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 жорадновой 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. $a_1, .., a_n \notin \odot \iff$ **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, $\mathscr{A}$ — 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 $\mathscr{A}$, если

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

Утверждение 1. V_λ — инвариантное подпространство.

Доказательство.

- Подпространство
  - $u, v \in V_\lambda \implies \begin{cases} \mathscr{A}u = \lambda u \\ \mathscr{A}v = \lambda v \end{cases} \implies \mathscr{A}(u+v) \xlongequal[\text{линейность}]{} \mathscr{A}u + \mathscr{A}v = \lambda u + \lambda v = \lambda(u+v) \implies$ $u + v \in V_\lambda$
  - $u \in V_\lambda, k \in K \implies \mathscr{A}(ku) \xlongequal[\text{линейность}]{} k\mathscr{A}(u) = k\lambda u = \lambda(ku) \implies ku \in V_\lambda$
- Инвариантность
$$u \in V_\lambda \implies \mathscr{A}u = \lambda u \in V_\lambda$$

□

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

Доказательство. **Индукция** по k

- **База.** $k = 1$. Сумма из одного слагаемого — прямая.
- **Переход.** $k - 1 \to k$
Пусть $u_1 + \cdots + u_{k-1} + u_k = 0, \qquad u_i \in V_{\lambda_i}$
$$0 = \mathscr{A}\underbrace{(u_1 + \cdots + u_{k-1} + u_k)}_{=0} - \lambda_k \underbrace{(u_1 + \cdots + u_{k-1} + u_k)}_{=0} =$$
$$= \lambda_1 u_1 + \cdots + \lambda_{k-1}u_{k-1} + \cancel{\lambda_k u_k} - \lambda_k u_1 - \cdots - \lambda_k u_{k-1} - \cancel{\lambda_k u_k} = \underbrace{(\lambda_1 - \lambda_k)}_{\neq 0} u_1 + \cdots + \underbrace{(\lambda_{k-1} - \lambda_k)}_{\neq 0} u_{k-1}$$
(т. к. по условию собственные числа различны)
$$(\lambda_1 - \lambda_k)u_1 \in V_{\lambda_1}, \quad \ldots, \quad (\lambda_{k-1} - \lambda_k)u_{k-1} \in V_{\lambda_{k-1}}$$
По **индукционному предположению**, $V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_{k-1}}$
А мы представили 0 в виде суммы. Значит, все слагаемые нулевые:
$$(\lambda_1 - \lambda_k)u_1 = \cdots = (\lambda_{k-1} - \lambda_k)u_{k-1} = 0 \implies u_1 = \cdots = u_{k-1} = 0 \implies u_k = 0$$

□

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

Доказательство. Пусть $a_1u_1 + \cdots + a_ku_k = 0$
$$a_1u_1 \in V_{\lambda_1}, \ldots, a_ku_k \in V_{\lambda_k} \implies a_1u_1 = \cdots = a_ku_k = 0 \implies a_1 = \cdots = a_k = 0$$

□

2. Критерий диагонализуемости в терминах геометрических кратностей

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

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

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

Теорема 2 (критерий диагонализуемости в терминах геометрической кратности).
(I) $\mathscr{A}$ диагонализуем $\iff$ (II) **сумма геометрических кратностей** всех с. ч. равна $\mathbf{dim}\,\boldsymbol{V}$

Доказательство.

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

$\iff$ для некоторого базиса $e_1, \dots, e_n$ выполнено

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

$\iff$ (I$'$) существует базис из с. в.
Докажем, что (I$'$) $\iff$ (II):
Пусть $U = V_{\lambda_1} + \dots + V_{\lambda_k}$

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

- (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):

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

$$\underset{\text{(т. к. они лежат в большом базисе)}}{e_1^{(i)}, \dots, e_{t_i}^{(i)} \text{ ЛНЗ}} \implies t_i \le d_i \quad \forall i$$

  Сложим все эти неравенства:

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

□

Следствие (достаточное условие диагонализуемости). Пусть $\dim V = n$
Если у $\mathscr{A}$ есть $\boldsymbol{n}$ **различных** с. ч., то $\mathscr{A}$ диагонализуем

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

$$n \ge \dim(V_{\lambda_1} + \dots + V_{\lambda_k}) \xlongequal[\oplus]{} \dim V_{\lambda_1} + \dots + \dim V_{\lambda_k} \ge n$$

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. $\mathscr{A}$
Геом. кратность $\lambda \le$ **арифм.** кратности λ

Доказательство. Пусть $n = \dim V$, $\quad k$ — 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 $i \le k$ выполнено $\mathscr{A} e_i = \lambda e_i = 0 \cdot e_1 + \dots + \lambda e_i + \dots + 0 \cdot e_n$
Матрица $\mathscr{A}$ в базисе $e_1, \dots, e_n$:

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

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

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

□

Следствие (критерий диагонализуемости в терминах арифметических и геометрических кратностей).
Оператор $\mathscr{A}$ **диагонализуем** $\iff$

1. $\chi_{\mathscr{A}}(t)$ **раскладывается** на линейные множители
2. $\forall$ с. ч. λ $\quad$ **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.

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

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

4. Блочные матрицы и инвариантные подпространства. Делители характеристического многочлена

Определение 5. *Блочной матрицей* называется матрица вида

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

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

Определение 6. *Блочно-диагональной матрицей* называется матрица вида

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

где A_i — квадратные

Определение 7. U — инвариантное подпространство оператора $\mathscr{A}$
Через $\mathscr{A}\big|_U$ обозначим *сужение* $\mathscr{A}$ на U, т. е.

$$\mathscr{A}\big|_U : U \to U, \qquad \mathscr{A}\big|_U(x) = \mathscr{A}(x) \quad \forall x \in U$$

Теорема 4 (блочные матрицы и инвариантные подпространства).
$\mathscr{A}$ — оператор на конечномерном пространстве V

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

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

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

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

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

Доказательство.

1. Пусть

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

   Возьмём $1 \le i \le s$
   Посмотрим, как $\mathscr{A}$ действует на e_i:

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

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

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

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

2. Пусть $\dim U_1 = d_1, \quad \dim U_2 = d_2, \quad \dots$
   Рассмотрим столбец матрицы A с номером $d_1 + d_2 + d_{i-1} + t$, где $1 \le t \le d_i$ (т. е. t-й столбец i-го набора)
   Обозначим элементы базисов:

$$U_1 : e_1^{(1)}, \dots, e_{d_1}^{(1)}$$
$$U_2 : e_2^{(2)}, \dots, e_{d_2}^{(2)}$$
$$\dots\dots\dots\dots\dots$$

   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:

$$\underbrace{0\cdot e_1^{(1)}+\dots+0\cdot d_1^{(1)}}_{d_1}+\underbrace{0\cdot e_1^{(2)}+\dots}_{d_2}+\dots+\underbrace{a_1e_1^{(i)}+\dots+a_{d_i}e_d^{(i)}}_{d_i}+0\cdot e_1^{(i+1)}+\dots$$

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

$$\begin{pmatrix}0 & \cdots & 0 & a_1 & \cdots & a_{d_i} & 0 & \cdots & 0\end{pmatrix}^T$$

□

Следствие (делители характеристического многочлена).
$\mathscr{A}$ — оператор на конечномерном пространстве V, $\chi(t)$ — его характ. многочлен

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

$$\implies \chi(t) \,\vdots\, \chi_U(t)$$

2. $V=U_1\oplus\dots\oplus U_k$, где U_i — инвариатные
   $\chi_i(t)$ — характ. многочлен $\mathscr{A}\big|_{U_i}$

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

Доказательство. Рассмотрим базисы как в теореме

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

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

□

5. Ранг блочно-диагональной матрицы

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

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

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

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 $\widetilde{s_j}^{(i)}$ соответствующую строку матрицы A
Достаточно доказать, что

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

- $\implies$
  Докажем **от противного**:
  Предположим, что $s_1^{(i)},\dots,s_{r_i}^{(i)}$ ЛЗ
  То есть, $\exists\, a_1,\dots,a_{r_i}\notin\odot$, такие, что $a_1s_1^{(i)}+\dots+a_{r_i}s_{r_i}^{(i)}=0$
  Дополним нулями:

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

То есть, $\widetilde{s_1}^{(i)}, \dots, \widetilde{s_{r_i}}^{(i)}$ ЛЗ
А значит, и весь набор ЛЗ — $\lightning$

- $\Longleftarrow$
Докажем **от противного**:
Пусть все наборы $s_1^{(i)}, \dots, s_{r_i}^{(i)}$ ЛНЗ, а $\widetilde{s_1}^{(1)}, \dots, s_{r_i}^{(1)}, \dots\dots\dots, \widetilde{s_{r_k}}^{(k)}$ ЛЗ, то есть

$$\sum_{i,j} a_j^{(i)} \widetilde{s_j}^{(i)} = 0, \qquad \text{не все } a_j^{(i)} \text{ равны нулю}$$

Положим

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

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

$$\widetilde{T_1} + \widetilde{T_2} + \dots + \widetilde{T_k} = 0 \implies \widetilde{T_1} = \widetilde{T_2} = \dots = 0$$

Строки $\widetilde{T_1}, \dots, \widetilde{T_k}$ **не** содержат ненулевые элементы в одном столбце (т. е. в нашей записи нет полностью нулевых столбцов)

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

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

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

□

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

$$\implies \dim \operatorname{Im} \mathscr{A} = \dim \operatorname{Im} \mathscr{A}\big|_{U_1} + \dots + \dim \operatorname{Im} \mathscr{A}\big|_{U_k}$$

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

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

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

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

Определение 10. $\mathscr{A}$ — нильпотентный оператор
Жордановой цепочкой называется такой набор векторов $e_1, e_2, \dots, e_r$, что $\mathscr{A}(e_i) = e_{i+1}$ при $i < r$ и $\mathscr{A}(e_r) = 0$

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

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

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

$$\dots\dots$$

$$e_1^{(k)} \to e_2^{(k)} \to \dots \to e_{r_k}^{(k)} \to 0$$

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

Доказательство. **Индукция** по $r \coloneqq \max\{\, r_1, \dots, r_k \,\}$

- **База.** $r = 1$
  Все цепочки длины 1
  Все векторы — последние и, по условию, ЛНЗ

- **Переход.** $r - 1 \to r$

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

Применим s раз:

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

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.

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

От противного: пусть набор ЛЗ:

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

Применим к этому равентсву $\mathscr{A}^{r-1}$:

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

То есть,

$$e_1^{(j)} \to e_r^{(j)}, \qquad a_1^{(j)} e_1^{(j)} \to a_1^{(j)} e_r^{(j)}, \qquad \text{остальные } \to 0$$

Получится сумма:

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

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

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

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

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

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). $\mathscr{A}$ — оператор на V.
$e_1, e_2, \dots, e_n$ — базис, являющийся объединением жордановых цепочек (в естественном порядке):

$$e_1 \to e_2 \to \dots \to e_{r_1} \to 0$$

$$e_{r_1+1} \to e_{r_2+2} \to \dots \to e_{r_1+r_2} \to 0$$

$$\dots\dots$$

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

Тогда матрица $\mathscr{A}$ в этом базисе

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

Доказательство.

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

Значит, при $i = r_1, r_1 + r_2, \dots\dots\dots\dots, r_1 + \dots + r_k,\quad$ i-й столбец — нулевой

При $i \neq r_1, \dots\dots\dots\dots, r_1 + \dots + r_k,\quad \mathscr{A}(e_i) = e_{i+1} \implies i$-й столбец:

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

□

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 $W := \ker \mathscr{A}$

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

Положим $U_i := \operatorname{Im} \mathscr{A}^i$

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

где k — степень нильпотентности $\mathscr{A}$

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 достроть 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:

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

Объединение цепочек — ЛНЗ (по лемме)

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

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

Докажем **индукцией** по s:

- **База.** $s = 1$

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

- **Переход.** $s \to s + 1$

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

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

$$\underbrace{\overbrace{v \to \dots \to \dots \to u}^{s} \to 0}_{s+1}$$

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

  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 $s+1$

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

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

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

При этом, $\mathscr{A}^s(v) \overset{\text{def}}{=} u$
Получили 2 линейных представления u, значит,

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

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

$\square$

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

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

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

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

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

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

$$\implies (PQ)(\mathscr{A}) = P(\mathscr{A}) \circ Q(\mathscr{A})$$

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

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

Положим $\mathscr{B} = P(\mathscr{A}), \quad \mathscr{C} = Q(\mathscr{A}), \quad \mathscr{D} = R(\mathscr{A})$
Нужно доказать, что $\mathscr{B}\Big(\mathscr{C}(v)\Big) = \mathscr{D}(v) \quad \forall v$

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

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

$\square$

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

$$\implies \mathscr{B} \circ \mathscr{C} = \mathscr{C} \circ \mathscr{B}$$

Доказательство. $PQ = QP \implies (PQ)(A) = (QP)(A)$ $\square$

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

Доказательство.

- $\ker \mathscr{B}$

$$v \in \ker \mathscr{B} \implies \mathscr{B}(v) = 0 \implies \mathscr{A}\Big(\mathscr{B}(v)\Big) = 0 \xRightarrow[\text{лемма}]{} \mathscr{B}\Big(\mathscr{A}(v)\Big) = 0 \implies \mathscr{A}(v) \in \ker \mathscr{B}$$

- $\operatorname{Im} \mathscr{B}$

$$v \in \operatorname{Im} \mathscr{B} \implies v = \mathscr{B}(w) \implies \mathscr{A}(v) = \mathscr{A}\Big(\mathscr{B}(w)\Big) \overset{}{\underset{\text{лемма}}{=\!=}} \mathscr{B}\Big(\mathscr{A}(w)\Big)$$

$\square$

9. Свойства аннулятора вектора

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

- *Аннулятором* v называется такой многочлен P, что $P(\mathscr{A})(v) = 0$
- *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 $\deg P_0 \le \dim V$
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.

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

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

Доказательство.

1. Пусть $n := \dim V$
   Докажем, что $\exists\, P : \deg P \le n,\ P$ — аннулятор, $P \ne 0$
   Возьмём

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

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

$$\exists\, a_i \ne \odot : a_0 v + a_1 \mathscr{A}(v) + \dots + a_n \mathscr{A}^n(v) = 0$$

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

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

$$\mathscr{D}(v) = \mathscr{C}_1\Big(\underbrace{\mathscr{B}_1(v)}_{=0}\Big) + \dots + \mathscr{C}_k\Big(\underbrace{\mathscr{B}_k(v)}_{=0}\Big) = \mathscr{C}_1(0) + \dots + \mathscr{C}_k(0) = 0$$

3. Поделим с остатком:
$$P(t) = Q(t)P_0(t) + R(t), \qquad \deg R < \deg P_0$$
   - $\Longleftarrow$
$$R(t) = 0, \qquad P(t) = \underbrace{P_0(t)}_{\text{аннулятор}}\, Q(t) \text{ — аннулятор (по (2.))}$$
   - $\Longrightarrow$
$$R(t) = \underbrace{P(t)}_{\text{аннул.}} - Q(t)\underbrace{P_0(t)}_{\text{аннул.}} \text{ — аннулятор (по (2.))}$$
4.
$$\exists\, P_1, P_2 \text{ — мин. аннул.} \implies \underbrace{P_1}_{\text{аннул.}} \,\vdots\, \underbrace{P_2}_{\text{мин. аннул.}}$$

□

10. Базис циклического подпространства

Определение 12. $\mathscr{A}$ — оператор на V, $\qquad v \in V$
Циклическим подпространством, порождённым v называется минимальное по включению инвариантное подпространство, содержащее v

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

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

Тогда первый набор является базисом циклического подпространства, порождённого v

Доказательство. Пусть U — циклическое, порождённое v
$$U \text{ — инвар.} \implies v \in U \implies \mathscr{A}v \in U \implies \underbrace{\mathscr{A}^2 v}_{=\mathscr{A}(\mathscr{A}(v))} \in U \implies \dots \implies v, \mathscr{A}v, \dots, \mathscr{A}^{k-1}v \in U$$
Они ЛНЗ. Чтобы доказать, что это базис, надо доказать, что они порождают U:
Положим $W = \langle v, \mathscr{A}v, \dots, \mathscr{A}^{k-1}v \rangle$
Докажем, что $W = U$:

- Докажем, что W — инвар.:
  $\mathscr{A}^k v$ — ЛК $v, \mathscr{A}v, \dots, \mathscr{A}^{k-1}v$
$$w \in W, \qquad w = a_0 v + \dots + a_{k-1}\mathscr{A}^{k-1}v$$
$$\mathscr{A}(w) = a_0\mathscr{A}v + \dots + a_{k-2}\mathscr{A}^{k-1}v + \underbrace{a_{k+1}\mathscr{A}^k v}_{\text{ЛК } v, \dots, \mathscr{A}^{k-1}v}$$
  Значит, w является ЛК $v, \dots, \mathscr{A}^{k-1}v$
- Докажем, что W — минимальное:
  Докажем, что если W_1 инвариантно и $v \in W_1$, то $W \subset W_1$:
$$\left.\begin{array}{l} W_1 \text{ инвар.} \\ v \in W_1 \end{array}\right\} \implies \mathscr{A}v \in W_1, \qquad \left.\begin{array}{l} W_1 \text{ инвар.} \\ \mathscr{A}v \in W_1 \end{array}\right\} \implies \mathscr{A}^2 v \in W_1, \quad \dots, \quad \underbrace{\mathscr{A}^i v}_{\text{порожд.}W} \in W_1 \implies$$
$$\implies W_1 \subset W$$

□

11. Циклическое подпространство и минимальный аннулятор

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

Доказательство. Пусть k такое, что

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

Выберем a_i, не все равные нулю, такие, что

$$a_0 v + a_1 \mathscr{A}v + \dots + a_{k-1}\mathscr{A}^{k-1}v + a_k \mathscr{A}^k v = 0$$

Значит, $a_k \neq 0$ (т. к. $v \dots, \mathscr{A}^{k-1}v$ ЛНЗ)
Поделим на a_k, не меняя обозначений (т. е. $a_i \coloneqq \frac{a_i}{a_k}$):

$$\mathscr{A}^k v + \dots + a_1 \mathscr{A} v + a_0 v = 0$$

Положим $P(t) \coloneqq t^k + a_{k-1}t^{k-1} + \dots + a_1 t + a_0 \implies P(t)$ — аннулятор

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

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

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

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

- Докажем, что $P(t) = \pm\chi$:
Знаем, что $v, \dots, \mathscr{A}^{k-1}v$ — базис U. Образы этих векторов:

$$\mathscr{A}\big(\mathscr{A}^i(v)\big) = \mathscr{A}^{i+1}(v), \quad 0 \le i < k-1$$

$$\mathscr{A}\big(A^{k-1}(v)\big)(v) = \mathscr{A}^k(v) = -a_0 v - a_1\mathscr{A}(v) - \dots - a_{k-1}\mathscr{A}^{k-1}(v)$$

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

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

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

Это будет $(-1)^k P(t)$

□

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

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

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

Свойства. $\mathscr{A}$ — оператор на V

1. $P_1, \dots, P_k$ аннулируют $\mathscr{A}$
$$\forall \text{ многочл. } Q_1, \dots, Q_k \quad S(t) = P_1(t)Q_1(t) + \dots + Pk(t)Q_k(t) \text{ аннулирует } \mathscr{A}$$
2. P_0 — минимальный многочлен для $\mathscr{A}$
$$P \text{ аннулирует } \mathscr{A} \iff P \,\vdots\, P_0$$
3. Минимальный многочлен $\mathscr{A}$ единственнен с точностью до ассоциирования
4. $e_1, \dots, e_n$ — базис V, $\qquad P_1(t), \dots, P_n(t)$ — 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 $v \implies S(\mathscr{A})$ — аннулятор $v \implies S$ аннулирует $\mathscr{A}$
2. Пусть $P = P_0Q + R$
   - Если $P \,\vdots\, P_0$, то $P = P_0Q \underset{1.}{\implies} P$ аннулирует $\mathscr{A}$
   - Если P аннулирует $\mathscr{A}$, то $R = P - P_0Q$ аннулирует $\mathscr{A} \underset{1.}{\implies} R = 0 \implies P \,\vdots\, P_0$
3. Если P_1, P_2 — минимальные многочлены, то $P_1 \,\vdots\, P_2$ и $P_2 \,\vdots\, P_1$.
4. Пусть $P =$ НОК$(P_1, \dots, P_n)$
   - Проверим, что P аннулирует A:
     Пусть $v \in V$, $\qquad v = a_1e_1 + \dots + a_ne_n$
     Применим P:
     $$P(\mathscr{A})(v) = a_1P(\mathscr{A})e_1 + \dots + a_nP(\mathscr{A})e_n$$
     $$P \,\vdots\, P_i \implies P \text{ — аннул. для } e_i \implies P(\mathscr{A})e_i = 0$$
     $$P(\mathscr{A})(v) = a_1 \cdot 0 + \dots + a_n \cdot 0 = 0$$
   - Проверим, что P минимальный:
     Пусть $Q(t)$ аннулирует $\mathscr{A}$
     $$\implies Q(\mathscr{A})v = 0 \quad \forall v \implies Q(\mathscr{A})e_i = 0 \quad \forall i \xRightarrow[P_i \text{ — мин. аннул.}]{} $$
     $$\implies Q \,\vdots\, P_i \quad \forall i \implies Q \,\vdots\, P \implies \deg Q \geq \deg P$$

$\square$

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

Доказательство. Нужно доказать, что $\forall v \quad \chi(\mathscr{A})v = 0$
Докажем, что $\chi_{\mathscr{A}} \,\vdots\, P_0$, где P_0 — минимальный аннулятор (все аннуляторы делятся на минимальный):
Пусть U — циклическое подпространство, порождённое v
χ_U — характеристический многочлен $\mathscr{A}\big|_U$ (он определён, т. к. пространство инвариантно)
По следствию о делителях характеристического многочлена, $\chi \,\vdots\, \chi_U$
Знаем, что χ_U — минимальный аннулятор для v на U (по т. о циклическом подпространстве и минимальном аннуляторе)
$$\left.\begin{aligned} \chi_U &= P_0 \\ \chi &\,\vdots\, \chi_U \end{aligned}\right\} \implies \chi \,\vdots\, P_0$$

$\square$

Следствие. Если P — минимальный многочлен $\mathscr{A}$, то $\chi \,\vdots\, P$.

13. Свойства взаимно простых многочленов от оператора

Свойства. $\mathscr{A}$ — оператор на V

1. $P_1, P_2, \ldots, P_k$ — попарно взаимно просты, $\quad T(t) = P_1(t) \cdots P_k(t), \quad v \in V, \quad T$ аннулир. v.
   Тогда $\exists\, v_1, \ldots, v_k : \quad v = v_1 + \cdots + v_k$ и P_i аннулирует v_i

2. P, Q взаимно просты, $\quad P, Q$ аннуляторы $v \quad \Longrightarrow \quad v = 0$

Доказательство.

1. **Индукция.**

   - **База.** $k = 2$
     P, Q взаимно просты, $\quad v \in V$
     Докажем, что $\exists\, v, w : v = u + w, \quad P(\mathscr{A})u = 0, \quad Q(\mathscr{A})w = 0$
     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 $\mathscr{A}$:

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

     Применим к v:

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

     Положим $u = (QG)(\mathscr{A})v, \quad w = (PF)(\mathscr{A})v$
     Проверим, что $P(\mathscr{A})u = 0$ (для w — аналогично):

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

   - **Переход.** $k - 1 \to k$

     $$T = \underbrace{P_1 \ldots P_{k-1}}_{P}\,\underbrace{P_k}_{Q}$$

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

     По **индукционному предположению**,

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

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

2. Пусть T — минимальный аннулятор v

   $$\left.\begin{matrix} P \,\vdots\, T \\ Q \,\vdots\, T \end{matrix}\right\} \Longrightarrow T = \mathrm{const}, \quad T(t) = c \Longrightarrow cv = 0 \Longrightarrow v = 0$$

$\square$

14. Разложение пространства в прямую сумму примарных подпространств

Определение 15. K — поле, $\quad V$ — векторное пространство над K, $\quad \mathscr{A}$ — оператор на V
$P(t)$ — минимальный многочлен $\mathscr{A}$ со старшим коэффициентом, равным 1.
Пространство V называется *примарным* (относительно $\mathscr{A}$), если $P(t) = Q^s(t)$ для некоторого $Q(t)$, неприводимого над K

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

$$P(t) = P_1(t) \cdots P_k(t), \qquad \text{где } P_i(t) = Q_i^{s_i}(t), \qquad Q_i \text{ — неприв{о}д. над } K$$

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

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

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

1. Знаем, что ядро многочлена от оператора инвариантно
2. (a) Докажем, что $V = U_1 + \dots + U_k$
   $P_1, \dots, P_k$ попарно взаимно просты, и $P_1 \cdots P_k$ аннулирует любой v, значит
   $$\forall v \quad \exists v_1, \dots, v_k : \quad v = v_1 + \dots + v_k, \qquad P_i \text{ аннул. } v_i \implies v_i \in U_i$$
   (b) Докажем, что сумма прямая:
   Нужно проверить, что $U_s \cap \Big(U_1 + \dots + U_{s-1} + U_{s+1} + \dots + U_k\Big) = \{\, 0 \,\} \quad \forall s$
   НУО проверим, что $(U_1 + \dots + U_{k-1}) \cap U_k = \{\, 0 \,\}$
   Возьмём $v \in (U_1 + \dots + U_{k-1}) \cap U_k$
   $$v = v_1 + \dots + v_{k-1}, \qquad v_i \in U_i, \qquad v \in U_k$$
   По первому свойству, $P_1 \cdots P_{k-1}$ аннулирует $v_1 + \dots + v_{k-1} = v$
   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. $$U_i = \ker P_i(\mathscr{A}) \implies P_i(\mathscr{A})\big|_{U_i} = 0$$
   P_i аннулирует $\mathscr{A}\big|_{U_i}$
   Значит, P_i делится на минимальный многочлен $\mathscr{A}\big|_{U_i}$
   При этом, $P_i = Q_i^{s_i}$
   Отсюда минимальный тоже является $Q_i^{r_i}, \qquad r_i \le s_i$
   Хотим доказать, что $r_i = s_i$
   Пусть $T = Q_1^{r_1} \dots Q_k^{r_k}$
   Т. к. у нас прямая сумма, сущестует $e_1, \dots, e_n$ — базис V, он является объединением базисов U_i
   $$\implies T(\mathscr{A})e_1 = 0, \quad \dots, \quad T(\mathscr{A})e_k = 0$$
   $$\implies T \text{ аннулирует } \mathscr{A} \xRightarrow[P\text{ — мин. многочл.}]{} \underbrace{T}_{\prod Q_i^{r_i}} \; \vdots \; \underbrace{P}_{\prod Q_i^{s_i}}, \quad r_i \ge s_i \implies r_i = s_i$$

$\square$

15. Корневые подпространства

Определение 16. λ — с. ч. $\mathscr{A}$
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.

1. Корневое подпространство инвариантно
2. V конечномерно, минимальный многочлен $\mathscr{A}$ раскладывается на линейные множители
$$P(t) = (\lambda_1 - t)^{s_1} \cdots (\lambda_k - t)^{s_k}$$
Тогда $\ker\Big((\lambda_i\mathscr{E} - \mathscr{A})^{s_i}\Big)$ — корневые подпространства

Доказательство.

1. Пусть $P(t) = (\lambda - t)^k$ — аннул. v, т. е. $P(\mathscr{A})v = 0$
$$P(\mathscr{A})(\mathscr{A}v) = \Big(P(\mathscr{A}) \circ \mathscr{A}\Big)v = \Big(\mathscr{A} \circ P(\mathscr{A})\Big)v = \mathscr{A}\Big(\underbrace{P(\mathscr{A})v}_{=0}\Big) = \mathscr{A}(0) = 0$$
2. Пусть $U_i = \ker\Big((\lambda_i\mathscr{E} - \mathscr{A})^{s_i}\Big)$, $\qquad W_i$ — корневое подпространство для λ_i
   - $U_i \subset W_i$ — очевидно ($v \in U_i \implies (\lambda_i\mathscr{E} - \mathscr{A})^{s_i}v = 0, \qquad$ 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 $(\lambda_i\mathscr{E} - \mathscr{A})^k$ аннулирует v
     Тогда $(\lambda - t)^k$ — минимальный аннулятор v
     При этом, $P(t)$ — аннулятор v
$$\implies P(t) \,\vdots\, (\lambda - t)^k \implies k \le s_i \implies v \in U_i$$

□

16. Существование жордановой формы

Определение 17. *Жордановой клеткой* порядка r с с. ч. λ называется матрица порядка r вида
$$J_r(\lambda) = \begin{pmatrix} \lambda & \cdots & 0 \\ 1 & \ddots & \vdots \\ \vdots & \ddots & \\ 0 & \cdots\, 1 & \lambda \end{pmatrix}$$

Определение 18. *Жордановой матрицей* называется блочно-диагональная матрица вида
$$\begin{pmatrix} J_{1_1}(\lambda_1) & & 0 \\ & \ddots & \\ 0 & & J_{r_k}(\lambda_k) \end{pmatrix} \qquad \text{(как } r_i\text{, так и } \lambda_i \text{ могут совпадать)}$$

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

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

Доказательство.

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

- Общий случай
$$\chi_{\mathscr{A}} = (-1)^n (t-\lambda_1)^{s_1} \cdots (t-\lambda_m)^{s_m}$$
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:
Пусть $Q_i \coloneqq (t-\lambda_i)^{r_i}$
По теореме
$$V = U_1 \oplus \cdots \oplus U_k$$
U_i инвариантны
$Q_i(t)$ — минимальный многочлен $\mathscr{A}$ на U_i
К U_i применяем нильпотентный случай:
Существует жорданов базис U_i
Матрица $\mathscr{A}\big|_{U_i}$ имеет вид
$$J_i = \begin{pmatrix} J_{r_1}(\lambda_i) & & 0 \\ & \ddots & \\ 0 & & J_{r_k}(\lambda_k) \end{pmatrix}$$
Значит, в базисе, полученном объединением базисов U_i матрица $\mathscr{A}$ имеет вид
$$J = \begin{pmatrix} J_1 & & 0 \\ & \ddots & \\ 0 & & J_m \end{pmatrix}$$
□

17. Возведение жордановой клетки в степень

Свойства.

1. - $$\Big(J_r(0)\Big)^s = \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & & & \vdots \\ 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots 1 & 0 & \cdots 0 \end{pmatrix} \qquad \text{при } s < r$$
     То есть,
     $$a_{ij} = \begin{cases} 1, & i - j = s \\ 0, & \text{иначе} \end{cases}$$
   - $$\Big(J_r(0)\Big)^s = \mathbb{O} \qquad \text{при } s \geq r$$
2. Пусть $\lambda \neq 0, \qquad A = \Big(J_r(\lambda)\Big)^s$
   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. $$\operatorname{rk}\Big(\big(J_r(0)\big)^s\Big) = \begin{cases} r - s, & s < r \\ 0, & s \geq r \end{cases}$$

Доказательство.

1. **Индукция** по s.

- **База.** $s = 1$

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

- **Переход.** $s \to s+1$

$$J_r^s(0) = a_{ij}, \qquad J_r(0) = b_{ij}, \qquad J_r^{s+1}(0) = c_{ij}$$

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2i} + \dots + a_{in}b_{ni} \tag{1}$$

Среди a_{ij} не более одной единицы, остальные нули
Среди b_{xj} не более одной единицы, остальные нули
Значит, $c_{ij} = 0$ или $c_{ij} = 1$

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

2. $J_r(\lambda) = \lambda \cdot E + J_r(0)$
   Возведём в степень и распишем как бином Ньютона (учитывая, что λE коммутирует с чем угодно, а значит, можно приводить подобные):

$$\Big(J_r(\lambda)\Big)^s = (\lambda E)^s + C_s^1(\lambda E)^{s-1}J_r(0) + \dots + C_s^{r-1}(\lambda E)^{s-r+1}J_r(0)^{r-1} + \underbrace{J_r^r(0)}_{=0}(\dots) \xlongequal[\text{св-во } 1a]{}$$

$$= \lambda^s E + C_s^1 \lambda^{s-1} J_r(0) + \dots + C_s^{r-1}\lambda^{s-r+1}J_r^{r-1}(0) =$$

$$= \begin{pmatrix} \lambda^s & . & 0 \\ . & . & . \\ 0 & . & \lambda^s \end{pmatrix} + \begin{pmatrix} 0 & . & . & 0 \\ \lambda^{s-1}C_s^1 & . & . & 0 \\ . & . & . & . \\ 0 & . & \lambda^{s-1}C_s^1 & 0 \end{pmatrix} + \dots + \begin{pmatrix} 0 & . & 0 \\ . & . & . \\ \lambda^{s-r+1}C_s^{r-1} & . & 0 \end{pmatrix}$$

□

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

Теорема 12 (количество клеток и ранг). J — жорданова матрица
Тогда количество клеток вида $J_r(\lambda)$ равно

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

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

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

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

Какое-то из λ_i совпало с λ

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

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

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

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

- Если $\lambda_i = \lambda, \quad r_i \leq s$, то i-е слагаемое равно $0 - 0 = 0$
- Если $\lambda_i = \lambda, \quad r_i > s$, то i-е слагаемое равно $(r_i - s) - \Big(r_i - (s+1)\Big) = 1$

$f(s+1) - f(s)$ — количество клеток, для которых $\lambda_i = \lambda, \quad r_i > s$
$\Big(f(s+1) - f(s)\Big) - \Big(f(s) - f(s-1)\Big)$ — количество клеток размера s
Это равно $f(s+1) - 2f(s) + f(s-1)$ □

Следствие (единственность жордановой формы). J, J' — жордановы матрицы $\mathscr{A}$ 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, $\qquad \lambda_1, \dots, \lambda_k$ — 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 $J_r(\lambda)$

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

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

Минимальный многочлен — это НОК многочленов вида $(t - \lambda_i)^s, \quad s \leq r_i$
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 $\mathbb{C} \times \widehat{V} \to \widehat{V}$, заданной равенством

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

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

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

Определение 21. $w = (u, v)$
$(u, -v)$ называется сопряжённым к w

Обозначение. $\overline{w}$

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 $\square$

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 u и v по базису $e_1, \dots, e_n$ в V:

$$u = a_1 e_1 + \dots + a_n e_n, \qquad v = b_1 e_1 + \dots + b_n e_n, \qquad a_s, b_s \in \mathbb{R}$$

$$w = \underbrace{(a_1 + b_1 i)}_{\in \mathbb{C}} e_1 + \dots + \underbrace{(a_n + b_n i)}_{\in \mathbb{C}} e_n$$

- Докажем ЛНЗ:
  Пусть $c_1 e_1 + \dots + c_n e_n = 0, \quad c_s \in \mathbb{C}, \quad c_s = a_s + b_s i, \quad a_s, b_s \in \mathbb{R}$

$$(a_1 + b_1 i)(e_1 + 0i) + \dots + (a_n + b_n i)(e_n + 0i) = 0$$

  Разделим вещественную и мнимую части:

$$\Big((a_1 e_1 - b_1 0) + \dots + (a_n e_n - b_n 0)\Big) + \Big((a_1 0 + b_1 e_1) + \dots + (a_n 0 + b_n e_n)\Big) i = 0 + 0i$$

  Значит, каждое большое слагаемое равно нулю:

$$\begin{cases} a_1 e_1 + \dots + a_n e_n = 0 \\ b_1 e_1 + \dots + b_n e_n = 0 \end{cases} \xRightarrow[e_1, \dots, e_n \text{ ЛНЗ в } V]{} \begin{cases} a_1 = \dots = a_n = 0 \\ b_1 = \dots = b_n = 0 \end{cases}$$

$\square$

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

Свойства (сопряжённых векторов)**.**

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

Доказательство.

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

Пусть $z = a + bi, \quad w = u + vi$

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

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

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

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

$$0 = \overline{0} = \overline{c_1\overline{w_1} + \dots + c_n\overline{w_n}} \xlongequal[\text{2 св-во}]{} \overline{c_1}\overline{\overline{w_1}} + \dots + \overline{c_n}\overline{\overline{w_n}} \xlongequal[\text{1 св-во}]{} \overline{c_1}w_1 + \dots + \overline{c_n}w_n$$

$$c_i \notin \odot \implies \overline{c_i} \notin \odot$$

$w_1, \dots, w_n$ ЛЗ — $\lightning$

□

Определение 22. $\mathscr{A}$ — оператор на V
Продолжением $\mathscr{A}$ на $\widehat{V}$ называется отображение $\widehat{\mathscr{A}} : \widehat{V} \to \widehat{V}$, заданное равенством $\widehat{\mathscr{A}}(u+vi) = \mathscr{A}(u) + \mathscr{A}(v)i$

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

21. Каноническая матрица оператора в вещественном пространстве

Обозначение. $P(t) = c_k t^k + c_{k-1}t^{k-1} + \dots + c_0, \qquad c_s \in \mathbb{C}$
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). $\mathscr{A}$ — оператор на V. Тогда

1. $\widehat{\mathscr{A}}(\overline{w}) = \overline{\widehat{\mathscr{A}}(w)}$
2. $P(\widehat{\mathscr{A}})(w_1) = w_2 \implies \overline{P}(\widehat{\mathscr{A}})(\overline{w_1}) = \overline{w_2}$
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 $\overline{\lambda}$
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 $\overline{\lambda}$ (если один жорданов, то и второй жорданов)

Доказательство.

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

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

2. Из первого свойства $\widehat{\mathscr{A}}^{(s)}(\overline{w_1}) = \overline{\mathscr{A}^{(s)}(w_1)}$
Пусть $P(t) = c_k t^k + \dots + c_0$

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

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

3. $P(\widehat{\mathscr{A}})(w) = 0 \implies \overline{P}(\widehat{\mathscr{A}})(\overline{w}) \xlongequal[\text{2 св-во}]{} \overline{P(\widehat{\mathscr{A}})(w)} = \overline{0} = 0$

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

5.
   - ЛНЗ доказана
   - Докажем, что это порождающая система:
     Пусть $\overline{w}$ принадлежит пространству, соответтсвующему $\overline{\lambda} \implies w$ принадлежит пространству, соотв. λ
     Разложим по базису:
     $$\exists c_i : \quad w = c_1e_1 + \cdots + c_ne_n$$
     $$\implies \overline{w} = \overline{c_1e_1} + \cdots + \overline{c_ne_n}$$
   - Докажем, что сопряжённый к жорданову базису жорданов:
     $$\widehat{\mathscr{A} - \lambda\mathscr{E}} = \widehat{\mathscr{A}} - \lambda\widehat{\mathscr{E}}$$
     $$(\widehat{\mathscr{A}} - \lambda\widehat{\mathscr{E}})e_i = e_{i-1} \implies (\widehat{\mathscr{A}} - \overline{\lambda}\mathscr{E})\overline{e_i} = \overline{e_{i+1}}$$

□

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

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

Доказательство. Пусть минимальный многочлен $\mathscr{A}$ равен

$$P(t) = (t - a_1)^{m_1} \cdots (t^2 + p_1t + q_1)^{s_1} \cdots ,$$

где $t^2 + p_it + q_i$ 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 $\mathscr{A}$ жорданова
Рассмотрим подпространство, соответствующее $(t^2 + pt + q)^s$:
Пусть $\lambda, \overline{\lambda}$ — комплексные корни $t^2 + ptq$

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

Пусть $P_1 = (t^2 + pt + q)^s$
Знаем, что $P_1(\mathscr{A}) = 0$ на корневом подпространстве U
Тогда $P_1(\widehat{\mathscr{A}}) = 0$ на $\widehat{U}$

$$\widehat{U} = \widehat{W_1} + \widehat{W_2}, \qquad \widehat{W_1}, \widehat{W_2} \text{ — корневые подпространства для } \lambda, \overline{\lambda}$$

Существует жорданов базис $w_1, \ldots, w_k$ для $\widehat{W_1}$
Тогда $\overline{w_1}, \ldots, \overline{w_k}$ — жорданов базис для $\widehat{W_2}$
$w_1, \ldots, w_k, \overline{w_1}, \ldots, \overline{w_k}$ — базис $\widehat{U}$
Пусть $w_i = u_i + iv_i$
Докажем, что $u_1, v_1, u_2, v_2, \ldots, u_k, v_k$ — базис U:
Следующие элементарные преобразования переводят базис $\widehat{U}$ в базис $\widehat{U}$, а значит, и в базис U:

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

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:

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

Пусть $\lambda = a + bi$
При $m < r$,

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

При $m = r$,

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

□

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 $V \to K$

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 $\varphi : V^* \to K^n : \quad \varphi(y) = \big(y(e_1), \dots, y(e_n)\big)$
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):

$$\varphi(y_1+y_2) = \Big((y_1+y_2)(e_1),\dots,(y_1+y_2)(e_n)\Big) = \Big(y_1(e_1)+y_2(e_1),\dots,y_1(e_n)+y_2(e_n)\Big) = $$
$$= \Big(y_1(e_1),\dots,y_1(e_n)\Big) + \Big(y_2(e_1),\dots,y_2(e_n)\Big) = \varphi(y_1)+\varphi(y_2)$$

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

- Биективность:
Пусть $a \in K^n, \qquad a = (a_1, ..., a_n), \quad a_i \in K$

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

2. - Проверим, что $y_v \in V^*$, т. е. что y_v линейно:
     - $y_v(x_1+x_2) = (x_1+x_2, v) \xlongequal[\text{лин. скал. произв.}]{} (x_1,v)+(x_2,v) = y_v(x_1)+y_v(x_2)$
     - $y_v(kx) = (kx, v) = k(x,v) = ky_v(x)$
   - Пусть $\varphi(v) = y_v$. Докажем, что φ — изоморфизм $V \to V^*$:
     - Линейность:
       * $\varphi(u+v) \overset{?}{=} \varphi(u)+\varphi(v)$

$$\varphi(u+v) \overset{?}{=} \varphi(u)+\varphi(v) \quad\iff\quad y_{u+v} \overset{?}{=} y_u + y_v \quad\iff$$
$$\iff\quad y_{u+v}(x) \overset{?}{=} y_u(x)+y_v(x) \quad \forall x \quad\iff$$
$$\iff\quad (x, u+v) \xlongequal[\text{лин. скалярного произв.}]{} (x,u)+(x,v)$$

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

$$\varphi(kv) \overset{?}{=} k\varphi(v) \quad\iff\quad y_{kv} \overset{?}{=} ky_v \quad\iff\quad y_{kv}(x) \overset{?}{=} ky_v(x) \quad \forall x \quad\iff$$
$$(x, kv) \xlongequal[\text{лин. скалярного произв.}]{} k(x,v)$$

     - Инъективность:
       Пусть $\varphi(v) = 0$. Тогда

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

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

$\square$

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 $V^* \to K$, 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 $\varphi : V \to (V^*)^*$, заданное формулой $\varphi(x) = z_x$ является линейным
3. если V конечномерно, то φ — изоморфизм

Доказательство.

1. • $z_x(y_1+y_2) \stackrel{?}{=} z_x(y_1)+z_x(y_2)$
$$z_x(y_1+y_2)=(y_1+y_2)(x)$$
$$z_x(y_1)+z_x(y_2)=y_1(x)+y_2(x)$$
   • $z_x(ky) \stackrel{?}{=} kz_x(y)$
$$z_x(ky)=(ky)(x)=ky(x)=kz_x(y)$$

2. • $\varphi(x_1+x_2) \stackrel{?}{=} \varphi(x_1)+\varphi(x_2)$
$$z_{x_1+x_2} \stackrel{?}{=} z_{x_1}+z_{x_2}$$
$$\forall y \quad z_{x_1+x_2}(y)=z_{x_1}(y)+z_{x_2}(y)$$
$$y(x_1+x_2) \stackrel{?}{=} y(x_1)+y(x_2)$$
   Это верно, так как y линейно
   • $\varphi(kx) \stackrel{?}{=} k\varphi(x)$
$$z_{kx} \stackrel{?}{=} kz_x$$
$$\forall y \quad z_{kx}(y) \stackrel{?}{=} kz_x(y)$$
$$y(kx) \stackrel{?}{=} ky(x)$$
   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 $x=0$ $\iff$ $z_x(y)=0$ $\forall y$ только при $x=0$ $\iff$ $y(x)=0$ $\forall y$ только при $x=0$
   Нужно проверить, что $\forall x \neq 0$ $\exists$ линейное отображение $y: \quad y(x)\neq 0$
   Дополним до базиса:
   Пусть $x, e_2, ..., e_n$ — базис V
   Определим $y: y(x)=1, \quad y(e_i)=0$
$$y(\alpha x+\beta_2 e_2+...+\beta_n e_n)=\alpha$$
   Оно линейно, $y(x)\neq 0$

□

24. Двойственный базис. Матрица перехода для двойственного базиса

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

Доказательство. Знаем, что $\dim V=\dim V^*$
Достаточно доказать ЛНЗ:
Возьмём ЛК:
Пусть $a_1, ..., a_n \in K$ такие, что $f=a_1f_1+...+a_nf_n$ — нулевой функционал
$$0=f(e_i)=a_1\underbrace{f_1(e_i)}_{0}+...+a_i\underbrace{f_i(e_i)}_{1}+...+a_n\underbrace{f_n(e_i)}_{0}=a_i \quad \forall i$$

□

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

Теорема 19. e_i, e_i' — базисы V, $\qquad C$ — матрица перехода от e_i к e_i'
f_i, f_i' — соответствующие двойственные базисы

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

Доказательство.

1. Пусть $D = (d_{ij})$ — матрица перехода от f_i к f'_i
   $$U = (u_{ij}), \qquad U = D^T C$$
   Докажем, что $U = E$
   $$e'_i = c_{1i}e_1 + c_{2i}e_2 + \dots, \qquad f'_j = d_{1j}f_1 + d_{2j}f_2 + \dots$$
   Применим одно к другому:
   $$\left.\begin{matrix} 1, & i = j \\ 0, & i \neq j \end{matrix}\right\} = f'_j(e'_i) = d_{1j}f_1(c_{1i}e_1 + c_{2i}e_2 + \dots) + d_{2j}f_2(c_{1i}e_i + c_{2i}e_2 + \dots) + \dots =$$
   $$= d_{1j}c_{1i} \cdot 1 + d_{1j}c_{2i} \cdot 0 + \dots + d_{2j}c_{1i} \cdot 0 + d_{2j}c_{2i} \cdot 1 + \dots = d_{1j}c_{1i} + d_{2j}c_{2i} + \dots$$
   d — этой j-я строка D^T, $\quad c$ — i-й столбец C
   Значит, $f'_j(e'_i) = u_{ji}$
2. $(C^{-1})^T$ — 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. $\mathscr{A}$ — оператор в евклидовом или унитарном пространстве
$\mathscr{B}$ называется *сопряжённым* к $\mathscr{A}$, если $(\mathscr{A}x, y) = (x, \mathscr{B}y) \quad \forall x, y$

Обозначение. $\mathscr{A}^*$

Свойства.

1. $\mathscr{A}^{**} = \mathscr{A}$
2. Пусть A, A^* — матрицы $\mathscr{A}, \mathscr{A}^*$ 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 $\mathscr{A}^*\mathscr{A} = \mathscr{A}\mathscr{A}^*$
- *ортогональным* (*унитарным*), если $\mathscr{A}\mathscr{A}^* = \mathscr{A}^*\mathscr{A} = \mathscr{E}$
- *самосопряжённым*, если $\mathscr{A}^* = \mathscr{A}$

Определение 29. Квадратная матрица называется

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

- *эрмитовой*, если $A = \overline{A}^T$

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

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

Доказательство.

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

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

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

□

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

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

Теорема 20 (о собственных числах самосопряжённого оператора)**.**
$\mathscr{A}$ — оператор на унитарном пространстве

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

Доказательство.

1. Знаем, что существует ОНБ из с. в.
   Пусть λ_i — с. ч.
   A, A^* — матрицы $\mathscr{A}$ и $\overline{\mathscr{A}^*}$ в этом базисе $\implies A^* = \overline{A^T}$
   $\mathscr{A}$ — самосопряжённый $\iff A = A^* \iff A = \overline{A^T} \iff$

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

2. Пусть e_i — ОНБ из с. в., λ_i — с. ч., $\lambda_i \in \mathbb{R}$
   Пусть $x = a_1 e_1 + ... + a_n e_n$

$$(\mathscr{A}x, x) = (a_1\lambda_1 e_1 + ... + a_n\lambda_n e_n, \quad a_1 e_1 + ... + a_n e_n) = \sum \lambda_i a_i \overline{a_j} \underbrace{(e_i, e_j)}_{0 \text{ или } 1} =$$

$$= \sum \lambda_i a_i \overline{a_i} = \sum \lambda_i |a_i|^2 \in \mathbb{R}$$

- Если $\lambda_i > 0 \quad \forall i$, то $\sum \underbrace{\lambda_i}_{>0} |a_i|^2 \geq 0$
  Равенство достигается только при $|a_i|^2 \in \odot$, то есть $a_i \in \odot$. Значит, $x = 0$
- Пусть не все $\lambda_i > 0$, $\lambda_{i_0} \leq 0$
  Для $x = e_{i_0} \quad x \neq 0, \quad (\mathscr{A}x, x) = \lambda_{i_0} \leq 0$ — ↯

□

Лемма 8. A — эрмитова матрица
Тогда все корни $\chi_A(t)$ вещественны

Доказательство. A — матрица порядка n

Определим оператор $\mathscr{A} : \mathbb{C}^n$ как $X \mapsto AX$
Тогда A — матрица $\mathscr{A}$ в стандартном базисе
A — эрмитова; станд. базис является ОНБ $\implies \mathscr{A}$ — самосопряжённый
Все с. ч. $\mathscr{A}$ вещественны, это и есть корни $\chi_A(t)$ □

Лемма 9 (ортогональность с. в.). $\mathscr{A}$ самосопряжённый на $\mathbb{R}^n$, μ, λ — различные с. ч., x, y — соответствующие с. в.
Тогда $(x, y) = 0$

Доказательство.

$$\lambda(x,y) \xlongequal[\text{линейность}]{} (\lambda x, y) \xlongequal[\text{с. в.}]{} (\mathscr{A}x, y) \xlongequal{\text{def } \mathscr{A}^*} (x, \mathscr{A}^* y) \xlongequal[\text{самоспр.}]{} (x, \mathscr{A}y) \xlongequal[\text{с. в.}]{} (x, \mu x) \xlongequal[\text{линейность}]{} \mu(x,y)$$

□

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

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

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

Доказательство.

1. Разложим $\chi_A(t)$ на линейные множиетли над $\mathbb{C}$:
$$\chi_A(t) = (-1)^n (t - \lambda_1)...(t - \lambda_n), \qquad \lambda_i \in \mathbb{C}$$
Пусть A — матрица $\mathscr{A}$ в стандартном базисе $\implies A = A^T \xRightarrow[A \text{ вещ.}]{} A = \overline{A^T} \implies$
$\implies A$ эрмитова $\xRightarrow[\text{лемма 8}]{} \lambda_i \in \mathbb{R} \quad \forall i$
2. $\mathscr{A}$ 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). $\mathscr{A}$ — положительно определённый самосопряж.
Тогда существует положительно определённый самосопряжённый $\mathscr{B} : \quad \mathscr{A} = \mathscr{B}^2$

Доказательство. $\mathscr{A}$ — самосопряжённый $\implies \mathscr{A}$ — нормальный $\implies \exists$ ОНБ из с. в. $\mathscr{A}$
Пусть $e_1, ..., e_n$ — ОНБ из с. в., $\lambda_1, ...\lambda_n$ — с. ч.
$\mathscr{A}$ — самоспряжённый $\implies \lambda_i \in \mathbb{R}$
$\mathscr{A}$ — полож. опред. $\implies \lambda_i > 0$

Определим $\mathscr{B}$ как $\mathscr{B}(e_i) = \sqrt{\lambda_i} e_i$
Проверим, что он подойдёт:
Рассмотрим матрицу $\mathscr{B}$ в базисе $e_1, ..., e_n$:

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

Она эрмитова $\implies$ $\mathscr{B}$ самосопряжённый
$\sqrt{\lambda_i} > 0 \implies \mathscr{B}$ положиетльно определён

$$\mathscr{B}\big(\mathscr{B}(e_i)\big) = \mathscr{B}(\sqrt{\lambda_i} e_i) = \lambda_i e_i = \mathscr{A}(e_i) \quad \forall i \qquad \implies \mathscr{B}^2 = \mathscr{A}$$

□

Лемма 10. $\mathscr{A}$ невырожденный
Тогда $\mathscr{A}\mathscr{A}^*$ — самосопряжённый положительно определённый

Доказательство.

$$\left(\mathscr{A}\mathscr{A}^*\right)^* = \left(\mathscr{A}^*\right)^* \mathscr{A}^* = \mathscr{A}\mathscr{A}^*$$

$$\left(\mathscr{A}^*\mathscr{A}x, x\right) = \left(\mathscr{A}^*(\mathscr{A}x), x\right) = \left(\mathscr{A}x, (\mathscr{A}^*)^* x\right) = (\mathscr{A}x, \mathscr{A}x) \underset{\mathscr{A}x \neq 0, \text{ т. к. } \mathscr{A} \text{ невырожд.}}{>} 0$$

□

Теорема 23 (полярное разложение оператора).
$\mathscr{A}$ — невырожденный оператор на унитарном пространстве
Тогда $\exists\, \mathscr{U}, \mathscr{B}$ такие, что:

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

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

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

$\mathscr{A}^*, \mathscr{A}$ невырожденные $\implies$ $\mathscr{A}^*\mathscr{A}$ невырожденный $\implies$ $\mathscr{B}$ невырожденный $\implies \exists\, \mathscr{B}^{-1}$
Положим $\mathscr{U} = \mathscr{A}\mathscr{B}^{-1}$
Докажем, что эти $\mathscr{U}, \mathscr{B}$ подойдут:
Осталось проверить только унитарность, т. е. что $\mathscr{U}^* \overset{?}{=} \mathscr{U}$

$$\mathscr{U}^* = \left(\mathscr{A}\mathscr{B}^{-1}\right)^* = \left(\mathscr{B}^{-1}\right)^* \mathscr{A}^* \underset{\text{видно из матрицы}}{=\!=\!=\!=} \left(\mathscr{B}^*\right)^{-1} \mathscr{A}^* \underset{\mathscr{B} \text{ самоспр.}}{=\!=\!=} \mathscr{B}^{-1}\mathscr{A}^*$$

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

□

Следствие (перестановка сомножителей). $\mathscr{A}$ — невырожденный оператор
Тогда $\exists$ унитарный $\mathscr{U}$ и самосопряжённый положительно определённый $\mathscr{B}$ такие, что $\mathscr{A} = \mathscr{B}\mathscr{U}$

Доказательство. Применим теорему к $\mathscr{A}^*$:
$\mathscr{A}^* = \mathscr{U}_1\mathscr{B}, \qquad \mathscr{U}_1$ — унитарный, $\quad \mathscr{B}$ — самосопряжённый пол. опред.

$$\mathscr{A} = \left(\mathscr{A}^*\right)^* = \left(\mathscr{B}\mathscr{U}_1\right)^* = \mathscr{U}_1^*\mathscr{B}^* = \mathscr{U}_1^*\mathscr{B}$$

Подойдёт $\mathscr{U} = \mathscr{U}_1$ □

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^TAC — диагональная, то на диагонали матрицы C^TAC записаны с. ч. матрицы A

Доказательство.

1. $\mathscr{A}$ — оператор на $\mathbb{R}^n$, $\quad A$ — его матрица в стандартном базисе
   $\mathscr{A}$ самосопряжённый $\implies \exists$ ОНБ $T_1, ..., T_n$ из с. в.
   Пусть $\lambda_1, ..., \lambda_n$ — с. ч.
   Матрица $\mathscr{A}$ в $T_1, ..., T_n$ является диагональной
   Матрица $\mathscr{A}$ в $T_1, ..., T_n$ 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, $\quad \mu_1, \ldots, \mu_n$ — числа на диагонали
   $S_1, ..., S_n$ — столбцы $B \quad \implies \quad B = C^{-1}AC \implies B$ — матрица $\mathscr{A}$ в ОНБ $S_1, ..., S_n \implies \mathscr{A}S_i = \mu_i S_i \implies \mu_i$ — с. ч.

□

Теорема 25 (преобразование двух форм).
$f(x_1, ..., x_n)$, $\quad g(x_1, ..., x_n)$ — вещественные квадратичные формы, $\quad$ ***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:
$$f_1(y_1, ..., y_n) = \lambda_1 y_1^2 + ... + \lambda_n y_n^2, \qquad \lambda_i > 0$$
2. Избавимся от λ:
$$z_i = \sqrt{\lambda_i} y_i$$
$$f_2(z_1, ..., z_n) = z_1^2 + ... + z_n^2$$
   При этом, g_2 тоже как-то изменилась:
$$g_2(z_1, ..., z_n)$$
   Нужно доказать, что форму $f_2 = z_1^2 + ... + z_n^2$ и любую форму g_2 можно одновеременно привести к диагоналному виду
3. Приведём g_2 к диагональному виду ортогональным преобразованием C
   Матрица f_2 равна E
$$E \to C^TEC = C^TC = E$$
   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 $I \neq \{0\}, \quad a$ — 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. $\exists b : b \in I, \quad b \not\vdots\, a$
     Поделим с остатком:
     $$b = aq + r, \qquad a < r < a$$
     $$r = b - aq = \underbrace{b}_{\in I} + (-q)\underbrace{a}_{\in I} \in I \quad \lightning$$
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, $\quad I$ — идеал
Элементы a и b называются *сравнимыми по модулю* I, если $a - b \in I$

Обозначение. $a \equiv b \pmod I \qquad a \underset{I}{\equiv} b$

Свойство. $\underset{I}{\equiv}$ 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, $\quad I$ — идеал
На множестве классов эквивалентности по отношению $\underset{I}{\equiv}$ введём операции сложения и умножения:
$$\overline{x} + \overline{y} = \overline{x + y}, \qquad \overline{x} \cdot \overline{y} = \overline{xy}$$

Теорема 27 (факторкольцо)**.** A — коммутативное ассоциативное кольцо, $\quad I$ — 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.
$$\left.\begin{aligned} &x_1, x_2 \text{ в одном классе} \\ &y_1, y_2 \text{ в одном классе} \end{aligned}\right\} \overset{?}{\implies} \begin{cases} x_1 + y_1 \text{ и } x_2 + y_2 \text{ в одном классе} \\ x_1 y_1 \text{ и } x_2 y_2 \text{ в одном классе} \end{cases}$$
Пусть $x := x_1 - x_2, \quad y := y_1 - y_2 \qquad \implies x, y \in I$
$$(x_1 + y_1) - (x_2 + y_2) = x + y \in I$$
$$x_1 y_1 - x_2 y_2 = (x + x_2)(y + y_2) - x_2 y_2 = xy + y_2 x + x_2 y \in I$$

2. ${}^{A}\!/_{I}$ — абелева группа (по т. о факторгруппе)
Нужно доказать, что $(\overline{x} + \overline{y})\overline{z} = \overline{xz} + \overline{yz}$
Выберем $x \in \overline{x}, \quad y \in \overline{y}, \quad z \in \overline{z}$
$$(\overline{x} + \overline{y})\overline{z} = \overline{xz} + \overline{yz} \quad \Longleftarrow \quad \overline{(x + y)z} = \overline{xz + yz}$$
Остальное — аналогично
Если A — кольцо с единицей, то $\overline{1}$ — 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 $X \in A/_I, \quad x \in X$
Тогда $X = 0 \iff \overline{x} = \overline{0} \iff x \underset{I}{\equiv} 0 \iff x - 0 \in I \iff x \in I$

- $\implies$

  Пусть $X, Y \in A/_I, \qquad XY = \overline{0}$

  Пусть $x \in X, \quad y \in Y \implies \overline{xy} = \overline{0} \implies xy \in I \xRightarrow[I \text{ простой}]{} \left[\begin{array}{l} x \in I \implies X = \overline{0} \\ y \in I \implies Y = \overline{0} \end{array}\right.$

- $\impliedby$

  Пусть $xy \in I \implies \overline{xy} = \overline{0} \implies \overline{x} \cdot \overline{y} = \overline{0} \xRightarrow[\text{обл. цел.}]{} \left[\begin{array}{l} \overline{x} = 0 \implies x \in I \\ \overline{y} = 0 \implies y \in I \end{array}\right.$

□

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

Теорема 29 (факторкольцо по максимальному идеалу).
A — коммутативное ассоциативное кольцо с единицей, $\qquad I$ — идеал

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

Доказательство.

- $\implies$

  $A/_I$ — коммутативное ассоциативное кольцо с единицей
  Осталось доказать, что $\forall X \in A/_I, \; X \neq \overline{0} \quad \exists X^{-1}$

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

  Пусть $x \in X$
  Пусть $J := \langle x, I \rangle$

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

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

  $$\implies 1 \underset{I}{\equiv} bx \implies \overline{1} = \overline{b} \cdot \overline{x} = \overline{b} X \implies \overline{b} = X^{-1}$$

- $\impliedby$

  Пусть J — идеал, $I \subset J, \; I \neq J$
  Докажем, что $J = A$:
  Пусть $x \in J \setminus I$

  $$\overline{x} \in A/_I, \qquad \overline{x} \neq \overline{0} \quad \implies \exists Y : \overline{x} Y = \overline{1}$$

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

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

$\square$

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 $J = \langle Q(x) \rangle$

$$\langle P(x) \rangle \subset \langle Q(x) \rangle \implies P(x) \,\vdots\, Q(x) \xrightarrow[P \text{ неприводимый}]{}$$

$$\implies \left[\begin{array}{l} Q(x) = cP(x), \quad c \in K, \quad c \neq 0 \implies J = I \\ Q(x) = c, \quad c \in K, \quad c \neq 0 \implies J = A \end{array}\right. \implies I \text{ максимальный}$$

- $\impliedby$
  Пусть P приводим

$$\implies \exists Q(x): \quad P(x) \,\vdots\, Q(x), \qquad Q(x) \neq cP(x), \quad Q(x) \neq c$$

$$\implies \langle P(x) \rangle \subsetneq \langle Q(x) \rangle \subsetneq A \implies I \text{ не максимальный}$$

$\square$

32. Гомоморфизм колец. Теорема о гомоморфизме

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

$$f(x +_A y) = f(x) +_B f(y)$$

$$f(x \cdot_A y) = f(x) \cdot_B f(y)$$

Определение 41. Отображение $f : A \to B$ 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, $f : A \to B$ — 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, $f : A \to B$ - 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. $0_A \in \ker f$

- $x, y \in \ker f \implies f(x+y) = \underbrace{f(x)}_{0} + \underbrace{f(y)}_{0} = 0 + 0 = 0$
- $\underbrace{f(0)}_{0} = f\big(x + (-x)\big) = \underbrace{f(x)}_{0} + f(x) \implies f(-x) = 0$
- $a \in A \qquad f(ax) = f(a)f(x) = f(a) \cdot 0 = 0$

3. $\operatorname{Im} f \subset B$
   Нужно преверить, что $\operatorname{Im} f$ замкнут относительно операции
   Для сложения — можно сослаться на группы
   Для умножения:
$$x, y \in \operatorname{Im} f \implies a, b \in A : \quad f(a) = x, \quad f(b) = y$$
$$\implies xy = f(a)f(b) = f(ab) \in \operatorname{Im} f$$

□

Теорема 31 (о гомоморфизме колец). A, B — коммутативные ассоциативные кольца
$f : A \to B$ — гомоморфизм
$$A/_{\ker f} \simeq \operatorname{Im} f$$

Доказательство. Определим $\varphi : A/_{\ker f} \to \operatorname{Im} f : \quad \varphi(X) = f(x)$ для некоторого $x \in X$.

- Корректность:
  Пусть $x, x' \in X$
  Проверим, что $f(x') = f(x)$
$$\overline{x} = \overline{x'} \implies x \underset{\ker f}{\equiv} x' \implies x - x' \in \ker f \implies f(x) = f\big(x' + (x - x')\big) = f(x') + \underbrace{f(x - x')}_{0 \ (x - x' \in \ker f)}$$

- Гомоморфизм:
$$X, Y \in A/_{\ker f}, \qquad x \in X, \quad y \in Y$$
$$X = \overline{x}, \quad Y = \overline{y}, \qquad X + Y = \overline{x + y}, \quad XY = \overline{xy}$$
$$\varphi(X + Y) = \varphi(\overline{x + y}) = f(x + y) \xlongequal[f \text{ гомоморф.}]{} f(x) + f(y) = \varphi(\overline{x}) + \varphi(\overline{y}) = \varphi(\overline{x} + \overline{y})$$
  Для умножения — то же самое

- Сюръективность:
  Пусть $b \in \operatorname{Im} f \quad \implies \quad \exists x \in A : \quad f(x) = b \quad \implies \quad \varphi(\overline{x}) = b$

- Инъективность:
  Пусть $\varphi(X) = \varphi(Y), \quad x \in X, \ y \in Y$
$$\implies f(x) = f(y) \implies f(x - y) = 0 \implies x - y \in \ker f \implies \overline{x} \underset{\ker f}{\equiv} y \implies \overline{x} = \overline{y} \implies X = Y$$

□

33. Характеристика кольца и поля. Классификация простых полей

Определение 44. A — кольцо
Характеристикой A называется 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. $\operatorname{char} A$

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

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

Доказательство. Нужно доказать, что

$$\underbrace{a+a+\dots+a}_{n} = 0 \quad \forall a \in A \qquad \Longleftrightarrow \qquad \underbrace{1+1+\dots+1}_{n} = 0$$

- $\Longrightarrow$
  Подставим $a = 1$
- $\Longleftarrow$
  $$a+a+\dots+a = a(1+\dots+1) = a \cdot 0 = 0$$

□

Свойство. A — поле
Тогда $\operatorname{char} A = 0$ или $\operatorname{char} A \in \mathbb{P}$

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

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

$$0 = \underbrace{1+\dots+1}_{n} = (\underbrace{1+\dots+1}_{m})(\underbrace{1+\dots+1}_{k}) \Longrightarrow \left[\begin{array}{l} \underbrace{1+\dots+1}_{m} = 0 \\ \underbrace{1+\dots+1}_{k} = 0 \end{array}\right.$$

Получили противоречие с минимальностью n □

Определение 45. L — поле, $\quad K \subset L, \quad K$ является полем с теми же операциями
Тогда K называется *подполем* L, $\quad L$ 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 $\mathbb{Q}$ $\quad \Longrightarrow 0, 1 \in K$
     $$\underbrace{1+1+\dots+1}_{n} \in K \quad \forall n \qquad \Longrightarrow \mathbb{N} \subset K$$
     Если $n \in K$, то $-n \in K \quad \Longrightarrow \mathbb{Z} \subset K$
     Если $n \in K$, $n \neq 0$, то $\frac{1}{n} \in K \quad \Longrightarrow \frac{1}{n} \in K \quad \forall n \in \mathbb{N}$
     $$m \in \mathbb{Z},\ n \in \mathbb{N} \Longrightarrow \frac{m}{n} = m \cdot \frac{1}{n} \in K \qquad \Longrightarrow \mathbb{Q} = K$$
   - $\mathbb{Z}_p$
     Аналогично, пусть K — подполе $\mathbb{Z}_p$
     $$\overline{1} \in K$$
     $$\underbrace{\overline{1}+\overline{1}+\dots+\overline{1}}_{n} \in K \quad \forall n \qquad \Longrightarrow \overline{n} \in K \quad \forall n \qquad \Longrightarrow \mathbb{Z}_p = K$$

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 $f : \mathbb{Z} \to A$ такое, что

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

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. Знаем, что $1^n * 1^k = 1^{n+k}$, где $*$ — это $+$
- $f(nk) = f(n) \cdot f(k)$:
  - $n, k > 0$
  $$(\underbrace{1 + \dots + 1}_{n})(\underbrace{1 + \dots + 1}_{k}) = \underbrace{1 \cdot 1 + \dots + 1 \cdot 1}_{nk} = \underbrace{1 + \dots + 1}_{nk}$$
  - $n = 0$
  $$f(0) = f(0)f(k)$$
  - $n > 0,\ k < 0$
  Положим $k_1 \coloneqq -k$
  $$f\Big(n(-k_1)\Big) = f(n)f(-k_1) \quad \Longleftarrow \quad -f(nk_1) = f(n)\Big(-f(k_1)\Big)$$

По теореме о гомоморфизме $\operatorname{Im} f \simeq \mathbb{Z}/_{\ker f}$
$\operatorname{Im} f$ — подкольцо $A \quad \Longrightarrow \operatorname{Im} f = A$ (из минимальности A)
$\ker f$ — идеал $\Longrightarrow \ker f = \langle m \rangle$

- $m = 0$
$$\ker f = \{ 0 \} \Longrightarrow \mathbb{Z}/_{\ker f} = \mathbb{Z}/_{\{ 0 \}} \simeq \mathbb{Z}$$
- $m \neq 0$
$$\operatorname{Im} f \simeq \mathbb{Z}/_{\langle m \rangle} \simeq \mathbb{Z}_m$$

$\operatorname{Im} f$ — подкольцо поля $K \Longrightarrow \operatorname{Im} f$ — область целостности
$\Longrightarrow \langle m \rangle$ — простой идеал $\Longrightarrow m \in \mathbb{P}$

□

34. Степень расширения. Мультипликативность степени, следствия

Лемма 11 (корректность). K — поле, $\quad L$ — расширение K
Тогда L является векторным пространством над K

Доказательство.

- Операции:
  - $l_1 + l_2, \quad l_1, l_2 \in L$
  - $kl, \quad k \in K,\ l \in L$

k, l — элементы L, для них операции определены

- L — абелева группа по сложению:
$$(k_1k_2)l = k_1(k_2l)$$

$\square$

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 $g_{ij} := e_if_j$ ЛНЗ над K:
Пусть $a_{ij} \in K : \sum a_{ij}g_{ji} = 0$
$$a_{11}e_1f_1 + a_{12}e_1f_2 + \dots + a_{21}e_2f_1 + a_{22}e_2f_2 + \dots\dots\dots = 0$$
Сгруппируем по элементам f:
$$\Big(a_{11}e_1f_1 + a_{21}e_2f_1 + \dots\Big) + \Big(a_{12}e_1f_2 + a_{22}e_2f_2 + \dots\Big) + \dots\dots\dots = 0$$
$$\underbrace{(a_{11}e_1 + a_{21}e_2 + \dots)}_{\in M}f_1 + \underbrace{(a_{12}e_1 + a_{22}e_2 + \dots)}_{\in M}f_2 + \dots\dots\dots = 0$$
Пусть $b_j := a_{1j}e_1 + a_{2j}e_2 + \dots + a_{rj}e_r$
Тогда $b_j \in M$, $\quad b_1f_1 + \dots b_sf_s = 0$
$f_1, \dots f_s$ 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, $\quad f_1, \dots, f_s$ — базис L над M
Докажем, что $g_{ij} := e_if_j$ — базис L над K:
ЛНЗ уже доказана. Осталось доказать, что любой элемент порождается g_{ij}:
Пусть $c \in L \quad \implies \exists b_i \in M : \quad c = b_1f_1 + \dots + b_sf_s$
$$b_j \in M, \quad e_i \text{ порожд. } M \text{ над } K \implies \forall j \quad \exists a_{ij} : \quad b_j = a_{1j}e_1 + \dots + a_{rj}e_r$$
$$\implies c = \sum a_{ij}e_if_j = \sum a_{ij}g_{ij}$$

- Бесконечный случай
Нужно доказать, что $\forall N \quad \exists N$ ЛНЗ 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_if_j ЛНЗ над K

$\square$

Следствие. L — конечное расширение над K, $\quad K \subset M \subset L$
Тогда $|M : K|$ и $|L : M|$ — делители $|L : K|$

Следствие. L — конечное расширение K, $\quad |L : K|$ — простое число
$$\implies \nexists M : \quad K \subset M \subset L, \quad M \neq K, \ M \neq L$$

Следствие. $K \subset M \subset L$

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

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

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

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

Доказательство.

1. $$F(x) = P(x)Q(x) + R(x), \qquad \deg R < \deg P$$
   - $\Longleftarrow$
   $$F(x) \,\vdots\, P(x) \implies R(x) = 0$$
   $$F(x) = P(x)Q(x)$$
   Подставим α:
   $$F(\alpha) = \underbrace{P(\alpha)}_{0} Q(x) = 0$$
   - $\implies$
   $$\underbrace{P(\alpha)}_{0} Q(\alpha) + R(\alpha) = 0$$
   $$R(\alpha) = 0 \implies R \text{ — нулевой}$$
2. Пусть $P_1 P_2$ — минимальные
$$\xrightarrow[\text{св-во 1}]{} \begin{cases} P_1(x) \,\vdots\, P_2(x) \\ P_2(x) \,\vdots\, P_1(x) \end{cases} \implies P_1(x) = P_2(x)$$

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

$$0 = P(\alpha) = \underbrace{S(\alpha)}_{\in L}\underbrace{T(\alpha)}_{\in L} \xrightarrow[L\,-\,\text{поле}]{} \left[\begin{array}{l} S(\alpha) = 0 \\ T(\alpha) = 0 \end{array}\right. \qquad \lightning \quad \text{миним. } \deg P$$

4.

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

$\square$

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, $\quad n \coloneqq |L : K|, \quad \alpha \in L$.
Докажем, что α — алгебраическое:
Элементы $\underbrace{1, \alpha, \ldots, \alpha^{n-1}, \alpha^n}_{n+1} \in L$ ЛЗ над K, т. е.

$$\exists\, k_0, k_1, \ldots, k_{n-1} k_n \in K \notin \odot : \quad k_0 \cdot 1 + k_1\alpha + \cdots + k_{n-1}\alpha^{n-1} + k_n\alpha^n = 0$$

Пусть $P(x) = k_0 + k_1 x + \cdots + k_{n-1}x^{n-1} + k_n x^n$.
Тогда $P(x) \in K[x], \quad P(x)$ — ненулевой, $\quad P(\alpha) = 0 \quad \implies \alpha$ — алгебраичсекое. $\square$

36. Строение простого алгебраического расширения. Следствия

Определение 52. L — поле, $\qquad K$ — подполе L, $\qquad \alpha_1, \ldots \alpha_n \in L$
Через $K(\alpha_1, \ldots, \alpha_n)$ будем обозначать наименьшее подполе L, содержащее K и $\alpha_1, \ldots, \alpha_n$.
Если $M = K(\alpha_1, \ldots \alpha_n)$, то говорят, что M получено из K *присоединением* $\alpha_1, \ldots, \alpha_n$.
Поле, полученное из K присоединением одного элемента, называется *простым расширением* K.

Теорема 35 (строение простого алгебраического расширения). L — поле, $\qquad K$ — подполе L
$\alpha \in L, \qquad \alpha$ алг. над $K, \qquad P(x)$ — минимальный многочлен для α над K

1. $K[x]/\langle P(x)\rangle \simeq K(\alpha), \qquad \overline{F(x)} \mapsto F(\alpha)$ является изоморфизмом.
2. $K(\alpha)$ конечно над $K, \qquad |K(\alpha) : K| = \deg P, \qquad 1, \alpha, \ldots, \alpha^{n-1}$ образуют базис $K(\alpha)$ над K.

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

$$f(c_0 + c_1 x + \ldots c_k x^k) = c_0 + c_1\alpha + \cdots + c_k\alpha^k, \qquad c_i \in K$$

- 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 $\ker f$:

$$F(x) \in \ker f \iff f(F) = 0 \iff F(\alpha) = 0 \iff F(x) \vdots P(x)$$
$$\implies \ker f = \langle P(x)\rangle$$

- Применим теорему о гомоморфизме:

$$\operatorname{Im} f \simeq {}^{K[x]}\!\diagup_{\ker f}$$

Изоморфизм $\varphi(\overline{F}) = f(F) = F(\alpha)$
Получили изоморфизм ${}^{K[x]}\!\diagup_{\langle P(x)\rangle} \to \operatorname{Im} f$

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

$K(\alpha)$ — минимальное, содержащее K и α.
$\operatorname{Im} f$ тоже содержит K и α.
Значит, $\operatorname{Im} f = K(\alpha)$.

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

Пусть $n \coloneqq \deg P$

  – ЛНЗ:
  Пусть ЛЗ:

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

  Пусть $F(x) \coloneqq a_0 + a_1x + \dots + a_{n-1}x^{n-1} \implies F(\alpha) = 0$

$$\implies F(x) \vdots P(x) \xRightarrow[F(x)\text{ — ненулевой}]{} \deg F \geq \deg P = n \quad \lightning$$

  – Порождающий:

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

  Пусть $u \in K(\alpha) \implies \exists\, F \in K[x]: \quad f(F) = u \quad \implies F(\alpha) = u$
  Делим с остатком:

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

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

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

$$R(x) = a_0 + a_1x + \dots a_{n-1}x^{n-1} \implies F(\alpha) = a_0 + a_1\alpha + \dots a_{n-1}\alpha^{n-1}$$

$\square$

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

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

Доказательство. Обозначим $K_0 \coloneqq K, \quad K_i \coloneqq K(\alpha_1, \dots, \alpha_i)$.

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

Достаточно доказать, что K_{i+1} кончено 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. $\square$

Следствие. α, β алгебраичны над K
$\implies \alpha + \beta, \quad \alpha - \beta, \quad \alpha\beta, \quad {}^{\alpha}\!/\!_{\beta}$ алгебраичны над K

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

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

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

Введём отношение эквивалентности:
Если

$$s = a_0 + a_1X + \dots, \qquad t = b_0 + b_1X + \dots$$
$$S(x) \coloneqq a_0 + a_1x + \dots, \qquad T(x) \coloneqq b_0 + b_1x + \dots$$

и $S(x) - T(x) \,\vdots\, P(x)$, то $s \sim t$.
Определим на множестве классов элквивалентности сложение и умножение:
Если

$$s = a_0 + a_1X + \dots, \qquad t = b_0 + b_1X + \dots, \qquad u = c_0 + c_1X + \dots$$
$$S(x) = a_0 + a_1x + \dots, \qquad T(x) = b_0 + b_1x + \dots, \qquad U(x) = c_0 + c_1x + \dots$$

и $S(x)T(x) - U(x) \,\vdots\, P(x)$, то положим $u \coloneqq st$.
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. $P(x) \mapsto \overline{P(x)} = 0$). ☐

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

Теорема 37 (эквивалентные простые расширения). α, β — алгебраические над K, их минимальные многочлены совпадают.
Тогда $K(\alpha)$ и $K(\beta)$ эквивалентны, причём существует изоморфизм $f : K(\alpha) \to K(\beta)$ такой, что

$$f\big|_K = \mathrm{id}, \quad f(\alpha) = \beta$$

Доказательство. Пусть $P(x)$ — минимальный многочлен для α и β, $\quad n \coloneqq \deg P$.
Элементы $K(\alpha)$ — это $u_0 + u_1\alpha + \dots + u_{n-1}\alpha^{n-1}$.
Положим

$$f(u_0 + u_1\alpha + \dots + u_{n-1}\alpha^{n-1}) \coloneqq u_0 + u_1\beta + \dots + u_{n-1}\beta^{n-1}$$

Пусть

$$s = u_0 + u_1\alpha + \dots, \qquad t = v_0 + v_1\alpha + \dots$$
$$S(x) = u_0 + u_1x + \dots, \qquad T(x) = v_0 + v_1x + \dots$$

Пусть $R(x) = w_0 + w_1x + \dots + w_{n-1}x^{n-1}$ — такой, что $S(x)T(x) - R(x) \,\vdots\, P(x)$

$$r = w_0 + w_1\alpha + \dots + w_{n-1}\alpha^{n-1}$$

Тогда $s = S(\alpha), \quad t = T(\alpha), \quad r = R(\alpha)$

$$f(s) = S(\beta), \qquad f(t) = T(\beta), \qquad f(r) = R(\beta)$$

$$st = S(\alpha)T(\alpha) \xlongequal[ST-R\vdots P]{} R(\alpha) = r^2$$

$$f(ST) = f(r) = R(\beta)$$

$$f(s)f(t) = S(\beta)T(\beta) = R(\beta)$$

Сложение — аналогично.
Биективность:

- Инъективность:

$$u_0 + u_1\alpha + \dots \to 0$$

$$u_0 + u_1\beta + \dots = 0$$

$$\implies u_i = 0$$

- Сюръективность:
  Любой элемент $K(\beta)$ — это $u_0 + u_1\beta + \dots$

□

38. Поле разложения многочлена: существование, эквивалентность

Определение 54. K — поле, $\quad P(x) \in K[x]$.
Полем разложения $P(x)$ называется такое расширение L поля K, что в L многочлен $P(x)$ раскладывается на линейные множители

$$P(x) = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n), \qquad a \in K, \quad \alpha_i \in L$$

и $L = K(\alpha_1, \dots, \alpha_n)$.

Теорема 38 (существование поля разложения)**.** K — поле, $\quad P(x) \in K[x]$.

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, $\quad M = K$

- **Переход** к n:
  Разложим $P(x)$ на неприводимые над K:

$$P(x) = P_1(x) \dots P_k(x)$$

  Присоединим корень α многочлена $P_1(x)$, получим $K(\alpha)$.
  $K(\alpha)$ — поле, в нём верна теорема Безу:

$$P_1(x) \vdots x - \alpha \text{ в } K(\alpha)[x]$$

$$P_1(x) = (x-\alpha)Q(x)$$

$$P(x) = (x-\alpha)\underbrace{Q(x)P_2(x)\dots P_k(x)}_{H(x)} = (x-\alpha)H(x)$$

  Применим **предположение индукции** к $K(\alpha)$ и $H(x)$:
  Существует M, в котором $H(x)$ раскладывается на линейные множиетели, $K(\alpha) \subset M$.

Это M подходит для K и $P(x)$.
Поле разложения — минимальное подполе M, содержащее K и $\alpha_1, \dots, \alpha_n$, т. е. $L = K(\alpha_1, \dots, \alpha_n)$.

$\square$

Теорема 39 (эквивалентность полей разложения многочлена). K — поле, $\quad P \in K[x]$
L, M — поля разложения.

1. L и M эквивалентны над K;
2. можно выбрать такие $\alpha_i \in L, \quad \beta_i \in M$ такие, что

$$P(x) = \underset{\in K}{a}(x-\alpha_1)\cdots(x-\alpha_n), \qquad P(x) = \underset{\in K}{b}(x-\beta_1)\cdots(x-\beta_n)$$

для которых существует изоморфизм $f : L \to M, \quad f(\alpha_i) = \beta_i, \quad f\big|_K = \mathrm{id}$

Доказательство. Строим последовательно $\alpha_1, \dots, \alpha_s, \quad \beta_1, \dots, \beta_s$.

$$f_s : K(\alpha_1, \dots, \alpha_s) \to K(\beta_1, \dots, \beta_s) : \quad f(\alpha_i) = \beta_i$$

Пусть построены $\alpha_1, \dots, \alpha_s, \quad \beta_1, \dots, \beta_s, \quad f_s$.
Положим $L' = K(\alpha_1, \dots, \alpha_s), \quad M' = K(\beta_1, \dots, \beta_s)$
(на первом шаге считаем, что $L' = M' = K, \quad f_0 = \mathrm{id}$)
Разложение $P(x)$ на неприводимые над L'

$$P(x) = (x-\alpha_1)\cdots(x-\alpha_s)Q_1(x)Q_2(x)\cdots$$

$$f_s = L' \to M'$$

$$P(x) = f_s(P(x)) = (x-\beta_1)\cdots(x-\beta_s)R_1(x)R_2(x)\cdots, \qquad R_i(x) = f_s(Q_i(x))$$

$R_i(x)$ неприводимы

- Если $Q_i(x)$ — линейный, обозначим его корень $\alpha_{s+1}, \quad \beta_{s+1} \coloneqq f(\alpha_{s+1})$

$$f_s\big(Q_i(x)\big) = (x - \beta_{s+1})$$

$$f_{s+1} \coloneqq f_s$$

- Если нет линейных, то положим α_{s+1} — корень $Q_1(x), \quad \beta_{s+1}$ — корень $R_1(x)$

$$L'(\alpha_{s+1}) \simeq {}^{L'(x)}\!\big/\!{}_{\langle Q_1(x)\rangle} \simeq {}^{M'(x)}\!\big/\!{}_{\langle R_1(x)\rangle} \simeq M'(\beta_{s+1})$$

Отображение

$$\varphi : {}^{L'[x]}\!\big/\!{}_{\langle Q_1(x)\rangle} \to {}^{M'[x]}\!\big/\!{}_{\langle R_1(x)\rangle} : \qquad \varphi\big(\overline{H}(x)\big) = \overline{f_{s+1}\big(H(x)\big)}$$

является изоморфизмом. Существуют изоморфизмы

$$\varphi_1 : {}^{L'[x]}\!\big/\!{}_{\langle Q_1(x)\rangle} \to L'(\alpha_{s+1}) : \quad \varphi_1(\overline{x}) = \alpha_{s+1}$$

$$\varphi_2 : {}^{M'[x]}\!\big/\!{}_{\langle R_1(x)\rangle} \to M'(\beta_{s+1}) : \quad \varphi_2(\overline{x}) = \beta_{s+1}$$

Отображение $\varphi_1^{-1} \circ \varphi \circ \varphi_2$ подойдёт в качестве f_{s+1}.

$\square$

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 $1 \le k < n$

Свойства.

1. Корни n-й степени из 1 образуют абелеву группу по умножению
2. $\operatorname{char} K = p \in \mathbb{P} \neq 0$, $n = p^m h$, $h \not\vdots\, p$, ε — корень n-й степени из 1.
   Тогда ε — корень h-й степени из 1.

Доказательство.

1. Пусть U — множество корней n-й степени.
   - $\varepsilon_1, \varepsilon_2 \in U \implies (\varepsilon_1\varepsilon_2)^n = \varepsilon_1^n\varepsilon_2^n = 1 \cdot 1 = 1 \implies \varepsilon_1\varepsilon_2 \in U$
   - $\varepsilon \in U \implies \left(\frac{1}{\varepsilon}\right)^n = \frac{1^n}{\varepsilon^n} = \frac{1}{1} = 1 \implies \varepsilon^{-1} \in U$
2. Докажем, что если $\varepsilon^{ps} = 1$, то $\varepsilon^s = 1$:
   $$C_p^i = \frac{p!}{(p-i)! \cdot i!} \quad \vdots\, p \text{ при } 1 \le i \le p-1 \text{ в } \mathbb{Z}$$
   (т. к. $p! \,\vdots\, p$, $(p-i)! \cdot i! \not\vdots\, p$)
   $$\operatorname{char} K = p \implies C_p^i = 0 \text{ при } 1 \le i \le p$$
   $$(\varepsilon^s - 1)^p = (\varepsilon^s)^p + 0 \cdot (\varepsilon^s)^{p-1} \cdot (-1) + \dots + 0 \cdot \varepsilon^s \cdot (-1)^{p-1} + (-1)^p = \varepsilon^{sp} - 1 = 1 - 1 = 0 \xRightarrow[\text{обл. цел.}]{} \varepsilon^s = 1$$

$\square$

Теорема 40 (существование примитивного корня). K — поле, $h \in \mathbb{N}$
$x^h - 1$ раскладывается в K на линейные множители, $h \not\vdots \operatorname{char} K$

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 $\exists \varepsilon \in U : \quad \operatorname{ord} \varepsilon = h$
   Пусть $h = p_1^{a_1} \cdot \dots \cdot p_k^{a_k}$, $p_i \in \mathbb{P}$
   Докажем, что $\exists x_1, \dots, x_k \in U : \quad \operatorname{ord}(x_i) = p_i^{a_i}$:
   Докажем для $i = 1$ (остальное — аналогично):
   $$x_1 : \operatorname{ord} x_1 \overset{?}{=} p_1^{a_1}$$
   Докажем, что $\exists y : \quad \operatorname{ord} y \,\vdots\, p_1^{a_1}$:
   Пусть $\forall y \in U \quad \operatorname{ord} y \not\vdots\, p_1^{a_1}$
   $$\left.\begin{array}{l} p_1^{a_1}p_2^{a_2}\dots p_k^{a_k} \,\vdots \operatorname{ord} y \\ \operatorname{ord} y \not\vdots\, p_1^{a_1} \end{array}\right\} \implies \underbrace{p_1^{a_1-1}p_2^{a_2}\dots p_k^{a_k}}_{h'} \vdots \operatorname{ord} y$$
   $$h' \,\vdots \operatorname{ord} y \implies y^{h'} = 1 \quad \forall y \in U$$

y — корень кногочлена $x^{h'}-1 \quad \forall y \in U$

У него $h > h'$ корней — $\lightning$

$$\operatorname{ord} y = p_1^{a_1} \cdot t \implies \operatorname{ord}(y^t) = p_1^{a_1}$$

Подойдёт $x_1 = y^t$. Аналогично x_i

Докажем, что для $\varepsilon = x_1 x_2 \dots x_k$ выполнено $\operatorname{ord}\varepsilon = h$:

Положим $b_i \coloneqq p_1^{a_1} \dots p_i^{a_i - 1} \dots p_k^{a_k}$

$x_i^{b_i} \neq 1$ т. к. $b_i \not\vdots \operatorname{ord} x_i$

$$x_i^{b_i} - 1, \qquad j \neq i$$

$x_j^{b_i} = 1$ при $i \neq j$

$$\varepsilon^{b_i} = \underbrace{x_1^{b_i}}_{1} \dots \underbrace{x_i^{b_i}}_{\neq 1} \dots \underbrace{x_k^{b_i}}_{1} \neq 1$$

$$h \vdots \operatorname{ord}\varepsilon, \qquad b_i \not\vdots \varepsilon \quad \forall i \qquad \implies \operatorname{ord}\varepsilon = h$$

3. ε — примитивный

   $1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{h-1}$ различны $\implies$ $1, \varepsilon, \dots, \varepsilon^{h-1}$ — все элементы U $(\varepsilon^i = \varepsilon^j \implies \varepsilon^{i-j} = 1)$

$\square$

40. Количество примитивных корней. Многочлен деления круга

Лемма 12 (количество примитивных корней). K — поле, $\quad h \in \mathbb{N}, \quad h \not\vdots \operatorname{char} K$
$x^h - 1$ раскладывается на линейные множители

Тогда в K есть $\varphi(h)$ примитивных корней из единицы.

Доказательство. ε — примитивный корень
Все корни: $\varepsilon^0 = 1, \quad \varepsilon^1 = \varepsilon, \quad \varepsilon^2, \quad \dots, \quad \varepsilon^{n-1}$

Докажем, что ε^s примитивный $\iff$ НОД$(s, h) = 1$:

- Пусть НОД$(s, h) = 1$, $\quad (\varepsilon^s)^k = 1 \implies \varepsilon^{sk} = 1 \implies sk \vdots h \implies k \vdots h$

$$\operatorname{ord}\varepsilon^s = h$$

- Пусть НОД$(s, h) = d \neq 1$

$$(\varepsilon^s)^{\frac{h}{d}} = \varepsilon^{\frac{sh}{d}} = (\underbrace{\varepsilon^h}_{=1})^{\frac{s}{d}} = 1 \implies \operatorname{ord}\varepsilon^s = \frac{h}{d} \implies \varepsilon^s \text{ не примитивный}$$

$\square$

Определение 56. K — поле, $\quad h \in \mathbb{N}, \quad h \not\vdots \operatorname{char} K, \quad x^h - 1$ 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, $\quad h \in \mathbb{N}, \quad h \not\vdots \operatorname{char} K$
$x^h - 1$ раскладывается на линейные множители

1. $x^h - 1 = \prod\limits_{d \mid h} \Phi_d(x)$;

2. если $K = \mathbb{C}$, то коэффициенты $\Phi_h(x)$ — целые числа.

Доказательство.

1.
$$x^h - 1 = \prod_{\varepsilon \in U} (x - \varepsilon), \qquad U \text{ — группа корней } h\text{-й степени из } 1$$
$$\prod_{d | h} \Phi_d(x) \overset{?}{=} \prod_{\varepsilon \in U} (x - \varepsilon)$$

- Пусть $x - \varepsilon$ входит в $\Phi_d(x) \implies \varepsilon^d = 1, \quad \varepsilon^k \neq 1$ при $k < d \implies \varepsilon^h = 1$ (т. к. $h \vdots d$), $\varepsilon \in U$
- Пусть $x - \varepsilon$ входит в правую часть
  Тогда $\varepsilon \in U$
  Пусть $\operatorname{ord} \varepsilon = d \implies x - \varepsilon$ входит в $\Phi_d(x)$, не входит в $\Phi_{\widetilde{d}}(x), \quad \widetilde{d} \neq d$

2. **Индукция.**
   - **База** — проверено в примерах.
   - **Переход** к h от меньших чисел.
   $$\Phi_h(x) = \frac{x^h - 1}{\Phi_{d_1}(x) \cdots \Phi_{d_k}(x)}, \qquad d_1, \dots, d_k \text{ — делители } h, \text{ не равные } h$$
   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 $p \in \mathbb{P}, \quad n \in \mathbb{N}$ такие, что

1. K содержит простое поле $F \simeq \mathbb{Z}_p$;
2. $\operatorname{char} K = p$;
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 $\exists\, p: \quad F \simeq \mathbb{Z}_p$
2. $\operatorname{char} k = \min \left\{ n \;\middle|\; \underbrace{1 + \dots + 1}_{n} = 0 \right\}$
   $$1, \quad 1+1, \quad 1+1+1, \quad \dots \in F \implies \operatorname{char} k = \operatorname{char} F = p$$
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 $a_1 e_1 + a_2 e_2 + \dots a_n e_n \in F$
   $|K|$ — количество наборов $a_1, \dots, a_n \in F \implies |K| = p^n$
4. Пусть $U = K^*$ (группа ненулевых элементов K по умножению)
   $$\implies |U| = p^n - 1$$
   $$\forall x \in U \quad p^n - 1 \vdots \operatorname{ord} x \implies x^{p^n - 1} = 1 \quad \forall x \in K \setminus \{ 0 \} \implies x^{p^n} - x = 0 \quad \forall x \in K$$

$\implies$ все элементы K — корни $x^{p^n} - x = 0$

$$\deg(x^{p^n} - x) = p^n = |K| \implies \text{других корней нет}$$

$\square$

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 $\mathbb{Z}_p$. $\square$

42. Существование поля с данным количеством элементов

Теорема 43. Для любых $p \in \mathbb{P}, \quad n \in \mathbb{N}$ существует поле из p^n элементов

Доказательство. Пусть L — поле разложения $P(x) = x^{p^n} - x$ над $\mathbb{Z}_p$, $\quad K$ — подмножество L, состоящее из корней $P(x)$.

$$P'(x) = \underset{0}{p^n} x^{p^n - 1} - 1 = -1 \text{ не имеет корней} \implies \text{у } P, P' \text{ нет общих корней}$$

$\implies$ 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, то $0, 1 \in K, \quad K$ замкнуто относительно $=, \cdot$, взятия обратного по $+, \cdot$:

- $P(0) = 0^{P^n} - 0 = 0, \qquad P(1) = 1 - 1 \quad \implies 0, 1 \in K$
- $x, y \in K \implies x^{p^n} - x = 0, \quad y^{p^n} - y = 0$

$$(x = y)^{p^n} = \Big((x = y)^p\Big)^{p^n - 1} = (x^p + y^p)^{x^{p^{n-1}}} = \Big((x^p + y^p)^p\Big)^{p^{n-p}} =$$
$$= (x^{p^2} + y^{p^2})^{p^{n-p}} = \dots = x^{p^n} + y^{p^n} = x + y$$

$$(x + y)^{p^n} - (x + y) = 0$$

- $P(-x) = (-x)^{p^n} - (-x) = -(x^{p^n} - x) = \dots = -P(x)$

$$x \in K \implies p(x) = 0 \implies p(-x) = 0 \implies -x \in K$$

- $x, y \in K \implies x^{p^n} = x, \quad y^{p^n} = y$

$$P(xy) = (xy)^{p^n} - xy = x^{p^n} y^{p^n} - xy = 0 \implies xy \in K$$

- $x \in K$

$$x^{p^n} = x \implies \left(\frac{1}{x}\right)^{p^n} = \frac{1}{x^{p^n}} = \frac{1}{x}$$

$\square$