Содержание

Обозначение. $A \Subset B$ – непустое подмножество

23. Подгруппа. Подгруппы целых чисел. Порождающее множество

Определение 1. G – группа, $\quad H \subset G$
Если H является группой относительно той же операции, то H называется подгруппой G

Обозначение. $H < G$

Свойства.

1. $e_H = e_G$
2. Если a' – обратный к a в группе H, то a' – обратный к a в группе G

Теорема 1 (подгруппы группы $\mathbb{Z}$). $H < \mathbb{Z}$

$$\implies \exists d \in \mathbb{Z} : H = \{\, dx \mid x \in \mathbb{Z} \,\}$$

Доказательство.

- Если $H = \{\, 0 \,\}$, то $d = 0$
- Пусть $H \neq \{\, 0 \,\}$
  Тогда H содержит хотя бы одно положительное число, так как $\forall x \in H \quad -x \in H$
  Пусть d – наименьший положительный элемент H
  Положим $K := \{\, dx \mid x \in \mathbb{Z} \,\}$ и докажем, что $K = H$:
  - $H \subset K$
    * Элементы $d, 2d, 3d, \ldots$ принадлежат H, т. к. H замкнута относительно сложения
    * Элемент $-d$ принадлежит H, т. к. H замкнута относительно взятия обратного
    * Элементы $-d, -2d, -3d, \ldots$ принадлежат H, т. к. $-d \in H$ и H замкнута относительно сложения
  - $K \subset H$
    Нужно доказать, что в H нет лишних
    Пусть это не так, и существует $a \in (H \setminus K)$
    Поделим a на d с остатком. Пусть $x = aq + r, \quad 0 < r < d$

$$\left.\begin{array}{l} H \subset K \implies dq \in H \\ a \in H \end{array}\right\} \implies r = a + (-dq) \in H - \lightning \text{ с минимальностью } d$$

$\square$

Лемма 1 (критерий подгруппы). G – группа, $H \Subset G$

$$H < G \iff \begin{cases} a, b \in H \implies ab \in H & (1) \\ a \in H \implies a^{-1} \in H & (2) \end{cases}$$

Доказательство.

- $\implies$
  Очевидно из того, что H – группа и подгруппа G
- $\impliedby$
  - Соответствие операций:
    Из (1) следует, что операция G является бинарной операцией в H
  - Ассоциативность:
    $$a, b, c \in H \implies a, b, c \in G \implies (ab)c = a(bc)$$
  - Единица и обратный:

Пусть $a \in H$

$$\left.\begin{aligned}(2) &\implies a^{-1} \in H \\ (1) &\implies aa^{-1} \in H\end{aligned}\right\} \implies a^{-1}a = aa^{-1} = e_H$$

$\square$

Следствие. $\left(\bigcap_{H<G} H\right) < G$

Теорема 2 (порождающее множество). G – группа, $S \Subset G$
Тогда

1. $\exists\, H_0 < G : \begin{cases} S \subset H_0 \\ H_0 \text{ – минимальная по включению} \end{cases}$

2. $H_0 = \bigcap_{S \subset H} H$

   Доказательство. Пусть M – множество всех подгрупп, содержащих S
   Обозначим
   $$H_0 \coloneqq \bigcap_{H \in M} H$$
   По следствию к критерию подгруппы, H_0 является подгруппой. При этом H_0 содержит S
   Проверим, что H_0 – минимальная по включению:
   Пусть H_1 содержит S. Тогда $H_1 \in M$ и
   $$H_1 \supset \bigcap_{H \in M} H = H_0$$
   $\square$

3. H_0 состоит из всех произведений элементов вида x и x^{-1}, где $x \in S$

   Доказательство. Обозначим через S^{-1} множество элементов, обратным к элементам из S
   Положим $T \coloneqq S \cup S^{-1}$
   Обозначим $K \coloneqq \{\, x_1 x_2 \dots x_n \mid x_i \in T \,\}$
   Нужно доказать, что K – минимальная по включению подгруппа:

   - Докажем, что K – подгруппа
     Применим критерий:
     - $a, b \in K, \quad a = x_1 \dots x_n, \quad b = y_1 \dots y_m$
       $$ab = x_1 \dots x_n y_1 \dots y_m$$
       Все сомножители принадлежат T
     - $a \in K, \quad a = x_1 \dots x_n$
       $$a^{-1} = x_n^{-1} \dots x_1^{-1}$$
       Все сомножители принадлежат T
   - Проверим минимальность K:
     Пусть H – произвольная подгруппа, содержащая S
     Тогда $S^{-1} \subset H$ (т. к. любая подгруппа вместе с каждым элементом содержит его обратный)
     Значит, $T \subset H$, и произведение любого набора элементов из N принадлежит H

   $\square$

Определение 2. Пусть H – минимальная подгруппа, содержащая S
Тогда говорят, что S порождает H

Обозначение. $H = \langle S \rangle$

24. Порядок элемента. Циклические группы

Определение 3. G – группа, $a \in G$
Порядком a называется

$$\operatorname{ord} a := \min \{\, n \in \mathbb{N} \mid a^n = e \,\}$$

Если $\nexists n \in \mathbb{N} : a^n = e$, то $\operatorname{ord} a := \infty$

Свойства.

1. $\operatorname{ord} a < \infty, \quad k \in \mathbb{Z}$

$$a^k = e \iff k \vdots \operatorname{ord} a$$

Доказательство. Пусть $n := \operatorname{ord} a$
Разделим k на n с остатком:

$$k = nq + r, \qquad 0 \le r < n$$

$$a^k = (a^n)^q a^r = e^q a^r = a^r$$

- Если $k \vdots n$, то $r = 0 \implies a^r = e$
- Иначе $r \in \mathbb{N}, \quad r \neq 0$
  Тогда $a^r \neq e$ (т. к. n – минимальная натуральная степень, при возведении в которую элемент a обращается в e)

$\square$

2. $\operatorname{ord} a < \infty, \quad k, m \in \mathbb{Z}$

$$a^k = a^m \iff k \underset{\operatorname{ord} a}{\equiv} m$$

Доказательство.

$$a^k = a^m \iff a^k (a^m)^{-1} = e \iff a^{k-m} = e \iff k - m \vdots \operatorname{ord} a$$

$\square$

Определение 4. Группа G называется циклической, если $G = \langle a \rangle$ для некоторого $a \in G$

Свойства.

1. Если $G = \langle a \rangle$, то G состоит из элементов $a^n, \quad n \in \mathbb{Z}$
2. Циклическая группа абелева

Теорема 3 (строение циклических групп). G – циклическая группа

- $|G| = \infty \implies G \cong \mathbb{Z}$
- $|G| = n < \infty \implies G \cong \mathbb{Z}_n$

Доказательство. Пусть $G = \langle a \rangle$

- Если $\operatorname{ord} a = \infty$, то все элементы $a^k, \quad k \in \mathbb{Z}$ различны, и, следовательно, $|G| = \infty$
  Пусть $f : \mathbb{Z} \to G$ определяется равенством $f(x) = a^x$
  - Проверим, что f согласовано с операцией:

$$f(x + y) = a^{x+y} = a^x y^x = f(x) f(y)$$

  - Проверим биективность:
    Мы только что выяснили, что элементы a^x различны при различных x

- Если $\operatorname{ord} a$ конечен, то элементы $a^0, a^1, ..., a^{\operatorname{ord} a - 1}$ различны, и любой другой элемент a^k совпадает с одним из них, следовательно, $|G| = \operatorname{ord} a$
  Определим $f : \mathbb{Z}_n \to G$
  Пусть $x \in \mathbb{Z}, \quad 0 \le x \le n-1$, и $\overline{x} \in \mathbb{Z}_n$ – соответствующий вычет
  Положим $f(\overline{x}) := a^x$

  - Проверим, что f согласовано с операцией:
    Пусть
    $$\overline{x}, \overline{y} \in \mathbb{Z}_n, \qquad x, y \in \mathbb{Z}, \qquad 0 \le x, y \le n-1$$
    Тогда $f(\overline{x}) = a^x, \quad f(\overline{y}) = a^y$
    Положим
    $$z := \begin{cases} x+y, & x+y < n \\ x+y-n, & x+y \ge n \end{cases}$$
    Тогда $\overline{z} = \overline{x} + \overline{y}$ в $\mathbb{Z}_n$, и
    $$f(\overline{x} + \overline{y}) = f(\overline{z}) = a^z = \begin{cases} a^{x+y} = a^x a^y, & x+y < n \\ a^{x+y-n} = a^x a^y (a^n)^{-1}, & x+y \ge n \end{cases}$$
    Учитывая, что $\operatorname{ord} a = |G| = n$, получаем, что $a^n = e$, и правая часть равна $a^x a^y = f(\overline{x}) f(\overline{y})$
  - Проверим биективность:
    Пусть $0 \le x, y \le n-1$, и $f(\overline{x}) = f(\overline{y})$
    $$a^x = a^y \implies x \underset{n}{\equiv} y \implies x = y$$

□

Свойство. $|\langle a \rangle| = \operatorname{ord} a$

25. Левые и правые смежные классы. Теорема Лагранжа и следствие из неё

Обозначение. G – группа, $\qquad H < G$
На множестве элементов G введём отношение $\sim$:
$a \sim b$, если $b = ah$ для некоторого $h \in H$

Свойство. $\sim$ является отношением эквивалентности

Определение 5. Класс эквивалентности элемента a называется левым смежным классом a относительно H
Аналогично опредляются правые смежные классы

Свойство. Левый смежный класс $\overline{a}$ равен aH, где $aH = \{\, ah \mid h \in H \,\}$
Правый смежный класс равен Ha

Определение 6. Если H имеет конечное количество левых смежных классов, то их количество называется индексом H в G

Обозначение. $[G : H]$

Теорема 4 (Лагранжа).
G – конечная группа, $\quad H < G$
Тогда $|G| = [G : H] \cdot |H|$

Доказательство. Количество элементов в любом смежном классе равно $|H|$
Группа G разбивается на левые смежные классы, в каждом из них $|H|$ элементов □

Следствие. G – конечная группа
Тогда $|G| \vdots \operatorname{ord} a \quad \forall a \in G$

Доказательство. Положим $H = \langle a \rangle$
Применяя теорему Лагранжа, получаем, что $|G| \vdots \operatorname{ord} a$ □

26. Нормальные подгруппы

Определение 7. G – группа
Подгруппа H называется нормальной, если $aH = Ha \quad \forall a \in G$

Обозначение. $H \lhd G$

Теорема 5 (равносильные определения нормальной подгруппы). G – группа, $\quad H < G$
Следующие условия равносильны:

1. $H \lhd G$
2. $a^{-1}Ha = H \quad \forall a \in G$
3. $a^{-1}ha \in H \quad \forall a \in G, h \in H$

Доказательство.

- $1 \iff 2$
$$aH = Ha \iff a^{-1}aH = a^{-1}Ha \iff eH = a^{-1}H \iff H = a^{-1}Ha$$
- $2 \implies 3$
$$a^{-1}Ha = H \implies a^{-1}Ha \subset H \implies a^{-1}ha \in H \quad \forall h \in H$$
- $3 \implies 2$
  - $\subset$ – очевидно
  - $\supset$
    Зафиксируем $a \in G$
    Нужно доказать, что $H \subset a^{-1}Ha$, то есть, что
    $$\forall h \in H \quad \exists h_1 \in H : a^{-1}h_1a = h$$
    Применим утверждение 3 к h и $a_1 = a^{-1}$. Получим, что
    $$a_1^{-1}ha_1 = aha^{-1} \in H$$
    Элемент aha^{-1} подойдёт в качестве h_1

□

27. Факторгруппа

Определение 8. $H \lhd G$
На множестве левых смежных классов относительно H определим операцию умножения:
Пусть A, B – классы. Выберем в каждом классе произвольный элемент, пусть $a \in A, b \in B$
Тогда AB – такой класс, что $ab \in AB$

Теорема 6 (факторгруппа). $H \lhd G$

1. Операция умножения левых смежных классов определена корректно, то есть не зависит от выбора элементов в классах

Доказательство. Докажем, что, если a_1, a_2 лежат в одном смежном классе, и b_1, b_2 лежат в одном смежном классе, то a_1b_1, a_2b_2 лежат в одном смежном классе
Существуют $x, y \in H$, такие, что $a_2 = a_1x, \quad b_2 = b_1y$. Подставим:

$$a_2b_2 = a_1b_1b_1^{-1}a_1^{-1}a_2b_2 = a_1b_1b_1^{-1}\cancel{a_1^{-1}}\cancel{a_1}xb_1y = a_1b_1b_1^{-1}xb_1y = (a_1b_1)\Big((b_1^{-1}xb_1)y\Big)$$

Из того, что $H \lhd G$ следует, что $b_1^{-1}xb_1 \in H$
Следовательно, $(b_1^{-1}xb_1)y \in H$ □

2. Множество левых смежных классов с операцией умножения является группой

Доказательство.

- Ассоциативность: $(\overline{a}\overline{b})(\overline{c}) = (\overline{ab})(\overline{c}) = (\overline{abc})$
- Единица: $\overline{e} = H$
- Обратный: $(\overline{a})^{-1} = \overline{a}^{-1}$

□

Определение 9. Группа смежных классов по подгруппе H назвывается факторгруппой G по H

Обозначение. G/H

28. Центр группы

Определение 10. Центром группы G называется множество элементов, которые коммутируют со всеми элементами G, т. е.

$$Z(G) \coloneqq \{\, a \mid ax = xa \quad \forall x \in G \,\}$$

Свойство. G абелева $\iff G = Z(G)$

Теорема 7. Центр группы является нормальной подгруппой

Доказательство.

- $Z(G) < G$

$$e \in Z(G) \implies Z(G) \neq \emptyset$$

  Применим критерий:
  Пусть $a, b \in Z(G)$

  – Проверим, что $ab \in Z(G)$, то есть, что $(ab)x = x(ab) \quad \forall x \in G$
  Воспользуемся тем, что a и b коммутируют с любым элементом:

$$abx = axb = xab$$

  – Проверим, что $a^{-1} \in Z(G)$, то есть $a^{-1}x = xa^{-1} \quad \forall G$

$$a \in G \implies xa = ax \iff a(a^{-1}x)a = a(xa^{-1}) \iff a^{-1}x = xa^{-1}$$

- $Z(G) \lhd G$
  Пусть $a \in Z(G), x \in G$

$$x^{-1}ax = ax^{-1}x = a \in Z(G)$$

□

Определение 11. Если $Z(G) = \{\, e \,\}$, то группа G называется группой с тривиальным центром или группой без центра

29. Коммутант группы: нормальность, факторгруппа

Определение 12. Коммутатором элементов a и b называется элемент $a^{-1}b^{-1}ab$

Обозначение. $[a,b]$

Свойства.

1. $ba[a,b] = ab$
2. $[a,b]^{-1} = [b,a]$
3. $ab = ba \iff [a,b] = e$

Определение 13. Коммутантом группы G называется подгруппа

$$[G,G] \coloneqq \langle [a,b] | a,b \in G \rangle$$

Замечание. G абелева $\iff [G,G] = \{\, e \,\}$

Определение 14. $L, M \subset G$
Взаимным коммутантом L и M называется подгруппа

$$[L,M] \coloneqq \langle [a,b] | a \in L, b \in M \rangle$$

Теорема 8. Коммутант группы является нормальной подгруппой

Доказательство. Пусть $g \in G, k \in K$
Докажем, что $g^{-1}kg \in K$:
Пусть a_i, b_i таковы, что

$$k = [a_1,b_1][a_2,b_2]...[a_n,b_n]$$

$$g^{-1}kg = g^{-1}[a_1,b_1][a_2,b_2]...[a_n,b_n]g = g^{-1}[a_1,b_1]gg^{-1}...gg^{-1}[a_n,b_n]g = \\ = (g^{-1}[a_1,b_1]g)(g^{-1}[a_2,b_2]g)...(g^{-1}[a_n,b_n]g)$$

Достаточно доказать, что произведение в любой скобке принадлежит K, то есть для любых $g,a,b \in G$ выполнено $g^{-1}[a,b]g \in K$

$$g^{-1}[a,b]g = g^{-1}a^{-1}b^{-1}abg = (g^{-1}a^{-1}ga)(a^{-1}g^{-1}b^{-1}abg) = [g,a][a,bg]$$

□

Теорема 9 (факторгруппа по коммутанту). G – группа, $\quad K = [G,G]$

1. группа $G/[G,G]$ абелева

   Доказательство. Частный случай следующего □

2. $H \lhd G$

$$[G,G] \subset H \iff G/H \text{ абелева}$$

Доказательство.

$$G/H \text{ абелева } \iff \forall a,b \in G \quad \overline{a}\overline{b} = \overline{b}\overline{a} \iff \overline{ab} = \overline{ba} \iff \exists\, h \in H : ab = bah \iff \\ \iff (ba)^{-1}ab \in H \iff [a,b] \in H \iff [G,G] \subset H$$

□

30. Гомоморфизм: определение, примеры, свойства ядра и образа

Определение 15. $(G, *), (H, \times)$ – группы
Отображение $f : G \to H$ называется гомоморфизмом, если

$$\forall a, b \in G \quad f(a * b) = f(a) \times f(b)$$

Примеры.

1. $f : \underset{(\mathbb{C}\setminus\{0\})}{\mathbb{C}*} \to \mathbb{C}*, \qquad f(z) = |z|$
2. $f : \mathbb{R}* \to \mathbb{C}*, \qquad f(z) = z$
3. $f : \mathbb{Z} \to \mathbb{Z}, \qquad f(z) = 2z$

Свойства.

1. (a) $f(e_G) = e_H$

   Доказательство. $f(a)e_H = f(a) = f(ae_G) = f(a)f(e_G) \implies f(e_G)$ □

   (b) $f(a^{-1}) = \Big(f(a)\Big)^{-1}$

   Доказательство. $f(a)f(a^{-1}) = f(aa^{-1}) = f(e_G) = e_H$ □

2. G, H, K – группы, $\qquad f : G \to H, \quad g : H \to K$ – гомоморфизмы
   Тогда $g \circ f : G \to K$ – гомоморфизм

   Доказательство.

   $$(g \circ f)(ab) = g\big(f(ab)\big) = f\big(f(a)f(b)\big) = g\big(f(a)\big)g\big(f(b)\big) = (g \circ f)(a)(g \circ f)(b)$$

   □

Определение 16 (ядро и образ). $f : G \to H$ – гомоморфизм

$$\ker f := \{\, x \in G \mid f(x) = e_H \,\}$$

$$\operatorname{Im} f := \{\, f(a) \mid a \in G \,\}$$

Свойства (ядра).

1. $\ker f \lhd G$

   Доказательство.

   - $\ker f < G$
     Пусть $a, b \in \ker f$
     – $f(ab) = f(a)f(b) = e_He_H = e_H \implies ab \in \ker f$
     – $f(a^{-1}) = \big(f(a)\big)^{-1} = e_H^{-1} = e_H \implies a^{-1} \in \ker f$
   - $\ker f \lhd G$
     Пусть $a \in G, h \in \ker f$

     $$f(a^{-1}ha) = f(a^{-1})f(h)f(a) = f(a)^{-1}e_Hf(a) = f(a)^{-1}f(a) = e_H \implies a^{-1}ha \in \ker f$$

   □

2. f – инъекция $\iff \ker f = \{\, e_G \,\}$

Доказательство.

- $\Longrightarrow$
$$x \in \ker G \implies f(x) = e_H \implies f(x) = f(e_G) \implies x = e_G$$
- $\Longleftarrow$
$$f(x) = f(y) \implies f(x)\big(f(y)\big)^{-1} = e_H \implies f(x)f(y^{-1}) = e_H \implies f(xy^{-1}) = e_H \implies$$
$$\implies xy^{-1} \in \ker f \implies xy^{-1} = e_G \implies x = y$$

□

Свойство (образа). $\operatorname{Im} f < H$

Доказательство. Пусть $a, b \in \operatorname{Im} f$
Тогда
$$\exists\, x, y \in G : \begin{cases} a = f(x) \\ b = f(y) \end{cases}$$

- $ab = f(xy) \in \operatorname{Im} f$
- $a^{-1} = f(x^{-1}) \in \operatorname{Im} f$

□

31. Теорема о гомоморфизме

Теорема 10. $f : G \to H$ – гомоморфизм
$$\implies G/\ker f \cong \operatorname{Im} f$$

Доказательство. Определим отображение $\varphi : G/\ker f \to \operatorname{Im} f$
Пусть $A \in G/\ker f$, то есть A – некоторый смежный класс по подгрупе $\ker f$
Выберем произвольный элемент $a \in A$
Положим $\varphi(A) \coloneqq f(a)$, т. е. $\varphi(\overline{a}) = f(a)$

- Корректность
Проверим, что $\forall a, a' \in A \quad f(a) = f(a')$:
Элементы a и a' принадлежат одному смежному классу, следовательно, $a = a'x$ для некоторого $x \in \ker f$
Применим f:
$$f(a) = f(a'x) = f(a')f(x) = e_H f(a') = f(a')$$
- φ – гомоморфизм
Пусть A, B – смежные классы
Выберем произвольные $a \in A, b \in B$
Тогда AB – это класс, которому принадлежит ab
То есть, $A = \overline{a}, \quad B = \overline{b}, \quad AB = \overline{ab}$
Применим φ:
$$\varphi(AB) = \varphi(\overline{ab}) = f(ab) = f(a)f(b) = \varphi(\overline{a})\varphi(\overline{b}) = \varphi(A)\varphi(B)$$
- φ – сюръекция
$$x \in \operatorname{Im} f \implies \exists\, a \in G : x = f(a) \implies x = \varphi(\overline{a})$$
- φ – инъекция
$$\ker \varphi = e_{G/\ker f} = \{\ker f\}$$
$$\overline{a} \in \ker \varphi \implies \varphi(\overline{a}) = e_H \implies f(a) = e_H \implies a \in \ker f \implies \overline{a} = \ker f$$

□

32. Теорема Кэли

Обозначение. S_n – группа перестановок (т. е. биекций $X = \{1, 2, ..., n\}$ в себя)

Теорема 11. G – конечная группа, $|G| = n$
Тогда G изоморфна некоторой подгрупе группы S_n

Доказательство. Пронумеруем произвольным образом элементы группы, пусть это $g_1, ..., g_n$
Заметим, что для любого $a \in G$ элементы $ag_1, ..., ag_n$ различны
Следовательно, $ag_1, ..., ag_n$ – это некоторая перестановка элементов $g_1, ..., g_n$
Определим отображение $\varphi : G \to S_n$ следующим образом:
Для элемента $a \in G$ обозначим через $\varphi(a)$ такую перестановку σ, что

$$ag_1 = g_{\sigma(1)}, \quad \dots\dots\dots\dots\dots, \quad ag_n = g_{\sigma(n)}$$

- Докажем, что φ – гомоморфизм:
  Пусть $\varphi(a) := \sigma, \quad \varphi(b) := \tau$
  Нужно проверить, что $\varphi(ab) = \sigma\tau$, т. е.

  $$\forall i \quad (ab)g_i = g_{(\sigma\tau)(i)}$$

  Пусть $\tau(i) = j, \quad \sigma(j) = k$

  $$\left.\begin{aligned} &bg_i = g_j \\ &(ab)g_i = a(bg_i) = ag_j = g_k \\ &(\sigma\tau)(i) = k \end{aligned}\right\} \implies (ab)g_i = g_k = g_{(\sigma\tau)(i)}$$

  Положим $H = \operatorname{Im} f$
  Тогда $H < S_n$
  Докажем, что $G \cong H$:
  Гомоморфизм φ можно рассматривать как отображение $G \to H$
- Проверим, что это биекция:
  Для этого нужно проверить, что $\ker\varphi = \{e\}$
  Пусть $a \in \ker\varphi$
  Тогда $\varphi(a)$ – тождественная перестановка

  $$ag_1 = g_1, \quad \dots\dots\dots\dots\dots, \quad ag_n = g_n$$

  По свойству сокращения, из этого следует, что $a = e$

$\square$

33. Действие группы на множество. Орбиты. Стабилизаторы

Определение 17. G – группа, M – множество
Говорят, что группа G действует (слева) на множество M, если каждой паре элементов $g \in G, m \in M$ сопоставлен элемент $g(m) \in M$, и при этом выполнены свойства:

1. $(gh)(m) = g\big(h(m)\big) \quad \forall g, h \in G, m \in M$
2. $e(m) = m \quad \forall m \in M$

Примечание. Аналогично определяется действие справа

Определение 18. Введём на M отношение эквивалентности:
$m \sim l$, если $\exists\, g \in G : gm = l$
Классы эквивалентости по отношению $\sim$ называются орбитами

Обозначение. Орбита, содержащая элемент m обозначается $\operatorname{Orb} m$ или Gm

Доказательство (корректности). Проверим, что $\sim$ является отношением эквивалентности:

- $em = m \implies m \sim m$
- Пусть $m \sim l$
  Тогда $gm = l$ для некоторого $g \in G$
  $$\implies g^{-1}l = m \implies l \sim m$$
- Пусть $\sim l, l \sim k$
  Тогда $gm = l, hl = k$ для некоторых $g, h \in G$
  $$\implies k = h(gm) = (hg)m \implies m \sim k$$

$\square$

Определение 19. Стабилизатором элемента $m \in M$ называется множество

$$\mathrm{St}(m) \coloneqq \{ g \in G \mid gm = m \}$$

Определение 20. Фиксатором элемента $g \in G$ называется множество

$$\mathrm{Fix}(g) \coloneqq \{ m \in M \mid gm = m \}$$

Свойства.

1. $\mathrm{St}(m) < G \quad \forall m \in M$
2. G – конечная группа
$$|G| = |\operatorname{Orb}(m)| \cdot |\operatorname{St}(m)|$$

Доказательство. Пусть $k \coloneqq |\operatorname{Orb}(m)|$, и $m_i \in M, g_i \in G$ таковы, что

$$\operatorname{Orb}(m) = \{ m_1, ..., m_k \}, \qquad m_i = g_i m$$

Докажем, что $g_1, ..., g_k$ принадлежат различным смежным классам по подгруппе $\mathrm{St}(m)$ и являются представителями всех классов:

- Пусть g_i, g_j принадлежат одному классу
  $$g_i^{-1}g_j \in \mathrm{St}(m) \implies g_i^{-1}g_j m = m \implies g_j m = g_i m \implies m_j = m_i \text{ – } \lightning$$
- Докажем, что любой элемент $g \in G$ попадает в смежный класс, содержащий некоторый g_i:
  $$gm \in \operatorname{Orb}(m) \implies \exists\, i : gm = m_i \implies gm = g_i m = g_i^{-1}gm = m \implies g_i^{-1}g \in \mathrm{St}(m)$$
  Значит, элементы g и g_i принадлежат одному смежному классу
  Получили, что $k = [G : \mathrm{St}(m)]$
  По теореме Лагранжа, выполнено $|G| = k \cdot |\operatorname{St}(m)|$

$\square$

34. Лемма Бернсайда, примеры применения

Лемма 2 (Бернсайда). G – конечная группа, M – конечное множество, G действует на M
Тогда количество орбит равно среднему арифметическому мощностей фиксаторов элементов G, т. е.

$$\frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix}(g)|$$

Доказательство. Рассмотрим количество всех пар (g, m), для которых выполнено $gm = m$:

- Если найти количество пар для каждого m, а затем просуммировать, получится $\sum_{m\in M} |\operatorname{St}(m)|$
- Если найти количество пар для каждого g, а затем просуммировать, получится $\sum_{g\in G} |\operatorname{Fix}(m)|$

Приравняем и разделим на $|G|$:

$$\frac{1}{|G|}\sum_{g\in G} |\operatorname{Fix}(g)| = \frac{1}{|G|}\sum_{m\in M} |\operatorname{St}(m)|$$

Достаточно доказать, что правая часть равна количеству орбит. Преобразуем её, используя свойство стабилизатора:

$$\frac{1}{|G|}\sum_{m\in M} |\operatorname{St}(m)| = \sum_{m\in M} \frac{|\operatorname{St}(m)|}{|G|} = \sum_{m\in M} \frac{1}{|\operatorname{Orb}(m)|}$$

Пусть есть n орбит, содержащих $a_1, a_2, \ldots,$ элементов
Запишем сумму в правой части:

$$\sum_{m\in M} \frac{1}{|\operatorname{Orb}(m)|} = \underbrace{\left(\frac{1}{a_1} + \frac{1}{a_1} + \ldots\right)}_{a_1 \text{ слаг.}} + \underbrace{\left(\frac{1}{a_2} + \frac{1}{a_2} + \ldots\right)}_{a_2 \text{ слаг.}} + \ldots\ldots\ldots\ldots\ldots$$

Следовательно, в каждой скобке сумма равна 1, а вся сумма равна n $\square$

Примеры.

1. Сколькими способами можно составить ожерелье из 5 чёрных и 5 белых бусин? Ожерелья считаются одинаковыми, если их можно перевести друг в друга поворотом или симметрией

   Решение. Пусть M – множество различных раскрасок ожерелья, зафиксированного в пространстве, G – группа самосовмещений ожерелья
   Тогда G состоит из 10 поворотов и 10 осевых симметрий:

Повороты	$\lvert\operatorname{Fix}\rvert$
$0°$	$C_{10}^5 = 252$
$36k°, \quad k = 1, 3, 7, 9$	0
$36k°, \quad k = 2, 4, 6, 8$	2
$180°$	0
Симметрии	
Относительно прямой, проходящей через вершины	$2 \cdot C_4^2 = 12$
Относительно прямой, проходящей через середины сторон	0

   Искомое число:
   $$\frac{1}{20}(1\cdot 252 + 4\cdot 0 + 4\cdot 2 + 1\cdot 0 + 5\cdot 12 + 5\cdot 0) = 16$$

2. Требеутся найти количество раскрасок прямоугольника $a \times b$ в k цветов с точностью до осевой или центральной симметрии

Решение. Пусть M – множество всех раскрасок прямоугольника, G – группа самосовмещений прямоугольника. Тогда количество раскрасок с точностью до симметрии – это количество орбит
Группа состоит из 4-х элементов:

- нейтральный e
- осевые симметрии σ_1, σ_2
- центральная симметрия τ

Фиксатор любого элемента группы – множество раскрасок, которые при данном преобразовании переходят сами в себя:

- $\mathrm{Fix}(e)$ – множество всех раскрасок, $|\mathrm{Fix}(e)| = k^{ab}$
- $\mathrm{Fix}(\sigma_{1,2})$ – множество раскрасок, симметричных относительно оси:
  - Раскраска, симметричная относительно горизонтальной оси, определяется раскраской верхней половины, и, в случае нечётного количества строк – раскраской средней строки
    Следовательно, она определяется раскраской прямоугольника $\lceil \frac{a}{2} \rceil \times b$
    Количество таких раскрасок равно $k^{\lceil a/2 \rceil b}$
  - Количество раскрасок, симметричных относительно вертикальной оси вычисляется аналогично, оно равно $k^{a \lceil b/2 \rceil}$
- $\mathrm{Fix}(\tau)$ – количество раскрасок, которые переходят в себя при центральной симметрии. Такая раскраска задаётся раскраской $\lceil \frac{ab}{2} \rceil$ клеток, количество раскрасок равно $k^{\lceil ab/2 \rceil}$

Количество орбит равно

$$\frac{1}{4}\left(k^{ab} + k^{\lceil a/2 \rceil b} + k^{a \lceil b/2 \rceil} + k^{\lceil ab/2 \rceil}\right)$$

35. Прямое произведение групп: определение, подгруппы прямого произведения

Определение 21. $(G, *), (H, \cdot)$ – группы
(Внешнее) прямое произведение G и H – это множество $G \times H$ с операцией $\circ$, определяемой равенством $(g_1, h_1) \circ (g_2, h_2) = (g_1 * g_2, h_1 \cdot h_2)$

Примечание. Аналогично определяется произведение нескольких групп

Теорема 12. Прямое произведение групп является группой

Доказательство. Пусть задано произведение групп $G \times H \times ...$

- Ассоциативность:

$$\Big((g_1, h_1, ...)(g_2, h_2, ...)\Big)(g_3, h_3, ...) = (g_1 g_2, h_1 h_2, ...)(g_3, h_3, ...) = (g_1 g_2 g_3, h_1 h_2 h_3, ...)$$

$$(g_1, h_1, ...)\Big((g_2, h_2, ...)(g_3, h_3, ...)\Big) = (g_1, h_1, ...)(g_2 g_3, h_2 h_3, ...) = (g_1 g_2 g_3, h_1 h_2 h_3, ...)$$

- Нейтральный:

$$e_{G \times H \times ...} = (e_G, e_H, ...)$$

- Обратный:

$$(g, h, ...)^{-1} = (g^{-1}, h^{-1}, ...)$$

□

Свойство.

- Если группы H_i конечны, то G тоже конечна, $|G| = |H_1| \cdot |H_2| \cdot ... \cdot |H_k|$
- Если хотя бы одна из H_i бесконечна, то G бесконечна

Напоминание. $A_1, A_2, ..., A_k$ – подмножества G
Произведением $A_1 A_2 ... A_k$ называется множество элементов $a_1 a_2 ... a_k$, где $a_i \in A_i$

Свойства (подгруппы прямого произведения). $G = G_1 \times G_2 \times ... \times G_k$, e_i – нейтральный элемент G_i
H_i – множество элементов вида $(e_1, ..., e_{i-1}, g_i, e_{i+1}, ..., e_k)$

1. $H_i \simeq G_i \quad \forall i$

   Доказательство. Отображение $f : G_i \to H_i$, заданное формулой

   $$f(x) = (e_1, ..., e_{i-1}, x, e_{i+1}, ..., e_k) \quad \text{является изоморфизмом}$$

   □

2. $H_i \lhd G \quad \forall i$

   Доказательство.

   - $H_i < G$
     Надо доказать, что у произведений элементов из H_i, все j-е компоненты (при $i \neq j$) равны e_j. Это верно, т. к. $e_j e_j = e_j$
     То же самое для обратных
   - $H_i \lhd G$
     Пусть $h \in H_i, \quad x \in G, \quad x = (g_1, ..., g_k)$

   $$\underset{j \neq i}{\forall j} \quad j\text{-я комп. } x^{-1}hx \text{ равна } g_j^{-1} e_j g_j = g_j^{-1} g_j = e_j \quad \Longrightarrow \quad x^{-1}hx \in H_i$$

   □

3. $\forall i \neq j, h_i \in H_i, h_j \in H_j \qquad h_i h_j = h_j h_i$

   Доказательство. Пусть $h_i = (e_1, ..., g_i, ..., e_j, ..., e_k), \quad h_j = (e_1, ..., g_j, ..., e_i, ..., e_k)$
   Тогда каждый из элементов $h_i h_j, h_j h_i$ равен $(e_1, ..., g_i, ..., g_j, ..., e_k)$ □

4. $H_i \cap H_1 ... H_{i-1} H_{i+1} ... H_k = \{ e \}$

   Доказательство. У элементов H_i все компоненты, кроме i-й равны нейтральным элементам
   У элементов произведения $H_1 ... H_{i-1} H_{i+1} ... H_k$, i-я компонента равна e_i
   Следовательно, у элемента из пересечения все компоненты – нейтральные □

5. $H_1 H_2 ... H_k = G$

   Доказательство. Элемент $(g_1, ..., g_k)$ равен произведению элементов $(e_1, ..., g_i, ..., e_k) \in H_i$
   □

6. $G / H_i \simeq G_1 \times ... \times G_{i-1} \times G_{i+1} \times ... \times G_k$

   Доказательство. Пусть $T \coloneqq G_1 \times ... \times G_{i-1} \times G_{i+1} \times ... \times G_k$
   Определим отображение $f : G \to T$ как

   $$f(g_1, ..., g_{i-1}, g_i, g_{i+1}, ..., g_k) = \varphi(g_1, ..., g_{i-1}, g_{i+1}, ..., g_k)$$

   Образ f равен T
   Ядро f состоит из элементов, которые φ отображает в $e_T = (e_1, ..., e_{i-1}, e_{i+1}, ..., e_k)$

   $$\ker f = \{ (e_1, ..., e_{i-1}, e_{i+1}, ..., e_k) \} = H_i$$

   Применяя теорему о гомоморфизме, получаем, что $G / H_i \simeq T$ □

36. Порядки элементов в прямом произведении. Прямое произведение циклических подгрупп

Лемма 3 (порядки элементов). $G = H_1 \times H_2 \times \ldots \times H_k, \qquad h_i \in H_i, \qquad g = (h_1, \ldots, h_k)$

1. $\exists\, i : \mathrm{ord}_{H_i}(h_i) = \infty \quad \Longrightarrow \quad \mathrm{ord}_G(g) = \infty$

   Доказательство. Пусть e_i – нейтральный элемент H_i, и e – нейтральный элемент G
   Пусть $\mathrm{ord}(g)$ конечен и равен n

   $$(e_1, \ldots, e_k) = e = g^n = (h_1^n, \ldots, h_k^n) \implies h_i^n = e_i \quad \forall n \implies \mathrm{ord}(h_i) \le n - \lightning$$

   □

2. $\forall i \quad \mathrm{ord}_{H_i}(h_i)$ конечен $\quad \Longrightarrow \quad \mathrm{ord}_G(g) = \text{НОД}\,(\mathrm{ord}_{H_1}(h_1), \ldots, \mathrm{ord}_{H_k}(h_k))$

   Доказательство. Положим $a_i \coloneqq \mathrm{ord}(h_i), \quad n \coloneqq \text{НОД}\,(a_1, \ldots, a_n)$
   Из свойств порядка следует, что

   $$h_i^{b_i} = e_i \iff b_i \,\vdots\, a_i$$

   - Докажем, что $n \ge \mathrm{ord}(g)$:
     Для этого достаточно проверить, что $g^n = e$

     $$n \,\vdots\, a_i \quad \forall i \implies g^n = (h_1^n, \ldots, h_k^n) = (e_1, \ldots, e_k) = e$$

   - Докажем, что $\mathrm{ord}(g) \ge n$:

     $$(h_1^{\mathrm{ord}(g)}, \ldots, h_k^{\mathrm{ord}(g)}) = g^{\mathrm{ord}(g)} = e = (e_1, \ldots, e_k) \implies h_i^{\mathrm{ord}(g)} = e_i \quad \forall i \implies$$
     $$\implies \mathrm{ord}(g) \,\vdots\, a_i \implies \mathrm{ord}(g) \,\vdots\, n \implies \mathrm{ord}(g) \ge n$$

   □

Теорема 13 (прямое произведение). $a_1, \ldots, a_k \in \mathbb{N}, \qquad G = \mathbb{Z}_{a_1} \times \ldots \times \mathbb{Z}_{a_k}, \qquad a \coloneqq a_1 \cdot \ldots \cdot a_k$

- $a_1, \ldots, a_k$ попарно взаимно просты $\implies G \simeq \mathbb{Z}_a$
- $a_1, \ldots, a_k$ **не** попарно взаимно просты $\implies G$ – **не** циклическая

Доказательство. Используем аддитивные обозначения:

- Нейтральный элемент группы G – это $0 = (\overline{0}, \ldots, \overline{0})$
- $x + x + \ldots + x = s \cdot x$

Выполнено $|G| = a_1 \ldots a_k$, следовательно,

$$G - \text{цикл.} \iff \exists\, g \in G : \mathrm{ord}(g) = a_1 \ldots a_k$$

Кроме того,

$$a_1, \ldots, a_k \text{ попарно вз. просты} \iff \text{НОД}\,(a_1, \ldots., a_k) = a_1 \ldots a_k$$

- $\mathrm{ord}_{H_i}(\overline{1}) = a_i \quad \forall i \implies \mathrm{ord}_G(\overline{1}, \ldots, \overline{1}) = \text{НОД}\,(a_1, \ldots, a_k) = a_1 \ldots a_k$
- Пусть $g \in G, \quad g = (h_1, \ldots, h_k)$
  По следствию к теореме Лагранжа,

  $$a_i \,\vdots\, \mathrm{ord}_{H_i}(h_i) \implies \text{НОД}\,(a_1, \ldots, a_k) \,\vdots\, \mathrm{ord}_{H_i}(h_i) \implies \text{НОД}\,(a_1, \ldots, a_k) \cdot h_i = \overline{0}$$

  $$\text{НОД}\,(a_1, \ldots, a_k) \cdot g = \Big(\text{НОД}\,(a_1, \ldots, , a_k) \cdot h_1, \ldots\ldots\ldots, \text{НОД}\,(a_1, \ldots, a_k) \cdot h_k\Big) = (\overline{0}, \ldots, \overline{0}) = 0$$

  $$\implies \forall g \in G \quad \mathrm{ord}(g) \le \text{НОД}\,(a_1, \ldots, a_k) \le a_1 a_2 \ldots a_k$$

□

37. Лемма о нормальных подгруппах с единичным пересечением. Прямое произведение подгрупп

Определение 22. G – группа, $\quad H_1, ..., H_k \lhd G$
Говорят, что G является (внутренним) прямым произведением подгрупп $H_1, ..., H_k$ (разложена в произведение подгрупп $H_1, ..., H_k$), если

1. $\forall g \in G \quad \exists! \underset{h_i \in H_i}{h_1, ..., h_k} : g = h_1 ... h_k$
2. $\forall \underset{i \neq j}{h_i \in H_i, h_j \in H_j} \quad h_i h_j = h_j h_i$

Обозначение. $G = H_1 \times ... \times H_k$

Лемма 4 (нормальные подгруппы с единичным пересечением). $H \lhd G, \quad K \lhd G, \qquad H \cap K = \{\, e \,\}$
Тогда элементы H коммутируют с элементами K

Доказательство. По свойствам коммутанта,

$$hk = kh \iff \underset{(h^{-1}k^{-1}hk)}{[h, k]} = e \iff \begin{cases} [h, k] \in H \\ [h, k] \in K \end{cases}$$

Докажем первое включение (второе – аналогично):
Запишем коммутант как $h^{-1}(k^{-1}hk)$

$$H \lhd G \implies \begin{Bmatrix} h^{-1} \in H \\ k^{-1}hk \in H \end{Bmatrix} \implies h^{-1}(k^{-1}hk) \in H$$

□

Теорема 14 (прямое произведение двух подгрупп). $H \lhd G, \quad K \lhd G, \qquad H \cap K = \{\, e \,\}, \qquad HK = G$

$$\implies G = H \times K$$

Доказательство. По лемме, элементы H коммутируют с элементами K
Условие $G = HK$ означает, что любой элемент $g \in G$ представим в виде $g = hk, \quad h \in H, k \in K$
Докажем единственность представления:
Пусть $h_1 k1 = h_2 k_2, \quad h_i \in H, k_i \in K$

$$\underbrace{h_2^{-1} h_1}_{\in H} = \underbrace{k_2 k_1^{-1}}_{\in K} \xRightarrow[H \cap K = \{\, e \,\}]{} \begin{cases} h_1 = h_2 \\ k_1 = k_2 \end{cases}$$

□

Теорема 15 (прямое прозведение нескольких подгрупп). $H_1 \lhd G, \ldots\ldots\ldots, H_k \lhd G$
$\forall i \quad H_1 ... H_{i-1} \cap H_i = \{\, e \,\}, \qquad H_1 ... H_k = G$

$$\implies G = H_1 \times ... \times H_k$$

Доказательство. Пусть $i \neq j$

- Докажем, что элементы из подгрупп H_i и H_j коммутируют:
  НУО считаем, что $i < j$

  $$\forall h_i \in H_i \quad h_i = e...eh_ie...e \implies H_i \subset H_1 ... H_{j-1} \implies H_i \cap H_j = \{\, e \,\} \xRightarrow[\text{лемма}]{} \text{эл-ты коммутируют}$$

- Докажем, что представление элемента $g \in G$ в виде произвдения $g = h_1 h_2 ... h_k, \quad h_i \ni H_i$ единственно:

Пусть
$$h_1h_2...h_k = h'_1h'_2...h'_k, \qquad h_i, h'_i \in H_i, \qquad \exists\, s : \begin{cases} h_s \neq h'_s \\ h_i = h'_i \quad \forall i > s \end{cases}$$
Тогда выполнено
$$h_1h_2...h_s = h'_1h'_2...h'_s$$
Следовательно,
$$(h_1h_1'^{-1})(h_2h_2'^{-1})...(h_{s-1}h_{s-1}'^{-1}) = h'_sh_s^{-1}$$
Этот элемент принадлежит $H_1...H_{s-1} \cap H_s$, следовательно, он равен e. Получили, что
$$h'_sh_s^{-1} = e \implies h'_s = h_s$$
Это противоречит выбору s

□

38. Разложение конечной циклической группы в прямое произведение двух подгрупп

Теорема 16. G – конечная циклическая группа, $\quad |G| = mn, \quad$ НОД$\,(m, n) = 1$
Тогда G можно разложить в прямое произведение двух подгрупп, изоморфных $\mathbb{Z}_m$ и $\mathbb{Z}_n$

Доказательство. Положим
$$G := \langle a \rangle\,, \qquad b := a^m, \qquad c := a^n, \qquad H := \langle b \rangle\,, \qquad K := \langle c \rangle$$

- Проверим, что $\mathrm{ord}(b) = n$ и $\mathrm{ord}(c) = m$:
  Имеем $b^n = a^{mn} = e$
  $$\forall 0 < t < n \quad \begin{Bmatrix} b^t = a^{mt} \\ 0 < mt < mn \end{Bmatrix} \implies a^{mt} \neq e \implies b^t \neq e$$
  Для c аналогично
  Получаем, что $|H| = n, |K| = n$
  Эти подгруппы циклические, следовательно, $H \simeq \mathbb{Z}_n, K \simeq \mathbb{Z}_m$
- Проверим, что $G = H \times K$:
  - Условие $H, K \lhd G$ выполнено, так как любая подгруппа абелевой группы нормальна
  - Проверим, что $H \cap K = \{\, e \,\}$:
    Пусть $x \in H \cap K$ и $x = a^t$
    $$\exists\, s, r : \begin{Bmatrix} x = b^s = a^{ms} \\ x = c^r = a^{nr} \end{Bmatrix} \implies a^{ms} = a^{nr} \implies ms - nr \,\vdots\, mn \implies \begin{cases} nr \,\vdots\, m \implies r \,\vdots\, m \\ ms \,\vdots\, n \implies s \,\vdots\, n \end{cases}$$
    Получили, что $ms \,\vdots\, mn$ и $x = a^{ms} = e$
  - Докажем, что $HK = G$:
    Элементы произведения HK имеют вид $b^sc^r = a^{ms+nr}$
    По теореме о линейном представлении НОД,
    $$\exists\, s_0, r_0 : ms_0 + nr_0 = 1 \implies \forall x \quad a^x = a^{ms_0x + nr_0x} \in HK$$

□

39. Разложение конечной циклической группы в прямое произведение примарных подгрупп

Определение 23. Группа называется примарной, если она изоморфна $\mathbb{Z}$ или $\mathbb{Z}_{p^n}$ для некоторого $p \in \mathbb{P}$

Теорема 17. G – конечная циклическая группа
Тогда G можно разложить в прямое произведение нескольких примарных подгрупп

Доказательство. Пусть

$$|G| := n, \qquad G := \langle a \rangle, \qquad n := p_1^{s_1} ... p_k^{s_k}, \quad p_i \in \mathbb{P}, \qquad \forall i \quad q_i := \frac{n}{p^{s_i}}, \quad b_i := a^{q_i}, \quad H_i := \langle b_i \rangle$$

Тогда $\mathrm{ord}(b_i) = p^{s_i}$, и, следовательно, H_i – примарная подгруппа, изоморфная $\mathbb{Z}_{p^{s_i}}$
Докажем, что $G = H_1 \times ... \times H_k$:

- Условие $H_i \lhd G$ выполнено, так как любая подгруппа абелевой группы нормальна
- Проверим, что $H_1 ... H_{i-1} \cap H_i = \{ e \}$:
  Пусть x принадлежит пересечению

$$\left.\begin{aligned} &x \in H_1 ... H_{i-1} \implies x = b_1^{t_1} ... b_{i-1}^{t_{i-1}} = a^{q_1 t_1 + ... + q_{i-1} t_{i-1}}, \qquad t_1, ..., t_{i-1} \in \mathbb{Z} \\ &x \in H_i \implies xx = b_i^{t_i} = a^{q_i t_i}, \qquad t_i \in \mathbb{Z} \end{aligned}\right\} \implies$$
$$\implies q_1 t_1 + ... + q_{i-1} t_{i-1} - q_i t_i \vdots n \vdots p_i^{s_i}$$

  Числа $q_1, ..., q_{i-1}$ делятся на $p_i^{s_i}$, а значит, $q_i t_i \vdots n$ и $x = a^{q_i t_i} = e$

- Докажем, что $H_1 ... H_k = G$:
  Элементы произведения $H_1 ... H_k$ имеют вид $a^{q_1 t_1 + ... + q_k t_k}$

$$\text{НОД}(q_1, ..., q_k) = 1 \implies \forall x \in \mathbb{Z} \quad x = q_1 t_1 + ... + q_k t_k, \qquad a^x \in H_1 ... H_k$$

□

Следствие. G – циклическая группа, $|G| = m_1 m_2 ... m_k$, $m_1, ..., m_k$ попарно взаимно просты
Тогда G можно разложить в прямое произведение подгрупп, изоморфных $\mathbb{Z}_{m_1}, ..., \mathbb{Z}_{m_k}$

Доказательство. Нужные группы – произведения нескольких (или одной) примарных □

40. Определение евклидова и унитарного пространства. Углы и расстояния. Неравенство Коши

Обозначение. $\overline{a} = \begin{cases} a & \text{в евклидовом пространстве} \\ \overline{a} & \text{в унитраном пространстве} \end{cases}$

Определение 24. Векторное пространство над $\mathbb{R}$ будем называть вещественным
Векторное пространство над $\mathbb{C}$ будем называть комплексным

Определение 25. V – вещественое векторное пространство
Скалярным произведением на V называется функция $(\cdot, \cdot) : V \times V \to \mathbb{R}$, обладающая следующими свойствами:

1. Линейность по первому аргументу: $(au + bv, w) = a(u, w) + b(v, w)$
2. Симметричность: $(u, v) = (v, u)$
3. Положительная определённость: $(v, v) > 0 \quad \forall v \in (V \setminus \{ 0 \})$

Примечание. Из первых двух свойств следует линейность по второму аргументу
Из линейности следует, что $(v, 0) = (0, v) = 0$

Определение 26. Евклидовым пространством называется конечномерное вещественное векторное пространство со скалярным произведением

Определение 27. V – комплексное векторное пространство
Скалярным произведением на V называется функция $(\cdot,\cdot) : V \times V \to \mathbb{C}$, обладающая следующими свойствами:

1. Линейность по первому аргументу: $(au + bv) = a(u, w) + b(v, w)$
2. $(u, v) = \overline{(v, u)}$
3. Положительная определённость:
   (v, v) является вещественным положительным числом $\forall v \in (V \setminus \{\, 0 \,\})$

Примечание. Скалярное произведение на комплексном пространстве не линейно по второму аргументу, но выполняется равенство:

$$(u, av + bw) = \overline{a}(u, v) + \overline{b}(u, w)$$

Определение 28. Унитарным пространством называется конечномерное комплексное векторное пространство со скалярным произведением

Определение 29. Длина вектора v в евклидовом или унитарном пространстве определяется как

$$|v| = \sqrt{(v, v)}$$

Определение 30. Угол между векторами u и v в евклидовом пространстве определяется как

$$\arccos\left(\frac{(u, v)}{|u| \cdot |v|}\right)$$

Примечание. В унитарном пространстве углы не определяются

Теорема 18 (неравенство Коши)**.** V – евклидово или унитарное пространство
Для любых $u, v \in V$ выполнено

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

Равенство достигается тогда и только тогда, когда $u = sv$ для некторого $s \in \mathbb{R}, \mathbb{C}$ или при $v = 0$

Доказательство. Будем пользоваться линейностью по первому аргументу и равенством $(u, av+bw) = \overline{a}(u, v) + \overline{b}(u, w)$
Пусть $v \neq 0$. Тогда

$$(v, v) > 0, \qquad (v, v) \in \mathbb{R} \tag{3}$$

Положим

$$a \coloneqq (u, u), \qquad b \coloneqq (u, v), \qquad c \coloneqq (v, v), \qquad t \coloneqq \frac{b}{c}$$

Заметим, что $(3) \implies \overline{t}c = \overline{b}$
Применим свойство положительной определённости к вектору $u - tv$:

$$0 \leq (u-tv, u-tv) = (u, u)+(u, -tv)+(-tv, u)+(-tv, -tv) = a-\overline{t}b-t\overline{b}+t\overline{t}c = a-\frac{b\overline{b}}{c}-t(-\overline{b}+\overline{t}c) = a-\frac{|b|^2}{c}$$

Получаем, что $a \geq \dfrac{|b|^2}{c}$
Умножая на положительное число c, получаем нужное неравенство
Равенство достигается тогда и только тогда, когда $(u - tv, u - tv) = 0$, т. е. $u - tv = 0$ $\square$

Следствие (неравенство Коши-Буняковского)**.** Для любых $x_1, ..., x_n, y_1, ..., y_n \in \mathbb{R}$ выполнено

$$(x_1y_1 + ... + x_ny_n)^2 \leq (x_1^2 + ... + x_n^2)(y_1^2 + ... + y_n^2)$$

Следствие (неравенство треугольника). Для любых векторов u, v евклидова или унитарного пространства выполнено $|u+v| \le |u| + |v|$

Доказательство. Возведём левую часть в квадрат и оценим сверху, пользуясь неравенством Коши:

$$|u+v|^2 = (u+v, u+v) = |(u+v, u+v)| = |(u,u)+(u,v)+(v,u)+(v,v)| \le$$
$$\le |(u,u)| + |(u,v)| + |(v,u)| + |(v,v)| \underset{\text{(Коши)}}{\le} (u,u) + \sqrt{(u,u)(v,v)} + \sqrt{(u,u)(v,v)} + (v,v) = (|u|+|v|)^2$$

□

41. Матрица Грама: вычисление скалярного произведения, замена базиса

Определение 31. V – евклидово или унитарное пространство размерности n
Матрицей Грама для набора $e_1, \ldots, e_n$ называется матрица $\Gamma = (g_{ij})$, где $g_{ij} = e_i e_j$

Определение 32. Матрица с условием $A^T = A$ называется симметричной, а с условием $A^T = \overline{A}$ – эрмитовой

Свойство. Матрица Грама является симметричной (эрмитовой)

Теорема 19 (вычисление скалярного произведения).
V – евклидово (унитарное) пространство с базисом $e_1, \ldots, e_n$, $\quad \Gamma(g_{ij})$ – матрица Грама в этом базисе

1. $\forall \begin{cases} u = x_1e_1 + \ldots + x_ne_n \\ v = y_1e_1 + \ldots + y_ne_n \end{cases} \qquad (u,v) = \sum_{i,j} x_i\overline{y_j}g_{ij}$

   Доказательство. В евклидовом и унитарном пространстве выполняется аддитивность по обеим координатам, следовательно,

   $$(u,v) = \sum_{i,j}(x_ie_i,\ y_je_j) = \sum x_i\overline{y_j}(e_i,e_j)\sum = x_i\overline{y_j}g_{ij}$$

   □

2. $(u,v) = X^T\Gamma\overline{Y}$

   Доказательство. Запишем матрицы X^T и Y в стандартном виде $X^T = (x_{ki})$ и $Y = (y_{il})$
   Тогда $x_{1i} = x_i$ и $y_{j1} = y_j$
   Применим формулу произведения трёх матриц к $X\Gamma\overline{Y}$:
   Произведение – матрица 1×1, её единственный элемент равен $\sum_{i,j} x_{1i}\overline{g_{ij}}y_{j1}$ □

3. Если для матрицы Γ' выполнено $(u,v) = X^T\Gamma'\overline{Y}$, то Γ' является матрицей Грама

   Доказательство. Пусть $\Gamma = (g_{ij})$ и $\Gamma' = (g'_{ij})$
   Возьмём $u = e_i,\ v = e_j$
   Тогда X и Y – векторы, у которых i-я и j-я координаты равны 1, а остальные – 0
   Перемножая матрицы получаем, что $(e_j, e_i) = g'_{ij}$ □

Теорема 20 (замена базиса). Дано евклидово (унитарное) пространство
Γ, Γ' – матрицы Грама в базисах e_i и e'_i, $\qquad C$ – матрица перехода от e_i к e'_i

$$\implies \Gamma' = C^T\Gamma\overline{C}$$

Доказательство. Положим $\Gamma'' := C^T\Gamma\overline{C}$

Пусть u, v – векторы, X, X', Y, Y' – их столбцы координат в базисах e_i, e_i'. Тогда

$$X = CX', \qquad Y = CY', \qquad (u, v) = X^T \Gamma \overline{Y}$$

Нужно проверить, что $(u, v) = (X')^T \Gamma'' \overline{Y'}$. Подставим:

$$X^T \Gamma \overline{Y} = (CX')^T \Gamma (\overline{CY'}) = X' C^T \Gamma \overline{C} \overline{Y'} = X' \Gamma'' \overline{Y'}$$

□

42. Свойства ортогональных векторов. Процесс ортогонализации Грама-Шмидта

Определение 33. Векторы u и v евклидова (унитарного) пространства называются ортогональными, если $(u, v) = 0$

Обозначение. $u \perp v$

Свойства.

1. $u \perp v \implies v \perp u$

   Доказательство. $(v, u) = \overline{(u, v)} = \overline{0} = 0$ □

2. Если u ортогонален векторам $v_1, ..., v_n$, то он ортогонален любой их линейной комбинации

   Доказательство. $(a_1 v_1 + ... + a_k v_k,\ u) = a_1(v_1, u) + ... + a_k(v_k, u) = a_1 \cdot 0 + ... + a_k \cdot 0 = 0$ □

3. Если u ортогонален любому вектору, то $u = 0$

   Доказательство. $u \perp u \implies (u, u) = 0 \implies u = 0$ □

4. Если u ортогонален всем векторам некоторого базиса, то $u = 0$

   Доказательство. Следует из предыдущих двух □

5. $e_1, ..., e_k$ – базис, u, v – некоторые векторы
   Если $\forall i \quad (u, e_i) = (v, e_i)$, то $u = v$

   Доказательство. Применим предыдущее свойство к $(u - v)$ □

6. Попарно ортогональные ненулевые векторы ЛНЗ

   Доказательство. Пусть $a_1 e_1 + ... + a_k e_k = 0$. Тогда

   $$\forall i \qquad 0 = (a_1 e_1 + ... + a_k e_k,\ e_i) = a_i (e_i, e_i) \implies a_i = 0$$

   □

Теорема 21 (ортогонализация Грама-Шмидта)**.** $u_1, ..., u_n$ – ЛНЗ в евклидовом (унитарном) пр-ве
Тогда существуют попарно ортогональные векторы $x_1, ..., x_n$, такие, что

$$\langle x_1, ..., x_i \rangle = \langle u_1, ..., u_i \rangle \quad \forall i$$

Доказательство.

- Положим $x_1 := u_1$
- Пусть уже построены ортогональные векторы $x_1, ..., x_k$, такие, что

  $$\langle x_1, ..., x_i \rangle = \langle u_1, ..., u_i \rangle \quad \forall i \le k$$

  Заметим, что $x_i \neq 0 \quad \forall i$,т. к.

  $$\dim \langle x_1, ..., x_{i-1}, 0 \rangle = \dim \langle x_1, ..., x_{i-1} \rangle \le i - 1 < i = \dim \langle u_1, ..., u_i \rangle$$

Докажем, что сущестует вектор x_{k+1}, такой, что

$$\begin{cases} x_{k+1} \perp v_i \quad \forall i \le k & (4) \\ \langle x_1, ..., x_k, x_{k+1}\rangle = \langle u_1, ..., u_k, u_{k+1}\rangle & (5) \end{cases}$$

Будем искать x_{k+1} в виде

$$x_{k+1} = u_{k+1} - a_1 x_1 - ... - a_k x_k$$

где $a_1, ..., a_k$ – скаляры
Выполнено $\langle u_1, ..., u_i, u_{k+1}\rangle = \langle x_1, ..., x_i, u_{k+1}\rangle$ и для любых скаляров $a_1, ..., a_k$ выполнено

$$\langle x_1, ..., x_i, u_{k+1}\rangle = \langle x_1, ..., x_i, u_{k+1} - a_1 x_1 - ... - a_k x_k\rangle$$

Следовательно, для любого набора $a_1, ..., a_k$ выполнено условие (5)
Найдём такой набор, для которого выполнено условие (4):
Запишем скалярное произведение:

$$(x_{k+1}, x_i) = (u_{k+1} - a_1 x_1 - ... - a_i x_i - ... - a_k x_k,\ x_i) =$$
$$= (u_{k+1}, x_i) - a_1(x_1, x_i) - ... - a_i(x_i, x_i) - ... + a_k(x_k, x_i) = (u_{k+1}, x_i) - a_1 \cdot 0 - ... - a_i(x_i, x_i) - ... - a_k \cdot 0 =$$
$$= (u_{k+1}, x_i) + a_i(x_i, x_i)$$

Подойдут скаляры

$$a_i = \frac{(u_{k+1}, x_i)}{(x_i, x_i)}$$

□

Определение 34. Вектор называтся нормированным, если его длина равна 1

Определение 35. Базис называется ортонормированным, если он состоит из попарно ортогональных нормированных векторов

Следствие. V – евклидово или унитарное пространство

1. Существует ОНБ пространства V
2. U – подпространство V
   Тогда существует ОНБ $e_1, ..., e_n$ пространства V, такой, что при некотором $k \le n$ векторы $e_1, ..., e_k$ образуют базис U

43. Ортогональное дополнение

Определение 36. V – евклидово или унитарное пространство, U – подпространство V
Ортогональным дополнением к подпространству V называется множество

$$U^\perp := \{\, x \mid x \perp u \quad \forall u \in U \,\}$$

Свойства. V – евклидово или унитарное пространство, U, W – подпространства V

1. $U^\perp$ является подпространством

   Доказательство. $x \in U^\perp \iff (x, u) = 0 \quad \forall u \in U$
   Применим линейность □

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

Доказательство. Достаточно доказать, что существуют такие базисы U и $U^\perp$, что их объединение является базисом V
Выберем ОНБ $e_1...., e_k, g_1, ..., e_m$ пространства V так, что $e_1, ..., e_k$ – базис U
Докажем, что g_i – базис $U^\perp$
Проверим, что g_i порождают $U^\perp$:
Пусть $v \in U^\perp$
Разложим v по базису всего пространства: $v = \sum x_i e_i + \sum y_i g_i$

$$x_i = (v, e_i) = 0 \quad \forall i$$

Следовательно, $v = \sum y_i g_i$
Набор векторов g_i является ЛНЗ, т. к. это – подмножество базиса
Следовательно, векторы g_i образуют базис $U^\perp$ □

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

Доказательство. Следует из предыдущего □

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

Доказательство. Любой вектор из U ортогонален всем векторам из $U^\perp$
Следовательно, $U \subset U^\perp$
Применяя предыдущее к U и $U^\perp$, получаем, что

$$\dim U + \dim U^\perp = \dim V = \dim U^\perp + \dim (U^\perp)^\perp \implies \dim (U^\perp)^\perp = \dim U$$

□

5. $U \subset W \implies W^\perp \subset U^\perp$

Доказательство. Если $v \in W^\perp$, то он ортогонален всем векторам из W
Следовательно, он ортогонален всем векторам из U □

6. $(U + W)^\perp = U^\perp \cap W^\perp$

Доказательство.

- $\subset$
Применим предыдущее:

$$\left.\begin{matrix} U \subset (U + W) \implies (U + W)^\perp \subset U^\perp \\ W \subset (U + W) \implies (U + W)^\perp \subset W^\perp \end{matrix}\right\} \implies (U + W)^\perp \subset (U^\perp \cap W^\perp)$$

- $\supset$
Пусть $v \in (U^\perp \cap W^\perp)$
Нужно доказать, что v ортогонален любому вектору из $(U + W)$, т. е.

$$v \perp (u + w) \quad \forall u \in U, w \in W$$

Это следует из того, что $v \perp u$ и $v \perp w$

□

7. $(U \cap W)^\perp = U^\perp + W^\perp$

Доказательство. Применим предыдущее к $U^\perp$ и $W^\perp$ и воспользуемся (4):

$$(U^\perp + W^\perp)^\perp = (U^\perp)^\perp \cap (W^\perp)^\perp = U \cap W$$

Возьмём ортогональное дополнение к обеим частям, получим нужное равенство □

Определение 37. V – евклидово или унитарное пространство, U – подпространство V, $v \in V$

Проекцией вектора v на подпространство U называется такой вектор p, что

$$\begin{cases} p \in U \\ v - p \in U^{\perp} \end{cases}$$

Вектор $(v-p)$ называется ортогональным дополнением

Свойство. Для любых v и U существует единственная проекция v на U

Доказательство. Утверждение следует из того, что $U \oplus U^{\perp} = V$ □

44. Ортогональные и унитарные матрицы

Определение 38. Квадратная матрица A с вещественными элементами называется ортогональной, если $AA^T = E$
Квадратная матрица A с комплексными элементами называется унитарной, если $A\overline{A}^T = E$

Свойства.

1. Ортогональные (унитарные) матрицы порядка n образуют группу по умножению

   Доказательство. Докажем для унитарных:
   Нужно доказать два утверждения:

   (a) если A и B – унитарные матрицы, то AB – унитарная матрица

   $$(AB)(\overline{AB})^T = AB\overline{B}^T\overline{A}^T = AE\overline{A}^T = A\overline{A}^T = E$$

   (b) если A – унитарная матрица, то A обратима и A^{-1} является унитарной матрицей
   Из равенства $A\overline{A}^T = E$ следует, что A обратима, и $A^{-1} = \overline{A}^T$
   Проверим, что A^{-1} унитарна:

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

   □

2. A – квадратная матрица порядка n с вещественными (комплексными) элементами
   Следующие условия равносильны:

   (a) A – ортогональная (унитарная)

   (b) строки A образуют ОНБ $\mathbb{R}^n$ $(\mathbb{C}^n)$

   (c) столбцы A образуют ОНБ $\mathbb{R}^n$ $(\mathbb{C}^n)$

Доказательство.

- Докажем $2a \iff 2b$ для унитарной матрицы:
  Пусть $X_1, ..., X_n$ – строки A и $B := A\overline{A}^T, \quad B = (b_{ij})$
  Тогда $\overline{X_1}^T, ..., \overline{X_n}^T$ – столбцы $\overline{A}^T$, и

$$b_{ij} = X_i \overline{X_j}^T = (X_i, X_j)$$

  Таким образом,

$$A \text{ – унитарная} \iff B = E \iff b_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases} \iff X_i \text{ – ОНБ}$$

- Доказательство $2a \iff 2c$ аналогично, нужно рассмотреть равенство $\overline{A}^T A = E$

□

3. u_i – ОНБ, v_i – базис, C – матрица перехода $u_i \to v_i$
   C – ортогональная (унитарная) $\iff$ v_i – ОНБ

Доказательство. Докажем для унитарной
Пусть $C = (c_{ij})$, и C_i – это i-й столбец матрицы C, то есть

$$C_i = \begin{pmatrix} c_{1i} \\ . \\ . \\ . \\ c_{ni} \end{pmatrix}$$

Запишем $(v_i,\ v_j)$ и воспользуемся тем, что u_i – ОНБ:

$$(v_i, v_j) = (c_{1i}u_1 + ... + c_{ni}u_n,\ c_{1j}u_1 + ... + c_{nj}u_n) = \sum_{s,t} c_{ti}\overline{c_{tj}}\underbrace{(u_s, u_t)}_{=1} = c_{1i}\overline{c_{1j}} + ... + c_{ni}\overline{c_{nj}} = C_i^T \overline{C_j}$$

Следовательно, v_i – ОНБ $\iff$ C_i – ОНБ в $\mathbb{C}^n$
Применяя предыдущее свойство, получаем нужное утверждение □

45. Сопряжённый оператор

Напоминание. Оператором на векторном пространстве V называется линейное отображение $V \to V$

Обозначение. Будем обозначать операторы в евклидовом или унитарном пространстве (если не обговорено другое) буквами $\mathcal{A}, \mathcal{B}, ...$, а их матрицы в некотором базисе – буквами $A, B, ...$

Обозначение. В записи $\mathcal{A}(x)$ будем опускать скобки и писать $\mathcal{A}x$

Напоминание. Столбцы матрицы A – это столбцы координат векторов $\mathcal{A}e_i$ в выбранном базисе
Выполнено равенство $AX = \mathcal{A}x$, где X – столбец координат вектора x

Определение 39. $\mathcal{B}$ называется сопряжённым к $\mathcal{A}$, если

$$(\mathcal{A}x,\ y) = (x,\ \mathcal{B}y) \quad \forall x, y$$

Обозначение. $\mathcal{A}^*$

Теорема 22 (существование и единственность сопряжённого оператора).

1. Для любого $\mathcal{A}$ существует единственный $\mathcal{A}^*$
2. Пусть выбран базис, и Γ – матрица Грама в этом базисе

$$A^* = \overline{\Gamma^{-1}A^T\Gamma}$$

Доказательство. Докажем два утверждения:

- Если $\mathcal{B}$ – оператор, заданный формулой из (2), то $(\mathcal{A}x,\ y) = (x,\ \mathcal{B}y) \quad \forall x, y$
  Будем доказывать для унитарного пространства
  Пусть X, Y – столбцы координат векторов x, y

$$(\mathcal{A}x,\ y) = (AX)^T \Gamma \overline{Y} = X^T A^T \Gamma \overline{Y}$$

$$(x,\ \mathcal{B}y) = X^T \Gamma \overline{BY} = X^T \Gamma \overline{\overline{\Gamma^{-1} A^T \Gamma} Y} = X^T \Gamma \Gamma^{-1} A^T \Gamma \overline{Y} = X^T A^T \Gamma \overline{Y}$$

- Если $\mathcal{B}_1, \mathcal{B}_1$ – такие операторы, что $\begin{cases} (\mathcal{A}x,\ y) = (x,\ \mathcal{B}_1 y) \\ (\mathcal{A}x,\ y) = (x,\ \mathcal{B}_2 y) \end{cases} \quad \forall x, y$, то $\mathcal{B}_1 = \mathcal{B}_2$

$$0 = (x,\ \mathcal{B}_1 y) - (x,\ \mathcal{B}_2 y) = \Big(x,\ (\mathcal{B}_1 y - \mathcal{B}_2 y)\Big) \quad \forall x, y$$

  Вектор $(\mathcal{B}_1 y - \mathcal{B}_2 y)$ ортогонален любому вектору $x \in V$, значит, он равен 0, и $\mathcal{B}_1 y = \mathcal{B}_2 y$

$\square$

Определение 40. Подпространство U называется инвариантным для $\mathcal{A}$, если

$$\forall x \in U \quad \mathcal{A}x \in U$$

Свойства.

1. В случае ОНБ выполнено $A* = \overline{A}^T$

   Доказательство. В ОНБ выполнено $\Gamma = E$ $\square$

2. $(\mathcal{A}^*)^* = \mathcal{A}$

   Доказательство. Нужно проверить, что $\mathcal{A}$ является сопряжённым к $\mathcal{A}^*$, то есть

$$(\mathcal{A}^* x,\ y) = (x,\ \mathcal{A}y) \quad \forall x, y$$

   Левая часть равна $\overline{(y,\ \mathcal{A}^* x)}$, правая – $\overline{\mathcal{A}y,\ x}$
   Они равны по определению сопряжённого оператора, применённого к паре y, x $\square$

3. (полуторалинейность)

$$\begin{cases} (\mathcal{A} + \mathcal{B})^* = \mathcal{A}^* + \mathcal{B}^* \\ (k\mathcal{A})^* = \overline{k}\mathcal{A}^* \quad \forall k \in \mathbb{R}(\mathbb{C}) \end{cases}$$

   Доказательство.

   - Докажем второе равенство:
     Проверим, что оператор $\overline{k}\mathcal{A}^*$ является сопряжённым к $k\mathcal{A}$:

$$\Big((k\mathcal{A})x,\ y\Big) = \Big(k(\mathcal{A}x),\ y\Big) = k(\mathcal{A}x,\ y) = k(x,\ \mathcal{A}^* y) = (x,\ \overline{k}\mathcal{A}^* y) = \Big(x,\ (\overline{k}\mathcal{A}^*)y\Big)$$

   - Первое равенство доказывается аналогично

   $\square$

4. $(\mathcal{A}\mathcal{B})^* = \mathcal{B}^* \mathcal{A}^*$

Доказательство.

$$\Big((\mathcal{A}\mathcal{B})x,\ y\Big) = \Big(\mathcal{A}(\mathcal{B}x),\ y\Big) = (\mathcal{B}x,\ \mathcal{A}^* y) = \Big(x,\ \mathcal{B}^*(\mathcal{A}^* y)\Big) = \Big(x, (\mathcal{B}^*\mathcal{A}^*)y\Big)$$

Значит, $\mathcal{B}^*\mathcal{A}^*$ является сопряжённым к $\mathcal{A}\mathcal{B}$ □

5. Если U инвариантно для $\mathcal{A}$, то $U^\perp$ инвариантно для $\mathcal{A}^*$

Доказательство. Пусть $y \in U^\perp$
Нужно доказать, что $\mathcal{A}^* y \in U^\perp$, то есть $\mathcal{A}^* y \perp x \quad \forall x \in U$
Тогда

$$\forall x \in U \quad \mathcal{A}x \in U \quad \Longrightarrow y \perp \mathcal{A}x$$

Запишем скалярное произведение:

$$0 = (\mathcal{A}x,\ y) = (x,\ \mathcal{A}^* y) \implies \mathcal{A}^* y \perp x$$

□

Обозначение. $\mathcal{E}$ – тождественный оператор

Определение 41. $\mathcal{A}$ называется

- Нормальным, если $\mathcal{A}\mathcal{A}^* = \mathcal{A}^*\mathcal{A}$
- Ортогональным (унитарным), если $\mathcal{A}\mathcal{A}^* = \mathcal{A}^*\mathcal{A} = \mathcal{E}$
- Самосопряжённым, если $\mathcal{A} = \mathcal{A}^*$

Определение 42. Матрица A называется нормальной, если $A\overline{A}^T = \overline{A}^T A$

46. Собственные числа и собственные векторы

В этом вопросе рассматривается проивольное векторное пространство над произвольным полем

Определение 43. $\mathcal{A}$ – оператор, действующий на векторном пространстве V
Число λ называется собственным числом $\mathcal{A}$, если существует ненулевой вектор v, такой, что $\mathcal{A}v = \lambda v$
Если λ – с. ч. $\mathcal{A}$, то любой вектор, удовлетворяющий условию $\mathcal{A}v = \lambda v$, называется собственным вектором $\mathcal{A}$, соотвестсвующим λ

Определение 44. A – квадратная матрица
Число λ называется собственным числом A, если существует ненулевой столбец X, такой, что $AX = \lambda X$
Если λ – с. ч. A, то любой столбец X, удовлетворяющий условию $AX = \lambda X$, называется собственным столбцом A, соотвестсвующим λ

Определение 45. A – квадратная матрица
Характеристическим многочленом A называется многочлен от t, равный $\det(A - tE)$

Обозначение. $\chi(t), \chi_A(t)$

Свойства. $A = (a_{ij})$ – матрица порядка n, и $\chi(t)$ – её характеристический многочлен

1. $\chi(t)$ является многочленом
2. $\deg \chi = n$
3. Старший коэффициент $\chi(t)$ равен $(-1)^n$
4. Свободный член равен $\det A$

Доказательство. Подставим $t = 0$ □

5. Коэффициент при t^{n-1} равен $(-1)^{n-1}(a_{11} + ... + a_{nn})$

Доказательство. Без доказательства □

Теорема 23 (о корнях характеристического многочлена)**.** Число λ является с. ч. матрицы A тогда и только тогда, когда оно является корнем характеристического многочлена A

Доказательство.

$$\lambda \text{ является с. ч.} \iff \exists \underset{\text{не все равны нулю}}{x_1, ..., x_n} : \begin{pmatrix} a_{11} & ... & a_{1n} \\ . & . & . \\ a_{n1} & ... & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ . \\ . \\ . \\ x_n \end{pmatrix} = \lambda \begin{pmatrix} x_1 \\ . \\ . \\ . \\ x_n \end{pmatrix} \iff$$

$$\iff \text{система} \begin{cases} a_{11}x_1 + ... + a_{1n}x_n = \lambda x_1 \\ \dots\dots\dots\dots\dots\dots \\ a_{11}x_1 + ... + a_{nn}x_n = \lambda x_n \end{cases} \text{имеет ненулевое решение} \iff$$

$$\iff \text{система} \begin{cases} (a_{11} - \lambda)x_1 + ... + a_{1n}x_n = 0 \\ \dots\dots\dots\dots\dots\dots \\ a_{11}x_1 + ... + (a_{nn} - \lambda)x_n = 0 \end{cases} \text{имеет ненулевое решение} \iff$$

$$\iff \text{однородная система с матрицей } (A - \lambda E) \text{ имеет ненулевое решение}$$

Если $\det(A - \lambda E) \neq 0$, то по теореме Крамера, система имеет единственное решение
Это решение – $x_1 = ... = x_n = 0$

- Если $\det(A - \lambda E) = 0$, то $\text{rk}(A - \lambda E) \leq n - 1 < n$
По теореме о пространстве решений однородной системы, размерность пространства решений не равна 0, и, следовательно, пространство решений не равно $\{0\}$
Значит, в этом случае система имеет ненулевое решение

□

Определение 46. $\mathcal{A}$ – оператор на конечномерном векторном пространстве V
Характеристическим многочленом $\mathcal{A}$ назыается характеристический многочлен его матрицы в произвольном базисе

Обозначение. $\chi\mathcal{A}$

Свойства.

1. Характ. многочлен не зависит от выбора базиса

Доказательство. Пусть A, B – матрицы оператора в разных базисах, C – матрица перехода от первого базиса ко второму
Тогда $B = C^{-1}AC$

$$B - tE = C^{-1}AC - C^{-1}(tE)C = C^{-1}(A - tE)C$$

$$\chi_B(t) = \det(B - tE) = \det(C^{-1})\det(A - tE)\det(C) = \det(A - tE) = \chi_A(t)$$

□

2. С. ч. оператора на конечномерном пространстве совпадают с корнями его характ. многочлена

Доказательство. С. ч. оператора совпадают с с. ч. его матрицы в произвольном баисе, т. к. если X – столбец координат v, то

$$\mathcal{A}v = \lambda v \iff AX = \lambda X, \qquad v \neq 0 \iff X \neq 0$$

□

Определение 47. λ – с. ч. оператора $\mathcal{A}$, действующего на пространстве V
Собственным подпространством $\mathcal{A}$, соответствующим λ, называется множество с. в., соответствующих λ

Обозначение. V_λ

Свойство. V_λ является подпространством

47. Свойства нормального оператора

Свойства. $\mathcal{A}$ – нормальный оператор в евклидовом или унитарном пространстве

1. $\forall x \quad (\mathcal{A}x,\ \mathcal{A}x) = (\mathcal{A}^*x,\ \mathcal{A}^*x)$, то есть $|\mathcal{A}x| = |\mathcal{A}^*x|$

   Доказательство. $(\mathcal{A}x,\ \mathcal{A}x) = (x,\ \mathcal{A}^*\mathcal{A}x) = (x,\ \mathcal{A}\mathcal{A}^*x) = (\mathcal{A}^*x,\ \mathcal{A}^*x)$ □

2. v – скаляр
   Тогда $\mathcal{A} - v\mathcal{E}$ – тоже нормальный оператор

   Доказательство. Положим $\mathcal{B} \coloneqq \mathcal{A} - \lambda\mathcal{E}$
   Тогда $\mathcal{B}^* = \mathcal{A}^* - \overline{\lambda}\mathcal{E}$
   Подставим:

$$(\mathcal{B}\mathcal{B}^*)(x) = \mathcal{B}(\mathcal{B}^*x) \overset{\text{def}}{=} \mathcal{B}(\mathcal{A}^*x - \overline{\lambda}\mathcal{E}x) = \mathcal{B}(\mathcal{A}^*x - \overline{\lambda}x) \overset{\text{def}}{=} \\ = \mathcal{A}(\mathcal{A}^*x - \overline{\lambda}x) - \lambda(\mathcal{A}^*x - \overline{\lambda}x) = \mathcal{A}(\mathcal{A}^*x) - \overline{\lambda}\mathcal{A}x - \lambda\mathcal{A}^*x + \lambda\overline{\lambda}x$$

$$(\mathcal{B}^*\mathcal{B})(x) = \mathcal{B}^*(\mathcal{B}x) \overset{\text{def}}{=} \mathcal{B}^*(\mathcal{A}x - \lambda\mathcal{E}x) = \mathcal{B}^*(\mathcal{A}x - \lambda x) \overset{\text{def}}{=} \\ = \mathcal{A}^*(\mathcal{A}x - \lambda x) - \overline{\lambda}(\mathcal{A}x - \lambda x) = \mathcal{A}(\mathcal{A}^*x) - \lambda\mathcal{A}^*x - \overline{\lambda}\mathcal{A}x + \overline{\lambda}\lambda x$$

   □

3. λ – с. ч. оператора $\mathcal{A}$
   Тогда $\overline{\lambda}$ является с. ч. $\mathcal{A}^*$, и собств. подпр-во λ для $\mathcal{A}$ равно собств. подпр-ву $\overline{\lambda}$ для $\mathcal{A}^*$

   Доказательство. Нужно доказать, что $\mathcal{A}v = \lambda v \iff \mathcal{A}^*v = \lambda x$
   Положим $\mathcal{B} \coloneqq \mathcal{A} - \lambda\mathcal{E}$
   Тогда $\mathcal{B}^* = \mathcal{A}^* - \overline{\lambda}\mathcal{E}$
   Нужно доказать, что $\mathcal{B}x = 0 \iff \mathcal{B}^*x = 0$
   По (2), оператор $\mathcal{B}$ нормальный. Применим (1):

$$\mathcal{B}x = 0 \iff |\mathcal{B}x| = 0 \iff |\mathcal{B}^*x| = 0 \iff \mathcal{B}^*x = 0$$

   □

4. С. в. $\mathcal{A}$, относящиеся к разным с. ч., ортогональны

   Доказательство. Пусть x, y – с. в. $\mathcal{A}$, соответствующие с. ч. λ, μ, где $\lambda \neq \mu$
   Тогда x, y – с. в. $\mathcal{A}^*$, соответствующие с. ч. $\overline{\lambda}, \overline{\mu}$
   Преобразуем $(\mathcal{A}x,\ y)$ двумя способами:

$$\begin{cases} (\mathcal{A}x,\ y) = (\lambda x, y) = \lambda(x, y) \\ (\mathcal{A}x,\ y) = (x,\ \mathcal{A}^*y) = (x, \overline{\mu}u) = \mu(x, y) \end{cases}$$

   Из того, что $\lambda(x, y) = \mu(x, y)$, следует, что $(x, y) = 0$ □

48. Диагонализуемость нормального оператора. Следствия (без доказательства)

Теорема 24. $\mathcal{A}$ – нормальный оператор в унитарном пространстве
Тогда существует ОНБ, состоящий из с. в. оператора $\mathcal{A}$
То есть, существует ОНБ, в котором матрица этого оператора диагональна

Доказательство. Индукция по размерности пространства
База. $\dim = 1$ – очевидно
Переход
У оператора $\mathcal{A}$ существует хотя бы одно с. ч. λ_1, т. к. характ. многочлен $\chi_{\mathcal{A}}$ имеет корень в $\mathbb{C}$
Пусть e_1 – с. в. $\mathcal{A}$, соотв. λ_1, такой, что $|e_1| = 1$
Тогда e_1 является с. в. и для $\mathcal{A}^*$
Положим $U \coloneqq \langle e_1 \rangle$
Тогда U инвариантно для $\mathcal{A}$ и $\mathcal{A}^*$, и, следовательно, $\mathcal{U}^T$ инвариантно для $\mathcal{A}$ и $\mathcal{A}^*$
Положим $\mathcal{B} \coloneqq \mathcal{A}\Big|_{U^\perp}$
Тогда $\mathcal{A}^*\Big|_{U^\perp}$ является сопряжённым к $\mathcal{B}$ на $U^\perp$, т. .к равенство из определения сопряжённого оператора выполнено на подпространстве
По **индукционному предположению**, в $U^\perp$ существует ОНБ из с. в. $\mathcal{B}$
Эти векторы являются собств. для $\mathcal{A}$, и все они ортогональны e_1 $\square$

Следствие (канонический вид матрицы нормального оператора)**.** A – нормальная матрица в унитарном пространстве
Тогда существует унитарная матрица C, такая, что матрица $C^{-1}AC$ диагональна

Следствие (унитарный оператор)**.** $\mathcal{A}$ – нормальный оператор, λ_i – с. ч. $\mathcal{A}$
$\mathcal{A}$ – унитарный $\iff |\lambda_i| = 1 \quad \forall i$