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 диагоналиуемом операторе — 4

4 Блочные матрицы и инвариантные подпространства. Делители характеристичсекого многочлена — 5

5 Ранг блочно-диагональной матрицы — 7

6 Жордановы цепочки: линейная независимость, матрица оператора в базисе из цепочек — 9

7 Существование жордановой формы нильпотентного оператора — 11

8 Многочлен от оператора: произведение многочленов, инвариантность ядра и образа — 12

9 Свойства аннулятора вектора — 13

10 Базис циклического подпространства — 14

11 Циклическое подпространство и минимальный аннулятор — 15

12 Минимальный многочлен оператора. Теорема Гамильтона—Кэли и следствие из неё — 16

13 Свойства взаимно простых многочленов от оператора — 17

14 Разложение пространства в прямую сумму примарных подпространств — 19

15 Корневые подпространства — 20

16 Существование жордановой формы — 20

17 Возведение жордановой клетки в степень — 21

18 Количество жордановых блоков и ранг. Следствие о единственности жорадновой формы — 23

19 Минимальный многчлен оператора, у которого известна жорданова форма — 24

20 Комплексификация вещественного векторного пространства. Продолжение операторов — 24

21 Каноническая матрица оператора в вещественном пространстве — 26

II Линейные отображения в евклидовых и унитарных пространствах — 28

22 Изоморфизм векторного пространства и двойственного к нему — 28

23 Дважды двойственное пространство — 30

24 Двойственный базис. Матрица перехода для двойственного базиса — 31

25 Собственные числа самосопряжённого оператора. Лемма об эрмитовой матрице — 32

26 Ортогональность собственных векторов. Самосопряжённый оператор на $\mathbb{R}^n$ — 34

27 Корень из самосопряжённого оператора. Полярное разложение 34

28 Квадратичные формы: ортогональное преобразование, преобразование двух форм 36

III Кольца и поля 37

29 Идеал кольца. Примеры главных идеалов. Определения простого и максимального идеала 37

30 Построение факторкольца. Факторкольцо по простому идеалу 40

31 Факторкольцо по максимальному идеалу. Факторкольцо кольца многочленов над полем 42

32 Гомоморфизм колец. Теорема о гомоморфизме 43

33 Характеристика кольца и поля. Классификация простых полей 45

34 Степень расширения. Мультипликативность степени, следствия 47

35 Минимальный многочлен алгебраического элемента. Конечность алгебраического расширения 49

36 Строение простого алгебраического расширения. Следствия 51

37 Существование простого расширения. Эквивалентные расширения 53

38 Поле разложения многочлена: существование, эквивалентность 55

39 Свойства корней из единицы. Существование примитивного корня 57

40 Количество примитивных корней. Многочлен деления круга 59

41 Строение конечного поля. Единственность 60

42 Существование поля с данным количеством элементов 61

Часть I
Жорданова форма оператора

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

Определение 1. V — векторное пространство, $\mathcal{A}$ — оператор на V, λ — с. ч.
Собственным подпространством, соответствующим λ, называется множество с. в., соответствующих λ

Обозначение. V_λ

Определение 2. U — подпространство V
U называется инвариантным относительно $\mathcal{A}$, если

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

Утверждение 1. V_λ — инвариантное подпространство

Доказательство.

- Подпространство

– $u, v \in V_\lambda \implies \begin{cases} \mathcal{A}u = \lambda u \\ \mathcal{A}v = \lambda v \end{cases} \implies \mathcal{A}(u+v) \xlongequal[\text{линейность}]{} \mathcal{A}u + \mathcal{A}v = \lambda u + \lambda v = \lambda(u+v) \implies u + v \in V_\lambda$

– $u \in V_\lambda, k \in K \implies \mathcal{A}(ku) \xlongequal[\text{линейность}]{} k\mathcal{A}(u) = k\lambda u = \lambda(ku) \implies ku \in V_\lambda$

- Инвариантность

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

□

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

Доказательство. **Индукция** по k

- **База.** $k = 1$ — очевидно
- **Переход.** $k - 1 \to k$
Пусть $u_1 + \cdots + u_{k-1} + u_k = 0, \qquad u_i \in V_{\lambda_i}$

$$0 = \mathcal{A}(\underbrace{u_1 + \cdots + u_{k-1} + u_k}_{=0}) - \lambda_k(\underbrace{u_1 + \cdots + u_{k-1} + u_k}_{=0}) =$$

$$= \lambda_1 u_1 + \cdots + \lambda_{k-1}u_{k-1} + \cancel{\lambda_k u_k} - \lambda_k u_1 - \cdots - \lambda_k u_{k-1} - \cancel{\lambda_k u_k} = \underbrace{(\lambda_1 - \lambda_k)}_{\neq 0} u_1 + \cdots + \underbrace{(\lambda_{k-1} - \lambda_k)}_{\neq 0} u_{k-1}$$

(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 $\mathcal{A}$, действующий на V называется диагонализуемым, если его матрица в некотором базисе диагональна

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

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

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

Доказательство.

$\mathcal{A}$ диагонализуем $\iff$ в нек. базисе $e_1, \dots, e_n$ матрица $\mathcal{A}$ имеет вид $A = \begin{pmatrix} a_1 & 0 & . \\ 0 & a_2 & . \\ . & . & . \end{pmatrix}$

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

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

$\iff$ (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.
  Объединение базисов состоит из с. в.
  Это 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):

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

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

  Сложим все эти неравенства:

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

$\square$

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

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

$$n \ge \dim(V_{\lambda_1} + \dots + V_{\lambda_k}) \xlongequal[\text{пр. сумма}]{} \dim V_{\lambda_1} + \dots + \dim V_{\lambda_k} \ge n$$

Значит, достигается равенство $\square$

3. Теорема об арифметической и геометрической кратности. Следствие о диагоналиуемом операторе

Напоминание (определитель ступенчатой матрицы)**.**

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

Теорема 3 (арифм. и геом. кратности). λ — с. ч. $\mathcal{A}$
Геом. кратность $\lambda \leq$ арифм. кратности λ

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

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

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 $\mathcal{A}$ диагонализуем $\iff$

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

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

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

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

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

4. Блочные матрицы и инвариантные подпространства. Делители характеристичсекого многочлена

Определение 5. Блочной матрицей называется матрица вида

$$A = \begin{pmatrix} A_{11} & A_{12} & \dots & A_{1n} \\ . & . & . & . \\ A_{m1} & A_{m2} & \dots & A_{mn} \end{pmatrix}$$

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

Пример.

$$\left(\begin{array}{cc|c} . & . & . \\ \hline . & . & . \\ . & . & . \end{array}\right)$$

Определение 6. Блочно-диагональной матрицей называется матрица вида

$$\begin{pmatrix} A_1 & 0 & . & 0 \\ 0 & A_2 & . & 0 \\ . & . & . & . \\ 0 & . & 0 & A_n \end{pmatrix}$$

где A_i — квадратные

Замечание. Блочно-диагональная матрица всегда квадратная

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

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

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

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

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

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

$$\implies A = \begin{pmatrix} A_1 & 0 & . & 0 \\ 0 & A_2 & . & 0 \\ . & . & . & . \\ 0 & . & 0 & A_k \end{pmatrix}$$

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

Доказательство.

1. Пусть

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

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

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

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

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

$$\implies A = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{s1} & * & * \\ . & . & . & . & * & * \\ a_{s1} & a_{s2} & \dots & a_{ss} & . & . \\ 0 & 0 & \dots & 0 & . & . \\ . & . & . & . & . & . \\ 0 & 0 & \dots & 0 & * & * \end{pmatrix}$$

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

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

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

$$\begin{pmatrix} 0 \\ \vdots \\ 0 \\ a_1 \\ \vdots \\ a_{d_i} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

□

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

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

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

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

$$\chi(t) = \chi_1(t) \cdot \dots \cdot \chi_k(t)$$

Доказательство. Рассмотрим базисы как в теореме

1.

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

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

□

5. Ранг блочно-диагональной матрицы

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

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

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

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

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

- $\implies$
  Докажем **от противного**:
  Предположим, что $s_1^{(i)}, \dots, s_{r_i}^{(i)}$ ЛЗ
  То есть, $\exists\, a_1, \dots, a_{r_i}$, не все равные нулю, такие, что $a_1 s_1^{(i)} + \dots + a_{r_i} s_{r_i}^{(i)} = 0$
  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 всеь набор ЛЗ — $\lightning$

- $\impliedby$
  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
  $$T_i \coloneqq a_1^{(i)} s_1^{(i)} + \dots + a_{r_i}^{(i)} s_{r_i}^{(i)}$$
  $$\widetilde{T_i} \coloneqq a_1^{(i)} \widetilde{s_1}^{(i)} + \dots + a_{r_i}^{(i)} \widetilde{s_{r_i}}^{(i)}$$
  $$\widetilde{T_1} + \widetilde{T_2} + \dots + \widetilde{T_k} = 0 \implies \widetilde{T_1} = \widetilde{T_2} = \dots = 0$$
  Строки $\widetilde{T_1}, \dots, \widetilde{T_k}$ **не** содержат ненулевые элементы в одном столбце (т. е. в нашей записи нет полностью нулевых столбцов)
  $$\implies T_1 = 0, \quad T_2 = 0, \quad T_k = 0$$

  > **Замечание.** Эти нули разной длины

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

□

Замечание. На самом деле, блочно-диагональная матрица — избыточное условие (достаточно, чтобы в каждой строке был ЛНЗ набор, и не было полностью нулевых столбцов), однако нам понадобится именно такой случай

Следствие. $V = U_1 \oplus \dots \oplus U_k, \qquad U - i$ — инвариантно для $\mathcal{A}$

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

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

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

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

$$\begin{pmatrix} J_{r_1}(0) & 0 & . & 0 \\ 0 & J_{r_2}(0) & . & 0 \\ . & . & . & . \\ 0 & . & F_{r_k}(0) & 0 \end{pmatrix}$$

Пример.

$$J = \left(\begin{array}{ccc|cc} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right)$$

Пусть это матрица оператора в базисах e_1, e_2, e_3, e_4, e_5

$$Je_1 = 0e_1 + 1e_2 + 0e_3 + 0e_4 + 0e_5 = e_2$$

$$Je_2 = e_3, \qquad Je_3 = 0, \qquad Je_4 = e_5, \qquad Je_5 = 0$$

Обозначение. $e_1 \to e_2 \to e_3 \to 0, \qquad e_4 \to e_5 \to 0$

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

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

Замечание. Вектор e_r является собственным вектором, соотв. $\lambda = 0$

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 $r := \max\{ r_1, \dots, r_k \}$

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

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

Применим s раз:

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

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 $\mathcal{A}^{r-1}$:

- 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). $\mathcal{A}$ — 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 $\mathcal{A}$ в этом базисе

$$A = \begin{pmatrix} J_{r_1}(0) & 0 & . & 0 \\ 0 & J_{r_2}(0) & . & 0 \\ . & . & . & . \\ 0 & . & 0 & J_{r_k}(0) \end{pmatrix}$$

Доказательство.

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

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

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

$$\begin{array}{cl} \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} & \begin{array}{c} \\ \\ \\ \\ \\ i \\ i+1 \\ \\ \\ \\ \\ \end{array} \end{array}$$

□

7. Существование жордановой формы нильпотентного оператора

Теорема 5 (жорданова форма нильпотентного оператора). Для любого нильпотентного оператора на конечномерном векторном пространстве существует жорданов базис

Доказательство. Будем доказывать, что существует базис из жордановых цепочек
Положим $W \coloneqq \ker \mathcal{A}$
Если мы возьмём ЛНЗ векторы из ядра и достроим (слева от них) цепочки, то получим жорданов базис
Положим $U_i \coloneqq \operatorname{Im} \mathcal{A}^i$

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

где k — степень нильпотентности $\mathcal{A}$
Заметим, что если $v \in U_t \cap W$, то существует цепочка длины $t+1$ с концом v
Построим базис W (такой, чтобы можно было 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 $e_1, e_2, \ldots$ пространства W
Для $e_i \in W \cap U_t$ построим цепочку длины $t+1$ с концом e_i:

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

Объединение цепочек — ЛНЗ (по лемме)
Докажем, что это базис, т. е. что набор порождающий:
Докажем, что если $\mathcal{A}^s(v) = 0$, то v является ЛК векторов цепочек
Докажем **индукцией** по s:

- **База.** $s = 1$

$$\mathcal{A}^1(v) = 0, \qquad v \in W, \qquad e_1, e_2, \ldots \text{ — базис } W$$

- **Переход.** $s \to s+1$
Пусть $\mathcal{A}^{s+1}(v) = 0, \quad \mathcal{A}^s(v) \neq 0$
Положим $u = \mathcal{A}^s \implies u \in U_s$

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

Значит, $\mathcal{A}(u) = 0 \implies u \in W$
Значит, $u \in U_s \cap W$
Представим его в виде ЛК базиса $U_s \cap W$ (того, до которого мы дошли на каком-то очередном шагу 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 $\mathcal{A}^s(e_i') = e_i$ (вектор, который на s шагов раньше)

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

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

$$\mathcal{A}^s(v) = \mathcal{A}^s\left(\sum a_i e_i'\right) \implies \mathcal{A}^s\left(v - \sum a_i e_i'\right) = 0$$

Тогда, **по индукционному предположению**, $v - \sum a_i e_i'$ представляется в виде ЛК векторов из цепочек
Значит, v представляется в виде ЛК векторов цепочек

$\square$

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

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

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

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

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

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

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

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

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

$$\mathcal{B}\Big(\mathcal{C}(v)\Big) = \mathcal{B}(w) = \mathcal{B}\left(\sum p_j \mathcal{A}^j(v)\right) = \sum q_j \mathcal{B}\Big(\mathcal{A}^j(v)\Big) = \sum q_j \left(\sum p_i \mathcal{A}^i(\dashv^{|}(v))\right) =$$
$$= \sum q_j \left(\sum p_i \mathcal{A}^{i_j}\right) = \sum q_j p_i \mathcal{A}^{i+j} = \mathcal{D}(v)$$

$\square$

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

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

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

Обозначение. $a_1, .., a_n \neq \odot \iff$ **не** все они равны нулю

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

Доказательство. По лемме,

$$\mathcal{A} \circ \mathcal{B} = \mathcal{B} \circ \mathcal{A} \tag{1}$$

- $\ker \mathcal{B}$

$$v \in \ker \mathcal{B} \implies \mathcal{B}(v) = 0 \implies \mathcal{A}\Big(\mathcal{B}(v)\Big) = 0 \underset{(1)}{\implies} \mathcal{B}\Big(\mathcal{A}(v)\Big) = 0 \implies \mathcal{A}(v) \in \ker \mathcal{B}$$

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

$$v \in \operatorname{Im} \mathcal{B} \implies v = \mathcal{B}(w) \implies \mathcal{A}(v) = \mathcal{A}\Big(\mathcal{B}(w)\Big) \underset{(1)}{=} \mathcal{B}\Big(\mathcal{A}(w)\Big)$$

□

9. Свойства аннулятора вектора

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

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

Замечание. Минимальный аннулятор задаётся с точностью до умножения на константу

Свойства.

1. V — конечномерно. Тогда
   (a) у любого вектора существует ненулевой аннулятор

   Доказательство. См. доказательство следующего пункта. □

   (b) если P_0 — минимальный аннулятор, то $\deg P_0 \le \dim V$

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

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

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

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

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

2. $P_1, \dots, P_k$ — аннуляторы v
   Тогда

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

   Доказательство. Пусть $\mathcal{B}_i \coloneqq P_i(\mathcal{A})$, $\qquad \mathcal{C}_i = Q_i(\mathcal{A})$, $\qquad \mathcal{D} = S(\mathcal{A})$

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

   □

3. $P_0(t)$ — минимальный аннулятор. Тогда
$$P(t) \text{ — аннулятор } \iff P(t) \,\vdots\, P_0(t)$$

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

Доказательство.
$$\exists\, P_1, P_2 \text{ — мин. аннул. } \Longrightarrow \underbrace{P_1}_{\text{аннул.}} \,\vdots\, \underbrace{P_2}_{\text{мин. аннул.}}$$

□

10. Базис циклического подпространства

Определение 12. $\mathcal{A}$ — 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. $v, \mathcal{A}(v), \dots, \mathcal{A}^{k-1}(v)$ ЛНЗ
2. $v, \mathcal{A}(v), \dots, \mathcal{A}^{k-1}(v), \mathcal{A}^k(v)$ ЛЗ

Тогда первый набор является базисом цикического подпространства, порождённого v

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

- Докажем, что W — инвар.:
  $\mathcal{A}^k v$ — ЛК $v, \mathcal{A}v, \dots, \mathcal{A}^{k-1}v$
  $$w \in W, \qquad w = a_0 v + \dots + a_{k-1}\mathcal{A}^{k-1}v$$
  $$\mathcal{A}(w) = a_0\mathcal{A}v + \dots + a_{k-2}\mathcal{A}^{k-1}v + \underbrace{a_{k+1}\mathcal{A}^k v}_{\text{ЛК } v,\dots,\mathcal{A}^{k-1}v}$$
  Значит, w является ЛК $v, \dots, \mathcal{A}^{k-1}v$

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

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

$$\implies W_1 \subset W$$

□

11. Циклическое подпространство и минимальный аннулятор

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

Доказательство. Пусть k такое, что

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

Путь a_i, не все равные нулю, такие, что

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

Значит, $a_k \neq 0$ (т. к. $v \dots, \mathcal{A}^{k-1}v$ ЛНЗ)
Делим на a_k, НУО считая что $a_k = 1$:

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

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**:

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

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

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

- Докажем, что $P(t) = \pm\chi$:
  Знаем, что

$$v, \dots, \mathcal{A}^{k-1}v \text{ — базис } U$$

  Матрица $\mathcal{A}\big|_U$ в этом базисе:

$$A = \begin{pmatrix} v & \mathcal{A}v & \dots & \mathcal{A}^{k-2}v & \mathcal{A}^{k-1}v \\ 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & . & -a_1 \\ 0 & 1 & \dots & . & . \\ . & . & . & . & . \\ 0 & 0 & \dots & 0 & . \\ 1 & 1 & \dots & 1 & -a_{k-1} \end{pmatrix}$$

  В первом столбце (начиная со второй строки) — координаты $\mathcal{A}v = 0 \cdot v + 1 \cdot \mathcal{A}v + 0 \cdot \dots$
  Во втором столбце — координаты $\mathcal{A}^2 v$

....
В последнем столбце — координаты $\mathcal{A}^k v$

$$\chi_A(t) = \begin{vmatrix} -t & 0 & 0 & \dots & 0 & -a_0 \\ 1 & -t & 0 & \dots & 0 & -a_1 \\ . & . & . & . & . & . \\ . & . & . & -t & 0 & -a_{k-2} \\ . & . & . & . & . & -a_{k-1} - t \end{vmatrix}$$

Прибавим ко 2-й строке 1-ю, умноженную на $^1\!/_t$
Прибавим к 3-й строке 2-ю, умноженную на $^1\!/_t$ ....

$$\chi(t) = \begin{vmatrix} -t & 0 & 0 & \dots & 0 & -a_1 \\ 0 & -t & 0 & \dots & 0 & -a_1 - \frac{a_0}{t} \\ 0 & 0 & -t & \dots & 0 & -a_2 - \frac{a_1}{t} - \frac{a_0}{t^2} \\ . & . & . & . & . & . \\ 0 & . & . & . & 0 & t - a_{k-1} - \frac{a_{k-2}}{t} - \dots - \frac{a_1}{t^{k-2}} - \frac{a_1}{t^{k-1}} \end{vmatrix}$$

Это будет $(-1)^k P(t)$

□

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

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

Замечание. Он является аннулятором для всех векторов

Пример. $\mathcal{A} : \mathbb{R}^2 \to \mathbb{R}^2$

$$\mathcal{A} : X \mapsto \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix} X$$

$$P(t) = (t-2)^2 \text{ — аннулирует } A$$

$Q(t) = t - 2$ не аннулирует $\mathcal{A}$, т. к. $\Big(Q(\mathcal{A})\Big) = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$

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

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

1. $P_1, \dots, P_k$ аннулируют $\mathcal{A}$
   Тогда для любых многочленов $Q_1, \dots, Q_k$ многочлен $S(t) = P_1(t)Q_1(t) + \dots + Pk(t)Q_k(t)$ аннулирует $\mathcal{A}$

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

$$P \text{ аннулирует } \mathcal{A} \iff P \,\vdots\, P_0$$

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

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

Доказательство.

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

2. Пусть $P = P_0 Q + R$

- Если $P \vdots P_0$, то $P = P_0Q \underset{1.}{\Longrightarrow} P$ аннулирует $\mathcal{A}$
- Если P аннулирует $\mathcal{A}$, то $R = P - P_0Q$ аннулирует $\mathcal{A} \underset{1.}{\Longrightarrow} R = 0 \implies P \vdots P_0$

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

   - Проверим, что P аннулирует A:
     Пусть $v \in V, \qquad v = a_1e_1 + \dots + a_ne_n$
     Применим P:
     $$P(\mathcal{A})(v) = a_1P(\mathcal{A})e_1 + \dots + a_nP(\mathcal{A})e_n$$
     $$P \vdots P_i \implies P \text{ — аннул. для } e_i \implies P(\mathcal{A})e_i = 0$$
     $$P(\mathcal{A})(v) = a_1 \cdot 0 + \dots + a_n \cdot 0 = 0$$

     > **Замечание.** Тем самым, мы доказали, что аннулятор многочлена существует

   - Проверим, что P минимальный:
     Пусть $Q(t)$ аннулирует $\mathcal{A}$
     $$\implies Q(\mathcal{A})v = 0 \quad \forall v \implies Q(\mathcal{A})e_i = 0 \quad \forall i \xRightarrow[P_i \text{ — мин. аннул.}]{} $$
     $$\implies Q \vdots P_i \quad \forall i \implies Q \vdots P \implies \deg Q \geq \deg P$$

□

Теорема 9 (Гамильтона-Кэли). Характеристический многочлен оператора $\mathcal{A}$ аннулирует $\mathcal{A}$, т. е.
$$\chi_{\mathcal{A}}(\mathcal{A}) = 0$$

Доказательство. Нужно доказать, что $\forall v \quad \chi(\mathcal{A})v = 0$
Докажем, что $\chi_{\mathcal{A}} \vdots P_0$, где P_0 — минимальный аннулятор (все аннуляторы делятся на минимальный):
Пусть U — циклическое подпространство, порождённое v
χ_U — характеристический многочлен $\mathcal{A}\big|_U$ (он определён, т. к. пространство иварианто)
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)
$$\left.\begin{array}{l} \chi_U = P_0 \\ \chi \vdots \chi_U \end{array}\right\} \implies \chi \vdots P_0$$

□

Пример.
$$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \qquad \chi_{\mathcal{A}}(t) = (1-t)^2 = t^2 - 2t + t$$
$$A^2 - 2A + E = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} - \begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Следствие. P_0 — минимальный многочлен $\mathcal{A}$
Тогда $\chi \vdots P$

13. Свойства взаимно простых многочленов от оператора

Определение 15. K — поле, $\qquad V$ — векторное пространство над K, $\qquad \mathcal{A}$ — оператор на V
$P(t)$ — минимальный унитарный многочлен $\mathcal{A}$ (старший коэффициент P равен 1)
Пространство V называется примарным относительно $\mathcal{A}$, если $P(t) = Q^s(t)$ для некоторого $Q(t)$, неприводимого над K

Примеры.

1. $K = \mathbb{R}, \qquad V = \mathbb{R}^4, \qquad \mathcal{A} : X \mapsto AX$

$$A = \begin{pmatrix} 2 & & & \\ 0 & 2 & * & \\ 0 & 0 & 2 & \\ 0 & 0 & 0 & 2 \end{pmatrix}, \qquad \chi_A = (2-t)^4$$

$(2-t)^4 \vdots$ минимальный многочлен $\implies$ минимальный многочлен $= (2-t)^s, \quad s \le 4$

2. $V = \mathbb{R}^2, \qquad \mathcal{A} : X \mapsto AX$

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad \chi_{\mathcal{A}} = t^2 + 1 \text{ — неприв.} \implies \text{примарно}$$

3. То же самое, но $K = \mathbb{C}$

$$\chi_{\mathcal{A}} = t^2 + 1 = (t-i)(t+i)$$

$$P_1(t) = t - i, \qquad P_2(t) = t + i$$

P_1, P_2 — не аннул. $\mathcal{A}$:

$$\begin{pmatrix} i & -1 \\ 1 & i \end{pmatrix} \ne 0, \qquad \begin{pmatrix} -i & -1 \\ 1 & -i \end{pmatrix} \ne 0$$

$\implies \chi_{\mathcal{A}}(t)$ — минимальный многочлен. Пространство не примарно

Свойства (взаимно простых многочленов от оператора). $\mathcal{A}$ — оператор на V

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

Доказательство.

1. **Индукция.**
   - **База.** $k = 2$
     P, Q взаимно просты, $\qquad v \in V$
     Докажем, что $\exists\, v, w : v = u + w, \qquad P(\mathcal{A})u = 0, \qquad Q(\mathcal{A})w = 0$
     Т. к. P, Q взаимно просты, можно разложить их НОД $(= 1)$:

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

     Применим к $\mathcal{A}$:

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

     Применим к v:

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

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

     $$P(\mathcal{A}) \circ \Big(QG(\mathcal{A})\Big)v = \Big(PQG\Big)(\mathcal{A})v \xlongequal[\text{коммут.}]{} \Big(GPQ\Big)(\mathcal{A})v =$$

     $$= G(\mathcal{A}) \underbrace{(PQ)(\mathcal{A})v}_{=0 \text{ (т. к.} T = PQ \text{ анн. } v)} = 0$$

   - **Переход.** $k - 1 \to k$

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

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

По **индукционному предположению**,

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

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

2. Пусть T — минимальный аннулятор v

$$\left.\begin{aligned} P &\,\vdots\, T \\ Q &\,\vdots\, T \end{aligned}\right\} \implies T = \text{const}, \qquad T(t) = c \implies cv = 0 \implies v = 0$$

□

14. Разложение пространства в прямую сумму примарных подпространств

Теорема 10 (разложение пространства в прямую сумму примарных подпространств). K — поле, V — векторное пространство над K, $\mathcal{A}$ — оператор на V
$P(t)$ — минимальный моногочлен $\mathcal{A}$, он разложен на множители:

$$P(t) = P_1(t) \dots P_k(t), \qquad \text{где } P_i(t) = Q_i^{s_i}(t), \qquad Q_i \text{ — неприпод. над } K$$

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 $\mathcal{A}$ на U_i $\quad \forall i$

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

1. Ядро многочлена от оператора инвариантно (было такое свойство)
2. (a) Докажем, что $V = U_1 + \dots + U_k$
   $P_1, \dots, P_k$ попарно взаимно просты, и $P_1 \cdot \dots \cdot P_k$ аннулируют любой v, значит

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

   (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 $(U_1 + \dots + U_k) \cap U_k = \{\, 0 \,\}$
   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 одному из свойств,

   $$P_1 \cdot \dots \cdot P_{k-1} \text{ аннулирует } v_1 + \dots + v_{k-1} = v$$

   При этом, P_k аннулирует v
   Заметим, что $(P_1 \cdot \dots \cdot P_{k-1}, P_k) = 1$
   По одному из свойств, это означает, что $v = 0$
3. $$U_i = \ker P_i(\mathcal{A}) \implies P_i(\mathcal{A})\big|_{U_i} = 0$$

   P_i аннулирует $\mathcal{A}\big|_{U_i}$
   Значит, P_i делится на минимальный многочлен $\mathcal{A}\big|_{U_i}$
   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, существует $e_1, \dots, e_n$ — базис V, он является объединением базисов U_i

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

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

$\square$

15. Корневые подпространства

Определение 16. λ — с. ч. $\mathcal{A}$
Вектор v называется корневым вектором, соответствующим λ, если для некоторого k многочлен $P(t) = (t-\lambda)^k$ является аннулятором v
Множество корневых векторов называется корневым подпространством, соотв. λ

Свойства.

1. Корневое подпространство инвариантно
2. V конечномерно, минимальный многочлен $\mathcal{A}$ раскладывается на линейные множители

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

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

Доказательство.

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

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

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

- $U_i \subset W_i$ — очевидно ($v \in U_i \implies (\lambda_i\mathcal{E} - \mathcal{A})^{s_i}v = 0, \qquad$ 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 $(\lambda_i\mathcal{E} - \mathcal{A})^k$ аннулирует v
Тогда $(\lambda - t)^k$ — минимальный аннулятор v
При этом, $P(t)$ — аннулятор v

$$\implies P(t) \,\vdots\, (\lambda - t)^k \xrightarrow[(\lambda - t)\text{ входит в } P \text{ только в степени } s_i]{} k \le s_i \implies v \in U_i$$

$\square$

16. Существование жордановой формы

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

$$J_r(\lambda) = \begin{pmatrix} \lambda & 0 & . & 0 \\ 1 & \lambda & . & 0 \\ . & . & . & . \\ 0 & . & 1 & \lambda \end{pmatrix}$$

Определение 18. Жордановой матрицей называется блочно-диагональная матрица вида

$$\begin{pmatrix} J_{r_1}(\lambda_1) & 0 & . & 0 \\ 0 & J_{r_2}(\lambda_2) & . & 0 \\ . & . & . & . \\ 0 & . & 0 & J_{r_k}(\lambda_k) \end{pmatrix} \qquad \text{(как } r_i\text{, так и } \lambda_i \text{ могут совпадать)}$$

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

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

Доказательство.

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

- Общий случай
  $$\chi_{\mathcal{A}} = (-1)^n (t - \lambda_1)^{s_1} \cdot \dots \cdot (t - \lambda_m)^{s_m}$$
  По следствию к теореме Гамильтона—Кэли минимальный многочлен — делитель $\chi \implies$ минимальный многочлен имеет вид
  $$P(t) = (t - \lambda_1)^{r_1} \cdot \dots \cdot (t - \lambda_m)^{r_m}$$
  Применим теорему о разложении в сумму примарных подпространств:
  Пусть $Q_i \coloneqq (t - \lambda_i)^{r_i}$
  По теореме
  $$V = U_1 \oplus \dots \oplus U_k$$
  U_i инвариантны
  $Q_i(t)$ — минимальный многочлен $\mathcal{A}$ на U_i
  К U_i применяем нильпотентный случай:
  Существует жорданов базис U_i
  Матрица $\mathcal{A}\big|_{U_i}$ имеет вид
  $$J_i = \begin{pmatrix} J_{r_1}(\lambda_i) & . & . \\ . & . & . \\ . & . & J_{r_k}(\lambda_1) \end{pmatrix}$$
  Значит, в базисе, полученном объединением базисов U_i матрица $\mathcal{A}$ имеет вид
  $$J = \begin{pmatrix} J_1 & . & . \\ . & . & . \\ . & . & J_m \end{pmatrix}$$

□

17. Возведение жордановой клетки в степень

Свойства (возведения в степень жордановой клетки).

1. • $$\Big(J_r(0)\Big)^s = \begin{pmatrix} 0 & . & . & . & . \\ 0 & 0 & . & . & . \\ . & . & . & . & . \\ 1 & . & . & . & . \\ . & . & . & . & . \\ . & 1 & . & 0 & 0 \end{pmatrix} \qquad \text{при } s < r$$

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

   • $\Big(J_r(0)\Big)^s = 0$ при $s \geq r$

2. Пусть $\lambda \neq 0$, $A = \Big(J_r(\lambda)\Big)^s$
   Тогда A нижнетреугольная
   $$a_{ij} = \begin{cases} \lambda^{i-j} C_s^{i-j}, & i > j, i - j \leq s \\ 0, & i > j, i - j > s \end{cases}$$

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

Пример (1.). $r = 4$

$$\Big(J_4(0)\Big)^1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \qquad \Big(J_4(0)\Big)^2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$\Big(J_4(0)\Big)^3 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \qquad \Big(J_4(0)\Big)^4 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Пример (2.).

$$\Big(J_4(2)\Big)^5 = \begin{pmatrix} 2^5 & 0 & 0 & 0 \\ C_5^1 \cdot 2^4 & 2^5 & 0 & 0 \\ C_5^2 \cdot 2^3 & C_5^1 \cdot 2^4 & 2^5 & 0 \\ C_5^3 \cdot 2^3 & C_5^2 \cdot 2^5 & C_5^1 \cdot 2 & 2^5 \end{pmatrix} = \begin{pmatrix} 2^5 & 0 & 0 & 0 \\ 5 \cdot 2^4 & 2^5 & 0 & 0 \\ 10 \cdot 2^3 & 5 \cdot 2^4 & 2^5 & 0 \\ 10 \cdot 2^3 & 10 \cdot 2^3 & 5 \cdot 2^4 & 2^5 \end{pmatrix} =$$
$$= \begin{pmatrix} 32 & 0 & 0 & 0 \\ 80 & 32 & 0 & 0 \\ 80 & 80 & 32 & 0 \\ 40 & 80 & 80 & 32 \end{pmatrix}$$

Доказательство.

1. Формально — **индукция** по s. На самом деле, повторяем действия из примера

   • **База.** $s = 1$
   $$J_1(0) = (0)$$

   • **Переход.** $s \to s + 1$
   $$J_r^s(0) = a_{ij}, \qquad J_r(0) = b_{ij}, \qquad J_r^{s+1}(0) = c_{ij}$$

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

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

$$c_{ij} = 1 \iff \exists x : \begin{cases} a_{ix} = 1 \\ b_{xi} = 1 \end{cases} \underset{(2)}{\iff} \exists x : \begin{cases} i - x = s \\ x - j = 1 \end{cases} \iff i - j = s + 1$$

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

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

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

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

□

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

$$J = \begin{pmatrix} J_{r_1}(\lambda_1) & . & . \\ . & . & . \\ . & . & J_{r_k}(\lambda_k) \end{pmatrix}, \qquad J - \lambda E = \begin{pmatrix} J_{r_1}(\lambda_1 - \lambda) & . & . \\ . & . & . \\ . & . & J_{r_k}(\lambda_k - \lambda) \end{pmatrix}$$

$$(J - \lambda E)^s = \begin{pmatrix} \Big(J_{r_1}(\lambda_1 - \lambda)\Big)^s & . & . \\ . & . & . \\ . & . & \Big(J_{r_k}(\lambda_k - \lambda)\Big)^s \end{pmatrix}$$

Какое-то из λ_i совпало с λ

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

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

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

  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 клесток, 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
Применяя три случая, получаем, что это равно $f(s+1) - 2f(s) + f(s-1)$ □

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

Доказательство. J, J' — матрицы $\mathcal{A}$
$J - \lambda E, J' - \lambda E$ — матрицы $\mathcal{A} - \lambda\mathcal{E}$
$(J - \lambda E)^s, (J' - \lambda E)^s$ — матрицы $(\mathcal{A} - \lambda\mathcal{E})^s$
rk не зависит от выбора базиса □

19. Минимальный многчлен оператора, у которого известна жорданова форма

Теорема 13 (минимальный многочлен). J — жоданова матрица, $\qquad \lambda_1, \dots, \lambda_k$ — с. ч. J
r_i — максимальный размер жордановой клетки, соотв. λ_i
Тогда минимальный многочлен равен $(t - \lambda_1)^{r_1} \dots (t - \lambda_k)^{r_k}$

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 соответстсвует j-му столбцу клетки $J_r(\lambda)$

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

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

Минимальный многочлен — это НОК многочленов вида $(t - \lambda_i)^s, \quad s \le r_i$
Среди них есть $(t - \lambda_1)^{r_1}, \dots, (t - \lambda_k)^{r_k}$
Значит, среди них есть P_i, а остальные — не делители

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

□

20. Комплексификация вещественного векторного пространства. Продолжение операторов

Мы доказали, что жорданова форма существует, если многочлен раскладывается на простейшие множители. Это всегда верно над $\mathbb{C}$. В этом параграфе рассмотрим жордановы формы над $\mathbb{R}$

Идея построения $\;V$ — вект. пространство над $\mathbb{R}$
Построим $\widehat{V}$ над $\mathbb{C}$, состоящее из $u + vi, \quad u, v \in \mathbb{R}$
Для этого определим сложение и умножение, как в комплексных числах:

- $(u_1 + v_1 i) + (u_2 + v_2 i) = (u_1 + u_2) + (v_1 + v_2)i$
- $(a + bi)(u + vi) = au + bui + avi + bvi^2$

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 $\widehat{V} \times \widehat{V}$, 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 □

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

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

Теорема 15 (базис комплексификации)**.** Пусть $e_1, .., e_n$ — бизс V
Тогда $e_1 = e_1 + 0 \cdot i, \dots, e_n = e_n + 0 \cdot i$ — базс $\widehat{V}$

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 $c_1 e_1 + \dots + c_n e_n = 0, \quad c_s \in \mathbb{C}, \quad c_s = a_+ b_s i, \quad a_s, b_s \in \mathbb{R}$

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

  Разделим вещественную и мнимую части:

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

  Значит, каждое большое слагаемое равно нулю:

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

□

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

Свойства (сопряжённых векторов)**.**

1. $\overline{\overline{w}} = w$

Доказательство. $w = u + vi, \qquad \overline{w} = u - vi, \qquad \overline{\overline{w}} = u - (-v)i = u + vi = w$ □

2. $\overline{w_1 + w_2} = \overline{w_1} + \overline{w_2}, \qquad \overline{z \cdot w} = \overline{z} \cdot \overline{w}$

Доказательство. Первое равенство — упражнение. Проверим второе:
Пусть $z = a + bi, \quad w = u + vi$

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

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

□

3. $w_1, \dots, w_n$ ЛНЗ $\iff \overline{w_1}, \dots, \overline{w_n}$ ЛНЗ

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

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

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

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

$w_1, \dots, w_n$ ЛЗ — $\lightning$ □

21. Каноническая матрица оператора в вещественном пространстве

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

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

Доказательство. Упражнение □

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). $\mathcal{A}$ — оператор на V. Тогда

1. $\widehat{\mathcal{A}}(\overline{w}) = \overline{\widehat{\mathcal{A}}(w)}$
2. $P(\widehat{\mathcal{A}})(w_1) = w_2 \implies \overline{P}(\widehat{\mathcal{A}})(\overline{w_1}) = \overline{w_2}$
3. Если $P(t)$ аннулирует w, то $\overline{P}(t)$ аннулирует $\overline{w}$
4. Если w — корневой вектор, соответствующий λ, то $\overline{w}$ — корневой вектор, соответствующий $\overline{\lambda}$
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 $w = u + iv, \qquad \overline{w} = u - iv$

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

2. Из первого свойства $\widehat{\mathcal{A}}^{(s)}(\overline{w_1}) = \overline{\mathcal{A}^{(s)}(w_1)}$
   Пусть $P(t) = c_k t^k + \dots + c_0$
$$w_2 = c_k P(\widehat{\mathcal{A}})(w_1) + \dots + c_0 w_1$$
$$\overline{w_2} = \overline{c_k} \overline{P}(\widehat{\mathcal{A}})(\overline{w_1}) + \dots + c_0 \overline{w_1} = \overline{P}(\widehat{\mathcal{A}})(\overline{w_1})$$
3. $P(\widehat{\mathcal{A}})(w) = 0 \implies \overline{P}(\widehat{\mathcal{A}})(\overline{w}) \xlongequal[\text{2 св-во}]{} \overline{P(\widehat{\mathcal{A}})(w)} = \overline{0} = 0$
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, соответстсвующему $\overline{\lambda} \implies w$ принадлежит пространству, соотв. λ
     Разложим по базису:
$$\exists\, c_i : \quad w = c_1 e_1 + \dots + c_n e_n$$
$$\implies \overline{w} = \overline{c_1 e_1} + \dots + \overline{c_n e_n}$$
   - Докажем, что сопряжённый к жорданову базису жорданов:
$$\widehat{\mathcal{A} - \lambda \mathcal{E}} = \widehat{\mathcal{A}} - \lambda \widehat{\mathcal{E}}$$
$$(\widehat{\mathcal{A}} - \lambda \widehat{\mathcal{E}}) e_i = e_{i-1} \implies (\widehat{\mathcal{A}} - \overline{\lambda} \mathcal{E}) \overline{e_i} = \overline{e_{i+1}}$$

□

Теорема 16. Пусть V - конечномерное векторное пространство над $\mathbb{R}$, $\mathcal{A}$ — оператор на V
Тогда существует базис V, в котором матрица $\mathcal{A}$ является блочно-диагональной, и каждый блок — либо жорданова клетка, либо имеет вид
$$\begin{pmatrix}
a & b & . & . & . & . & . & . & . & . \\
-b & a & . & . & . & . & . & . & . & . \\
1 & 0 & a & b & . & . & . & . & . & . \\
0 & 1 & -b & a & . & . & . & . & . & . \\
. & . & 1 & 0 & a & b & . & . & . & . \\
. & . & 0 & 1 & -b & a & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & a & b \\
. & . & . & . & . & . & . & . & -b & a
\end{pmatrix}$$

Доказательство. Пусть минимальный многочлен $\mathcal{A}$ равен
$$P(t) = (t - a_1)^{m_1} \dots\dots (t^2 + p_1 t + a_1)^{s_1} \dots\dots$$
где $t + p_1 t + q_1, \dots\dots$ не имеют вещественных корней
Разложим V в прямую сумму примарных подпространств
Достаточно доказать для одного подпростанства
Для пространства, соответствующего $(t-a)^m$ есть базис, в котором матрица $\mathcal{A}$ является блочно-диагональной, и в котром матрица $\mathcal{A}$ жорданова
Рассмотрим подпространство, соответствующе $t^2 + pt + q)^s$:
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 $P_1(\mathcal{A}) = 0$ на корневом подпространстве U

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

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

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 $w_i = u_i + v_i$
Докажем, что $u_1, v_1, u_2, v_2, \ldots, u_k, v_k$ — базис U:
$u_1 + iv_1, u_2 - iv_1, u_2 + iv_2 u_2 - iv_2, \ldots\ldots\ldots$ — базис $\widehat{U}$
$u_1 + iv_1, (u_1 - iv_1) + (u_1 + iv_1), u_2 + iv_2, (u_2 - iv_2) + (u_2 + iv_2), \ldots\ldots\ldots$ — базис $\widehat{U}$
$u_1, u_1 + iv_1, u_2, u_2 + iv_2, \ldots\ldots\ldots$ — базис $\widehat{U}$
$u_1, u_1 + iv_1 - u_1, u_2, u_2 + iv_2 - v_2, \ldots\ldots\ldots$ — базис $\widehat{U}$
$u_1, v_1, u_2, v_2, \ldots\ldots\ldots$ — базис $\widehat{U}$, а значит и базис U
Проверим, что в этом базисе получается правильная жорданова матрица:
Рассмотрим жордановы цепочки

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

Докажем, что им соотвествуют клетки размера $2r_1, 2r_2, \ldots$:
Рассмотрим первую цепочку:

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

Пусть $\lambda = a + bi$
При $m < r$,

$$\mathcal{A}(u_m) + \mathcal{A}(v_m)i = (au_m - bv_m) + (bu_m + av_m)i = \underbrace{(au_m - bv_m + u_{m+1})}_{\mathcal{A}(u_m)} + \underbrace{(bu_m + av_m + v_{m+1})}_{\mathcal{A}(v_m)} i$$

тут надо проверить
При $m = r$,

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

□

Часть II
Линейные отображения в евклидовых и унитарных пространствах

22. Изоморфизм векторного пространства и двойственного к не”-му

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 веторное пространство над K

Доказательство. Очевидно □

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 $n \coloneqq \dim V$
Достаточно доказать, что $\dim V^* = n$ (тогда можно будет построить изоморфизм из базиса в базис)
Зафиксируем базис:
Пусть $e_1, ..., e_n$ – базис V
Пусть $\varphi : V^* \to K^n$ такое, что $\varphi(y) = \Big(\underbrace{y(e_1)}_{\in K}, ..., \underbrace{y(e_n)}_{\in K}\Big)$
Мы знаем, что протранства одной размерности изоморфны, так что $K^n \simeq V$
Докажем, что это изоморфизм:
    - Линейность:
        - Надо проверить, что $\varphi(y_1 + y_2) \stackrel{?}{=} \varphi(y_1) + \varphi(y_2)$
$$\varphi(y_1 + y_2) = \Big((y_1 + y_2)(e_1), \ldots\ldots\ldots\ldots, (y_1 + y_2)(e_n)\Big) =$$
$$= \Big(y_1(e_1) + y_2(e_1), \ldots\ldots\ldots\ldots, y_1(e_n) + y_2(e_n)\Big) \xlongequal[\text{сложение в } K^n \text{ покомпонентно}]{}$$
$$= \Big(y_1(e_1), ..., y_1(e_n)\Big) + \Big(y_2(e_1), ..., y_2(e_n)\Big) = \varphi(y_1) + \varphi(y_2)$$
        - Надо проверить, что $\varphi(ky) \stackrel{?}{=} k\varphi(y)$
$$\varphi(ky) = \Big((ky)(e_1), \ \ldots\ldots, (ky)(e_n)\Big) = \Big(ky(e_1), \ \ldots\ldots, ky(e_n)\Big) =$$
$$\xlongequal[\text{умножение в } K^n \text{ покомпонентно}]{} k\Big(y(e_1), \ \ldots\ldots, y(e_n)\Big) = k\varphi(y)$$
    - Биективность:
    Пусть $a \in K^n, \quad a = (a_1, ..., a_n), \quad a_i \in K$
$$\exists! y \in V^* : \quad \varphi(y) = a$$
    так как
$$\exists! y \in V^* : y(e_1) = a_1, \ldots\ldots\ldots, y(e_n) = a_n$$
2.
    - Проверим, что $y_v \in V^*$, т. е. что y_v линейно:
        - $y_v(x_1 + x_2) = (x_1 + x_2, v) \xlongequal[\text{скалярное произведение линейно по первой координате}]{} (x_1, v) + (x_2, v) = y_v(x_1) + y_v(x_2)$
        - $y_v(kx) = (kx, v) = k(x, v) = ky_v(x)$
    - Пусть $\varphi(v) = y_v$. Докажем, что φ – изоморфизм $V \to V^*$:
        - Линейность:

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

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

> **Замечание.** В унитарном пространстве не будет этого равенства

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

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

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

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

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

□

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

23. Дважды двойственное пространство

Теорема 18 (дважды двойственное пространство). V – векторное пространство над K
Для любого $x \in V$ обозначим через z_x отображение $V^* \to K$, заданное формулой $z_x(\underset{\in V^*}{y}) = \underbrace{y(x)}_{\in K}$

Тогда:

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
• $\varphi(kx) \stackrel{?}{=} k\varphi(x)$
$$z_{kx} \stackrel{?}{=} kz_x$$

$$\forall y \quad z_{kx}(y) \overset{?}{=} kz_x(y)$$

$$y(kx) \overset{?}{=} ky(x)$$

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 $x = 0$ $\iff$ $z_x(y) = 0 \quad \forall y$ $\iff$ $y(x) = 0 \quad \forall y$
Нужно проверить, что $\forall x \neq 0 \quad \exists$ 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, $\quad e_1, ..., e_n$ – базис V
$f_1, ..., f_n \in V^*$ такие, что $f_i(e_i) = 1, \quad f_i(e_j) = 0$ при $i \neq j$ (здесь существование не утверждается, но понятно, что их всегда можно построить)
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 $f = a_1 f_1 + ... + a_n f_n$ – 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. $e_1, ..., e_n$ – базис V, $\quad f_1, ..., f_n$ – базис V^*, $\quad f_i(e_i) = 1, \quad f_i(e_j) = 0$ при $i \neq j$
Тогда $f_1, ..., f_n$ называется двойственным базисом к $e_1, ..., e_n$

Напоминание. e_i, e'_i – базисы V
Матрицей перехода от e_i к e'_i называется такая матрица C, что в i-м столбце записаны координаты e'_i в $e_1, ..., e_n$
Пусть X, X' – координаты c в e_i, e'_i. Тогда $X = CX'$

Теорема 19. e_i, e'_i – базисы V, $\quad C$ – матрица перехода от e_i к e'_i
f_i, f'_i – соответствующие двойственные базисы
Тогда:

1. Матрица перехода от f_i к f'_i равна $(C^{-1})^T = (C^T)^{-1}$
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 $U = E$

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

Применим одно к другому:

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

$$= d_{1j}c_{1i} \cdot 1 + d_{1j}c_{2i} \cdot 0 + \ \dots\dots \ + d_{2j}c_{1i} \cdot 0 + d_{2j}c_{2i} \cdot 1 + \ \dots\dots \ = d_{1j}c_{1i} + d_{2j}c_{2i} + \ \dots\dots$$

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

Обозначение. $\mathcal{A}^*$

Свойства.

1. $(\mathcal{A}^*)^* = \mathcal{A}$
2. Пусть A, A^* – матрицы $\mathcal{A}, \mathcal{A}^*$ в некотором ОНБ
Тогда
   - $A^* = A^T$ в евклидовом пространстве
   - $A^* = \overline{A}^T$ в унитарном пространстве

Определение 28. Оператор в веклидовом или унитарном пространстве назвыается

- нормальным, если $\mathcal{A}^*\mathcal{A} = \mathcal{A}\mathcal{A}^*$
- ортогональным (унитарным), если $\mathcal{A}\mathcal{A}^* = \mathcal{A}^*\mathcal{A} = \mathcal{E}$
- самосопряжённым, если $\mathcal{A}^* = \mathcal{A}$

Определение 29. Квадратная матрица называется

- симметричной (симметрической), если $A = A^T$
- эрмитовой, если $A = \overline{A}^T$

Свойство. $\mathcal{A}$ – оператор в евлидовом/унитарном пространстве, $\quad A$ – его матрица **в ОНБ**
Тогда
$\mathcal{A}$ самосопряжённый $\iff$ A симметрична/эрмитова

Теорема 20. $\mathcal{A}$ – нормальный оператор в унитарном пространстве
Тогда

1. если λ – с. ч. $\mathcal{A}$, то $\overline{\lambda}$ – с. ч. $\mathcal{A}^*$
2. с. в. $\mathcal{A}^*$, соответствующие разным с. ч. ортогональны
3. Существует ОНБ, состоящий из с. в. $\mathcal{A}$ $\implies$ он диагонализуем

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

Доказательство.

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

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

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

$\square$

Определение 30. Самосопряжённый оператор назвыается положительно определённым, если

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

Обозначение. $a_i \in \odot \quad \iff a_1 = \dots = a_n = 0$

Теорема 21 (о собственных числах самосопряжённого оператора).
$\mathcal{A}$ – оператор на унитарном пространстве

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

Доказательство.

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

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

2. Пусть e_i – ОНБ из с. в., λ_i – с. ч., $\lambda_i \in \mathbb{R}$ (т. к. самосопр. – частный случай нормального)
   Пусть $x = a_1e_1 + \dots + a_ne_n$

$$(\mathcal{A}x, x) = (a_1\lambda_1e_1 + \dots + a_n\lambda_ne_n, \quad a_1e_1 + \dots + a_ne_n) = \sum \lambda_i a_i \overline{a_j} \underbrace{(e_i, e_j)}_{0 \text{ или } 1} =$$

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

   - 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 $x = e_{i_0}$ $x \neq 0$, $(\mathcal{A}x, x) = \lambda_{i_0} \leq 0$ – $\lightning$

$\square$

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

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

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

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

Замечание. Доказательство для $\mathbb{C}^n$ здесь не пожходит

Доказательство.

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

□

Теорема 22. $\mathcal{A}$ – самосопряжённый оператор на $\mathbb{R}^n$
Тогда

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

Доказательство.

1. Разложим $\chi_A(t)$ на линейные множиетли над $\mathbb{C}$:
$$\chi_A(t) = (-1)^n(t - \lambda_1)...(t - \lambda_n), \qquad \lambda_i \in \mathbb{C}$$
Пусть A – матрица $\mathcal{A}$ 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. $\chi_A(t)$ раскладывается на линейные множители над $\mathbb{R}$
$\mathcal{A}$ диагонализуем над $\mathbb{C}$. Есть базис из с. в. в $\mathbb{C}^n$
$\implies$ есть базис из с. в. в $\mathbb{R}^n$ (т. к. $\mathbb{R}$ – поле, там неоткуда взяться комплексным числам, а коэффициенты изначально были вещественные, *надо нормально это записать*)
$\implies \dim U_{\lambda_i} = r_i$
Выберем ОНБ в каждом подпространстве U_{λ_i}
По лемме об ортогональный с. в. объединение этих базисов – ОНБ $\mathbb{R}^n$

□

27. Корень из самосопряжённого оператора. Полярное разложение

Теорема 23 (корень из самосопряжённого оператора).
$\mathcal{A}$ – положительно определённый самосопряжённый
Тогда существует положиетльно определённый самосопряжённый $\mathcal{B}$: $\mathcal{A} = \mathcal{B}^2$ в смысле композиции

Доказательство. $\mathcal{A}$ – самосопряжённый $\implies$ $\mathcal{A}$ – нормальный $\implies$ $\exists$ ОНБ из с. в. $\mathcal{A}$
Пусть $e_1, ..., e_n$ – ОНБ из с. в., $\lambda_1, ...\lambda_n$ – с. ч.
$\mathcal{A}$ – самосопряжённый $\implies$ $\lambda_i \in \mathbb{R}$
$\mathcal{A}$ – полож. опред. $\implies$ $\lambda_i > 0$
Определим $\mathcal{B}$ как $\mathcal{B}(e_i) = \sqrt{\lambda_i} e_i$
Проверим, что он подойдёт:
Рассмотрим матрицу $\mathcal{B}$ в базисе $e_1, ..., e_n$:

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

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

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

□

Лемма 10. $\mathcal{A}$ невырожденный
Тогда $\mathcal{A}\mathcal{A}^*$ - самосопряжённый положительно определённый

Доказательство.

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

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

□

Теорема 24 (полярное разложение оператора).
$\mathcal{A}$ – невырожденный (обратимый) оператор на унитарном пространстве
Тогда $\exists \mathcal{U}, \mathcal{B}$ такие, что:

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

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

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

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

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

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

□

Следствие (перестановка сомножителей). $\mathcal{A}$ – невырожденный оператор
Тогда $\exists$ уинтарный $\mathcal{U}$ и самосопряжённый положиетльно определённый $\mathcal{B}$ такие, что $\mathcal{A} = \mathcal{B}\mathcal{U}$

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

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

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

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

28. Квадратичные формы: ортогональное преобразование, преобразование двух форм

A – симметрическая матрица, $\quad A = (a_{ij})$
Соответствующая квадратичная форма $f(x_1, ..., x_n) = \sum a_{ij}x_ix_j$
Матричная запись: $f(x_1, ..., x_n) = X^TAX$
Линейное преобразование $X = CY \quad \Longrightarrow \quad A \mapsto C^TAC$
Неособое преобразование: C обратима
Диагональный (канонический) вид – если A – диагональна

Теорема 25 (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

Пример.

$$\underbrace{2x_1^2 + x_2^@ - 4x_1x_2 - 4x_2x_3}_{Q} + 12x_1 - 8x_2 + 8x_3 + 6 = 0$$

Приведём Q к диагональному виду:

$$C = \begin{pmatrix} 2/3 & 2/3 & 1/3 \\ -2/3 & 1/3 & 2/3 \\ 1/3 & -2/3 & 2/3 \end{pmatrix}$$

С. ч.: $\lambda_1 = 4, \quad \lambda_2 = 1, \quad \lambda_3 = -2$

$$4y_1^2 + 1y_2^2 - 2y_3^2 + 12\left(\frac{2}{3}y_1 + \frac{2}{3}y_2 + \frac{1}{3}y_3\right) - 8$$

$$4y_1^2 + 16y_1 = 4(y_1 + 2)^2 - 16$$

TODO: Этот пример есть в Боревиче. Надо посмотреть

Доказательство.

1. $\mathcal{A}$ – оператор на $\mathbb{R}^n$, матрица в стандартном базисе TODO: что-то
   $\mathcal{A}$ самосопряжённый $\Longrightarrow \exists$ ОНБ $T_1, ..., T_n$ из с. в.
   Пусть $\lambda_1, ..., \lambda_n$ – с. ч.
   Матрица $\mathcal{A}$ в $T_1, ..., T_n$ является диагональной
   Матрица $\mathcal{A}$ 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, $\quad \mu_1, ..., \mu_n$ – числа на диагонали
   $S_1, ..., S_n$ – столбцы $B \quad \Longrightarrow \quad B = C^{-1}AC \quad \Longrightarrow \quad B$ – матрица $\mathcal{A}$ в ОНБ $S_1, ..., S_n \quad \Longrightarrow \quad \mathcal{A}S_i = \mu_iS_i \quad \Longrightarrow \quad \mu_i$ – с. ч.

☐

Теорема 26 (преобразование двух форм).
$f(x_1, ..., x_n)$, $g(x_1, ..., x_n)$ – вещественные квадратичные формы, f положительно определена
Тогда существует неособое преобразование, при котором обе формы приводятся к диагональному виду

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

1. Приведём f к диагональному виду f_1:
$$f_1(y_1, ..., y_n) = \lambda_1 y_1^2 + ... + \lambda_n y_n^2, \qquad \lambda_i > 0$$
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 перобразованием C
Матрица f_2 равна E
$$E \to C^T E C = C^T C = E$$
Значит, f приведена к диагональному виду

□

Часть III
Кольца и поля

29. Идеал кольца. Примеры 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. $a \in I,\ t \in A \implies ta \in I$

Примеры.

1. $\{ 0 \}, A$ – идеалы
2. $A = \mathbb{Z}$
$I = 2\mathbb{Z}$ – идеал:
   (a) i. $a \vdots 2, b \vdots 2 \implies a + b \vdots 2$
       ii. $a \vdots 2 \implies -a \vdots 2$
   (b) $a \vdots 2,\ t \in \mathbb{Z} \implies ta \vdots 2$

   Аналогично $k\mathbb{Z}$ – идеал $\quad \forall k$
3. $\mathbb{R}[x]$
   (a) $I = \{ p(x) = a_n x^n + ... + a_1 x \}$ Свободный член равен 0

(b) $I = \{ s_n x^n + \ldots + a_k x^k \}$
k – фиксированный

(c) $I = \{ p(x) \mid p(1) = 0 \}$

i. $p(1) = 0, q(1) = 0 \implies (p+q)(1) = 0$

ii. $p(1) = 0 \implies -p(1) = 0$

iii. $p(1) = 0, \ \forall q \implies (pq)(1) = p(1)q(1) = 0$

(d) I – множество многочленов, делящихся на заданный $p_0(x)$

4. $A = \mathbb{Z}_{10}$
$I = \{ 0, 2, 4, 6, 8 \}$ – идеал

5. $\mathbb{Z}[x]$
I – множество многочленов с чётным свободным членом

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

Обозначение. $\langle S \rangle$

Свойства.

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

Определение 33. Идеал, порождённый одним элементом, называется главным

Примеры.

1. $\mathbb{Z}$
$m\mathbb{Z} = \langle m \rangle$ – главный

2. A – любое коммутативное ассоциативное кольцо с единицей

$$\langle 0 \rangle = \{ 0 \}, \qquad \langle 1 \rangle = A$$

> **Замечание.** Если идеал содержит единицу, то это всё кольцо:
>
> $$a \cdot 1 \in I \quad \forall a \in A$$

3. $A = \mathbb{Z}[x]$
I – множество многочленов с чётным свободным членом

$$I = \langle 2, x \rangle$$

4. K – поле, $\quad K[x, y]$ – кольцо многочленов от двух переменных, т. е. многочленов вида $\sum a_{ij} x^i y^j$, только конечное число a_{ij} отлично от нуля
I – мноежство многочленов таких, что $a_{00} = 0$
$I = \langle x, y \rangle$ – не главный

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

Теорема 27 (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 $I = \langle a \rangle$:
     $\langle a \rangle$ – мноежство 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:

   - $\{ 0 \} = \langle 0 \rangle$
   - Если $I \neq \{ 0 \}$, то $I = \langle p \rangle$, где p – многочлен наименьшей степени, лежащий в I

$\square$

Замечание. Любое евклидово кольцо – кольцо главных идеалов
Не доказываем, т. к. долго вспоминать, что такое евклидово кольцо
Доказательство то же (берём элемент с наименьшей евклидовой нормой)

Определение 35. A – коммутативное ассоциативное кольцо, $\qquad I$ – идеал
I называется простым, если
$$\forall a, b \in A \quad ab \in I \implies a \in I \quad \text{или} \quad b \in I$$

Пример. $\mathbb{Z}$, $\qquad I = \langle k\mathbb{Z} \rangle$
I простой $\iff k \in \mathbb{P}$

Доказательство.
$$a, b \in I \overset{?}{\implies} a \in I \quad \text{или} \quad b \in I$$
$$ab \,\vdots\, k \overset{?}{\implies} \left[\begin{array}{l} a \,\vdots\, k \\ b \,\vdots\, k \end{array} \right.$$
Это верно для простого k и не верно для составного $\square$

K – поле, $\qquad A = K[x]$
$\langle p(x) \rangle$ простой $\iff p(x)$ неприводим
K – поле, $\qquad A = K[x, y]$
$$I = \langle x \rangle, \qquad J = \langle x, y \rangle$$
Оба простые

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

Примеры.

1. $A = \mathbb{Z}$, $\qquad I = \langle k \rangle$
   I – максимальный $\iff k \in \mathbb{P}$
   Например,

   (a) $k = 10$
   $$\langle 10 \rangle \subset \langle 2 \rangle$$

   (b) $k = 5$
   Пусть $\langle 5 \rangle \subset J$

$J = \langle d \rangle$, т. к. все идеалы главные

$$\langle 5 \rangle \subset \langle d \rangle \implies 5 \,\vdots\, d \implies \left[\begin{array}{l} d = \pm 5 \implies J = I \\ d = \pm 1 \implies J = A \end{array} \right.$$

2. $K[x, y]$
   $\langle x \rangle$ – не максимальный, $\langle x \rangle \subset \langle x, y \rangle$
   $\langle x, y \rangle$ – максимальный

Замечание. Любой максимальный идеал простой

30. Построение факторкольца. Факторкольцо по простому идеалу

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

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

Примеры.

1. $\mathbb{Z}$, $\quad I = \langle k \rangle$
$$a \underset{\langle k \rangle}{\equiv} b \iff a \underset{k}{\equiv} b$$
2. $\mathbb{Z}[x]$, $\quad I = \langle 2, x \rangle$
   $P(x) \underset{I}{\equiv} Q(x)$, если свободные коэффициенты одной чётности

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

$\square$

Определение 38. A – коммутативное кольцо, 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 28 (корректность). A – коммутативное ассоциативное кольцо, I – идеал
Тогда

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

Доказательство.

1. $$x_1, x_2 \text{ в одном классе } \} \overset{?}{\Longrightarrow} \begin{cases} x_1 + y_1 \text{ и } x_2 + y_2 \text{ в одном классе} \\ x_1 y_1 \text{ и } x_2 y_2 \text{ в одном классе} \end{cases}$$

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

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

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

   TODO: надо дописать

   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

Примеры.

1. $\mathbb{Z}/\langle m \rangle = \mathbb{Z}_m$

2. $A/\langle 0 \rangle \simeq A$
   A/A – кольцо из одного элемента

3. $\mathbb{R}[x]/\langle x^2 + 1 \rangle$

   Утверждение 2. Классы вычетов имеют вид $\overline{ax + b} = \overline{a} \cdot \overline{x} + \overline{b}$

   Доказательство. Рассмотрим класс $T, \qquad P(x) \in T$
   Поделим $P(x)$ на $x^2 + 1$ с остатком:

   $$P(x) = (x^2 + 1)Q(x) + (ax + b), \qquad a, b \in \mathbb{R}$$

   $$P(x) - (ax + b) = (x^2 + 1)Q(x) \in \langle x^2 + 1 \rangle$$

   $$P(x) \underset{\langle x^2+1 \rangle}{\equiv} ax + b \Longrightarrow ax + b \in T$$

   □

   Значит, в каждом классе можно выбрать представителя вида $ax + b$, причём единственным образом

   $$\overline{x} \cdot \overline{x} = \overline{x^2} = \overline{x^2 - (x^2 + 1)} = \overline{-1}$$

   Если обозначить $\overline{x}$ за i, то $i^2 = 1$. Получаем $\mathbb{C}$

Теорема 29 (факторкольцо по простому идеалу)**.** A – коммутативное ассоциативное кольцо, I – идеал. Следующие условия равносильны:

1. I – простой

2. $\frac{A}{I}$ – область целостности

Доказательство. Пусть $X \in {}^{A}\!/_{I}, \quad x \in X$
Тогда $X = 0 \iff \overline{x} = \overline{0} \iff x \underset{I}{\equiv} 0 \iff x - 0 \in I \iff x \in I$

- $(1) \implies (2)$
  Пусть $X, Y \in {}^{A}\!/_{I}, \qquad XY = \overline{0}$
  Пусть $x \in X, \quad y \in Y \implies \overline{xy} = \overline{0} \implies xy \in I \xRightarrow[I\text{ простой}]{} \left[\begin{array}{l} x \in I \implies X = \overline{0} \\ y \in I \implies Y = \overline{0} \end{array}\right.$
- $(2) \implies (1)$
  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 30 (факторкольцо по максимальному идеалу). A – коммутативное ассоциативное кольцо с единицей, I – идеал. Следующие условия равносильны:

1. I – максимальный
2. ${}^{A}\!/_{I}$ – поле

Доказательство.

- $(1) \implies (2)$
  ${}^{A}\!/_{I}$ – 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 $x \in X \implies x \in I$
  Пусть $J := \langle x, I \rangle$ (он существует, это обсуждалось в прошлый раз)
  $$J \supset I, \ J \neq I \xRightarrow[I\text{ – макс.}]{} J = A \implies A \in J$$
  $$1 \in \langle I, x \rangle \implies 1 = \underbrace{a_1 s_1 + \ldots + a_k s_k}_{\in I} + bx \text{ для некоторых } s_i \in I, \quad a_i, b \in A$$
  $$\implies 1 \equiv bx \pmod I \implies \overline{1} = \overline{b} \cdot \overline{x} = \overline{b}X \implies \overline{b} = X^{-1}$$
- $(2) \implies (1)$
  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 $\overline{y} \in Y \implies \overline{x} \cdot \overline{y} = \overline{1} \implies xy - 1 \in I$
  $$\left.\begin{array}{l} x \in J \\ xy - 1 \in I \end{array}\right\} \implies 1 = \underbrace{xy}_{\in J} - \underbrace{(xy-1)}_{\in I} \in J \implies J = A$$

□

Замечание. Поле является областью целостности $\implies$ в кольце с единицей максимальный идеал является простым

Теорема 31 (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), $B = A/I$
Тогда равносильны условия:

1. P неприводим $\iff$ A/I – поле

Доказательство. Правая часть равносильна тому, что I максимальный

- $\implies$
  Пусть $I \in J$, $Q(x)$ – такой, что $J = \langle Q(x) \rangle$

$$\langle P(x) \rangle \subset \langle Q(x) \rangle \implies P(x) \mathrel{\vdots} Q(x) \xRightarrow[P \text{ неприводимый}]{} \\ \implies \left[\begin{array}{l} Q(x) = cP(x), \quad c \in K, \quad c \neq 0 \implies J = I \\ Q(x) = c, \quad c \in K, \quad c \neq 0 \implies J = A \end{array} \right. \implies I \max$$

- $\impliedby$
  Пусть P приводим

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

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

□

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

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

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

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. $A \simeq B$

Все тривиальные свойства верны: про обратный, про композицию, про отношение “эквивалентности” (настоящей эквивалентности здесь нет – нет множества всех колец)

Определение 43. A, B – цольцо, $f : A \to B$ – гомоморфизм
Ядро: $\{ x \in A \mid f(x) = 0 \}$

Обозначение. $\ker f$

Образ: $\{ f(x) \mid x \in A \}$

Обозначение. $\operatorname{Im} A$

Свойства. A, B – коммутативные, $f : A \to B$ - гомоморфизм

1. $f(0) = 0$

   Замечание. Коммутативность здесь не нужна

   Замечание. Для единицы не верно

2. $\ker f$ – идеал

3. $\operatorname{Im} f$ – подкольцо B

Доказательство.

1. Следует из аналогичного свойства для гомоморфизма групп

2. $\ker f \neq 0$, 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 32 (о гомоморфизме колец). A, B – коммутативные ассоциативные кольца
$f : A \to B$ – гомоморфизм
Тогда ${}^{A}\!/\!{}_{\ker f} \simeq \operatorname{Im} f$

Доказательство. Определим $\varphi : {}^{A}\!/\!{}_{\ker f} \to \operatorname{Im} f$
Пусть $X \in {}^{A}\!/\!{}_{\ker f}, \quad x \in X$
Положим $\varphi(X) := f(x)$
$$x \in X \implies X = \overline{x} \implies \varphi(\overline{x}) = f(x)$$

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

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

- 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

$$\underbrace{a + a + ... + a}_{n} = 0 \quad \forall a \in A$$

Если такого n не существует, то характеристика равна нулю

Определение 45. $\operatorname{char} A$

Примеры. $\mathbb{R}, \mathbb{Z}, \mathbb{Q}$ – $\operatorname{char} = 0$
$\operatorname{char}(\mathbb{Z}_2) = 2$

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

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

Доказательство. Нужно доказать, что

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

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

$\square$

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

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

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

Получили противоречие с минимальностью n $\square$

NB. Достаточно области целостности с единицей

Определение 46. L – поле, $\qquad K \subset L, \qquad K$ является полем с теми же операциями
Тогда K называется подполем L
L называется расширением K

Примеры.

1. $\mathbb{R}$ – подполе $\mathbb{C}$
2. $\mathbb{R}(x)$ – расширение $\mathbb{R}$

Определение 47. Поле K называется простым, если оно не содержит подполей, отличных от K (считаем, что поле не может состоять из одного элемента, т. е. $0 \neq 1$)

Теорема 33 (классификация простых полей).

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

Доказательство.

1. • $\mathbb{Q}$
   Пусть $\mathbb{Q}$ **не простое**, и K – подполе $\mathbb{Q}$ $\implies 0, 1 \in K$

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

   Если $n \in K$, то $(-1) \in K \quad \implies \mathbb{Z} \subset K$
   Если $n \in K,\ n \neq 0$, то $\frac{1}{n} \in K \quad \implies \frac{1}{n} \in K \quad \forall n \in \mathbb{N}$

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

   • $\mathbb{Z}_p$
   Аналогично, пусть K – подполе $\mathbb{Z}_p$

$$\overline{1} \in K$$

$$\underbrace{\overline{1} + \overline{1} + \dots + \overline{1}}_{n} \in K \quad \forall n \quad \implies \overline{n} \in K \quad \forall n \quad \implies \mathbb{Z}_p = K$$

2. Пусть K — поле
   Докажем, что K содержит подполе, изоморфное $\mathbb{Q}$ или $\mathbb{Z}_p$
   Возьмём A — минимальное подкольцо K, содержащее 1
   Докажем, что $A \simeq \mathbb{Z}$ (взяв все частные из A, получим множество дробей) или $A \simeq \mathbb{Z}_p$:
   Пусть $f : \mathbb{Z} \to A$ такое, что

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

   • 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 $k_1 := -k$

$$f\Big(n(-k_1)\Big) = f(n)f(-k_1) \quad \Longleftarrow \quad -f(nk_1) = f(n)\Big(-f(k_1)\Big)$$

     По теореме о гомомрфизме $\operatorname{Im} f \simeq \mathbb{Z}/_{\ker f}$
     $\operatorname{Im} f$ — подкольцо A
     $\ker f$ — идеал $\implies \ker f = \langle m \rangle$
       ∗ $m = 0$

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

* $m \neq 0$

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

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

□

Замечание. Характеристику можно определять по простому полю:

$$K \simeq \mathbb{Z}/_{\langle m \rangle} \implies \operatorname{char} \mathbb{Z} = m$$

Отсюда видно, почему характеристика 0, если не существует нужной степени

34. Степень расширения. Мультипликативность степени, следствия

Лемма 11. K — поле, 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:

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

□

Примеры.

1. $\mathbb{R} \subset \mathbb{C}$
   Базис — $\{ 1, i \}$
2. $\mathbb{R}(x)$ — бесконечномерное векторное пространство над $\mathbb{R}$

Определение 48. L — расширение K
Степенью расширения L над K называется $\dim_K L$

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

Если $|L : K|$, то L — конечное расширение K (L конечно над K)
Иначе — бесконечное

Примеры.

1. $|\mathbb{C} : \mathbb{R}| = 2$
2. $|\mathbb{R}(x) : \mathbb{R}| = \infty$
3. $|K : K| = 1$
   Базис — $\{ 1 \}$ ($k \cdot 1$ — множество всех $k \in K$)
   Если $K \subset L$, $|L : K| = 1$, то $L = K$
4. $\mathbb{Q}(\sqrt{2})$ — наименьшее поле, содержащее $\mathbb{Q}$ и $\sqrt{2}$
   Такое поле существует, т. к. $\mathbb{Q} \subset \mathbb{R}$, $\sqrt{2} \in \mathbb{R}$, можно взять наименьшее подполе $\mathbb{R}$, которое содержит $\mathbb{Q}$ и $\sqrt{2}$

Оно состоит из чисел вида $a+b\sqrt{2}$
Проверим, что это поле:

$$(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2db)+(ad+bc)\sqrt{2}$$

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}\sqrt{2}$$

$$|\mathbb{Q}(\sqrt{2}):\mathbb{Q}| = 2$$

Базис — $\{\, 1, \sqrt{2} \,\}$

5. $\mathbb{Q}(\sqrt{2}, i)$ — наименьшее поле, содержащее $\mathbb{Q}, \sqrt{2}, i$
Оно аналогично является подполем $\mathbb{C}$

Утверждение 3. $|\mathbb{Q}(\sqrt{2}, i):\mathbb{Q}| = 4$

Доказательство.

$$\mathbb{Q}(\sqrt{2}, i) = \left\{\, a+bi \mid a, b \in \mathbb{Q}(\sqrt{2}) \,\right\}$$

$|\mathbb{Q}(\sqrt{2}, i):\mathbb{Q}(\sqrt{2})| = 2$, базис — $\{\, 1, i \,\}$
Базис $\mathbb{Q}(\sqrt{2}, i)$ над $\mathbb{Q}$: $\{\, 1\cdot 1, 1\cdot i, \sqrt{2}\cdot 1, \sqrt{2}\cdot i \,\}$ □

Теорема 34 (мультипликативность степени). $K \subset M \subset L$ — поля с общими операциями
Тогда $|L:K| = |L:M|\cdot|M:K|$

NB. Если M конечно над K и L конечно над M, то L конечно над K и выполнено равенство
Иначе L бесконечно над K

Доказательство.

- Докажем, что если $e_1, \ldots, e_r \in M$ ЛНЗ над K и $f_1, \ldots, f_s \in L$ ЛНЗ над M, то $g_{ij} \coloneqq e_i f_j$ ЛНЗ над K:
  Пусть $a_{ij} \in K : \sum a_{ij} g_{ji} = 0$

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

  Сгруппируем по элементам f:

  $$\Big(a_{11}e_1f_1 + a_{21}e_2f_1 + \ldots\Big) + \Big(a_{12}e_1f_2 + a_{22}e_2f_2 + \ldots\Big) + \ldots\ldots\ldots = 0$$

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

  Пусть $b_j \coloneqq a_{1j}e_1 + a_{2j}e_2 + \cdots + a_{rj}e_r$
  Тогда $b_j \in M, \quad b_1f_1 + \ldots b_sf_s = 0$
  $f_1, \ldots f_s$ ЛНЗ над $M \implies b_1 = b_2 = \cdots = b_s = 0$

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

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

- Конечный случай
  Пусть $e_1, \ldots, e_r$ — базис M над K, $\quad f_1, \ldots, f_s$ — базис L над M
  Докажем, что $g_{ij} \coloneqq e_i f_j$ — базис L над K:
  ЛНЗ уже доказана. Осталось доказать, что любой элемент порождается g_{ij}:
  Пусть $c \in L \quad \implies \exists b_i \in M : \quad c = b_1f_1 + \cdots + b_sf_s$

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

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

- 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 $e_i f_j$ ЛНЗ над K

$\square$

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

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

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

Пример. Не существует поля $M : \quad \mathbb{R} \subset M \subset \mathbb{C}$, отличного от них
По основной теореме алгебры поле $\mathbb{C}$ большое — в нём есть корень любого многочлена
С другой стороны, оно маленькое — только что мы выяснили, что оно довольно близко к $\mathbb{R}$

Следствие. $K \subset M \subset L$
Тогда

- 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

Пример. $\mathbb{R}(x)$ над $\mathbb{R}$ бесконечно
Значит, не существует $M : \quad \mathbb{R} \subset M \subset \mathbb{R}(x)$, и M кончено над $\mathbb{R}$, и $\mathbb{R}(x)$ конечно над M

Замечание. Нельзя построить “башню” из любого количества полей так, чтобы все шаги были конечны

35. Минимальный многочлен алгебраического элемента. Конечность алгебраического расширения

Определение 49. 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 50. α — алгебраическое над K, $\qquad P(x) \in K[x], \qquad P(\alpha) = 0.$
Тогда

- $P(x)$ — алгебраический над α
- $P(x)$ аннулирует α

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

Определение 51. Алгебраическим числом называется комплексное число, алгебраическое над $\mathbb{Q}$

Примеры. $K = \mathbb{Q}, \quad L = \mathbb{C}$

1. $\alpha = i$ — алгебраическое
   Минимальный многочлен $P(x) = x^2 + 1$

2. $\alpha = \sqrt[3]{5}$
   $P(x) = x^3 - 5$ — аннулирующий, минимальный

3. $\alpha = 1 + \sqrt[3]{5}$ — алгебраическое
   Найдём аннулирующий многочлен:
$$(\alpha - i)^3 = 5$$
$$\alpha^3 - 3\alpha^2 i + 3\alpha i^2 - i^3 = 5$$
$$(\alpha^3 - 3\alpha - 5) + (-3\alpha + 1)i = 0$$
$$\alpha^3 - 3\alpha - 5 = (-3\alpha + 1)i$$
$$(\alpha^2 - 3\alpha - 5)^2 = -(-3\alpha + 1)^2$$
$$(\alpha^3 - 3\alpha + 5)^2 + (3\alpha + 1)^2 = 0$$
$$P(x) = (x^3 - 3x + 5)^2 + (3x + 1)^2$$

4. $\alpha = \sqrt[3]{2 + 4\sqrt[4]{5}}$ — алгебраич.
$$\alpha^3 = 2 + 4\sqrt[4]{5}$$
$$\alpha^3 - 2 = 4\sqrt[4]{5}$$
$$(\alpha^3 - 2)^4 = 4^4 \cdot 5$$
$$(\alpha^3 - 2)^4 - 4^4 \cdot 5 = 0$$
$$P(x) = (x^3 - 2)^4 - 4^4 \cdot 5$$

5. e, π — трансцендентные

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

1. Пусть $P(x)$ — минимальный для α.
   Тогда
$$F(\alpha) = 0 \iff F(x) \vdots P(x)$$

2. Минимальный многочлен для α единственен

3. Минимальный многочлен неприводим над K

4. Если $P(x)$ неприводим над K, $P(x) \neq 0$, $P(\alpha) = 0$
$$\implies P(x) \text{ — минимальный для } \alpha$$

Доказательство.

1.
$$F(x) = P(x)Q(x) + R(x), \qquad \deg R < \deg P$$

   - $\Longleftarrow$
$$F(x) \vdots P(x) \implies R(x) = 0$$
$$F(x) = P(x)Q(x)$$
     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 $P(x) = S(x)T(x), \quad 0 < \deg S, \deg T < \deg P$

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

4.
$$\left.\begin{array}{l} P(x) \vdots \text{ миним.} \\ P(x) - \text{неприводим.} \end{array}\right\} \implies P(x) - \text{миним.}$$

□

Пример. $x^3 - 5$ — минимальный для $\sqrt[3]{5}$ над $\mathbb{Q}$, т. к. он неприводим над $\mathbb{Q}$

Определение 52. Расширение L над K называется алгебраическим, если любой элемент L является алгебраическим над K
Иначе — тренсцендентным

Теорема 35. 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. □

36. Строение простого алгебраического расширения. Следствия

Определение 53. 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 оного элемента, называется простым расширением K.

Пример. $\mathbb{Q}(\sqrt{2})$ — простое расширение $\mathbb{Q}$

Теорема 36 (строение простого алгебраического расширения). L — поле, $\qquad K$ — подполе L, $\qquad \alpha \in L$, $\qquad \alpha$ алг. над K, $\qquad P(x)$ — минимальный многочлен для α над K
Тогда

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

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

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

- 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 гомомрфизме:

$$\operatorname{Im} f \simeq {}^{K[x]}\!\big/_{\ker f}$$

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

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

$$\left.\begin{aligned} &\alpha \in \operatorname{Im} f, \ \text{т. к.} \alpha = f(x) \\ &K \subset \operatorname{Im} f, \ \text{т. к.} \underset{\in K}{k} = f(k) \end{aligned}\right\} \xRightarrow[\operatorname{Im} f \text{ — поле}]{} \operatorname{Im} f \supset K(\alpha)$$

- 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 $F(x) \coloneqq a_0 + a_1 x + \dots + a_{n-1}x^{n-1} \implies F(\alpha) = 0$
  $$\implies F(x) \vdots P(x) \xRightarrow[F(x) \text{ — ненулевой}]{} \deg F \geq \deg P = n \quad ↯$$

  - Попрождающий:
  $$K(\alpha) = \operatorname{Im} f$$
  Пусть $u \in K(\alpha) \implies \exists\, F \in K[x] : \quad f(F) = u \quad \implies F(\alpha) = u$
  Делим с остатком:
  $$F(x) = Q(x)P(x) + R(x), \qquad \deg R < \deg P$$
  $$\implies \deg R \leq n + 1$$
  $$F(\alpha) = Q(\alpha)\underbrace{P(\alpha)}_{0} + R(\alpha) = R(\alpha)$$
  $$R(x) = a_0 + a_1 x + \dots a_{n-1}x^{n-1} \implies F(\alpha) = a_0 + a_1\alpha + \dots a_{n-1}\alpha^{n-1}$$

□

Примеры.

1. $\mathbb{Q}(\sqrt[3]{2}), \quad \alpha = \sqrt[3]{2}$
$1, \sqrt[3]{2}, (\sqrt[3]{2})^2$ — базис ${}^{\mathbb{Q}(\sqrt[3]{2})}\!\big/_{\mathbb{Q}}$.
Любой элемент можно представить в виде $a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2, \quad a, b, c \in \mathbb{Q}$.
Пример сложения:
$$\left(1 + 2\sqrt[3]{2} + 3(\sqrt[3]{2})^2\right) + (-1 + \sqrt[3]{2}) = 3\sqrt[3]{2} + 3(\sqrt[3]{2})^2$$
Пример умножения:
$$(1 + \sqrt[3]{2})(2\sqrt[3]{2} + 3\sqrt[3]{2})^2 = 2\sqrt[3]{2} + 3(\sqrt[3]{2})^2 + 2\sqrt[3]{2}^2 + 3(\sqrt[3]{2})^3 = 2\sqrt[3]{2} + 5(\sqrt[3]{2})^2 + 6$$

2. $P(x) = x^5 - 5x^4 + 5$ — неприводимый над $\mathbb{Q}$ по критерию Эйзенштейна
$$x^5 - \underset{\vdots 5}{5}x^4 + \underset{\vdots 5}{0}x^3 + \underset{\vdots 5}{0}x^2 + \underset{\vdots 5}{0}x + \underset{\vdots 5}{5}$$

α — комплексный корень

$$K = \mathbb{Q}, \quad L = \mathbb{C}$$

Рассмотрим $\mathbb{Q}(\alpha)$:

$$|\mathbb{Q}(\alpha) : \mathbb{Q}| = 5$$

$1, \alpha, \alpha^2, \alpha^3, \alpha^4$ — базис $\mathbb{Q}(L)$ над $\mathbb{Q}$.

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. L — расширение K, $\quad \alpha \in L$

$$\implies \beta \subset L$$

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 $\square$

Примеры.

1. α — алг. над K.
   Тогда $\frac{\alpha^2+3}{\alpha+1}$ — алг. над K
2. $\dfrac{\sqrt[3]{2}+1}{(\sqrt[3]{2})^2+5}$ — алг. число

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

Доказательство.

$$K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset \dots \subset K(\alpha_1, \dots, \alpha_n)$$

Достаточно доказать, что $K(\alpha_1, \dots, \alpha_i, \alpha_{i+1})$ кончено над $K(\alpha_1, \dots, \alpha_i)$:
.... TODO: Дописать доказательство $\square$

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

Доказательство. TODO: Дописать доказательство $\square$

37. Существование простого расширения. Эквивалентные расширения

Теорема 37 (существование простого расширения)**.** K — поле, $\quad P(x) \in K[x]$ — неприводимый.
Тогда существует расширение 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

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

$$S(x) \coloneqq a_0 + a_1 x + \dots, \qquad T(x) \coloneqq b_0 + b_1 x + \dots$$

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

$$s = a_0 + a_1 X + \dots, \qquad t = b_0 + b_1 X + \dots, \qquad u = c_0 + c_1 X + \dots$$

$$S(x) = a_0 + a_1 x + \dots, \qquad T(x) = b_0 + b_1 x + \dots, \qquad U(x) = c_0 + c_1 x + \dots$$

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: $\overline{a_0 + a_1 X + \dots} \mapsto \overline{a_0 + a_1 x + \dots}$
$\overline{X}$ подойдёт в качестве α (т. к. $P(x) \mapsto \overline{P(x)} = 0$). □

Пример. $K = \mathbb{Z}_3$
$p(x) = x^3 + 2x + 1$ — неприводимый над $\mathbb{Z}_3$
α — корень. Существует поле $K(\alpha)$.
Теперь знаем, что $K(\alpha)$ алгебраическое над K, $\quad |K(\alpha) : K| = 3$
Элементы имеют вид $a + b\alpha + c\alpha^2, \quad a, b, c \in \mathbb{Z}_3$
Знаем, что $\alpha^3 + 2\alpha + 1 = 0$
Пример умножения.

$$a = 1 + 2\alpha + \alpha^2, \qquad b = 2 + \alpha + \alpha^2$$

$$ab = (1 + 2\alpha + \alpha^2)(2 + \alpha + \alpha^2) = 2 + (1+1)\alpha + (2+2+1)\alpha^2 + (2+1)\alpha^3 + \alpha^4 \underset{3}{\equiv} 2 + 2\alpha + \alpha^2 + \alpha^4$$

Поделим $x^4 + x^2 + 2x + 2$ на $x^3 + 2x + 1$:

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$ab = (\underbrace{\alpha^3 + \alpha + 2}_{0}) \cdot \alpha + 2 = 2$$

Пример деления.

$$\frac{1}{\alpha^2 + 1}$$

$x^2 + 1$ и $P(x)$ взаимно просты. Значит есть линейное представление НОД:

$$(x + 2)P(x) + (2x^2 + x + 2)(x^2 + 1) = 1$$

Подставим $x = \alpha$:

$$(\alpha + 2) \cdot 0 + (2\alpha + \alpha + 2)(\alpha^2 + 1) = 1 \quad \Longrightarrow \quad \frac{1}{\alpha^2 + 1} = 2\alpha^2 + \alpha + 2$$

Определение 54. 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 38 (эквивалентные простые расширения). α, β — алгебраические над K, их минимальные многочлены совпадают.
Тогда $K(\alpha)$ и $K(\beta)$ эквивалентны K, причём существует изоморфизм $f : K(\alpha) \to K(\beta)$ такой, что

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

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

$$s = u_0 + u_1\alpha + \dots, \qquad t = v_0 + v_1\alpha + \dots$$

$$S(x) = u_0 + u_1 x + \dots, \qquad T(x) = v_0 + v_1 x + \dots$$

Пусть $R(x) = w_0 + w_1 x + \dots + w_{n-1} x^{n-1}$ — 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 $u_0 + u_1 \beta + \dots$

$\square$

Примеры.

1. $\mathbb{Q}, \quad P(x) = x^3 - 2$
Корни $P(x)$:
$$\alpha = \sqrt[3]{2}, \qquad \left(-\frac{1}{2} + \frac{\sqrt{3}}{2} i\right) \sqrt[3]{2}, \qquad \gamma = \left(-\frac{1}{2} - \frac{\sqrt{3}}{2} i\right) \sqrt[3]{2}$$
$$L_1 = K(\alpha), \qquad L_2 = K(\beta)$$
$$a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \quad \mapsto \quad a + b\left(-\frac{1}{2} + \frac{\sqrt{3}}{2} i\right)\sqrt[3]{2} + c\left(\dots\right)^2, \qquad a, b, c \in \mathbb{Q}$$
Это — изоморфизм $L_1 \to L_2$
Аналогично, $K(\beta) \to K(\gamma)$ — сужение комплексного сопряжения.

2. $\mathbb{Q}, \quad P(x) = x^2 - 2$
$$\alpha = \sqrt{2}, \qquad \beta = -\sqrt{2}$$
$$\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$$
По теореме, существует изоморфизм $f : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ такой, что $f\big|_Q = \mathrm{id}, \quad f(\sqrt{2}) = -\sqrt{2}$

38. Поле разложения многочлена: существование, эквивалентность

Определение 55. K — поле, $\qquad P(x) \in K[x]$.
Полем разложениия $P(x)$ называется такое расширение L поля K, что в L многочлен $P(x)$ раскладывается на линейные множители

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

и $L = K(\alpha_1, \dots, \alpha_n)$.

Теорема 39 (существование поля разложения)**.** K — поле, $\qquad P(x) \in K[x]$.
Тогда

1. существует поле разложения;
2. любое поле разложения является конечным расширением K.

Доказательство. Будем считать, что старший коэффициент P равен 1.
Докажем, что существует M, в котором $P(x)$ раскладывается на линейные множители.
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 — линейное подполе L, содержащее K и $\alpha_1, \dots, \alpha_n$.

$\square$

Примеры.

1. $\mathbb{Q}, \quad P(x) = x^2 - 2$
   Поле разложения: $\mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$
   $$|\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2$$
2. $K = \mathbb{Q}, \qquad P(x) = x^3 - 2, \qquad L$ — поле разложения $P(x)$
   $$\alpha = \sqrt[3]{2}, \qquad \beta = \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)\sqrt[3]{2}, \qquad \gamma = \left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right)\sqrt[3]{2}$$
   - $\mathbb{Q}(\alpha) \neq L$ (т. к. $\mathbb{Q}(\alpha) \subset \mathbb{R}, \quad L \not\subset \mathbb{R}$)
   - $Q(\beta),\ \mathbb{Q}(\gamma)$
   $$|\mathbb{Q}(\alpha) : \mathbb{Q}| = \deg(x^3 - 2) = 3, \qquad |\mathbb{Q}(\alpha) : \mathbb{Q}| = |\mathbb{Q}(\beta) : \mathbb{Q}| = |\mathbb{Q}(\gamma) : \mathbb{Q}|$$
   $$\mathbb{Q}(\alpha) \subset L, \quad \mathbb{Q}(\alpha) \neq L \quad \implies |L : \mathbb{Q}| > 3 \implies L \neq \mathbb{Q}(\beta), \quad L \neq \mathbb{Q}(\gamma)$$
   - $L = \mathbb{Q}(\alpha, \beta)$ т. к. $\gamma = -\alpha - \beta$
   $$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\alpha, \beta) = L$$
   $$|\mathbb{Q}(\alpha, \beta) : \mathbb{Q}| = \underbrace{|\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)|}_{2} \cdot \underbrace{|\mathbb{Q}(\alpha) : \mathbb{Q}|}_{3} = 6$$
   β — корень уравнения
   $$\frac{x^3 - 2}{x - \alpha} = \frac{x^3 - 2}{x - \sqrt[3]{2}} = \frac{x^3 - \alpha^3}{x - \alpha} = x^2 + \alpha x + \alpha^2$$

Теорема 40 (эквивалентность полей разложения многочлена). K — поле, $P \in K[x]$, L, M — поля разложения.
Тогда

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

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

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

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

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

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

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

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

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

$R_i(x)$ неприводимы

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

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

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

- Если нет линейных, то воложим α_{s+1} — корень $Q(x)$, β_{s+1} — корень $R_1(x)$

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

□

Замечание. Порядок важен:

$$P(x) = (x^2+1)(x^2+4)$$

Корни: i, $-i$, $2i$, $-2i$
Нет изоморфизма над $\mathbb{Q}$:

$$i \to 2i, \qquad i^2 \to (2i)^2, \qquad -1 \to -4$$

39. Свойства корней из единицы. Существование примитивного корня

Определение 56. 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 $1 \le k < n$

Пример. $K = \mathbb{Z}_5(\alpha)$, $\alpha^2 - 3 = 0$

$$\alpha^8 = 3^4 = 81 = 1 \implies \alpha \text{ — корень 8-й степени из единицы}$$

Свойства.

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

Пример. $K + \mathbb{Z}_5(\alpha), \quad \alpha^2 - 3 = 0$
Проверим, что α — примитивный корень 8-й степени:

$$\alpha^8 = 1 \implies 8 \,\vdots\, \operatorname{ord}\alpha \implies \operatorname{ord}\alpha = \left[\begin{array}{l} 8 \\ 4 \\ 2 \\ 1 \end{array}\right.$$

Если $\operatorname{ord}\alpha = \left[\begin{array}{l} 4 \\ 2 \\ 1 \end{array}\right.$, то $\alpha^4 = 1$

$$\alpha^4 = 3^2 = 9 = 4 \neq 1$$

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 $\varepsilon^s = 1$:

$$C_p^i = \frac{p!}{(p-i)! \cdot i!} \qquad \vdots\, p \text{ при } 1 \leq i \leq p-1 \text{ в } \mathbb{Z}$$

(т. к. $p! \,\vdots\, p, \quad (p-i)! \cdot i! \not\vdots\, p$)

$$\operatorname{char} K = p \implies C_p^i = 0 \text{ при } 1 \leq i \leq p$$

$$(\varepsilon^s - 1)^p = (\varepsilon^s)^p + 0 \cdot (\varepsilon^s)^{p-1} \cdot (-1) + \dots + 0 \cdot \varepsilon^s \cdot (-1)^{p-1} + (-1)^p = \varepsilon^{sp} - 1 = 1 - 1 = 0 \xRightarrow[\text{обл. цел.}]{} \varepsilon^s - 1$$

$\square$

Теорема 41 (существование примитивного корня). K — поле, $\qquad h \in \mathbb{N}$
$x^h - 1$ раскладывается в K на линейные множители, $\qquad h \not\vdots\, \operatorname{char} K$
Тогда

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, $\quad |U| = h$

   Нужно доказать, что $\exists \varepsilon \in U: \quad \operatorname{ord}\varepsilon = h$

   Пусть $h = p_1^{a_1} \cdot \dots \cdot p_k^{a_k}, \quad p_i \in \mathbb{P}$

   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):

$$x_1 : \operatorname{ord} x_1 \stackrel{?}{=} p_1^{a_1}$$

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 $\operatorname{ord} \varepsilon = h$:

Положими $b_i := \frac{h}{p_i}$, т. е. $b_i = p_1^{a_1} \dots p_i^{a_i-1} \dots p_k^{a_k}$

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

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

$x_j^{b_i} = 1$ 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 $(\varepsilon^i = \varepsilon^j \implies \varepsilon^{i-j} = 1)$

□

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$(s, h) = d \neq 1$

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

□

Определение 57. K — поле, $\quad h \in \mathbb{N}, \quad h \not\vdots\, \operatorname{char} K$
$x^h - 1$ раскладывается на линейные множители
$\varepsilon_1, \dots, \varepsilon_{\varphi(h)}$ — все примитивные корни степени h

Многочлен деления круга (круговой многочлен) — это

$$\Phi_h(x) = (x - \varepsilon_1)(x - \varepsilon_2) \dots (x - \varepsilon_{\varphi(h)})$$

Пример. $\mathbb{C}$

$$\Phi_1(x) = x - 1$$

$$\Phi_2(x) = x + 1$$

$$\Phi_3(x) = (x-\varepsilon_1)(x-\varepsilon_2) = \frac{(x-1)(x-\varepsilon_1)(x-\varepsilon_2)}{x-1} = \frac{x^3-1}{x-1} = x^2+x+1$$

$$\forall p \in \mathbb{P} \quad \Phi_p = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \dots + x + 1$$

$$\Phi_4(x) = (x-i)(x+i) = x^2+1$$

$$\Phi_4(x) = \frac{x^4-1}{\underbrace{(x-1)}_{\Phi_1}\underbrace{(x+1)}_{\Phi_2}} = x^2+1$$

Теорема 42 (многочлен деления круга)**.** K — поле, $\quad h \in \mathbb{N}, \quad h \not\vdots \operatorname{char} K$
$x^h - 1$ раскладывается на линейные множители
Тогда

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

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

Доказательство.

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

$$\prod_{d \mid h} \Phi_d(x) \stackrel{?}{=} \prod_{\varepsilon \in U} (x - \varepsilon)$$

   - Пусть $x - \varepsilon$ входит в $\Phi_d(x) \implies \varepsilon^d = 1, \quad \varepsilon^k \neq 1$ при $k < d \quad \implies \varepsilon^h = 1$ (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.

$$\Phi_h(x) = \frac{x^h - 1}{\Phi_{d_1}(x) \dots \Phi_{d_k}(x)}, \qquad d_1, \dots, d_k \text{ — делители } h, \text{ не равные } h$$

   Знаменатель — многочлен с целыми коэффициентами, старший коэффициент равен 1. При делении на такой многочлен получаем целые коэффициенты.

□

41. Строение конечного поля. Единственность

Теорема 43 (строение конечного поля)**.** K — конечное поле
Существует $p \in \mathbb{P}, \quad n \in \mathbb{N}$ 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 $\le |K|$ 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 $x^{p^n} - x = 0$

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

□

Следствие (единственность)**.** Любые два конечных поля с одинаковым числом элементов изоморфны.

Доказательство. $|K| = p^n \implies K$ изоморфно полю разложения $x^{p^n} - x$ над $\mathbb{Z}_p$. □

42. Существование поля с данным количеством элементов

Теорема 44 (сущетсвование)**.** 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 $+, \cdot$:

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

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

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

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

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

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

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

- $x \in K$

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

$\square$