# ЛИНЕЙНЫЕ ФУНКЦИИ НА ВЕКТОРНЫХ ПРОСТРАНСТВАХ

Пусть $V \subseteq \mathbb{R}^n$ - подпространство в $\mathbb{R}^n$, $W \subseteq \mathbb{R}^m$ - подпространство в $\mathbb{R}^m$.

**ОПР.** Отображение $f : V \to W$ называется ЛИНЕЙНЫМ, если

$$f(x+y) = f(x)+f(y),\ f(\alpha x) = \alpha f(x) \quad \forall\, x, y \in V,\ \alpha \in \mathbb{R}.$$

**ПРЕДЛОЖЕНИЕ**. Пусть $e_1, \ldots, e_k$ - базис $V$. Тогда линейное отображение $f : V \to W$ однозначно определено своими значениями на базисных векторах.

**Д-ВО.** Пусть заданы значения $f(e_1) = w_1, \ldots, f(e_k) = w_k$. Любой вектор $v \in V$ однозначно разлагается по базису: $v = \alpha_1 e_1 + \cdots + \alpha_k e_k$. В силу линейности

$$f(v) = f(\sum_i \alpha_i e_i) = \sum_i \alpha_i f(e_i) = \sum_i \alpha_i w_i.$$

$\square$

==============================

МАТРИЦА Линейного отображения

Пусть $V = W$ и $e_1, \ldots, e_k$ - базис $V$. Разложим вектор $f(e_j)$ по базису:

$$f(e_j) = \sum_{i=1}^{k} a_{ij} e_i \quad (1 \leq j \leq k).$$

**ОПР.** Матрица $A = (a_{ij})$ называется матрицей $f$ в базисе $e_1, \ldots, e_k$.

Пусть $f, g$ - линейные отобрражения $V \to V$. Тогда их композиция - тоже линейное отображение $V \to V$:

$$(fg)(x+y) = f(g(x+y)) = f(g(x)+g(y)) = f(g(x))+f(g(y)) =$$
$$= (fg)(x) + fg)(y)$$

$$(fg)(\alpha x) = f(g(\alpha x)) = f(\alpha g(x)) = \alpha f(g(x)) = \alpha (fg)(x)$$

**ТЕОРЕМА.** Пусть $v = x_1 e_1 + \cdots + x_k e_k$; $w = f(v) = y_1 e_1 + \cdots + y_k e_k$. Тогда $Y = AX$.

**Д-ВО.** $w = \sum_i y_i e_i$ - разложение по базису. Но

$$w = f(v) = f(x_1 e_1 + \cdots + x_k e_k) = \sum_j x_j f(e_j) =$$

$$= \sum_j x_j \left( \sum_i a_{ij} e_i \right) = \sum_i \left( \sum_j a_{ij} x_j \right) e_i$$

- тоже разложение по базису. Из единственности разложения и следует, что

$$y_i = \sum_j a_{ij} x_j, \quad \text{т.е} \quad Y = AX.$$

$\square$

==================================

Пусть теперь $\{e_1, \ldots, e_m\}$ - базис $V$, $A = (a_{ij})_{m \times m}$ - матрица $f$, а $B = (b_{ij})_{m \times m}$ - матрица $g$ в этом базисе.

**ТЕОРЕМА.** Отображение $fg$ имеет матрицу $AB$ в базисе $\{e_1, \ldots, e_m\}$.

**Д-ВО.** Обозначим $h = fg$. Тогда

$$h(e_j) = f(g(e_j) = f\left(\sum_k b_{kj} e_k\right) = \sum_k b_{kj} f(e_k) =$$

$$= \sum_k \sum_i b_{kj} a_{ik} e_i = \sum_i \left(\sum_k a_{ik} b_{kj}\right) e_i,$$

т.е.

$$h(e_j) = \sum_i c_{ij} e_i, \quad \text{где} \quad C = (c_{ij}) = AB.$$

В силу однозначности разложения по базису, $C$ является матрицей $fg = h$ в базисе $\{e_1, \ldots, e_m\}$. $\square$

# СИММЕТРИЧЕСКАЯ ГРУППА

## I. Напоминание

Пусть $M$ и $N$ - некоторые множества. Отображение $f : M \to N$ называется

- *сюрьективным*, если $\forall y \in N \ \exists x \in M : f(x) = y$ (отображение „на“);
- *инъективным*, если $\forall x \neq y \in M$ выполнено неравенство $f(x) \neq f(y)$ (разные элементы переходят в разные);
- *биективным*, если $f$ инъективно и сюръективно одновременно (другое название - взаимно-однозначное соответствие)

Если $f : M \to N$ - биекция, то можно построить отображение $g : N \to M$ по правилу: если $f(x) = y$, то $g(y) = x$. Т.к. $f$ сюръективно, то $g$ определено для всех $y \in N$. Т.к. $f$ инъективно, то у любого $y$ есть только один прообраз, поэтому $g$ определено корректно. При этом $g$ - тоже биекция $N \to M$. Более того,

$$f(g(x)) = x \ \ \forall x \in N, \ g(f(y)) = y \ \ \forall y \in M,$$

т.е. $fg$ - тождественное отображение на $N$, а $gf$ - тождественное отображение на $M$.

## II. Перестановки чисел {1,. . . ,n }

Перестановка - последовательность $(i_1, i_2, \ldots, i_n)$, составленная из чисел $1, 2, \ldots, n$, в которой каждое из них встречается ровно 1 раз.

Всего перестановок - $n! = n(n-1)\cdots 2 \cdot 1$.

Инверсия: пара чисел $(i, j)$ в перестановке $(\cdots i \cdots j \cdots)$ образует *инверсию*, если $i > j$ (т.е. большее число стоит левее меньшего).

ПРИМЕР. Перестановка (31254)

Инверсии - $(3, 1), (3, 2), (5, 4)$

Четность перестановки - четность числа инверсий.

ПРИМЕР. Перестановка (31254) нечетная, а перестановка (12345) - четная

**ТЕОРЕМА 1.** Если в перестановке поменять местами любую пару чисел, то четность числа инверсий изменится.

**Д-ВО.**

1). Сначала рассмотрим случай, когда меняется местами пара соседних чисел:

$$A = (\cdots i\ j \cdots) \to (\cdots j\ i \cdots) = B$$

Инверсии вида $(i, \alpha), i > \alpha$, $(\beta, i), \beta > i$, $(j, \gamma), j > \gamma$, $(\delta, j), \delta > j$, у $A$ и $B$ одни и те же. Поэтому при $i > j$ общее число инверсий уменьшается на 1, а при $i < j$ - увеличивается на 1 $\Rightarrow$ четность меняется.

2) Общий случай.

$$A = (\cdots i\ t_1 \cdots t_s\ j \cdots) \to (\cdots j\ t_1 \cdots\ t_s\ i \cdots) = B$$

Переход от $A$ к $B$ можно осуществить, меняя последовательно местами $i$ с $t_1, \ldots, t_s$, затем $i$ с $j$, а затем $j$ с $t_s, \ldots, t_1$. Во всех случаях меняются местами соседние индексы $\Rightarrow$ четностьь меняется $2s + 1$ раз $\Rightarrow$ четности $A$ и $B$ различны. $\square$

## II. Подстановки

Пусть $M = \{1, \ldots, n\}$.

**ОПР.** Совокупность всех биекций (обозначаемая как $S_n$) множества $M$ в себя называется <u>группой подстановок</u> или <u>симметрической группой</u>.

<u>Подстановка</u> - любой элемент из $S_n$ (т.е. любая биекция $M \to M$)

## ОБЩИЕ СВОЙСТВА $S_n$

1) в $S_n$ есть операция - композиция подстановок ($f \circ g$ или $fg$), она АССОЦИАТИВНА
2) $\exists e \in S_n : ef = fe = f \quad \forall f \in S_n$ ($e$ - тождественная подстановка)
3) $\forall f \in S_n \ \exists g \in S_n : fg = gf = e$ ($g = f^{-1}$ - обратная подстановка)

### Форма записи подстановок

$$\sigma \in S_n \Rightarrow \sigma = \begin{pmatrix} i_1 & \dots & i_n \\ j_1 & \dots & j_n \end{pmatrix}$$

где $(i_1, \dots, i_n)$ и $(j_1, \dots, j_n)$ - перестановки, $\sigma(i_1) = j_1, \dots, \sigma(i_n) = j_n$.

Запись подстаноки $\sigma$ в такой форме неоднозначна. Наиболее естественной является форма

$$\sigma = \begin{pmatrix} 1 & \dots & n \\ j_1 & \dots & j_n \end{pmatrix}$$

если $\sigma(1) = j_1, \dots, \sigma(n) = j_n$

**ТЕОРЕМА 2.** Четность суммарного числа инверсий в верхней и нижней строках не зависит от способа записи подстановки.

**Д-ВО**. От любой записи

$$\sigma = \begin{pmatrix} i_1 & \dots & i_n \\ j_1 & \dots & j_n \end{pmatrix}$$

к любой другой записи

$$\sigma = \begin{pmatrix} i'_1 & \dots & i'_n \\ j'_1 & \dots & j'_n \end{pmatrix}$$

можно перейти, поменяв несколько раз местами столбцы таблицы. По теореме 1 при перестановке двух столбцов число инверсий как в верхней, так и в нижней строке меняет четность $\Rightarrow$ четность суммарного числа инверсий не меняется. $\square$

==============================

**ОПР.** Четность подстановки $\sigma$ - это четность суммарного числа инверсий в верхней и нижней строках в записи

$$\sigma = \begin{pmatrix} i_1 & \dots & i_n \\ j_1 & \dots & j_n \end{pmatrix}$$

**ОПР.** Знак подстановки $\sigma$:

$$\varepsilon_\sigma = \begin{cases} +1, & \text{если} \quad \sigma \text{ четная} \\ -1, & \text{если} \quad \sigma \text{ нечетная} \end{cases}$$

**Следствие** (предыдущей теоремы). $\varepsilon_{\sigma^{-1}} = \varepsilon_\sigma$

**Д-ВО.** Если

$$\sigma = \begin{pmatrix} i_1 & \dots & i_n \\ j_1 & \dots & j_n \end{pmatrix}$$

то

$$\sigma^{-1} = \begin{pmatrix} j_1 & \dots & j_n \\ i_1 & \dots & i_n \end{pmatrix}$$

Суммарное число инверсий в двух строках - одно и то же. $\square$

==============================

<u>УМНОЖЕНИЕ ПОДСТАНОВОК</u>

Так как $(fg)(i) = f(g(i))$, то

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$$

**ОПР.** ТРАНСПОЗИЦИЯ -подстановка вида

$$\sigma = \begin{pmatrix} 1 & \dots & i & \dots & j & \dots & n \\ 1 & \dots & j & \dots & i & \dots & n \end{pmatrix}$$

т.е. $\sigma(i) = j, \sigma(j) = i, \sigma(k) = k \ \forall k \neq i, j$. Другая форма записи такой траспозиции: $\sigma = (ij)$.

**ТЕОРЕМА 3.** Умножение слева подстановки $\sigma$ на транспозицию $(ij)$ равносильно перестановке чисел $i$ и $j$ в нижней строке таблицы $\sigma$.

**Д-ВО.** Пусть $\sigma(a) = i, \sigma(b) = j$ и $\sigma' = (ij)\sigma$. Тогда $\sigma'(a) = j, \sigma'(b) = i$ и $\sigma'(k) = \sigma(k)\ \forall k \neq a, b$. Т.е.

$$(ij)\begin{pmatrix} 1 & \ldots & a & \ldots & b & \ldots & n \\ k_1 & \ldots & i & \ldots & j & \ldots & k_n \end{pmatrix} = \begin{pmatrix} 1 & \ldots & a & \ldots & b & \ldots & n \\ k_1 & \ldots & j & \ldots & i & \ldots & k_n \end{pmatrix}.$$

□

**ТЕОРЕМА 4.** Любая подстановка раскладывается в произведение транспозиций.

**Д-ВО.** Пусть $\sigma \in S_n$. запишем

$$\sigma = \begin{pmatrix} 1 & \ldots & n \\ i_1 & \ldots & i_n \end{pmatrix} \quad \text{и} \quad e = \begin{pmatrix} 1 & \ldots & n \\ 1 & \ldots & n \end{pmatrix}$$

($e$ - тождественная подстановка). Меняя местами попарно числа в нижней строке $e$, т.е. умножая $e$ на какие-то транспозиции (по теореме 3) слева, можно получить $\sigma$. В результате получаем: $\sigma = \tau_1 \cdots \tau_k e = \tau_1 \cdots \tau_k$. □

**ТЕОРЕМА 5.** Пусть $\sigma = \tau_1 \cdots \tau_m$ - произведение $m$ транспозиций. Тогда $\varepsilon_\sigma = (-1)^m$.

**Д-ВО.**

$$1)\ m = 1,\ \sigma = \tau_1 = \begin{pmatrix} 1 & \ldots & i & \ldots & j & \ldots & n \\ 1 & \ldots & j & \ldots & i & \ldots & n \end{pmatrix}.$$

Нижняя строка получается из верхней перестановкой пары чисел $(i, j)$. В верхней строке инверсий нет. По теореме 1 общее число инверсий нечетно, $(-1)^m = (-1)^1 = -1$.

2) $m > 1$. Пусть $\sigma = \tau_1 \cdots \tau_m$ и $\pi = \tau_2 \cdots \tau_m$. По предположению индукции $\varepsilon_\pi = (-1)^{m-1}$ и $\sigma = \tau_1 \pi$. Если $\tau_1 = (ij)$, а

$$\pi = \begin{pmatrix} 1 & \dots & a & \dots & b & \dots & n \\ r_1 & \dots & i & \dots & j & \dots & r_n \end{pmatrix},$$

то по теореме 3

$$\sigma = \tau_1 \pi = \begin{pmatrix} 1 & \dots & a & \dots & b & \dots & n \\ r_1 & \dots & j & \dots & i & \dots & r_n \end{pmatrix},$$

а по теореме 1 четность нижней строки $\sigma$ не совпадает с четностью числа инверсий нижней строки $\pi$, т.е. $\varepsilon_\sigma = -\varepsilon_\pi = -(-1)^{m-1} = (-1)^m$. $\square$

**СЛЕДСТВИЕ.** $\varepsilon_{\sigma\tau} = \varepsilon_\sigma \varepsilon_\tau$

**Д-ВО.** Если $\sigma = \pi_1 \cdots \pi_k, \tau = \rho_1 \cdots \rho_m$, то $\sigma\tau = \pi_1 \cdots \pi_k \rho_1 \cdots \rho_m$. Тогда $\varepsilon_\sigma = (-1)^k$, $\varepsilon_\tau = (-1)^m$, $\varepsilon_{\sigma\tau} = (-1)^{k+m} = (-1)^k (-1)^m = \varepsilon_\sigma \varepsilon_\tau$. $\square$