$\tau = (1\,2) \in S_k$

$$\underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 6 & 3 & 4 & 5 & 1 & 2 \end{pmatrix}}_{\overset{\text{ozn.}}{=}\sigma}^{2} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 5 & 6 & 3 & 4 & 8 & 7 \end{pmatrix} = (1,2)(3,5)(4,6)(7,8)$$

$$\sigma^{2018} = \big((1\,8\,2\,7)(3\,6\,5\,4)\big)^{2018} = \overbrace{(1827)(3654)\cdots\cdots(1827)(3654)}^{2018 \text{ bloczków}} =$$

$$= \underbrace{(1827)^{2018}(3654)^{2018}}_{\sigma^2} = \{2018 : 4 = 504 \text{ r } 2\} = (1827)^2(3654)^2 = (1,2)(8,7)(3,5)(6,4)$$

Stwierdzenie

Każdą permutację $\sigma \in S_k$ można zapisać jako iloczyn transpozycji.

Dowód: Wystarczy sprawdzić, że cykle dają się rozłożyć na iloczyn transpozycji. W tym celu zauważmy, że zachodzi równość $(i_1, \dots, i_k) = (i_1, i_k)(i_1, i_{k-1}) \dots (i_1, i_2)$ (jest $k-1$ transpozycji)

Inny rozkład $(i_1, \dots, i_k) = (i_{k-1}, i_k) \dots (i_2, i_k)(i_1, i_k)$ (jest $k-1$ transpozycji)

Definicja: Wielomianem zmiennych $X_1, \dots, X_k$ nazywamy dowolną funkcję będącą sumą funkcji k-zmiennych $x_1, \dots, x_k \in \mathbb{R}$ postaci $a \cdot x_1^{m_1} \dots x_k^{m_k}$ gdzie $a \in \mathbb{R}$ oraz $m_1, \dots, m_k \in \{0, 1, 2, \dots\}$. Zbiór takich wielomianów ozn. $\mathbb{R}[X_1, \dots, X_k]$.

Przykład

$k=3$ $\quad w(x,y,z) = \frac{1}{2}x^2y + 3\cdot\pi\, xyz - z^5 + x$

$V_3(x,y,z) = (y-x)(z-x)(z-y)$ – wielomian Vandermonde'a dla $k=3$

k - dowolne. $V_k \in \mathbb{R}[X_1, \dots, X_k]$ – – " – – " – – " – – dowolnego k

$$V_k(X_1, \dots, X_k) = \prod_{1 \le i < j \le k} (X_j - X_i).$$

Definicja: Niech $w \in \mathbb{R}[X_1, \dots, X_k]$ oraz $\sigma \in S_k$. Wielomian $u \in \mathbb{R}[X_1, \dots, X_k]$ t. że $u(X_1, \dots, X_k) = w(X_{\sigma(1)}, \dots, X_{\sigma(k)})$ oznaczamy $\sigma \cdot w \ (= u)$

Przykład $(1,2) \cdot V_3 = -V_3$ Ogólniej: $\tau \in S_k$ jest transpozycją to $\tau \cdot V_k = -V_k$.

Stwierdzenie: Jeśli $w \in \mathbb{R}[X_1, \dots, X_k]$ & $\rho, \sigma \in S_k$ to

$$\rho \cdot (\sigma \cdot w) = (\rho\sigma) \cdot w$$

Dowód

$$\rho \cdot \underline{(\sigma \cdot w)}(X_1, \dots, X_k) = (\sigma \cdot w)(X_{\rho(1)}, \dots, X_{\rho(k)}) = \left\{ \begin{array}{l} \tilde{X}_i = X_{\rho(i)} \\ X_j = \tilde{X}_{\rho^{-1}(j)} \end{array} \right\}$$

$$= (\sigma \cdot w)(\tilde{X}_1, \dots, \tilde{X}_k) = w(\tilde{X}_{\sigma(1)}, \dots, \tilde{X}_{\sigma(k)}) =$$

$$= w(\tilde{X}_{\rho^{-1}(\rho\sigma(1))}, \dots, \tilde{X}_{\rho^{-1}(\rho\sigma(k))}) = w(X_{\rho\sigma(1)}, \dots, X_{\rho\sigma(k)}) = (\rho\sigma) w(X_1, \dots, X_k)$$

Wniosek. Dla każdego $\sigma \in S_k$ $\exists\, \varepsilon \in \{+1, -1\}$ t. że $\sigma \cdot v_k = \varepsilon v_k$

$\sigma = \tau_1 \cdots \tau_\ell$ gdzie τ_i - transpozycji

$\sigma \cdot v_k = (\tau_1 \cdots \tau_\ell) v_k = \tau_1 (\cdots \tau_\ell \cdot v_k) = (-1)^\ell v_k$ Zatem $\varepsilon = (-1)^\ell$.

ε jak wyżej nazywamy znakiem permutacji σ i oznaczamy symbolem $\operatorname{sgn}(\sigma) = \varepsilon = (-1)^\ell$

Mówimy σ jest permutacją

(a) parzystą jeśli $\operatorname{sgn}(\sigma) = 1$

(b) nieparzystą jeśli $\operatorname{sgn}(\sigma) = -1$

Uwaga: $\varrho, \sigma \in S_k$

$\operatorname{sgn}(\varrho \circ \sigma) = \operatorname{sgn}(\varrho) \operatorname{sgn}(\sigma)$.

$\operatorname{sgn}(i_1, \ldots, i_k) = (-1)^{k-1}$.

Ciało

Definicja Niech $\mathbb{F}$ będzie zbiorem niepustym i $0, 1 \in \mathbb{F}$ t. że $0 \neq 1$. Niech $+, \cdot : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ będą działaniami dwuargumentowymi. Mówimy, że $(\mathbb{F}, 0, 1, +, \cdot)$ jest ciałem jeśli:

1) $(\mathbb{F}, +)$ jest grupą przemienną.

2) $(\mathbb{F} \setminus \{0\}, \cdot)$ jest grupą przemienną.

3) $\forall \lambda, \mu, \nu \in \mathbb{F}$ zachodzi $\lambda \cdot (\mu + \nu) = \lambda\mu + \lambda \cdot \nu$.

Przykład

$\mathbb{F} = \{0, 1\}$ z $+$ i $\cdot$ modulo 2. | $\mathbb{R}, \mathbb{C}, \mathbb{Q}$ |

Antyprzykład: $A = \{0, 1, 2, 3\}$ z $+, \cdot$ mod 4, nie jest ciałem bo $2 \cdot 2 = 0$.

Definicja (przestrzeń wektorowa)

Niech $(V, +)$ będzie grupą abelową („przemienną"), $\mathbb{F}$ będzie ciałem oraz $\cdot : \mathbb{F} \times V \to V$, $(\lambda, v) \mapsto \lambda \cdot v$.

Mówimy, że $(V, +, \cdot)$ jest przestrzenią wektorową nad ciałem $\mathbb{F}$ jeśli

$\forall \lambda, \mu \in \mathbb{F}$ i $u, w \in V$

$(\lambda + \mu) u = \lambda u + \mu \cdot u$

$\lambda \cdot (u + w) = \lambda u + \lambda w$

$\lambda (\mu \cdot u) = (\lambda \mu) \cdot u$

$1 \cdot u = u$.

Elementy V nazywamy wektorami a el. $\mathbb{F}$ skalarami.

Przykład: $n \in \mathbb{N}$ i niech $V = \underbrace{\mathbb{F} \times \ldots \times \mathbb{F}}_{n\text{-razy}} = \mathbb{F}^n$

Dodawanie $(\lambda_1, \ldots, \lambda_n); (\mu_1, \ldots, \mu_n) \in \mathbb{F}^n$ to

$(\lambda_1, \ldots, \lambda_n) + (\mu_1, \ldots, \mu_n) = (\lambda_1 + \mu_1, \ldots, \lambda_n + \mu_n) \in \mathbb{F}^n$.

$\cdot\ \mathbb{F} \times \mathbb{F}^n \to \mathbb{F}^n$, $\nu \cdot (\lambda_1, \ldots, \lambda_n) = (\nu \lambda_1, \ldots, \nu \lambda_n)$ gdzie $\nu, \mu_i, \lambda_j \in \mathbb{F}$.

$(\mathbb{F}^n, +, \cdot)$ jest przestrzenią wektorową nad $\mathbb{F}$.

Przykład 2

$\mathbb{C}_n[\cdot]$ - zbiór wielomianów stopnia nie większego niż n jest p-nią wektorową nad $\mathbb{C}$.

Przykład 3 $\mathbb{C}[\cdot]$ - zbiór wielomianów dowolnego stopnia jest przestrzenią wektorową nad $\mathbb{C}$. Zauważmy, że $\mathbb{C}_n[\cdot] \subset \mathbb{C}[\cdot]$

Definicja Niepusty podzbiór W p-ni wektorowej V nazywamy podprzestrzenią wektorową V jeśli $\forall \lambda \in \mathbb{F}$ oraz $u_1, u_2 \in W$: $u_1 + u_2 \in W$, $\lambda u_1 \in W$

(a) parzysta jeśli ...

(b) nieparzysta jeśli $\operatorname{sgn}(\sigma) = -1$.

$0 \in \mathbb{F}$, $\vec{0} \in V$.

Stwierdzenie

Zachodzą następujące tożsamości:

$\forall v \in V$, $\lambda \in \mathbb{F}$:

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

(b) $(-1) \cdot v = -v$

(c) $\lambda \cdot \vec{0} = \vec{0}$

(d) jeśli $\lambda \cdot v = \vec{0}$ to $\lambda = 0$ lub $v = 0$.

Dowód

a) $v + 0 \cdot v = (1+0) \cdot v = 1 \cdot v = v \Rightarrow 0v = \vec{0}$.

b) $v + (-1) \cdot v = (1 + (-1)) \cdot v = 0 \cdot v = \vec{0}$

c) $\lambda = 0$ to oczywiste z a) | $\lambda \neq 0$. $v + \lambda \cdot \vec{0} = \lambda\left(\frac{1}{\lambda} v + \vec{0}\right) = \lambda \cdot \frac{1}{\lambda} v = v$
$\Rightarrow \lambda \vec{0} = \vec{0}$

Dowód d) $\lambda \neq 0$ to $v = \frac{1}{\lambda} \cdot (\lambda \cdot v) = \frac{1}{\lambda} \cdot \vec{0} = \vec{0}$

$v \neq \vec{0}$ i jednocześnie $\lambda \neq 0$ oraz $\lambda v = \vec{0}$ to $v = \frac{1}{\lambda}(\lambda v) = 0$ sprzeczność

$\square$