancel{U} D^+ U^T b \stackrel{?}{=} VD^T U^T b$$

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

Опр

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

Свойства

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

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

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

Пусть \sup достигается в z_1, z_2

$$\|Az_1\| \geq \|Ay\|$$

$$\|Az_2\| \geq \|Ay\|$$

Подробное док-во:

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

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

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

$$M \leq m_1 + m_2$$

$$\forall z : \|z\| = 1 \quad \|Az\| \leq m_1$$

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

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

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

$$A = UDV^T$$

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

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

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

$$\hat{A} \in M_{m,n}(\mathbb{R}) \quad \|A - \hat{A}\| \rightarrow \min \quad \text{rk } \hat{A} \leq r$$

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

$$A = UDV^T$$

$$U = (U_1 U_2)$$

$$V = (V_1 V_2)$$

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

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

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

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

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

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

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

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

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

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

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

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

Можно взять орт. дополнение

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

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

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

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

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

$$\|w\| = 1$$

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

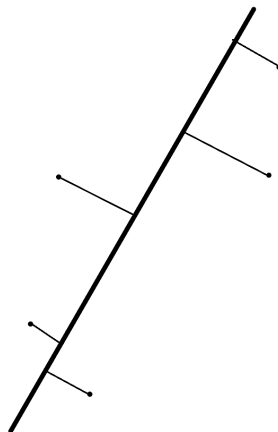
$$w \in \hat{\mathcal{V}} \Rightarrow w = V \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_{r+1} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$\begin{aligned} \|A - B\|^2 &\geq \|(A - B)w\|^2 = \|Aw\|^2 = \|UDV^T V \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_{r+1} \\ 0 \\ \vdots \\ 0 \end{pmatrix}\|^2 = \|D \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_{r+1} \\ 0 \\ \vdots \\ 0 \end{pmatrix}\|^2 \\ &= \sigma_1^2 \gamma_1^2 + \dots + \sigma_{r+1}^2 \gamma_{r+1}^2 \geq \sigma_{r+1}^2 \end{aligned}$$

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

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 аппроксимация 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)

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

$$\dim L = k \quad L = \langle u_1, \dots, u_k \rangle_{\text{ортнорм}}$$

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

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

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

$$U^T U = I_k$$

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

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

$$U^T U = I_k$$

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

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)

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

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

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

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

У этой матрицы есть система из ортонорм 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 $u_0 = \bar{x}$

Теорема

Такая задача о минимизации имеет след. решение. Взять $u_0 = \bar{x}$

Взять в качестве U матрицу, сост из первых k веторов матрицы $\tilde{X}^T \tilde{X}$, упорядоч. по собс. числу

Лемма

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

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

Док-во

$$\begin{aligned} \frac{1}{m} \sum \|y_1 - b\|^2 &= \frac{1}{m} \sum \|(y_1 - \bar{y}) + (\bar{y} - b)\|^2 = \\ &= \frac{1}{m} \sum \|y_1 - \bar{y}\|^2 + \|\bar{y} - b\|^2 + \frac{2}{m} \sum_{i=1}^m (y_1 - \bar{y}, \bar{y} - b) = \\ &= \frac{1}{m} \sum \|y_1 - \bar{y}\|^2 + \|\bar{y} - b\|^2 + \frac{2}{m} \left(\sum_{i=1}^m (y_i - \bar{y}), \bar{y} - b \right) \\ &\qquad\qquad\qquad = 0 \end{aligned}$$

2019-11-19

Док-во (теоремы)

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

$$\begin{aligned} & \min_{U^T U = I_n} \sum_{i=1}^m \|(I - UU^T)(x_i - \bar{x})\|^2 \\ & \sum_{i=1}^m \|(I - UU^T)(x_i - \bar{x})\|^2 \stackrel{1}{=} \sum_{i=1}^m \|x_i - \bar{x}\|^2 - \sum_{i=1}^m \|U^T(x_i - \bar{x})\|^2 \stackrel{2}{=} \\ & = \sum_{i=1}^m \|x_i - \bar{x}\|^2 - \text{Tr}(U^T \tilde{X}^T \tilde{X} U) \end{aligned}$$

Откуда взялись равенства? Объясним первое:

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

т.к. было: $(U^T a, b) = (a, Ub)$

$$\begin{aligned} \Rightarrow (*) &= (U^T(x_i - \bar{x}), U^T(x_i - \bar{x})) \stackrel{\text{U-трансп.}}{=} (U^T(x_i - \bar{x}), U^T UU^T(x_i - \bar{x})) \stackrel{\text{лемма}}{=} \\ &= \|UU^T(x_i - \bar{x})\|^2 \end{aligned}$$

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

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

Теперь объясним второй переход:

$$\sum_{i=1}^m \|U^T(x_i - \bar{x})\|^2 \stackrel{?}{=} \text{Tr}(U^T \tilde{X}^T \tilde{X} U)$$

$$x_i - \bar{x} = \begin{pmatrix} x_{i1} \\ \vdots \\ x_{in} \end{pmatrix} \quad \tilde{X} = \begin{pmatrix} x_{11} & \dots & x_{1n} \\ \vdots & & \vdots \\ x_{n1} & \dots & x_{nn} \end{pmatrix}$$

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

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

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

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

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

То есть ПЧ = ЛЧ

Задача свелась к:

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

Лемма

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

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

$$\lambda_1 \geq \dots \geq \lambda_n$$

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

Док-во

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

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

Что мы знаем про c_j ?

1. $\sum_{j=1}^n c_j$ т.к. столбцы ортонорм. ($W^T W = I$) $\stackrel{=}{=} k$
(сумма квадратов по строкам равна сумме квадратов по столбцам, но все они равны 1, а их k штук)
2. $0 \leq c_j \leq 1$
(у матрицы W столбцы ОНБ вектора, любой набор ОН может дополнен до ОНБ, тогда матрица будет ортогональной, но у нее ОН строки, в частности сумма квадратов элементов 1, значит у недополненной ≤ 1)

Задача свелась к тому, чтобы д-ть:

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

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

$$\begin{aligned} & \lambda_1 + \dots + \lambda_k - \lambda_1 c_1 - \dots - \lambda_n c_n \stackrel{\text{по } 1}{=} \\ &= \lambda_1 + \dots + \lambda_k - \lambda_1 c_1 - \dots - \lambda_k c_k - \lambda_{k+1}(k - c_1 - \dots - c_k - c_{k+2} - \dots - c_n) - \\ & \quad - \lambda_{k+2} c_{k+2} - \dots - \lambda_n c_n = \\ &= (\lambda_1 - \lambda_{k+1})(1 - c_1) + \dots + (\lambda_k - \lambda_{k+1})(1 - c_n) + (\lambda_{k+1} - \lambda_{k+2})c_{k+2} + \dots + (\lambda_{k+1} - \lambda_n)c_n \geq 0 \\ & \tilde{X}^T \tilde{X} = S^T D S, \quad S \in Q_n(\mathbb{R}), \quad D - \text{диаг} \end{aligned}$$

$$\begin{aligned} & \max_{\substack{W \in M_{n,k}(\mathbb{R}) \\ W^T W = I}} \text{Tr}(U^T \tilde{X}^T \tilde{X} U) = \text{Tr}((SU)^T D (SU)) \end{aligned}$$

Док-во (продолжение д-ва теоремы)

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

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

Такое решение называется методом главных компонент (РСА)

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 - подгруппа аддитивной группы

Опр (конструкция)

$$a_1, \dots, a_n \in R$$

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

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. $a : b \Leftrightarrow (a) \subset (b)$
2. $a \sim b \Leftrightarrow (a) = (b)$

Док-во (1) (\Leftarrow) :

$$a \div b \Rightarrow a = bc$$

$$ra = rcb$$

 (\Rightarrow) :

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

$$\Rightarrow a = bc \Rightarrow a \div b$$

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:

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

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

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

Значит $c \in I$ и $0 \leq c < a \Rightarrow c = 0$

Значит любой элемент делится нацело 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. Далее также. Берем любой, делим на минимальной степени. Степень остатка меньше степени исходного многочлена

Теорема

В \mathbb{Z} (в $R[x]$)

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

Док-во (\mathbb{Z})

$$(a, b) \subset (\text{НОД}(a, b)):$$

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

Возьмем xd

По теореме о линейном представлении: $t_1a + t_2b = d$

$$\Rightarrow xd = (t_1x)a + (t_2x)b \in (a, b)$$

Док-во (в $R[x]$)

Аналогично

Опр

$$I \subset R$$

Идеал является подгруппой аддитивной группы кольца, которая коммутативна.

Профакторизуем: R/I (фактор-группа по сложению)

Сложение такое же.

Умножение: $\bar{a} \cdot \bar{b} \stackrel{\text{def}}{=} \overline{ab}$

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

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

Перемножим равенства:

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

Утв

R/I - кольцо (ком., асс., с 1)

Замечание

Достаточно д-ть:

$$1. (\bar{a}\bar{b})\bar{c} = \bar{a}(\bar{b}\bar{c})$$

$$2. \bar{a}\bar{b} = \bar{b}\bar{a}$$

$$3. \bar{1}\bar{a} = \bar{a}$$

$$4. \overline{a}(\overline{b} + \overline{c}) = \overline{a}\overline{b} + \overline{a}\overline{c}$$

Док-во

Докажем коммутативность:

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

(остальные аналогично)

У нас получилось новое кольцо, которое мы будем называть фактор-кольцом (\mathbb{R}/I) по идеалу I

Напоминание

$$\mathbb{Z}/p\mathbb{Z} - \text{поле (было)}$$

Утв

$$K[x]/(f) - \text{поле (f - непр.)}$$

Док-во

Достаточно доказать, что любой $\overline{g} \neq \overline{0} \quad g \in K[x]$ - обратим

$$\Leftrightarrow g \neq (f)$$

Рассмотрим (g, f) , f - неприводим, значит либо $f|g$, либо НОД = 1

Но первый вариант не может быть, значит $(g, f) = 1$

Значит существует линейное представление:

$$gh_1 + fh_2 = 1, \quad h_1, h_2 \in K[x]$$

Обратно перейдем в фактор-кольцо

$$gh_1 - 1 \in I$$

$$\Leftrightarrow \overline{gh_1} = \overline{1}, \text{ но } \overline{gh_1} = \overline{g}\overline{h_1}$$

Нашли обратный

Поняли, как строить определенные поля. Как строить любые?

Утв

$$f \in \mathbb{Z}/p\mathbb{Z}[x] - \text{непр.} \quad \deg f = n$$

$$\left| \mathbb{Z}/p\mathbb{Z}[x]/(f) \right| = p^n$$

Док-во

$$g \in \mathbb{Z}/p\mathbb{Z}[x]$$

Поделим с остатком на f :

$$g = fh + r, \quad \deg r < n$$

Утверждается, что в фактор-кольце лежат такие элементы:

$$\overline{\alpha_1 + \alpha_1 x + \dots + \alpha_{n-1} x^{n-1}} \in \mathbb{Z}/p\mathbb{Z}[x]/(f)$$

Всего таких классов p^n в силу произвольности выбора

1. Докажем, что любой элемент поля равен одному из них

$$\bar{g} = \bar{n}, \quad \text{т.к. } \deg r < n$$

2. Докажем, что никакие два элемента не совпадают

$$\overline{\alpha_1 + \alpha_1 x + \dots + \alpha_{n-1} x^{n-1}} = \overline{\beta_1 + \beta_1 x + \dots + \beta_{n-1} x^{n-1}}$$

$$\text{Рассмотрим } \overline{\alpha_1 + \alpha_1 x + \dots + \alpha_{n-1} x^{n-1} - \beta_1 - \beta_1 x - \dots - \beta_{n-1} x^{n-1}} = 0 \Rightarrow \alpha_1 + \alpha_1 x + \dots + \alpha_{n-1} x^{n-1} - \beta_1 - \beta_1 x - \dots - \beta_{n-1} x^{n-1} \in (f)$$

Многочлен $\deg = n$ делится на многочлен $\deg < n$, такое может быть только тогда, когда многочлен нулевой

Научились строить поля, у которых p^n элементов

Пусть хотим найти многочлен степени 6 над конечным полем

Как это сделать?

Рекурсивно. Составляем список унитарных мн-ов степени 2. Вычеркиваем все, у которых есть корень (подставляем элементы нашего конечного поля). Мн-н неприводим, когда у него нет корней.

Дальше составляем список унитарных мн-ов степени 3.

Составляем список мн-ов степени 4. Вычеркиваем все, у которых есть корень и которые делятся на мн-ны степени 2...

За конечное время можно получать такие списки А можно ли сделать поле из 24 элементов? Нельзя.

Напоминание

Характеристика поля 0 или простое число

Опр

K'/K , $K \subset K'$, K , K' - поля.

Называем K'/K - расширением полей (это не факторизация!)

Пример

$$\mathbb{C}/\mathbb{R}$$

$$\mathbb{R}/\mathbb{Q}$$

Опр

$[K', K]$ - степень расширения K'/K

Пусть K'/K , $K \subset K'$

Рассмотрим \mathbb{C} как векторное пр-во над \mathbb{R}

Замечание

Степень расширения - размерность K' , рассмотренного как векторное пр-во над K

$$[K', K] = \dim_K K'$$

Пример

Степень расширения \mathbb{C} над \mathbb{R} - 2

Степень расширения \mathbb{Q} над \mathbb{R} - $+\infty$

(не существует конечного набора над \mathbb{R} такого, чтобы любое другое являлось комбинацией этих коэф. из \mathbb{Q})

Утв

Рассмотрим $|K| < \infty$

1. $\Gamma K \neq 0 (\Rightarrow \Gamma K = p)$

Т.к. когда-то $\underbrace{1 + \dots + 1}_n = 1 + \dots + 1_m \quad m > n$, т.к. поле конечно

$$\Rightarrow \underbrace{1 + \dots + 1}_{m+n} = 0$$

Значит конечная ненулевая характеристика

$$\exists \Gamma K = p$$

$$\Omega = \{0, 1, 1 + 1, \dots, 1 + 1 + 1, \dots\} \subset K$$

$$\hat{\Omega} = \{0, 1, 1 + 1, \dots, \underbrace{1 + \dots + 1}_{p+1}\}$$

$$\hat{\Omega} \subset \Omega$$

- (a) Докажем, что в них нет совпадающих элементов. Пусть это не так

$$\underbrace{1 + 1 + \dots + 1}_n = \underbrace{1 + \dots + 1}_m \quad 0 \leq n < m \leq p + 1$$

$$\underbrace{1 + \dots + 1}_{m-n} \quad p - 1 \geq m - n > 0$$

Но $\Gamma = p$, а тут не так

- (b) Любой элемент из Ω лежит в $\hat{\Omega}$

Возьмем $\underbrace{1 + \dots + 1}_n$

Поделим с остатком:

$$\underbrace{1 + \dots + 1}_n = \overset{=0}{\underbrace{(1 + \dots + 1)}_p} \underbrace{(1 + \dots + 1)}_s + \underbrace{(1 + \dots + 1)}_q$$

$$n = ps + q, \quad 0 \leq p < p$$

- (c) Хотим д-ть, что Ω - поле

i. $(1 + \dots + 1) + (1 + \dots + 1) = 1 + \dots + 1$ (замкнутость относительно сложения)

ii. $(1 + \dots + 1) \cdot (1 + \dots + 1) = 1 + \dots + 1$

iii. $0 \in \Omega$

iv. $1 \in \Omega$

v. $|\Omega| = p$

vi. $\underbrace{1 + \dots + 1}_n + \underbrace{1 + \dots + 1}_{\leq p-n} = \overset{=0}{\underbrace{(1 + \dots + 1)}_s} \underbrace{(1 + \dots + 1)}_p$

$$sp - n \geq 0$$

vii. $1 + \dots + 1 \neq 0 \Leftrightarrow n \not\equiv p$

$$(n, p) = 1$$

$$ns - pq = 1, \text{ либо } pq - ns = 1$$

В первом случае:

$$\underbrace{(1 + \dots + 1)}_p \underbrace{(1 + \dots + 1)}_s = 1 + \overset{=0}{\underbrace{(1 + \dots + 1)}_p} \underbrace{(1 + \dots + 1)}_q$$

Во втором случае:

$$1 + \underbrace{(1 + \dots + 1)}_p \underbrace{(1 + \dots + 1)}_s = \underbrace{(1 + \dots + 1)}_p \overset{=0}{\underbrace{(1 + \dots + 1)}_q}$$

Получилось:

$$\underbrace{(1 + \dots + 1)}_n \underbrace{(1 + \dots + 1)}_s = -1$$

$$\underbrace{(1 + \dots + 1)}_n \underbrace{(1 + \dots + 1)}_{pt-s} = 1, \quad pt > s$$

2019-12-03

УТВ

$$K/\Omega \quad \text{char } K = p \quad |\Omega| = p$$

$\alpha_1, \dots, \alpha_n \in K$ - базис K над Ω

$$\Rightarrow \forall \alpha \in K \quad \alpha = \xi_1 \alpha_1 + \dots + \xi_n \alpha_n, \quad \xi_i \in \Omega$$

УТВ

Если есть два поля одинаковой мощности, то они изоморфны

УТВ

$K/L, N/K$ - конечные расширения

$$\Rightarrow N/L - \text{конечно и } [N : L] = [N : K][K : L]$$

Док-во

$$K/L - \text{конечно} \Rightarrow \exists \beta_1, \dots, \beta_n \in K : \forall \beta \in K \quad \exists! \alpha_1, \dots, \alpha_n \in L :$$

$$\beta = \alpha_1 \beta_1 + \dots + \alpha_n \beta_n$$

$$N/K - \text{конечно} \Rightarrow \exists \gamma_1, \dots, \gamma_m \in N : \forall \gamma \in N \quad \exists! \tilde{\beta}_1, \dots, \tilde{\beta}_m \in L :$$

$$\gamma = \tilde{\beta}_1 \gamma_1 + \dots + \tilde{\beta}_m \gamma_m$$

$$\{\beta_i \gamma_j\} \quad 1 \leq i \leq n$$

$$1 \leq j \leq m$$

Докажем, что это действительно базис N :

Возьмём $\gamma \in N$

$$\gamma = \sum \tilde{\beta}_j \gamma_j = \sum (\sum \alpha_{ij} \beta_i) \gamma_j, \quad \alpha_{ij} \in L$$

Теперь нужно док-ть линейную независимость

$$\sum \delta_{ij} \beta_i \gamma_j = 0 \quad \delta_{ij} \in L$$

$$\sum_j (\sum_i \delta_{ij} \beta_i) \gamma_j = 0$$

Так как базис, то в каждой скобке стоит ноль, снова применяем это рассуждение

$$\Rightarrow \delta_{ij} = 0$$

Пример

$$\mathbb{R}/\mathbb{Q}$$

$$\mathbb{C}/\mathbb{R}$$

Замечание

Такая конструкция называется башней расширения

Напоминание

$$G - \text{группа, } \text{ord } a = s \quad a^t = e \Rightarrow t : s$$

Утв

G - абелева (=коммутативная) группа

$$1. \quad \left. \begin{array}{l} \text{ord } a = n \\ \text{ord } b = m \\ (n, m) = 1 \end{array} \right| \Rightarrow \text{ord } ab = nm$$

$$(ab)^{nm} = a^{nm}b^{nm} = e$$

$$\text{Предположим } (ab)^k = e \Rightarrow \underset{=a^{nk}b^{nk}=b^{nk}}{(ab)^{nk}} \Rightarrow nk : m \Rightarrow k : m$$

Аналогично $k : n$

$$\left. \begin{array}{l} k : m \\ k : n \end{array} \right| \Rightarrow k : m$$

$$2. \quad \left. \begin{array}{l} \text{ord } a = n \\ \text{ord } b = m \end{array} \right| \Rightarrow \exists n', m' : \left. \begin{array}{l} n : n', m : m' \\ (n', m') = 1 \\ n'm' = \text{НОК}(n, m) \end{array} \right| \Rightarrow \exists c \in G :$$

$$\text{ord } c = \text{НОК}(m, n)$$

Док-во первой части:

$$(a) \quad \text{Пусть } n = p^\alpha, \quad m = p^\beta, \quad \alpha \geq \beta$$

$$n' = p^\alpha, \quad m' = 1$$

$$(b) \quad n = p_1^{\alpha_1} \dots p_s^{\alpha_s}, \quad m = p_1^{\beta_1} \dots p_s^{\beta_s}$$

Док-во второй части: достаточно д-ть, что \exists эл-ты порядка n', m'

Пусть $n = n'm'$

$$a^n = e$$

$$\Rightarrow (a^{s'})^{n'} = e$$

$$? \text{ord } a^{s'} = n'$$

$$(a^{s'})^t = e \quad (t < e') \Rightarrow a^{st} = e \Rightarrow st < s'n' = n$$

Противоречие с порядком

Значит мы нашли эл-т порядка n' , аналогично порядка m' . Пользуемся предыдущим пунктом и утверждение доказано

Теорема

Мультипликативная группа конечного поля циклическая

Док-во

Пусть $|K^*| = m$ (мультипликативная группа)

$$\alpha \in K^* - \text{ макс. порядка, } \text{ord } \alpha = s$$

По следствию из теоремы Лагранжа $m \geq s$

$$\beta \in K^* \quad \deg \beta = r$$

$$\exists \gamma \in K^* : \text{ord } \gamma = \text{НОК}(s, r) \geq s$$

$$\Rightarrow \text{НОК}(s, r) = s \Rightarrow s : r$$

$$\beta^r = 1 \Rightarrow \beta^s = 1$$

Рассмотрим $x^s - 1 \in K[x]$. Доказали, что каждый ненулевой элемент будет корнем. Значит у него по крайней мере m корней

Степень многочлена не превосходит числа корней

$$\Rightarrow s \geq m \Rightarrow s = m$$

Значит есть образующий элемент и группа циклическая

Утв

$$K/L - \text{ конечно, } \alpha \in K$$

$$\Rightarrow \exists f \in L[x] : f(\alpha) = 0$$

ДОК-ВО

Пусть $[K : L] = n$

Рассмотрим $1, \alpha, \alpha^2, \dots, \alpha^n \in K$

Если рассматривать это как вектора, то они ЛЗ

$$\Rightarrow \exists \gamma_i : \sum \gamma_i \alpha^i = 0$$

$$f(x) = \sum \gamma_i x^i$$

Опр

$f \in L[x]$ - минимальный мн-н для $\alpha \in K$ (в расширении K/L), если:

1. $f(\alpha) = 0$

$$2. \ g(\alpha) = 0 \Rightarrow \deg g \geq \deg f$$

$$g \in L[x]$$

Пример

Мн-н минимальной степени в \mathbb{R} у которого корень i - это $x^2 + 1$

Свойства

1. f - минимальный мн-н над L - неприводим

ДОК-ВО:

$$f = gh, \quad g, h \in L[x] : \deg g < \deg f, \quad \deg h < f$$

$$\underset{=0}{f(\alpha)} = f(\alpha)h(\alpha)$$

Противоречие

$$2. \ g(\alpha) = 0, \quad g \in L[x] \Rightarrow g \vdash f$$

ДОК-ВО:

$$g = fh + r, \quad \deg r < \deg f, \quad r \in L[x]$$

$$\underset{=0}{g(\alpha)} = \underset{=0}{f(\alpha)}h(\alpha) + r(\alpha)$$

$$\Rightarrow r - \text{ТОЖД. МН-Н} \Rightarrow g \text{ делится на } f \text{ без остатка}$$

Следствие

Значит минимальный многочлен единственный с точностью до ассоциированности

Следствие

Унитарный минимальный многочлен единственный

3. $[K : L] : \deg f$

Рассмотрим $L(\alpha) := \{\lambda_0 + \lambda_1\alpha + \dots + \lambda_s\alpha^s, \quad \lambda_i \in L\} \subset K$

Хотим доказать, что это поля. Очевидно кроме

$$\left. \begin{array}{l} \varphi(\alpha) \neq 0 \\ \varphi \in L(x) \end{array} \right| \Rightarrow \varphi(\alpha)^{-1} \in L(\alpha)$$

Рассмотрим $(\varphi, f) \stackrel{f-\text{неприв.}}{=} \begin{bmatrix} f \\ 1 \end{bmatrix} \Rightarrow \varphi : f - \text{невозможно}$

$$\Rightarrow (\varphi, f) = 1 \Rightarrow 1 = \varphi h + fg, \quad h, g \in L[x]$$

$$1 = \varphi(\alpha)h(\alpha) + \underbrace{f(\alpha)g(\alpha)}_{=0}$$

Замечание

Получили башню расширения: $K - L(\alpha) - L$

$$[K : L] = [K : L(\alpha)][L(\alpha) : L] \stackrel{?}{=} \deg f$$

$$\deg f = n$$

$1, \alpha, \alpha^2 \dots \alpha^{n-1}$ - базис $L(\alpha)$ над L ?

(а) ЛН?

$$\sum_{i=0}^{n-1} c_i \alpha^i = 0, \quad c_i \in L$$

$$\psi(x) = \sum_{i=0}^{n-1} c_i x^i \in L[x]$$

$$\begin{array}{l} \psi(\alpha) = 0 \\ \deg \psi \leq n-1 \end{array} \Rightarrow \psi = 0 \Rightarrow c_i = 0$$

(b) Порождаемость?

$$\varphi(\alpha) \in L(\alpha), \quad \varphi \in L[x]$$

$$\varphi = fg + r, \quad \deg f < n, \quad r \in L[x]$$

$$\varphi(\alpha) = f(\alpha)g(\alpha) + r(\alpha)$$

т.е. $r(\alpha)$ - ЛК базисных векторов

2019-12-10

УТВ

$$x^{p^n} - x = \prod_{d|n} \text{унитарные непр. мн-ны над } \mathbb{Z}/p\mathbb{Z} \text{ степени } d$$

Пример

$$p = 2 \quad n = 4$$

$$x^{16} - x = x(x+1)(x^2+x+1)(x^4+x^3+x^2+x+1)(x^4+x^3+1)(x^4+x+1)$$

Опр

$m_p(d)$ - кол-во непр. унит. мн-нов степ d над $\mathbb{Z}/p\mathbb{Z}$

$$p^n = \sum_{d|n} m_p(d)d \quad m_p(1) = p$$

Следствие

все $M_p(d)$ - полож.

Док-во (следствия)

$$M_p(d) = m_p(d)d$$

$$p^n = \sum_{d|n} M_p(d) \quad M_p(d) \leq p^d$$

$$\begin{aligned} M_p(n) &= p^n - \sum_{\substack{d|n \\ d \neq n}} M_p(d) \geq p^n - \sum_{\substack{d|n \\ d \neq n}} p^d \geq p^n - (p^{n-1} + p^{n-2} + \dots + p) = \\ &= p^n - \frac{p^n - p}{p - 1} = \frac{p^{n+1} - 2p^n + p}{p - 1} > 0 \end{aligned}$$

Утв (предложение)

$$f \in \mathbb{Z}/p\mathbb{Z}[x] - \text{непр } \deg f = d$$

$$x^{p^n} - x \vdots f \Leftrightarrow n \vdots d$$

Док-во

Только часть док-ва

$$h \vdots g^2$$

$$\Rightarrow h' \vdots g$$

Лемма (для док-ва предложения)

$$(x^{p^n} - x, x^{p^d} - x) = x^{p^{(n,d)}} - x$$

Док-во (предложения)

$$\Leftarrow n \vdots d$$

$$F = \mathbb{Z}/p\mathbb{Z}[x] / (f) \quad |F| = p^d$$

\bar{x} - класс по модулю

$$|F^*| = p^d - 1$$

$$\forall \alpha \in F^* \quad \text{ord } \alpha = t \quad ts = p^d - 1$$

$$\alpha^t = 1$$

$$\alpha^{p^d-1} = \alpha^{st} = 1$$

$$\alpha^{p^d} = \alpha$$

$$\bar{x}^{p^d} = \bar{x} \text{ в } F$$

$$x^{p^d} - x \vdots f$$

$$(x^{p^n} - x, x^{p^d} - x) = x^{p^{(n,d)}} - x = x^{p^d} - x \vdots f$$

Если НОД делится на $f \Rightarrow$ каждый делится

$$\Rightarrow x^{p^n} - x \vdots f$$

$$x^{p^d} - x \vdots f$$

$$\Rightarrow (x^{p^n} - x, x^{p^d} - x) = x^{p^{(n,d)}} - x \vdots f$$

$$d' = (n, d)$$

$$\overline{x}^{p^{d'}} = \overline{x} \quad \text{в } F$$

$$\varphi(\overline{x})^{p^{d'}} = \varphi(\overline{x}) \quad \varphi \in \mathbb{Z}/p\mathbb{Z}[t]$$

$$1) \quad \left. \begin{array}{l} \lambda^{p^{d'}} = \lambda \\ \eta^{p^{d'}} = \eta \end{array} \right| \Rightarrow (\lambda + \eta)^{p^{d'}} = (\lambda + \eta) \quad \lambda, \eta \in F$$

$$2) \quad \lambda^{p^{d'}} = \lambda \Rightarrow (a\lambda)^{p^{d'}} = a\lambda \quad a \in \mathbb{Z}/p\mathbb{Z}, \quad \lambda \in F$$

$$1) \quad (x + y)^p = x + y \quad \text{в поле хар-ки } p$$

$$2) \quad a \in \mathbb{Z}/p\mathbb{Z} \quad a^p = a$$

$$\lambda^{p^{d'}} = \lambda \quad \forall \lambda \in F$$

$$\Rightarrow \lambda^{p^{d'}-1} = 1$$

Это происходит с любым элементом поля F , в котором p^d элементов.

В $|F^*| = p^d - 1$ элемент, а мы получили, что \forall элемента $\lambda^{p^{d'}} = 1$, это возможно, только, если $d' = d$

$$\Rightarrow n \vdots d$$

Док-во (леммы)

$$n = dq + r$$

$$\begin{aligned} x^{p^n} - x &= x^{p^{dq+r}} - x = \\ &= \underbrace{(x^{p^d} - x)^{p^{d(q-1)+r}} + (x^{p^d} - x)^{p^{d(q-2)+r}} + \dots + (x^{p^d} - x)^{p^r}}_{\vdots x^{p^d} - x} + (x^{p^r} - x) \end{aligned}$$

$$\begin{aligned} n &= dq + r & x^{p^n} - x &= (x^{p^d} - x)g + x^{p^r} - x \\ d &= rq_1 + r_1 & x^{p^d} - x &= (x^{p^r} - x)g_1 + x^{p^{r_1}} - x \\ r &= r_1q_2 + r_2 & & \dots \end{aligned}$$

УТВ

F_1, F_2 - изоморфны, если $\exists \varphi : F_1 \rightarrow F_2 :$

$$1. \quad \varphi(a + b) = \varphi(a) + \varphi(b)$$

$$2. \varphi(ab) = \varphi(a)\varphi(b)$$

3. φ - биекция

УТВ (предложение)

$$|F_1| = |F_2| = p^n \Rightarrow F_1 \cong F_2$$

Док-во

$$\mathbb{Z}_p\mathbb{Z}[x] \Big/_{(f)}, \quad f \in \mathbb{Z}_p\mathbb{Z}[x] \quad \deg f = n$$

$$|F| = p^n$$

$$\bar{x}^{p^n} = \bar{x} \text{ в } \mathbb{Z}_p\mathbb{Z}[x] \Big/_{(f)}$$

$$\Rightarrow x^{p^n} - x \vdots f$$

$$\forall \alpha \in F \quad \alpha^{p^n} = \alpha$$

$$x^{p^n} - x \text{ над } F(\text{произв. поле})$$

$$x^{p^n} - x = \prod_{\alpha \in F} (x - \alpha)$$

$$\Rightarrow \exists \alpha \in F : f(\alpha) = 0$$

$$\mathbb{Z}_p\mathbb{Z}[x] \Big/_{(f)} \rightarrow F$$

$$\varphi(\bar{x}) \rightarrow \varphi(\alpha), \quad \varphi \in \mathbb{Z}_p\mathbb{Z}[t]$$

$$\text{Нужно ядро} = 0$$

$$\varphi(\bar{x}) \quad \varphi(\alpha) = 0 \quad f(\alpha) = 0 \quad f - \text{непр}$$

$$\Rightarrow \varphi \vdots f$$