

Алгебра 2 семестр ПИ,

Лекции

Собрано 5 мая 2022 г. в 11:04

Содержание

1. Системы линейных уравнений	1
1.1. Ранг матрицы	1
1.2. Структура решений СЛУ	3
1.3. Неоднородные СЛУ	4
2. Линейные отображения векторных пространств	6
2.1. Матрица линейного отображения	6
2.2. Линейные операторы	8
2.3. Собственные векторы и числа	10
2.4. Жорданова нормальная форма	13
2.5. Теорема Гамильтона-Кэли	13
2.6. Билинейные формы	14
2.6.1. Замена базиса	15
2.7. Квадратичные формы	15
2.7.1. Квадратичная форма над \mathbb{R}	16
2.7.2. Теорема Якоби	17
2.7.3. Ортогональные преобразования	19
3. Элементы теории полей	21
3.1. Факторкольцо	21
3.2. Расширение полей	23

Раздел #1: Системы линейных уравнений

$$(*) \begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = b_2 \\ \dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = b_n \end{cases}$$

$$A = (a_{ij}) - \text{матрица коэффициентов}, X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}.$$

Определение 1. Решение СЛУ $(*)$ называется $\alpha_1, \dots, \alpha_n \in K$: при $x_i = \alpha_i$ все уравнения становятся верными.

Определение 2. СЛУ $(*)$ совместна, если \exists хотя бы одно решение. Иначе - несовместна.

1.1. Ранг матрицы

$A - m \times n$, $A = (A_1, A_2, \dots, A_m)$, A_i - строки.

$A = (A^1, A^2, \dots, A^n)$, A^j - столбцы.

Определение 3. Строчным (столбцовым) рангом матрицы A называется максимальное число ЛНЗ строк (столбцов).

Иначе, количество элементов в базисе $\langle A_1, \dots, A_m \rangle (\langle A^1, \dots, A^n \rangle)$.

Теорема 1. Строчный и столбцовый ранги совпадают.

Обозначение: $\text{rank } A$.

Определение 4. Минором матрицы $A - m \times n$ k -го порядка называется определитель, составленный из элементов матрицы A , стоящих на k выбранных строках и на k выбранных столбцов.

Пример. $\begin{pmatrix} 1 & 4 & 8 & -3 \\ 2 & 5 & 9 & -4 \\ 3 & 6 & -2 & -5 \end{pmatrix}$. Если вы выберем вторую и третью строку, а также первый и последний столбец, то минор второго порядка:

$$\begin{vmatrix} 2 & -4 \\ 3 & -5 \end{vmatrix}$$

Теорема 2. Ранг матрицы A равен наибольшему порядку минора, отличного от нуля.

Теорема 3 (Связь определителя с рангом матрицы). $A - n \times n$. Тогда $\text{rank } A < n \Leftrightarrow \det A = 0$.

Доказательство. \Rightarrow . $\text{rank } A < n \Rightarrow$ строки A_1, \dots, A_n ЛЗ, т.е. $\exists \alpha_1, \dots, \alpha_n \in K : \alpha_1 A_1 + \alpha_2 A_2 + \dots + \alpha_n A_n = 0$ (α_i не все равны нулю). Пусть $\alpha_1 \neq 0 \Rightarrow A_1 = -\frac{\alpha_2}{\alpha_1} A_2 - \dots - \frac{\alpha_n}{\alpha_1} A_n$. Обнулیم первую строку: прибавим к ней A_2 , умноженную на $-\frac{\alpha_2}{\alpha_1}$, A_3 , умноженную на $-\frac{\alpha_3}{\alpha_1}$ и т.д. Поскольку теперь первая строка целиком нулевая, то $\det A = 0$.

\Leftarrow . Индукция $n = 1 \Rightarrow a_{11} = 0$. $n - 1 \rightarrow n$.

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} =$$

Можем считать, что $A^1 \neq 0, a_{11} \neq 0$. Домножим первую строку на $-\frac{a_{21}}{a_{11}}$ и прибавляем ко второй строке. Затем домножаем первую строку на $-\frac{a_{31}}{a_{11}}$ и прибавляем ко третьей строке и т.д.

$$= \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a'_{22} & \cdots & a'_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a'_{n2} & \cdots & a'_{nn} \end{vmatrix} = a_{11} \cdot \begin{vmatrix} a'_{22} & \cdots & a'_{2n} \\ \vdots & \ddots & \vdots \\ a'_{n2} & \cdots & a'_{nn} \end{vmatrix}$$

По предположению A'_2, \dots, A'_n — ЛЗ. $\begin{cases} A'_2 = A_2 - \frac{a_{21}}{a_{11}} \cdot A_1 \\ \dots \\ A'_n = A_n - \frac{a_{n1}}{a_{11}} \cdot A_1 \end{cases}$.

$0 = \alpha_2 A'_2 + \dots + \alpha_n A'_n = (\dots) A_1 + \alpha_2 \cdot A_2 + \dots + \alpha_n A_n \Rightarrow A_1, \dots, A_n$ — ЛЗ $\Rightarrow \text{rank } A < n$. \square

Определение 5. Элементарными преобразованиями над строками (столбцами) называется

1. Перестановка строк (столбцов).
2. Умножение строки (столбца) на $\lambda \neq 0$.
3. Прибавление к одной строке (столбцу) другой строки (столбца), умноженной на $\lambda \neq 0$.

Теорема 4. При элементарных преобразованиях ранг матрицы не меняется.

Доказательство. 1, 2 — очевидно. $(A_1, \dots, A_i, \dots, A_j, \dots, A_n) \rightarrow (A_1, \dots, A_i + \lambda A_j, \dots, A_j, \dots, A_n)$ \square

Определение 6. Матрица называется трапецевидной, если у неё в \forall ненулевой строке число нулей слева различно.

Замечание. rank трапецевидной матрицы равен числу ненулевых строк.

Теорема 5 (О вычислении ранга). Любую матрицу с помощью элементарных преобразований можно привести к трапецевидной.

1.2. Структура решений СЛУ

Определение 7. СЛУ (*) называется однородной, если все свободные члены равны нулю.

Определение 8. Нулевое решение однородной СЛУ называется тривиальным. Любое другое решение – нетривиальным.

Лемма 1. Пусть Y, Z – решения $AX = 0 \Rightarrow \alpha Y + \beta Z$ – тоже решение, $\alpha, \beta \in K$.

Доказательство.

$$AY = 0, AZ = 0 \Rightarrow A(\alpha Y + \beta Z) = \alpha AY + \beta AZ = 0$$

□

Теорема 6 (Структура решений однородной СЛУ). $AX = 0$, $A - m \times n$, n – число неизвестных, $r = \text{rank } A \Rightarrow \exists n - r$ ЛНЗ решений $X_1, \dots, X_{n-r} : \forall$ решение $X = \alpha_1 X_1 + \dots + \alpha_{n-r} X_{n-r}$.

Доказательство. $A = (A^1, \dots, A^n)$, A^1, \dots, A^r – ЛНЗ столбцы \Rightarrow

$$\begin{cases} A_{r+1} = \beta_{r+1 \ 1} A^1 + \dots + \beta_{r+1 \ n} A^n \\ \dots \\ A^n = \beta_{n \ 1} A^1 + \dots + \beta_{n \ r} A^r \end{cases}$$

$$AX = 0 \Leftrightarrow x_1 A^1 + x_2 A^2 + \dots + x_n A^n = 0.$$

$$X_1 = \begin{pmatrix} \beta_{r+1 \ 1} \\ \vdots \\ \beta_{r+1 \ r} \\ -1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, X_2 = \begin{pmatrix} \beta_{r+2 \ 1} \\ \vdots \\ \beta_{r+2 \ r} \\ 0 \\ -1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, X_{n-r} = \begin{pmatrix} \beta_{n \ 1} \\ \vdots \\ \beta_{n \ r} \\ 0 \\ \vdots \\ -1 \end{pmatrix} - \text{решения.}$$

Пусть $Z = \begin{pmatrix} x_1^* \\ \vdots \\ x_r^* \\ \vdots \\ x_n^* \end{pmatrix}$ – решение. Рассмотрим $Y = Z + x_{r+1}^* X_1 + x_{r+2}^* X_2 + \dots + x_n^* X_{n-r}$. $Y = \begin{pmatrix} y_1 \\ \vdots \\ y_r \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ – решение $\{y_1 A_1 + \dots + y_r A_r = 0\}$. Но A_1, \dots, A_r – ЛНЗ $\Rightarrow Y = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \Rightarrow 0 = Z + x_{r+1}^* X_1 + x_{r+2}^* X_2 + \dots + x_n^* X_{n-r}$. \square

Определение 9. $\forall n-r$ ЛНЗ решений однородной системы линейных уравнений называется **фундаментальной системой решений**, решение вида $X = \alpha_1 X_1 + \dots + \alpha_{n-r} X_{n-r}$ – **общее решение**.

1.3. Неоднородные СЛУ

$$AX = B, A - m \times n, X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, B = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}.$$

$\bar{A} = (A \mid B)$ – расширенная матрица $m \times (n+1)$.

Теорема 7 (Кронекера-Капелли). $(*)$ – совместна $\Leftrightarrow \text{rank } A = \text{rank } \bar{A}$.

Доказательство. \Rightarrow . $AX = B$ – совместна $\Rightarrow \exists$ решение $x_1 A^1 + \dots + x_n A^n = B \Rightarrow B$ – линейная комбинация $A^1, \dots, A^n \Rightarrow \text{rank } A = \text{rank } \bar{A}$.

\Leftarrow . $\text{rank } A = \text{rank } \bar{A} = r \Rightarrow \exists A^1, \dots, A^r$ – ЛНЗ $\Rightarrow A^1, \dots, A^r, B$ – ЛЗ $\Rightarrow B = \alpha_1 A^1 + \dots + \alpha_r A^r$, не все $\alpha_i = 0 \Rightarrow (\alpha_1, \dots, \alpha_r, 0, \dots, 0)$ – решение системы. \square

Теорема 8 (О структуре решений неоднородной СЛУ). $AX = B, \text{rank } A = r, n$ – число неизвестных, система совместна. X_* – какое-то решение СЛУ, X_1, \dots, X_{n-r} – фундаментальные решения $AX = 0$. Тогда любое решение $(*)$ имеет вид $X = \alpha_1 X_1 + \dots + \alpha_{n-r} X_{n-r} + X_*, \alpha_1, \dots, \alpha_{n-r} \in K$.

Доказательство. $AX_* = B \Rightarrow AX = AX_* \Rightarrow A(X - X_*) = 0 \Rightarrow X - X_* = \alpha_1 X_1 + \dots + \alpha_{n-r} X_{n-r}$. \square

Пример (Решение СЛУ методом Гаусса).

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = 4 \\ x_1 + x_2 + 2x_3 + 2x_4 = 2 \\ 2x_1 + 2x_2 + 3x_3 + 3x_4 = 6 \end{cases} \sim \left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 4 \\ 1 & 1 & 2 & 2 & 2 \\ 2 & 2 & 3 & 3 & 6 \end{array} \right) \sim$$

$$\sim \left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 4 \\ 0 & 0 & 1 & 1 & -2 \\ 0 & 0 & 1 & 1 & -2 \end{array} \right) \sim \left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 4 \\ 0 & 1 & 1 & 1 & -2 \\ 0 & 0 & 1 & 1 & -2 \end{array} \right) \sim \left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 4 \\ 0 & 1 & 0 & 0 & \alpha \\ 0 & 0 & 1 & 1 & -2 \\ 0 & 0 & 0 & 1 & \beta \end{array} \right) \sim \left(\begin{array}{cccc|c} 1 & 1 & 1 & 0 & 4 - \beta \\ 0 & 1 & 0 & 0 & \alpha \\ 0 & 0 & 1 & 0 & -2 - \beta \\ 0 & 0 & 0 & 1 & \beta \end{array} \right) \sim$$

$$\sim \left(\begin{array}{cccc|c} 1 & 1 & 0 & 0 & 6 \\ 0 & 1 & 0 & 0 & \alpha \\ 0 & 0 & 1 & 0 & -2 - \beta \\ 0 & 0 & 0 & 1 & \beta \end{array} \right) \sim \left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 6 - \alpha \\ 0 & 1 & 0 & 0 & \alpha \\ 0 & 0 & 1 & 0 & -2 - \beta \\ 0 & 0 & 0 & 1 & \beta \end{array} \right) \Rightarrow \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 6 \\ 0 \\ -2 \\ 0 \end{pmatrix} + \alpha \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 0 \\ -1 \\ 1 \end{pmatrix}$$

Раздел #2: Линейные отображения векторных пространств

Определение 10. V, W – векторные пространства над K . Отображение $f : V \rightarrow W$ называется линейным, если:

1. $f(x + y) = f(x) + f(y) \quad \forall x, y \in V$
2. $f(\alpha x) = \alpha f(x) \quad \forall x \in V, \alpha \in K$

Замечание. $1, 2 \sim f(\alpha x + \beta y) = \alpha f(x) + \beta f(y) \quad \forall x, y \in V, \alpha, \beta \in K$.

Определение 11. $\text{Hom}(V, W) = \{f : V \rightarrow W \text{ – линейные}\}$

Лемма 2. $\text{Hom}(V, W)$ – векторное пространство над K .

Доказательство. $f, g \in \text{Hom}(V, W), (f + g)(x) = f(x) + g(x), (\alpha f)(x) = \alpha f(x) \Rightarrow f + g, \alpha f \in \text{Hom}(V, W)$. \square

Определение 12. $f \in \text{Hom}(V, W), \ker f = \{x \in V : f(x) = 0\}$ – ядро отображения f , $\text{Im } f = \{f(x), x \in V\}$ – образ f .

Лемма 3. $\ker f \subset V, \text{Im } f \subset W$ – подпространства.

Доказательство. $x, y \in \ker f, f(x + y) = f(x) + f(y) = 0 + 0 = 0 \Rightarrow x + y \in \ker f$. Аналогично, $f(\alpha x) = \alpha f(x) = 0 \Rightarrow \alpha x \in \ker f \quad \forall \alpha \in K \Rightarrow \ker f$ – подпространство. \square

Упражнение. $\text{Im } f$ – подпространство.

Теорема 9. $f \in \text{Hom}(V, W)$.

1. f – инъективно $\Leftrightarrow \ker f = \{0\}$.
2. f – сюръективно $\Leftrightarrow \text{Im } f = W$.

Доказательство. \Leftarrow . $x_1 \neq x_2$, если $f(x_1) = f(x_2) \Rightarrow f(x_1 - x_2) = 0 \Rightarrow x_1 - x_2 \in \ker f \Rightarrow x_1 - x_2 = 0$!?
 \Rightarrow . Пусть $x \in \ker f, x \neq 0 \Rightarrow f(x) = f(0) = 0$!?. \square

2.1. Матрица линейного отображения

e_1, \dots, e_n – базис V, e'_1, \dots, e'_m – базис $W, f \in \text{Hom}(V, W)$

$x \in V, x = x_1 e_1 + \dots + x_n e_n, x_i \in K, f(x) = x_1 f(e_1) + \dots + x_n f(e_n) \Leftrightarrow$ задать f значит задать

$f(e_i), i = 1, \dots, n$.

$$\begin{cases} f(e_1) = a_{11}e'_1 + a_{21}e'_2 + \dots + a_{m1}e'_m \\ \dots \\ f(e_n) = a_{1n}e'_1 + a_{2n}e'_2 + \dots + a_{mn}e'_m \end{cases}$$

Определение 13. Матрицей $f \in \text{Hom}(V, W)$ в базисе e_1, \dots, e_n и e'_1, \dots, e'_m называется

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} = \begin{pmatrix} f(e_1) & f(e_2) & \dots & f(e_n) \end{pmatrix}$$

Теорема 10. 1. $\text{Hom}(V, W)$ взаимно-однозначно соответствует $M(m, n, K)$.

2. e_1, \dots, e_n – базис V , e'_1, \dots, e'_m – базис W , $x \in V \rightarrow X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, $f(x) \in W \rightarrow Y = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}$, $f \rightarrow A$
 $\Rightarrow AX = Y$.

Доказательство. 1. $f \rightarrow A$ отображение однозначно определяется $f(e_i) \Rightarrow A$ определена однозначно. С другой стороны, взяв произвольную матрицу B , можем построить по ней отображение g .

2. $f \rightarrow A = (a_{ij}), 1 \leq i \leq n, 1 \leq j \leq m$.

$$\begin{aligned} f(x) &= f(x_1e_1 + \dots x_ne_n) = x_1f(e_1) + \dots + x_nf(e_n) = \\ &= x_1(a_{11}e'_1 + a_{21}e'_2 + \dots + a_{m1}e'_m) + \dots + x_n(a_{1n}e'_1 + a_{2n}e'_2 + \dots + a_{mn}e'_m) = \\ &= \underbrace{(a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n)}_{y_1}e'_1 + \dots + \underbrace{(a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n)}_{y_m}e'_m \Rightarrow Y = AX \end{aligned}$$

□

Следствие. 1. $\dim \text{Hom}(V, W) = \dim V \cdot \dim W$

2. $\alpha, \beta \in K, f, g \in \text{Hom}(V, W), f \rightarrow A, g \rightarrow B$ в фиксированных базисах $\Rightarrow \alpha f + \beta g \rightarrow \alpha A + \beta B$.
 3. $f : V \rightarrow W, g : W \rightarrow U \Rightarrow g \circ f : V \rightarrow U, g \circ f(x) = g(f(x))$. Фиксируем базисы, $f \rightarrow A, g \rightarrow B \Rightarrow g \circ f \rightarrow BA$

Доказательство. 1. Соответствие матриц.

2. $(\alpha f + \beta g)(e_i) = \alpha f(e_i) + \beta g(e_i) \in \alpha A + \beta B$.

3. $V \rightarrow n, W \rightarrow l, U \rightarrow m, A \rightarrow l \times n, B \rightarrow m \times l$

$$g \circ f(e_i) = g(\sum_{k=1}^n a_{ki}e_k) = \sum_{k=1}^n a_{ki}g(e_k) = \sum_{k=1}^n a_{ki} \sum_{j=1}^l b_{jk}e'_j = \sum_{j=1}^m \sum_{k=1}^l b_{jk}a_{ki}e'_j, \text{ где } b_{jk}a_{ki} \rightarrow BA.$$

□

Теорема 11. $f : V \rightarrow W$, $\dim V, \dim W < \infty$

$$\Rightarrow \dim \ker f + \dim \operatorname{Im} f = \dim V$$

Доказательство. $\ker f \subset V$, e_1, \dots, e_k – базис $\ker f$. Дополним до базиса V : $e_1, \dots, e_k, e_{k+1}, \dots, e_n$ – базис V .

$$x \in V, f(x) \in \operatorname{Im} f \quad f(x) = x_{k+1}f(e_{k+1}) + \dots + x_nf(e_n) \in \operatorname{Im} f$$

$f(e_1) = \dots = f(e_k) = 0 \Rightarrow \operatorname{Im} f = \langle f(e_{k+1}), \dots, f(e_n) \rangle$. Надо доказать, что $f(e_{k+1}), \dots, f(e_n)$ – ЛНЗ.

Предположим обратное. $\alpha_{k+1}f(e_{k+1}) + \dots + \alpha_nf(e_n) = 0 \Rightarrow f(\alpha_{k+1}e_{k+1} + \dots + \alpha_ne_n) = 0 \Rightarrow \alpha_{k+1}e_{k+1} + \dots + \alpha_ne_n \in \ker f = \langle e_1, \dots, e_k \rangle$ – невозможно.

$$\dim \ker f = k, \dim V = n, \dim \operatorname{Im} f = n - k.$$

□

2.2. Линейные операторы

Определение 14. Линейным оператором называется линейное отображение $a : V \rightarrow V$, т.е. $a \in \operatorname{Hom}(V, V)$.

Обозначается $\operatorname{End} V = \operatorname{Hom}(V, V)$.

Определение 15. Тожественным отображением называется отображение

Определение 16.

Пример. 1. Нулевой оператор. $0 \in \operatorname{End} V$. $0(x) = 0$. $0 \rightarrow \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix} = 0$

2. Оператор подобия. $\forall x \in V \quad ax = \lambda x \rightarrow \begin{pmatrix} \lambda & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \lambda \end{pmatrix}$

3. Оператор поворота в \mathbb{R}^2 . $z \rightarrow ze^{i\varphi}$ – поворот на φ . Зафиксируем базис $-1, i \Rightarrow a(1) = \cos \varphi + i \sin \varphi$, $a(i) = i(\cos \varphi + i \sin \varphi) = -\sin \varphi + i \cos \varphi \rightarrow \begin{pmatrix} \cos \varphi & -\sin \varphi \\ \sin \varphi & \cos \varphi \end{pmatrix}$

4. Оператор дифференцирования. $V = \mathbb{R}[x]$. $\frac{d}{dx}f \rightarrow f'$, зафиксируем базис $-1, x, x^2, x^3$.

$$\frac{d}{dx}(1) = 0, \frac{d}{dx}(x) = 1, \frac{d}{dx}(x^2) = 2x, \frac{d}{dx}(x^3) = 3x^2. \text{ Тогда матрица имеет вид: } \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Возьмём другой базис $-1, x+1, x^2+x+1, x^3+x^2+x+1$.

Посчитаем значения: $\frac{d}{dx}(1) = 0$, $\frac{d}{dx}(x+1) = 1$, $\frac{d}{dx}(x^2+x+1) = 2x+1$, $\frac{d}{dx}(x^3+x^2+x+1) = 3x^2+2x+1$.

Матрица имеет вид:
$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Определение 17. $(e_i), (e'_i)$ – базисы V , $\dim V = n$. Разложим
$$\begin{cases} e'_1 = c_{11}e_1 + c_{21}e_2 + \dots + c_{n1}e_n \\ \dots \\ e'_n = c_{1n}e_1 + c_{2n}e_2 + \dots + c_{nn}e_n \end{cases}.$$
 Тогда матрица вида $C = \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \vdots & \ddots & \vdots & \vdots \\ c_{n1} & c_{n2} & \dots & c_{nn} \end{pmatrix}$ называется матрицей перехода от базиса (e_i) к (e'_i) .

Теорема 12 (Преобразование координат вектора при переходе к другому базису). V – вектор-

ное пространство над полем K , $(e_i), (e'_i)$ – базисы V , $x \in V$, $x \rightarrow X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ – координаты

вектора в базисе (e_i) . $x \rightarrow X' = \begin{pmatrix} x'_1 \\ x'_2 \\ \vdots \\ x'_n \end{pmatrix}$ – координаты вектора в базисе (e'_i) , C – матрица перехода от (e_i) к (e'_i) .

1. $X = CX'$
2. C – обратима ($\det C \neq 0$)

Доказательство. 1. $x = x'_1e'_1 + \dots + x'_ne'_n = x'_1(c_{11}e_1 + c_{21}e_2 + \dots + c_{n1}e_n) + \dots + x'_n(c_{1n}e_1 + c_{2n}e_2 + \dots + c_{nn}e_n) = \underbrace{(c_{11}x'_1 + c_{12}x'_2 + \dots + c_{1n}x'_n)}_{x_1}e_1 + \dots + \underbrace{(c_{n1}x'_1 + c_{n2}x'_2 + \dots + c_{nn}x'_n)}_{x_n}e_n$

$$\Rightarrow \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = C \begin{pmatrix} x'_1 \\ x'_2 \\ \vdots \\ x'_n \end{pmatrix}$$

2. $\forall X \ X = CX'$ по доказанному, тогда $X = CX' = CDX \Rightarrow CD = E \Rightarrow \det C \neq 0$. □

Теорема 13 (Изменение матрицы линейного оператора при переходе к другому базису). V – векторное пространство, $\dim V = n$, $a \in \text{End } V$, фиксируем базисы $(e_i), (e'_i)$, A – матрица оператора в базисе (e_i) , A' – в базисе (e'_i) , C – матрица перехода от (e_i) к (e'_i) .

$$\Rightarrow A' = C^{-1}AC$$

Лемма 4. $U \subset V, a \in \text{End } V$

U – a -инвариантно $\Leftrightarrow \exists$ базис $V: A = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix}, B = \dim U \times \dim U$

Доказательство. U – a -инвариантно. Выберем базис $U: e_1, \dots, e_k$ и дополним его до базиса

V матрицы a $ae_i = b_{1i}e_1 + \dots + b_{ki}e_k \Leftrightarrow \begin{pmatrix} b_{1i} & \cdot \\ b_{ki} & \cdot \\ 0 & \cdot \\ 0 & \cdot \end{pmatrix} \quad \square$

Лемма 5. $U, W \subset V, a \in \text{End } V$

$V = U \oplus W, U, W$ – a -инвариантны $\Leftrightarrow \exists$ базис $A = \begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix}$
 $B = \dim U \times \dim U, C = \dim W \times \dim W$

Доказательство. $V = U \oplus W$, выберем $U: e_1, \dots, e_k, W: e_{k+1}, \dots, e_n$

$a(e_i) \in U, i = 1, \dots, k, a(e_j) \in W, j = k + 1, \dots, n \Leftrightarrow A = \begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix} \quad \square$

Пример. 1. $V = M(2, \mathbb{R}) \quad a: X \rightarrow X^T, X \in M(2, \mathbb{R})$

$$E_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad E_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad E_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad E_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$a(E_{11}) = E_{11}, \quad a(E_{12}) = E_{21}, \quad a(E_{21}) = E_{12}, \quad a(E_{22}) = E_{22}$$

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \langle E_{11} \rangle \oplus \langle E_{12}, E_{21} \rangle \oplus \langle E_{22} \rangle = V \text{ инвариантны}$$

2. $V = K[x]_3 \quad a: \frac{d}{dx}(f) \rightarrow f' \quad 1, x, x^2, x^3$

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \frac{d}{dx}: \langle 1, x, x^2 \rangle \rightarrow \langle 1, x \rangle \subset \langle 1, x, x^2 \rangle$$

2.3. Собственные векторы и числа

Определение 18. Собственным вектором оператора a называется \forall ненулевой вектор одномерного инвариантного подпространства.

Определение 19. x – собственный вектор, $ax = \lambda x$, тогда λ = собственное число, ассоциированное вектору x

$$a \rightarrow A, x \rightarrow X \quad AX = \lambda X \Rightarrow (A - \lambda E)X = 0$$

Определение 20. Характеристическим многочленом оператора a (матрицы A) называется $\chi_a(t) = \det(A - tE)$

Теорема 14 (О собственных числах). Все собственные числа оператора a и только они являются корнями характеристического многочлена.

Доказательство. $AX = \lambda X \Leftrightarrow (A - \lambda E)X = 0$ – имеет ненулевое решение $\Leftrightarrow \det(A - \lambda E) = 0 \Leftrightarrow$ все собственные числа корни $\chi_a(t)$ \square

Лемма 6 (Независимость собственных чисел от выбора базиса). Характеристические многочлены оператора a в разных базисах совпадают.

Доказательство. $a(e_i) \rightarrow A \quad (e'_i) \rightarrow A' \quad C$ – матрица перехода от (e_i) к (e'_i)
 $A' = C^{-1}AC \quad \chi_a(t) = \det(A' - tE) = \det(C^{-1}AC) = \det(C^{-1}AC - t \cdot C^{-1}C) = \det(C^{-1}(A - tE)C) = \det C^{-1} \cdot \det(A - tE) \cdot \det C = \det(A - tE) = \chi_a(t)$ \square

Теорема 15 (Линейная независимость собственных векторов). Собственные векторы, соответствующие различным собственным числам, линейно независимы.

Доказательство. $n = 1$ – очевидно. Пусть доказали при $n - 1$. Индукционный переход: $n - 1 \rightarrow n : V_1, V_2, \dots, V_n$ – собственные векторы
 $aV_i = \lambda_i V_i, \quad \lambda_1, \dots, \lambda_n$ – различны
 Пусть V_1, V_2, \dots, V_n – линейно зависимы. Тогда $\alpha_1 V_1 + \alpha_2 V_2 + \dots + \alpha_n V_n = 0, \alpha_i \in K \Rightarrow$ под действием a : $\alpha_1 \lambda_1 V_1 + \alpha_2 \lambda_2 V_2 + \dots + \alpha_n \lambda_n V_n = 0$
 Будем считать, что $\lambda_1 \neq 0 \Rightarrow \alpha_1 \lambda_1 V_1 + \alpha_2 \lambda_2 V_2 + \dots + \alpha_n \lambda_n V_n - \lambda_1(\alpha_1 V_1 + \dots + \alpha_n V_n) = \alpha_2(\lambda_2 - \lambda_1)V_2 + \dots + \alpha_n(\lambda_n - \lambda_1)V_n = 0 \Rightarrow$ по предположению индукции $\alpha_2 = \dots = \alpha_n = 0$ \square

Определение 21. Оператор a называется диагонализируемым, если существует базис та-

кой, что $A = \begin{pmatrix} \lambda_1 & 0 & 0 & 0 \\ 0 & \lambda_2 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & \lambda_n \end{pmatrix}$

Теорема 16 (Критерий диагонализируемости). Если $\chi_a(t)$ имеет n различных корней ($n = \dim V$) над рассматриваемым полем, то оператор a – диагонализируем.

Доказательство. В качестве базиса берём собственные векторы. \square

Пример. Оператор поворота $A = \begin{pmatrix} \cos \varphi & -\sin \varphi \\ \sin \varphi & \cos \varphi \end{pmatrix}$ – недиагонализируем над \mathbb{R}

Лемма 7. Над полем \mathbb{C} любой оператор имеет одномерное инвариантное подпространство.

Определение 22. Кратность λ как кратность корня $\chi_a(t) = 0$ называется алгебраической кратностью собственного числа.

Определение 23. λ – собственное число, $V^\lambda = \{x \in V : ax = \lambda x\}$
 $\dim V^\lambda$ – геометрическая кратность собственного числа λ

Пример. $A = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ $\chi_a(t) = \begin{vmatrix} \lambda - t & 0 \\ 0 & \lambda - t \end{vmatrix} = (A - tE) = (\lambda - t)^2 \Rightarrow \lambda$ собственное число алгебраической кратности 2.

$(A - \lambda E)X = 0$
 $\left(\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} - \lambda \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) \begin{pmatrix} X_1 \\ X_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$
 $\dim V^\lambda = 2$ – геометрическая кратность

Пример. $A = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$
 $\chi_a(t) = \begin{vmatrix} \lambda - t & 1 \\ 0 & \lambda - t \end{vmatrix} = (\lambda - t)^2 \Rightarrow$ алгебраическая кратность $\lambda = 2$
 $\left(\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} - \lambda \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) \begin{pmatrix} X_1 \\ X_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$
 $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad V^\lambda = \left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\rangle$
 $\dim V^\lambda = 1$ – геометрическая кратность

Лемма 8. Геометрическая кратность собственного числа $\lambda \leq$ алгебраической кратности

Доказательство. V^λ – инвариантно относительно a , $V^\lambda = \{x : ax = \lambda x\}$

По лемме: $a \rightarrow \begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$ $B - m \times m, \dim V^\lambda = m$

$a|_{V^\lambda} = \chi_a|_{V^\lambda} = (t - \lambda)^m$

$\chi_a = \det \left(\begin{pmatrix} B & C \\ 0 & d \end{pmatrix} - tE \right) = (t - \lambda)^m p(t) \Rightarrow$ алгебраическая кратность $\lambda \geq m$ □

Теорема 17 (Критерий диагонализуемости). $a \in \text{End } V$ – диагонализуема \Leftrightarrow 1. Все собственные числа $\in K$ 2. \forall собственных чисел λ алгебраическая кратность = геометрическая кратность

2.4. Жорданова нормальная форма

Определение 24. Жордановой клеткой порядка m соответствующей собственному числу λ называется

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

Пример. 1. $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$

$$2. \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{pmatrix}$$

Определение 25. ЖНФ оператора $a \in \text{End } V$ называется

$$\begin{pmatrix} J_{k_1}(\lambda_1) & & & \\ & J_{k_2}(\lambda_2) & & \\ & & \ddots & \\ & & & J_{k_n}(\lambda_n) \end{pmatrix}$$

Определение 26. Базис, в котором оператор a имеет ЖНФ называется жордановым

Теорема 18 (ЖНФ). 1. Над алгебраическим замкнутым полем $\forall a \in \text{End } V$ имеет ЖНФ
2. ЖНФ определена с точностью до перестановки клеток

Теорема 19. $a \in \text{End } V$ имеет ЖНФ над произвольным полем \Leftrightarrow характеристический многочлен раскладывается на линейные множители

2.5. Теорема Гамильтона-Кэли

Определение 27. $f(x) = a_n x^n + \dots + a_1 x + a_0 \in K[x]$
 $A - m \times m$

$f(A) = a_n A^n + \dots + a_i A + a_0 E$, E – $m \times m$ – матрица

Определение 28. $a \in \text{End } V$

$f(a) = a_n \cdot a^n + \dots + a_1 \cdot a + a_0 \cdot \text{id}$ – многочлен от оператора

Теорема 20 (Гамильтона-Кэли). $\chi_a(A) = 0$, $a \in \text{End } V$, $a \rightarrow A \in M(m, K)$

Доказательство. $\chi_a(t) = \det(tE - A)$

$B = tE - A$, $\tilde{B} = (B_{ij})^T$ – взаимная матрица

$$\tilde{B} = \begin{pmatrix} c_{11}^{m-1}t^{m-1} + \dots + c_{11}^0 & \dots \\ c_{12}^{m-1}t^{m-1} + \dots + c_{12}^0 & \dots \end{pmatrix} = t^{m-1}B_{m-1} + t^{m-2}B_{m-2} + \dots + B_0$$

$$\tilde{B} \cdot B = \det(tE - A) \cdot E$$

$$(t^{m-1}B_{m-1} + \dots + B_0) \cdot (tE - A) = (a_m t^m + \dots + a_0) \cdot E$$

Приравняем коэффициенты, домножим: $t^m : B_m - 1 = a_m E \quad | \cdot A^m$

$$t^{m-1} : B_{m-1} - B_{m-1}A = a_{m-1}E \quad | \cdot A^{m-1}$$

...

$$t : B_0 - B_1A = a_1E \quad | \cdot A$$

$$1 : -B_0A = a_0E \quad | \cdot E$$

$$\text{Вычтем строки: } \Rightarrow 0 = \chi_a(A)$$

□

2.6. Билинейные формы

Определение 29. $f : V \times V \rightarrow K$ линейное по каждому аргументу называется билинейным отображением, то есть выполняется

$$1. \quad f(\alpha x + \beta y, z) = \alpha f(x, z) + \beta f(y, z)$$

$$2. \quad f(x, \alpha y + \beta z) = \alpha f(x, y) + \beta f(x, z)$$

$(e_i)_{i=1}^n$ – базис V , $x = \sum_{i=1}^n x_i e_i$, $y = \sum_{j=1}^n y_j e_j$

$$f(x, y) = f(\sum_i x_i e_i, \sum_j y_j e_j) = \sum_{i,j=1}^n x_i y_j f(e_i, e_j)$$

Определение 30. $B = (b_{ij})$, $b_{ij} = f(e_i, e_j)$, $1 \leq i, j \leq n$

$$B \text{ – матрица билинейной формы } f \quad X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \Rightarrow f(x, y) = X^T B Y$$

Пример. 1. Скалярное произведение $(x, y) = x_1 y_1 + \dots + x_n y_n =$

$$(x_1, \dots, x_n) \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

$$2. \ f, g \in C[a, b], (f, g) = \int_a^b f(x)g(x)dx$$

Определение 31. Билинейные формы f

1. Симметрические: $f(x, y) = f(y, x) \forall x, y \in V$ $B = B^T$ (симметрическая матрица)
2. Кососимметрические: $f(x, y) = -f(y, x) \forall x, y \in V$ $-B = B^T$ (кососимметрическая матрица)

2.6.1. Замена базиса

Теорема 21 (Преобразование матрицы билинейной формы при изменении базиса). $f : V \times V \rightarrow K$ в базисе $(e_i) : B$, в базисе $(e'_i) : B'$
Тогда $B' = C^T B C$

Доказательство. $x \rightarrow X$ в базисе (e_i) , X' в базисе (e'_i) $X = C X'$,

$y \rightarrow Y$ в (e_i) , Y' в (e'_i) $Y = C Y'$

$$f(x, y) = X^T B Y = (C X')^T B (C Y') = X'^T C^T B C Y' = X'^T B' Y' \Rightarrow B' = C^T B C$$

□

2.7. Квадратичные формы

Определение 32. Квадратичной формой $Q : V \rightarrow K$, ассоциированной с некоторой симметрической билинейной формой $f : V \times V \rightarrow K$, называется $q(x) = f(x, x)$

Матрица квадратичной формы A ($A = A^T$) $q(x) = X^T A X$, $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

$$q(x) = (x_1, \dots, x_n) \begin{pmatrix} a_{11} & & \\ & \ddots & \\ & & a_{nn} \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \sum_{i,h=1}^n a_{ij} x_i y_j - \text{однородный многочлен 2 степени от } n \text{ переменных}$$

$$a_{ij} = a_{ji} \quad a_{ij} x_i x_j + a_{ji} x_i x_j = 2a_{ij} x_i x_j$$

$$q(x) = \sum_{i=1}^n a_{ii} x_i^2 + 2 \sum_{1 \leq u < j \leq n} a_{ij} x_i x_j$$

Определение 33. Каноническим видом квадратичной формы называется $\sum_{i=1}^n \lambda_i x_i^2$

Определение 34. Базис, в котором квадратичная форма имеет канонический вид, называется каноническим.

Замечание. Замена переменной \leftrightarrow переход к другому базису

Теорема 22 (Преобразование Лагранжа). V – векторное пространство над полем K , $\text{char} K \neq 2 \Rightarrow \forall q: V \rightarrow K$ может быть приведена к каноническому виду (\exists базис: q имеет канонический вид)

Доказательство. $q(x) = \sum_{i=1}^n a_{ii}x_i^2 + 2 \sum_{i < j}^{a_{ij}} x_i x_j$
 $q = 0$ – доказывать нечего, будем считать $q \neq 0$.

1. Пусть $a_{11} = 0, \exists i > 1 : a_{ii} \neq 0 \Rightarrow$ сделаем замену $y_i = x_1, x_i = y_1 \Rightarrow a_{11}y_1^2 + \dots$, где $a_{11} \neq 0$

2. $a_{ii} = 0 \forall i = 1, \dots, n \Rightarrow \exists a_{ij} \neq 0, i < j \Rightarrow x_i = y_i + y_j, x_j = y_i - y_j$
 $a_{ij}x_i x_j \rightarrow a_{ij}(y_i + y_j)(y_i - y_j) = a_{ij} \cdot y_i^2 - a_{ij}y_j^2 \Rightarrow$ по п.1 можно считать, что $a_{11} \neq 0$

3. Индукция

База: $n = 1 \quad q(x) = a_{11}x_1^2$

Индукционный переход: $n - 1 \rightarrow n, a_{11} \neq 0$ в силу пункта один

$$\begin{aligned} q(x) &= a_{11} \left(x_1^2 + \frac{2a_{12}}{a_{11}}x_1x_2 + \frac{2a_{13}}{a_{11}}x_1x_3 + \dots + \frac{2a_{1n}}{a_{11}}x_1x_n \right) + \varphi(x_2, \dots, x_n) = \\ &a_{11} \left(x_1^2 + \frac{2a_{12}}{a_{11}}x_1x_2 + \dots + \frac{2a_{1n}}{a_{11}}x_1x_n \right) + a_{11} \left(\left(\frac{a_{12}}{a_{11}}x_2 \right)^2 + \dots + \dots \right) - (\dots) + \varphi(x_2, \dots, x_n) = \\ &a_{11} \left(x_1 + \frac{a_{12}}{a_{11}}x_2 + \dots + \frac{a_{1n}}{a_{11}}x_n \right)^2 - \psi(x_2, \dots, x_n) = a_{11}y_1^2 + b_{22}z_1^2 + \dots + b_{nn}z_n^2 \end{aligned}$$

□

2.7.1. Квадратичная форма над \mathbb{R}

$$\lambda_1 x_1^2 + \dots + \lambda_n x_n^2$$

Если находимся над полем \mathbb{C} , тогда $y_i = \sqrt{\lambda_i}x_i \Rightarrow y_1^2 + \dots + y_r^2, r$ – ранг формы, $r \leq n$

Над \mathbb{R} ситуация иная. $\lambda_i > 0 \quad y_i = \sqrt{\lambda_i}x_i, \quad \lambda_j < 0 \quad y_i = \sqrt{-\lambda_j}x_j \Rightarrow$

$$y_1^2 + \dots + y_s^2 - y_{s+1}^2 - \dots - y_r^2$$

Определение 35. Говорят, что квадратичная форма приведена к нормальному виду, если она представляет собой сумму чистых квадратов $(y_1^2 + \dots + y_s^2 - y_{s+1}^2 - \dots - y_r^2)$.

Определение 36. Ранг квадратичной формы равен рангу соответствующей матрицы.
 $\text{rank } q = \text{rank } A$

Теорема 23 (Закон инерции квадратичных форм). $q: V \rightarrow \mathbb{R}$ – квадратичная форма.

$$\dim V = n, \text{rank } q = r$$

Параметры s и $r - s$ при приведении квадратичной формы к нормальному виду не зависят от базиса.

Доказательство. A – матрица квадратичной формы в базисе $(e_i) \Rightarrow C^T A C$ – матрица квадратичной формы в базисе (e'_i) , где C – матрица перехода от e_i к (e'_i) , $\det C \neq 0$ Несложно показать, что количество линейно независимых строк одинаково у A и $C^T A C$. $\text{rank } A =$

$\text{rank } C^T A C = r$ (было доказано)

Предположим, что в базисе (e_i) квадратичная форма имеет следующий вид: $q = x_1^2 + \dots + x_s^2 - x_{s+1}^2 - \dots - x_r^2$

А в базисе $(e'_i) : q = x_q^2 + \dots + x_t^2 - x_{t+1}^2 - \dots - x_r^2$

Предположим, что $t < s$ Рассмотрим два подпространства пространства $V : U_1 = \langle e_1, \dots, e_s \rangle$
 $U_2 = \langle e'_{t+1}, \dots, e'_n \rangle$

Рассмотрим размерность подпространства $U_1 + U_2 :$

$$\dim(U_1 + U_2) \leq n$$

С другой стороны $\dim(U_1 + U_2) = \dim U_1 + \dim U_2 - \dim(U_1 \cap U_2) = s + n - t - \dim(U_1 \cap U_2) \Rightarrow$
 $\dim(U_1 \cap U_2) \geq s + n - t - n = s - t > 0 \Rightarrow x \in U_1 \cap U_2, \quad q(x) > 0, x \in U_1; \quad q(x) < 0, x \in U_2 \Rightarrow$
 противоречие \square

Определение 37. Предположим, что квадратичная форма приведена. Тогда числа s и $r - s$ называются индексами инерции или положительным и отрицательным индексами инерции. А пары чисел $(s, r - s)$ – сигнатура квадратичной формы.

Замечание (Мотивация изучения квадратичных форм). Квадратичные формы нужны, чтобы исследовать экстремумы функций. $f(x) - f(x_0) = \sum f'_{x_i} \Delta x_i + \sum f''_{x_i x_j} \Delta x_i \Delta x_j + \dots$

Определение 38. Всё рассматриваем над \mathbb{R}

$q : V \rightarrow \mathbb{R}$ называется

1. Положительно определенной, если $q(x) > 0 \quad \forall x \neq 0, x \in V$
2. Отрицательно определенной, если $q(x) < 0 \quad \forall x \neq 0$
3. Положительно полуопределенной, если $q(x) \geq 0 \quad \forall x$
4. Отрицательно полуопределенной, если $q(x) \leq 0 \quad \forall x$
5. Неопределенной, если $q(x) \cdot q(y) < 0 \quad \exists x, y \in V$

Пример. $n = 2$

1. $x^2 + y^2$
2. $-x^2 - y^2$
3. $x^2 - 2xy + y^2$
4. $-$
5. $x^2 - y^2$

2.7.2. Теорема Якоби

Определение 39. $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$

$\Delta_1 = a_{11}, \Delta_2 = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}, \dots, \Delta_n = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}$ – Главные миноры

$\Delta_0 = 1$

Определение 40. $\text{char} K \neq 2$

$f(x, y) = \frac{1}{2}(q(x+y) - q(x) - q(y))$ называется билинейной формой, полученной поляризацией квадратичной формы q

Упражнение. Показать, что $f(x, y)$ – билинейная форма
 $q(x) = f(x, x) \quad q(ax) = a^2 q(x)$

Определение 41. Если q положительно/отрицательно определена/полуопределена, то её поляризация $f(x, y)$ называется положительно/отрицательно определенной/полуопределенной

Определение 42. Матрица A называется положительно определенной, если соответствующая ей билинейная форма положительно определена.

Теорема 24. Матрица A (Над \mathbb{R}) – положительно определенная $\Leftrightarrow \exists$ невырожденная $C : A = C^T \cdot C$

Доказательство. A – положительно определена \Leftrightarrow соответствующая ей билинейная форма $f(x, y)$ положительно определена, $q(x)$ – положительно определена. $\Leftrightarrow \exists$ базис: матрица квадратичной формы q – E ($x_1^2 + \dots + x_n^2$) $\Leftrightarrow \exists$ матрица перехода $C : E = C^T A C \Leftrightarrow A = (C^T)^{-1} \cdot C^{-1}$ \square

Теорема 25 (Якоби, критерий положительной определенности). Теорема верна для любого поля, но в основном мы находимся над \mathbb{R}

$q : V \rightarrow K, \text{char} K \neq 2, q \rightarrow A, \Delta_i \neq 0, i = 1, \dots, n \Rightarrow \exists$ базис $(e'_i) : q(x) = \frac{\Delta_0}{\Delta_1} x_1^2 + \frac{\Delta_1}{\Delta_2} x_2^2 + \dots + \frac{\Delta_{n-1}}{\Delta_n} x_n^2$

Доказательство. По индукции.

$n = 1 q(x) = a_{11} x_1^2 = \frac{1}{a_{11}} (a_{11} x_1)^2$

Индукционный переход: $n - 1 \rightarrow n$

$(e_i), i = 1, \dots, n$ – исходный произвольный базис $U = \langle e_1, \dots, e_{n-1} \rangle \subset V$

$\bar{q} = q|_U, \bar{A}$ – матрица A , в которой вычеркнули последнюю строчку и столбец.

Для \bar{q} утверждение верно. Заметим, что $\overline{\Delta_1} = \Delta_1, \dots, \overline{\Delta_{n-1}} = \Delta_{n-1} (\overline{\Delta_i})$ – главные миноры для $\bar{A} \Rightarrow \exists (e'_i), i = 1, \dots, n - 1 : \bar{q} = \frac{\Delta_0}{\Delta_1} x_1'^2 + \dots + \frac{\Delta_{n-2}}{\Delta_{n-1}} x_{n-1}'^2$

Возвращаемся в пространство V , ищем вектор x $\{f(x, e'_i) = 0, i = 1, \dots, n-1$ – система линейных уравнений, $n-1$ уравнение, n неизвестных. $\text{rank СЛУ} < n \Rightarrow \exists$ нетривиальное решение $\Rightarrow \exists \tilde{e}_n$ – решение СЛУ. На данный момент имеем, что q почти нужна к нужному виду, но последний коэффициент неизвестный. $q = \frac{\Delta_0}{\Delta_1} x_1'^2 + \dots + \frac{\Delta_{n-2}}{\Delta_{n-1}} x_{n-1}'^2 + ? x_n'^2$

$e'_n = \lambda \tilde{e}_n$ λ выберем: C – матрица перехода от (e_i)

$K(e'_i, \tilde{e}_n)$ $\det C$ – линейно зависит от λ

$$\begin{cases} e_1 = \dots \\ \dots \\ \lambda \tilde{e}_n = \lambda \dots \lambda \end{cases}$$

$$\lambda : \det C = \frac{1}{\det A} = \frac{1}{\Delta_n}$$

В базисе $(e'_i), i = 1, \dots, n$ A' – матрица квадратичной формы q – диагональная

$$\frac{f(e'_n, e'_n)}{\Delta_{n-1}} = \frac{\Delta_0}{\Delta_1} \cdot \frac{\Delta_1}{\Delta_2} \cdot \dots \cdot \frac{\Delta_{n-1}}{\Delta_{n-1}} \cdot f(e'_n, e'_n) = \det A' = \det(C^T A C) = (\det C)^2 \cdot \det A = \frac{1}{\Delta_n^2} \cdot \Delta_n = \frac{1}{\Delta_n} \Rightarrow$$

$$f(e'_n, e'_n) = \frac{\Delta_{n-1}}{\Delta_n}$$

□

Следствие. $q : V \rightarrow \mathbb{R}$ – квадратичная форма

Тогда отрицательный индекс инерции q равен числу перемен знака в последовательности $\Delta_0, \Delta_1, \dots, \Delta_n$

Теорема 26 (Критерий Сильвестра). $q : V \rightarrow \mathbb{R}$

q – положительно определена $\Leftrightarrow \Delta_i > 0, i = 1, \dots, n$

Доказательство. \Leftarrow . Очевидно.

\Rightarrow . По индукции.

$$n = 1 \quad q = a_{11} x_1^2, a_{11} > 0$$

Индукционный переход: $n-1 \rightarrow n$ $U = \langle e_1, \dots, e_{n-1} \rangle$

$\bar{q} = q|_U$ – положительно определена $\Rightarrow \Delta_i > 0, i = 1, \dots, n-1$

q – положительно определена $\Rightarrow A$ – положительно определена $\Rightarrow A = C^T C \Rightarrow \Delta_n = \det A = (\det C)^2 > 0$

□

2.7.3. Ортогональные преобразования

Определение 43. $X = CY$ – замена переменных. Соответствует переходу от одного базиса к другому.

Определение 44. Матрица C называется ортогональной, если она обладает следующим

$$\text{свойством } C^T C = E \Leftrightarrow \sum_{k=1}^n c_{ik} c_{jk} = \begin{cases} 1, i = j \\ 0, i \neq j \end{cases} \Leftrightarrow \sum_{k=1}^n c_{ki} c_{kj} = \begin{cases} 1, i = j \\ 0, i \neq j \end{cases}$$

Пример. $\begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}, \quad \frac{1}{3} \begin{pmatrix} -1 & 2 & 2 \\ 2 & -1 & 2 \\ 2 & 2 & -1 \end{pmatrix}$

Теорема 27. $\forall q: V \rightarrow \mathbb{R} \exists$ ортогональное преобразование C :
 $q = \lambda_1 x_1^2 + \dots + \lambda_n x_n^2, \lambda_i$ – собственные числа матрицы A

Раздел #3: Элементы теории полей

Пример. Примеры полей: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p, K(x)$.

Notation. $\mathbb{Z}_p = \mathbb{F}_p$ – конечное поле с p элементами.

Определение 45. Если $K \subset L$, K, L – поля, то K называется *подполем* поля L , а L – *расширением* поля K .

Определение 46. Если в поле K нет подполей, отличных от K , то поле называется *простым*.

Теорема 28 (О простых подполях). Любое поле содержит простое подполе, изоморфное либо полю \mathbb{Q} , либо \mathbb{F}_p .

Доказательство. Возьмем единицу и будем прибавлять её к самой себе. Если $\text{char } K = 0$, то таким образом мы сможем получить любое целое число. К тому же, у нас есть противоположные по знаку числа, а значит $\mathbb{Z} \subset K$. Более того, в поле есть также и обратные числа, а значит и $\mathbb{Q} \subset K$.

Если же $\text{char } K = p$, то $\underbrace{1 + \dots + 1}_p = 0$. Рассмотрим множество $\{0, 1, \dots, p-1\} = \mathbb{F}_p$. □

Пример. $\mathbb{R}(i) = \mathbb{C}$.

3.1. Факторкольцо

Пусть R – ассоциативное коммутативное кольцо с 1, K – поле.

Определение 47. Множество $I \subset R$ называется *идеалом* кольца R , если

1. I – аддитивная группа кольца R
2. $\forall r \in R \forall a \in I \quad ra \in I$

Пример. $I = \{0\}$.

Пример. $R = \mathbb{Z}, I = m\mathbb{Z}$.

Пример. $R = K[x]$. Тогда $I = \{f \in K[x] : f(a) = 0\}$.

Пример. $a_1, \dots, a_n \in R$. Тогда $I = \{r_1 a_1 + \dots + r_n a_n, r_i \in R, i = 1, \dots, n\}$.

Определение 48. $I = \{r_1 a_1 + \dots + r_n a_n, r_i \in R\}$ – идеал, порожденный $a_1, \dots, a_n \in R$.

Notation. $I = (a_1, \dots, a_n)$ – идеал, порожденный $a_1, \dots, a_n \in R$.

Определение 49. Если идеал $I = (a)$, то он называется *главным*.

Определение 50. Если в области целостности R любой идеал является главным, то R – кольцо главных идеалов.

Теорема 29 (Кольцо многочленов – кольцо главных идеалов). У любого $I \neq (0)$ идеала в $K[x]$ $\exists!$ нормированный $f \in K[x] : I = (f)$.

Доказательство. Выберем среди $f \in I$ многочлен с наименьшей степенью. Пусть

$$f = a_n x^n + \dots, \quad a_n \neq 0$$

Тогда $g = a_n^{-1} f \in I$.

Возьмем произвольный $h \in I$ и поделим его на g , т.е.

$$h = gq + r, \quad g, r \in K[x], \deg r < \deg g$$

Тогда $r = h - gq \in I$. Получаем противоречие, а значит $r = 0 \Rightarrow I = (g)$.

Докажем теперь однозначность. Пусть $I = (g_1), I = (g_2)$. Тогда

$$g_1 = c_1 \cdot g_2, \quad c_1 \in R, \quad g_2 = c_2 \cdot g_1, \quad c_2 \in R$$

Поэтому

$$g_1 = c_1 \cdot c_2 \cdot g_1 \Rightarrow c_1 \cdot c_2 = 1 \Rightarrow c_1 = c_2 = 1$$

□

Пример. $\mathbb{R}[x]$.

- $(x^2 + 1) = \{f(x) \cdot (x^2 + 1)\}$
- $(x - 1) = \{f(x) \cdot (x - 1)\}$
- $(x^2 - 5x + 4) = \{f(x)(x^2 - 5x + 4)\}$

Определение 51 (Конструкция факторкольца). I – идеал, R – ассоциативное коммутативное кольцо с 1. Рассмотрим

$$R/I = \{r + I, r \in R\}$$

Будем говорить, что r и r' сравнимы по $\text{mod } I$ и писать $r \equiv r' \pmod{I}$, если $r - r' \in I$. Определим сложение и умножение на R/I .

1. $\bar{r} + \bar{s} = \overline{r + s}$, т.е. $(r + I) + (s + I) = r + s + I$
2. $\bar{r} \cdot \bar{s} = \overline{rs}$, т.е. $(r + I) \cdot (s + I) = rs + I$.

Теорема 30 (Корректность определения операций). Операции сложения и умножения в факторкольце определены корректно.

Доказательство. 1. Самостоятельно

2. $r \equiv r' \pmod{I}$, $s \equiv s' \pmod{I}$. Тогда

$$\bar{r}' \cdot \bar{s}' = (r' + I) \cdot (s' + I) = r' \cdot s' + I = (r + a) \cdot (s + b) + I = rs + rb + as + ab + I = rs + I = \bar{r} \cdot \bar{s}$$

Третье равенство верно, т.к. $r \equiv r' \pmod{I} \Leftrightarrow r = r' + a, a \in I$. Аналогично, $s' = s + b, b \in I$. □

Теорема 31. R/I – кольцо.

Определение 52. Множество R/I называется *факторкольцом*.

3.2. Расширение полей

Определение 53. Поле $K(\theta_1, \dots, \theta_n)$ – минимальное поле, содержащее само поле K и элементы $\theta_1, \dots, \theta_n$.

Определение 54 (Простое расширение). Если $L = K(\theta), \theta \notin K$, то L – простое расширение.

Пример. $\mathbb{R}(i)$

Пример. $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d}, a, b \in \mathbb{Q}\}$, d – свободное от квадратов.

Пример. $\mathbb{Q}(\sqrt[n]{d}) = \{a_0 + a_1 \sqrt[n]{d} + a_2 \sqrt[n]{d^2} + \dots + a_{n-1} \sqrt[n]{d^{n-1}}, a_i \in \mathbb{Q}, i = 0, \dots, n-1\}$, где $\forall p \ d \nmid p^n$, p – простое.

Пример. $\mathbb{Q}(\pi) \simeq \mathbb{Q}(x)$. π – трансцендентный элемент.

Определение 55. Элемент $\theta \in L$ алгебраичен над полем K , если θ – корень многочлена $f \in K[x]$. Иначе, θ – трансцендентный элемент над K .

Определение 56. Пусть $K \subset L$ и $\theta \in L$ – алгебраичен над K . Нормированный многочлен минимальной степени $f \in K[x] : f(\theta) = 0$ называется *минимальным многочленом*. Степень минимального многочлена – это степень элемента θ над K .

Теорема 32 (Неприводимость минимального многочлена). Пусть $K \subset L$, θ – алгебраичен над K , f – минимальный многочлен θ . Тогда

1. f – неприводим над K ;
2. Если $g \in K[x] : g(\theta) = 0$, то $f|g$.

Доказательство. 1. Предположим, что f приводим. Тогда $f = h_1 h_2$, $\deg h_i \geq 1, i = 1, 2$. Тогда

$$f(\theta) = 0 \Rightarrow h_1(\theta)h_2(\theta) = 0 \Rightarrow h_i(\theta) = 0$$

Но $\deg h_i < \deg f$, а значит мы получили противоречие минимальности f . Отсюда, f – неприводим.

2. Поделим g на f :

$$g = f \cdot q + r, \quad \deg r < \deg f$$

Тогда

$$g(\theta) = f(\theta) \cdot q(\theta) + r(\theta) \Rightarrow r(\theta) = 0 \Rightarrow r = 0$$

Откуда получаем, что $f|g$.

□

Определение 57. Пусть $K \subset L$. Рассмотрим L как векторное пространство над полем K . Тогда *степенью расширения* L над K называется размерность векторного пространства L над K .

Notation. $[L : K] = \dim_K L$ – степень расширения L над K .

Замечание. Расширение называется конечным, если $[L : K] < \infty$.

Теорема 33. Любое конечное расширение является алгебраичным.

Доказательство. Пусть $K \subset L$, $[L : K] = n$. Возьмем произвольный элемент $\theta \in L$ и рассмотрим его степени: $1, \theta, \theta^2, \dots, \theta^{n-1}, \theta^n$. Этот набор элементов – линейно зависимый, поэтому существует $a_i \in K$ такие, что

$$a_0 + a_1\theta + \dots + a_n\theta^n = 0$$

где не все a_i нулевые. А это и значит, что существует $g \in K[x] : g(\theta) = 0$.

□

Теорема 34. Пусть $K \subset L \subset M$. Предположим, что $[L : K], [M : L] < \infty$. Тогда расширение M над K конечно и $[M : K] = [M : L] \cdot [L : K]$.

Теорема 35 (Структура простых алгебраических расширений). Пусть $K \subset K(\theta)$, где θ – алгебраичен над K , $\theta \notin K$; f – минимальный многочлен θ , $\deg f = n$. Тогда

1. $K(\theta) \simeq K[x]/(f)$;
2. $[K(\theta) : K] = n$ и $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ – базис $K(\theta)$ над K ;
3. Если $\alpha \in K(\theta)$ – алгебраичен над K , то степень элемента α делит n .

Пример. $\mathbb{F}_2 = \{0, 1\}$. Рассмотрим неприводимый многочлен 2-й степени над \mathbb{F}_2 :

$$f = x^2 + x + 1, \quad \theta - \text{корень}$$

$$\mathbb{F}_2[x]/(x^2 + x + 1) = \{0, 1, x, x + 1\}.$$

$$x \cdot x \equiv x + 1 \pmod{x^2 + x + 1}$$

$$x(x + 1) \equiv 1$$

$$(x + 1)(x + 1) \equiv x$$