Алгебра 2 семестр ПИ,
Лекции

Собрано 31 мая 2022 г. в 18:15

Содержание

Раздел #1: Системы линейных уравнений

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

$A = (a_{ij})$ – 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 $\alpha_1, ..., \alpha_n \in K$: 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

$A - m \times n, A = (A_1, A_2, ..., A_m), A_i$ – строки.
$A = (A^1, A^2, ..., A^n), A^j$ – столбцы.

Определение 3. Строчным (столбцовым) рангом матрицы A называется максимальное число ЛНЗ строк (столбцов).
Иначе, количество элементов в базисе $\langle A_1, ..., A_m \rangle (\langle A^1, ..., A^n \rangle)$.

Теорема 1. Строчный и столбцовый ранги совпадают.

Обозначение: $\operatorname{rank} A$.

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 $\operatorname{rank} A < n \Leftrightarrow \det A = 0$.

Доказательство. $\Rightarrow$. $\operatorname{rank} A < n \Rightarrow$ строки $A_1, ..., A_n$ ЛЗ, т.е. $\exists \alpha_1, ..., \alpha_n \in K$: $\alpha_1 A_1 + \alpha_2 A_2 + ... + \alpha_n A_n = 0$ (α_i не все равны нулю). Пусть $\alpha_1 \neq 0 \Rightarrow A_1 = -\frac{\alpha_2}{\alpha_1} A_2 - ... - \frac{\alpha_n}{\alpha_1} A_n$. Обнулим 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 $n = 1 \Rightarrow a_{11} = 0$. $n - 1 \to n$.

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

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

$0 = \alpha_2 A'_2 + ... + \alpha_n A'_n = (...) A_1 + \alpha_2 \cdot A_2 + ... + \alpha_n A_n \Rightarrow A_1, ..., A_n$ – ЛЗ $\Rightarrow \operatorname{rank} A < n$. □

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. $(A_1, ..., A_i, ..., A_j, ..., A_n) \to (A_1, ..., A_i + \lambda A_j, ..., A_j, ..., A_n)$ □

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, $r = \operatorname{rank} A \Rightarrow \exists n - r$ ЛНЗ решений $X_1, ..., X_{n-r} : \forall$ решение $X = \alpha_1 X_1 + ... + \alpha_{n-r} X_{n-r}$.

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

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

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

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

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

Получили следующую систему линейных уравнений: $\{y_1 A_1 + ... + y_r A_r = 0$.

Но $A_1, ..., A_r$ – ЛНЗ $\Rightarrow Y = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \Rightarrow 0 = Z + x_{r+1}^* X_1 + x_{r+2}^* X_2 + ... + x_n^* X_{n-r}$. □

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

1.3. Неоднородные СЛУ

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

$\overline{A} = \left(\begin{array}{c|c} A & B \end{array} \right)$ – расширенная матрица $m \times (n+1)$.

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

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

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

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

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

Пример (Решение СЛУ методом Гаусса).

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

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

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

Раздел #2: Линейные отображения векторных пространств

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

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

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

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

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

Доказательство. Пусть $f, g \in \mathrm{Hom}(V, W)$. Тогда

$$(f+g)(x) = f(x) + g(x) \in \mathrm{Hom}(V, W)$$
$$(\alpha f)(x) = \alpha f(x) \in \mathrm{Hom}(V, W)$$

□

Определение 12 (Ядро линейного отображения). Пусть $f \in \mathrm{Hom}(V, W)$. Тогда

$$\ker f = \{x \in V : f(x) = 0\}$$

называется *ядром отображения* f.

Определение 13 (Образ линейного отображения). Пусть $f \in \mathrm{Hom}(V, W)$. Тогда

$$\mathrm{Im}\, f = \{f(x), x \in V\}$$

называется *образом* f.

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

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

Упражнение. $\mathrm{Im}\, f$ – подпространство.

Теорема 9. $f \in \mathrm{Hom}(V,W)$.

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

Доказательство. $\Leftarrow$. Пусть $x_1 \neq x_2$; если $f(x_1) = f(x_2)$, то $f(x_1 - x_2) = 0 \Rightarrow x_1 - x_2 \in \ker f \Rightarrow x_1 - x_2 = 0$ – противоречие.
$\Rightarrow$. Пусть $x \in \ker f, x \neq 0 \Rightarrow f(x) = f(0) = 0$!?. □

2.1. Матрица линейного отображения

Пусть $e_1, ..., e_n$ – базис $V, e'_1, ..., e'_m$ – базис $W, f \in \mathrm{Hom}(V,W)$
Возьмем $x \in V$ и разложим его по базису $\{e_i\} : x = x_1e_1 + ... + x_ne_n,\ x_i \in K$. Тогда, по линейности, $f(x) = x_1f(e_1) + ... + x_nf(e_n)$, т.е. задать f значит задать $f(e_i),\ i = 1, ..., n$.
Положим

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

Определение 14. Матрицей $f \in \mathrm{Hom}(V,W)$ в базисе $e_1, ..., e_n$ и $e'_1, ..., e'_m$ называется

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

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

2. Если $e_1, ..., e_n$ – базис V, $e'_1, ..., e'_m$ – базис W, $x \in V$ соответствует столбец $X = \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix}^T$, $f(x) \in W$ соответствует столбец $Y = \begin{pmatrix} y_1 & \cdots & y_m \end{pmatrix}^T$, линейному оператору f соответствует матрица A, то

$$AX = Y$$

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

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

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

□

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

2. Пусть $\alpha,\beta \in K$, $f,g \in \mathrm{Hom}(V,W)$, $f \to A$, $g \to B$. Тогда в фиксированных базисах $\alpha f + \beta g \to \alpha A + \beta B$.
3. Пусть $f : V \to W$, $g : W \to U \Rightarrow g \circ f : V \to U$, $g \circ f(x) = g(f(x))$. Тогда если $f \to A$, $g \to B$, то в фиксированных базисах $g \circ f \to BA$.

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. Пусть $V \to M(n,K)$, $W \to M(l,K)$, $U \to M(m,K)$, $A \in M(l,n,K)$, $B \in M(m,l,K)$. Тогда

$$g \circ f(e_i) = g\left(\sum_{k=1}^{l} a_{ki} e_k\right) = \sum_{k=1}^{n} a_{ki} g(e'_k) = \sum_{k=1}^{l} a_{ki} \sum_{j=1}^{m} b_{jk} e''_j = \sum_{j=1}^{m} \sum_{k=1}^{l} b_{jk} a_{ki} e''_j$$

где $b_{jk}a_{ki} \to BA$.

□

Теорема 11. Пусть $f : V \to W$, $\dim V, \dim W < \inf$. Тогда

$$\dim \ker f + \dim \mathrm{Im}\, f = \dim V$$

Доказательство. $\ker f \subset V$, $e_1, ..., e_k$ - базис $\ker f$. Дополним до базиса $V : e_1, ..., e_k, e_{k+1}, ..., e_n$ – базис V. Возьмем $x \in V$. Поскольку $f(x) \in \mathrm{Im}\, f$, то

$$f(x) = x_{k+1} f(e_{k+1}) + ... + x_n f(e_n) \in \mathrm{Im}\, f$$

Так как $e_1, ..., e_k$ – базис $\ker f$, то $f(e_1) = ... = f(e_k) = 0 \Rightarrow \mathrm{Im}\, f = \langle f(e_{k+1}), ..., f(e_n)\rangle$.
Докажем, что $f(e_{k+1}), ..., f(e_n)$ – ЛНЗ. Предположим обратное: пусть существует такой набор $\alpha_{k+1}, ..., \alpha_n$, что $\alpha_{k+1} f(e_{k+1}) + ... + \alpha_n f(e_n) = 0$. Но тогда $f(\alpha_{k+1} e_{k+1} + ... + \alpha_n e_n) = 0 \Rightarrow \alpha_{k+1} e_{k+1} + ... + \alpha_n e_n \in \ker f = \langle e_1, ..., e_k\rangle$, что невозможно.
Отсюда получаем, что если $\dim \ker f = k$, $\dim V = n$, то $\dim \mathrm{Im}\, f = n - k$. □

2.2. Линейные операторы

Определение 15. Линейным оператором называется линейное отображение $a : V \to V$, т.е. $a \in \mathrm{Hom}(V,V)$.

Обозначение. $\mathrm{End}\, V = \mathrm{Hom}(V,V)$

Определение 16. Тождественным отображением называется отображение $\mathrm{id} : x \to x$ (любой вектор переходит сам в себя)

Определение 17. Если a линейный оператор, то b – обратный линейный оператор к a, если $b \circ a = a \circ b = \mathrm{id}$

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

2. Оператор подобия. $\forall x \in V \; ax = \lambda x \to \begin{pmatrix} \lambda & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda \end{pmatrix}$

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

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

   $\frac{d}{dx}(1) = 0, \frac{d}{dx}(x) = 1, \frac{d}{dx}(x^2) = 2x, \frac{d}{dx}(x^3) = 3x^2$. 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 18. Пусть $(e_i), (e'_i)$ – базисы V, $\dim V = n$. Разложим (e'_i) по базису (e_i):

$$\begin{cases} e'_1 = c_{11}e_1 + c_{21}e_2 + \ldots + c_{n1}e_n \\ \ldots \\ e'_n = c_{1n}e_1 + c_{2n}e_2 + \ldots + c_{nn}e_n \end{cases}$$

Тогда матрица вида

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

называется *матрицей перехода* от базиса (e_i) к (e'_i).

Теорема 12 (Преобразование координат вектора при переходе к другому базису). Пусть V

– векторное пространство над полем K, $(e_i), (e'_i)$ – базисы V, $x \in V$, $x \to X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ – координаты вектора в базисе (e_i). $x \to X' = \begin{pmatrix} x'_1 \\ x'_2 \\ \vdots \\ x'_n \end{pmatrix}$ – координаты вектора в базисе (e'_i), C – матрица перехода от (e_i) к (e'_i). Тогда

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

Доказательство. 1. Запишем x в базисе (e'_i):

$$\begin{aligned} x &= x'_1 e'_1 + \ldots + x'_n e'_n = \\ &= x'_1(c_{11}e_1 + c_{21}e_2 + \ldots + c_{n1}e_n) + \ldots + x'_n(c_{1n}e_1 + c_{2n}e_2 + \ldots + c_{nn}e_n) = \\ &= \underbrace{(c_{11}x'_1 + c_{12}x'_2 + \ldots + c_{1n}x'_n)}_{x_1} e_1 + \ldots + \underbrace{(c_{n1}x'_1 + c_{n2}x'_2 + \ldots + c_{nn}x'_n)}_{x_n} e_n \end{aligned}$$

Откуда

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

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). Пусть V – векторное пространство, $\dim V = n$, $a \in \operatorname{End} V$, 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). Тогда

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

Определение 19. Матрицы $A, B \in M(n, K)$ называются подобными, если $\exists C \in M(n, K)$: $A = C^{-1}BC$.

Обозначение. $A \sim B$.

Теорема 14. Отношение подобия матриц – отношение эквивалентности.

Доказательство. Самостоятельно. □

2.3. Инвариантные подпространства

Определение 20. Подпространство U пространства V называется инвариантным (неизменным) под действием оператора a, если $\forall x \in U,\ ax \in U$

Лемма 4. Пусть $U \subset V,\ a \in \operatorname{End} V$. Тогда U – a-инвариантно $\Leftrightarrow$ существует базис V:

$$A = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix}, \quad B = \dim U \times \dim U$$

Доказательство. Пусть U – a-инвариантно. Выберем базис U: $e_1, ..., e_k$ и дополним его до базиса V. Рассмотрим действие оператора a на e_i. Поскольку U – a-инвариантно, то разложение $a(e_i)$ по базису выглядит следующим образом:

$$a(e_i) = b_{1i}e_1 + \cdots + b_{ki}e_k$$

А значит матрица оператора принимает вид:

$$A = \begin{pmatrix} b_{1i} & \cdot \\ b_{ki} & \cdot \\ 0 & \cdot \\ 0 & \cdot \end{pmatrix}$$

В обратную сторону: если есть такая матрица A, то при действии оператора a на первых k базисных векторах мы получим разложение лишь по первым k базисным векторам, а значит U – a-инвариантно.

□

Лемма 5. Пусть $U, W \subset V,\ a \in \operatorname{End} V,\ V = U \oplus W$. Тогда U, W – a-инвариантны $\Leftrightarrow$ существует базис V:

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

где $B = \dim U \times \dim U,\ C = \dim W \times \dim W$

Доказательство. Выберем базис $U : e_1, ..., e_k$ и базис $W : e_{k+1}, ..., e_n$. Тогда

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

□

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

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

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

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

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

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

2.4. Собственные векторы и числа

Определение 21 (Собственный вектор). Собственным вектором оператора a называется любой ненулевой вектор одномерного инвариантного подпространства.

Определение 22 (Собственное число). Пусть x - собственный вектор, $a(x) = \lambda x$, тогда λ – собственное число, ассоциированное вектору x.

Определение 23 (Характеристический многочлен). Если оператору a соответствует матрица A, а собственному вектору x – столбец X, то

$$AX = \lambda X \Leftrightarrow (A - \lambda E)X = 0$$

Характеристическим многочленом оператора a (матрицы A) называется

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

Теорема 15 (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 $\chi_a(t)$. □

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

Доказательство. Пусть $a(e_i) \to A$, $a(e'_i) \to A'$, C – матрица перехода от (e_i) к (e'_i). Как мы знаем, $A' = C^{-1}AC$, поэтому

$$\begin{aligned} \chi_a(t) &= \det(A' - tE) = \det(C^{-1}AC - t \cdot C^{-1}C) = \det(C^{-1}(A - tE)C) = \\ &= \det C^{-1} \cdot \det(A - tE) \cdot \det C = \det(A - tE) \end{aligned}$$

□

Теорема 16 (Линейная независимость собственных векторов). Собственные векторы, соответствующие различным собственным числам, линейно независимы.

Доказательство. Докажем по индукции: для $n = 1$ очевидно.
Предположим, что верно при $n-1$. Индукционный переход: $n-1 \to n$: пусть $V_1, V_2, ..., V_n$ – собственные векторы, $aV_i = \lambda_i V_i$, $\lambda_1, ..., \lambda_n$ – различны. Если $V_1, V_2, ..., V_n$ – линейно зависимы, то $\alpha_1 V_1 + \alpha_2 V_2 + ... + \alpha_n V_n = 0, \alpha_i \in K \Rightarrow$ под действием a: $\alpha_1\lambda_1 V_1 + \alpha_2\lambda_2 V_2 + ... + \alpha_n\lambda_n V_n = 0$
Будем считать, что $\alpha_1 \neq 0 \Rightarrow \alpha_1\lambda_1 V_1 + \alpha_2\lambda_2 V_2 + ... + \alpha_n\lambda_n V_n - \lambda_1(\alpha_1 V_1 + ... + \alpha_n V_n) = \alpha_2(\lambda_2 - \lambda_1)V_2 + ... + \alpha_n(\lambda_n - \lambda_1)V_n = 0 \Rightarrow$ по предположению индукции $\alpha_2 = ... = \alpha_n = 0$ □

Определение 24. Оператор a называется диагонализируемым, если существует базис такой, 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 17 (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. □

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 25 (Алгебраическая кратность собственного числа). Кратность λ как кратность корня $\chi_a(t) = 0$ называется *алгебраической кратностью* собственного числа.

Определение 26 (Геометрическая кратность собственного числа). Пусть λ – собственное число, $V^\lambda = \{x \in V : ax = \lambda x\}$. Тогда $\dim V^\lambda$ называется *геометрической кратностью* 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 λ не превосходит алгебраической кратности

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

$$a \to \begin{pmatrix} B & C \\ 0 & D \end{pmatrix} \quad B - m \times m,\ \dim V^\lambda = m$$

Рассмотрим сужение $a\big|_{V^\lambda}$. Тогда характеристический многочлен этого сужения имеет вид:

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

Построим теперь характеристический многочлен оператора a:

$$\chi_a = \det\left(\begin{pmatrix} B & C \\ 0 & D \end{pmatrix} - tE\right) = (t - \lambda)^m p(t)$$

Отсюда получаем, что алгебраическая кратность $\lambda \geqslant m$. □

Теорема 18 (Критерий диагонализируемости). $a \in \operatorname{End} V$ – диагонализируем тогда и только тогда, когда

1. Все собственные числа из K;
2. $\forall$ собственных чисел λ алгебраическая кратность равна геометрической кратности.

2.5. Жорданова нормальная форма

Определение 27 (Жорданова клетка). *Жордановой клеткой* порядка m, соответствующей

собственному числу λ называется

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

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 28 (Жорданова нормальная форма). *Жордановой нормальной формой* оператора $a \in \operatorname{End} V$ называется

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

Определение 29 (Жорданов базис). Базис, в котором оператор a имеет ЖНФ называется *жордановом*.

Теорема 19 (ЖНФ). 1. Над алгебраическим замкнутым полем $\forall a \in \operatorname{End} V$ имеет ЖНФ

2. ЖНФ определена с точностью до перестановки клеток

Теорема 20. $a \in \operatorname{End} V$ имеет ЖНФ над произвольным полем $\Leftrightarrow$ характеристический многочлен раскладывается на линейные множители.

2.6. Теорема Гамильтона-Кэли

Определение 30. Пусть $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in K[x]$, $A - m \times m$. Тогда

$$f(A) = a_n A^N + \ldots + a_i A + a_0 E, \quad E \in M(m, K)$$

есть многочлен f от матрицы A.

Определение 31. Пусть $a \in \operatorname{End} V$. Тогда

$$f(a) = a_n \cdot a^n + \ldots + a_1 \cdot a + a_0 \cdot \mathrm{id}$$

есть многочлен от оператора.

Теорема 21 (Гамильтона-Кэли). Пусть $a \in \operatorname{End} V$, $a \to A \in M(m, K)$. Тогда $\chi_a(A) = 0$.

Доказательство. По определению, $\chi_a(t) = \det(tE - A) = t^m + c_{m-1}t^{m-1} + \ldots + c_1 t + c_0$. Положим $B = tE - A$, тогда $\widetilde{B} = (B_{ij})^T$ – взаимная матрица. Тогда

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

Элементы матрицы $\widetilde{B}$ – многочлены от переменной t, причем их степени не превосходят $m-1$. Действительно, каждый элемент B это, с точностью до знака, определитель матрицы порядка $m-1$, составленной из многочленов степени $\leqslant 1$, причем в каждой строке не больше одного не-константного многочлена. Тогда можно представить $\widetilde{B}$ в виде

$$\widetilde{B} = \widetilde{B}_0 + t\widetilde{B}_1 + \ldots + t^{m-1}\widetilde{B}_{m-1}, \quad \widetilde{B}_i \in M(n, F)$$

Тогда формула выше может быть переписана следующим образом:

$$\begin{aligned}\chi_a \cdot E = B \cdot \widetilde{B} = (tE - A) \cdot (\widetilde{B}_0 + t\widetilde{B}_1 + \ldots + t^{m-1}\widetilde{B}_{m-1}) = \\ = t^m \widetilde{B}_{m-1} + t^{m-1}(\widetilde{B}_{m-2} - A\widetilde{B}_{m-1}) + \ldots + t(\widetilde{B}_0 - A\widetilde{B}_1) - A\widetilde{B}_0\end{aligned}$$

С другой стороны,

$$\chi_a \cdot E = t^m E + t^{m-1} c_{m-1} E + \ldots + t c_1 E + c_0 E$$

Сравнивая слагаемые при соответствующих степенях, получаем следующее:

$$\widetilde{B}_{m-1} = E, \qquad \widetilde{B}_{i-1} - A\widetilde{B}_i = c_i E, \ i = 1, \ldots, m-1, \qquad -A\widetilde{B}_0 = c_0 E$$

Умножим слева равенство, отвечающее за t^i, на A^i, и сложим все полученные:

$$A^m \widetilde{B}_{m-1} + A^{m-1}(\widetilde{B}_{m-2} - A\widetilde{B}_{m-1}) + \ldots + A(\widetilde{B}_0 - A\widetilde{B}_1) - A\widetilde{B}_0 = A^m + c_{m-1}A^{m-1} + \ldots + c_1 A + c_0 E$$

Все слагаемые в левой части сокращаются, а в правой части стоит $\chi_a(A)$. □

2.7. Билинейные формы

Определение 32. $f : V \times V \to K$ линейное по каждому аргументу называется билинейным отображением, то есть выполняется

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

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

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

Определение 33. Пусть $B = (b_{ij})$, $b_{ij} = f(e_i, e_j)$, $1 \leqslant i, j, \leqslant n$. Тогда матрица B называется *матрицей билинейной формы* f

Замечание. Пусть B – матрица билинейной формы f, $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, $Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$. Тогда билинейную форму f можно записать в матричном виде:

$$f(x,y) = X^T B Y$$

Пример. 1. Скалярное произведение $(x,y) = x_1y_1 + \ldots + x_ny_n = (x_1, \ldots, x_n)\begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$

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

Определение 34. Билинейная форма f называется

1. Симметрической, если $f(x,y) = f(y,x) \forall x, y \in V \quad B = B^T$ (симметрическая матрица)
2. Кососимметрической, если $f(x,y) = -f(y,x) \forall x, y \in V \quad -B = B^T$ (кососимметрическая матрица)

2.7.1. Замена базиса

Теорема 22 (Преобразование матрицы билинейной формы при изменении базиса). Пусть $f : V \times V \to K$ – билинейная форма и в базисе (e_i) ей соответствует матрица B, а в базисе (e'_i) – матрица B'. Тогда

$$B' = C^T B C$$

где C – матрица перехода от (e_i) к (e'_i).

Доказательство. Пусть $x \to X$, $y \to Y$ в базисе (e_i), X', Y' в базисе (e'_i) соответственно. Тогда $X = CX'$ и $Y = CY'$, поэтому

$$f(x,y) = X^T B Y = (CX')^T B (CY') = X'^T C^T B C Y' = X'^T B' Y'$$

Откуда и получаем искомое равенство. □

2.8. Квадратичные формы

Определение 35 (Квадратичная форма). *Квадратичной формой* $Q : V \to K$, ассоциированной с некоторой симметрической билинейной формой $f : V \times V \to K$, называется $q(x) = f(x, x)$.

Определение 36 (Матрица квадратичной формы). Матрицу квадратичной формы можно записать так: $q(x) = X^T A X$, где $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

$$q(x) = \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix} \begin{pmatrix} a_{11} & & \\ & \ddots & \\ & & a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \sum_{i,h=1}^{n} a_{ij} x_i x_j$$

Но последняя сумма – это однородный многочлен 2 степени от n переменных. Поскольку матрица симметрическая, т.е. $a_{ij} = a_{ji}$, то $a_{ij}x_ix_j + a_{ji}x_ix_j = 2a_{ij}x_ix_j$, поэтому квадратичную форму можно также записать в следующем виде:

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

Определение 37 (Канонический вид к.ф.). *Каноническим видом* квадратичной формы называется $\sum_{i=1}^{n} \lambda_i x_i^2$

Определение 38 (Канонический базис). Базис, в котором квадратичная форма имеет канонический вид, называется *каноническим*.

Замечание. Замена переменной ↔ переход к другому базису

Теорема 23 (Преобразование Лагранжа). Пусть V – векторное пространство над полем K, $\operatorname{char} K \neq 2$. Тогда любая квадратичная форма $q : V \to K$ может быть приведена к каноническому виду (т.е. существует базис, в котором q имеет канонический вид)

Доказательство. Пусть $q(x) = \sum_{i=1}^{n} a_{ii}x_i^2 + 2\sum_{i<j}^{a_ij} x_ix_j$
Если $q = 0$, то доказывать нечего, поэтому будем считать, что $q \neq 0$.

1. Пусть $a_{11} = 0, \exists i > 1 : a_{ii} \neq 0 \Rightarrow$ сделаем замену $y_i = x_1,\ x_i = y_1 \Rightarrow a_{11}y_1^2 + \ldots$, где $a_{11} \neq 0$;
2. $a_{ii} = 0\ \forall i = 1, \ldots, n \Rightarrow \exists a_{ij} \neq 0, i < j \Rightarrow x_i = y_i + y_j, x_j = y_i - y_j$. Тогда $a_{ij}x_ix_j$ примет вид

$a_{ij}(y_i+y_j)(y_i-y_j) = a_{ij}\cdot y_i^2 - a_{ij}y_j^2 \Rightarrow$ по п.1 можно считать, что $a_{11}\neq 0$;

3. Докажем по индукции. База: $n=1 : q(x) = a_{11}x_1^2$.
Индукционный переход: $n-1 \to n$, $a_{11}\neq 0$ в силу первого пункта. Тогда

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

□

2.8.1. Квадратичная форма над $\mathbb{R}$

Определение 39 (Нормальный вид к.ф.). Говорят, что квадратичная форма приведена к *нормальному* виду, если она представляет собой сумму чистых квадратов $(y_1^2+\ldots+y_s^2-y_{s+1}^2-\ldots-y_r^2)$.

Замечание. Пусть мы хотим привести форму вида

$$\lambda_1x_1^2 + \ldots + \lambda_nx_n^2$$

к нормальному виду. Если находимся над полем $\mathbb{C}$, тогда $y_i = \sqrt{\lambda_i}x_i \Rightarrow y_1^2+\ldots+y_r^2, r$ – ранг формы, $r\leqslant n$
Над $\mathbb{R}$ ситуация иная. $\lambda_i>0$ $y_i = \sqrt{\lambda_i}x_i$, $\lambda_j<0$ $y_i = \sqrt{-\lambda_j}x_j \Rightarrow$

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

Определение 40 (Ранг к.ф.). *Ранг* квадратичной формы равен рангу соответствующей матрицы: $\operatorname{rank} q = \operatorname{rank} A$

Теорема 24 (Закон инерции квадратичных форм). Пусть $q : V\to\mathbb{R}$ – квадратичная форма, $\dim V = n$, $\operatorname{rank} q = r$. Тогда параметры s и $r-s$ при приведении квадратичной формы к нормальному виду не зависят от базиса.

Доказательство. Пусть A – матрица квадратичной формы в базисе $(e_i) \Rightarrow C^TAC$ – 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^TAC. $\operatorname{rank} A = \operatorname{rank} C^TAC = r$ (было доказано)

Предположим, что в базисе (e_i) квадратичная форма имеет следующий вид:

$$q = x_1^2 + ... + x_s^2 - x_{s+1}^2 - ... - x_r^2$$

А в базисе (e'_i):

$$q = x_q^2 + ... + x_t^2 - x_{t+1}^2 - ... - x_r^2$$

Предположим, что $t < s$ Рассмотрим два подпространства пространства $V : U_1 = \langle e_1, ..., e_s \rangle$ и $U_2 = \langle e'_{t+1}, ..., e'_n \rangle$. Рассмотрим размерность подпространства $U_1 + U_2$. С одной стороны, $\dim(U_1 + U_2) \leqslant n$. С другой,

$$\dim(U_1 + U_2) = \dim U_1 + \dim U_2 - \dim(U_1 \cap U_2) = s + n - t - \dim(U_1 \cap U_2)$$

Поэтому $\dim(U_1 \cap U_2) \geqslant s + n - t - n = s - t > 0$, т.е. существует ненулевой вектор $x \in U_1 \cap U_2$. Тогда $q(x) > 0$, т.к. $x \in U_1$ Но в то же время $q(x) < 0$, поскольку $x \in U_2 \Rightarrow$ противоречие. □

Определение 41 (Индексы инерции). 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. $f(x) - f(x_0) = \sum f'_{x_i} \Delta x_i + \sum f''_{x_i x_j} \Delta x_i \Delta x_j + ...$

Определение 42. Всё рассматриваем над $\mathbb{R}$. Квадратичная форма $q : V \to \mathbb{R}$ называется

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

Пример. $n = 2$

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

2.8.2. Теорема Якоби

Определение 43 (Главные миноры). Пусть $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$

Тогда

$$\Delta_0 = 1,\ \Delta_1 = a_{11},\ \Delta_2 = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}, \dots,\ \Delta_n = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}$$

называются *главными минорами.*

Определение 44. Пусть $\operatorname{char} K \neq 2$. Тогда

$$f(x,y) = \frac{1}{2}(q(x+y) - q(x) - q(y))$$

называется билинейной формой, полученной поляризацией квадратичной формы q.

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

Определение 45. Если q положительно/отрицательно определена/полуопределена, то её поляризация $f(x,y)$ называется положительно/отрицательно определенной/полуопределенной

Определение 46. Матрица A называется положительно определенной, если соответствующая ей билинейная форма положительно определена.

Теорема 25. 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 (т.е. квадратичная форма имеет вид $x_1^2 + \dots + x_n^2$) $\Leftrightarrow \exists$ матрица перехода $C : E = C^T A C \Leftrightarrow A = (C^T)^{-1} \cdot C^{-1}$ □

Теорема 26 (Якоби). Теорема верна для любого поля, но в основном мы находимся над $\mathbb{R}$. Пусть $q : V \to K,\ \operatorname{char} K \neq 2,\ q \to A,\ \Delta_i \neq 0,\ i = 1, \dots, n \Rightarrow \exists$ 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. Докажем по индукции. $n = 1$

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

Индукционный переход: $n-1 \to n$. Пусть $(e_i),\ i = 1,...,n$ – исходный произвольный базис $U = \langle e_1,...,e_{n-1}\rangle \subset V$, $\overline{q} = q\big|_U$, $\overline{A}$ – матрица A, в которой вычеркнули последнюю строчку и столбец. Для $\overline{q}$ утверждение верно. Заметим, что $\overline{\Delta}_1 = \Delta_1, ..., \overline{\Delta}_{n-1} = \Delta_{n-1}(\overline{\Delta}_i)$ – главные миноры для $\overline{A} \Rightarrow \exists(e_i'),\ i = 1,...,n-1$:

$$\overline{q} = \frac{\Delta_0}{\Delta_1}x_1'^2 + ... + \frac{\Delta_{n-2}}{\Delta_{n-1}}x_{n-1}'^2$$

Возвращаемся в пространство V, ищем вектор x. $\{f(x, e_i') = 0,\ i = 1,..,n-1$ – система линейных уравнений, $n-1$ уравнение, n неизвестных, rank СЛУ $< n \Rightarrow \exists$ нетривиальное решение $\Rightarrow \exists\widetilde{e}_n$ – решение СЛУ. На данный момент имеем, что q почти приведена к нужному виду, но последний коэффициент неизвестный: $q = \frac{\Delta_0}{\Delta_1}x_1'^2 + ... + \frac{\Delta_{n-2}}{\Delta_{n-1}}x_{n-1}'^2 + ?x_n'^2$
Возьмем $e_n' = \lambda\widetilde{e}_n$, а λ выберем так: пусть C – матрица перехода от (e_i) к $(e_i', \widetilde{e}_n)$. Заметим, что $\det C$ – линейно зависит от λ. Положим $\lambda : \det C = \frac{1}{\det A} = \frac{1}{\Delta_n}$
Тогда в базисе $(e_i'),\ i = 1,...,n'$ – матрица квадратичной формы q – диагональная. Покажем, что квадратичная форма в этом базисе имеет требуемый вид. Действительно,

$$\frac{f(e_n', e_n')}{\Delta_{n-1}} = \frac{\Delta_0}{\Delta_1}\cdot\frac{\Delta_1}{\Delta_2}\cdot ...\cdot\frac{\Delta_{n-1}}{\Delta_{n-1}}\cdot f(e_n', e_n') = \det A' = \det(C^TAC) = (\det C)^2\cdot\det A = \frac{1}{\Delta_n^2}\cdot\Delta_n = \frac{1}{\Delta_n}$$

□

Следствие. $q : V \to \mathbb{R}$ – квадратичная форма
Тогда отрицательный индекс инерации q равен числу перемен знака в последовательности $\Delta_0, \Delta_1, ..., \Delta_n$

Теорема 27 (Критерий Сильвестра положительной определенности). Пусть $q : V \to \mathbb{R}$ – квадратичная форма. Тогда q – положительно определена $\Leftrightarrow \Delta_i > 0, i = 1,...,n$

Доказательство. $\Leftarrow$. Очевидно.
$\Rightarrow$. По индукции. $n = 1 : q = a_{11}x_1^2, a_{11} > 0$.
Индукционный переход: $n-1 \to n$. $U = \langle e_1,...,e_{n-1}\rangle$. $\overline{q} = q\big|_U$ – положительно определена $\Rightarrow \Delta_i > 0,\ i = 1,...,n-1$. Т.к. q – положительно определена, то и A положительно определена $\Rightarrow A = C^TC \Rightarrow \Delta_n = \det A = (\det C)^2 > 0$ □

2.8.3. Ортогональные преобразования

Определение 47. $X = CY$ – замена переменных. Соответствует переходу от одного базиса к другому.

Определение 48. Матрица C называется ортогональной, если она обладает следующим 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. $\begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}$, $\frac{1}{3}\begin{pmatrix} -1 & 2 & 2 \\ 2 & -1 & 2 \\ 2 & 2 & -1 \end{pmatrix}$

Теорема 28. Пусть $\forall q : V \to \mathbb{R}$ – квадратичная форма. Тогда существует ортогональное преобразование C :

$$q = \lambda_1 x_1^2 + ... + \lambda_n x_n^2$$

где, λ_i – собственные числа матрицы A.

Раздел #3: Элементы теории полей

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

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

Определение 49. Если $K \subset L$, K, L – поля, то K называется *подполем* поля L, а L – *расширением поля* K.

Определение 50. Если в поле K нет подполей, отличных от K, то поле называется *простым*.

Теорема 29 (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 $\operatorname{char} K = 0$, 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 $\operatorname{char} K = p$, то $\underbrace{1 + \ldots + 1}_{p} = 0$. Рассмотрим множество $\{0, 1, \ldots, p-1\} = \mathbb{F}_p$. □

Пример. $\mathbb{R}(i) = \mathbb{C}$.

3.1. Факторкольцо

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

Определение 51 (Идеал). Множество $I \subset R$ называется *идеалом* кольца R, если

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

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. $a_1, ..., a_n \in R$. Тогда $I = \{r_1a_1 + ... + r_na_n,\ r_i \in R,\ i = 1, ..., n\}$.

Определение 52. $I = \{r_1a_1 + ... + r_na_n,\ r_i \in R\}$ – идеал, порожденный $a_1, ..., a_n \in R$.

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

Определение 53 (Главный идеал). Если идеал $I = (a)$, то он называется *главным*.

Определение 54 (Кольцо главных идеалов). Если в области целостности R любой идеал является главным, то R – *кольцо главных идеалов*.

Теорема 30 (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

$$f = a_nx^n + ..., \quad a_n \neq 0$$

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

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

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 55 (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 $\bmod I$ и писать $r \equiv r' (\bmod I)$, если $r - r' \in I$. Определим сложение и умножение на R/I.

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

Теорема 31 (Корректность определения операций). Операции сложения и умножения в факторкольце определены корректно.

Доказательство. 1. Самостоятельно

2. $r \equiv r' \bmod I$, $s \equiv s' \bmod I$. Тогда

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

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

Теорема 32. R/I – кольцо.

Определение 56 (Факторкольцо). Множество R/I называется *факторкольцом*.

3.2. Расширение полей

Определение 57. Поле $K(\theta_1, ..., \theta_n)$ – минимальное поле, содержащее само поле K и элементы $\theta_1, ..., \theta_n$.

Определение 58 (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. $\mathbb{Q}(\sqrt[n]{d}) = \{a_0 + a_1 \sqrt[n]{d} + a_2 \sqrt[n]{d^2} + ... + a_{n-1} \sqrt[n]{d^{n-1}}, a_i \in \mathbb{Q}, i = 0, ..., n-1\}$, где $\forall p \; d \not\vdots p^n$, p – простое.

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

Определение 59. Элемент $\theta \in L$ *алгебраичен* над полем K, если θ – корень многочлена $f \in K[x]$. Иначе, θ – *трансцендентный* элемент над K.

Определение 60. 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 33 (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 $f = h_1 h_2$, $\deg h_i \geqslant 1$, $i = 1, 2$. Тогда

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

Но $\deg h_i < \deg f$, а значит мы получили противоречие минимальности f. Поэтому 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 61 (Степень расширения). Пусть $K \subset L$. Рассмотрим L как векторное пространство над полем K. Тогда *степенью расширения* L над K называется размерность размерность векторного пространства L над K.

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

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

Теорема 34. Любое конечное расширение является алгебраичным.

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

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

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

Теорема 35. 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 36 (Структура простых алгебраичных 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 $\{1, \theta, \theta^2, ..., \theta^{n-1}\}$ – 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 $\mathbb{F}_2$:

$$f = x^2 + x + 1, \qquad \theta \text{ – корень}$$

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

$$\begin{aligned} x \cdot x &\equiv x + 1 \pmod{x^2 + x + 1} \\ x(x+1) &\equiv 1 \\ (x+1)(x+1) &\equiv x \end{aligned}$$

Лемма 9. Пусть f – неприводимый многочлен. Тогда $K[x]/(f)$ – поле.

Доказательство. $K[x]/(f) = \{g + (f)\}, \overline{1} = 1 + (f)$ – здесь выполняются все аксиомы поля, кроме одного. Докажем, что $\forall \overline{g}\ \exists (\overline{g})^{-1}$. Рассмотрим $g \notin (f)$. Тогда $\overline{g} \neq 0$. Если g делит f, тогда $g \in (f)$, но это не так. Поэтому $(g, f) = 1 \Rightarrow \exists u, v \in K[x]$. Тогда

$$u \cdot g + v \cdot f = 1 \Rightarrow ug \equiv 1 (\mathrm{mod}\, f)$$

Отсюда $\overline{u} \cdot \overline{g} = 1 \Rightarrow K[x]/(f)$ – поле. □

Теорема 37. Пусть f – неприводимый многочлен. Тогда $K[x]/(f) \simeq K(\theta)$, где θ – некоторый корень f.

3.3. Строение конечных полей

Теорема 38 (Количество элементов конечного поля). Пусть K – конечное поле, $\mathrm{char}\, K = p$. Тогда $|K| = p^n, n \in \mathbb{N}$.

Доказательство. $\mathbb{F}_p \subset K$ – простое подполе K. Рассмотрим K как векторное пространство над $\mathbb{F}_p$, $[K : \mathbb{F}_p] = n$. Тогда $\forall a \in K\ a = \alpha_1 a_1 + ... + \alpha_n a_n$, (a_i) – базис K, $\alpha_1, ..., \alpha_n \in \mathbb{F}_p$. Различных наборов $(\alpha_1, ..., \alpha_n)$ ровно p^n, поэтому $|K| = p^n$. □

Лемма 10. Пусть K – конечное поле, $|K| = q$. Тогда $\forall a \in K\ a^q = a$.

Доказательство. Для нуля очевидно, поэтому будем сразу рассматривать $a \neq 0$, $a^{q-1} = 1$. Если выкинуть 0 из поля K, то получим K^* – мультипликативную группу поля, $|K^*| = q-1$. Поскольку $\forall a \in G$ – конечная группа, $a^{|G|} = 1$, то $a^{q-1} = 1$. □

Лемма 11 (Бином двоечника). Пусть K – конечное поле, $|K| = q$. Тогда $(a+b)^q = a^q + b^q$ и $(a-b)^q = a^q - b^q$.

Доказательство. Докажем по индукции. Если $q = p$, то $(a+b)^p = a^p + \sum_{k=1}^{p-1} C_p^k a^{p-k} b^k + b^p$. Заметим, что $C_p^k = \frac{p\cdot(p-1)\cdot\ldots\cdot 1}{k!(p-k)!} \vdots p \Rightarrow C_p^k \vdots p,\ k = 1, \ldots, p-1$. Поэтому $C_p^k = 0 (\mathrm{mod}\, p)$.
Индукционный переход: пусть верно для $q = p^{n-1}$. Тогда

$$(a+b)^{p^n} = \underbrace{(a+b)^{p^{n-1}} \cdot \ldots \cdot (a+b)^{p^{n-1}}}_{p} = \left(a^{p^{n-1}} + b^{p^{n-1}}\right)^p = a^q + b^q$$

Для разности:

$$a^q = (a-b+b)^q = (a-b)^q + b^q$$

□

Определение 62. Пусть $f \in K[x],\ L \supset K$. Тогда поле L называется *полем разложения* f, если

1. $f = a\prod_i (x - \alpha_i)$ в поле L;
2. $L = K(\alpha_1, \ldots, \alpha_n)$.

Иначе говоря, L – наименьшее поле, в котором f раскладывается на линейные множители.

Пример. Пусть $x^2 + 1 \in \mathbb{R}[x]$. Тогда $\mathbb{R}(i) = \mathbb{C}$.

Пример. Рассмотрим тот же многочлен над полем $\mathbb{Q}: x^2 + 1 \in \mathbb{Q}[x]$. Но тогда $\mathbb{Q}(i) \neq \mathbb{C}$.

Лемма 12. Пусть K – конечное поле, $|K| = q$, $x^q - x \in F[x], F \subset K$. Тогда K – поле разложения $x^q - x$.

Доказательство. У многочлена $x^q - x$ корней $\leqslant q$. Любой элемент поля K по лемме является корнем $x^q - x$. K – наименьшее поле, т.к. $|K| = q$. □

Теорема 39. Для любого $f \in K[x]$ существует единственное (с точностью до изоморфизма) поле разложения.

Теорема 40. 1. $\forall p$ – простого, $\forall n \in \mathbb{N}$ существует конечное поле K такое, что $|K| = p^n$.

2. Любое поле $K : |K| = p^n$ является полем разложения $x^q - x,\ q = p^n$.

Доказательство. 1. Рассмотрим $x^q - x$, $q = p^n$, K – поле разложения $x^q - x$. Положим

$$S = \{a \in K : a^q = a\} \subset K$$

Докажем, что S – поле. Действительно, $\forall a, b \in S$, то $(a \pm b)^q = a^q \pm b^q = a \pm b \Rightarrow a \pm b \in S$. Покажем, что $0, 1 \in S$: $\forall a, b \in S\ (ab)^q = a^q b^q = ab \Rightarrow ab \in S$. Таким образом, S – поле. Поскольку $(x^q - x, qx^{q-1} - 1) = 1$, то $x^q - x$ не имеет кратных корней над $\mathbb{F}_p$. Получается, что S ровно q корней многочлена $x^q - x$, поэтому S – наименьшее поле в котором $x^q - x$ раскладывается на линейные множители $\Rightarrow S = K,\ |S| = q$.

2. Пусть K – конечное поле, $|K| = p^n$. По построению K – поле разложения $x^q - x$, но по теореме поле разложения определено однозначно (с точностью до изоморфизма).

□

Лемма 13. Если $m|n$, то $x^m - 1|x^n - 1$.

Доказательство. $x^n - 1 = x^{md} - 1 = (x^m - 1)\left((x^m)^{d-1} + (x^m)^{d-2} + \ldots + 1\right)$. □

Замечание. Утверждение верно и в другую сторону.

Теорема 41 (Подполя конечного поля). 1. Пусть K – конечное поле, $|K| = p^n$. Если $L \subset K$, то $|L| = p^m,\ m|n$;

2. $|K| = p^n,\ m|n$. Тогда существует единственное подполе $L \subset K : |L| = p^m$

Доказательство. 1. $\operatorname{char} K = p \Rightarrow \exists \mathbb{F}_p : \mathbb{F}_p \subset L \subset K$. По теореме $|L| = p^m$. Так как $[K : L] \cdot [L : \mathbb{F}_p] = [K : \mathbb{F}_p]$, то $m|n$.

2. $m|n$. Значит, $x^m - 1 \mid x^n - 1 \Rightarrow p^m - 1 \mid p^n - 1 \Rightarrow x^{p^m-1} - 1 \mid x^{p^n-1} - 1 \Rightarrow x^{p^m} - x \mid x^{p^n} - x$. K – поле разложения $x^{p^n} - x$ Тогда рассмотрим L – поле разложения $x^{p^m} - x$. Тогда любой корень $x^{p^m} - x$, т.е. элемент L, является корнем $x^{p^n} - x$, т.е. элементом $K \Rightarrow |L| = p^m$. Таким образом, мы построили $L \subset K : |L| = p^m$.
Докажем единственность. Если L_1, L_2 – различные поля с p^m элементами, то $x^{p^m} - x$ имеет больше, чем p^m корней.

□

3.4. Мультпликативная группа поля

Будем рассматривать K – конечное поле и K^* – его мультипликативную группу.

Определение 63. G – конечная группа, $G = \langle a \rangle = \{1, a, \ldots, a^{n-1}\}$ – циклическая группа.

Определение 64. Порядок элемента b – наименьшее $m : b^m = 1$.

Обозначение. $\mathrm{ord}(b) = m$ – порядок b.

Теорема 42. K^* – циклическая.

Доказательство. Пусть $|K^*| = q - 1 = r$. Разложим r на простые множители: $r = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$. $\forall i, 1 \leqslant i \leqslant k$ рассмотрим $x^{r/p_i} - 1$. Он имеет $\frac{r}{p_i} < r$ корней. Значит $\exists a_i, 1 \leqslant i \leqslant k : a_i^{r/p_i} \neq 1,\ a_i \in K^*$.
$\forall i, 1 \leqslant i \leqslant k$ обозначим $b_i = a_i^{r/p_i^{\alpha_i}}$. Докажем, что $\mathrm{ord}(b_i) = p_i^{\alpha_i}$. Пусть $\mathrm{ord}(b_i) = p_i^{\beta_i}$. Так как $b_i^{p_i^{\alpha_i}} = 1$, то $\mathrm{ord}(b_i) \mid p_i^{\alpha_i}$. Но $b_i^{p_i^{\alpha_i - 1}} = a_i^{r/p_i} \neq 1 \Rightarrow \beta_i < \alpha_i$ – не может быть.
Теперь положим $b = b_1 \cdot \ldots \cdot b_k$ и докажем, что $\langle b \rangle = K^*$, т.е. что $\mathrm{ord}(b) = r$. Пусть $\mathrm{ord}(b) \neq r \Rightarrow \mathrm{ord}(b) \mid \frac{r}{p_i}$. Не умаляя общности, можно считать, что $i = 1$. То есть

$$b^{r/p_1} = b_1^{r/p_1} \cdot b_2^{r/p_1} \cdot \ldots \cdot b_k^{r/p_1} = b_1^{r/p_1} = \left(b_1^{r/p_1}\right)^{(\text{какие-то множители})} = 1$$

но это невозможно, т.к. $b_1^{p_1^{\alpha_1}} = 1$. □