Алгебра и Теория чисел

Конспект по 2 семестру специальности «прикладная информатика»

(лектор Г. В. Матвеев)

Содержание

1 Прямая сумма подпространств

Пусть W_1, W_2 — подпространства.

• $W_1 \oplus W_2$ *— сумма называется* ***прямой****, если* $W_1 \cap W_2 = \vec{0}$.

Справедливо и следующее: $W_1 \oplus W_2 \oplus ... \oplus W_k$ называется прямой, если $W_i \cap \sum\limits_{i \neq j} W_j = \vec{0}$

Теорема.

$$\dim(W_1 \oplus W_2) = \dim W_1 + \dim W_2$$

⧫ По теореме о сумме подпространств

$$\dim(W_1 + W_2) = \dim W_1 + \dim W_2 - \dim(W_1 \cap W_2)$$

А так как $W_1 \cap W_2 = \vec{0}$, то $\dim(W_1 \cap W_2) = 0$. ⊠

Следствие.

$$\dim(W_1 \oplus W_2 \oplus \ldots \oplus W_k) = \dim W_1 + \dim W_2 + \ldots + \dim W_k$$

Теорема. *Если* $W \subset V_n \Rightarrow V_n = W \oplus U$*, где* U *— подпространство.*

⧫

1. $W = \vec{0} \Rightarrow U = V_n$, $V_n = \vec{0} \oplus V_n$
2. $W = V_n \Rightarrow U = \vec{0}$, $V_n = V_n + \vec{0}$
   Оба равенства справедливы, так как $\vec{0} \cap V_n = \vec{0}$
3. Рассмотрим нетривиальный случай:

$$W = L(v_1, v_2, ..., v_r), \quad 0 < r < n$$

$$U = L(v_{r+1}, v_{r+2}, ..., v_n)$$

Возьмем произвольный вектор x, не нарушая общности:

$$x = (\alpha_1 v_1 + ... + \alpha_r v_r) + (\alpha_{r+1} v_{r+1} + ... + \alpha_n v_n) \Rightarrow x = W + U$$

Докажем, что $W \cap U = \vec{0}$.
Пусть $x \in W \cap U$.

$$x = \alpha_1 v_1 + ... + \alpha_r v_r = \alpha_{r+1} v_{r+1} + ... + \alpha_n v_n \Rightarrow \forall \alpha_i = 0 \Rightarrow x = 0 \Rightarrow W \cap U = \vec{0}$$

⊠

Следствие. *Каждое пространство раскладывается в прямую сумму* n *одномерных подпространств.*

$$V_n = L(e_1) \oplus L(e_2) \oplus ... \oplus L(e_n)$$

$e_1, e_2, ..., e_n$-базис.
То есть любой вектор раскладываетя по базису:

$$x = \alpha_1 e_1 + \alpha_2 e_2 + ... + \alpha_n e_n$$

2 Критерий совместности системы линейных уравнений

Теорема. *Система линейных алгебраических уравнений совместна тогда и только тогда, когда ранг матрицы коэффицентов равен рангу расширенной матрицы.*

♦ Рассмотрим систему алгебраических уравнений

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

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \text{— матрица коэффицентов } A.$$

$$\left(\begin{array}{cccc|c} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{array}\right) = \widetilde{A} = (A|B) \text{ — расширенная матрица.}$$

Система совместна $\Leftrightarrow \operatorname{rank} A = \operatorname{rank} \widetilde{A}$.
$\Rightarrow$ Пусть система совместна с решением $(j_1, j_2, \dots, j_n)$

$$\begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{n1} \end{pmatrix} \cdot j_1 + \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{n2} \end{pmatrix} \cdot j_2 + \dots + \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{nn} \end{pmatrix} \cdot j_n = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} \tag{1}$$

Это значит, что при добавлении столбца свободных членов базис не изменился, так как новый столбец выражается через старый. Следовательно, $\operatorname{rank} A = \operatorname{rank} \widetilde{A}$.

$\Leftarrow$ Базисный минор матрицы A есть базисный минор матрицы $\widetilde{A}$, так как $rankA = rank\widetilde{A}$.
Следовательно, столбец свободных членов $\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$ выражается через базисные столбцы по принципу (1). Коэффиценты остальных столбцов равны 0. И тогда полученные коэффиценты будут являться решением системы. ⊠

Решение системы линейных алгебраических уравнений с помощью критерия

1. Нахождение базисного минора матрицы A методом окаймления минора.
2. Проверяем условие $\operatorname{rank} A = \operatorname{rank} \widetilde{A}$ методом окаймления миноров.
3. Отбрасываем все небазисные строки.
4. Базисные неизвестные оставляем слева, а свободные переносим вправо.

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1r}x_r = b_1 - a_{1,r+1}x_{r+1} - \dots - a_{1n}x_n \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_{n1}x_1 + a_{n2}x_2 + \dots + a_{nr}x_r = b_n - a_{n,r+1}x_{r+1} - \dots - a_{nn}x_n \end{cases}$$

Полученную систему рассматриваем как крамеровскую.

$$M = \begin{vmatrix} a_{11} & \dots & a_{1r} \\ \dots & \ddots & \dots \\ a_{r1} & \dots & a_{rr} \end{vmatrix} \neq 0$$

$$\begin{cases} x_1 = f_1(x_{r+1}, \dots, x_n) \\ \dots\dots\dots\dots\dots\dots \\ x_r = f_r(x_{r+1}, \dots, x_n) \end{cases}$$

3 Однородные системы линейных уравнений

Рассмотрим однородную систему линейных уравнений

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = 0, \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = 0 \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = 0 \end{cases} \tag{1}$$

Где $A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$ — матрица системы, $X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ — столбец неизвестных.

$$0 = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \text{ — столбец нулей.}$$

Тогда систему (1) можно записать в матричном виде как

$$\mathbf{AX{=}0}$$

Теорема. *Решения однородной системы линейных уравнений образуют векторное пространство, размерность которого* $\dim W = n - r$ *(n — число неизвестных, r — ранг системы,* $r = \operatorname{rank} A = \operatorname{rank}(A|0)$.

⧫ Докажем, что это пространство. Вспомним необходимые критерии:

$$W_1, W_2 \in W \Rightarrow W_1 + W_2 \in W$$

$$W_1 \in W \Rightarrow \lambda W_1 \in W$$

Пусть X_1 — конкретный набор, $X_1 = \begin{pmatrix} x_1\prime \\ x_2\prime \\ \vdots \\ x_n\prime \end{pmatrix}$. Тогда выполняются свойства

$$AX_1 = 0,\ AX_2 = 0 \Rightarrow A(X_1 + X_2) = 0$$

$$AX_1 = 0 \Rightarrow \lambda AX_1 = 0$$

Перенесем свободные неизвестные в системе в левую сторону.

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1r}x_r = b_1 - a_{1,r+1}x_{r+1} - \ldots - a_{1n}x_n \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mr}x_r = b_m - a_{m,r+1}x_{r+1} - \ldots - a_{mn}x_n \end{cases} \tag{3}$$

Базисный минор для этой системы

$$M = \begin{vmatrix} a_{11} & \ldots & a_{1r} \\ \ldots & \ddots & \ldots \\ a_{r1} & \ldots & a_{rr} \end{vmatrix} \neq 0$$

Где неизвестные $x_1, \ldots, x_r$ — базисные, а $x_{r+1}, \ldots, x_n$ — свободные.
Выражаем базисные неизвестные через свободные по правилу Крамера или Гаусса:

$$\begin{cases} x_1 = f_1(x_{r+1}, \ldots, x_n) \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x_r = f_r(x_{r+1}, \ldots, x_n) \end{cases}$$

Найдем базисные решения. Для этого передадим значения

$$\begin{cases} c_1 = (c_{11}, c_{12}, \ldots, c_{1r}, 1, 0, \ldots, 0) \\ c_2 = (c_{21}, c_{22}, \ldots, c_{2r}, 0, 1, \ldots, 0) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ c_{n-r} = (c_{n-r,1}, c_{n-r,2}, \ldots, c_{n-r,r}, 0, 0, \ldots, 1) \end{cases}$$

Переменные, которым были переданы значения 0 и 1, являются базисными. Векторы являются линейно независимыми благодаря этим переменным.

Докажем, что любое решение выражается через базис.

$$(\gamma_1, \ldots, \gamma_r, \gamma_{r+1}, \ldots, \gamma_n) - \gamma_{r+1}c_1 - \ldots - \gamma_n c_{n-r} = (\gamma_1 c_1, \gamma_2 c_2, \ldots, \gamma_n c_{n-r})$$

Значит все решения выражаются через базис. $\boxtimes$

- *Базисные решения ОСЛУ называются* ***фундаментальной системой решений****.*

Решение неоднородной системы через однородную

Будем обозначать $AX = B$ — **неоднородная система**, $AY = 0$ — **однородная система**.

$$\left.\begin{matrix} AX = B \\ AY = 0 \end{matrix}\right\} = A(X + Y) = AX + AY = B + 0 = B$$

1. Разность 2-ух решений неоднородной системы будет решением однородной.
2. Если от решения неоднородной системы отнять фиксированное решение неоднородной системы, то получится решение однородной системы.

$$AX - AX_0 = B - B = 0$$

3. Произвольное решение неоднородной системы можно получить, добавляя к фиксированному решению некоторые решения однородной системы.

4 Линейные преобразования векторных пространств

- *Отображение $\varphi : V \to V$ (само в себя) называется* ***линейным***, *если*

1. *Образ суммы равен сумме образов:*

$$\varphi(a+b) = \varphi(a) + \varphi(b)$$

2. *При умножении вектора на скаляр его образ умножается на этот же скаляр:*

$$\varphi(\lambda a) = \lambda\varphi(a)$$

Если $\varphi : V \to W$, то φ — линейное отображение.

Свойства линейного преобразования:

1. *Образ линейной комбинации равен такой же линейной комбинации образов (под действием линейного преобразования)*

$$\varphi(\lambda_1 a_1 + \lambda_2 a_2 + \dots + \lambda_n a_n = \lambda_1\varphi(a_1) + \lambda_2\varphi(a_2) + \dots + \lambda_n\varphi(a_n)$$

2. *Преобразование $\vec{0}$*

$$\varphi(\vec{0}) = \vec{0}$$

$$\varphi(\vec{0}) = \varphi(\vec{0}\cdot\vec{a}) = 0\cdot\varphi(\vec{a}) = \vec{0}$$

3. *Вынесение минуса*

$$\varphi(-\vec{a}) = -\varphi(\vec{a})$$

4. *Линейное преобразование переводит линейно зависимые векторы в линейно зависимые с такими же скалярами.*

Теорема. *Любое линейное преобразование вполне определяется своими значениями на базисных векторах и эти значения могут быть любыми.*

♦ Пусть $e_1, e_2, \dots, e_n$ — базис, $a_1, a_2, \dots, a_n$ — системы векторов.
Возьмем функцию φ такую, что:

$$\begin{cases} \varphi(e_1) = a_1 \\ \varphi(e_2) = a_2 \\ \dots\dots\dots\dots \\ \varphi(e_n) = a_n \end{cases}$$

Докажем, что такое пространство существует:

$$x = x_1e_1 + x_2e_2 + \dots + x_ne_n$$

$$\varphi(x) = x_1a_1 + x_2a_2 + \dots + x_na_n$$

Докажем, что оно линейное:

$$y = y_1e_1 + y_2e_2 + \dots + y_ne_n$$

- $\varphi(x+y) = (x_1+y_1)a_1+(x_2+y_2)a_2+\ldots+(x_n+y_n)a_n = x_1a_1+y_1a_1+\ldots+x_na_n+y_na_n = (x_1a_1 + x_2a_2 + \ldots + x_na_n) + (y_1a_1 + y_2a_2 + \ldots + y_na_n) = \varphi(x) + \varphi(y)$;
- $\varphi(\lambda x) = \lambda x_1a_1 + \lambda x_2a_2 + \ldots + \lambda x_na_n = \lambda\varphi(x)$.

Докажем, что единственное:
Пусть существует

$$\begin{cases} \psi(e_1) = a_1 \\ \psi(e_2) = a_2 \\ \dots\dots\dots\dots \\ \psi(e_n) = a_n \end{cases}$$

с такими же свойствами. Тогда

$$\psi(x) = \psi(x_1e_1+x_2e_2+\dots+x_ne_n) = x_1\psi(e1)+x_2\psi(e_2)+\dots+x_n\psi(e_n) = x_1a_1+x_2a_2+\dots+x_na_n = \varphi(x)$$

⊠

5 Операции над линейными преобразованиями

Пусть f, φ — линейные преобразования векторного пространства V.

1. **Сумма линейных преобразований:**

$$f(x) + \varphi(x) = (f + \varphi)(x),\ \forall x \in V.$$

♦ $(f + \varphi)(\lambda_1x_1 + \lambda_2x_2) = f(\lambda_1x_1 + \lambda_2x_2) + \varphi(\lambda_1x_1 + \lambda_2x_2) = f(\lambda_1x_1) + f(\lambda_2x_2) + \varphi(\lambda_1x_1) + \varphi(\lambda_2x_2) = \lambda_1f(x_1) + \lambda_2f(x_2) + \lambda_1\varphi(x_1) + \lambda_2\varphi(x_2) = \lambda_1(f(x_1) + \varphi(x_1)) + \lambda_2(f(x_2) + \varphi(x_2)) = \lambda_1(f + \varphi)(x_1) + \lambda_2(f + \varphi)(x_2)$. ⊠

2. **Умножение на скаляр линейного преобразования:**

$$(\lambda f)(x) = \lambda f(x),\ \forall x \in V.$$

♦ $(\lambda f)(\lambda_1x_1 + \lambda_2x_2) = (\lambda f)(\lambda_1x_1) + (\lambda f)(\lambda_2x_2) = \lambda f(\lambda_1x_1) + \lambda f(\lambda_2x_2) = \lambda(f(\lambda_1x_1) + \lambda(f(\lambda_2x_2)) = \lambda f(\lambda_1x_1 + \lambda_2x_2)$. ⊠

3. **Композиция линейных преобразований:**

$$(f \circ \varphi)(x) = f(\varphi(x)),\ \forall x \in V.$$

♦ $(f\varphi)(\lambda_1x_1 + \lambda_2x_2) = f(\varphi(\lambda_1x_1 + \lambda_2x_2)) = f(\varphi(\lambda_1x_1) + \varphi(\lambda_2x_2)) = f)\lambda_1\varphi(x_1) + \lambda_2\varphi(x_2)) = \lambda_1f(\varphi(x_1)) + \lambda_2f(\varphi(x_2)) = \lambda_1(f\varphi)(x_1) + \lambda_2(f\varphi)(x_2)$. ⊠

6 Ядро и образ линейного преобразования

Пусть $\varphi : V \to V$ — линейное преобразование.

• *Множество* $\ker\varphi = \{x \mid \varphi(x) = \vec{0}\}$ — ***ядро*** *линейного преобразования.*
$\dim\ker\varphi$ - **дефект** линейного преобразования (размерность ядра).

• *Множество* $\operatorname{Im}\varphi = \varphi(v) = \{\varphi(x) \mid x \in V\}$ — ***образ*** *линейного преобразования.*
$\dim\operatorname{Im}\varphi$ - **ранг** линейного преобразования (размерность образа).

Пример 1
Рассмотрим функцию $\sin(x)$. Функция синуса не является линейной, в чем легко убедиться ($\sin(a+b) \neq \sin a + \sin b$), однако для нее можно определить ядро и образ. Таким образом

$$\ker(\sin) = \pi n$$

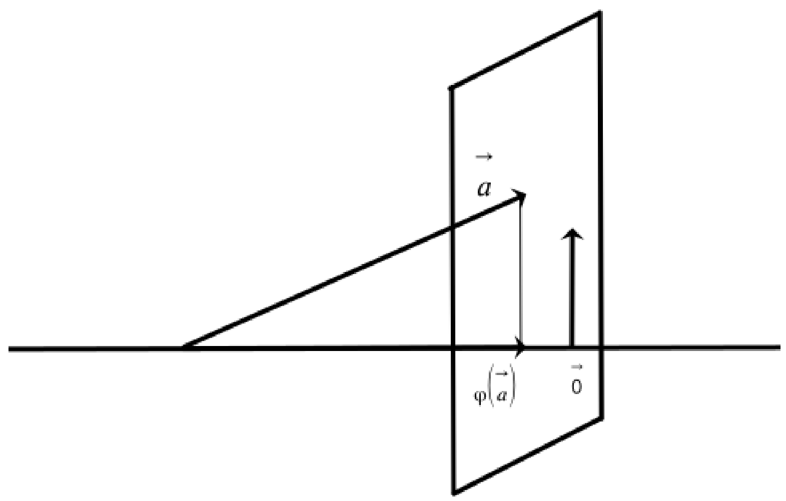
$$\operatorname{Im}(\sin) = [-1, 1]$$

Пример 2
Тождественное преобразование - $\varphi(v) = v \quad \forall v \in V$

$$\ker(\varphi) = \vec{0}$$

$$\operatorname{Im}(\varphi) = V$$

Пример 3
Возьмем прямую l и плоскость P, где $l \perp P$.



$$\varphi(\vec{a}) = \vec{p}ra$$

$$\operatorname{Im}(\varphi) = l = V_1$$

$$\ker(\varphi) = P = V_2$$

Теорема. *Ядро и образ линейного преобразования — подпространства исходного векторного пространства.*

♦ Проверим выполнимость свойств:

1. $w_1, w_2 \in \ker(\varphi) \Rightarrow \varphi(w_1) = \varphi(w_2) = \vec{0}$ $\varphi(w_1 + w_2) = \varphi(w_1) + \varphi(w_2) = \vec{0} + \vec{0} = \vec{0} \Rightarrow$ $w_1 + w_2 \in \ker(\varphi)$
2. $\lambda\varphi(w) = \lambda\vec{0} = \vec{0} \Rightarrow \lambda\varphi \in \ker(\varphi)$
3. $\varphi(w_1), \varphi(w_2) \in \mathrm{Im}(\varphi)$
   $\varphi(w_1) + \varphi(w_2) = \varphi(w_1 + w_2) \in \mathrm{Im}(\varphi)$
4. $\lambda\varphi(w_1) = \varphi(\lambda w_1) \in \mathrm{Im}(\varphi)$

⊠

- *Размерность ядра —* ***дефект****. Будем обозначать* $d = \dim(\ker(\varphi))$.
- *Размерность образа —* ***ранг****. Будем обозначать* $r = \operatorname{rank}\varphi = \dim(\mathrm{Im}(\varphi))$.

Тогда φ — **нулевое преобразование**, если $d = n$, $r = 0$.
φ — **тождественное преобразование**, если $d = 0$, $r = n$.
φ — **проектирование векторов**, если $d = 2$, $r = 1$.

Теорема. *Сумма ранга и дефекта равняется размерности пространства.*

⧫ Рассмотрим образ $\varphi(V)$. Пусть базис $\varphi(V) : \varphi(\varphi(l_1), \varphi(l_2), \ldots, \varphi(l_r))$
Докажем, что
$$V_n = L(l_1, l_2, \ldots, l_r) \oplus \ker(\varphi)$$
$$n = r + d$$

1. $l_1, l_2, \ldots, l_r$ — линейно независимы.
   По свойству линейное преобразование сохраняет зависимость. Если бы $l_1, l_2, \ldots, l_r$ были зависимы, то и $\varphi(l_1), \varphi(l_2), \ldots, \varphi(l_r)$ были бы зависимы, но это базис, значит не зависимы.
2. $\vec{v} \in V_n = \vec{x} \in L(l_1, l_2, \ldots, l_r) + \vec{y} \in ker\varphi$
   $$\varphi(V) = \alpha_1\varphi(l_1) + \alpha_2\varphi(l_2) + dots + \alpha_r\varphi(l_r)$$
   $$\varphi(v - \alpha_1 l_1 - \ldots - \alpha_r l_r) = \vec{0} \Rightarrow v - \alpha_1 l_1 - \ldots - \alpha_r l_r = y \in \ker\varphi$$
   $$v = \alpha_1 l_1 - \ldots - \alpha_r l_r + y = x + y$$
3. $L \cap ker\varphi = \vec{0}$
   Пусть $x \in L \cap \ker\varphi$.
   $x = \alpha_1 l_1 + \ldots + \alpha_r l_r$
   $\varphi(x) = \vec{0}, \quad \varphi(x) = \varphi(\alpha_1 l_1 + \ldots + \alpha_r l_r) = \varphi(\alpha_1 l_1) + \varphi(\alpha_2 l_2) + \ldots + \varphi(\alpha_r l_r) = \alpha_1\varphi(l_1) + \alpha_2\varphi(l_2) + \ldots + \alpha_r\varphi(l_r) = \vec{0} \Rightarrow \alpha_1 = \alpha_2 = \ldots = \alpha_r = 0 \Rightarrow x = \vec{0}$

⊠

7 Матрица линейного преобразования

Пусть V — векторное пространство с базисом $e_1, e_2, \ldots, e_n$.
$$x \in V, \quad x = x_1e_1 + x_2e_2 + \cdots + x_ne_n$$

• Пусть $\varphi : V \to V$ — **линейное преобразование** векторного пространства V. Подействуем этим преобразованием поочередно на все базисные векторы и полученные векторы выразим через базис:

$$\begin{cases} \varphi(e_1) = \alpha_{11}e_1 + \alpha_{21}e_2 + \dots + \alpha_{n1}e_n \\ \varphi(e_2) = \alpha_{12}e_1 + \alpha_{22}e_2 + \dots + \alpha_{n2}e_n \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ \varphi(e_n) = \alpha_{1n}e_1 + \alpha_{2n}e_2 + \dots + \alpha_{nn}e_n \end{cases} \tag{1}$$

Матрица $A = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn} \end{pmatrix}$ — матрица линейного преобразования φ.

• Столбцами матрицы линейного преобразования являются координаты образов базисных векторов.

Рассмотрим пример:
На вектор $x = x_1e_1 + x_2e_2 + \dots + x_ne_n$ подействуем линейным преобразованием.

$$\varphi(x) = x_1\varphi(e_1) + x_2\varphi(e_2) + \ldots + x_n\varphi(e_n),$$

где $\varphi(e_1), \varphi(e_2), \ldots, \varphi(e_n)$ — столбцы матрицы A.
Тогда систему (1) можно переписать следующим образом:
Пусть $e = (e_1, e_2, \ldots, e_n)$, тогда

$$(e_1, e_2, \ldots, e_n)A = (\varphi(e_1), \varphi(e_2), \ldots, \varphi(e_n))$$

$$\varphi(e) = eA$$

Вектор x запишем как $x = eX$, где $X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$. Тогда линейное преобразование вектора x примет вид:

$$\varphi(x) = \varphi(e)X$$

$$\varphi(x) = eAX$$

Это говорит о том, что $X \xrightarrow{\varphi} AX \sim \varphi(X) = AX$.

Теорема.

1. *При сложении линейных преобразований их матрицы в данном базисе складываются.*

2. *При умножении линейных преобразований их матрицы в данном базисе умножаются.*

3. *При умножении линейного преобразования на скаляр его матрица умножается на тот же скаляр.*

♦ Пусть V — векторное пространство с базисом $e_1, e_2, \ldots, e_n$.
И пусть f, φ — линейные преобразования.
Подействовав этими линейными преобразованиями на базис V получим следующие системы:

$$\begin{cases} f(e_1) = \alpha_{11}e_1 + \alpha_{21}e_2 + \cdots + \alpha_{n1}e_n \\ f(e_2) = \alpha_{12}e_1 + \alpha_{22}e_2 + \cdots + \alpha_{n2}e_n \\ \dotfill \\ f(e_n) = \alpha_{1n}e_1 + \alpha_{2n}e_2 + \cdots + \alpha_{nn}e_n \end{cases} \tag{1}$$

$$\begin{cases} \varphi(e_1) = \beta_{11}e_1 + \beta_{21}e_2 + \cdots + \beta_{n1}e_n \\ \varphi(e_2) = \beta_{12}e_1 + \beta_{22}e_2 + \cdots + \beta_{n2}e_n \\ \dotfill \\ \varphi(e_n) = \beta_{1n}e_1 + \beta_{2n}e_2 + \cdots + \beta_{nn}e_n \end{cases} \tag{2}$$

Запишем матрицы линейных преобразований для f, φ:

$$A = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \ldots & \alpha_{nn} \end{pmatrix} \text{ — матрица линейного преобразования } f.$$

$$B = \begin{pmatrix} \beta_{11} & \beta_{12} & \ldots & \beta_{1n} \\ \beta_{21} & \beta_{22} & \ldots & \beta_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{n1} & \beta_{n2} & \ldots & \beta_{nn} \end{pmatrix} \text{ — матрица линейного преобразования } \varphi.$$

1. Сложим почленно строки систем (1) и (2).

$$\begin{cases} f(e_1) + \varphi(e_1) = (\alpha_{11} + \beta_{11})e_1 + (\alpha_{21} + \beta_{21})e_2 + \cdots + (\alpha_{n1} + \beta_{n1})e_n \\ f(e_2) + \varphi(e_2) = (\alpha_{12} + \beta_{12})e_1 + (\alpha_{22} + \beta_{22})e_2 + \cdots + (\alpha_{n2} + \beta_{n2})e_n \\ \dotfill \\ f(e_n) + \varphi(e_n) = (\alpha_{1n} + \beta_{1n})e_1 + (\alpha_{2n} + \beta_{2n})e_2 + \cdots + (\alpha_{nn} + \beta_{nn})e_n \end{cases}$$

   Отсюда получим матрицу линейного преобразования $f + \varphi$:

$$\begin{pmatrix} \alpha_{11} + \beta_{11} & \alpha_{12} + \beta_{12} & \ldots & \alpha_{1n} + \beta_{1n} \\ \alpha_{21} + \beta_{21} & \alpha_{22} + \beta_{22} & \ldots & \alpha_{2n} + \beta_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} + \beta_{n1} & \alpha_{n2} + \beta_{n2} & \ldots & \alpha_{nn} + \beta_{nn} \end{pmatrix} = A + B$$

2. Будем рассматривать умножение линейных преобразований как компзицию отображений $\varphi(f(e))$. Подействуем линейным преобразованием f на базисные векторы:

$$\begin{cases} f(e_1) = \alpha_{11}e_1 + \alpha_{21}e_2 + \cdots + \alpha_{n1}e_n \\ f(e_2) = \alpha_{12}e_1 + \alpha_{22}e_2 + \cdots + \alpha_{n2}e_n \\ \dotfill \\ f(e_n) = \alpha_{1n}e_1 + \alpha_{2n}e_2 + \cdots + \alpha_{nn}e_n \end{cases} \tag{1}$$

На полученные векторы подействуем линейным преобразованием φ:

$$\begin{cases} \varphi(f(e_1)) = \beta_{11}f(e_1) + \beta_{21}f(e_2) + \dots + \beta_{n1}f(e_n) \\ \varphi(f(e_2)) = \beta_{12}f(e_2) + \beta_{22}f(e_2) + \dots + \beta_{n2}f(e_n) \\ \varphi(f(e_n)) = \beta_{1n}f(e_1) + \beta_{2n}f(e_2) + \dots + \beta_{nn}f(e_n) \end{cases}$$

Подставим в полученную систему уравнения системы (1):

$$\begin{cases} \varphi(f(e_1)) = \beta_{11}(\alpha_{11}e_1 + \alpha_{21}e_2 + \dots + \alpha_{n1}e_n) + \beta_{21}(\alpha_{12}e_1 + \alpha_{22}e_2 + \dots + \alpha_{n2}e_n) + \dots \\ \varphi(f(e_2)) = \beta_{12}(\alpha_{11}e_1 + \alpha_{21}e_2 + \dots + \alpha_{n1}e_n) + \beta_{22}(\alpha_{12}e_1 + \alpha_{22}e_2 + \dots + \alpha_{n2}e_n) + \dots \\ \varphi(f(e_n)) = \beta_{1n}(\alpha_{11}e_1 + \alpha_{21}e_2 + \dots + \alpha_{n1}e_n) + \beta_{2n}(\alpha_{12}e_1 + \alpha_{22}e_2 + \dots + \alpha_{n2}e_n) + \dots \end{cases}$$

Раскроем скобки:

$$\begin{cases} \varphi(f(e_1)) = \beta_{11}\alpha_{11}e_1 + \beta_{11}\alpha_{21}e_2 + \dots + \beta_{11}\alpha_{n1}e_n + \beta_{21}\alpha_{12}e_1 + \beta_{21}\alpha_{22}e_2 + \dots + \beta_{21}\alpha_{n2}e_n + \dots \\ \varphi(f(e_2)) = \beta_{12}\alpha_{11}e_1 + \beta_{12}\alpha_{21}e_2 + \dots + \beta_{12}\alpha_{n1}e_n + \beta_{22}\alpha_{12}e_1 + \beta_{22}\alpha_{22}e_2 + \dots + \beta_{22}\alpha_{n2}e_n + \dots \\ \varphi(f(e_n)) = \beta_{1n}\alpha_{11}e_1 + \beta_{1n}\alpha_{21}e_2 + \dots + \beta_{1n}\alpha_{n1}e_n + \beta_{2n}\alpha_{12}e_1 + \beta_{2n}\alpha_{22}e_2 + \dots + \beta_{2n}\alpha_{n2}e_n + \dots \end{cases}$$

Сгрупируем подобные слагаемые:

$$\begin{cases} \varphi(f(e_1)) = (\beta_{11}\alpha_{11} + \beta_{21}\alpha_{12} + \dots)e_1 + (\beta_{11}\alpha_{21} + \beta_{21}\alpha_{22} + \dots)e_2 + \dots \\ \varphi(f(e_2)) = (\beta_{12}\alpha_{11} + \beta_{22}\alpha_{12} + \dots)e_1 + (\beta_{12}\alpha_{21} + \beta_{22}\alpha_{22} + \dots)e_2 + \dots \\ \varphi(f(e_n)) = (\beta_{1n}\alpha_{11} + \beta_{2n}\alpha_{12} + \dots)e_1 + (\beta_{1n}\alpha_{21} + \beta_{2n}\alpha_{22} + \dots)e_2 + \dots \end{cases}$$

Запишем координаты векторов в матрицу линейного преобразования:

$$\begin{pmatrix} \beta_{11}\alpha_{11} + \beta_{21}\alpha_{12} + \dots & \beta_{12}\alpha_{11} + \beta_{22}\alpha_{12} + \dots & \dots & \beta_{1n}\alpha_{11} + \beta_{2n}\alpha_{12} + \dots \\ \beta_{11}\alpha_{21} + \beta_{21}\alpha_{22} + \dots & \beta_{12}\alpha_{21} + \beta_{22}\alpha_{22} + \dots & \dots & \beta_{2n}\alpha_{21} + \beta_{2n}\alpha_{22} + \dots \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{11}\alpha_{n1} + \beta_{21}\alpha_{n2} + \dots & \beta_{12}\alpha_{n1} + \beta_{22}\alpha_{n2} + \dots & \dots & \beta_{1n}\alpha_{n1} + \beta_{2n}\alpha_{n2} + \dots \end{pmatrix} = A \cdot B$$

3. Умножим каждую строку системы (1) на произвольный скаляр γ:

$$\begin{cases} \gamma f(e_1) = \gamma\alpha_{11}e_1 + \gamma\alpha_{21}e_2 + \dots + \gamma\alpha_{n1}e_n \\ \gamma f(e_2) = \gamma\alpha_{12}e_1 + \gamma\alpha_{22}e_2 + \dots + \gamma\alpha_{n2}e_n \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ \gamma f(e_n) = \gamma\alpha_{1n}e_1 + \gamma\alpha_{2n}e_2 + \dots + \gamma\alpha_{nn}e_n \end{cases}$$

Получаем матрицу линейного преобразования γf:

$$\begin{pmatrix} \gamma\alpha_{11} & \gamma\alpha_{12} & \dots & \gamma\alpha_{1n} \\ \gamma\alpha_{21} & \gamma\alpha_{22} & \dots & \gamma\alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma\alpha_{n1} & \gamma\alpha_{n2} & \dots & \gamma\alpha_{nn} \end{pmatrix} = \gamma A$$

⊠

Теорема. *Ранг линейного преобразования равен рангу его матрицы.*

⧫

$$\operatorname{rank}\varphi = \dim\varphi(V)$$

Так как образ есть *линейная оболочка* $L(\varphi(e_1), \varphi(e_2), \ldots, \varphi(e_n))$, то

$$\dim \varphi(V) = \dim L(\varphi(e_1), \varphi(e_2), \ldots, \varphi(e_n)) = \operatorname{rank}(\varphi(e_1), \varphi(e_2), \ldots, \varphi(e_n)) = \operatorname{rank} A$$

$$\operatorname{rank} \varphi = \operatorname{rank} A$$

⊠

Пример 1
$\varphi(x) = \vec{0}, \quad \forall x$ — нулевое преобразование.

$$\begin{cases} \varphi(e_1) = 0e_1 + 0e_2 + \cdots + 0e_n \\ \varphi(e_2) = 0e_1 + 0e_2 + \cdots + 0e_n \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \varphi(e_n) = 0e_1 + 0e_2 + \cdots + 0e_n \end{cases}$$

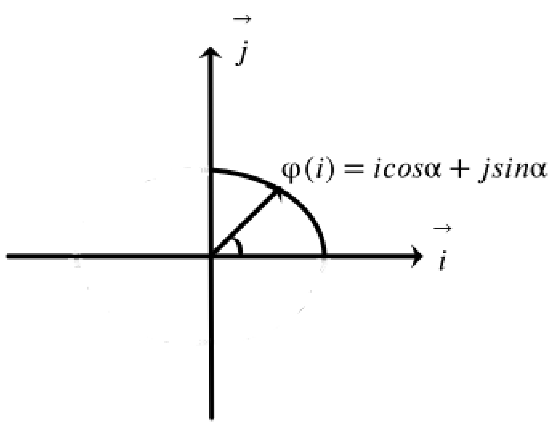
$$A = \begin{pmatrix} 0 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 \end{pmatrix} \text{ — матрица нулевого преобразования.}$$

Пример 2
$\varphi(x) = x, \quad \forall x$ — тождественное преобразование.

$$\begin{cases} \varphi(e_1) = 1e_1 + 0e_2 + \cdots + 0e_n \\ \varphi(e_2) = 0e_1 + 1e_2 + \cdots + 0e_n \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \varphi(e_n) = 0e_1 + 0e_2 + \cdots + 1e_n \end{cases}$$

$$A = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix} \text{ — матрица тождественного преобразования.}$$

Пример 3



$$A = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$$ — матрица угла поворота системы координат на угол α.

• *Биективное (взаимооднозначное) линейное преобразование называется* ***автоморфизмом.***

Если $\varphi : V \to V$ — линейное преобразование, то φ — автоморфизм $\Leftrightarrow$ φ — биекция.

Теорема. *Линейное преобразование* φ *— автоморфизм* $\Leftrightarrow$ *его матрица невырожденная.*

♦

$$\varphi(X) = AX$$

$\Rightarrow$ Предположим, что $|A| = 0$ (т.е. матрица вырожденная).
Тогда $AX = 0 \Rightarrow$ система уравнений линейного преобразования имеет несколько решений и ноль имеет несколько прообразов, чего быть не может.

$\Leftarrow$ Имеем, что $|A| \neq 0$ (т.е. матрица невырожденная).
Значит для $AX = B$ имеется только одно решение по правилу Крамера $\Rightarrow$ φ — биекция.
⊠

8 Подобные матрицы

Для определения подобия матриц рассмотрим задачу.

Задача
Пусть u, v — некоторые базисы, φ — линейное преобразование. Применим его к обоим базисам:

$$\varphi(u) = \varphi(u_1), \varphi(u_2), \ldots, \varphi(u_n) = (u_1, u_2, \ldots, u_n)A$$

Запишем полученные преобразования в матричном виде:

$$\varphi(u) = uA$$

$$\varphi(v) = vB$$

Пусть S — матрица перехода от базиса u к базису v ($|S| \neq 0$ — матрица невырожденная), то есть $v = uS$.
Найти: связь между матрицами A и B.
Решение:
Подействуем линейным преобразованием φ на $v = uS$:

$$\varphi(v) = \varphi(u)S$$

Подставим в это равенство значение $\varphi(u)$, полученное выше:

$$\varphi(v) = uAS \tag{1}$$

Так как $\varphi(v) = vB$ и $v = uS$, то, подставив значение v в первое уравнение, получим:

$$\varphi(v) = uSB \tag{2}$$

Приравняем правые части уравнений (1) и (2):

$$uAS = uSB$$

$$u(SB - AS) = (\vec{0}, \vec{0}, \dots, \vec{0})$$

Так как векторы $u_1, u_2, \dots, u_n$ линейно независимы как базис и их линейные комбинации равны $\vec{0}$, то элементы матрицы $SB - AS$ равны 0 $\Rightarrow SB = AS \Rightarrow B = S^{-1}AS$.

• Матрицы A и B, связанные соотношением $B = S^{-1}AS$, называются **подобными**.

• Матрицы одного и того же преобразования в разных базисах **подобны**.

• Если для матриц A и B справедливо равенство $B = S^{-1}AS$, то можно найти линейное преобразование и базисы, которые будут иметь эти матрицы.

Теорема. *Две квадратных матрицы одного и того же порядка являются матрицами одного и того же преобразования $\Leftrightarrow$ они подобны.*

Свойства подобных матриц

1. *Всякая матрица подобна самой себе:*
$$A = E^{-1}AE$$

2. *Подобие матриц транзитивно:*
Возьмем матрицы A, B, C, связанные соотношением:
$$C = T^{-1}BT$$
$$B = S^{-1}AS$$
Подставим значение B:
$$C = T^{-1}S^{-1}AST$$
Используя свойство обратных матриц
$$T^{-1}S^{-1} = (ST)^{-1}$$
и подставя полученное значение в предыдущее равенство, получаем:
$$C = (ST)^{-1}A(ST)$$

3. *Подобие матриц симметрично:*
$$A = T^{-1}BT \Leftrightarrow B = S^{-1}AS$$
Рассмотрим равенство $B = S^{-1}AS$. Домножим левую и правую часть на S^{-1} и S:
$$A = SBS^{-1}$$
Пусть $T = S^{-1} \Rightarrow T^{-1} = S$. Подставим это в равенство и получим:
$$A = T^{-1}BT$$
То есть если матрица B подобна матрице A, то мы можем найти такую матрицу T, чтобы матрица A была подобна матрице B.

4. *Определители подобных матриц равны:*
$$|B| = |S^{-1}AS| = |S^{-1}| \cdot |A| \cdot |S| = |A| \cdot |S| \cdot |S^{-1}| = |A| \cdot |SS^{-1}| = |A| \cdot |E| = |A| \cdot 1 = |A|$$

5. *Ранги подобных матриц равны:*
$$B = S^{-1}AS \Rightarrow \operatorname{rank} A = \operatorname{rank} B = \operatorname{rank} f$$
Это объясняется тем, что ранг преобразования равен рангу матрицы:
$$\operatorname{rank} A = \operatorname{rank} f, \quad \operatorname{rank} B = \operatorname{rank} f \Rightarrow \operatorname{rank} A = \operatorname{rank} B$$

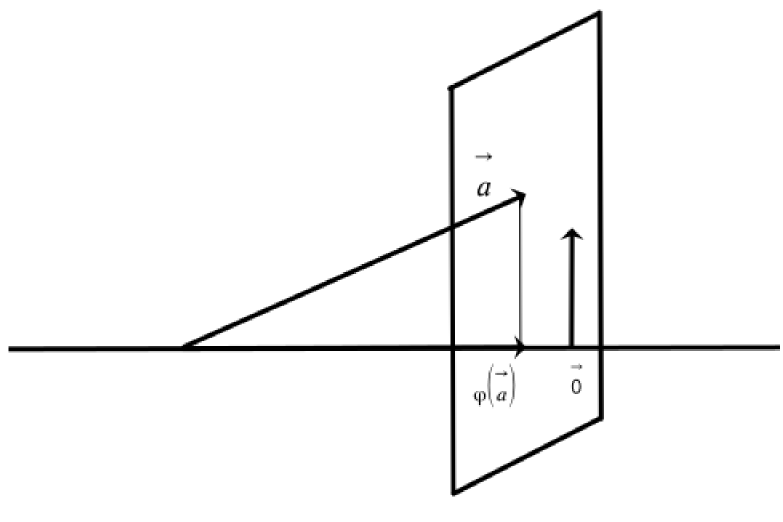
9 Инвариантные подпространства

Пусть $\varphi : V \to V$ — преобразование векторного пространства, W – подпространство.
W называется **инвариантным**, если $\varphi(W) \subset W$.

Примеры

1. $\varphi(V) = V,\ \varphi = e$ — все подпространства инвариантны.
2. $W = \vec{0},\ \varphi(\vec{0}) = \vec{0}$ — нулевое подпространство всегда инвариантно.
3. $W = V$ — само пространство инвариантно.
4. $\varphi(W) = 0 \in W,\ \varphi = 0$ — нулевое преобразование.
   Все подпространства инвариантны.
5. $\varphi = \lambda e$ — скалярное преобразование.
   Все подпространства инвариантны.
6. Проектирование в 3-х мерном пространстве на прямую:

$$\varphi = \text{пр}_l\, P$$



Инвариантные подпространства:

- Все векторы прямой;
- Векторы, перпендикулярные плоскости.

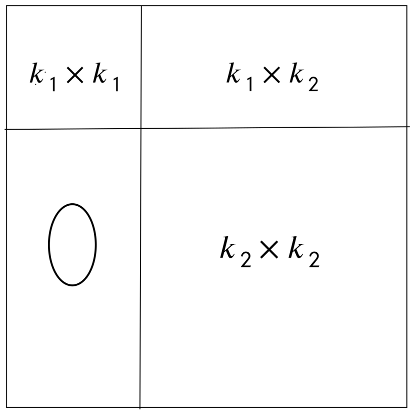
Теорема. *Сумма и пересечение инвариантных пространств инвариантны.*

♦ Пусть $x = W_1 \cap W_2$.
Так как W_1 — инвариантно, то $\varphi(x) \in W_1$, аналогично для W_2.
Так как $\varphi(x) \in W_1$ и $\varphi(x) \in W_2$, то $\varphi(x) \in W_1 \cap W_2 \Rightarrow W_1 \cap W_2$ — инвариантно.

Пусть $x \in W_1 + W_2 \Rightarrow x \in W_1$ или $x \in W_2$.
Так как W_1 и W_2 — инвариантны, то $\varphi(x) \in W_1$ или $\varphi(x) \in W_2 \Rightarrow \varphi(x) \in W_1 + W_2 \Rightarrow$

$W_1 + W_2$ — инвариантно. $\boxtimes$

• Матрица называется **полураспавшейся**, если она имеет вид



где $k_1 + k_2 = n,\ k_1, k_2 > 0$.

Теорема. *У данного преобразования имеется нетривиальное инвариантное подпространство $\Leftrightarrow$ его матрица в некотором базисе **полураспавшаяся**.*

♦ Пусть линейное преобразование φ имеет имеет инвариантное подпространство:

$$\varphi(W) \subset W$$

$\Rightarrow$ Возьмем базис подпространства $w_1, w_2, \dots, w_{k1}$ и дополним его до базиса пространства:

$$w_1, w_2, \dots, w_{k1}, v_1, v_2, \dots, v_{k2}$$

Посчитаем матрицу линейного преобразования в новом базисе:

$$\varphi(w_1) \in W,\ \varphi(w_1) = \alpha_{11}w_1 + \alpha_{21}w_2 + \dots + \alpha_{k+1\ 1}w_{k1} + 0v_1 + \dots + 0v_{k2} \tag{1}$$

$\Leftarrow$ Если для линейного преобразования существует полураспавшаяся матрица, то выполнется разложение (1). А значит

$$\begin{cases} \varphi(w_1) \in L(w_1, w_2, \dots, w_{k1}) \\ \varphi(w_2) \in L(w_1, w_2, \dots, w_{k1}) \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots \\ \varphi(w_{k1}) \in L(w_1, w_2, \dots, w_{k1}) \end{cases}$$

Отсюда следует, что L — инвариантно.

Рассмотрим произвольный вектор w:

$$w = \alpha_1 w_1 + \alpha_2 w_2 + \dots + \alpha_{k1} w_{k1}$$

$$\varphi(w) = \alpha_1\varphi(w_1) + \alpha_2\varphi(w_2) + \dots + \alpha_{k1}\varphi(w_{k1})$$

Так как $\varphi(w_i) \in L$ то и $\varphi(w) \in L$. $\boxtimes$

Замечание. Инвариантность подпространства достаточно проверять только на базисных векторах.

10 Характеристическая матрица и характеристический многочлен

Пусть A — квадратная матрица.
• Характеристическая матрица матрицы A имеет вид:

$$xE - A$$

• Характеристическим многочленом называется определитель характеристической матрицы:

$$|xE - A|$$

Примеры.

1. $A = E$ — единичная матрица.

$$(xE - E) = \begin{pmatrix} x-1 & 0 & \dots & 0 \\ 0 & x-1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & x-1 \end{pmatrix}, \quad |xE - E| = (x-1)^n$$

2. $A = 0$ — нулевая матрица.

$$xE - 0 = xE = \begin{pmatrix} x & 0 & \dots & 0 \\ 0 & x & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & x \end{pmatrix}, \quad |xE - 0| = x^n$$

• **Следом** линейного преобразования называется выражение

$$\operatorname{tr} \varphi = \operatorname{tr} A = \sum_{i=1}^{n} a_{ii}$$

где $A = (a_{ij})$ — матрица линейного преобразования φ.

Свойства характеристических матрицы и многочлена:

1. • *Характеристическая матрица всегда невырожденная.*
   • *Характеристический многочлен всегда* $\neq 0$.
   • *Степень многочлена равна* n *— порядок матрицы.*
2. $f(x) = \begin{vmatrix} x-a_{11} & -a_{12} & \dots & -a_{1n} \\ -a_{21} & x-a_{22} & \dots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & a_{n2} & \dots & x-a_{nn} \end{vmatrix} = x^n - (a_{11} + a_{22} + \dots + a_{nn})x^{n-1} + \dots$
3. $f(0) = (-1)^n \cdot |A|$ — свободный член.
4. *Матрица будет вырожденной* $\Leftrightarrow$ 0 *является корнем ее многочлена.*

   ♦ $f(0) = |-A| = 0$ ⊠

5. *Характеристические многочлены подобных матриц равны.*

   ♦ Пусть $B = S^{-1}AS$
   $|xE-B| = |xE-S^{-1}AS| = |S^{-1}xES-S^{-1}AS| = |S^{-1}(xE-A)S| = |S^{-1}|\cdot|xE-A|\cdot|S| = |S^{-1}|\cdot|S|\cdot|xE-A| = |S\cdot S^{-1}|\cdot|xE-A| = |E|\cdot|xE-A| = |xE-A|$ ⊠

6. *Характеристический многочлен полураспавшейся (распавшейся) матрицы равен произведению характеристических многочленов ее диагональных блоков.*

$$\begin{pmatrix} A_1 & C \\ 0 & A_2 \end{pmatrix}, \quad \begin{vmatrix} xE_{n1} - A_1 & -C \\ 0 & xE_{n2} - A_2 \end{vmatrix} = |xE_{n1} - A_1| \cdot |xE_{n2} - A_2|$$

11 Собственные векторы и собственные значения линейного преобразования

Пусть φ — линейное преобразование пространства V_n.
• $\vec{x} \neq 0$ — **собственный вектор** линейного преобразования φ, отвечающий собственному значению λ:

$$\varphi(x) = \lambda x$$

Примеры

1. $\varphi(v) = v$ — тождественное преобразование.
   Все векторы собственные, отвечают значению 1.

$$\varphi(v) = 1 \cdot v$$

2. $\varphi(v) = \vec{0}$ — нулевое преобразование.
   Все векторы собственные, отвечают значению 0.

$$\varphi(v) = \vec{0} = 0 \cdot v$$

3. Проектирование
   Векторы прямой: $\varphi(\vec{a}) = 1 \cdot \vec{a}$ — отвечают значению 1.
   Векторы перпендикулярной плоскости: $\varphi(\vec{a}) = \vec{0} = 0 \cdot \vec{a}$ — отвечают значению 0.

$$X \xrightarrow{\varphi} AX$$

$$AX = \lambda X$$

$$AX = \lambda EA$$

$$(A - \lambda E)X = 0 \sim (A - \lambda E|0)$$

То есть решения ОСЛУ образуют векторное пространство.

$$\varphi(x) = \lambda x \sim (\varphi - \lambda e)x = \vec{0}$$

Образует инвариантное подпространство.

Теорема. *Собственные значения линейного преобразования — это корни характеристического многочлена (характеристические числа, принадлежащие основному полю).*

♦ По определению $\varphi(x) = \lambda x$. Запишем условие существования собственного вектора в виде:

$$(\varphi - \lambda E)x = \vec{0}$$

Так как $\vec{x} \neq 0$ по определению, то преобразование $\varphi - \lambda e$ должно быть вырожденным:

$$\det(\varphi - \lambda e) = 0 \tag{1}$$

Пусть в каком-нибудь базисе преобразование φ имеет матрицу A, тогда преобразование $\varphi - \lambda e$ будет иметь матрицу $A - \lambda E$.
Тогда условие (1) можно записать в следующем виде:

$$\det(A - \lambda E) = \begin{vmatrix} a_{11} - \lambda & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} - \lambda & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} - \lambda \end{vmatrix} = 0$$

А $\det(A - \lambda E)$ — характеристический многочлен, корнями которого являются собственные значения λ. ⊠ Собственные векторы, отвечающие найденным собственным значениям, и нулевой вектор образуют инвариантное подпространство $\ker(\varphi - \lambda e)$, и их можно найти, решая ОСЛУ $(A - \lambda E|0)$ и отбрасывая 0.

Теорема. *Собственные векторы, отвечающие попарно различным собственным значениям, линейно независимы.*

♦ Пусть $\lambda_1, \lambda_2, \dots, \lambda_k,\ \lambda_i \neq \lambda_j,\ i \neq j$ — некоторые собственные значения.
$\varphi(x_i) = \lambda_i x_i,\ i = 1, 2, \dots, k$ — собственные векторы. Докажем теорему методом от противного.
Предположим, что векторы линейно зависимы. Следовательно, один вектор линейно выражается через все остальные, которые будут линейно независимы:

$$x_k = \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_{k-1} x_{k-1} \tag{2}$$

где $x_1, x_2, \dots, x_{k-1}$ — линейно независимы. Подействуем на обе части уравнения (2) линейным преобразованием φ:

$$\lambda_k x_k = \alpha_1 \lambda_1 x_1 + \alpha_2 \lambda_2 x_2 + \dots + \alpha_{k-1} \lambda_{k-1} x_{k-1} \tag{3}$$

Умножим обе части уравнения (2) на λ_k:

$$\lambda_k x_k = \alpha_1 \lambda_k x_1 + \alpha_2 \lambda_k x_2 + \dots + \alpha_{k-1} \lambda_k x_{k-1} \tag{4}$$

Вычтем из уравнения (3) уравнение (4):

$$\alpha_1(\lambda_1 - \lambda_k)x_1 + \alpha_2(\lambda_2 - \lambda_k)x_2 + \dots + \alpha_{k-1}(\lambda_{k-1} - \lambda_k)x_{k-1} = \vec{0}$$

Так как векторы x_i линейно независимы, то $\alpha_i(\lambda_i - \lambda_k) = 0,\ i = 1, 2, \dots, k-1$.
Так как вектор $x_k \neq 0$, то $\alpha_i \neq 0$ одновременно. Положим, что $\alpha_1 \neq 0$.
Так как $\alpha_1 \neq 0,\ \lambda_k \neq \lambda_i \Rightarrow \alpha_i(\lambda_1 - \lambda_k) \neq 0$.
Полученное противоречие доказывает наше утверждение. ⊠

Теорема. *Если у преобразования φ пространства V_n имеется n попарно различных собственных значений, то для него существует базис, состоящий из собственных векторов, отвечающих этим значениям, и его матрица в этом базисе будет диагональной.*

♦ Пусть $\lambda_1, \lambda_2, \dots, \lambda_n,\ \lambda_i \neq \lambda_j,\ i \neq j$ — собственные значения.
$v_1, v_2, \dots, v_n$ — векторы, отвечающие данным значениям.
Разложим эти векторы:

$$\begin{cases} \varphi(v_1) = \lambda_1 v_1 + 0v_2 + \dots + 0v_n \\ \varphi(v_2) = 0v_1 + \lambda_2 v_2 + \dots + 0v_n \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ \varphi(v_n) = 0v_1 + 0v_2 + \dots + \lambda_n v_n \end{cases}$$

Тогда матрица преобразования имеет вид:

$$\begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$$

⊠

Следствие. *Если у квадратной матрицы имеется n попарно различных характеристических чисел, то эта матрица подобна диагональной.*

12 Основные свойства делимости в кольце целых чисел

$\mathbb{N} = \{1, 2, \dots\}$
$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$

• Говорят, что a делит b $(a|b)$, когда $a \neq 0$ и $\exists q :\ b = aq$.

Свойства делимости:

1. $b|a,\ b|c \Rightarrow b|a \pm c$

   ♦ $a = bq_1$
   $c = bq_2$
   $a \pm c = b(q_1 \pm q_2)$ ⊠

2. $b|a \Rightarrow b|ac$

   ♦ $a = bq_1$
   $ac = bq_1 c$ ⊠

3. $a|b,\ b|a \Leftrightarrow a = \pm b$

   ♦ $b = aq_1$
   $a = bq_2$
   $b = bq_2 q_1$
   $1 = q_1 q_2 \Leftrightarrow \left[\begin{array}{l} q_2 = q_1 = -1 \\ q_2 = q_1 = 1 \end{array}\right.$ ⊠

4. $b|a \Rightarrow (a, b) = b$

Теорема. *Всякое число a представимо единственным образом через положительное b в виде*

$$a = bq + r, \quad 0 \leq r < b$$

♦ Возьмем наибольшее q с условием, что $bq \le a$.
Тогда $r = a - bq \Rightarrow r$ удовлетворяет условию $0 \le r < b$.
Покажем однозначность:

$$a = bq + r$$
$$a = bq_1 + r_1$$

Вычтем из одного равенства другое:

$$b(q - q_1) = r_1 - r$$

Очевидно, что $r_1 - r < b$. Пусть тогда $r_1 > r$. Тогда $q - q_1 > 0 \Rightarrow$ равенство невозможно $\Rightarrow r = r_1 \Rightarrow r_1 - r = 0$.
А так как $b \neq 0$, то $q - q_1 = 0 \Rightarrow q = q_1$. ⊠

12.1 НОД

• **НОД** — наибольший общий делитель 2 чисел, обозначается (a, b).

Свойства НОДа:

1. Для $(0, 0)$ НОД не существует.
2. $(a, 0) = a,\ a \neq 0$.
3. Знак не влияет на делимость.
4. $a = bq + r \Rightarrow (a, b) = (b, r)$
   ♦ Если $d|a$ и $d|b \Rightarrow d|r$.
   Если $d|r$ и $d|b \Rightarrow d|a$. ⊠

12.2 Алгоритм Евклида

1. *Большее из чисел поделить с остатком на меньшее:*
$$a = bq_1 + r_1$$
2. *Делитель делим с остатком на остаток r_1:*
$$b = r_1 q_2 + r_2$$
3. *Продолжаем до тех пор, пока не получим первый нулевой остаток. Последний, отличный от 0 остаток, будет НОДом.*
$$r_1 = r_2 q_3 + r_3$$
$$r_{n-1} = r_n q_{n+1} + r_{n+1}$$
$$r_n = r_{n+1} q_{n+2}$$
$$(a, b) = r_{n+1}$$

♦
$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = r_{n+1}$$
⊠

12.3 Расширенный алгоритм Евклида

Под расширенным алгоритмом Евклида, или линейным разложением НОДа, понимается представление НОДа в виде:

$$d = au + bv$$

13 Взаимно простые числа

• Числа a, b называются **взаимно простыми**, если их НОД равен 1, то есть

$$(a, b) = 1$$

Теорема. ***Критерий взаимной простоты***

$$(a, b) = 1 \Leftrightarrow \exists u, v \ au + bv = 1$$

.

♦ $\Rightarrow$ По расширенному алгоритму Евклида $d = au + bv$.
Так как $(a, b) = 1$, то $1 = au + bv$.

$\Leftarrow$ Всякий делитель a и b будет делителем 1. ⊠

Свойства взаимно простых чисел

1. $a|bc$, $(a, b) = 1 \Rightarrow a|c$

   ♦

   $$au + bv = 1$$

   Умножим обе части равенства на c.

   $$acu + bcv = c$$

   Так как $a|acu$, $a|bcv$ ($a|bc$ по условию), то $a|c$. ⊠

2. $a, b|c, \ (a, b) = 1 \ \Rightarrow \ ab|c$

   ♦

   $$au + bv = 1$$

   Умножим обе части равенства на c.

   $$acu + bcv = c$$

   Так как $ab|acu$, $ab|bcv$, то $ab|c$. ⊠

3. $(a, c) = (b, c) = 1 \Rightarrow (ab, c) = 1$

14 НОК

Под наименьшим общим кратным понимается наименьшее число, которое делят и a, и b.

Теорема.

$$a|M, \ b|M \ \Rightarrow [a, b]|M$$

♦
$$M = [a,b]q + r$$
$$a|M,\ a|[a,b] \Rightarrow a|r$$
$$b|M,\ b|[a,b] \Rightarrow b|r$$
$$a,b|r,\ r < [a,b] \Rightarrow r = 0$$

⊠

Теорема.
$$ab = (a,b)[a,b]$$

- $[ak, bk] = [a,b]k$

НОД и НОК можно вычислять последовательно:

$$(a,b,c) = ((a,b),c)$$

$$[a,b,c,d] = [[a,b,c],d] = [[a,b],c],d]$$

15 Простые числа

Число $p > 1,\ p \in \mathbb{N}$ называется простым, если $1|p$ и $p|p$, других делителей нет.

• Либо $(p,a) = 1$ — p взаимно простое с a, либо $p|a$.

Теорема. *Простых чисел бесконечно много.*

♦ Если число простых чисел конечно, то их можно перечислить и перемножить:

$$2 \cdot 3 \cdot\ \ldots\ \cdot p$$

Добавим 1:
$$2 \cdot 3 \cdot\ \ldots\ \cdot p + 1$$

Полученное число не может быть простым, так как простые числа мы перечислили в произведении. Значит оно составное.
Если это число составное, то оно должно раскладываться на простые делители, при этом $q \neq 2, 3, \ldots\ \Rightarrow$ число должно иметь другие простые числа, которые его делят, или само быть простым.
Так как оба условия невозможны, то получаем противоречие. ⊠

Теорема. *Любое число представимо в виде степеней попарно простых чисел:*

$$m = p_1^{k_1} \cdot p_2^{k_2} \cdot\ \ldots\ \cdot p_r^{k_r}$$

♦ **Возможность**
$m = m_1 \cdot p_1$, где p_1 — наименьший простой делитель.
Если $m_1 > 1$, то $m = m_2 \cdot p_1 \cdot p_2$ и т.д., пока $p_i \neq 1$. В конечном итоге получим разложение:

$$m = p_1 \cdot p_2 \cdot p_3 \cdot\ \ldots\ \cdot p_i$$

где $p_i = 1$.
С учетом кратности простых чисел в полученном разложении, его можно переписать в виде:
$$m = p_1^{k_1} \cdot p_2^{k_2} \cdot \ \dots \ \cdot p_r^{k_r}$$
Единственность
Пусть $m = p_1 \cdot p_2 \cdot \ \dots \ \cdot p_l$ и $m = q_1 \cdot q_2 \cdot \ \dots \ \cdot q_s$.
Следовательно $p_1 \cdot p_2 \cdot \ \dots \ \cdot p_l = q_1 \cdot q_2 \cdot \ \dots \ \cdot q_s$.
Так как левая часть делится на p_1, то и правая часть тоже. Значит среди множителей правой части есть хотя бы один, который делится на p_1.
А так как все они простые, то какой-то из множителей равен p_1 (пусть это q_1), значит на него можно сократить.
Продолжая алгоритм до конца, приходим к выводу, что все множители обеих частей попарно равны. ⊠

16 Сравнения

Возьмем $m \in \mathbb{N},\ m > 1$.

a и b **сравнимы по модулю** m, если у a и b одинаковый остаток при делении на m.
• $a \equiv b \pmod m,\ m | a - b$

Пример
$10 \equiv 12 \pmod 2$, так как $10 \bmod 2 = 12 \bmod 2 = 0$.

Свойства сравнений

1. $a \equiv a \pmod m$ — *рефлексивность.*
2. $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$ — *симметричность.*
3. $a \equiv b \pmod m,\ b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$ — *транзитивность.*
4. $a \equiv b \pmod m \Rightarrow a + c \equiv b + c \pmod m$

   $m | (a + c) - (b + c) = a - b$
5. *Сравнения по одному и тому же модулю можно почленно складывать*
$$a \equiv b \pmod m$$
$$a' \equiv b' \pmod m$$
$$a + a' \equiv b + b' \pmod m$$
$$m | (a + a' - (b + b')) = (a - b) + (a' + b')$$
6. *Сравнения по одному и тому же модулю можно почленно умножать*
$$a \cdot a' \equiv b \cdot b' \pmod m$$
$$a = mq_1 + r_1$$
$$a' = mq_2 + r_2$$
$$a \cdot a' = mQ_1 + r_1 r_2$$

$$b = mq_3 + r_1$$
$$b' = mq_4 + r_2$$
$$b \cdot b' = mQ_2 + r_1 r_2$$
$$m | aa' - bb' = m(Q_1 - Q_2)$$

7. *Обе части сравнения можно умножить на одно и то же число*

$$a \equiv b \pmod m$$
$$ak \equiv bk \pmod m$$
$$m | k(a - b)$$

8. *Обе части сравнения и модуль можно умножать на одно и то же число*

$$a \equiv b \pmod m$$
$$ak \equiv bk \pmod{mk}$$
$$mk | k(a - b)$$

9. *Обе части сравнения и модуль можно сокращать на одно и то же число*

$$ak \equiv bk \pmod{mk} \Rightarrow a \equiv b \pmod m$$
$$\frac{(a-b)k}{mk} = \frac{a-b}{m}$$

10. *Обе части сравнения можно сокращать на число, взаимно простое с модулем.*

$$ak \equiv bk \pmod m \Rightarrow a \equiv b \pmod m,\ (k, m) = 1$$
$$m | k(a - b)$$

11. $a \equiv b \pmod m \Rightarrow (a, m) = (b, m)$
    $a = b + km$

17 Классы вычетов

• В класс вычетов входят все числа с данным остатком.
• Класс вычетов определяет бинарное отношение эквивалентности.

Пример

$$m = 3 :\ 3\mathbb{Z},\ 3\mathbb{Z} + 1,\ 3\mathbb{Z} + 2$$

• **Вычет** — любой элемент класса.
• $\bar{a}$ — класс, в который входят элементы с таким же остатком, как у a.

Пример

$$\bar{1} = \{2k + 1\},\ m = 2$$

• $\bar{a} = \bar{b}$ — классы совпадают $\Leftrightarrow\ a \equiv b \pmod m$
• $\bar{a} = \bar{b}$ либо $\bar{a} \cap \bar{b} = \varnothing$
• **Полной системой вычетов** называется система представителей всех классов вычетов.

Теорема. *Пусть* $(a, m) = 1$, *x пробегает полную систему вычетов* $\Rightarrow$ $ax + b$ *пробегает полную систему вычетов.*

♦ Рассмотрим вычеты x_1 и x_2, которые относятся к разным классам (1).
Предположим, что $ax_1 + b \equiv ax_2 + b \pmod{m}$.
Тогда по свойству **4** мы можем отнять число b. А так как по условию $(a, m) = 1$, то по свойству **10** можно сократить на число a.
Таким образом получим

$$x_1 \equiv x_2 \pmod{m}$$

что противоречит условию (1). ⊠
• Полная система вычетов: $m : 0, 1, 2, \dots, m - 1$.
• Приведенная система вычетов: взаимно простые с модулем числа.
• Если один представитель класса взаимно простой с модулем, то все элементы класса взаимно простые с модулем.

Теорема. *Пусть* $(a, m) = 1$. *Тогда* x *и* ax *одноименно пробегают приведенную систему вычетов или нет.*

♦ $ax_1 \equiv ax_2 \pmod{m} \Leftrightarrow x_1 \equiv x_2 \pmod{m}$ ⊠

18 Функция Эйлера

Определяется для любого натурального m.
• $\varphi(m)$ — число классов вычетов, взаимно простых с модулем.

Пример
$\varphi(1) = 1$
$\varphi(2) = 1$ — классы вычетов $(0, 1)$, но 0 не взаимно простой с 2.
$\varphi(3) = 2$ — классы вычетов $(0, 1, 2)$, но 0 не взаимно простой с 3.
$\varphi(4) = 2$
$\varphi(5) = 4$

Теорема. $\varphi(p) = p - 1$, *где* p — *простое число.*

♦ Полная система вычетов для p: $0, 1, 2, \dots, p - 1$.
Так как p — простое число, то все вычеты с ним взаимно простые. ⊠

Теорема. $\varphi(p^n) = p^n - p^{n-1}$

♦

$$1, 2, \dots, p, \dots, 2p, \dots, p^n - 1, p^n$$

В этом ряду каждое p-ое число делится на p, остальные взаимно простые, следовательно

$$p^n - \frac{p_n}{p} = p^n - p^{n-1}$$

⊠

Теорема. $(a, b) = 1 \Rightarrow \varphi(ab) = \varphi(a)\varphi(b)$

♦ Запишем матрицу

$$\begin{pmatrix} 1 & 2 & 3 & \dots & a \\ a+1 & a+2 & a+3 & \dots & 2a \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (b-1)a+1 & (b-1)a+2 & (b-1)a+3 & \dots & ab \end{pmatrix}$$

Найдем числа такие, что $(x, ab) = 1$.

$$(x, ab) = 1 \Leftrightarrow (x, a) = (x, b) = 1$$

Вначале ищем x взаимно простые с a. Эти числа могут быть только в столбцах с номерами, взаимно простыми с a. А таких столбцов $\varphi(a)$.
Более того, все числа таких столбцов взаимно простые с a и этот столбец — полная система вычетов по модулю b.
Значит чисел взаимно простых с b — $\varphi(b)$.
Тогда $\varphi(ab) = \varphi(a)\varphi(b)$. ⊠

Теорема. ***Эйлера***
$(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod m$

♦ Возьмем такое a, что $(a, m) = 1$.
Пусть $l = \varphi(m)$.
И возьмем приведенную систему вычетов $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_l$.
Рассмотрим сравнение

$$(a\varepsilon_1) \cdot (a\varepsilon_2) \cdot \ \dots \ (a\varepsilon_l) \equiv \varepsilon_1 \cdot \varepsilon_2 \cdot \ \dots \ \varepsilon_l \pmod m$$

Так как мы взяли приведенную систему вычетов, то ε_i взаимно простое с m, значит мы можем сократить на все ε обе части.
В конце получим

$$a^{\varphi(m)} \equiv 1 \pmod m$$

⊠

Теорема. ***Ферма***
$(a, p) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod m$

♦ Доказательство следует из предыдущей теоремы.
Используем лемму о том, что $\varphi(p) = p - 1$ и подставим это значение в $a^{\varphi(m)} \equiv 1 \pmod m$.
Получаем

$$a^{p-1} \equiv 1 \pmod m$$

⊠

19 RSA-криптосистема

• С помощью теоремы Эйлера появилась первая система цифровой подписи и первая криптосистема с открытым ключом.
Рассмотрим факторизацию числа N:

$$N = pq$$

Найдем значение функции Эйлера:

$$\varphi(N) = (p-1)(q-1)$$

Далее подбираются числа e и d такие, что

$$ed \equiv 1 \pmod{c}, \;\; c = \varphi(N)$$

e — **открытый** ключ.
d — **закрытый** ключ.

Шифрование
Берем число x такое, что $(x, N) = 1$.

$$x \to x^e \bmod N$$

Дешифрование

$$x^e = (x^e)^d \bmod N$$

♦ $x^{ed} = x^{1+ke} = (x^e)^k \cdot x \equiv x \pmod{N}$
Так как $(x, N) = 1$, можно сократить на x:

$$(x^e)^k \equiv 1 \pmod{N}$$

⊠

20 Сравнения первой степени

$$ax \equiv b \pmod{m}$$

Теорема. *Сравнение разрешимо* $\Leftrightarrow$ $d|b$. *В случае разрешимости оно имеет единственное решение по модулю* m' *и* d *решений по модулю* m*:*

$$x \equiv x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \ldots, (d-1)\frac{m}{d}$$

♦ $(a, m) = d|b$ — необходимое условие разрешимости.

$$\frac{ax - b}{m} \in \mathbb{Z}$$

$d|ax$ и $d|m$ (так как $d = (a, m)$) $\Rightarrow d|b$.
Поделим обе части сравнения и модуль на d.

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

Обозначим как

$$a'x \equiv b' \pmod{m'}, \;\; (a', m') = 1$$

И тогда это сравнение имеет единственное решение по модулю m' по 2 лемме о пробегании.
Таким образом условие $(a, m) = d|b$ является и достаточным. ⊠

Способы решения

1. *Подбор (при маленьком модуле)*

$$5x \equiv 1 \pmod 7$$

Проверяем полную систему вычетов по модулю 7:

$$0, 1, 2, 3, 4, 5, 6$$

$$x \equiv 3 \pmod 7$$

2. *Способ Эйлера*
Проверяем условие разрешимости по теореме.
Если решения есть, то домножим обе части сравнения на $a^{\varphi(m)-1}$:

$$a^{\varphi(m)-1}ax \equiv ba^{\varphi(m)-1} \pmod m$$

По теореме Эйлера

$$a^{\varphi(m)} \equiv 1 \pmod m \Rightarrow \ x \equiv ba^{\varphi(m)-1} \pmod m$$

3. *Расширенный алгоритм Евклида*
Нужно найти такие u и v, что

$$au + mv = 1$$

Домножим обе части сравнения на u:

$$aux \equiv bu \pmod m$$

$$(1 - mv)x \equiv bu \pmod m$$

$$mv \equiv 0 \pmod m \Rightarrow \ x \equiv bu \pmod m$$

21 Системы сравнений

$$\begin{cases} a_1x \equiv b_1 \pmod{m_1} \\ a_2x \equiv b_2 \pmod{m_2} \\ \dots\dots\dots\dots\dots\dots \\ a_sx \equiv b_s \pmod{m_s} \end{cases} \quad \text{сводится к} \quad \begin{cases} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \\ \dots\dots\dots\dots\dots \\ x \equiv c_s \pmod{m_s} \end{cases}$$

Способ 1
Выражаем x из первого сравнения

$$x = c_1 + m_1t \tag{1}$$

и подставляем во второе.
Находим оттуда t и подставляем в уравнение (1):

$$m_1t \equiv (c_2 - c_1) \pmod{m_2}, \ (m_1, m_2)|c_2 - c_1$$

$$t = t_0 + \frac{m_2}{(m_1, m_2)}k, \ k \in \mathbb{Z}$$

Подставляя t в уравнение (1), получаем:

$$x = c_1 + m_1t_0 + \frac{m_1m_2}{(m_1, m_2)}k \Rightarrow \ x = x_0 + [m_1, m_2]k$$

где $x_0 = c_1 + m_1 t$.
Тогда вместо первых двух сравнений в систему запишем

$$x \equiv x_0 \pmod{[m_1, m_2]}$$

Этот алгоритм либо установит неразрешимость системы, либо найдет одно решение по модулю $[m_1, m_2, \ldots, m_s]$.

CRT (Китайская теорема об остатках)

Предназначена для решения систем вида: $\begin{cases} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv c_s \pmod{m_s} \end{cases} \quad (m_i, m_j) = 1,\ i \neq j$

Домножим каждое сравнение на модули других сравнений (имеем право, так как модули попарно взаимно простые):

$$\begin{cases} x_1 m_2 m_3 \ldots m_s \equiv 1 \pmod{m_1} \\ x_2 m_2 1 m_3 \ldots m_s \equiv 1 \pmod{m_2} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_s m_1 m_2 \ldots m_{s-1} \equiv 1 \pmod{m_s} \end{cases}$$

Все они разрешимы по критерию разрешимости: $(a, m) = 1|1$.
Составляем решение:

$$X = c_1 x_1 m_2 m_3 \ldots m_s + c_2 x_2 m_1 m_3 \ldots m_s + \cdots + c_s x_s m_1 m_2 \ldots m_{s-1}$$

Так как все модули попарно взаимно простые, то их НОК $= m_1 m_2 \ldots m_s$.

Теорема. *Система сравнений с попарно взаимно простыми модулями разрешима и имеет единственное решение*

$$x \equiv c \pmod{m_1 m_2 \ldots m_s}$$

22 Показатели

$$a^{\varphi(m)} \equiv 1 \pmod{m},\ (a, m) = 1$$

• $a \sim \delta$, если $a^{\delta} \equiv 1 \pmod{m}, \delta \in \mathbb{N}, \delta - min$.

Свойства показателя

1. $a^k \equiv 1 \pmod{m} \Rightarrow \delta | k$

   ⧫

   $$k = \delta q + r,\ 0 \leq r \leq \delta$$
   $$a^k = a^{\delta q} \cdot a^r$$
   $$a^{\delta q} \equiv 1 \pmod{m} \Rightarrow a^k \equiv a^r \equiv 1 (\operatorname{mod} m)$$

   Так как $0 \leq r \leq \delta$ и $a^r \equiv 1 \pmod{m}$, то $r = 0$. ⊠

2. $a^{\varphi(m)} \equiv 1 \pmod{m} \Rightarrow \delta | \varphi(m)$

3. $a^0 = 1, a^1, \ldots, a^{\delta-1}$ — в этом ряду все числа попарно не сравнимы по модулю m.

   ♦
$$a^i \equiv a^j \pmod m,\ i < j$$
   где $i > 0,\ j \leq \delta - 1$.
   Сократим обе части сравнения на a^j:
$$a^{i-j} \equiv 1 \pmod m,\ i - j < \delta$$
   Однако $\delta - min\ \Rightarrow$ противоречие. ⊠

4. $a \sim \delta_1,\ b \sim \delta_2,\ (\delta_1, \delta_2) = 1 \Rightarrow\ ab \sim \delta_1\delta_2$

   ♦ Пусть $ab \sim \delta,\ \delta \leq \delta_1\delta_2$, так как $(ab)^{\delta_1\delta_2} \equiv 1 \pmod m$.
   $1 \equiv ((ab)^{\delta_1})^{\delta_2} \equiv a^{\delta} b^{\delta_1\delta_2} \equiv a^{\delta} \pmod m \Rightarrow\ \delta_1|\delta,\ \delta_2|\delta \Rightarrow \delta_1\delta_2|\delta\ ((\delta_1, \delta_2) = 1) \Rightarrow \delta_1\delta_2 = \delta$.
   ⊠

5. $a \sim \delta \Rightarrow\ a^k \sim \dfrac{\delta}{(k, \delta)}$

   ♦ $(a^k)^l$
   Так как $a^m \equiv 1 \Rightarrow \delta|m$, то необходимо найти при каком минимальном значении l дробь $\dfrac{kl}{\delta}$ целая.
$$\frac{kl}{\delta} = \frac{k/(\delta, k)l}{\delta/(\delta, k)} \Rightarrow l = \frac{\delta}{(\delta, k)}$$
   ⊠

23 Первообразные корни

$$a^{\delta} \equiv 1 \pmod m$$

• Первообразный корень по модулю m — число g такое, что $g \sim \delta = \varphi(m)$.

Теорема. *Первообразный корень может быть только при $m = 2, 4, p, p^k, 2p^k$.*

♦ Рассмотрим 2^k.
Пусть $k = 1$. Тогда $2^k = 2,\ \varphi(2) = 1$. Первообразным корнем по модулю 2 будет $1 \equiv -1 \pmod 2$.
Пусть $k = 2$. Тогда $2^k = 4,\ \varphi(2) = 2$. Первообразным корнем по модулю 4 будет $3 \equiv -1 \pmod 4$.
Пусть $k \geq 3$. Тогда $2^k \geq 8,\ \varphi(k) = 2^{k-1}$. Первообразных корней в таком случае нет, так как для нечетного числа $a = 2^k t + 1$ показатель по модулю 2^{α} не будет превосходить $2^{\alpha-2} = \dfrac{1}{2}\varphi(2^{\alpha})$:
$$a^3 = 1 + 8t \equiv 1 \pmod 8$$
$$a^4 = 1 + 16t \equiv 1 \pmod{16}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$a^{2^k-2} = 1 + 2^k \equiv 1 \pmod{2^k}$$

Рассмотрим случай $m = p$:
Возьмем приведенную систему вычетов $1, 2, \ldots, p-1$, где каждое число принадлежит показателям $\delta_1, \delta_2, \ldots, \delta_{p-1}$ соответственно, то есть $\exists g \sim \delta,\ \delta = [\delta_1, \delta_2, \ldots, \delta_{p-1}]$.
Если $g \sim \delta = \varphi(p) = p - 1$ выполняется, то g — первообразный корень.

Предположим $\delta < p-1$.
Тогда $\forall a (a,p)=1 \Rightarrow \ a^{\delta} \equiv 1 \pmod p$.
Все ненулевые элементы поля вычетов являются корнями многочлена $x^{\delta}-1$. Это уравнение имеет p корней.
$\delta < p-1,\ \delta+1 < p$, то есть степень многочлена меньше, чем количество корней — противоречие.

Покажем, что для других чисел корней нет.
$m \neq 2, 4, p, p^k, 2p^k$.
Это такие числа, для которых выполняется $m = m_1 m_2,\ (m_1, m_2) = 1,\ \varphi(m_1) \equiv \varphi(m_2) \equiv 0 \pmod 2$.
Возьмем такое a, что $(a,m)=1$.

$$a^{\frac{\varphi(m)}{2}} = (a^{\varphi(m_1)})^{\varphi(m_2)/2} \equiv 1 \pmod{m_1},\ a^{\varphi(m_1)} \equiv 1 \pmod{m_1}$$

Аналогично для m_2. Следовательно

$$a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod m \Rightarrow \delta \neq \varphi(m)$$

что противоречит определению первообразного корня. ⊠