

Содержание

I Жорданова форма оператора	2
1 Теорема о сумме собственных подпространств и следствие о линейно независимых векторах	2
2 Критерий диагонализуемости в терминах геометрических кратностей	3
3 Теорема об арифметической и геометрической кратности. Следствие о диагонализуемом операторе	4
4 Блочные матрицы и инвариантные подпространства. Делители характеристического многочлена	5
5 Ранг блочно-диагональной матрицы	7
6 Жордановы цепочки: линейная независимость, матрица оператора в базисе из цепочек	8
7 Существование жордановой формы нильпотентного оператора	10
8 Многочлен от оператора: произведение многочленов, инвариантность ядра и образа	11
9 Свойства аннулятора вектора	12
10 Базис циклического подпространства	13
11 Циклическое подпространство и минимальный аннулятор	13
12 Минимальный многочлен оператора. Теорема Гамильтона–Кэли и следствие из неё	14
13 Свойства взаимно простых многочленов от оператора	16
14 Разложение пространства в прямую сумму примарных подпространств	16
15 Корневые подпространства	17
16 Существование жордановой формы	18
17 Возведение жордановой клетки в степень	19
18 Количество жордановых блоков и ранг. Следствие о единственности жордановой формы	20
19 Минимальный многочлен оператора, у которого известна жорданова форма	21
20 Комплексификация вещественного векторного пространства. Продолжение операторов	21
21 Каноническая матрица оператора в вещественном пространстве	23
II Линейные отображения в евклидовых и унитарных пространствах	25
22 Изоморфизм векторного пространства и двойственного к нему	25
23 Дважды двойственное пространство	26
24 Двойственный базис. Матрица перехода для двойственного базиса	27
25 Собственные числа самосопряжённого оператора. Лемма об эрмитовой матрице	28

26 Ортогональность собственных векторов. Самосопряжённый оператор на \mathbb{R}^n	30
27 Корень из самосопряжённого оператора. Полярное разложение	30
28 Квадратичные формы: ортогональное преобразование, преобразование двух форм	32
III Кольца и поля	32
29 Идеал кольца. Примеры колец главных идеалов. Определения простого и максимального идеала	33
30 Построение факторкольца. Факторкольцо по простому идеалу	34
31 Факторкольцо по максимальному идеалу. Факторкольцо кольца многочленов над полем	35
32 Гомоморфизм колец. Теорема о гомоморфизме	36
33 Характеристика кольца и поля. Классификация простых полей	37
34 Степень расширения. Мультипликативность степени, следствия	39
35 Минимальный многочлен алгебраического элемента. Алгебраичность конечного расширения	41
36 Строение простого алгебраического расширения. Следствия	42
37 Существование простого расширения. Эквивалентные расширения	44
38 Поле разложения многочлена: существование, эквивалентность	45
39 Свойства корней из единицы. Существование примитивного корня	46
40 Количество примитивных корней. Многочлен деления круга	48
41 Строение конечного поля. Единственность	49
42 Существование поля с данным количеством элементов	50
Обозначение. $a_1, \dots, a_n \notin \odot \iff$ не все они равны нулю	

Часть I

Жорданова форма оператора

1. Теорема о сумме собственных подпространств и следствие о линейно независимых векторах

Определение 1. V — векторное пространство, \mathcal{A} — оператор на V , λ — с. ч.

Собственным подпространством, соответствующим λ , называется множество с. в., соответств. λ .

Обозначение. V_λ

Определение 2. U — подпространство V .

U называется *инвариантным* относительно \mathcal{A} , если

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

Утверждение 1. V_λ — инвариантное подпространство.

Доказательство.

- Подпространство

$$\begin{aligned} - u, v \in V_\lambda &\implies \begin{cases} \mathcal{A}u = \lambda u \\ \mathcal{A}v = \lambda v \end{cases} \implies \mathcal{A}(u+v) = \lambda(u+v) \quad \text{линейность} \\ u+v &\in V_\lambda \\ - u \in V_\lambda, k \in K &\implies \mathcal{A}(ku) = k\mathcal{A}(u) = k\lambda u = \lambda(ku) \implies ku \in V_\lambda \quad \text{линейность} \end{aligned}$$

- Инвариантность

$$u \in V_\lambda \implies \mathcal{A}u = \lambda u \in V_\lambda$$

□

Теорема 1 (о сумме собственных подпространств). $\lambda_1, \dots, \lambda_k$ — различные собственные числа. Тогда сумма $V_{\lambda_1} + \dots + V_{\lambda_k}$ является прямой.

Доказательство. Индукция по k

- База. $k = 1$. Сумма из одного слагаемого — прямая.

- Переход. $k - 1 \rightarrow k$

Пусть $u_1 + \dots + u_{k-1} + u_k = 0$, $u_i \in V_{\lambda_i}$

$$\begin{aligned} 0 &= \mathcal{A}(\underbrace{u_1 + \dots + u_{k-1}}_{=0} + u_k) - \lambda_k(\underbrace{u_1 + \dots + u_{k-1}}_{=0} + u_k) = \\ &= \lambda_1 u_1 + \dots + \lambda_{k-1} u_{k-1} + \lambda_k u_k - \lambda_k u_1 - \dots - \lambda_k u_{k-1} - \lambda_k u_k = (\underbrace{\lambda_1 - \lambda_k}_{\neq 0}) u_1 + \dots + (\underbrace{\lambda_{k-1} - \lambda_k}_{\neq 0}) u_{k-1} \end{aligned}$$

(т. к. по условию собственные числа различны)

$$(\lambda_1 - \lambda_k)u_1 \in V_{\lambda_1}, \dots, (\lambda_{k-1} - \lambda_k)u_{k-1} \in V_{\lambda_{k-1}}$$

По индукционному предположению, $V_{\lambda_1} \oplus \dots \oplus V_{\lambda_{k-1}}$.
А мы представили 0 в виде суммы. Значит, все слагаемые нулевые:

$$(\lambda_1 - \lambda_k)u_1 = \dots = (\lambda_{k-1} - \lambda_k)u_{k-1} = 0 \implies u_1 = \dots = u_{k-1} = 0 \implies u_k = 0$$

□

Следствие. $\lambda_1, \dots, \lambda_k$ — различные с. ч., $u_i \in V_{\lambda_i}$, $u_i \neq 0$.
Тогда u_1, \dots, u_k ЛНЗ.

Доказательство.

Пусть $a_1u_1 + \dots + a_ku_k = 0$

$$a_1u_1 \in V_{\lambda_1}, \dots, a_ku_k \in V_{\lambda_k} \implies a_1u_1 = \dots = a_ku_k = 0 \implies a_1 = \dots = a_k = 0$$

□

2. Критерий диагонализуемости в терминах геометрических кратностей

Определение 3. Оператор \mathcal{A} , действующий на V называется *диагонализуемым*, если его матрица в некотором базисе диагональна.

Определение 4. \mathcal{A} — оператор, λ — с. ч.

- Геометрической кратностью λ называется $\dim V_\lambda$;
- Арифметической кратностью λ называется кратность λ как корня $\chi_{\mathcal{A}}(t)$.

Теорема 2 (критерий диагонализуемости в терминах геометрической кратности).

(I) \mathcal{A} диагонализуем \iff (II) сумма геометрических кратностей всех с. ч. равна $\dim V$

Доказательство.

\mathcal{A} диагонализуем \iff в нек. базисе e_1, \dots, e_n матрица \mathcal{A} имеет вид $A = \begin{pmatrix} a_1 & & & 0 \\ 0 & \ddots & & \\ & & \ddots & \\ & & & a_n \end{pmatrix}$
 \iff для некоторого базиса e_1, \dots, e_n выполнено

$$\mathcal{A}e_i = 0e_1 + \dots + a_i e_i + \dots + 0e_n = a_i e_i$$

\iff (I') существует базис из с. в.

Докажем, что (I') \iff (II):

Пусть $U = V_{\lambda_1} + \dots + V_{\lambda_k}$

$$n := \dim V, \quad d_i := \dim V_{\lambda_i}$$

- (II) \implies (I')

Имеем $d_1 + \dots + d_k = n$

$$V_{\lambda_1} \oplus \dots \oplus V_{\lambda_k} \implies \dim U = n \xrightarrow[U - \text{подпр-во } V]{} U = V$$

$$V_{\lambda_1} \oplus \dots \oplus V_{\lambda_k} \implies \text{объединение базисов } V_{\lambda} \text{ является базисом } U = V$$

Эти базисы состоят из с. в. Значит, объединение базисов состоит из с. в. Это и есть базис V .

- (I') \implies (II)

Существует базис V из с. в.

Они распределяются по V_{λ} (но не обязательно для каждого V_{λ} представлен весь его базис):

$$\underbrace{e_1^{(1)}, \dots, e_{t_1}^{(1)}}_{\substack{\text{соотв. } \lambda_1 \\ \in V_{\lambda_1}}}, \underbrace{e_1^{(2)}, \dots, e_{t_2}^{(2)}}_{\substack{\text{соотв. } \lambda_2 \\ \in V_{\lambda_2}}}, \dots, \dots$$

$$e_1^{(i)}, \dots, e_{t_i}^{(i)} \text{ ЛНЗ} \quad \implies t_i \leq d_i \quad \forall i$$

(т. к. они лежат в большом базисе)

Сложим все эти неравенства:

$$\left. \begin{array}{l} d_1 + d_2 + \dots + d_k \geq t_1 + \dots + t_k = n \\ n \geq \dim U \xrightarrow[U=V_{\lambda_1} \oplus \dots \oplus V_{\lambda_k}]{} d_1 + \dots + d_k \end{array} \right\} \implies n = d_1 + \dots + d_k$$

□

Следствие (достаточное условие диагонализуемости). Пусть $\dim V = n$

Если у \mathcal{A} есть **n различных** с. ч., то \mathcal{A} диагонализуем

Доказательство. $\dim V_{\lambda_i} \geq 1$

$$n \geq \dim(V_{\lambda_1} + \dots + V_{\lambda_k}) = \dim V_{\lambda_1} + \dots + \dim V_{\lambda_k} \geq n$$

Значит, достигается равенство

□

3. Теорема об арифметической и геометрической кратности.

Следствие о диагонализуемом операторе

Напоминание (определитель ступенчатой матрицы).

$$M = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}, \quad A, C - \text{кв.} \implies |M| = |A| \cdot |C|$$

Теорема 3 (арифм. и геом. кратности). λ — с. ч. \mathcal{A}

Геом. кратность $\lambda \leq$ арифм. кратности λ

Доказательство. Пусть $n = \dim V$, k — геом. кр. λ

Выберем базис e_1, \dots, e_k пространства V_λ

Дополним его до базиса V : $e_1, \dots, e_k, \dots, e_n$

При $i \leq k$ выполнено $\mathcal{A}e_i = \lambda e_i = 0 \cdot e_1 + \dots + \lambda e_i + \dots + 0 \cdot e_n$

Матрица \mathcal{A} в базисе e_1, \dots, e_n :

$$A = \begin{pmatrix} \lambda & 0 & B \\ 0 & \lambda & \\ 0 & C & \end{pmatrix}$$

Для некоторых $B_{k \times n-k}$, $C_{n-k \times n-k}$

$$\chi(t) = \begin{vmatrix} (\lambda - t)E_k & B \\ 0 & C - tE_{n-k} \end{vmatrix} = \det((\lambda - t)E_k) \cdot \det(C - tE_{n-k}) = (\lambda - t)^k \cdot \det(C - tE_{n-k})$$

□

Следствие (критерий диагонализуемости в терминах арифметических и геометрических кратностей).

Оператор \mathcal{A} диагонализуем \iff

1. $\chi_{\mathcal{A}}(t)$ раскладывается на линейные множители
2. \forall с. ч. λ арифм. кр. = геом. кр.

Доказательство. Пусть λ_i — с. ч., d_i — геом. кр., a_i — арифм. кр., $n = \dim C$

$$\chi(t) = (t - \lambda_1)^{a_1} \dots (t - \lambda_k)^{a_k} \cdot P(t),$$

где $P(t)$ не имеет корней.

$$n = \deg \chi(t) \geq a_1 + \dots + a_k \geq d_1 + \dots + d_k$$

Диагонал. $\iff n = d_1 + \dots + d_k \iff$ везде достигаются равенства

□

4. Блоchные матрицы и инвариантные подпространства. Делители характеристического многочлена

Определение 5. Блоchной матрицей называется матрица вида

$$A = \begin{pmatrix} A_{11} & \dots & A_{1n} \\ \vdots & \ddots & \vdots \\ A_{m1} & \dots & A_{mn} \end{pmatrix}$$

где $\forall i$ A_{ix} имеют поровну строк и $\forall j$ A_{xj} имеют поровну столбцов

Определение 6. Блоchно-диагональной матрицей называется матрица вида

$$\begin{pmatrix} A_1 & & 0 \\ 0 & \ddots & \\ & & A_n \end{pmatrix}$$

где A_i — квадратные

Определение 7. U — инвариантное подпространство оператора \mathcal{A}

Через $\mathcal{A}|_U$ обозначим сужение \mathcal{A} на U , т. е.

$$\mathcal{A}|_U : U \rightarrow U, \quad \mathcal{A}|_U(x) = \mathcal{A}(x) \quad \forall x \in U$$

Теорема 4 (блочные матрицы и инвариантные подпространства).

\mathcal{A} — оператор на конечномерном пространстве V

1. U — инвариантное пространство \mathcal{A} , e_1, \dots, e_s — базис U , $e_1, \dots, e_s, \dots, e_n$ — базис V
 A_U, A — матрицы $\mathcal{A}|_U$ и \mathcal{A} на U, V в этих базисах

$$\implies A = \begin{pmatrix} A_U & B \\ \mathbf{0} & C \end{pmatrix} \quad \text{для некоторых } B, C$$

2. $V = U_1 \oplus \dots \oplus U_k$, где U_i — инвар. для \mathcal{A}
 A_1, \dots, A_k — матрицы \mathcal{A} на U_1, \dots, U_k в некоторых базисах
 A — матрица \mathcal{A} на V в базисе, являющемся объединением базисов U_i (в естественном порядке: базис U_1 , базис U_2 , ...)

$$\implies A = \begin{pmatrix} A_1 & & & 0 \\ & \ddots & & \\ 0 & & \ddots & \\ & & & A_k \end{pmatrix}$$

Так как A_1, \dots, A_k — квадратные, то A — блочно-диагональная

Доказательство.

1. Пусть

$$A_U = \begin{pmatrix} a_{11} & \dots & a_{1s} \\ \vdots & \ddots & \vdots \\ a_{s1} & \dots & a_{ss} \end{pmatrix}$$

Возьмём $1 \leq i \leq s$

Посмотрим, как \mathcal{A} действует на e_i :

$$\mathcal{A}(e_i) = a_{1i}e_1 + \dots + a_{si}e_s = a_{1i}e_1 + \dots + a_{si}e_s + \dots + 0 \cdot e_{s+1} + \dots + 0 \cdot e_n$$

Получили разложение $\mathcal{A}(e_i)$ по базису V , то есть, столбец матрицы оператора в базисе $e_1, \dots, e_s, \dots, e_n$:

$$\begin{pmatrix} a_{1i} \\ \vdots \\ e_{si} \\ 0 \\ \vdots \\ 0 \end{pmatrix} - i\text{-й столбец } A$$

$$\implies A = \begin{pmatrix} a_{11} & \dots & a_{s1} & * \\ \vdots & \ddots & \vdots & \vdots \\ a_{s1} & \dots & a_{ss} & * \\ 0 & \ddots & \ddots & \vdots \\ & & 0 & * \end{pmatrix}$$

2. Пусть $\dim U_1 = d_1, \dim U_2 = d_2, \dots$

Рассмотрим столбец матрицы A с номером $d_1 + d_2 + \dots + d_{i-1} + t$, где $1 \leq t \leq d_i$ (т. е. t -й столбец i -го набора)

Обозначим элементы базисов:

$$U_1 : e_1^{(1)}, \dots, e_{d_1}^{(1)}$$

$$U_2 : e_2^{(2)}, \dots, e_{d_2}^{(2)}$$

.....

В этом столбце записаны координаты вектора $e_t^{(i)}$ в базисе V
Разложим его по базису подпространства U_i :

$$e_t^{(i)} = a_1 e_1^{(i)} + \dots + a_{d_i} e_{d_i}^{(i)}$$

Дополним нулями:

$$\underbrace{0 \cdot e_1^{(1)} + \cdots + 0 \cdot d_1^{(1)}}_{d_1} + \underbrace{0 \cdot e_1^{(2)} + \cdots + \cdots}_{d_2} + \underbrace{a_1 e_1^{(i)} + \cdots + a_{d_i} e_d^{(i)}}_{d_i} + 0 \cdot e_1^{(i+1)} + \cdots$$

Получили разложение $e_r^{(i)}$ по базису V .
 $(d_1 + d_2 + \cdots + d_{i-1} + t)$ -й столбец равен

$$(0 \quad \cdots \quad 0 \quad a_1 \quad \cdots \quad a_{d_i} \quad 0 \quad \cdots \quad 0)^T$$

□

Следствие (делители характеристического многочлена).

\mathcal{A} — оператор на конечномерном пространстве V , $\chi(t)$ — его характерист. многочлен

1. U — инвариантное подпространство, $\chi_U(t)$ — характ. многочлен $\mathcal{A}|_U$

$$\implies \chi(t) : \chi_U(t)$$

2. $V = U_1 \oplus \cdots \oplus U_k$, где U_i — инвариантные

$\chi_i(t)$ — характ. многочлен $\mathcal{A}|_{U_i}$

$$\chi(t) = \chi_1(t) \cdots \chi_k(t)$$

Доказательство. Рассмотрим базисы как в теореме

$$1. \chi_A(t) = \left| \begin{pmatrix} A_U & B \\ 0 & C \end{pmatrix} - tE_n \right| = \left| \begin{matrix} A_U - tE_s & B \\ 0 & C - tE_{n-s} \end{matrix} \right| = |A_U - tE_s| \cdot |C - tE_{n-s}| = \chi_U(t) \cdot \chi_C(t)$$

$$2. \chi_A(t) = |A - tE| = \left| \begin{matrix} A_1 - tE & & 0 \\ 0 & \ddots & \\ & & A_k - tE \end{matrix} \right| = |A_1 - tE| \cdot |A_2 - tE| \cdots = \chi_1(t) \cdot \chi_2(t) \cdots$$

□

5. Ранг блочно-диагональной матрицы

Лемма 1 (ранг блочно-диагональной матрицы). A — блочно-диагональная

$$A = \begin{pmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_k \end{pmatrix}$$

$$\implies \operatorname{rk} A = \operatorname{rk} A_1 + \cdots + \operatorname{rk} A_k$$

Доказательство. Воспользуемся тем, что ранг — это количество ЛНЗ строк

Пусть для каждой матрицы A_i выбран набор строк $s_1^{(i)}, s_2^{(i)}, \dots, s_n^{(i)}$

Для строки $s_j^{(i)}$ обозначим через $\tilde{s}_j^{(i)}$ соответствующую строку матрицы A

Достаточно доказать, что

$$\text{набор } \tilde{s}_1^{(1)}, \dots, \tilde{s}_{r_1}^{(1)}, \tilde{s}_1^{(2)}, \dots, \tilde{s}_{r_2}^{(2)}, \dots \text{ ЛНЗ} \iff \text{все наборы } \begin{cases} s_1^{(1)}, \dots, s_{r_1}^{(1)} \\ s_1^{(2)}, \dots, s_{r_2}^{(2)} \\ \dots \dots \dots \end{cases} \text{ ЛНЗ}$$

• \implies

Докажем от противного:

Предположим, что $s_1^{(i)}, \dots, s_{r_i}^{(i)}$ ЛЗ

То есть, $\exists a_1, \dots, a_{r_i} \notin \bigcirc$, такие, что $a_1 s_1^{(i)} + \cdots + a_{r_i} s_{r_i}^{(i)} = 0$

Дополним нулями:

$$a_1 \tilde{s}_1^{(i)} + \cdots + a_{r_i} \tilde{s}_{r_i}^{(i)} = 0$$

То есть, $\tilde{s}_1^{(i)}, \dots, \tilde{s}_{r_i}^{(i)}$ ЛЗ
А значит, и весь набор ЛЗ — ↴

- ⇐

Докажем от противного:

Пусть все наборы $s_1^{(i)}, \dots, s_{r_i}^{(i)}$ ЛНЗ, а $\tilde{s}_1^{(1)}, \dots, \tilde{s}_{r_i}^{(1)}, \dots, \tilde{s}_{r_k}^{(k)}$ ЛЗ, то есть

$$\sum_{i,j} a_j^{(i)} \tilde{s}_j^{(i)} = 0, \quad \text{не все } a_j^{(i)} \text{ равны нулю}$$

Положим

$$T_i := a_1^{(i)} s_1^{(i)} + \dots + a_{r_i}^{(i)} s_{r_i}^{(i)}$$

$$\tilde{T}_i := a_1^{(i)} \tilde{s}_1^{(i)} + \dots + a_{r_i}^{(i)} \tilde{s}_{r_i}^{(i)}$$

$$\tilde{T}_1 + \tilde{T}_2 + \dots + \tilde{T}_k = 0 \implies \tilde{T}_1 = \tilde{T}_2 = \dots = 0$$

Строки $\tilde{T}_1, \dots, \tilde{T}_k$ не содержат ненулевые элементы в одном столбце (т. е. в нашей записи нет полностью нулевых столбцов)

$$\implies T_1 = 0, \quad T_2 = 0, \quad T_k = 0$$

$$\implies \forall i \quad a_1^{(i)} s_1^{(i)} + \dots + a_{r_i}^{(i)} s_{r_i}^{(i)} = 0$$

$$s_1^{(i)}, \dots, s_{r_i}^{(i)} \text{ ЛНЗ} \implies a_1^{(i)} = \dots = a_{r_i}^{(i)} = 0$$

□

Следствие. $V = U_1 \oplus \dots \oplus U_k$, U_i — инвариантно для \mathcal{A}

$$\implies \dim \text{Im } \mathcal{A} = \dim \text{Im } \mathcal{A}|_{U_1} + \dots + \dim \text{Im } \mathcal{A}|_{U_k}$$

6. Жордановы цепочки: линейная независимость, матрица оператора в базисе из цепочек

Определение 8. Жордановой клеткой порядка r с собств. знач. 0 называется квадратная матрица порядка r вида

$$J_r(0) = \begin{pmatrix} 0 & & & & 0 \\ 1 & \ddots & & & \vdots \\ & \ddots & \ddots & & \vdots \\ & & & \ddots & 0 \\ 0 & & & 1 & 0 \end{pmatrix}$$

Определение 9. Жордановой матрицей с собств. знач. 0 называется матрица вида

$$\begin{pmatrix} J_{r_1}(0) & & & 0 \\ 0 & \ddots & & J_{r_k}(0) \\ & & \ddots & \end{pmatrix}$$

Определение 10. \mathcal{A} — nilпотентный оператор

Жордановой цепочкой называется такой набор векторов e_1, e_2, \dots, e_r , что $\mathcal{A}(e_i) = e_{i+1}$ при $i < r$ и $\mathcal{A}(e_r) = 0$

Обозначение. $e_1 \rightarrow e_2 \rightarrow \dots \rightarrow e_r \rightarrow 0$

Лемма 2 (ЛНЗ жордановых цепочек). Дано несколько жордановых цепочек:

$$e_1^{(1)} \rightarrow e_2^{(1)} \rightarrow \dots \rightarrow e_{r_1}^{(1)} \rightarrow 0$$

.....

$$e_1^{(k)} \rightarrow e_2^{(k)} \rightarrow \cdots \rightarrow e_{r_k}^{(k)} \rightarrow 0$$

Если последние векторы цепочек, т. е. $e_{r_1}^{(1)}, \dots, e_{r_k}^{(k)}$ ЛНЗ, то объединение цепочек ЛНЗ

Доказательство. Индукция по $r := \max \{ r_1, \dots, r_k \}$

- **База.** $r = 1$

Все цепочки длины 1

Все векторы — последние и, по условию, ЛНЗ

- **Переход.** $r - 1 \rightarrow r$

$$\mathcal{A}(e_i^{(j)}) = \begin{cases} e_{i+1}^{(j)}, & i < r_j \\ 0, & i = r_j \end{cases}$$

Применим s раз:

$$\mathcal{A}^s(e_i^{(j)}) = \begin{cases} e_{i+s}^{(j)}, & i + s \leq r_j \\ 0, & i + s > r_j \end{cases}$$

Цепочки бывают двух видов: у некоторых длина r , а у некоторых — меньше (по определению r)
НУО считаем, что цепочки с номерами $1, 2, \dots, m$ имеют длину r , а остальные — меньше, т. е.

$$r_1 = r_2 = \cdots = r_m = r, \quad r_i < r \text{ при } i > m$$

От противного: пусть набор ЛЗ:

$$\sum_{j=1}^k \sum_{i=1}^{r_j} a_i^{(j)} e_i^{(j)} = 0, \quad \text{не все } a_i^{(j)} \text{ равны } 0$$

Применим к этому равенству \mathcal{A}^{r-1} :

- Если цепочка короче r , то она вся перейдёт в 0
- Иначе — останется только последний вектор

То есть,

$$e_1^{(j)} \rightarrow e_r^{(j)}, \quad a_1^{(j)} e_1^{(j)} \rightarrow a_1^{(j)} e_r^{(j)}, \quad \text{остальные} \rightarrow 0$$

Получится сумма:

$$\sum_{j=1}^m a_1^{(j)} e_r^{(j)}$$

Заметим, что это ЛК последних векторов (которые, по условию, ЛНЗ)

$$\implies a_1^{(j)} = 0 \quad \text{при } j \leq m$$

Уберём слагаемые $0 \cdot e_1^{(j)}$ при $j \leq m$

$$\sum_{j \leq m} \sum_{i=2}^r a_i^{(j)} e_i^{(j)} + \sum_{j > m} a_i^{(j)} e_i^{(j)} = 0$$

Это — ЛК векторов из цепочек длины $r - 1$ с теми же последними векторами

Применим **индукционное предположение**. Вместе с условием, что последние векторы ЛНЗ, получаем, что все они ЛНЗ

□

Лемма 3 (базис из жордановых цепочек). \mathcal{A} — оператор на V .

e_1, e_2, \dots, e_n — базис, являющийся объединением жордановых цепочек (в естественном порядке):

$$e_1 \rightarrow e_2 \rightarrow \cdots \rightarrow e_{r_1} \rightarrow 0$$

$$e_{r_1+1} \rightarrow e_{r_2+2} \rightarrow \cdots \rightarrow e_{r_1+r_2} \rightarrow 0$$

.....

$$e_{r_1+\dots+r_{k-1}+1} \rightarrow \dots \rightarrow e_{r_1+r_2+\dots+r_{k-1}+r_k} \rightarrow 0$$

Тогда матрица \mathcal{A} в этом базисе

$$A = \begin{pmatrix} J_{r_1}(0) & & & & & 0 \\ & \ddots & & & & \\ 0 & & & J_{r_k}(0) & & \end{pmatrix}$$

Доказательство.

$$\mathcal{A}(e_{r_1}) = \mathcal{A}(e_{r_1+r_2}) = \dots = \mathcal{A}(e_{r_1+\dots+r_k}) = 0$$

Значит, при $i = r_1, r_1 + r_2, \dots, r_1 + \dots + r_k$, i -й столбец — нулевой
При $i \neq r_1, \dots, r_1 + \dots + r_k$, $\mathcal{A}(e_i) = e_{i+1} \implies i$ -й столбец:

$$\begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{pmatrix}^T$$

□

7. Существование жордановой формы нильпотентного оператора

Теорема 5. Для любого нильпотентного оператора на конечномерном векторном пространстве существует жорданов базис.

Доказательство. Будем доказывать, что существует базис из жордановых цепочек

Положим $W := \ker \mathcal{A}$

Если мы возьмём ЛНЗ векторы из ядра и достроим (слева от них) цепочки, то получим жорданов базис

Положим $U_i := \text{Im } \mathcal{A}^i$

$$V = U_0 \supset U_1 \supset U_2 \supset \dots \supset U_{k-1} \supset U_k = \{0\}$$

где k — степень нильпотентности \mathcal{A}

Заметим, что если $v \in U_t \cap W$, то существует цепочка длины $t+1$ с концом v

Построим базис W (такой, чтобы можно было достроить цепочки):

Будем пересекать W с U_i

Выберем базис $W \cap U_{k-1}$. Он ЛНЗ, значит его можно дополнить до базиса $W \cap U_{k-2}$

В итоге получим базис $W \cap U_0 = W$

Получили базис e_1, e_2, \dots пространства W

Для $e_i \in W \cap U_t$ построим цепочку длины $t+1$ с концом e_i :

$$e_1^{(i)} \rightarrow e_2^{(i)} \rightarrow \dots \rightarrow e_{t+1}^{(i)} = e_i \rightarrow 0$$

Объединение цепочек — ЛНЗ (по лемме)

Докажем, что это базис, т. е. что набор порождающий:

Докажем, что если $\mathcal{A}^s(v) = 0$, то v является ЛК векторов цепочек

Докажем индукцией по s :

- **База.** $s = 1$

$$\ker \mathcal{A}^1 = W, \quad v \in W, \quad e_1, e_2, \dots \text{ — базис } W$$

- **Переход.** $s \rightarrow s+1$

Пусть $\mathcal{A}^{s+1}(v) = 0$, $\mathcal{A}^s(v) \neq 0$

Положим $u = \mathcal{A}^s v \implies u \in U_s$

$$\underbrace{v \rightarrow \dots \rightarrow}_{s+1} \underbrace{\dots \rightarrow u \rightarrow 0}_s$$

Значит, $\mathcal{A}(u) = 0 \implies u \in W$

Значит, $u \in U_s \cap W$

Разложим его по базису $U_s \cap W$ (тому, до которого мы дошли на каком-то очередном шаге

дополнения базисов):

$$u = \sum_i a_i e_i$$

$\forall e_i$ из этого базиса выбрана цепочка длины хотя бы $s + 1$

$$e_i = e_{s+t_i}^{(i)} \text{ — последний вектор цепочки}$$

Пусть e'_i — вектор цепочки, такой что $\mathcal{A}^s(e'_i) = e_i$ (вектор, который на s шагов раньше)

$$\mathcal{A}^s \left(\sum a_i e'_i \right) = \sum a_i e_i = u$$

При этом, $\mathcal{A}^s(v) \stackrel{\text{def}}{=} u$

Получили 2 линейных представления u , значит,

$$\mathcal{A}^s(v) = \mathcal{A}^s \left(\sum a_i e'_i \right) \Rightarrow \mathcal{A}^s \left(v - \sum a_i e'_i \right) = 0$$

Тогда, по индукционному предположению, $v - \sum a_i e'_i$ представляется в виде ЛК векторов из цепочек

Значит, v представляется в виде ЛК векторов цепочек

□

8. Многочлен от оператора: произведение многочленов, инвариантность ядра и образа

Обозначение. V — векторное пространство над K , \mathcal{A} — оператор на V , $P \in K[x]$

$$P(x) = a_n x^n + \cdots + a_1 x + a_0$$

Тогда $P(\mathcal{A}) = a_n \mathcal{A}^n + \cdots + a_1 \mathcal{A} + a_0 \mathcal{E}$, т. е. такой оператор \mathcal{B} , что

$$\mathcal{B}(v) = a_n \mathcal{A}^n(v) + \cdots + a_2 \mathcal{A}^2(v) + a_1 \mathcal{A}(v) + a_0 v$$

Лемма 4 (произведение многочленов от оператора). P, Q — многочлены, \mathcal{A} — оператор

$$\Rightarrow (PQ)(\mathcal{A}) = P(\mathcal{A}) \circ Q(\mathcal{A})$$

Доказательство. Пусть $P(t) = \sum p_i t^i$, $Q(t) = \sum q_i t^i$, $R(t) = P(t)Q(t)$

$$R(t) = \sum p_i q_j t^{i+j}$$

Положим $\mathcal{B} = P(\mathcal{A})$, $\mathcal{C} = Q(\mathcal{A})$, $\mathcal{D} = R(\mathcal{A})$

Нужно доказать, что $\mathcal{B}(\mathcal{C}(v)) = \mathcal{D}(v) \quad \forall v$

$$\mathcal{B}(v) = \sum p_i \mathcal{A}^i(v), \quad \mathcal{C}(v) = \sum q_j \mathcal{A}^j(v), \quad \mathcal{D}(v) = \sum p_i q_j \mathcal{A}^{i+j}(v)$$

$$\mathcal{B}(\mathcal{C}(v)) = \mathcal{B} \left(\sum q_j \mathcal{A}^j(v) \right) = \sum q_j \mathcal{B}(\mathcal{A}^j(v)) = \sum q_j \left(\sum p_i \mathcal{A}^{i+j}(v) \right) = \sum q_j p_i \mathcal{A}^{i+j} = \mathcal{D}(v)$$

□

Следствие. P, Q — многочлены, $\mathcal{A}, \mathcal{B}, \mathcal{C}$ — операторы, $\mathcal{B} = P(\mathcal{A})$, $\mathcal{C} = Q(\mathcal{A})$

$$\Rightarrow \mathcal{B} \circ \mathcal{C} = \mathcal{C} \circ \mathcal{B}$$

Доказательство. $PQ = QP \Rightarrow (PQ)(A) = (QP)(A)$

□

Теорема 6 (ядро и образ многочлена от оператора). \mathcal{A} — оператор на V , P — многочлен, $\mathcal{B} = P(\mathcal{A})$. Тогда $\ker \mathcal{B}$ и $\text{Im } \mathcal{B}$ — инвариантные подпространства относительно \mathcal{A} .

Доказательство.

- $\ker \mathcal{B}$

$$v \in \ker \mathcal{B} \implies \mathcal{B}(v) = 0 \implies \mathcal{A}(\mathcal{B}(v)) = 0 \xrightarrow{\text{лемма}} \mathcal{B}(\mathcal{A}(v)) = 0 \implies \mathcal{A}(v) \in \ker \mathcal{B}$$

- $\text{Im } \mathcal{B}$

$$v \in \text{Im } \mathcal{B} \implies v = \mathcal{B}(w) \implies \mathcal{A}(v) = \mathcal{A}(\mathcal{B}(w)) \xrightarrow{\text{лемма}} \mathcal{B}(\mathcal{A}(w))$$

□

9. Свойства аннулятора вектора

Определение 11. \mathcal{A} — оператор на V , $v \in V$

- *Аннулятором* v называется такой многочлен P , что $P(\mathcal{A})(v) = 0$
- *Минимальным аннулятором* v называется многочлен наименьшей степени среди ненулевых аннуляторов

Свойства.

1. V конечномерно.

- (a) у любого вектора существует ненулевой аннулятор
- (b) если P_0 — минимальный аннулятор, то $\deg P_0 \leq \dim V$

2. P_1, \dots, P_k — аннуляторы v

$$\forall \text{многочл. } Q_1, \dots, Q_k \quad \text{многочлен } S(t) = Q_1(t)P_1(t) + \dots + Q_k(t)P_k(t) \text{ — аннулятор } v$$

3. $P_0(t)$ — минимальный аннулятор.

$$P(t) \text{ — аннулятор} \iff P(t) : P_0(t)$$

4. Минимальный аннулятор — единственный с точностью до ассоциированности (умножения на обратимый, т. е. на константу)

Доказательство.

1. Пусть $n := \dim V$

Докажем, что $\exists P : \deg P \leq n$, P — аннулятор, $P \neq 0$
Возьмём

$$\underbrace{v, \mathcal{A}(v), \mathcal{A}^2(v), \dots, \mathcal{A}^n(v)}_{n+1 \text{ вектор}}$$

Они ЛЗ, т. к. их больше, чем размерность пространства. Значит,

$$\exists a_i \neq 0 : a_0 v + a_1 \mathcal{A}(v) + \dots + a_n \mathcal{A}^n(v) = 0$$

Подойдёт $P(t) = a_n t^n + \dots + a_1 t + a_0$

2. Пусть $\mathcal{B}_i := P_i(\mathcal{A})$, $\mathcal{C}_i = Q_i(\mathcal{A})$, $\mathcal{D} = S(\mathcal{A})$

$$\mathcal{D}(v) = \mathcal{C}_1 \left(\underbrace{\mathcal{B}_1(v)}_{=0} \right) + \dots + \mathcal{C}_k \left(\underbrace{\mathcal{B}_k(v)}_{=0} \right) = \mathcal{C}_1(0) + \dots + \mathcal{C}_k(0) = 0$$

3. Поделим с остатком:

$$P(t) = Q(t)P_0(t) + R(t), \quad \deg R < \deg P_0$$

• \Leftarrow

$$R(t) = 0, \quad P(t) = \underbrace{P_0(t)}_{\text{аннулятор}} \underbrace{Q(t)}_{\text{аннулятор}} - \text{аннулятор (по (2.))}$$

• \Rightarrow

$$R(t) = \underbrace{P(t)}_{\text{аннул.}} - \underbrace{Q(t)P_0(t)}_{\text{аннул.}} - \text{аннулятор (по (2.))}$$

4.

$$\exists P_1, P_2 - \text{мин. аннул.} \implies \underbrace{P_1}_{\text{аннул.}} : \underbrace{P_2}_{\text{мин. аннул.}}$$

□

10. Базис циклического подпространства

Определение 12. \mathcal{A} — оператор на V , $v \in V$

Циклическим подпространством, порождённым v называется минимальное по включению инвариантное подпространство, содержащее v

Теорема 7 (базис циклического подпространства). $k \in \mathbb{N}$ такое, что:

1. $v, \mathcal{A}(v), \dots, \mathcal{A}^{k-1}(v)$ ЛНЗ
2. $v, \mathcal{A}(v), \dots, \mathcal{A}^{k-1}(v), \mathcal{A}^k(v)$ ЛЗ

Тогда первый набор является базисом циклического подпространства, порождённого v

Доказательство. Пусть U — циклическое, порождённое v

$$U - \text{инвар.} \implies v \in U \implies \mathcal{A}v \in U \implies \underbrace{\mathcal{A}^2v}_{=\mathcal{A}(\mathcal{A}(v))} \in U \implies \dots \implies v, \mathcal{A}v, \dots, \mathcal{A}^{k-1}v \in U$$

Они ЛНЗ. Чтобы доказать, что это базис, надо доказать, что они порождают U :

$$\text{Положим } W = \langle v, \mathcal{A}v, \dots, \mathcal{A}^{k-1}v \rangle$$

Докажем, что $W = U$:

- Докажем, что W — инвар.:
 $\mathcal{A}^k v - \text{ЛК } v, \mathcal{A}v, \dots, \mathcal{A}^{k-1}v$

$$w \in W, \quad w = a_0v + \dots + a_{k-1}\mathcal{A}^{k-1}v$$

$$\mathcal{A}(w) = a_0\mathcal{A}v + \dots + a_{k-2}\mathcal{A}^{k-1}v + \underbrace{a_{k-1}\mathcal{A}^k v}_{\text{ЛК } v, \dots, \mathcal{A}^{k-1}v}$$

Значит, w является ЛК $v, \dots, \mathcal{A}^{k-1}v$

- Докажем, что W — минимальное:

Докажем, что если W_1 инвариантно и $v \in W_1$, то $W \subset W_1$:

$$\left. \begin{array}{l} W_1 \text{ инвар.} \\ v \in W_1 \end{array} \right\} \implies \mathcal{A}v \in W_1, \quad \left. \begin{array}{l} W_1 \text{ инвар.} \\ \mathcal{A}v \in W_1 \end{array} \right\} \implies \mathcal{A}^2v \in W_1, \dots, \underbrace{\mathcal{A}^i v}_{\text{порожд. } W} \in W_1 \implies \dots \implies W_1 \subset W$$

□

11. Циклическое подпространство и минимальный аннулятор

Теорема 8. V — конечномерное, \mathcal{A} — оператор на V , $v \in V$
 U — цикл. подпр-во, порождённое v , χ — хар. многочлен \mathcal{A} на U
Тогда χ — минимальный аннулятор v

Доказательство. Пусть k такое, что

1. $v, \mathcal{A}v, \dots, \mathcal{A}^{k-1}v$ ЛНЗ
2. $v, \mathcal{A}v, \dots, \mathcal{A}^{k-1}v, \mathcal{A}^k v$ ЛЗ

Выберем a_i , не все равные нулю, такие, что

$$a_0v + a_1\mathcal{A}v + \dots + a_{k-1}\mathcal{A}^{k-1}v + a_k\mathcal{A}^k v = 0$$

Значит, $a_k \neq 0$ (т. к. $v, \dots, \mathcal{A}^{k-1}v$ ЛНЗ)

Поделим на a_k , не меняя обозначений (т. е. $a_i := \frac{a_i}{a_k}$):

$$\mathcal{A}^k v + \dots + a_1\mathcal{A}v + a_0v = 0$$

Положим $P(t) := t^k + a_{k-1}t^{k-1} + \dots + a_1t + a_0 \implies P(t)$ — аннулятор

- Докажем, что $P(t)$ — минимальный. **Пусть это не так:**

$$\exists Q'(t) = b_m t^m + \dots + t_0, \quad Q' \neq 0, \quad Q' — \text{аннул.}, \quad m < k$$

$$b_m \mathcal{A}^m v + \dots + b_0 v = 0$$

$b_i \neq \odot \implies \mathcal{A}^m v, \dots, v$ — ЛЗ — ↳ (это был не первый момент линейной зависимости)

- Докажем, что $P(t) = \pm\chi$:

Знаем, что $v, \dots, \mathcal{A}^{k-1}v$ — базис U . Образы этих векторов:

$$\mathcal{A}(\mathcal{A}^i(v)) = \mathcal{A}^{i+1}(v), \quad 0 \leq i < k-1$$

$$\mathcal{A}(A^{k-1}(v))(v) = \mathcal{A}^k(v) = -a_0v - a_1\mathcal{A}(v) - \dots - a_{k-1}\mathcal{A}^{k-1}(v)$$

Значит, матрица $\mathcal{A}|_U$ в этом базисе:

$$A = \begin{pmatrix} 0 & \dots & 0 & -a_0 \\ 1 & & & \vdots \\ \vdots & & & \vdots \\ 0 & \dots & 1 & -a_{k-1} \end{pmatrix}$$

$$\chi_A(t) = \begin{vmatrix} -t & \dots & 0 & -a_0 \\ 1 & & \vdots & \vdots \\ \vdots & & \vdots & \vdots \\ \vdots & & -t & -a_{k-2} \\ 0 & \dots & 1 & -a_{k-1} - t \end{vmatrix} \begin{array}{l} + \text{I}/t \\ + \text{II}/t \end{array} = \begin{vmatrix} -t & \dots & 0 & -a_1 \\ \vdots & & \vdots & -a_1 - \frac{a_0}{t} \\ \vdots & & \vdots & -a_2 - \frac{a_1}{t} - \frac{a_0}{t^2} \\ \vdots & & -t & \vdots \\ 0 & \dots & 0 & -t - a_{k-1} - \frac{a_{k-2}}{t} - \dots - \frac{a_1}{t^{k-2}} - \frac{a_0}{t^{k-1}} \end{vmatrix}$$

Это будет $(-1)^k P(t)$

□

12. Минимальный многочлен оператора. Теорема Гамильтона—Кэли и следствие из неё

Определение 13. Многочлен $P(t)$ аннулирует \mathcal{A} , если $P(\mathcal{A}) = 0$

Определение 14. Минимальным многочленом оператора \mathcal{A} называется ненулевой многочлен наименьшей степени, аннулирующий \mathcal{A}

Свойства. \mathcal{A} — оператор на V

1. P_1, \dots, P_k аннулируют \mathcal{A}

$$\forall \text{ многочл. } Q_1, \dots, Q_k \quad S(t) = P_1(t)Q_1(t) + \dots + P_k(t)Q_k(t) \text{ аннулирует } \mathcal{A}$$

2. P_0 — минимальный многочлен для \mathcal{A}

$$P \text{ аннулирует } \mathcal{A} \iff P : P_0$$

3. Минимальный многочлен \mathcal{A} единственен с точностью до ассоциирования

4. e_1, \dots, e_n — базис V , $P_1(t), \dots, P_n(t)$ — минимальные аннуляторы для e_1, \dots, e_n
Тогда НОК(P_1, \dots, P_n) является минимальным многочленом для A

Доказательство.

1. $\forall v \quad P_i$ — аннулятор $v \implies S(\mathcal{A})$ — аннулятор $v \implies S$ аннулирует \mathcal{A}

2. Пусть $P = P_0Q + R$

- Если $P : P_0$, то $P = P_0Q \stackrel{1}{\implies} P$ аннулирует \mathcal{A}
- Если P аннулирует \mathcal{A} , то $R = P - P_0Q$ аннулирует $\mathcal{A} \stackrel{1}{\implies} R = 0 \implies P : P_0$

3. Если P_1, P_2 — минимальные многочлены, то $P_1 : P_2$ и $P_2 : P_1$.

4. Пусть $P = \text{НОК}(P_1, \dots, P_n)$

- Проверим, что P аннулирует A :

Пусть $v \in V, \quad v = a_1e_1 + \dots + a_ne_n$

Применим P :

$$P(\mathcal{A})(v) = a_1P(\mathcal{A})e_1 + \dots + a_nP(\mathcal{A})e_n$$

$$P : P_i \implies P \text{ — аннул. для } e_i \implies P(\mathcal{A})e_i = 0$$

$$P(\mathcal{A})(v) = a_1 \cdot 0 + \dots + a_n \cdot 0 = 0$$

- Проверим, что P минимальный:

Пусть $Q(t)$ аннулирует \mathcal{A}

$$\implies Q(\mathcal{A})v = 0 \quad \forall v \implies Q(\mathcal{A})e_i = 0 \quad \forall i \xrightarrow[P_i \text{ — мин. аннул.}]{} \\ \implies Q : P_i \quad \forall i \implies Q : P \implies \deg Q \geq \deg P$$

□

Теорема 9 (Гамильтона—Кэли). Характеристический многочлен оператора \mathcal{A} аннулирует \mathcal{A} .

Доказательство. Нужно доказать, что $\forall v \quad \chi(\mathcal{A})v = 0$

Докажем, что $\chi_{\mathcal{A}} : P_0$, где P_0 — минимальный аннулятор (все аннуляторы делятся на минимальный):
Пусть U — циклическое подпространство, порождённое v

χ_U — характеристический многочлен $\mathcal{A}|_U$ (он определён, т. к. пространство инвариантно)

По следствию о делителях характеристического многочлена, $\chi : \chi_U$

Знаем, что χ_U — минимальный аннулятор для v на U (по т. о циклическом подпространстве и минимальном аннуляторе)

$$\left. \begin{array}{l} \chi_U = P_0 \\ \chi : \chi_U \end{array} \right\} \implies \chi : P_0$$

□

Следствие. Если P — минимальный многочлен \mathcal{A} , то $\chi : P$.

13. Свойства взаимно простых многочленов от оператора

Свойства. \mathcal{A} — оператор на V

1. P_1, P_2, \dots, P_k — попарно взаимно просты, $T(t) = P_1(t) \cdots P_k(t)$, $v \in V$, T аннулир. v .
Тогда $\exists v_1, \dots, v_k : v = v_1 + \cdots + v_k$ и P_i аннулирует v_i
2. P, Q взаимно просты, P, Q аннуляторы $v \implies v = 0$

Доказательство.

1. **Индукция.**

• **База.** $k = 2$

P, Q взаимно просты, $v \in V$

Докажем, что $\exists v, w : v = u + w$, $P(\mathcal{A})u = 0$, $Q(\mathcal{A})w = 0$

Т. к. P, Q взаимно просты, можно разложить их НОД ($= 1$):

$$\exists F(t), G(t) : P(t)F(t) + Q(t)G(t) = 1$$

Применим к \mathcal{A} :

$$P(\mathcal{A}) \circ F(\mathcal{A}) + Q(\mathcal{A}) \circ G(\mathcal{A}) = \mathcal{E}$$

Применим к v :

$$(PF)(\mathcal{A})v + (QG)(\mathcal{A})v = v$$

Положим $u = (QG)(\mathcal{A})v$, $w = (PF)(\mathcal{A})v$

Проверим, что $P(\mathcal{A})u = 0$ (для w — аналогично):

$$\left(P(\mathcal{A}) \circ QG(\mathcal{A}) \right)v = \left(PQG \right)(\mathcal{A})v = \left(GPQ \right)(\mathcal{A})v = G(\mathcal{A}) \underbrace{\left(PQ \right)(\mathcal{A})v}_{0 \text{ (это анн. } v)} = 0$$

• **Переход.** $k - 1 \rightarrow k$

$$T = \underbrace{P_1 \dots P_{k-1}}_P \underbrace{P_k}_Q$$

$$(PQ)(\mathcal{A})v = 0 \xrightarrow{\text{база}} \exists u, w : v = u + w, \quad P(\mathcal{A})u = 0, \quad Q(\mathcal{A})w = 0$$

По индукционному предположению,

$$\exists v_1, \dots, v_{k-1} : P_i \text{ аннул. } v_i, \quad u = v_1 + \cdots + v_{k-1}$$

$$v = v_1 + \cdots + v_{k-1} + \underset{:= v_k}{w}$$

2. Пусть T — минимальный аннулятор v

$$\left. \begin{array}{l} P : T \\ Q : T \end{array} \right\} \implies T = \text{const}, \quad T(t) = c \implies cv = 0 \implies v = 0$$

□

14. Разложение пространства в прямую сумму примарных подпространств

Определение 15. K — поле, V — векторное пространство над K , \mathcal{A} — оператор на V

$P(t)$ — минимальный многочлен \mathcal{A} со старшим коэффициентом, равным 1.

Пространство V называется *примарным* (относительно \mathcal{A}), если $P(t) = Q^s(t)$ для некоторого $Q(t)$, неприводимого над K

Теорема 10. K — поле, V — векторное пространство над K , \mathcal{A} — оператор на V . $P(t)$ — минимальный многочлен \mathcal{A} , он разложен на множители:

$$P(t) = P_1(t) \cdots P_k(t), \quad \text{где } P_i(t) = Q_i^{s_i}(t), \quad Q_i \text{ — непривод. над } K$$

Тогда \exists подпространства U_1, \dots, U_k , такие что

1. все U_i инвариантны
2. $V = U_1 \oplus \cdots \oplus U_k$
3. $P_i(t)$ — минимальный многочлен \mathcal{A} на $U_i \quad \forall i$

Доказательство. Положим $U_i = \ker P_i(\mathcal{A})$. Докажем, что они подойдут:

1. Знаем, что ядро многочлена от оператора инвариантно
2. (a) Докажем, что $V = U_1 + \cdots + U_k$
 P_1, \dots, P_k попарно взаимно просты, и $P_1 \cdots P_k$ аннулирует любой v , значит

$$\forall v \quad \exists v_1, \dots, v_k : \quad v = v_1 + \cdots + v_k, \quad P_i \text{ аннул. } v_i \implies v_i \in U_i$$

- (b) Докажем, что сумма прямая:

Нужно проверить, что $U_s \cap \left(U_1 + \cdots + U_{s-1} + U_{s+1} + \cdots + U_k \right) = \{0\} \quad \forall s$
НУО проверим, что $(U_1 + \cdots + U_{k-1}) \cap U_k = \{0\}$
Возьмём $v \in (U_1 + \cdots + U_{k-1}) \cap U_k$

$$v = v_1 + \cdots + v_{k-1}, \quad v_i \in U_i, \quad v \in U_k$$

По первому свойству, $P_1 \cdots P_{k-1}$ аннулирует $v_1 + \cdots + v_{k-1} = v$

При этом, P_k аннулирует v

Заметим, что $(P_1 \cdots P_{k-1}, P_k) = 1$

По второму свойству, это означает, что $v = 0$.

- 3.

$$U_i = \ker P_i(\mathcal{A}) \implies P_i(\mathcal{A})|_{U_i} = 0$$

P_i аннулирует $\mathcal{A}|_{U_i}$

Значит, P_i делится на минимальный многочлен $\mathcal{A}|_{U_i}$

При этом, $P_i = Q_i^{s_i}$

Отсюда минимальный тоже является $Q_i^{r_i}, \quad r_i \leq s_i$

Хотим доказать, что $r_i = s_i$

Пусть $T = Q_1^{r_1} \cdots Q_k^{r_k}$

Т. к. у нас прямая сумма, существует e_1, \dots, e_n — базис V , он является объединением базисов U_i

$$\implies T(\mathcal{A})e_1 = 0, \quad \dots, \quad T(\mathcal{A})e_k = 0$$

$$\implies T \text{ аннулирует } \mathcal{A} \xrightarrow[P - \text{мин. многочл.}]{} \underbrace{T}_{\prod Q_i^{r_i}} : \underbrace{P}_{\prod Q_i^{s_i}}, \quad r_i \geq s_i \implies r_i = s_i$$

□

15. Корневые подпространства

Определение 16. λ — с. ч. \mathcal{A}

Вектор v называется *корневым вектором*, соответствующим λ , если для некоторого k многочлен $P(t) = (t - \lambda)^k$ является аннулятором v

Множество корневых векторов называется *корневым подпространством*, соотв. λ

Свойства.

- Корневое подпространство инвариантно
- V конечномерно, минимальный многочлен \mathcal{A} раскладывается на линейные множители

$$P(t) = (\lambda_1 - t)^{s_1} \cdots (\lambda_k - t)^{s_k}$$

Тогда $\ker((\lambda_i \mathcal{E} - \mathcal{A})^{s_i})$ — корневые подпространства

Доказательство.

- Пусть $P(t) = (\lambda - t)^k$ — аннул. v , т. е. $P(\mathcal{A})v = 0$

$$P(\mathcal{A})(\mathcal{A}v) = \left(P(\mathcal{A}) \circ \mathcal{A} \right) v = \left(\mathcal{A} \circ P(\mathcal{A}) \right) v = \mathcal{A} \left(\underbrace{P(\mathcal{A})v}_{=0} \right) = \mathcal{A}(0) = 0$$

- Пусть $U_i = \ker((\lambda_i \mathcal{E} - \mathcal{A})^{s_i})$, W_i — корневое подпространство для λ_i

- $U_i \subset W_i$ — очевидно ($v \in U_i \implies (\lambda_i \mathcal{E} - \mathcal{A})^{s_i} v = 0$, подойдёт $k = s_i$)
- $W_i \subset U_i$

Нужно показать, что если вектор аннулируется, то он это сделает не больше чем за s_i шагов
Пусть $v \in W_i$

Пусть k — минимальное число, такое что $(\lambda_i \mathcal{E} - \mathcal{A})^k$ аннулирует v

Тогда $(\lambda - t)^k$ — минимальный аннулятор v

При этом, $P(t)$ — аннулятор v

$$\implies P(t) : (\lambda - t)^k \implies k \leq s_i \implies v \in U_i$$

□

16. Существование жордановой формы

Определение 17. Жордановой клеткой порядка r с с. ч. λ называется матрица порядка r вида

$$J_r(\lambda) = \begin{pmatrix} \lambda & & & & 0 \\ 1 & \ddots & & & \vdots \\ \vdots & \ddots & \ddots & & \vdots \\ 0 & \cdots & 1 & \lambda & \end{pmatrix}$$

Определение 18. Жордановой матрицей называется блочно-диагональная матрица вида

$$\begin{pmatrix} J_{r_1}(\lambda_1) & & & 0 \\ 0 & \ddots & & J_{r_k}(\lambda_k) \end{pmatrix} \quad (\text{как } r_i, \text{ так и } \lambda_i \text{ могут совпадать})$$

Определение 19. Жорданов базис — базис, в котором матрица оператора жорданова

Теорема 11 (существование жордановой формы). K — поле, V — векторное пространство над K
 \mathcal{A} — оператор, $\chi_{\mathcal{A}}(t)$ раскладывается на линейные множители над K
 Тогда для \mathcal{A} существует жорданов базис

Доказательство.

- Докажем для случая, когда минимальный многочлен \mathcal{A} имеет вид $P(t) = (t - \lambda)^r$
 Сведём к случаю нильпотентного оператора:
 Положим $\mathcal{B} = \mathcal{A} - \lambda \mathcal{E}$
 $\mathcal{B}^r = 0$, \mathcal{B} — нильпотентный
 Значит, существует жорданов базис \mathcal{B} , причём на диагонали жордановой формы стоят нули

- Общий случай

$$\chi_{\mathcal{A}} = (-1)^n(t - \lambda_1)^{s_1} \cdots (t - \lambda_m)^{s_m}$$

По следствию к теореме Гамильтона–Кэли минимальный многочлен — делитель $\chi \implies$ минимальный многочлен имеет вид

$$P(t) = (t - \lambda_1)^{r_1} \cdots (t - \lambda_m)^{r_m}$$

Применим теорему о разложении в сумму примарных подпространств:

$$\text{Пусть } Q_i := (t - \lambda_i)^{r_i}$$

По теореме

$$V = U_1 \oplus \cdots \oplus U_k$$

U_i инвариантны

$Q_i(t)$ — минимальный многочлен \mathcal{A} на U_i

К U_i применяем нильпотентный случай:

Существует жорданов базис U_i

Матрица $\mathcal{A}|_{U_i}$ имеет вид

$$J_i = \begin{pmatrix} J_{r_1}(\lambda_i) & & & 0 \\ 0 & \ddots & & \\ & & J_{r_k}(\lambda_k) & \end{pmatrix}$$

Значит, в базисе, полученном объединением базисов U_i матрица \mathcal{A} имеет вид

$$J = \begin{pmatrix} J_1 & & & 0 \\ 0 & \ddots & & \\ & & J_m & \end{pmatrix}$$

□

17. Возвведение жордановой клетки в степень

Свойства.

$$1. \quad \bullet \left(J_r(0) \right)^s = \begin{pmatrix} 0 & & & & 0 \\ \vdots & & & & \vdots \\ 0 & & & & \vdots \\ 1 & & & & \vdots \\ \vdots & & & & \vdots \\ 0 & \cdots & 1 & 0 & \cdots 0 \end{pmatrix} \quad \text{при } s < r$$

То есть,

$$a_{ij} = \begin{cases} 1, & i - j = s \\ 0, & \text{иначе} \end{cases}$$

$$\bullet \left(J_r(0) \right)^s = \mathbb{O} \quad \text{при } s \geq r$$

$$2. \quad \text{Пусть } \lambda \neq 0, \quad A = \left(J_r(\lambda) \right)^s$$

Тогда A нижнетреугольная

$$a_{ij} = \begin{cases} \lambda^{s-(i-j)} C_s^{i-j}, & 0 \leq i - j \leq s \\ 0, & \text{иначе} \end{cases}$$

$$3. \quad \text{rk} \left(\left(J_r(0) \right)^s \right) = \begin{cases} r - s, & s < r \\ 0, & s \geq r \end{cases}$$

Доказательство.

1. Индукция по s .

- **База.** $s = 1$

$$J_1(0) = (0)$$

- **Переход.** $s \rightarrow s + 1$

$$\begin{aligned} J_r^s(0) &= a_{ij}, & J_r(0) &= b_{ij}, & J_r^{s+1}(0) &= c_{ij} \\ c_{ij} &= a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj} \end{aligned} \tag{1}$$

Среди a_{ij} не более одной единицы, остальные нули

Среди b_{xj} не более одной единицы, остальные нули

Значит, $c_{ij} = 0$ или $c_{ij} = 1$

$$c_{ij} = 1 \iff \exists x : \begin{cases} a_{ix} = 1 \\ b_{xi} = 1 \end{cases} \stackrel{(1)}{\iff} \exists x : \begin{cases} i - x = s \\ x - j = 1 \end{cases} \iff i - j = s + 1$$

2. $J_r(\lambda) = \lambda \cdot E + J_r(0)$

Возведём в степень и распишем как бином Ньютона (учитывая, что λE коммутирует с членами, а значит, можно приводить подобные):

$$\begin{aligned} \left(J_r(\lambda) \right)^s &= (\lambda E)^s + C_s^1 (\lambda E)^{s-1} J_r(0) + \cdots + C_s^{r-1} (\lambda E)^{s-r+1} J_r(0)^{r-1} + \underbrace{J_r^r(0)(\dots)}_{=0} \stackrel{\text{св-во 1a}}{=} \\ &= \lambda^s E + C_s^1 \lambda^{s-1} J_r(0) + \cdots + C_s^{r-1} \lambda^{s-r+1} J_r^{r-1}(0) = \\ &= \begin{pmatrix} \lambda^s & \cdot & 0 \\ \cdot & \cdot & \cdot \\ 0 & \cdot & \lambda^s \end{pmatrix} + \begin{pmatrix} 0 & \cdot & \cdot & 0 \\ \lambda^{s-1} C_s^1 & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & 0 \\ 0 & \cdot & \lambda^{s-1} C_s^1 & 0 \end{pmatrix} + \cdots + \begin{pmatrix} 0 & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot \\ \lambda^{s-r+1} C_s^{r-1} & \cdot & \cdot & 0 \end{pmatrix} \end{aligned}$$

□

18. Количество жордановых блоков и ранг. Следствие о единственности жордановой формы

Теорема 12 (количество клеток и ранг). J — жорданова матрица

Тогда количество клеток вида $J_r(\lambda)$ равно

$$\operatorname{rk} \left(J - \lambda E \right)^{r-1} - 2 \operatorname{rk} \left(J - \lambda E \right)^r + \operatorname{rk} \left(J - \lambda E \right)^{r+1}$$

Доказательство. Положим $f(s) := \operatorname{rk}(J - \lambda E)^s$

$$\begin{aligned} (J - \lambda E)^s &= \left(\begin{pmatrix} J_{r_1}(\lambda_1) & & 0 \\ & \ddots & \\ 0 & & J_{r_k}(\lambda_k) \end{pmatrix} - \lambda E \right)^s = \begin{pmatrix} J_{r_1}(\lambda_1 - \lambda) & & 0 \\ & \ddots & \\ 0 & & J_{r_k}(\lambda_k - \lambda) \end{pmatrix}^s = \\ &= \begin{pmatrix} J_{r_1}^s(\lambda_1 - \lambda) & & 0 \\ & \ddots & \\ 0 & & J_{r_k}^s(\lambda_k - \lambda) \end{pmatrix} \end{aligned}$$

Какое-то из λ_i совпало с λ

$$f(s) = \sum_{i=1}^k \operatorname{rk} \left(J_{r_i}^s(\lambda_i - \lambda) \right)$$

- Если $\lambda \neq \lambda_i$, то $\operatorname{rk} \left(J_{r_i}^s(\lambda_i - \lambda) \right) = r_i \quad \forall s$

$$f(s) - f(s+1) = \sum \left(\operatorname{rk} \left(J_{r_i}^s(\lambda_i - \lambda) \right) - \operatorname{rk} \left(J_{r_i}^{s+1}(\lambda - \lambda_i) \right) \right)$$

То есть, если $\lambda_i \neq \lambda_j$, то i -е слагаемое равно $r_i - r_j = 0$

- Если $\lambda_i = \lambda$, $r_i \leq s$, то i -е слагаемое равно $0 - 0 = 0$

- Если $\lambda_i = \lambda$, $r_i > s$, то i -е слагаемое равно $(r_i - s) - (r_i - (s + 1)) = 1$

$f(s+1) - f(s)$ — количество клеток, для которых $\lambda_i = \lambda$, $r_i > s$

$(f(s+1) - f(s)) - (f(s) - f(s-1))$ — количество клеток размера s

Это равно $f(s+1) - 2f(s) + f(s-1)$

□

Следствие (единственность жордановой формы). J, J' — жордановы матрицы \mathcal{A} в некоторых базисах. Тогда J, J' совпадают с точностью до перестановки жордановых клеток

Доказательство. Ранг не зависит от выбора базиса, значит, количество клеток каждого вида совпадает. □

19. Минимальный многочлен оператора, у которого известна жорданова форма

Теорема 13. J — жорданова матрица, $\lambda_1, \dots, \lambda_k$ — с. ч. J

r_i — максимальный размер жордановой клетки, соотв. λ_i

Тогда минимальный многочлен равен $(t - \lambda_1)^{r_1} \cdots (t - \lambda_k)^{r_k}$

Доказательство. Пусть e_1, \dots, e_n — жорданов базис

P_i — минимальный аннулятор e_i

Тогда минимальный многочлен равен НОК(P_1, \dots, P_n)

Пусть e_i соответствует j -му столбцу клетки $J_r(\lambda)$

$$(\mathcal{A} - \lambda \mathcal{E})^{r-i}(e_i) = 0, \quad (\mathcal{A} - \lambda \mathcal{E})^{r-i-1}(e_i) \neq 0$$

$$\implies P_i(t) = (t - \lambda)^{r-i}$$

Минимальный многочлен — это НОК многочленов вида $(t - \lambda_i)^s$, $s \leq r_i$

Среди них есть $(t - \lambda_1)^{r_1}, \dots, (t - \lambda_k)^{r_k}$

Значит, среди них есть P_i , а остальные — не делители

$$\implies \text{НОК} = (t - \lambda_1)^{r_1} \cdots (t - \lambda_k)^{r_k}$$

□

20. Комплексификация вещественного векторного пространства. Продолжение операторов

Определение 20. V — векторное пространство над \mathbb{R}

Комплексификация V — это множество \widehat{V} , состоящее из пар (u, v) с операцией $\mathbb{C} \times \widehat{V} \rightarrow \widehat{V}$, заданной равенством

$$(a + bi) \cdot (u, v) = (au - bv, av + bu)$$

и операцией $\widehat{V} \times \widehat{V} \rightarrow \widehat{V}$, заданной равенством

$$(u_1, v_1) + (u_2, v_2) = (u_1 + u_2, v_1 + v_2)$$

Определение 21. $w = (u, v)$

$(u, -v)$ называется сопряжённым к w

Обозначение. \bar{w}

Теорема 14. \widehat{V} – векторное пространство над \mathbb{C}

Доказательство.

1. \widehat{V} – абелева группа по сложению
2. $1 \cdot w = w$
3. Ассоциативность умножения
4. Две дистрибутивности умножения

Всё проверяется подстановкой □

Обозначение. Пару (u, v) будем обозначать $u + vi$

Обозначение. Множество пар $(u, 0)$ отождествим с V

Теорема 15 (базис комплексификации). Пусть e_1, \dots, e_n – базис V

Тогда $e_1 = e_1 + 0 \cdot i, \dots, e_n = e_n + 0 \cdot i$ – базис \widehat{V}

Доказательство.

- Докажем, что система является порождающей:

Пусть $w \in \widehat{V}$

Разложим w по базису e_1, \dots, e_n в V :

$$w = a_1e_1 + \dots + a_ne_n, \quad v = b_1e_1 + \dots + b_ne_n, \quad a_s, b_s \in \mathbb{R}$$

$$w = \underbrace{(a_1 + b_1i)}_{\in \mathbb{C}}e_1 + \dots + \underbrace{(a_n + b_ni)}_{\in \mathbb{C}}e_n$$

- Докажем ЛНЗ:

Пусть $c_1e_1 + \dots + c_ne_n = 0, \quad c_s \in \mathbb{C}, \quad c_s = a_s + b_si, \quad a_s, b_s \in \mathbb{R}$

$$(a_1 + b_1i)(e_1 + 0i) + \dots + (a_n + b_ni)(e_n + 0i) = 0$$

Разделим вещественную и мнимую части:

$$\left((a_1e_1 - b_10) + \dots + (a_ne_n - b_n0) \right) + \left((a_10 + b_1e_1) + \dots + (a_n0 + b_ne_n) \right)i = 0 + 0i$$

Значит, каждое большое слагаемое равно нулю:

$$\begin{cases} a_1e_1 + \dots + a_ne_n = 0 \\ b_1e_1 + \dots + b_ne_n = 0 \end{cases} \xrightarrow{e_1, \dots, e_n \text{ ЛНЗ в } V} \begin{cases} a_1 = \dots = a_n = 0 \\ b_1 = \dots = b_n = 0 \end{cases}$$

□

Следствие. $\dim_{\mathbb{C}} \widehat{V} = \dim_{\mathbb{R}} V$

Свойства (сопряжённых векторов).

1. $\overline{\bar{w}} = w$
2. $\overline{w_1 + w_2} = \overline{w_1} + \overline{w_2}, \quad \overline{z \cdot w} = \overline{z} \cdot \overline{w}$
3. w_1, \dots, w_n ЛНЗ $\iff \overline{w_1}, \dots, \overline{w_n}$ ЛНЗ

Доказательство.

1. $w = u + vi, \quad \overline{w} = u - vi, \quad \overline{\bar{w}} = u - (-v)i = u + vi = w$
2. Первое равенство – упражнение. Проверим второе:

Пусть $z = a + bi$, $w = u + vi$

$$\overline{(a+bi)(u+vi)} = \overline{(au-bv)+(av+bu)i} = (au-bv)-(av+bu)i$$

$$\overline{(a+bi) \cdot (u+vi)} = (a-bi)(u-vi) = \left(\underbrace{au - (-b)(-v)}_{au-bv} \right) + \left(\underbrace{a(-v) + (-b)u}_{-(av+bu)} \right)$$

3. Достаточно доказать в одну сторону (\implies), дальше сопьёмся на первое свойство
Пусть $\overline{w_1}, \dots, \overline{w_n}$ ЛЗ, то есть

$$c_1, \dots, c_n \in \mathbb{C} : c_1\overline{w_1} + \dots + c_n\overline{w_n} = 0, \quad c_i \notin \textcircled{\cdot}$$

$$0 = \overline{0} = \overline{c_1\overline{w_1} + \dots + c_n\overline{w_n}} \underset{2 \text{ сб-бо}}{=} \overline{c_1\overline{w_1}} + \dots + \overline{c_n\overline{w_n}} \underset{1 \text{ сб-бо}}{=} \overline{c_1}w_1 + \dots + \overline{c_n}w_n$$

$$c_i \notin \textcircled{\cdot} \implies \overline{c_i} \notin \textcircled{\cdot}$$

w_1, \dots, w_n ЛЗ — $\frac{1}{2}$

□

Определение 22. \mathcal{A} — оператор на V

Продолжением \mathcal{A} на \widehat{V} называется отображение $\widehat{\mathcal{A}} : \widehat{V} \rightarrow \widehat{V}$, заданное равенством $\widehat{\mathcal{A}}(u+vi) = \mathcal{A}(u) + \mathcal{A}(v)i$

Свойство. $\widehat{\mathcal{A}}$ линейно

21. Каноническая матрица оператора в вещественном пространстве

Обозначение. $P(t) = c_k t^k + c_{k-1} t^{k-1} + \dots + c_0$, $c_s \in \mathbb{C}$
Тогда $\overline{P}(t) = \overline{c_k} t^k + \overline{c_{k-1}} t^{k-1} + \dots + \overline{c_0}$ — сопряжённый к P

Лемма 5 (применение операторов к сопряжённым векторам). \mathcal{A} — оператор на V . Тогда

1. $\widehat{\mathcal{A}}(\overline{w}) = \overline{\widehat{\mathcal{A}}(w)}$
2. $P(\widehat{\mathcal{A}})(w_1) = w_2 \implies \overline{P}(\widehat{\mathcal{A}})(\overline{w_1}) = \overline{w_2}$
3. Если $P(t)$ аннулирует w , то $\overline{P}(t)$ аннулирует \overline{w}
4. Если w — корневой вектор, соответствующий λ , то \overline{w} — корневой вектор, соответствующий $\bar{\lambda}$
5. Если w_1, \dots, w_n — (жорданов) базис корневого подпространства, соответствующего λ , то $\overline{w}_1, \dots, \overline{w}_n$ — (жорданов) базис корневого подпространства, соответствующего $\bar{\lambda}$ (если один жорданов, то и второй жорданов)

Доказательство.

1. Пусть $w = u + iv$, $\overline{w} = u - iv$

$$\widehat{\mathcal{A}}(w) = \mathcal{A}u + \mathcal{A}vi, \quad \mathcal{A}(\overline{w}) = \mathcal{A}u + \mathcal{A}(-v)i = \mathcal{A}u - \mathcal{A}vi$$

2. Из первого свойства $\widehat{\mathcal{A}}^{(s)}(\overline{w_1}) = \overline{\widehat{\mathcal{A}}^{(s)}(w_1)}$

Пусть $P(t) = c_k t^k + \dots + c_0$

$$w_2 = c_k P(\widehat{\mathcal{A}})(w_1) + \dots + c_0 w_1$$

$$\overline{w_2} = \overline{c_k} \overline{P}(\widehat{\mathcal{A}})(\overline{w_1}) + \dots + \overline{c_0} \overline{w_1} = \overline{P}(\widehat{\mathcal{A}})(\overline{w_1})$$

3. $P(\widehat{\mathcal{A}})(w) = 0 \implies \overline{P}(\widehat{\mathcal{A}})(\overline{w}) \underset{2 \text{ сб-бо}}{=} \overline{P(\widehat{\mathcal{A}})(w)} = \overline{0} = 0$

4. $P(t) = (t - \lambda)^k$ аннулирует w для некоторого k
 $\Rightarrow \bar{P}(t)$ аннулирует \bar{w} (из 3 св-ва)
 $\bar{P}(t) = (t - \bar{\lambda})^k$

5. • ЛНЗ доказана
• Докажем, что это порождающая система:
Пусть \bar{w} принадлежит пространству, соответствующему $\bar{\lambda} \Rightarrow w$ принадлежит пространству, соотв. λ
Разложим по базису:

$$\begin{aligned}\exists c_i : \quad w &= c_1 e_1 + \cdots + c_n e_n \\ \Rightarrow \bar{w} &= \overline{c_1 e_1} + \cdots + \overline{c_n e_n}\end{aligned}$$

- Докажем, что сопряжённый к жорданову базису жорданов:

$$\begin{aligned}\widehat{\mathcal{A}} - \lambda \mathcal{E} &= \widehat{\mathcal{A}} - \bar{\lambda} \widehat{\mathcal{E}} \\ (\widehat{\mathcal{A}} - \lambda \mathcal{E})e_i &= e_{i-1} \Rightarrow (\widehat{\mathcal{A}} - \bar{\lambda} \mathcal{E})\bar{e}_i = \bar{e}_{i+1}\end{aligned}$$

□

Теорема 16. Пусть V - конечномерное векторное пространство над \mathbb{R} , \mathcal{A} – оператор на V . Тогда существует базис V , в котором матрица \mathcal{A} является блочно-диагональной, и каждый блок – либо жорданова клетка, либо имеет вид

$$\begin{pmatrix} a & b & & & & 0 \\ -b & a & & & & \vdots \\ 1 & 0 & \ddots & & & \vdots \\ 0 & 1 & & \ddots & & \vdots \\ \vdots & & 1 & 0 & a & b \\ 0 & & 0 & 1 & -b & a \end{pmatrix}$$

Доказательство. Пусть минимальный многочлен \mathcal{A} равен

$$P(t) = (t - a_1)^{m_1} \cdots (t^2 + p_1 t + q_1)^{s_1} \cdots,$$

где $t^2 + p_i t + q_i$ не имеют вещественных корней

Разложим V в прямую сумму примарных подпространств

Достаточно доказать для одного подпространства

Для подпространства, соответствующего $(t - a)^m$ есть базис, в котором матрица \mathcal{A} жорданова

Рассмотрим подпространство, соответствующее $(t^2 + pt + q)^s$:

Пусть $\lambda, \bar{\lambda}$ – комплексные корни $t^2 + pt + q$

$$(t^2 + pt + q)^s = (t - \lambda)^s (t - \bar{\lambda})^s$$

Пусть $P_1 = (t^2 + pt + q)^s$

Знаем, что $P_1(\mathcal{A}) = 0$ на корневом подпространстве U

Тогда $P_1(\widehat{\mathcal{A}}) = 0$ на \widehat{U}

$$\widehat{U} = \widehat{W}_1 + \widehat{W}_2, \quad \widehat{W}_1, \widehat{W}_2 \text{ – корневые подпространства для } \lambda, \bar{\lambda}$$

Существует жорданов базис w_1, \dots, w_k для \widehat{W}_1

Тогда $\overline{w_1}, \dots, \overline{w_k}$ – жорданов базис для \widehat{W}_2

$w_1, \dots, w_k, \overline{w_1}, \dots, \overline{w_k}$ – базис \widehat{U}

Пусть $w_i = u_i + iv_i$

Докажем, что $u_1, v_1, u_2, v_2, \dots, u_k, v_k$ – базис U :

Следующие элементарные преобразования переводят базис \widehat{U} в базис \widehat{U} , а значит, и в базис U :

$$u_i \pm iv_i \rightarrow (u_i + iv_i) + (u_i - iv_i), \quad u_i - iv_i \rightarrow u_i, \quad u_i - v_i \rightarrow u_i, \quad (u_i - iv_i) - u_i \rightarrow u_i, v_i$$

Проверим, что в этом базисе получается правильная жорданова матрица:
Рассмотрим жордановы цепочки

$$w_1, \dots, w_{r_1}, w_{r_1+1}, \dots, w_{r_1+r_2}, \dots \dots \dots$$

Докажем, что им соответствуют клетки размера $2r_1, 2r_2, \dots$:
Рассмотрим первую цепочку:

$$\widehat{\mathcal{A}}(u_m + iv_m) = \begin{cases} \lambda(u_m + iv_m) + (u_m + iv_m), & m < r_1 \\ \lambda(u_r + iv_r), & m = r \end{cases}$$

Пусть $\lambda = a + bi$

При $m < r$,

$$\mathcal{A}(u_m) + \mathcal{A}(v_m)i = (au_m - bv_m) + (bu_m + av_m)i = \underbrace{(au_m - bv_m)}_{\mathcal{A}(u_m)} + \underbrace{(bu_m + av_m)}_{\mathcal{A}(v_m)} i$$

При $m = r$,

$$\mathcal{A}(u_m) = (au_m - bv_m) + (bu_m + av_m)i = (au_m - bv_m) + (bu_m + av_m)i$$

□

Часть II

Линейные отображения в евклидовых и унитарных пространствах

22. Изоморфизм векторного пространства и двойственного к нему

Определение 23. V — векторное пространство над полем K

Линейным функционалом на V называется линейное отображение $V \rightarrow K$

Свойство. Линейные функционалы пространства V над K образуют векторное пространство над K

Определение 24. Пространство функционалов называется *двойственным* или *сопряжённым*.

Обозначение. V^*

Теорема 17 (изоморфизм пространства и двойственного к нему).

1. V — конечномерное пространство над K

$$V^* \simeq V$$

2. V — евклидово пространство

Для любого $v \in V$ определим $y_v \in V^*$ как $y_v(x) = (x, v)$

Тогда отображение $v \mapsto y_v$ является изоморфизмом

Доказательство.

1. Пусть $n := \dim V$

Пусть e_1, \dots, e_n — базис V

Рассмотрим $\varphi : V^* \rightarrow K^n$: $\varphi(y) = (y(e_1), \dots, y(e_n))$

Мы знаем, что пространства одной размерности изоморфны, так что $K^n \simeq V$

Докажем, что φ — изоморфизм:

- Линейность (сложение и умножение в K^n — покомпонентно):

$$\begin{aligned}\varphi(y_1 + y_2) &= \left((y_1 + y_2)(e_1), \dots, (y_1 + y_2)(e_n) \right) = \left(y_1(e_1) + y_2(e_1), \dots, y_1(e_n) + y_2(e_n) \right) = \\ &= \left(y_1(e_1), \dots, y_1(e_n) \right) + \left(y_2(e_1), \dots, y_2(e_n) \right) = \varphi(y_1) + \varphi(y_2)\end{aligned}$$

$$\varphi(ky) = \left((ky)(e_1), \dots, (ky)(e_n) \right) = \left(ky(e_1), \dots, ky(e_n) \right) = k \left(y(e_1), \dots, y(e_n) \right) = k\varphi(y)$$

- Биективность:

Пусть $a \in K^n$, $a = (a_1, \dots, a_n)$, $a_i \in K$

$$\exists !y \in V^* : \quad y(e_1) = a_1, \dots, y(e_n) = a_n \quad \Rightarrow \quad \exists !y \in V^* : \quad \varphi(y) = a$$

2. • Проверим, что $y_v \in V^*$, т. е. что y_v линейно:

– $y_v(x_1 + x_2) = (x_1 + x_2, v) \xrightarrow{\text{лин. скал. произв.}} (x_1, v) + (x_2, v) = y_v(x_1) + y_v(x_2)$

– $y_v(kx) = (kx, v) = k(x, v) = ky_v(x)$

- Пусть $\varphi(v) = y_v$. Докажем, что φ — изоморфизм $V \rightarrow V^*$:

- Линейность:

* $\varphi(u + v) \stackrel{?}{=} \varphi(u) + \varphi(v)$

$$\begin{aligned}\varphi(u + v) \stackrel{?}{=} \varphi(u) + \varphi(v) &\iff y_{u+v} \stackrel{?}{=} y_u + y_v \iff \\ &\iff y_{u+v}(x) \stackrel{?}{=} y_u(x) + y_v(x) \quad \forall x \iff \\ &\iff (x, u + v) \xrightarrow{\text{лин. скалярного произв.}} (x, u) + (x, v)\end{aligned}$$

* $\varphi(kv) \stackrel{?}{=} k\varphi(v)$

$$\begin{aligned}\varphi(kv) \stackrel{?}{=} k\varphi(v) &\iff y_{kv} \stackrel{?}{=} ky_v \iff y_{kv}(x) \stackrel{?}{=} ky_v(x) \quad \forall x \iff \\ &\iff (x, kv) \xrightarrow{\text{лин. скалярного произв.}} k(x, v)\end{aligned}$$

- Инъективность:

Пусть $\varphi(v) = 0$. Тогда

$$y_v = 0 \quad \Rightarrow \quad y_v(x) = 0 \quad \forall x \quad \Rightarrow \quad (x, v) = 0 \quad \forall x \quad \Rightarrow \quad v = 0$$

Вместе с тем, что $\dim V = \dim V^*$, это даёт биективность

□

Определение 25. Изоморфизм из пункта 2 называется *каноническим изоморфизмом* из V в V^*

23. Дважды двойственное пространство

Теорема 18. V — векторное пространство над K

Для любого $x \in V$ обозначим через z_x отображение $V^* \rightarrow K$, заданное формулой $z_x(y) = y(x)$

1. $\forall x \in K \quad z_x \in (V^*)^*$, т. е. z_x — линейный функционал на V^*
2. отображение $\varphi : V \rightarrow (V^*)^*$, заданное формулой $\varphi(x) = z_x$ является линейным
3. если V конечномерно, то φ — изоморфизм

Доказательство.

$$\begin{aligned}
1. \quad & \bullet z_x(y_1 + y_2) \stackrel{?}{=} z_x(y_1) + z_x(y_2) \\
& z_x(y_1 + y_2) = (y_1 + y_2)(x) \\
& z_x(y_1) + z_x(y_2) = y_1(x) + y_2(x) \\
& \bullet z_x(ky) \stackrel{?}{=} kz_x(y) \\
& z_x(ky) = (ky)(x) = ky(x) = kz_x(y)
\end{aligned}$$

$$\begin{aligned}
2. \quad & \bullet \varphi(x_1 + x_2) \stackrel{?}{=} \varphi(x_1) + \varphi(x_2) \\
& z_{x_1+x_2} \stackrel{?}{=} z_{x_1} + z_{x_2} \\
& \forall y \quad z_{x_1+x_2}(y) = z_{x_1}(y) + z_{x_2}(y) \\
& y(x_1 + x_2) \stackrel{?}{=} y(x_1) + y(x_2)
\end{aligned}$$

Это верно, так как y линейно

$$\begin{aligned}
& \bullet \varphi(kx) \stackrel{?}{=} k\varphi(x) \\
& z_{kx} \stackrel{?}{=} kz_x \\
& \forall y \quad z_{kx}(y) \stackrel{?}{=} kz_x(y) \\
& y(kx) \stackrel{?}{=} ky(x)
\end{aligned}$$

Это верно, так как y линейно

3. Размерности равны, так что достаточно доказать инъективность:

φ инъективно $\iff \varphi(x) = 0$ только при $x = 0 \iff z_x$ — нулевое отображение только при $x = 0 \iff z_x(y) = 0 \quad \forall y$ только при $x = 0 \iff y(x) = 0 \quad \forall y$ только при $x = 0$

Нужно проверить, что $\forall x \neq 0 \quad \exists$ линейное отображение $y : y(x) \neq 0$

Дополним до базиса:

Пусть x, e_2, \dots, e_n — базис V

Определим $y : y(x) = 1, \quad y(e_i) = 0$

$$y(\alpha x + \beta_2 e_2 + \dots + \beta_n e_n) = \alpha$$

Оно линейно, $y(x) \neq 0$

□

24. Двойственный базис. Матрица перехода для двойственного базиса

Лемма 6. V — конечномерное векторное пространство, e_1, \dots, e_n — базис V
 $f_1, \dots, f_n \in V^*$ такие, что $f_i(e_i) = 1, \quad f_i(e_j) = 0$ при $i \neq j$
Тогда f_1, \dots, f_n — базис V^*

Доказательство. Знаем, что $\dim V = \dim V^*$

Достаточно доказать ЛНЗ:

Возьмём ЛК:

Пусть $a_1, \dots, a_n \in K$ такие, что $f = a_1 f_1 + \dots + a_n f_n$ — нулевой функционал

$$0 = f(e_i) = a_1 \underbrace{f_1(e_i)}_0 + \dots + a_i \underbrace{f_i(e_i)}_1 + \dots + a_n \underbrace{f_n(e_i)}_0 = a_i \quad \forall i$$

□

Определение 26. f_1, \dots, f_n называется *двойственным базисом* к e_1, \dots, e_n .

Теорема 19. e_i, e'_i — базисы V , C — матрица перехода от e_i к e'_i
 f_i, f'_i — соответствующие двойственные базисы

- Матрица перехода от f_i к f'_i равна $(C^{-1})^T$
- Пусть Y, Y' — строки координат $y \in V^*$ в базисах f_i, f'_i
Тогда $Y' = YC$

Доказательство.

- Пусть $D = (d_{ij})$ — матрица перехода от f_i к f'_i

$$U = (u_{ij}), \quad U = D^T C$$

Докажем, что $U = E$

$$e'_i = c_{1i}e_1 + c_{2i}e_2 + \dots, \quad f'_j = d_{1j}f_1 + d_{2j}f_2 + \dots$$

Применим одно к другому:

$$\begin{aligned} \left. \begin{array}{ll} 1, & i = j \\ 0, & i \neq j \end{array} \right\} = f'_j(e'_i) &= d_{1j}f_1(c_{1i}e_1 + c_{2i}e_2 + \dots) + d_{2j}f_2(c_{1i}e_1 + c_{2i}e_2 + \dots) + \dots = \\ &= d_{1j}c_{1i} \cdot 1 + d_{1j}c_{2i} \cdot 0 + \dots + d_{2j}c_{1i} \cdot 0 + d_{2j}c_{2i} \cdot 1 + \dots = d_{1j}c_{1i} + d_{2j}c_{2i} + \dots \end{aligned}$$

d — этой j -я строка D^T , c — i -й столбец C

Значит, $f'_j(e'_i) = u_{ji}$

- $(C^{-1})^T$ — матрица перехода от f_i к f'_i
 Y^T, Y'^T — столбцы координат y
 $Y^T = (C^{-1})^T Y'^T$ — транспонированный

$$Y = Y'C^{-1} \implies YC = Y'$$

□

25. Собственные числа самосопряжённого оператора. Лемма об эрмитовой матрице

Определение 27. \mathcal{A} — оператор в евклидовом или унитарном пространстве
 \mathcal{B} называется *сопряжённым* к \mathcal{A} , если $(\mathcal{A}x, y) = (x, \mathcal{B}y) \quad \forall x, y$

Обозначение. \mathcal{A}^*

Свойства.

- $\mathcal{A}^{**} = \mathcal{A}$
- Пусть A, A^* — матрицы $\mathcal{A}, \mathcal{A}^*$ в некотором ОНБ
 - $A^* = A^T$ в евклидовом пространстве
 - $A^* = \overline{A}^T$ в унитарном пространстве

Определение 28. Оператор в евклидовом или унитарном пространстве 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 29. Квадратная матрица называется

- симметричной* (*симметрической*), если $A = A^T$

- эрмитовой, если $A = \bar{A}^T$

Свойство. \mathcal{A} — оператор в евклидовом/унитарном пространстве, A — его матрица в ОНБ
 \mathcal{A} самосопряжённый $\iff A$ симметрична/эрмитова

Лемма 7. \mathcal{A} — самосопряжённый оператор на унитарном пространстве
Тогда $(\mathcal{A}x, x) \in \mathbb{R} \quad \forall x$

Доказательство.

$$(\mathcal{A}x, x) \xlongequal[\text{самосопр.}]{} (x, \mathcal{A}^*x) = (x, \mathcal{A}x)$$

$$(\mathcal{A}x, x) \xlongequal[\text{полуторалинейность}]{} \overline{(x, \mathcal{A}x)}$$

$$\implies (x, \mathcal{A}x) \in \mathbb{R} \implies (\mathcal{A}x, x) \in \mathbb{R}$$

□

Определение 30. Самосопряжённый оператор называется *положительно определённым*, если

$$(\mathcal{A}x, x) > 0 \quad \forall x \neq 0$$

Теорема 20 (о собственных числах самосопряжённого оператора).

\mathcal{A} — оператор на унитарном пространстве

1. \mathcal{A} — нормальный
 \mathcal{A} самосопряжённый \iff все с. ч. \mathcal{A} вещественные
2. \mathcal{A} — самосопряжённый
 \mathcal{A} положительно определён \iff все с. ч. положительны

Доказательство.

1. Знаем, что существует ОНБ из с. в.

Пусть λ_i — с. ч.

$$A, A^* — матрицы \mathcal{A} и \overline{\mathcal{A}}^* в этом базисе \implies A^* = A^T \\ \mathcal{A} — самосопряжённый \iff A = A^* \iff A = \overline{A^T} \iff$$

$$\begin{pmatrix} \lambda_1 & & 0 \\ \cdot & \cdot & \cdot \\ 0 & \cdot & \lambda_n \end{pmatrix} = \begin{pmatrix} \overline{\lambda_1} & & 0 \\ \cdot & \cdot & \cdot \\ 0 & \cdot & \overline{\lambda_n} \end{pmatrix}^T \iff \lambda_i = \overline{\lambda_i} \quad \forall i \iff \lambda_i \in \mathbb{R}$$

2. Пусть e_i — ОНБ из с. в., λ_i — с. ч., $\lambda_i \in \mathbb{R}$

Пусть $x = a_1e_1 + \dots + a_ne_n$

$$(\mathcal{A}x, x) = (a_1\lambda_1e_1 + \dots + a_n\lambda_ne_n, a_1e_1 + \dots + a_ne_n) = \sum \lambda_i a_i \overline{a_j} (e_i, e_j) = \\ = \sum \lambda_i a_i \overline{a_i} = \sum \lambda_i |a_i|^2 \in \mathbb{R}$$

- Если $\lambda_i > 0 \quad \forall i$, то $\sum_{>0} \lambda_i |a_i|^2 \geq 0$

Равенство достигается только при $|a_i|^2 \in \{0\}$, то есть $a_i \in \{0\}$. Значит, $x = 0$

- Пусть не все $\lambda_i > 0$, $\lambda_{i_0} \leq 0$
Для $x = e_{i_0}, x \neq 0, (\mathcal{A}x, x) = \lambda_{i_0} \leq 0 \neq$

□

Лемма 8. A — эрмитова матрица

Тогда все корни $\chi_A(t)$ вещественны

Доказательство. A — матрица порядка n

Определим оператор $\mathcal{A} : \mathbb{C}^n$ как $X \mapsto AX$

Тогда A — матрица \mathcal{A} в стандартном базисе

A — эрмитова; станд. базис является ОНБ $\implies \mathcal{A}$ — самосопряжённый

Все с. ч. \mathcal{A} вещественны, это и есть корни $\chi_A(t)$

□

Лемма 9 (ортогональность с. в.). \mathcal{A} самосопряжённый на \mathbb{R}^n , μ, λ — различные с. ч., x, y — соответствующие с. в.

Тогда $(x, y) = 0$

Доказательство.

$$\lambda(x, y) \stackrel{\text{линейность}}{=} (\lambda x, y) \stackrel{\text{с. в.}}{=} (\mathcal{A}x, y) \stackrel{\text{def. } \mathcal{A}^*}{=} (x, \mathcal{A}^*y) \stackrel{\text{самоспр.}}{=} (x, \mathcal{A}y) \stackrel{\text{с. в.}}{=} (x, \mu x) \stackrel{\text{линейность}}{=} \mu(x, y)$$

□

26. Ортогональность собственных векторов. Самосопряжённый оператор на \mathbb{R}^n

Теорема 21. \mathcal{A} — самосопряжённый оператор на \mathbb{R}^n

1. $\chi_{\mathcal{A}}(t)$ раскладывается на линейные множители над \mathbb{R}
2. Существует ОНБ \mathbb{R}^n , состоящий из с. в. \mathcal{A}

Доказательство.

1. Разложим $\chi_A(t)$ на линейные множители над \mathbb{C} :

$$\chi_A(t) = (-1)^n(t - \lambda_1)\dots(t - \lambda_n), \quad \lambda_i \in \mathbb{C}$$

Пусть A — матрица \mathcal{A} в стандартном базисе $\implies A = A^T \implies A = \overline{A^T} \implies A$ венц.

$\implies A$ эрмитова $\stackrel{\text{лемма 8}}{\implies} \lambda_i \in \mathbb{R} \quad \forall i$

2. \mathcal{A} диагонализуем над \mathbb{C} .

Рассмотрим V_{λ_i} — собственные подпространства в \mathbb{R}^n , V'_{λ_i} — собств. подпр-ва в \mathbb{C}^n .

$$\dim_{\mathbb{R}} V_{\lambda_i} = \dim_{\mathbb{C}} V'_{\lambda_i}$$

По критерию диагонализуемости в терминах кратностей,

$$\sum \dim_{\mathbb{R}} V_{\lambda_i} = \sum \dim_{\mathbb{C}} V'_{\lambda_i} = n$$

Значит, объединение базисов V_{λ_i} будет базисом V .

Выберем в каждом из них ОНБ.

□

27. Корень из самосопряжённого оператора. Полярное разложение

Теорема 22 (корень из самосопряжённого оператора). \mathcal{A} — положительно определённый самосопряж.

Тогда существует положительно определённый самосопряжённый \mathcal{B} : $\mathcal{A} = \mathcal{B}^2$

Доказательство. \mathcal{A} — самосопряжённый $\implies \mathcal{A}$ — нормальный $\implies \exists$ ОНБ из с. в. \mathcal{A}

Пусть e_1, \dots, e_n — ОНБ из с. в., $\lambda_1, \dots, \lambda_n$ — с. ч.

\mathcal{A} — самосопряжённый $\implies \lambda_i \in \mathbb{R}$

\mathcal{A} — полож. опред. $\implies \lambda_i > 0$

Определим \mathcal{B} как $\mathcal{B}(e_i) = \sqrt{\lambda_i} e_i$

Проверим, что он подойдёт:

Рассмотрим матрицу \mathcal{B} в базисе e_1, \dots, e_n :

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

Она эрмитова $\Rightarrow \mathcal{B}$ самоспряжённый

$\sqrt{\lambda_i} > 0 \Rightarrow \mathcal{B}$ положительно определён

$$\mathcal{B}(\mathcal{B}(e_i)) = \mathcal{B}(\sqrt{\lambda_i} e_i) = \lambda_i e_i = \mathcal{A}(e_i) \quad \forall i \quad \Rightarrow \mathcal{B}^2 = \mathcal{A}$$

□

Лемма 10. \mathcal{A} невырожденный

Тогда $\mathcal{A}\mathcal{A}^*$ — самосопряжённый положительно определённый

Доказательство.

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

$$(\mathcal{A}^*\mathcal{A}x, x) = (\mathcal{A}^*(\mathcal{A}x), x) = (\mathcal{A}x, (\mathcal{A}^*)^*x) = (\mathcal{A}x, \mathcal{A}x)_{\mathcal{A}x \neq 0, \text{ т. к. } \mathcal{A} \text{ невырж.}} > 0$$

□

Теорема 23 (полярное разложение оператора).

\mathcal{A} — невырожденный оператор на унитарном пространстве

Тогда $\exists \mathcal{U}, \mathcal{B}$ такие, что:

1. \mathcal{U} унитарный
2. \mathcal{B} — самосопряжённый положительно определённый
3. $\mathcal{A} = \mathcal{U}\mathcal{B}$

Доказательство. $\mathcal{A}\mathcal{A}^*$ самосопряжённый положительно определённый (по лемме). Значит

$$\exists \mathcal{B} : \quad \mathcal{B}^2 = \mathcal{A}^*\mathcal{A}, \quad \mathcal{B} \text{ полож. опр. самосопряж.}$$

$\mathcal{A}^*, \mathcal{A}$ невырожденные $\Rightarrow \mathcal{A}^*\mathcal{A}$ невырожденный $\Rightarrow \mathcal{B}$ невырожденный $\Rightarrow \exists \mathcal{B}^{-1}$

Положим $\mathcal{U} = \mathcal{A}\mathcal{B}^{-1}$

Докажем, что эти \mathcal{U}, \mathcal{B} подойдут:

Осталось проверить только унитарность, т. е. что $\mathcal{U}^* = \mathcal{U}$

$$\mathcal{U}^* = (\mathcal{A}\mathcal{B}^{-1})^* = (\mathcal{B}^{-1})^* \mathcal{A}^* \xrightarrow{\text{видно из матрицы}} (\mathcal{B}^*)^{-1} \mathcal{A}^* \xrightarrow{\mathcal{B} \text{ самоспр.}} \mathcal{B}^{-1} \mathcal{A}^*$$

$$\mathcal{U}^*\mathcal{U} = (\mathcal{B}^{-1}\mathcal{A}^*)((\mathcal{A}\mathcal{B}^{-1})^*) = \mathcal{B}^{-1}(\mathcal{A}^*\mathcal{A})\mathcal{B}^{-1} = \mathcal{B}^{-1}\mathcal{B}^2\mathcal{B}^{-1} = \mathcal{E}$$

□

Следствие (перестановка сомножителей). \mathcal{A} — невырожденный оператор

Тогда \exists унитарный \mathcal{U} и самосопряжённый положительно определённый \mathcal{B} такие, что $\mathcal{A} = \mathcal{B}\mathcal{U}$

Доказательство. Применим теорему к \mathcal{A}^* :

$\mathcal{A}^* = \mathcal{U}_1\mathcal{B}$, \mathcal{U}_1 — унитарный, \mathcal{B} — самосопряжённый пол. опред.

$$\mathcal{A} = (\mathcal{A}^*)^* = (\mathcal{B}\mathcal{U}_1)^* = \mathcal{U}_1^*\mathcal{B}^* = \mathcal{U}_1^*\mathcal{B}$$

Подойдёт $\mathcal{U} = \mathcal{U}_1$

□

28. Квадратичные формы: ортогональное преобразование, преобразование двух форм

Теорема 24 (ортогональное преобразование квадратичной формы).

1. Вещественная квадратичная форма может быть приведена к диагональному виду ортогональным преобразованием
2. Если C — ортогональная матрица, $C^T AC$ — диагональная, то на диагонали матрицы $C^T AC$ записаны с. ч. матрицы A

Доказательство.

1. \mathcal{A} — оператор на \mathbb{R}^n , A — его матрица в стандартном базисе

\mathcal{A} самосопряжённый $\Rightarrow \exists$ ОНБ T_1, \dots, T_n из с. в.

Пусть $\lambda_1, \dots, \lambda_n$ — с. ч.

Матрица \mathcal{A} в T_1, \dots, T_n является диагональной

Матрица \mathcal{A} в T_1, \dots, T_n равна $C^{-1}AC$, где C — матрица перехода

C состоит из столбцов T_i , т. к. это матрица перехода от стандартного базиса к T_i

Значит, C — ортогональная матрица

$C^{-1}AC = C^TAC$, т. к. C ортогональна

2. Пусть $B = C^TAC$, она диагональна, μ_1, \dots, μ_n — числа на диагонали

S_1, \dots, S_n — столбцы $B \Rightarrow B = C^{-1}AC \Rightarrow B$ — матрица \mathcal{A} в ОНБ $S_1, \dots, S_n \Rightarrow \mathcal{A}S_i = \mu_i S_i \Rightarrow \mu_i$ — с. ч.

□

Теорема 25 (преобразование двух форм).

$f(x_1, \dots, x_n)$, $g(x_1, \dots, x_n)$ — вещественные квадратичные формы, f положительно определена

Тогда существует неособое преобразование, при котором **обе** формы приводятся к диагональному виду.

Доказательство. Композиция неособенных преобразований — неособенное преобразование, так что можно сделать несколько шагов:

1. Приведём f к диагональному виду f_1 :

$$f_1(y_1, \dots, y_n) = \lambda_1 y_1^2 + \dots + \lambda_n y_n^2, \quad \lambda_i > 0$$

2. Избавимся от λ :

$$z_i = \sqrt{\lambda_i} y_i$$

$$f_2(z_1, \dots, z_n) = z_1^2 + \dots + z_n^2$$

При этом, g_2 тоже как-то изменилась:

$$g_2(z_1, \dots, z_n)$$

Нужно доказать, что форму $f_2 = z_1^2 + \dots + z_n^2$ и любую форму g_2 можно одновременно привести к диагональному виду

3. Приведём g_2 к диагональному виду ортогональным преобразованием C
Матрица f_2 равна E

$$E \rightarrow C^T EC = C^T C = E$$

Значит, f приведена к диагональному виду

□

Часть III

Кольца и поля

29. Идеал кольца. Примеры колец главных идеалов. Определения простого и максимального идеала

Определение 31. A — коммутативное ассоциативное кольцо, $I \subset A$
 I называется *идеалом*, если:

1. I — подгруппа по сложению
2. $a \in I, t \in A \implies ta \in I$

Определение 32. A — ассоциативное коммутативное кольцо с единицей, $S \subset A$
Идеалом, *порождённым* S называется минимальный по включению идеал, содержащий S

Обозначение. $\langle S \rangle$

Свойство. Идеал $\langle S \rangle$ существует и единственный
Он состоит из элементов вида $t_1 s_1 + \dots + t_k s_k, \quad s_i \in S, \quad t_i \in A$

Без доказательства. □

Определение 33. Идеал, порождённый одним элементом, называется *главным*

Определение 34. Если все идеалы главные, то A называется *кольцом главных идеалов*

Теорема 26 (примеры колец главных идеалов).

1. \mathbb{Z} — кольцо главных идеалов
2. K — поле $\implies K[x]$ — кольцо главных идеалов

Доказательство.

1. I — идеал

- Если $I = \{0\}$, то $I = \langle 0 \rangle$ — главный
- Пусть $I \neq \{0\}$, a — наименьшее положительное число из I

Докажем, что $I = \langle a \rangle$:

$\langle a \rangle$ — множество чисел, делящихся на a

Допустим, что это не весь идеал, т. е. $\exists b : b \in I, \quad b \nmid a$

Поделим с остатком:

$$b = aq + r, \quad a < r < a$$

$$r = b - aq = \underbrace{b}_{\in I} + (-q) \underbrace{a}_{\in I} \in I \quad \nsubseteq$$

2. Аналогично, $I = \langle p \rangle$, где p — многочлен наименьшей степени, лежащий в I

□

Определение 35. A — коммутативное ассоциативное кольцо, I — идеал
 I называется *простым*, если

$$\forall a, b \in A \quad ab \in I \implies a \in I \quad \text{или} \quad b \in I$$

Определение 36. A — коммутативное ассоциативное кольцо, I — идеал
 I называется *максимальным*, если не существует такого идеала J , что $I \subset J, J \neq I, J \neq A$

30. Построение факторкольца. Факторкольцо по простому идеалу

Определение 37. A — коммутативное ассоциативное кольцо с единицей, I — идеал
Элементы a и b называются *сравнимыми по модулю I* , если $a - b \in I$

Обозначение. $a \equiv b \pmod{I}$ $a \equiv_I b$

Свойство. \equiv_I является отношением эквивалентности

Доказательство.

1. Рефлексивность:

$$a - a = 0 \in I$$

2. Симметричность:

$$a - b \in I \implies b - a = -(a - b) \in I$$

3. Транзитивность:

$$a - b \in I, b - c \in I \implies a - c = (a - b) + (b - c) \in I$$

□

Определение 38. A — коммутативное кольцо, I — идеал

На множестве классов эквивалентности по отношению \equiv_I введём операции сложения и умножения:

$$\bar{x} + \bar{y} = \overline{x + y}, \quad \bar{x} \cdot \bar{y} = \overline{xy}$$

Теорема 27 (факторкольцо). A — коммутативное ассоциативное кольцо, I — идеал

Тогда

1. операции сложения и умножения на классах эквивалентности определены корректно, то есть не зависят от выбора представителей
2. множество классов эквивалентности является ассоциативным коммутативным кольцом. Если в A была единица, то и в кольце классов эквивалентности будет единица

Доказательство.

1.

$$\left. \begin{array}{l} x_1, x_2 \text{ в одном классе} \\ y_1, y_2 \text{ в одном классе} \end{array} \right\} \stackrel{?}{\implies} \left\{ \begin{array}{l} x_1 + y_1 \text{ и } x_2 + y_2 \text{ в одном классе} \\ x_1 y_1 \text{ и } x_2 y_2 \text{ в одном классе} \end{array} \right.$$

Пусть $x := x_1 - x_2$, $y := y_1 - y_2 \implies x, y \in I$

$$(x_1 + y_1) - (x_2 + y_2) = x + y \in I$$

$$x_1 y_1 - x_2 y_2 = (x + x_2)(y + y_2) - x_2 y_2 = xy + y_2 x + x_2 y \in I$$

2. A/I — абелева группа (по т. о факторгруппе)

Нужно доказать, что $(\bar{x} + \bar{y})\bar{z} = \bar{xz} + \bar{yz}$

Выберем $x \in \bar{x}$, $y \in \bar{y}$, $z \in \bar{z}$

$$(\bar{x} + \bar{y})\bar{z} = \bar{xz} + \bar{yz} \iff (\overline{x + y})\bar{z} = \overline{xz + yz}$$

Остальное — аналогично

Если A — кольцо с единицей, то $\bar{1}$ — единица в A/I

□

Определение 39. Кольцо классов эквивалентности называется *факторкольцом* по идеалу I

Обозначение. A/I

Теорема 28 (факторкольцо по простому идеалу). A — коммутативное ассоциативное кольцо, I — идеал.

$$I \text{ простой} \iff A/I \text{ — область целостности}$$

Доказательство. Пусть $X \in A/I$, $x \in X$

$$\text{Тогда } X = 0 \iff \bar{x} = \bar{0} \iff x \equiv_I 0 \iff x - 0 \in I \iff x \in I$$

• \Rightarrow

$$\text{Пусть } X, Y \in A/I, \quad XY = \bar{0}$$

$$\text{Пусть } x \in X, \quad y \in Y \implies \bar{xy} = \bar{0} \implies xy \in I \xrightarrow[I \text{ простой}]{} \begin{cases} x \in I \implies X = \bar{0} \\ y \in I \implies Y = \bar{0} \end{cases}$$

• \Leftarrow

$$\text{Пусть } xy \in I \implies \bar{xy} = \bar{0} \implies \bar{x} \cdot \bar{y} = \bar{0} \xrightarrow[\text{обл. цел.}]{} \begin{cases} \bar{x} = 0 \implies x \in I \\ \bar{y} = 0 \implies y \in I \end{cases}$$

□

31. Факторкольцо по максимальному идеалу. Факторкольцо кольца многочленов над полем

Теорема 29 (факторкольцо по максимальному идеалу).

A — коммутативное ассоциативное кольцо с единицей, I — идеал

$$I \text{ максимальный} \iff A/I \text{ — поле}$$

Доказательство.

• \Rightarrow

A/I — коммутативное ассоциативное кольцо с единицей

Осталось доказать, что $\forall X \in A/I, X \neq \bar{0} \exists X^{-1}$

$$\bar{0} = I \implies X \neq I$$

Пусть $x \in X$

Пусть $J := \langle x, I \rangle$

$$J \supset I, \quad J \neq I \xrightarrow[I \text{ — макс.}]{} J = A \implies 1 \in J$$

$$1 \in \langle I, x \rangle \implies 1 = \underbrace{a_1 s_1 + \cdots + a_k s_k}_{\in I} + bx \text{ для некоторых } s_i \in I, \quad a_i, b \in A$$

$$\implies 1 \equiv_I bx \implies \bar{1} = \bar{b} \cdot \bar{x} = \bar{b}X \implies \bar{b} = X^{-1}$$

• \Leftarrow

Пусть J — идеал, $I \subset J, I \neq J$

Докажем, что $J = A$:

Пусть $x \in J \setminus I$

$$\bar{x} \in A/I, \quad \bar{x} \neq \bar{0} \implies \exists Y : \bar{x}Y = \bar{1}$$

Пусть $\bar{y} \in Y \implies \bar{x} \cdot \bar{y} = \bar{1} \implies xy - 1 \in I$

$$\left. \begin{array}{l} x \in J \\ xy - 1 \in I \end{array} \right\} \implies 1 = \underbrace{xy}_{\in J} - \underbrace{(xy - 1)}_{\in I} \in J \implies J = A$$

□

Теорема 30 (факторкольцо кольца многочленов). K — поле, $A = K[x]$, $P(x) \in A$
 $I = \langle P(x) \rangle$ (это не условие, а обозначение — известно, что все идеалы такие), $B = A/I$
 P неприводим $\iff A/I$ — поле

Доказательство. Правая часть равносильна тому, что I максимальный

• \implies

Пусть $I \subset J$, $Q(x)$ — такой, что $J = \langle Q(x) \rangle$

$$\begin{aligned} \langle P(x) \rangle \subset \langle Q(x) \rangle &\implies P(x) : Q(x) \xrightarrow[P \text{ неприводим}]{} \\ &\implies \begin{cases} Q(x) = cP(x), & c \in K, \quad c \neq 0 \implies J = I \\ Q(x) = c, & c \in K, \quad c \neq 0 \implies J = A \end{cases} \implies I \text{ максимальный} \end{aligned}$$

• \Leftarrow

Пусть P приводим

$$\begin{aligned} &\implies \exists Q(x) : P(x) : Q(x), \quad Q(x) \neq cP(x), \quad Q(x) \neq c \\ &\implies \langle P(x) \rangle \subsetneq \langle Q(x) \rangle \subsetneq A \implies I \text{ не максимальный} \end{aligned}$$

□

32. Гомоморфизм колец. Теорема о гомоморфизме

Определение 40. $(A, +_A, \cdot_A)$, $(B, +_B, \cdot_B)$ — кольца
Отображение $f : A \rightarrow B$ называется *гомоморфизмом*, если

$$\begin{aligned} f(x +_A y) &= f(x) +_B f(y) \\ f(x \cdot_A y) &= f(x) \cdot_B f(y) \end{aligned}$$

Определение 41. Отображение $f : A \rightarrow B$ называется *изоморфизмом*, если f — гомоморфизм и биекция.

Определение 42. Если существует изоморфизм из A в B , то A и B называются *изоморфными*.

Обозначение. $A \simeq B$

Определение 43. A, B — кольцо, $f : A \rightarrow B$ — гомоморфизм
Ядро: $\{x \in A \mid f(x) = 0\}$, образ: $\{f(x) \mid x \in A\}$.

Обозначение. $\ker f$, $\operatorname{Im} f$.

Свойства. A, B — коммутативные, $f : A \rightarrow B$ — гомоморфизм

1. $f(0) = 0$
2. $\ker f$ — идеал
3. $\operatorname{Im} f$ — подкольцо B

Доказательство.

1. Следует из аналогичного свойства для гомоморфизма групп
2. $\ker f \neq \emptyset$, т. к. $0_A \in \ker f$

- $x, y \in \ker f \implies f(x+y) = \underbrace{f(x)}_0 + \underbrace{f(y)}_0 = 0 + 0 = 0$

- $\underbrace{f(0)}_0 = f(x+(-x)) = \underbrace{f(x)}_0 + f(-x) \implies f(-x) = 0$

- $a \in A \quad f(ax) = f(a)f(x) = f(a) \cdot 0 = 0$

3. $\text{Im } f \subset B$

Нужно проверить, что $\text{Im } f$ замкнут относительно операции

Для сложения — можно сослаться на группы

Для умножения:

$$\begin{aligned} x, y \in \text{Im } f &\implies a, b \in A : f(a) = x, f(b) = y \\ &\implies xy = f(a)f(b) = f(ab) \in \text{Im } f \end{aligned}$$

□

Теорема 31 (о гомоморфизме колец). A, B — коммутативные ассоциативные кольца
 $f : A \rightarrow B$ — гомоморфизм

$$A/\ker f \simeq \text{Im } f$$

Доказательство. Определим $\varphi : A/\ker f \rightarrow \text{Im } f : \varphi(X) = f(x)$ для некоторого $x \in X$.

• Корректность:

Пусть $x, x' \in X$

Проверим, что $f(x') = f(x)$

$$\bar{x} = \bar{x'} \implies x \underset{\ker f}{\equiv} x' \implies x - x' \in \ker f \implies f(x) = f(x' + (x - x')) = f(x') + \underbrace{f(x - x')}_{0 \ (x - x' \in \ker f)}$$

• Гомоморфизм:

$$X, Y \in A/\ker f, \quad x \in X, \quad y \in Y$$

$$X = \bar{x}, \quad Y = \bar{y}, \quad X + Y = \overline{x+y}, \quad XY = \overline{xy}$$

$$\varphi(X+Y) = \varphi(\overline{x+y}) = f(x+y) \xrightarrow[f \text{ гомоморф.}]{} f(x) + f(y) = \varphi(\bar{x}) + \varphi(\bar{y}) = \varphi(\bar{x+y})$$

Для умножения — то же самое

• Сюръективность:

Пусть $b \in \text{Im } f \implies \exists x \in A : f(x) = b \implies \varphi(\bar{x}) = b$

• Инъективность:

Пусть $\varphi(X) = \varphi(Y), \quad x \in X, \quad y \in Y$

$$\implies f(x) = f(y) \implies f(x-y) = 0 \implies x-y \in \ker f \implies \bar{x} \underset{\ker f}{\equiv} y \implies \bar{x} = \bar{y} \implies X = Y$$

□

33. Характеристика кольца и поля. Классификация простых полей

Определение 44. A — кольцо

Характеристикой A называется наименьшее $n \in \mathbb{N}$ такое, что

$$\underbrace{a+a+\cdots+a}_n = 0 \quad \forall a \in A$$

Если такого n не существует, то характеристика равна нулю

Обозначение. $\text{char } A$

Свойство. Если A кольцо с единицей, то $\text{char } A$ — наименьшее $n \in \mathbb{N}$ такое, что

$$\underbrace{1 + 1 + \cdots + 1}_n = 0$$

Доказательство. Нужно доказать, что

$$\underbrace{a + a + \cdots + a}_n = 0 \quad \forall a \in A \quad \iff \quad \underbrace{1 + 1 + \cdots + 1}_n = 0$$

• \Rightarrow

Подставим $a = 1$

• \Leftarrow

$$a + a + \cdots + a = a(1 + \cdots + 1) = a \cdot 0 = 0$$

□

Свойство. A — поле

Тогда $\text{char } A = 0$ или $\text{char } A \in \mathbb{P}$

Доказательство. Пусть это не так и $\text{char } A$ — составное

$$\text{char } A = n = mk, \quad 1 < m, \quad k < n$$

$$0 = \underbrace{1 + \cdots + 1}_n = (\underbrace{1 + \cdots + 1}_m)(\underbrace{1 + \cdots + 1}_k) \implies \begin{cases} \underbrace{1 + \cdots + 1}_m = 0 \\ \underbrace{1 + \cdots + 1}_k = 0 \end{cases}$$

Получили противоречие с минимальностью n

□

Определение 45. L — поле, $K \subset L$, K является полем с теми же операциями
Тогда K называется подполем L , L называется расширением K .

Определение 46. Поле K называется простым, если оно не содержит подполей, отличных от K

Теорема 32 (классификация простых полей).

1. Поля \mathbb{Q} и \mathbb{Z}_p при $p \in \mathbb{P}$ — простые
2. Любое простое поле изоморфно \mathbb{Q} или \mathbb{Z}_p для некоторого $p \in \mathbb{P}$

Доказательство.

1. • \mathbb{Q}

Пусть \mathbb{Q} не простое, и K — подполе \mathbb{Q} $\implies 0, 1 \in K$

$$\underbrace{1 + 1 + \cdots + 1}_n \in K \quad \forall n \quad \implies \mathbb{N} \subset K$$

Если $n \in K$, то $-n \in K \implies \mathbb{Z} \subset K$

Если $n \in K$, $n \neq 0$, то $\frac{1}{n} \in K \implies \frac{1}{n} \in K \quad \forall n \in \mathbb{N}$

$$m \in \mathbb{Z}, n \in \mathbb{N} \implies \frac{m}{n} = m \cdot \frac{1}{n} \in K \implies \mathbb{Q} = K$$

• \mathbb{Z}_p

Аналогично, пусть K — подполе \mathbb{Z}_p

$$\bar{1} \in K$$

$$\underbrace{\bar{1} + \bar{1} + \cdots + \bar{1}}_n \in K \quad \forall n \quad \implies \bar{n} \in K \quad \forall n \quad \implies \mathbb{Z}_p = K$$

2. Пусть K — поле

Докажем, что K содержит подполе, изоморфное \mathbb{Q} или \mathbb{Z}_p

Возьмём A — минимальное подкольцо K , содержащее 1

Докажем, что $A \simeq \mathbb{Z}$ (взяв все частные из A , получим множество дробей) или $A \simeq \mathbb{Z}_p$:

Пусть $f : \mathbb{Z} \rightarrow A$ такое, что

$$f(n) := \begin{cases} \underbrace{1 + 1 + \cdots + 1}_{n}, & n > 0 \\ -(\underbrace{1 + 1 + \cdots + 1}_{n}), & n < 0 \\ 0, & n = 0 \end{cases}$$

Докажем, что f — гомоморфизм:

- Докажем, что $f(n) + f(k) = f(n + k)$:

Кольцо — это группа по сложению. Умножение n единиц — это возведение в n степень. Знам, что $1^n * 1^k = 1^{n+k}$, где $*$ — это $+$

- $f(nk) = f(n) \cdot f(k)$:

— $n, k > 0$

$$\underbrace{(1 + \cdots + 1)}_n \underbrace{(1 + \cdots + 1)}_k = \underbrace{1 \cdot 1 + \cdots + 1 \cdot 1}_{nk} = \underbrace{1 + \cdots + 1}_{nk}$$

— $n = 0$

$$f(0) = f(0)f(k)$$

— $n > 0, k < 0$

Положим $k_1 := -k$

$$f\left(n(-k_1)\right) = f(n)f(-k_1) \iff -f(nk_1) = f(n)\left(-f(k_1)\right)$$

По теореме о гомоморфизме $\text{Im } f \simeq \mathbb{Z}/\ker f$

$\text{Im } f$ — подкольцо $A \implies \text{Im } f = A$ (из минимальности A)

$\ker f$ — идеал $\implies \ker f = \langle m \rangle$

- $m = 0$

$$\ker f = \{0\} \implies \mathbb{Z}/\ker f = \mathbb{Z}/\{0\} \simeq \mathbb{Z}$$

- $m \neq 0$

$$\text{Im } f \simeq \mathbb{Z}/\langle m \rangle \simeq \mathbb{Z}_m$$

$\text{Im } f$ — подкольцо поля $K \implies \text{Im } f$ — область целостности

$\implies \langle m \rangle$ — простой идеал $\implies m \in \mathbb{P}$

□

34. Степень расширения. Мультипликативность степени, следствия

Лемма 11 (корректность). K — поле, L — расширение K

Тогда L является векторным пространством над K

Доказательство.

- Операции:

— $l_1 + l_2, l_1, l_2 \in L$

— $kl, k \in K, l \in L$

k, l — элементы L , для них операции определены

- L — абелева группа по сложению:

$$(k_1 k_2)l = k_1(k_2 l)$$

□

Определение 47. L — расширение K

Степенью расширения L над K называется $\dim_K L$

Обозначение. $|L : K|$, $(L : K)$, $[L : K]$

Теорема 33 (мультипликативность степени). $K \subset M \subset L$ — поля с общими операциями

Тогда $|L : K| = |L : M| \cdot |M : K|$

Доказательство.

- Докажем, что если $e_1, \dots, e_r \in M$ ЛНЗ над K и $f_1, \dots, f_s \in L$ ЛНЗ над M , то $g_{ij} := e_i f_j$ ЛНЗ над K :

Пусть $a_{ij} \in K : \sum a_{ij} g_{ji} = 0$

$$a_{11}e_1f_1 + a_{12}e_1f_2 + \dots + a_{21}e_2f_1 + a_{22}e_2f_2 + \dots = 0$$

Сгруппируем по элементам f :

$$\left(a_{11}e_1f_1 + a_{21}e_2f_1 + \dots \right) + \left(a_{12}e_1f_2 + a_{22}e_2f_2 + \dots \right) + \dots = 0$$

$$\underbrace{(a_{11}e_1 + a_{21}e_2 + \dots)}_{\in M} f_1 + \underbrace{(a_{12}e_1 + a_{22}e_2 + \dots)}_{\in M} f_2 + \dots = 0$$

Пусть $b_j := a_{1j}e_1 + a_{2j}e_2 + \dots + a_{rj}e_r$

Тогда $b_j \in M$, $b_1f_1 + \dots + b_sf_s = 0$

f_1, \dots, f_s ЛНЗ над $M \implies b_1 = b_2 = \dots = b_s = 0$

$$a_{1j}e_1 + \dots + a_{rj}e_r = b_j = 0$$

e_1, \dots, e_r ЛНЗ над $K \implies a_{ij} = 0 \quad \forall i, j$

- Конечный случай

Пусть e_1, \dots, e_r — базис M над K , f_1, \dots, f_s — базис L над M

Докажем, что $g_{ij} := e_i f_j$ — базис L над K :

ЛНЗ уже доказана. Осталось доказать, что любой элемент порождается g_{ij} :

Пусть $c \in L \implies \exists b_i \in M : c = b_1f_1 + \dots + b_sf_s$

$$b_j \in M, \quad e_i \text{ порожд. } M \text{ над } K \implies \forall j \quad \exists a_{ij} : \quad b_j = a_{1j}e_1 + \dots + a_{rj}e_r$$

$$\implies c = \sum a_{ij}e_i f_j = \sum a_{ij}g_{ij}$$

- Бесконечный случай

Нужно доказать, что $\forall N \quad \exists N$ линейных элементов L над K (т. е. существует сколь угодно большая ЛНЗ система)

Можно выбрать e_1, \dots, e_N ЛНЗ, или f_1, \dots, f_N ЛНЗ

Тогда $e_i f_j$ ЛНЗ над K

□

Следствие. L — конечное расширение над K , $K \subset M \subset L$

Тогда $|M : K|$ и $|L : M|$ — делители $|L : K|$

Следствие. L — конечное расширение K , $|L : K|$ — простое число

$$\implies \nexists M : \quad K \subset M \subset L, \quad M \neq K, \quad M \neq L$$

Следствие. $K \subset M \subset L$

- если $|M : K| = |L : K|$, то $M = L$
- если $|L : M| = |L : K|$, то $M = K$

Следствие. $K \subset M \subset L$, L бесконечно над K

Тогда M бесконечно над K или L бесконечно над M

35. Минимальный многочлен алгебраического элемента. Алгебраичность конечного расширения

Определение 48. L — расширение K , $\alpha \in L$

α называется *алгебраическим* над K , если $\exists P(x) \in K[x]$ такой, что $P(\alpha) = 0$, $P(x)$ — не нулевой.
Если такого $P(x)$ не существует, то α называется *трансцендентным*.

Определение 49. α — алгебраическое над K , $P(x) \in K[x]$, $P(\alpha) = 0$.

Тогда говорят, что $P(x)$ *аннулирует* α .

Минимальным многочленом α над K называется ненулевой аннулирующий многочлен наименьшей степени со старшим коэффициентом, равным 1

Определение 50. *Алгебраическим числом* называется комплексное число, алгебраическое над \mathbb{Q}

Свойства (минимального многочлена). K — поле, L — расширение K , $\alpha \in L$, α алг. над K

1. $P(x)$ — минимальный для α .
$$F(\alpha) = 0 \iff F(x) : P(x)$$
2. Минимальный многочлен для α единственен
3. Минимальный многочлен неприводим над K
4. $P(x)$ неприводим над K , $P(x) \neq 0$, $P(\alpha) = 0$

$$\implies P(x) — \text{минимальный для } \alpha$$

Доказательство.

1.

$$F(x) = P(x)Q(x) + R(x), \quad \deg R < \deg P$$

• \Leftarrow

$$F(x) : P(x) \implies R(x) = 0$$

$$F(x) = P(x)Q(x)$$

Подставим α :

$$F(\alpha) = \underbrace{P(\alpha)}_0 Q(\alpha) = 0$$

• \Rightarrow

$$\underbrace{P(\alpha)}_0 Q(\alpha) + R(\alpha) = 0$$

$$R(\alpha) = 0 \implies R — \text{нулевой}$$

2. Пусть P_1, P_2 — минимальные

$$\xrightarrow[\text{св-во 1}]{\quad} \begin{cases} P_1(x) : P_2(x) \\ P_2(x) : P_1(x) \end{cases} \implies P_1(x) = P_2(x)$$

3. Пусть $P(x) = S(x)T(x)$, $0 < \deg S, \deg T < \deg P$

$$0 = P(\alpha) = \underbrace{S(\alpha)}_{\in L} \underbrace{T(\alpha)}_{\in L} \xrightarrow{L-\text{поле}} \begin{cases} S(\alpha) = 0 \\ T(\alpha) = 0 \end{cases} \not\leq \text{миним. } \deg P$$

4.

$$\left. \begin{array}{l} P(x) : \text{миним.} \\ P(x) - \text{непривод.} \end{array} \right\} \implies P(x) - \text{миним.}$$

□

Определение 51. Расширение L над K называется *алгебраическим*, если любой элемент L является алгебраическим над K .

Иначе — *трансцендентным*.

Теорема 34. Конечное расширение полей является алгебраическим

Доказательство. Пусть L — конечное расширение K , $n := |L : K|$, $\alpha \in L$.

Докажем, что α — алгебраическое:

Элементы $\underbrace{1, \alpha, \dots, \alpha^{n-1}, \alpha^n}_{n+1} \in L$ ЛЗ над K , т. е.

$$\exists k_0, k_1, \dots, k_{n-1}, k_n \in K \notin \bigcirc : k_0 \cdot 1 + k_1 \alpha + \dots + k_{n-1} \alpha^{n-1} + k_n \alpha^n = 0$$

Пусть $P(x) = k_0 + k_1 x + \dots + k_{n-1} x^{n-1} + k_n x^n$.

Тогда $P(x) \in K[x]$, $P(x)$ — ненулевой, $P(\alpha) = 0 \implies \alpha$ — алгебраическое.

□

36. Строение простого алгебраического расширения. Следствия

Определение 52. L — поле, K — подполе L , $\alpha_1, \dots, \alpha_n \in L$

Через $K(\alpha_1, \dots, \alpha_n)$ будем обозначать наименьшее подполе L , содержащее K и $\alpha_1, \dots, \alpha_n$.

Если $M = K(\alpha_1, \dots, \alpha_n)$, то говорят, что M получено из K присоединением $\alpha_1, \dots, \alpha_n$.

Поле, полученное из K присоединением одного элемента, называется *простым расширением* K .

Теорема 35 (строение простого алгебраического расширения). L — поле, K — подполе L

$\alpha \in L$, α алг. над K , $P(x)$ — минимальный многочлен для α над K

1. $K[x]/\langle P(x) \rangle \cong K(\alpha)$, $\overline{F(x)} \mapsto F(\alpha)$ является изоморфизмом.

2. $K(\alpha)$ конечно над K , $|K(\alpha) : K| = \deg P$, $1, \alpha, \dots, \alpha^{n-1}$ образуют базис $K(\alpha)$ над K .

Доказательство. Определим $f : K[x] \rightarrow K(\alpha)$ как $f(F) := F(\alpha)$ ($x \mapsto \alpha$), т. е.

$$f(c_0 + c_1 x + \dots + c_k x^k) = c_0 + c_1 \alpha + \dots + c_k \alpha^k, \quad c_i \in K$$

- Проверим, что f — гомоморфизм:

$$f(F + G) = (F + G)(\alpha) = F(\alpha) + G(\alpha) = f(F) + f(G)$$

$$f(FG) = (FG)(\alpha) = F(\alpha)G(\alpha) = f(F)f(G)$$

- Найдём $\ker f$:

$$\begin{aligned} F(x) \in \ker f &\iff f(F) = 0 \iff F(\alpha) = 0 \iff F(x) : P(x) \\ &\implies \ker f = \langle P(x) \rangle \end{aligned}$$

- Применим теорему о гомоморфизме:

$$\text{Im } f \simeq K[x] / \ker f$$

Изоморфизм $\varphi(\bar{F}) = f(F) = F(\alpha)$

Получили изоморфизм $K[x] / \langle P(x) \rangle \rightarrow \text{Im } f$

- Проверим, что $\text{Im } f \stackrel{?}{=} K(\alpha)$:

$K(\alpha)$ — минимальное, содержащее K и α .

$\text{Im } f$ тоже содержит K и α .

Значит, $\text{Im } f = K(\alpha)$.

- Проверим, что $1, \alpha, \dots, \alpha^{\deg P-1}$ — базис:

Пусть $n := \deg P$

— ЛНЗ:

Пусть ЛЗ:

$$a_0 \cdot 1 + a_1 \alpha + \dots + a_{n-1} \alpha^{n-1} = 0, \quad a_i \in K$$

$$\text{Пусть } F(x) := a_0 + a_1 x + \dots + a_{n-1} x^{n-1} \implies F(\alpha) = 0$$

$$\implies F(x) : P(x) \xrightarrow[F(x) \text{ — ненулевой}]{} \deg F \geq \deg P = n \quad \checkmark$$

— Порождающий:

$$K(\alpha) = \text{Im } f$$

$$\text{Пусть } u \in K(\alpha) \implies \exists F \in K[x] : \quad f(F) = u \implies F(\alpha) = u$$

Делим с остатком:

$$F(x) = Q(x)P(x) + R(x), \quad \deg R < \deg P$$

$$\implies \deg R \leq n + 1$$

$$F(\alpha) = Q(\alpha) \underbrace{P(\alpha)}_0 + R(\alpha) = R(\alpha)$$

$$R(x) = a_0 + a_1 x + \dots + a_{n-1} x^{n-1} \implies R(\alpha) = a_0 + a_1 \alpha + \dots + a_{n-1} \alpha^{n-1}$$

□

Следствие. α — алгебраический над K , $F, G \in K[x]$, $G(\alpha) \neq 0$, $\beta = \frac{F(\alpha)}{G(\alpha)}$
Тогда β — алгебраический над K

Доказательство. Существует поле $K(\beta)$.

При этом $\beta \in K(\alpha)$.

$$K \subset K(\beta) \subset K(\alpha)$$

Применим одно из следствий из теоремы о мультипликативности расширения:

$K(\alpha)$ над K конечно $\implies K(\beta)$ над K конечно

\implies все элементы $K(\beta)$ алгебраичны над K

□

Следствие. $\alpha_1, \dots, \alpha_n$ алгебраичны над K

Тогда $K(\alpha_1, \dots, \alpha_n)$ конечно над K

Доказательство. Обозначим $K_0 := K$, $K_i := K(\alpha_1, \dots, \alpha_i)$.

$$K \subset K_1 \subset K_2 \subset \dots \subset K_n$$

Достаточно доказать, что K_{i+1} конечно над K_i :

Пусть $P(x)$ — ненулевой многочлен, аннулирующий α_{i+1} над K_i .

Выполнено $K_i[x] \subset K[x]$, следовательно, $P(x) \in K_i[x]$.

Получаем, что $P(x)$ аннулирует α_{i+1} над K_i , и α_{i+1} алгебраичен над K_i .

Расширение, полученное присоединением одного алгебраического элемента, конечно.

□

Следствие. α, β алгебраичны над K
 $\Rightarrow \alpha + \beta, \alpha - \beta, \alpha\beta, \alpha/\beta$ алгебраичны над K

Доказательство. Все эти элементы принадлежат конечному расширению $K(\alpha, \beta)$ над K , следовательно, они являются алгебраическими. \square

37. Существование простого расширения. Эквивалентные расширения

Теорема 36 (существование простого расширения). K — поле, $P(x) \in K[x]$ — неприводимый. Тогда существует расширение L поля K такое, что $P(x)$ имеет в L корень α и $L = K(\alpha)$.

Доказательство. Рассмотрим множество формальных сумм вида

$$a_0 + a_1X + a_2X^2 + \cdots + a_nX^n, \quad a_i \in K$$

Введём отношение эквивалентности:

Если

$$s = a_0 + a_1X + \dots, \quad t = b_0 + b_1X + \dots$$

$$S(x) := a_0 + a_1x + \dots, \quad T(x) := b_0 + b_1x + \dots$$

и $S(x) - T(x) : P(x)$, то $s \sim t$.

Определим на множестве классов эквивалентности сложение и умножение:

Если

$$s = a_0 + a_1X + \dots, \quad t = b_0 + b_1X + \dots, \quad u = c_0 + c_1X + \dots$$

$$S(x) = a_0 + a_1x + \dots, \quad T(x) = b_0 + b_1x + \dots, \quad U(x) = c_0 + c_1x + \dots$$

и $S(x)T(x) - U(x) : P(x)$, то положим $u := st$.

Сложение — аналогично.

Получается поле, изоморфное $K[x]/\langle P(x) \rangle$

Изоморфизм: $\overline{a_0 + a_1X + \dots} \mapsto \overline{a_0 + a_1x + \dots}$

\overline{X} подойдёт в качестве α (т. к. $P(x) \mapsto \overline{P(x)} = 0$). \square

Определение 53. Расширения L_1, L_2 поля K называются **эквивалентными** (относительно K), если $L_1 \simeq L_2$ и существует изоморфизм $f : L_1 \rightarrow L_2$ такой, что $f|_K = \text{id}$.

Теорема 37 (эквивалентные простые расширения). α, β — алгебраические над K , их минимальные многочлены совпадают.

Тогда $K(\alpha)$ и $K(\beta)$ эквивалентны, причём существует изоморфизм $f : K(\alpha) \rightarrow K(\beta)$ такой, что

$$f|_K = \text{id}, \quad f(\alpha) = \beta$$

Доказательство. Пусть $P(x)$ — минимальный многочлен для α и β , $n := \deg P$.

Элементы $K(\alpha)$ — это $u_0 + u_1\alpha + \cdots + u_{n-1}\alpha^{n-1}$.

Положим

$$f(u_0 + u_1\alpha + \cdots + u_{n-1}\alpha^{n-1}) := u_0 + u_1\beta + \cdots + u_{n-1}\beta^{n-1}$$

Пусть

$$s = u_0 + u_1\alpha + \dots, \quad t = v_0 + v_1\alpha + \dots$$

$$S(x) = u_0 + u_1x + \dots, \quad T(x) = v_0 + v_1x + \dots$$

Пусть $R(x) = w_0 + w_1x + \cdots + w_{n-1}x^{n-1}$ — такой, что $S(x)T(x) - R(x) : P(x)$

$$r = w_0 + w_1\alpha + \cdots + w_{n-1}\alpha^{n-1}$$

Тогда $s = S(\alpha)$, $t = T(\alpha)$, $r = R(\alpha)$

$$f(s) = S(\beta), \quad f(t) = T(\beta), \quad f(r) = R(\beta)$$

$$st = S(\alpha)T(\alpha) \underset{ST=R:P}{=} R(\alpha) = r^2$$

$$f(ST) = f(r) = R(\beta)$$

$$f(s)f(t) = S(\beta)T(\beta) = R(\beta)$$

Сложение — аналогично.

Биективность:

- Инъективность:

$$u_0 + u_1\alpha + \dots \rightarrow 0$$

$$u_0 + u_1\beta + \dots = 0$$

$$\implies u_i = 0$$

- Сюръективность:

Любой элемент $K(\beta)$ — это $u_0 + u_1\beta + \dots$

□

38. Поле разложения многочлена: существование, эквивалентность

Определение 54. K — поле, $P(x) \in K[x]$.

Полем разложения $P(x)$ называется такое расширение L поля K , что в L многочлен $P(x)$ раскладывается на линейные множители

$$P(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n), \quad a \in K, \quad \alpha_i \in L$$

и $L = K(\alpha_1, \dots, \alpha_n)$.

Теорема 38 (существование поля разложения). K — поле, $P(x) \in K[x]$.

1. существует поле разложения;
2. любое поле разложения является конечным расширением K .

Доказательство. Будем считать, что старший коэффициент P равен 1.

Индукцией по n (не фиксируя K) докажем, что для любого n выполнено утверждение:

Для любого K , для любого многочлена степени не выше n существует поле M , в котором $P(x)$ раскладывается на линейные множители

- **База.** $n = 1$

$P(x)$ — линейный, есть корень в K , $M = K$

- **Переход к n :**

Разложим $P(x)$ на неприводимые над K :

$$P(x) = P_1(x) \cdots P_k(x)$$

Присоединим корень α многочлена $P_1(x)$, получим $K(\alpha)$.

$K(\alpha)$ — поле, в нём верна теорема Безу:

$$P_1(x) : x - \alpha \text{ в } K(\alpha)[x]$$

$$P_1(x) = (x - \alpha)Q(x)$$

$$P(x) = (x - \alpha) \underbrace{Q(x)P_2(x) \cdots P_k(x)}_{H(x)} = (x - \alpha)H(x)$$

Применим **предположение индукции** к $K(\alpha)$ и $H(x)$:

Существует M , в котором $H(x)$ раскладывается на линейные множители, $K(\alpha) \subset M$.

Это M подходит для K и $P(x)$.

Поле разложения — минимальное подполе M , содержащее K и $\alpha_1, \dots, \alpha_n$, т. е. $L = K(\alpha_1, \dots, \alpha_n)$.

□

Теорема 39 (эквивалентность полей разложения многочлена). K — поле, $P \in K[x]$
 L, M — поля разложения.

1. L и M эквивалентны над K ;
2. можно выбрать такие $\alpha_i \in L$, $\beta_i \in M$ такие, что

$$P(x) = \prod_{\alpha \in K} (x - \alpha_1) \cdots (x - \alpha_n), \quad P(x) = \prod_{\beta \in K} (x - \beta_1) \cdots (x - \beta_n)$$

для которых существует изоморфизм $f : L \rightarrow M$, $f(\alpha_i) = \beta_i$, $f|_K = \text{id}$

Доказательство. Строим последовательно $\alpha_1, \dots, \alpha_s$, β_1, \dots, β_s .

$$f_s : K(\alpha_1, \dots, \alpha_s) \rightarrow K(\beta_1, \dots, \beta_s) : f(\alpha_i) = \beta_i$$

Пусть построены $\alpha_1, \dots, \alpha_s$, β_1, \dots, β_s , f_s .

Положим $L' = K(\alpha_1, \dots, \alpha_s)$, $M' = K(\beta_1, \dots, \beta_s)$
(на первом шаге считаем, что $L' = M' = K$, $f_0 = \text{id}$)

Разложение $P(x)$ на неприводимые над L'

$$P(x) = (x - \alpha_1) \cdots (x - \alpha_s) Q_1(x) Q_2(x) \cdots$$

$$f_s = L' \rightarrow M'$$

$$P(x) = f_s(P(x)) = (x - \beta_1) \cdots (x - \beta_s) R_1(x) R_2(x) \cdots, \quad R_i(x) = f_s(Q_i(x))$$

$R_i(x)$ неприводимы

- Если $Q_i(x)$ — линейный, обозначим его корень α_{s+1} , $\beta_{s+1} := f(\alpha_{s+1})$

$$f_s(Q_i(x)) = (x - \beta_{s+1})$$

$$f_{s+1} := f_s$$

- Если нет линейных, то положим α_{s+1} — корень $Q_1(x)$, β_{s+1} — корень $R_1(x)$

$$L'(\alpha_{s+1}) \simeq L'(x) / \langle Q_1(x) \rangle \simeq M'(x) / \langle R_1(x) \rangle \simeq M'(\beta_{s+1})$$

Отображение

$$\varphi : L'[x] / \langle Q_1(x) \rangle \rightarrow M'[x] / \langle R_1(x) \rangle : \varphi(\overline{H}(x)) = \overline{f_{s+1}(H(x))}$$

является изоморфизмом. Существуют изоморфизмы

$$\varphi_1 : L'[x] / \langle Q_1(x) \rangle \rightarrow L'(\alpha_{s+1}) : \varphi_1(\overline{x}) = \alpha_{s+1}$$

$$\varphi_2 : M'[x] / \langle R_1(x) \rangle \rightarrow M'(\beta_{s+1}) : \varphi_2(\overline{x}) = \beta_{s+1}$$

Отображение $\varphi_1^{-1} \circ \varphi \circ \varphi_2$ подойдёт в качестве f_{s+1} .

□

39. Свойства корней из единицы. Существование примитивного корня

Определение 55. K — поле, $\varepsilon \in K$, $n \in \mathbb{N}$

ε называется корнем n -й степени из единицы, если $\varepsilon^n = 1$.

ε — примитивный корень степени n , если $\varepsilon^n = 1$, $\varepsilon^k \neq 1$ при $1 \leq k < n$

Свойства.

1. Корни n -й степени из 1 образуют абелеву группу по умножению
2. $\text{char } K = p \in \mathbb{P} \neq 0$, $n = p^m h$, $h \nmid p$, ε — корень n -й степени из 1.
Тогда ε — корень h -й степени из 1.

Доказательство.

1. Пусть U — множество корней n -й степени.

$$\begin{aligned}\bullet \quad & \varepsilon_1, \varepsilon_2 \in U \implies (\varepsilon_1 \varepsilon_2)^n = \varepsilon_1^n \varepsilon_2^n = 1 \cdot 1 = 1 \implies \varepsilon_1 \varepsilon_2 \in U \\ \bullet \quad & \varepsilon \in U \implies \left(\frac{1}{\varepsilon}\right)^n = \frac{1^n}{\varepsilon^n} = \frac{1}{1} = 1 \implies \varepsilon^{-1} \in U\end{aligned}$$

2. Докажем, что если $\varepsilon^{ps} = 1$, то $\varepsilon^s = 1$:

$$C_p^i = \frac{p!}{(p-i)! \cdot i!} \quad : p \text{ при } 1 \leq i \leq p-1 \text{ в } \mathbb{Z}$$

(т. к. $p! : p$, $(p-i)! \cdot i! \nmid p$)

$$\text{char } K = p \implies C_p^i = 0 \text{ при } 1 \leq i \leq p$$

$$(\varepsilon^s - 1)^p = (\varepsilon^s)^p + 0 \cdot (\varepsilon^s)^{p-1} \cdot (-1) + \cdots + 0 \cdot \varepsilon^s \cdot (-1)^{p-1} + (-1)^p = \varepsilon^{sp} - 1 = 1 - 1 = 0 \xrightarrow{\text{обл. цел.}} \varepsilon^s = 1$$

□

Теорема 40 (существование примитивного корня). K — поле, $h \in \mathbb{N}$

$x^h - 1$ раскладывается в K на линейные множители, $h \nmid \text{char } K$

1. в K есть h различных корней n -й степени из единицы;
2. существует примитивный корень h -й степени из единицы;
3. группа корней h -й степени является циклической и порождается любым примитивным корнем.

Доказательство.

1. $P(x) = x^h - 1$ имеет h корней с учётом кратности
 $P'(x) = hx^{h-1}$: единственный корень — 0 — не является корнем $p(x)$

2. U — группа корней h -й степени из единицы, $|U| = h$

Нужно доказать, что $\exists \varepsilon \in U : \text{ord } \varepsilon = h$

Пусть $h = p_1^{a_1} \cdots p_k^{a_k}$, $p_i \in \mathbb{P}$

Докажем, что $\exists x_1, \dots, x_k \in U : \text{ord}(x_i) = p_i^{a_i}$:

Докажем для $i = 1$ (остальное — аналогично):

$$x_1 : \text{ord } x_1 \stackrel{?}{=} p_1^{a_1}$$

Докажем, что $\exists y : \text{ord } y : p_1^{a_1}$:

Пусть $\forall y \in U \quad \text{ord } y \nmid p_1^{a_1}$

$$\left. \begin{aligned} & p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} : \text{ord } y \\ & \text{ord } y \nmid p_1^{a_1} \end{aligned} \right\} \implies \underbrace{p_1^{a_1-1} p_2^{a_2} \cdots p_k^{a_k}}_{h'} : \text{ord } y$$

$$h' : \text{ord } y \implies y^{h'} = 1 \quad \forall y \in U$$

y — корень квадратичного многочлена $x^{h'} - 1 \quad \forall y \in U$

У него $h > h'$ корней — $\frac{h}{h'}$

$$\text{ord } y = p_1^{a_1} \cdot t \implies \text{ord}(y^t) = p_1^{a_1}$$

Подойдёт $x_1 = y^t$. Аналогично x_i

Докажем, что для $\varepsilon = x_1 x_2 \dots x_k$ выполнено $\text{ord } \varepsilon = h$:

Положим $b_i := p_1^{a_1} \dots p_i^{a_i-1} \dots p_k^{a_k}$

$x_i^{b_i} \neq 1$ т. к. $b_i \not\geq \text{ord } x_i$

$$x_i^{b_i} - 1, \quad j \neq i$$

$x_j^{b_i} = 1$ при $i \neq j$

$$\varepsilon^{b_i} = \underbrace{x_1^{b_i}}_1 \dots \underbrace{x_i^{b_i}}_{\neq 1} \dots \underbrace{x_k^{b_i}}_1 \neq 1$$

$$h : \text{ord } \varepsilon, \quad b_i \not\geq \varepsilon \quad \forall i \implies \text{ord } \varepsilon = h$$

3. ε — примитивный

$1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{h-1}$ различны $\implies 1, \varepsilon, \dots, \varepsilon^{h-1}$ — все элементы U ($\varepsilon^i = \varepsilon^j \implies \varepsilon^{i-j} = 1$)

□

40. Количество примитивных корней. Многочлен деления круга

Лемма 12 (количество примитивных корней). K — поле, $h \in \mathbb{N}, h \not\geq \text{char } K$

$x^h - 1$ раскладывается на линейные множители

Тогда в K есть $\varphi(h)$ примитивных корней из единицы.

Доказательство. ε — примитивный корень

Все корни: $\varepsilon^0 = 1, \varepsilon^1 = \varepsilon, \varepsilon^2, \dots, \varepsilon^{n-1}$

Докажем, что ε^s примитивный $\iff \text{НОД}(s, h) = 1$:

- Пусть $\text{НОД}(s, h) = 1, (\varepsilon^s)^k = 1 \implies \varepsilon^{sk} = 1 \implies sk : h \implies k : h$

$$\text{ord } \varepsilon^s = h$$

- Пусть $\text{НОД}(s, h) = d \neq 1$

$$(\varepsilon^s)^{\frac{h}{d}} = \varepsilon^{\frac{sh}{d}} = (\varepsilon^h)^{\frac{s}{d}} = 1 \implies \text{ord } \varepsilon^s = \frac{h}{d} \implies \varepsilon^s \text{ не примитивный}$$

□

Определение 56. K — поле, $h \in \mathbb{N}, h \not\geq \text{char } K, x^h - 1$ раскладывается на лин. множит.

$\varepsilon_1, \dots, \varepsilon_{\varphi(h)}$ — все примитивные корни степени h

Многочлен деления круга (круговой многочлен) — это

$$\Phi_h(x) = (x - \varepsilon_1)(x - \varepsilon_2) \cdots (x - \varepsilon_{\varphi(h)})$$

Теорема 41 (многочлен деления круга). K — поле, $h \in \mathbb{N}, h \not\geq \text{char } K$

$x^h - 1$ раскладывается на линейные множители

$$1. \quad x^h - 1 = \prod_{d|h} \Phi_d(x);$$

- если $K = \mathbb{C}$, то коэффициенты $\Phi_h(x)$ — целые числа.

Доказательство.

1.

$$x^h - 1 = \prod_{\varepsilon \in U} (x - \varepsilon), \quad U - \text{группа корней } h\text{-й степени из 1}$$

$$\prod_{d|h} \Phi_d(x) \stackrel{?}{=} \prod_{\varepsilon \in U} (x - \varepsilon)$$

- Пусть $x - \varepsilon$ входит в $\Phi_d(x) \implies \varepsilon^d = 1, \varepsilon^k \neq 1$ при $k < d \implies \varepsilon^h = 1$ (т. к. $h : d$), $\varepsilon \in U$
- Пусть $x - \varepsilon$ входит в правую часть
Тогда $\varepsilon \in U$
Пусть $\text{ord } \varepsilon = d \implies x - \varepsilon$ входит в $\Phi_d(x)$, не входит в $\Phi_{\tilde{d}}(x)$, $\tilde{d} \neq d$

2. Индукция.

- **База** — проверено в примерах.
- **Переход** к h от меньших чисел.

$$\Phi_h(x) = \frac{x^h - 1}{\Phi_{d_1}(x) \cdots \Phi_{d_k}(x)}, \quad d_1, \dots, d_k — \text{делители } h, \text{ не равные } h$$

Знаменатель — многочлен с целыми коэффициентами, старший коэффициент равен 1. При делении на такой многочлен получаем целые коэффициенты.

□

41. Строение конечного поля. Единственность

Теорема 42 (строение конечного поля). K — конечное поле

Существуют $p \in \mathbb{P}, n \in \mathbb{N}$ такие, что

1. K содержит простое поле $F \simeq \mathbb{Z}_p$;
2. $\text{char } K = p$;
3. $|K| = p^n$;
4. K является полем разложения многочлена $x^{p^n} - x$ над F .

Доказательство.

1. F — минимальное подполе $\implies F$ простое \implies оно изоморфно \mathbb{Q} или \mathbb{Z}_p
 \mathbb{Q} бесконечно, значит $\exists p : F \simeq \mathbb{Z}_p$

$$2. \text{char } k = \min \left\{ n \left| \underbrace{1 + \cdots + 1}_n = 0 \right. \right\}$$

$$1, 1+1, 1+1+1, \dots \in F \implies \text{char } k = \text{char } F = p$$

3. K конечно над F , т. к. есть $\leq |K|$ ЛНЗ над F элементов.

Пусть $n = |K : F|$

e_1, \dots, e_n — базис K над F .

\implies элементы K имеют вид $a_1e_1 + a_2e_2 + \dots + a_ne_n \in F$
 $|K|$ — количество наборов $a_1, \dots, a_n \in F \implies |K| = p^n$

4. Пусть $U = K^*$ (группа ненулевых элементов K по умножению)

$$\implies |U| = p^n - 1$$

$$\forall x \in U \quad p^n - 1 : \text{ord } x \implies x^{p^n - 1} = 1 \quad \forall x \in K \setminus \{0\} \implies x^{p^n} - x = 0 \quad \forall x \in K$$

\implies все элементы K — корни $x^{p^n} - x = 0$

$$\deg(x^{p^n} - x) = p^n = |K| \implies \text{других корней нет}$$

□

Следствие (единственность). Любые два конечных поля с одинаковым числом элементов изоморфны.

Доказательство. $|K| = p^n \implies K$ изоморфно полю разложения $x^{p^n} - x$ над \mathbb{Z}_p . □

42. Существование поля с данным количеством элементов

Теорема 43. Для любых $p \in \mathbb{P}$, $n \in \mathbb{N}$ существует поле из p^n элементов

Доказательство. Пусть L — поле разложения $P(x) = x^{p^n} - x$ над \mathbb{Z}_p , K — подмножество L , состоящее из корней $P(x)$.

$$P'(x) = p^n x^{p^n-1} - 1 = -1 \text{ не имеет корней} \implies \text{у } P, P' \text{ нет общих корней}$$

\implies у P нет кратных корней \implies у P ровно p^n корней $\implies |K| = p^n$

Докажем, что K — поле:
 K — подмножество поля. Достаточно доказать, что $0, 1 \in K$, K замкнуто относительно $=, \cdot$, взятия обратного по $+, \cdot$:

- $P(0) = 0^{p^n} - 0 = 0$, $P(1) = 1 - 1 = 0 \implies 0, 1 \in K$

- $x, y \in K \implies x^{p^n} - x = 0, y^{p^n} - y = 0$

$$(x - y)^{p^n} = ((x - y)^p)^{p^{n-1}} = (x^p + y^p)^{x^{p^{n-1}}} = ((x^p + y^p)^p)^{p^{n-p}} = \\ = (x^{p^2} + y^{p^2})^{p^{n-p}} = \dots = x^{p^n} + y^{p^n} = x + y$$

$$(x + y)^{p^n} - (x + y) = 0$$

- $P(-x) = (-x)^{p^n} - (-x) = -(x^{p^n} - x) = \dots = -P(x)$

$$x \in K \implies P(x) = 0 \implies P(-x) = 0 \implies -x \in K$$

- $x, y \in K \implies x^{p^n} = x, y^{p^n} = y$

$$P(xy) = (xy)^{p^n} - xy = x^{p^n}y^{p^n} - xy = 0 \implies xy \in K$$

- $x \in K$

$$x^{p^n} = x \implies \left(\frac{1}{x}\right)^{p^n} = \frac{1}{x^{p^n}} = \frac{1}{x}$$

□