Podzielność liczb całkowitych

+ Podzielność liczb całkowitych

Niech $a, b \in \mathbb{Z}$, oraz $a \in \mathbb{Z}^* (a \neq 0)$

Powiemy, że a dzieli b i napiszemy

$a | b$ gdy istnieje liczba całkowita

$k \in \mathbb{Z}$ taka, że $b = a \cdot k$

innymi słowy $\frac{b}{a} \in \mathbb{Z}$

$$a | b \Leftrightarrow \underset{k \in \mathbb{Z}}{\exists} \; b = a \cdot k$$

$a \nmid b$ tzn a nie dzieli b

$$a \nmid \Leftrightarrow \underset{k \in \mathbb{Z}}{\forall} \; b \neq a \cdot k$$

Największy wspólny dzielnik NWD

+ Największy wspólny dzielnik liczb $a, b \in \mathbb{Z}$ $(a^2 + b^2 > 0)$

Powiemy, że $g \in \mathbb{Z}$ jest $NWD(a, b)$ gdy

1) $g | a \wedge g | b$

2) $\forall_{\mathbb{Z} \ni G > g} \; G \nmid a \vee G \nmid b$

Oznaczenie $(a, b) := NWD(a, b) = g$

Def. a, b - są względnie pierwsze

$\Leftrightarrow (a, b) = 1 \leftarrow$ (największy wspólny dzielnik)

Własności NWD

Tw. Własności NWD: Niech $a, b \in \mathbb{Z}$, $a^2+b^2>0$

1) $(a,b)=(b,a)$

2) $\forall_{k\in\mathbb{Z}^*} \ (ka, kb) = |k|(a,b)$

3) $\forall_{k\in\mathbb{Z}} \ (a, b+ka) = (a,b)$

$(a,0) = |a|$

$(a,1) = 1$

Charakteryzacja NWD

Charakteryzacja NWD

Równanie $ax+by=g$, $g=(a,b$

(*) ma zawsze rozwiązanie

Jeżeli $c \in \mathbb{N}$, $c>0$ to równanie

(**) $ax+by=c$ to równanie

ma rozw $\iff g|c \iff c=k\cdot g$

dla pewnych $k \in \mathbb{N}^*$

Wynika stąd, że ~~jest to najmniej~~

~~liczba N~~

NWD(a,b) jest to najmniejsza liczba

$\mathbb{N}$ $c>0$ dla której (**)

ma rozwiązanie

- Tw NWD $(a,b)=1 \iff$

równanie $ax+by=1$ ma rozw.

Najmniejsza wspólna wielokrotność NWW

Najmniejsza wspólna wielokrotność

$NWW(a,b)$ dla $a,b \in \mathbb{Z}^*$

Powiemy, że $d \in \mathbb{N}^*$ jest najmniejszą wspólną wielokrotnością a, b gdy

1) $a \mid d \wedge b \mid d$

2) $\cancel{\forall_{a \in \mathbb{N}^*}}$ $\forall_{\mathbb{N}^*} \exists 0 < d \quad a \nmid 0 \vee b \nmid 0$

Oznaczenie $NWW(a,b) := [a,b]$

Twierdzenie: Niech $a, b \in \mathbb{Z}^*$ wtedy

$(a,b)[a,b] = |a \cdot b|$

Tw o dzieleniu z resztą

Tw. o dzieleniu z resztą

Dla dowolnej liczby całkowitej $a \in \mathbb{Z}$ i dowolnej liczby naturalnej $n \geq 1$ istnieją jedyne liczby $q \in \mathbb{Z}$ (nazywanej ilorazem) i $r \in \{0, 1, 2 \ldots n-1\}$ ~~liczby~~ (nazywana resztą) takie że

$$a = q \cdot n + r$$

Oznaczenie reszty z dzielenie

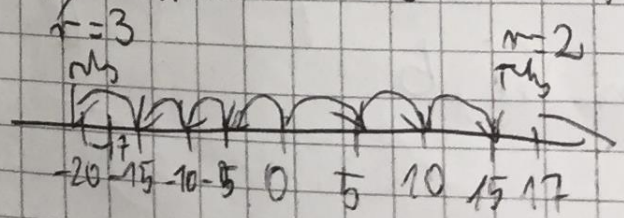
$$r = a \bmod n$$

$20 \bmod 6 = 2$ bo $20 = 3 \cdot 6 + 2$

$40 \bmod 50 = 0$ bo $40 = 8 \cdot 5 + 0$

$17 \bmod 5 = 2$ bo $17 = 3 \cdot 5 + 2$

$(-17) \bmod 5 =$ bo $-17 = -4 \cdot 5 + 3$



Algorytm Euklidesa

Algorytm Euklidesa

$a, b \quad a \in \mathbb{N}^*, b \in \mathbb{N}^*$

$a = q_1 \cdot b + r_1 \qquad r_1 > 0$

$b = q_2 \cdot r_1 + r_2 \qquad r_2 > 0$

$r_1 = q_3 \cdot r_2 + r_3 \qquad r_3 > 0$

$r_2 = q_4 \cdot r_3 + r_4 \qquad r_4 > 0$

$r_k = q_{k+2} \cdot r_{k+1} + r_{k+2} \qquad r_{k+2} > 0$

$r_{k+1} = q_{k+3} \cdot r_{k+2} + 0$

$r_{k+2} = (a, b)$

Innymi słowy ostatnia niezerowa reszta w algorytmie Euklidesa jest największym wspólnym dzielnikiem a, b

Przykład algorytm Euklidesa

$a = 963 \quad b = 657$

$963 = 1 \cdot 657 + 306$	$q_1 = 1$	$r_1 = 306$
$657 = 2 \cdot 306 + 45$	$q_2 = 2$	$r_2 = 45$
$306 = 6 \cdot 45 + 36$	$q_3 = 6$	$r_3 = 36$
$45 = 1 \cdot 36 + 9$	$q_4 = 1$	$r_4 = 9$
$36 = 4 \cdot 9 + 0$		

$E_{-1} : 1 \quad : 1 \cdot 963 + 0 \cdot 657 = 963$

$E_0 \quad : 0 \cdot 963 + 1 \cdot 657 = 657$

$E_1 = E_{-1} - q_1 \cdot E_0 \quad : 1 \cdot 963 - 1 \cdot 657 = 306$

$E_2 = E_0 - q_2 \cdot E_1 \quad : -2 \cdot 963 + 3 \cdot 657 = 45$

$E_3 = E_1 - q_3 \cdot E_2 \quad : 13 \cdot 963 - 19 \cdot 657 = 36$

$E_4 = E_2 - q_4 \cdot E_3 \quad : \underbrace{-15}_{x} \cdot 963 + \underbrace{22}_{y} \cdot 657 = 9$

Zatem $\begin{cases} x_0 = -15 \\ y_0 = 22 \end{cases}$ jest rozwiązaniem szczególnym (*)

Równania diofantyczne

Równania diofantyczne są to równania w liczbach całkowitych

Równanie diofantyczne liniowe jest to równanie w postaci

(*) $ax+by=c \quad a,b,c \in \mathbb{Z}$

Rozwiązaniem takiego równania jest każda para $x,y \in \mathbb{Z}$ spełniająca równanie (*)

Równania diofantyczne przykład

Równanie diofantyczne

$(*)\ 963x + 657y = 9$

Niech $g = (963, 657) = 9 \wedge 9 | 9$

Stąd $(*)$ ma rozwiązanie

Wyznaczymy rozwiązanie szczególne

Ogólne rozw $(*)$ wyraża się wzorem

$$\begin{cases} x = x_0 - \frac{b}{g}t = -15 - \frac{657}{9}t = -15 - 73t \\ y = y_0 + \frac{a}{g}t = 22 + \frac{963}{9}t = 22 + 103t \\ t \in \mathbb{Z} \end{cases}$$

Tw o rozwiązywalności równań biofantycznych

Tw. (o rozwiązywalności równań biofantycznych liniowych) Równanie (*) ma rozwiązanie

$\iff (a,b) \mid c$

Niech $g=(a,b)$. Załóżmy, że (*) rozwiązanie

Niech $x_0, y_0 \in \mathbb{Z}$ będzie rozwiązaniem szczególnym (*) tj

$ax_0 + by_0 = c$ wówczas ogół rozwiązań (*) wyraża się wzorem

$$\begin{cases} x = x_0 - \frac{b}{g}t \\ y = y_0 + \frac{a}{g}t \\ t \in \mathbb{Z} \end{cases}$$

$g = NWD$

Zasadnicze twierdzenie arytmetyki

Zasadnicze tw. arytmetyki

Niech $a, b, c \in \mathbb{Z}$ $a \neq 0$

Załóżmy, że ~~l~~ ~~a~~ liczba a, b są względnie pierwsze $(a, b) = 1$

Jeżeli $a \mid bc$ to $a \mid c$

$$\forall_{a,b,c \in \mathbb{Z}} \left((a \mid bc \wedge (a, b) = 1) \Rightarrow a \mid c \right)$$

Przykład

$a = 3$ $b = 5$ $c = 9$

$3 \mid 5 \cdot 9 \wedge (3, 5) = 1 \Rightarrow 3 \mid 9$

Funkcja Eulera

Funkcja Eulera

Funkcja Eulera $\varphi : \mathbb{N}^* \to \mathbb{N}^*$

$$\varphi(n) = \#\{k \in \mathbb{N}^+ : k \leq n \wedge (k, n) = 1\}$$

mod zbioru - liczba elementu zbioru

(card, $\overline{\overline{A}}$)

$\varphi(n)$ = liczba tych $1 \leq k \leq n$ takich że $(k, n) = 1$

Np.

$\varphi(2) = 1$ $\quad \varphi(5) = 4$ $\quad \varphi(8) = 4$

$\varphi(3) = 2$ $\quad \varphi(6) = 2$ $\quad \varphi(9) = 6$

$\varphi(4) = 2$ $\quad \varphi(7) = 6$ $\quad \varphi(10) = 4$

Własności funkcji Eulera

Własności funkcji Eulera

(1) Jeżeli p jest liczbą pierwszą to $f(p) = p - 1$

Np. $f(7) = 7 - 1 = 6$

(2) $\varphi(15) = 8$

$$\begin{array}{ccccc} 15 & = & 3 & \cdot & 5 \\ \| & & \| & & \| \\ f(15) & & f(3) & & f(5) \\ \| & & \| & & \| \\ 8 & = & 2 & \cdot & 4 \end{array}$$

Jeżeli liczby $(m, n) = 1$ to

$$f(m \cdot n) = f(m) \cdot f(n)$$

np. $f(3 \cdot 5) = f(3) \cdot f(5)$

$$f(2^3) = 4 = 2^2 \cdot 1 = 2^{3-1} \cdot \overbrace{(2-1)}^{f(2)} = 2^{3-1} \cdot f(2)$$

$$f(3^2) = 6 = 3^{2-1} \cdot \overset{2}{\overset{\|}{\varphi(3)}}$$

$$f(p^k) = p^{k-1} \cdot f(p) = p^{k-1} \cdot (p-1)$$

3) Dla dowolnej liczby pierwszej p oraz $k \in \mathbb{N}$ mamy

$$f(p^k) = p^{k-1} \cdot f(p) = p^{k-1} \cdot (p-1)$$

Np. $f(3^2) = 3^{2-1} \cdot (3-1)$

Rozkład liczby na czynniki pierwsze

Niech $n \in \mathbb{N} \geq 2$ mamy rozkład liczby n na czynniki pierwsze

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_s^{k_s}$$

gdzie p_1, p_2, p_s są parami różnymi liczb pierwszych, oraz

$k_1, k_2, k_s \in \mathbb{N}^*$

Np.

1200	2
600	2
300	2
150	2
75	3
25	5
5	5
1	

$$n = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 = 2^4 \cdot 3^1 \cdot 5^2$$

Oczywiście $(p_i^{k_i}, p_j^{k_j}) = 1$ dla $i \neq j$

$$\varphi(n) = \varphi(1200) = \varphi(2^4 \cdot 3^1 \cdot 5^2) = \varphi(2^4) \cdot \varphi(3^1) \cdot \varphi(5^2) =$$

$$= 2^3(2-1)\, 3^0(3-1)\, 5^1(5-1) = 2^6 \cdot 5 = 320$$

Liczby pierwsze

Liczby pierwsze

$\mathbb{P}$ - zbiór liczb pierwszych

Liczba naturalna $p \geq 1$ jest pierwsza gdy posiada dokładnie 2 różne dzielniki naturalne

1 nie jest liczbą pierwszą

$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23 \ldots\}$

Jedyną liczbą pierwszą parzystą jest 2

Zbiór liczb pierwszych jest nieskończenie wiele

Twierdzenie o istnieniu jednoznaczności rozkładu liczby naturalnej na iloczyn liczb pierwszych; jednoznaczność

Twierdzenie o istnieniu jednoznaczności rozkładu liczby naturalnej na iloczyn liczb pierwszych

Dla dowolnej liczby $\mathbb{N}$ $n \geq 2$ istnieją <u>jedyne</u> liczby pierwsze $p_1 \leq p_2 \leq \ldots \leq p_k$ $(p_j \in \mathbb{P})$ takie, że liczba $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$

Jedyność oznacza, że jeżeli mamy inny rozkład $n = q_1 \cdot q_2 \cdot \ldots \cdot q_s$ gdzie q_j są ~~liczbami~~ $\in \mathbb{P}$ oraz $q_1 \leq q_2 \leq q_s$ to $s = k$ oraz dla dowolnego $1 \leq j \leq k$ mamy $p_j = q_j$

Silnia

$n \in \mathbb{N}$

$$\begin{cases} 0! = 1 \\ (n+1)! = n!\,(n+1 \end{cases}$$

Jeśli $n \geq 1$ to $n! = 1 \cdot 2 \quad (n-1)\,n$

$3! = 1 \cdot 2 \cdot 3 = 6$

$4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24 = 6 \cdot 4 = 3! \cdot 4$

Dwumian Newtona

$$\binom{n}{k} = \frac{n!}{(n-k)!\,k!} \in \mathbb{N}$$

Dla dowolnego N istnieją liczby $k_1, k_2 = k_1 + 1, k_3 = k_2 + 1, k_N = k_{N-1}$ (kolejne liczby naturalne) z których żadna p nie jest pierwsza

Sito eratostenesa

Metoda sita Eratostenesa

Aby wyznaczyć wszystkie liczby pierwsze $\leq n$ $(n \in \mathbb{N}, n \geq 2)$

Wypisujemy kolejno wszystkie liczby naturalne od 2 do n

Wykonujemy następujące kroki

1) Bierzemy 2 (zostawiamy ją) i wykreślamy wszystkie jej wielokrotności

Kongruencje własności

Kongruencja

$a, b \in \mathbb{Z}, n \in \mathbb{N}^+$

Def. Powiemy, że a przystaje do b według modułu n

$a \equiv b \mod n$

gdy $n \mid (a-b)$

np. $7 \equiv 1 \mod 3$ tak

bo $3 \mid (7-1) = 3 \mid 6$

$5 \equiv 45 \mod 10$ tak

bo $10 \mid (5-45)$

$17 \not\equiv 3 \mod 5$

bo $5 \nmid (17-3)$

Kongruencje własności

Własności

Niech $a, b, c, d \in \mathbb{Z}$ oraz $n \in \mathbb{N}^*$

1) $a \equiv a \mod n$ (zwrotność)

2) $a \equiv b \mod n \Rightarrow b \equiv a \mod n$ (symetria)

3) $a \equiv b \mod n \wedge b \equiv c \mod n \Rightarrow$
$\Rightarrow a \equiv c \mod n$ (przechodniość)

np.

$a \equiv b \mod n \Leftrightarrow n \mid a-b$ (α)

$b \equiv c \mod n \Leftrightarrow n \mid b-c$ (β)

(α) $\exists_{k \in \mathbb{Z}}\ a-b = k \cdot n$

(β) $\exists_{l \in \mathbb{Z}}\ b-c = l \cdot n$

Mamy

$a-c = (a-b)+(b-c) = k \cdot n + l \cdot n =$
$= (k+l) \cdot n$

Zatem $l \mid a-c$

Relacje przystawania

* Relacja przystawania jest relacją równoważności.

Zbiór klas abstrakcji $\mathbb{Z}/_{\equiv}$ relacji przystawania według modułu n nazywamy jest pierścieniem reszt i oznaczamy symbolem $\mathbb{Z}_n$. W pierścieniu $\mathbb{Z}_n$ definiujemy działania dodawania i mnożenia następująco $[a] +_n [b] = [a+b]$

$[a] \cdot_n [b] = [a \cdot b]$

$\mathbb{Z}_n$ ma n elementów

Elementy te są reprezentowane przez liczby $0, 1, 2 \dots n-1$

$+_n$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$= n=4$

$a +_n b = (a+b) \bmod n$

$a \cdot_n b = (a \cdot b) \bmod n$

$\cdot_n$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$= n=4$

Relacje własności

* Własności

Niech $a, b, c, d \in \mathbb{Z}$, $n \in \mathbb{N}^+$

1) Jeżeli $a \equiv b \bmod n$

i $c \equiv d \bmod n$

to $a + c \equiv (b + d) \bmod n$

oraz $(a \cdot c) \equiv (b \cdot d) \bmod n$

2) Jeśli $a \equiv b \bmod n$ oraz $k \in \mathbb{N}$

to $a^k \equiv b^k \bmod n$

Kongruencje Przystawanie znajdowanie ostatniej cyfry

Znajdowanie ostatniej cyfry liczby naturalnej poprzez przystawanie mod 10

174 ostatnia cyfra to $c = 4$

$174 - c = 170 \wedge 10 | 170$

Stąd ~~174 przystaje~~

$174 \equiv 4 \mod 10$

Przypuśćmy, że c jest jakąc cyfrą $c \in \{0, 1 \dots 9\}$ oraz, że

$174 \equiv c \mod 10 \Leftrightarrow 10 | (174 - c)$

$\Rightarrow c = 4 \Rightarrow c$ - ostatnia cyfra 174

Każda liczba naturalna przystaje do swojej ostatniej cyfry według mod 10 oraz jeśli liczba N przystaje do pewnej cyfry mod 10

to cyfra ta jest jej ostatnią cyfrą

Kongruencje przykład

Zadanie: Znajdź ostatnią cyfrę liczby 2^{1000}

$2^5 = 32 \equiv 2 \mod 10$ — ~~wszę~~ pomijamy mod 10 → przy 2 łatwiejszy zapis

$2^5 \equiv 2 \quad /(\ )^5$

$2^{25} \equiv 2^5 \equiv 2 \mod 10$

$2^{25} \equiv 2 \quad /(\ )^5$

$2^{125} \equiv 2^5 \equiv 2$

$2^{125} \equiv 2 \quad /(\ )^5$

$2^{625} \equiv 2^5 \equiv 2$

$2^{625} \equiv 2$

$2^{1000} = 2^{625+375} = 2^{625} \cdot 2^{375} =$

$= 2^{625} \cdot 2^{3 \cdot 125} = 2^{625} \cdot (2^{125})^3 \equiv$

$\equiv 2 \cdot (2)^3 = 2^4 = 16 \equiv 6$

Zasadnicze twierdzenie w teorii kongruencji

Małe twierdzenie fermata

*1) Małe twierdzenie Fermata

Niech $a \in \mathbb{N}^*$ oraz $p \in \mathbb{P}$

Załóżmy, że $p \nmid a$ $[(a,p)=1]^*$

Wówczas $a^{p-1} \equiv 1 \mod p$

Np.

$p=5$, $a=3$ $(3,5)=1$

$3^{5-1}=3^4$

$3^{5-1}-1=80$

$5 \mid 80 \Rightarrow 3^{5-1} \equiv 1 \mod 5$

Wniosek:

Dla dowolnych $a \in \mathbb{N}^*$, $p \in \mathbb{P}$

mamy $a^p \equiv a \mod p$

np $3^7 \equiv 3 \mod 7$

Twierdzenie Wilsona

*2) Tw Wilsona

Jeśli $p \in \mathbb{P}$ to $(p-1)! \equiv -1 \mod p$

Np.

$p = 7$

$(7-1)! = 6! = 720$

$720 - (-1) = 721$

$7 \mid 721$

Względnie

Działania wewnętrzne dodawanie mnożenie w zbiorach

Niech $A \neq \emptyset$ Działaniem $\circ$ w A nazywamy działanie odwzorowanie $\circ : A \times A \to A$.

Piszemy $a \circ b$ zamiast $\circ(a,b)$, dla $a, b \in A$

Np. Zwykłe dodawanie, mnożenie są działaniami w zbiorach $\mathbb{R}$, liczb wymiernych, $\mathbb{Z}$ ale np. w zbiorze liczb niewymiernych $\mathbb{R} \setminus \mathbb{Q}$ bo ani dodawanie ani mnożenie nie jest działaniem wewnętrznym dla $x = \sqrt{2}$, $y = -\sqrt{2}$ $x, y \in \mathbb{R} \setminus \mathbb{Q}$ oraz $x + y = 0 \in \mathbb{Q}$, $x \cdot y = -2 \in \mathbb{Q}$

Działaniami wewnętrznymi są też $+_n$, $\cdot_n$ w zbiorze $\mathbb{Z}_n$

Jeżeli $X = \emptyset$ oraz $F(X)$ = zbiór funkcji $f: X \to X$ to operacja składania funkcji jest działaniem wewnętrznym

Grupa grupy Definicja

Grupa $(G, \circ)$ jest grupą gdy

1) $\circ$ jest łączne tzn

$$\forall_{a,b,c \in G} \; (a \circ b) \circ c = a \circ (b \circ c)$$

2) $\circ$ posiada element neutralny tzn

$$\exists_{e \in G} \forall_{a \in G} \; a \circ e = e \circ a = a$$

3) każdy element jest odwracalny tzn

$$\forall_{a \in G} \exists_{b \in G} \; a \circ b = b \circ a = e$$

Element $b \in G$ z pkt. 3 nazywamy odwrotnym i oznaczamy przez a^{-1}

Grupa abelowa nieabelowa

Grupę $(G, \circ)$ nazywamy abelową (przemienną) gdy działanie $\circ$ jest abelowe tz. spełniony jest warunek

4) $\forall_{a,b \in G} \; a \circ b = b \circ a$

Grupami abelowymi są $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Z}, +)$ w grupach tych elementem neutralnym jest $e = 0$

$(\mathbb{R}^*, \cdot)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}_{>0}, \cdot)$, $(\mathbb{Q}_{>0}, \cdot)$

Przykład grupy nieabelowej:
Permutacje: $(Perm(X), \circ)$, $e = id_X$ (#
$f \in Perm(X) \Leftrightarrow f \in F(X)$, f jest

Grupy macierzowe

Przykłady grup macierzowych:

1) $GL(n) = \{A \in M(n) : \det A \neq 0\}$

pełna grupa liniowa

$GL(n)$ jest nieabelowa gdy $n \geq 2$

2) $SL(n) = \{A \in M(n) : \det A = 1\}$

specjalna grupa liniowa

$SL(n)$ jest nie abelowa gdy $n \geq 2$

3) $O(n) = \{A \in M(n) : A \cdot A^T = Id\}$

4) $SO(n) = \{A \in M(n) : A \cdot A^T = Id \wedge \det A = 1\}$

specjalna grupa ortogonalna (wy gr. obrot)

~~grup~~ 3 i 4 są nieabelowe gdy $n \geq 3$

Grupą nie jest zbiór $(\mathbb{R}, \cdot)$ $(\mathbb{Q}, \cdot)$

$(\mathbb{R}_{<0}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{N}, +)$

Definicja podgrupy

* Def podgrupy

Niech $(G, \circ)$ będzie grupą oraz $H \subset G$

H jest podgrupą G gdy, $(H, \circ_H)$ jest grupą, gdzie $\circ_H = \circ|_{H \times H}$ ← obcięcie

Własność Niech $(G, \circ)$ będzie grupą oraz $H \subset G$. H jest podgrupą $G \Leftrightarrow$

$$\Leftrightarrow \forall_{a,b \in H} \; a \circ b^{-1} \in H \qquad (*)$$

$(*) \Leftrightarrow (*1) \wedge (*2)$ gdzie

$(*1) \; \forall_{a,b \in H} \; a \circ b \in H$

$(*2) \; \forall_{a \in H} \; a^{-1} \in H$

Oznaczenie

$H \leq G$

H jest podgrupą G

$(H, \circ) \leq (G, \circ)$ ← działanie

Przykłady:

$(\mathbb{Q}, +) \leq (\mathbb{R}, +)$

$(\mathbb{Z}, +) \leq (\mathbb{Q}, +)$

$(\mathbb{Q}_{>0}, \cdot) \leq (\mathbb{Q}^*, \cdot)$

$SL(n) \leq GL(n)$

$SO(n) \leq O(n)$

$O(n) \leq GL(n)$

$SO(n) \leq SL(n) \leq GL(n)$

Algebra Liniowa

ALGEBRA LINIOWA

*Macierzą typu $m \times n$ będziemy utożsamiać z tablicą prostokątną posiadającą m wierszy i n kolumn

$$m\{[A]\}^{n}$$

Elementy ustawione w tej tablicy będziemy nazywali wyrazami macierzy. Wyraz stojący w macierzy A na i-tym wierszu i w j-tej kolumnie a_{ij} lub a_{ij}. Symbolicznie taką macierz zapisujemy $A = [a_{ij}]_{\substack{i=1 \dots m \\ j=1 \dots n}}$

Zbiór wszystkich macierzy typu $m \times n$ oznaczamy $M(m, n)$

Dwie macierze tego samego typu można do siebie dodać. Wynikiem dodawania jest macierz tego samego typu której wyrazami są sumy wyrazów dodawanych macierzy.

Macierz można pomnożyć przez dowolną liczbę mnożąc każdy z wyrazów przez tę liczbę

Uwaga! Nie można dodawać macierzy dwóch różnych typów

Macierz typu $m \times n$ nazywamy macierzą kwadratową stopnia n i piszemy $M(n)$ zamiast $M(m, n)$

$$A = \begin{bmatrix} 2 & 1 \\ 3 & 0 \\ 5 & -1 \end{bmatrix} = M(3,2) \qquad B = \begin{bmatrix} 3 & 2 & 1 \\ 0 & 2 & 4 \end{bmatrix} \in M(2,3) \qquad C = \begin{bmatrix} 4 & 1 \\ -1 & 2 \end{bmatrix} \in M(2)$$

$$D = \begin{bmatrix} 1 \\ 5 \\ 0 \\ 3 \end{bmatrix} \in (4,1) \qquad E = \begin{bmatrix} 1 & 7 & 3 \end{bmatrix} \in (1,3) \qquad G = \begin{bmatrix} 2 & -1 \\ 0 & 5 \\ 4 & 2 \end{bmatrix} \in M(3,2)$$

$$H = \begin{bmatrix} 2 & 3 \\ 5 & 1 \end{bmatrix}$$

$$A + G = \begin{bmatrix} 4 & 0 \\ 3 & 5 \\ 9 & 1 \end{bmatrix}$$

$$2A = \begin{bmatrix} 4 & 2 \\ 6 & 0 \\ 10 & -2 \end{bmatrix}$$

Transpozycja macierzy (macierz transponowana)

Macierz transponowana powstaje z wyjściowej macierzy ~~po~~ poprzez zamianę jej wierszy na kolumny (to co było pierwszym wierszem starej macierzy staje się pierwszą kolumną nowej macierzy

$$A = \begin{bmatrix} 2 & 1 \\ 3 & 0 \\ 5 & -1 \end{bmatrix} \qquad A^T = \begin{bmatrix} 2 & 3 & 5 \\ 1 & 0 & -1 \end{bmatrix}$$

$$C = \begin{bmatrix} 4 & 1 \\ 1 & 2 \end{bmatrix} \qquad C^T = \begin{bmatrix} 4 & -1 \\ 1 & 2 \end{bmatrix}$$

* Mnożenie dwóch macierzy

Niech macierz $A \in M(m, k)$, $B = M(k, n)$

$$A = [a^i_r] \qquad B = [b^r_j]$$

Iloczyn macierzy $A \cdot B$ jest to macierz $C = [c^i_j] \in M(m, n)$ której wyrazy dane są wzorem

$$\boxed{c^i_j = \sum_{r=1}^{k} a^i_r \cdot b^r_j}$$

$$m\left\{\left[\overbrace{\quad A \quad}^{k}\right]\right. \left.\left[\overbrace{\quad B \quad}^{n}\right]\right\}k = \left[\overbrace{\quad C \quad}^{n}\right]\}m$$

Żeby sprawnie pomnożyć macierze trzeba opanować

$$A \cdot B = \begin{bmatrix} 2 & 1 \\ 3 & 0 \\ 5 & -1 \end{bmatrix} \cdot \begin{bmatrix} 3 & 2 & 1 \\ 0 & 2 & 4 \end{bmatrix} = \begin{bmatrix} 2\cdot 3 + 1\cdot 0, & 2\cdot 2 + 1\cdot 2, & 2\cdot 1 + 1 \\ & & \\ & & \end{bmatrix}$$

$$= \begin{bmatrix} 2\cdot 3+1\cdot 0 & 2\cdot 2+1\cdot 2 & 2\cdot 1+1\cdot 4 \\ 9 & 6 & 3 \\ 15 & 8 & 1 \end{bmatrix}$$

$$B\cdot A = \begin{bmatrix} 3 & 2 & 1 \\ 0 & 2 & 4 \end{bmatrix} \cdot \begin{bmatrix} 2 & 1 \\ 3 & 0 \\ 5 & -1 \end{bmatrix} = \begin{bmatrix} 17 & 2 \\ 26 & -4 \end{bmatrix}$$

F 1

D 1

$$C\cdot H = \begin{bmatrix} 4 & 1 \\ -1 & 2 \end{bmatrix} \begin{bmatrix} 2 & 3 \\ 5 & 1 \end{bmatrix} = \begin{bmatrix} 13 & 13 \\ 8 & -1 \end{bmatrix}$$

$$H\cdot C = \begin{bmatrix} 2 & 3 \\ 5 & 1 \end{bmatrix} \begin{bmatrix} 4 & 1 \\ -1 & 2 \end{bmatrix} = \begin{bmatrix} 5 & 8 \\ 19 & 7 \end{bmatrix}$$

F · D

D 4

F

Mnożenie macierzy jest nieprzemienne

——— || ——— jest działaniem wewnętrznym w zbiorze macierzy stopnia n

Mnożenie macierzy jest łączne, zachodzi dla każdych 3 macierzy jeśli tylko dadzą się pomnożyć

W przypadku macierzy kwadratowych stopnia n wyróżniamy macierz identycznościową (jednostkową) które jest

elementem neutralnym mnożenia macierzy

$$I_n = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$I_2 \cdot C = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 4 & 1 \\ -1 & 2 \end{bmatrix} = \begin{bmatrix} 4 & 1 \\ -1 & 2 \end{bmatrix}$$

* Macierz kwadratowa $A \in M(n)$ jest odwracalna $\iff \underset{B \in M(n)}{\exists} \; A \cdot B = B \cdot A = I_n$

Macierz B oznaczamy A^{-1}

W przeciwieństwie do liczb gdzie nieodwracalne jest tylko 0 istnieje bardzo wiele macierzy nieodwracalnych

Zbiór macierzy odwracalnych stopnia n oznaczamy $GL(n)$ i nazywamy pełną grupą liniową (gr. ze względu na mnożenie macierzy)

* Wyznacznik macierzy kwadratowej

O wyznaczniku możemy mówić tylko w przypadku macierzy kwadratowej

Wyznacznik macierzy jest liczbą

* Def rekurencyjna wyznacznika – rozwinięcie Laplace'a

1) Jeśli macierz $A = [a_1^1] \in M(1)$ to wyznacznik macierzy $\det A = a_1^1$

2) Jeśli $A = [a_j^i]$ $i, j = 1, n$, $n \geq 2$, to

$$\det A = \sum_{j=1}^{n} a_j^1 A_j^1,$$ gdzie

A_j^1 jest $(1, j)$ dopełnieniem algebraicznym macierzy A tj.

$$A_j^1 = (-1)^{1+j} M_j^1,$$

gdzie M_j^1 jest minorem macierzy A tj. M_j^1 jest wyznacznikiem macierzy powstałej z macierzy A poprzez wyjęcie 1-go wierszavi j-tej komórki

Powyższe rozwinięcie jest rozwinięciem względem pierwszego wiersza.
Taką samą wartość wyznacznika otrzymamy rozwijając go względem dowolnego wiersza lub dowolnej kolumny

* Wyznacznik macierzy stopnia 2

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

minor (wykreślenie)

$$\det A = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = a \cdot (-1)^{1+1} \cdot \det[d] + b \cdot (-1)^{1+2} \cdot \det[c] = a \cdot d - b \cdot c$$

Przykład

$$\begin{vmatrix} 2 & 5 & 1 \\ 0 & 3 & 2 \\ 4 & 5 & 0 \end{vmatrix} = 1 \cdot (-1)^{3} \cdot \begin{vmatrix} 0 & 3 \\ 4 & 5 \end{vmatrix} + 2 \cdot (-1)^{2+3} \cdot \begin{vmatrix} 2 & 5 \\ 4 & 5 \end{vmatrix} + \underbrace{0 \cdot (-1)^{3+3} \cdot \begin{vmatrix} 2 & 5 \\ 0 & 3 \end{vmatrix}}_{0} = \begin{vmatrix} 0 & 3 \\ 4 & 5 \end{vmatrix} - 2 \begin{vmatrix} 2 & 5 \\ 4 & 5 \end{vmatrix} =$$

$$= (0 \cdot 5 - 3 \cdot 4) - 2(2 \cdot 5 - 4 \cdot 5) =$$

$$= -12 + 20 = 8$$

Metoda obliczania

* Metoda obliczania wyznacznika stopnia 3 - wzór Sarusa

$$\begin{vmatrix} 2 & 5 & 1 \\ 0 & 3 & 2 \\ 4 & 5 & 0 \end{vmatrix} = 2\cdot 3\cdot 0 + 0\cdot 5\cdot 1 + 4\cdot 5\cdot 2 - 0\cdot 5\cdot 0 - 2\cdot 5\cdot 2 - 4\cdot 3\cdot 1 =$$

dopisujemy pierwsze 2 wiersze

$$\begin{matrix} 2 & 5 & 1 \\ 0 & 3 & 2 \end{matrix} \qquad = 40 - 20 - 12 = 8$$

$$\begin{vmatrix} 5 & 1 & 0 & 3 \\ 2 & 0 & 5 & -7 \\ 0 & 3 & 0 & 2 \\ -2 & -1 & 5 & 4 \end{vmatrix} = 3\cdot(-1)^{3+2}\begin{vmatrix} 5 & 0 & 3 \\ 2 & 5 & -7 \\ -2 & 5 & 4 \end{vmatrix} + 2\cdot(-1)^{3+4}\cdot\begin{vmatrix} 5 & 1 & 0 \\ 2 & 0 & 5 \\ -2 & -1 & 5 \end{vmatrix} = -3\begin{vmatrix} 5 & 0 & 3 \\ 2 & 5 & -7 \\ -2 & 5 & 4 \end{vmatrix} - 2\begin{vmatrix} 5 & 1 & 0 \\ 2 & 0 & 5 \\ -2 & -1 & 5 \end{vmatrix} =$$

$$= -3\cdot 335 - 2\cdot 5 = -1005 - 45 = -1050$$

$$\begin{matrix} 5 & 0 & 3 \\ 2 & 5 & -7 \\ -2 & 5 & 4 \\ 5 & 0 & 3 \\ 2 & 5 & -7 \end{matrix}$$

$5\cdot 5\cdot 4 + 2\cdot 5\cdot 3 +$
$- 3\cdot 5\cdot(-2) - (-7)\cdot 5\cdot 5 =$
$= 100 + 30 + 30 + 175 =$
$= 335$

Metoda elimiacji gaussa dla wyznaczników

* Metoda eliminacji Gaussa dla wyznaczników

Operacje elementarne na wierszach i kolumnach wyznacznika

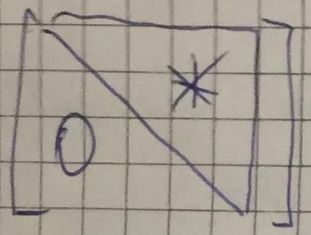
1) Zamiana 2 wierszy (kolumn) wyznacznika powoduje zmianę znaku wyznacznika na przeciwny

2) pomnożenie wybranego wiersza (kolumny) wyznacznika przez liczbę rzeczywistą powoduje pomnożenie wartości wyznacznika przez tę liczbę

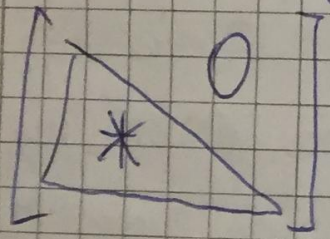
3) dodanie do wybranego wiersza (kolumny) wyznacznika dowolnej wielokrotności innego wiersza (kolumny) wyznacznika <u>nie</u> powoduje zmiany wartości wyznacznika

* Wyznacznik macierzy górnej trójkątnej dolnej Δ, diagonalnej równy jest iloczynowi wyrazów na głównej diagonali macierzy

Górna trójkątna



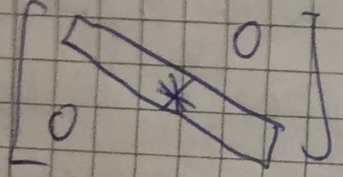
Dolna trójkątna



$$B = \begin{bmatrix} 2 & 0 & 0 \\ 1 & 5 & 0 \\ 8 & -2 & 4 \end{bmatrix}$$

$$\det B = 2 \cdot 5 \cdot 4 = 40$$

Diagonalna



$$C = \begin{bmatrix} 5 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\det C = 5 \cdot 1 \cdot 1 = 5$$

$$A = \begin{bmatrix} 2 & 5 & -8 \\ 0 & 1 & \sqrt{2} \\ 0 & 0 & 3 \end{bmatrix} \qquad \det A = 2 \cdot 1 \cdot 3 = 6$$

$$\begin{vmatrix} 2 & 5 & 1 \\ 0 & 3 & 2 \\ 4 & 5 & 0 \end{vmatrix} \xrightarrow{W_3 \to W_3 - 2W_1} \begin{vmatrix} 2 & 5 & 1 \\ 0 & 3 & 2 \\ 0 & -5 & -2 \end{vmatrix} \xrightarrow{W_2 \to \frac{1}{3} W_2}$$

$$3 \begin{vmatrix} 2 & 5 & 1 \\ 0 & 1 & \frac{2}{3} \\ 0 & -5 & -2 \end{vmatrix} \xrightarrow{W_3 \to W_3 + 5W_2} 3 \cdot \begin{vmatrix} 2 & 5 & 1 \\ 0 & 1 & \frac{2}{3} \\ 0 & 0 & \frac{4}{3} \end{vmatrix} =$$

$$= \cancel{3} \cdot 2 \cdot 1 \cdot \frac{4}{\cancel{3}} = 8$$

Własności det

* Twierdzenie. Następujące warunki są równoważne:

1) macierz jest odwracalna
2) wyznacznik macierzy jest różny od 0
3) rząd macierzy jest maksymalny

* Własność.

- jeżeli w macierzy występuje wiersz (kolumna) zerowa to wyznacznik tej macierzy jest równy 0. Wynika stąd oraz operacji elementarnej 3) że jeśli w macierzy występują 2 takie same wiersze lub 2 takie same kolumny to wyznacznik tej macierzy równy jest 0
- Dla $A \in M(n)$, $\det A = \det(A^T)$

$\det(A+B) \neq \det A + \det B$

* Tw. Cauchy'ego o mnożeniu wyznaczników

Niech $A, B \in M(n)$. Wówczas ~~wyzn~~

$$\det(A \cdot B) = \det(A) \cdot \det(B)$$

np.

$$A = \begin{bmatrix} 2 & 1 \\ 3 & 1 \end{bmatrix} \quad B = \begin{bmatrix} 4 & 2 \\ 1 & 1 \end{bmatrix}$$

$$A \cdot B = \begin{bmatrix} 2 & 1 \\ 3 & 1 \end{bmatrix} \cdot \begin{bmatrix} 4 & 2 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 9 & 5 \\ 13 & 7 \end{bmatrix}$$

$$\det(A \cdot B) = 9 \cdot 7 - 5 \cdot 13 = -2$$

$$\det A = -1 \qquad \det B = 2$$

*Wyznacznik macierzy odwrotnej

Niech $A \in \underbrace{GL(n)}_{\text{macierz odwracalna}}$ ~~wówczas~~ zatem

$$A \cdot A^{-1} = \underline{I} \leftarrow \text{identyczność}$$

Z tw. Cauchy'ego mamy

$$\det(A \cdot A^{-1}) = \det(I) = \det \begin{bmatrix} 1 & & & 0 \\ & 1 & & \\ & & 1 & \\ 0 & & & \ddots \; 1 \end{bmatrix} =$$

~~det(A)~~

det(A) * det(A^-1) = 1 ==>

==> det A^-1 = $\frac{1}{\det A}$

* Wyznaczanie macierzy odwrotnej za pomocą metody Cramera

Niech $A \in GL(n)$ wówczas

$$A^{-1} = \frac{1}{\det A} \cdot \begin{bmatrix} A^1_1 & A^1_2 & \cdots & A^1_n \\ A^2_1 & \vdots & & \\ \vdots & & & \\ A^n_1 & \cdots & & A^n_n \end{bmatrix}^T$$

dopełnienie algebraiczne

macierz transponowana

np.

$A = \begin{bmatrix} 2 & 1 \\ 3 & 5 \end{bmatrix}$ $\det A = 7 \neq 0$ zatem $A \in GL(2)$

$$A^{-1} = \frac{1}{7} \cdot \begin{bmatrix} (-1)^{1+1}\det[5] & (-1)^{1+2}\det[3] \\ (-1)^{2+1}\det[1] & (-1)^{2+2}\det[2] \end{bmatrix}^T =$$

$A^i_j = (-1)^{i+j} M^i_j$

$$= \frac{1}{7}\begin{bmatrix} 5 & -3 \\ -1 & 2 \end{bmatrix}^T = \frac{1}{7}\begin{bmatrix} 5 & -1 \\ -3 & 2 \end{bmatrix} = \begin{bmatrix} \frac{5}{7} & -\frac{1}{7} \\ -\frac{3}{7} & \frac{2}{7} \end{bmatrix}$$

$$A \cdot A^{-1} = \begin{bmatrix} 2 & 1 \\ 3 & 5 \end{bmatrix} \begin{bmatrix} 5 & -1 \\ -3 & 2 \end{bmatrix} \cdot \frac{1}{7} = \frac{1}{7}\begin{bmatrix} 7 & 0 \\ 0 & 7 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Metoda Cramera

* Metoda Cramera rozwiązywania układu równań

Dotyczy to jedynie kwadratowych układów równań tzn. takich w których jest tyle samo równań co niewiadomych

$$\begin{cases} a_1^1 x^1 + a_2^1 x^2 + \dots + a_n^1 x^n = b^1 \\ a_1^2 x^1 \qquad\qquad\qquad\qquad = b^2 \\ a_1^n x^1 + \qquad\qquad + a_n^n x^n = b^n \end{cases}$$

Metoda Cramera CDN

I

I

I

I

V

Przyjmijmy $W = \det[a_j^i]$

W jest nazywamy wyznacznikiem układu

$$W_{x^i} = W_i = \begin{bmatrix} b^1 \\ b^2 \\ b^n \end{bmatrix}$$

wyznacznik macierzy powstałej z macierzy układu poprzez zastąpienie i-tej kolumny kolumną $\begin{bmatrix} b^1 \\ b^2 \\ b^n \end{bmatrix}$

Jeżeli $W \neq 0$ to układ nazywamy Cramerowskim. Układ ten ma dokładnie jedno rozwiązanie

$$x^1 = \frac{W_1}{W}$$

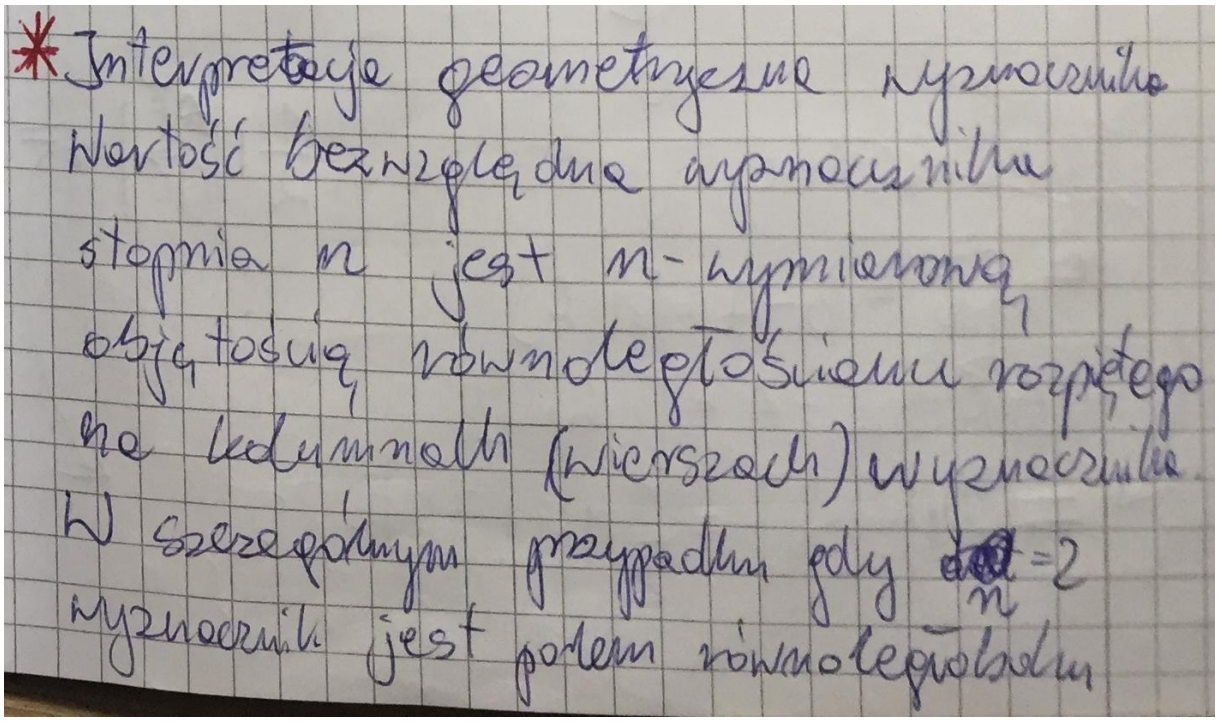
$$x^2 = \frac{W_2}{W}$$

$$x^3 = \frac{W_3}{W}$$

Jeżeli $W = 0$ oraz którykolwiek z $W_{x^i} \neq 0$ to układ jest sprzeczny (brak rozw.)

Jeżeli wszystkie wyznaczniki są równe 0 ~~układ jest nieoznaczony (ma nieskończenie rozwiązań)~~ to układ może być nieoznaczony albo sprzeczny

Interpretacja geometryczna wyznaczni



* Interpretacja geometryczna wyznacznika

Wartość bezwzględna wyznacznika stopnia n jest n-wymiarową objętością równoległościanu rozpiętego na kolumnach (wierszach) wyznacznika.

W szczególnym przypadku gdy $n=2$ wyznacznik jest polem równoległoboku

ka

Twierdzenie Kroneckera-Capellego

* Tw. Kroneckera-Capellego

1) Układ równań ma rozwiązania wtedy i tylko wtedy gdy rząd macierzy układu jest równy rzędowi macierzy rozszerzonej

2) Jeżeli układ równań z n niewiadomymi ma rozwiązanie to wymiar przestrzeni rozwiązań wynosi $n - r$ gdzie r jest rzędem macierzy układu.

Geometrycznie zbiór rozwiązań tego układu stanowi $n - r$ wymiarową płaszczyznę w R^n

Twierdzenie dla macierzy kwadratowej

* Tw. Dla macierzy kwadratowej następujące warunki są równoważne:

1) macierz jest odwracalna
2) wyznacznik różny od zera
3) macierz ma maksymalny rząd

Odwracanie macierzy za pomocą metody Gaussa

* Odwracanie macierzy za pomocą metody Gaussa

$A \in M(n)$

$$[A \mid J] \longrightarrow [J \mid A^{-1}]$$

$$[A \mid J_2] \longrightarrow \left[\begin{array}{cc|cc} 2 & 1 & 1 & 0 \\ 3 & 5 & 0 & 1 \end{array}\right] \xrightarrow{W_2 \to W_2 + W_1}$$

$$\to \left[\begin{array}{cc|cc} 2 & 1 & 1 & 0 \\ 1 & 4 & -1 & 1 \end{array}\right] \xrightarrow{W_1 \leftrightarrow W_2} \left[\begin{array}{cc|cc} 1 & 4 & -1 & 1 \\ 2 & 1 & 1 & 0 \end{array}\right] \xrightarrow{W_2 \to W_2 - 2W_1}$$

$$\to \left[\begin{array}{cc|cc} 1 & 4 & -1 & 1 \\ 0 & -7 & 3 & -2 \end{array}\right] \xrightarrow{W_2 \to -\frac{1}{7}W_2} \left[\begin{array}{cc|cc} 1 & 4 & -1 & 1 \\ 0 & 1 & -\frac{3}{7} & \frac{2}{7} \end{array}\right] \xrightarrow{W_1 \to W_1 - 4W_2}$$

$$\left[\begin{array}{cc|cc} 1 & 0 & \frac{5}{7} & -\frac{1}{7} \\ 0 & 1 & -\frac{3}{7} & \frac{2}{7} \end{array}\right]$$

Ślad macierzy kwadratowej

*Ślad macierzy kwadratowej nazywamy sumę wyrazów na przekątnej tej macierzy

$$A = [a_{ij}]_{i,j=1,n}$$

$$trA = \sum_{i=1}^{n} a_{ii}$$

Ślad

$$\rightarrow tr\begin{bmatrix} 2 & 7 \\ 1 & 4 \end{bmatrix} = 2 + 4 = 6$$

WŁASNOSC

Własność:

1) $tr(A \cdot B) = tr(B \cdot A)$

2) $tr(C \cdot A \cdot C^{-1}) = tr(A)$

Metoda eliminacji gaussa dla macierzy

* Metoda eliminacji Gaussa dla macierzy
Metoda ta polega na wykonywaniu operacji elementarnych na wierszach macierzy w celu sprowadzenia macierzy do postaci uproszczonej trójkątnej.

— Operacjami elementarnymi są:
1) zamiana kolejności dwóch wierszy macierzy
2) pomnożenie wybranego wiersza macierzy przez liczbę $\neq 0$
3) dodanie do wybranego wiersza macierzy dowolnej wielokrotności innego wiersza tej macierzy

Rzędem macierzy nazywamy liczbę jedynek wiodących postaci uproszczonej ~~tj~~ trójkątnej tej macierzy

Rząd macierzy jest niezmiennikiem przekształceń elementarnych tz. nie zależy od sposobu sprowadzenia macierzy do postaci uproszczonej trójkątnej za pomocą przekształceń elementarnych

Rząd macierzy rzad macierzy

Rząd macierzy równy jest wymiarowi przestrzeni liniowej rozpiętej na wierszach (kolumnach) tej macierzy

Zbadajmy powyższe ~~pojęcia~~ pojęcia na przykładzie macierzy ~~rów~~ układu równań

$$\begin{cases} 2x + y = 1 \\ x - y = 3 \end{cases}$$

$\cancel{y = -3 + x}$ $x = 3 + y$

$\cancel{2x - 3 + x = 1}$ $6 + 3y = 1$

$\cancel{3x = 4}$ $3y = -5$

$y = -\frac{5}{3}$

$x = \frac{9}{3} - \frac{5}{3} = \frac{4}{3}$

$$\begin{cases} 2x + y = 1 \\ x - y = 3 \end{cases}$$

$$\underbrace{\left[\begin{array}{cc|c} 2 & 1 & 1 \\ 1 & -1 & 3 \end{array}\right]}_{\text{macierz rozszerzona}}$$

$\underbrace{\begin{matrix} 2 & 1 \\ 1 & -1 \end{matrix}}_{\text{macierz układu}}$

$$\begin{cases} 1 \cdot x + 0 \cdot y = \frac{4}{3} \\ 0 \cdot x + 1 \cdot y = -\frac{5}{3} \end{cases}$$

metoda gaussa

$$\underbrace{\left[\begin{array}{cc|c} 1 & 0 & \frac{4}{3} \\ 0 & 1 & -\frac{5}{3} \end{array}\right]}_{\text{rząd 2}}$$

$$\left[\begin{array}{cc|c} 2 & 1 & 1 \\ 1 & -1 & 3 \end{array}\right] \xrightarrow{W_1 \leftrightarrow W_2} \left[\begin{array}{cc|c} 1 & -1 & 3 \\ 2 & 1 & 1 \end{array}\right] \xrightarrow{W_2 - 2W_1}$$

$$\rightarrow \left[\begin{array}{cc|c} 1 & -3 & 3 \\ 0 & 3 & -5 \end{array}\right] \xrightarrow{W_2 \to \frac{1}{3}W_2} \left[\begin{array}{cc|c} 1 & -1 & 3 \\ 0 & 1 & -\frac{5}{3} \end{array}\right]$$

$$\xrightarrow{W_1 \to W_1 + W_2} \begin{array}{c} \left[\begin{array}{cc|c} 1 & 0 & \frac{4}{3} \\ 0 & 1 & -\frac{5}{3} \end{array}\right] \\ x \quad y = \end{array} \quad \begin{cases} x = \frac{4}{3} \\ y = -\frac{5}{3} \end{cases}$$

W tym przypadku rząd macierzy układu ~~[illegible]~~ $= 2$ oraz rozszerzonej

$$\begin{cases} 2x + y - z = 0 \\ x - y + z = 3 \\ x + 2y - z = 4 \end{cases}$$

$$\left[\begin{array}{ccc|c} 2 & 1 & -1 & 0 \\ 1 & -1 & 1 & 3 \\ 1 & 2 & -1 & 1 \end{array}\right] \xrightarrow{W_1 \leftrightarrow W_3} \left[\begin{array}{ccc|c} 1 & 2 & -1 & 1 \\ 1 & -1 & 1 & 3 \\ 2 & 1 & -1 & 1 \end{array}\right]$$

$$\xrightarrow[W_3 \to W_3 - 2W_1]{W_2 \to W_2 - W_1} \left[\begin{array}{ccc|c} 1 & 2 & -1 & 1 \\ 0 & -3 & 2 & 2 \\ 0 & -3 & 1 & 2 \end{array}\right] \xrightarrow{W_2 \to -\frac{1}{3}W_2} \left[\begin{array}{ccc|c} 1 & 2 & -1 & 1 \\ 0 & 1 & -\frac{2}{3} & -\frac{2}{3} \\ 0 & -3 & 1 & 2 \end{array}\right]$$

$$\xrightarrow[W_3 \to W_3 + 3W_2]{W_1 \to W_1 - 2W_2} \left[\begin{array}{ccc|c} 1 & 0 & \frac{1}{3} & \frac{7}{3} \\ 0 & 1 & -\frac{2}{3} & -\frac{2}{3} \\ 0 & 0 & -1 & -4 \end{array}\right] \xrightarrow{W_3 \to -W_3} \left[\begin{array}{ccc|c} 1 & 0 & \frac{1}{3} & \frac{7}{3} \\ 0 & 1 & -\frac{2}{3} & -\frac{2}{3} \\ 0 & 0 & 1 & 4 \end{array}\right] \Rightarrow$$

$$\xrightarrow[w_2 \to w_2 + \frac{2}{3}w_3]{w_1 \to w_1 - \frac{1}{3}w_3} \left[\begin{array}{ccc|c} 1 & 0 & 0 & +1 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 4 \end{array}\right] \qquad \begin{cases} x = +1 \\ y = 2 \\ z = 4 \end{cases}$$

3 rzędy

3 rząd

$$\begin{cases} x + y - 3z = 1 \\ 2x + y + 4z = -2 \end{cases}$$

$$\left[\begin{array}{ccc|c} 1 & 1 & -3 & 1 \\ 2 & 1 & 4 & -2 \end{array}\right] \xrightarrow{w_2 = w_2 - 2w_1} \left[\begin{array}{ccc|c} 1 & 1 & 3 & 1 \\ 0 & -1 & 10 & -4 \end{array}\right] \xrightarrow{w_2 = w_2 \cdot -1}$$

$$\rightarrow \left[\begin{array}{ccc|c} 1 & 1 & 3 & 1 \\ 0 & 1 & -10 & 4 \end{array}\right] \xrightarrow{w_1 = w_1 - w_2} \left[\begin{array}{ccc|c} 1 & 0 & 7 & -3 \\ 0 & 1 & -10 & 4 \end{array}\right]$$

$$\begin{array}{ccc} x & y & z \\ & & \shortparallel \\ & & \alpha \end{array}$$

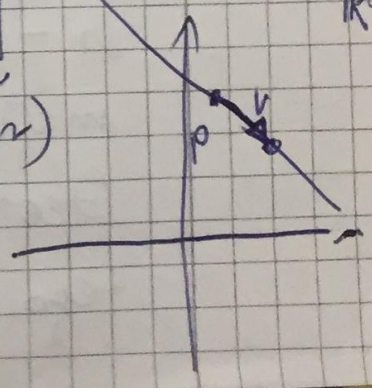
$$\begin{cases} x = -3 - 7\alpha \\ y = 4 + 10\alpha \\ z = \alpha, \ \alpha \in \mathbb{R} \end{cases}$$

$$(x, y, z) = (-3 - 7\alpha, 4 + 10\alpha, \alpha)$$

nawias nie zawiera α

$$= \underbrace{(-3, 4, 0)}_{p \text{ (punkt)}} + \alpha \underbrace{[-7, 10, 1]}_{V \text{ (wektor)}}$$

$$L(\alpha) = p + \alpha \cdot V \in \mathbb{R}^3$$



Pierścienie

* Pierścienie

Def Zbiór $(P, +, \cdot)$ nazywamy pierścieniem gdy

1) $(P, +)$ jest grupą abelową
2) a) zachodzi prawo rozdzielności

$$\forall_{a,b,c \in P} \quad (a+b)\cdot c = a\cdot c + b\cdot c$$
$$a\cdot(b+c) = a\cdot b + a\cdot c$$

b) $\cdot$ jest łączne tj

$$\forall_{a,b,c \in P} \quad (a\cdot b)\cdot c = a(b\cdot c)$$

Jeżeli dodatkowo

- $\cdot$ ma element neutralny to oznaczamy go przez 1 a pierścień nazywamy pierścieniem z jedynką
- jeśli $\cdot$ jest przemienne to pierścień nazywamy przemiennym
- jeśli $\cdot$ nie ma dzielników zera tz dla $\forall_{a,b \in P} (a \neq 0 \wedge b \neq 0 \Rightarrow a\cdot b \neq 0) \leq G$

to pierścień nazywamy bez dzielników zera

*Def Dziedziną całkowitości (pierścieniem całkowitym) nazywamy pierścień przemienny z jedynką bez dzielników zera np.

$(\mathbb{R}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{Z}, +, \cdot)$ pierścienie całkowite

$F(\mathbb{R}) = \{f: \mathbb{R} \to \mathbb{R}\}$

$(F(\mathbb{R}, +, \cdot)$ $(f+g)(x) = f(x) + g(x)$

$(f \cdot g)(x) = f(x) \cdot g(x)$

$F(\mathbb{R}, +, \cdot)$ – pierścień przemienny bo mnożenie przemienne

grupa jeden

$\mathbb{1}(x) \equiv 1$ pierścień przemienny z jedynką ~~z dzielnikiem~~

tożsame

$\mathbb{0}(x) \equiv 0$ z dzielnikiem 0

$(\mathbb{Z}, +_n, \cdot_n)$ pierścień przemienny z 1

$\mathbb{Z}_n = \{0, 1, \ldots n-1\}$ $a +_n b = (a+b) \bmod 4$

$a \cdot_n b = (a \cdot b) \bmod 4$

$\mathbb{Z}_n$ nie ma dzielników zera

$\iff n = p \in \mathbb{P}$ np $\mathbb{Z}_5, \mathbb{Z}_{11}, \mathbb{Z}_{1}$

Przykład pierścienia nieprzemiennego $(M(n), +, \cdot)$ $n \geq 2$ gdzie działaniami są dodawanie i odejmowanie macierzy.

Pojęcie ciała

* Pojęcie ciała

$(K, +, \cdot)$ jest ciałem gdy

1) $(K, +)$ jest grupą abelową
2) $(K^*, \cdot)$ jest gr. abelową
3) $\forall_{a,b,c \in K} \; a \cdot (b + c) = a \cdot b + a \cdot c$

Z def ciała wynika, że każdy pierścień jest ciałem, ale nie każde ciało pierścieniem np.

$(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ ← zespolone

ernione → $(\mathbb{H}, +, \cdot)$, $(\mathbb{Z}_p, +_p, \cdot_p)$

Pierścień wielomianów i ciała funkcji wymiernych

* Pierścień wielomianów i ciało funkcji wymiernych

$\mathbb{R}[x]$

$f \in \mathbb{R}[x] \quad f(x) = a_0 x^n + a_1 x^n \dots + a_{n-1} x + a_n$

np. $f(x) = 3x^7 + 5x + 8$

ciało funkcji wymiernych

$\mathbb{R}(x) \quad \varphi(x) = \frac{f(x)}{g(x)} \quad f, g \in \mathbb{R}[x]$

np. $\varphi(x) = \frac{5x^3 + x}{x^5 - x + 8}$

* Funkcje

$\forall_{x \in X} \exists_{y \in Y}! \quad (x, y) \in f$

$x f y$

$y = f(x)$

$(f \circ g)(x) = f(g(x))$

Grupa permutacji permutacje

* Grupa permutacji

Permutacją nazywamy dowolną bijekcję zbioru skończonego na siebie

Bijekcję nazywamy suriektywną i iniekcją

iniekcja – różnowartościowość

suriekcja – na

$S_1: \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

przechodzi na

$S_2: \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$

$S_3: \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

moc $\# S_1 = \overline{\overline{S}}_1 = 1$

$\overline{\overline{S}}_2 = 2$

$\overline{\overline{S}}_3 = 6 \qquad \overline{\overline{S}}_4 = 24$

Zbiór S_n wszystkich permutacji zbioru n elementowego ma n! elementów $\boxed{\overline{\overline{S}}_n = n!}$

$(S_n, \circ)$ S_n wraz z działaniem składanie permutacji stanowi grupę. Grupa ta jest nieabelowa (nieprzemienna) gdy $n \geq 3$. Elementem neutralnym w tej grupie jest permutacja identycznościowa

$$e = id_n = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}$$

* Mnożenie permutacji (składanie)

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

$\alpha, \beta \in S_5$

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

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

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

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

$$\alpha \circ \beta \neq \beta \circ \alpha$$

Permutacje cdn

* Technika znajdowania elementu odwrotnego

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

porządek

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

$$\alpha \circ \alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = id_5$$

* Rozkład permutacji na cykle i transpozycje

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 2 & 7 & 4 & 5 & 1 \end{pmatrix} =$$

α jest cyklem 7-mio elementowym ~~(wyk~~ (wszystko wykorzystane)

$$= (1\,3\,2\,6\,5\,4\,7)$$

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 1 & 2 & 6 & 3 & 4 & 7 \end{pmatrix} = (1\,5\,3\,2) \circ (4\,6) =$$

$$= (4\,6)(1\,5\,3\,2)$$

przyczo

- Mnożenie (składanie) cyklów rozłącznych jest przemienne
- Cykl 2-elementowy nazywamy transpozycją

Tw. Każdą permutację można rozłożyć na cykle (rozłączne) a każdy cykl można rozłożyć na transpozycje (nierozłączne)

W konsekwencji każdą permutację można przedstawić w postaci iloczynu transpozycji:

$\alpha = (1326547) = (13)(32)(26)(65)(54)(47)$

$\beta = (46)(1532) = (46)(15)(53)(32)$

Znak permutacji, parzystość permutacji:

$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 8 & 2 & 3 & 5 & 4 & 1 & 7 \end{pmatrix}$

liczby

własność znaku permutacji

Własność

1) $\operatorname{sgn}(id) = 1$

2) $\operatorname{sgn}(\alpha \circ \beta) = \operatorname{sgn}\alpha \cdot \operatorname{sgn}\beta$

3) $\operatorname{sgn}(\alpha^{-1}) = \operatorname{sgn}\alpha$

Tw cayleya

Tw Cayleya

Każda grupa skończona (mająca skończoną ilość elem) jest podgrupą pewnej grupy permutacji

Jest „podgrupą" należy rozumieć, że można ją zanurzyć w grupie permutacji

$G \leftarrow$ gr. skończona

$G = \{g_0, g_1, g_2, \dots g_k\} \rightarrow S_N = \{id_N, \alpha_1, \alpha_2, \dots \alpha_n$

Przestrzenie liniowe i odwzorowanie liniowe

Przestrzenie liniowe i odwzorowanie liniowe

Definicja przestrzeni liniowej

Układ $(V, +, \mathbb{K}, \cdot)$ nazywamy przestrzenią liniową (wektorową), ~~gdy~~ nad ciałem $\mathbb{K}$, gdy

I) $(V, +)$ jest grupą abelową

II) $\cdot : \mathbb{K} \times V \to V$ oraz spełnione są następujące warunki:

① $\forall_{a \in \mathbb{K}} \forall_{v, w \in V} \; a(v+w) = (av) + (aw)$

② $\forall_{a, b \in \mathbb{K}} \forall_{v \in V} \; (a+b)v = (av) + (bv)$

③ $\forall_{a, b \in \mathbb{K}} \forall_{v \in V} \; (ab)v = a(bv)$

④ $\forall_{v \in V} \; 1 \cdot v = v$

Elementy zbioru V nazywamy wektorami.
$+$ ma być w dodawaniu wektorem, natomiast
$\cdot$ – " – skalowaniem ich przez liczbę

Przykłady przestrzeni liniowych

Przykłady przestrzeni wektorowych:

- $(\mathbb{R}^n, +, \mathbb{R}, \cdot)$

$v, w \in \mathbb{R}^n \quad v = [v_1, \dots, v_n], \; w = [w_1, w_2, \dots, w_n]$

$v + w = [v_1 + w_1, v_2 + w_2, \dots, v_n + w_n]$

$a \in \mathbb{R} \quad a \cdot v = [a \cdot v_1, a \cdot v_2, \dots, a v_n]$

Wymiar przestrzeni $\mathbb{R}^n = n$

$\dim \mathbb{R}^n = n$

Przykład.

$\mathbb{R}[x]$ jest to przestrzeń liniowa wszystkich wielomianów.

$f, g \in \mathbb{R}[x]$

$f(x) = a_k x^k + a_{k-1} x^{k-1} + \dots + a_1 x^1 + a_0$

$g(x) = b_m x^m + b_{m-1} x^m + \dots + b_1 x^1 + b_0$

$c = \mathbb{R}$

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

$(cf)(x) = c(f(x)) = (ca_k)x^k + (ca_{k-1})x^{k-1} + \dots + (ca_0)$

$\mathbb{R}[x]$ jest przestrzenią liniową nieskończenie wymiarową.

$\dim \mathbb{R}[x] = +\infty$

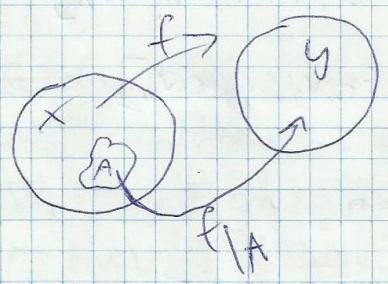
Podprzestrzeń liniowa

Niech V będzie przestrzenią liniową. ~~Podzbiór U~~

Podzbiór $U \subset V$ jest podprzestrzenią liniową, gdy

$(U, +|_{U \times U}, \mathbb{K}, \cdot|_{\mathbb{K} \times U})$ jest przestrzenią liniową

obcięto



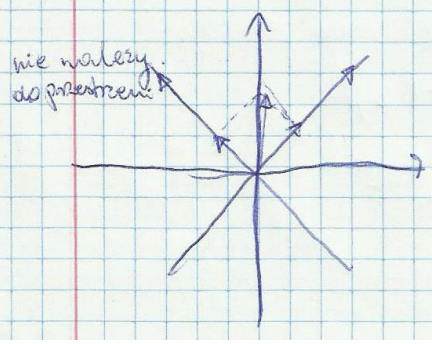
<u>Twierdzenie</u>

$U \subset V$ jest podprzestrzenią liniową V, gdy

$$\forall_{a,b \in \mathbb{K}} \ \forall_{u,w \in U} \quad au + bw \in U$$

Innymi słowy U jest podprzestrzenią liniową $V \iff$ dowolna kombinacja liniowa wektorów przestrzeni należy do U.

Wektor zerowy jest zawsze elementem każdej podprzestrzeni liniowej.



W dowolnej przestrzeni liniowej zbiór złożony z wektora zerowego jest podprzestrzenią liniową (trywialną) oraz cała przestrzeń jest podprzestrzenią liniową (nietrywialną). W przypadku przestrzeni $\mathbb{R}^n$ jej podprzestrzeniami są wszystkie k-wymiarowe płaszczyzny przechodzące przez środek układu współrzędnych.

Z twierdzenia Kronecker Capellego wynika, że każda taka podprzestrzeń jest zbiorem jednorodnego (kończący się zerami) układu równań liniowych o n-niewiadomych.

<u>Przykład podprzestrzeni liniowej w $\mathbb{R}[x]$</u>

Niech $U = \{ f \in \mathbb{R}[x] : f(1) = 0 \}$

Pokażemy, że U jest podprzestrzenią liniową.

Weźmy $f, g \in U$ oraz $a, b \in \mathbb{R}$ ~~ponieważ~~. Mamy pokazać, że $af + bg \in U$.

Ponieważ $f, g \in U \Rightarrow f(1) = 0 \wedge g(1) = 0$

Mamy

$$(af + bg)(1) = (af)(1) + (bg)(1) =$$
$$= a(f(1)) + b(g(1)) = a \cdot 0 + b \cdot 0 = 0$$

Stąd $af + bg \in U$.

Zatem U jest podprzestrzenią liniową.

Odwzorowanie liniowe

Niech $A: V \to W$, V, W - przestrzenie liniowe

Odwzorowanie A nazywane jest liniowym, gdy ~~dla~~

$$\forall_{v,u \in V} \ \forall_{a,b \in \mathbb{K}} \quad A(av + bu) = aA(v) + bA(u).$$

<u>Własność</u>

Niech $A: V \to W$ będzie odwzorowaniem liniowym

Połóżmy $\ker A = \{v \in V : A(v) = 0_W\}$ (jądro A)

oraz $\operatorname{im} A = \{A(v) : v \in V\}$ (obraz A)

Wówczas $\ker A \subset V$ jest podprzestrzenią liniową V oraz $\operatorname{im} A \subset W$ jest podprzestrzenią liniową W.

Co więcej jeśli ~~to~~ $\dim V < +\infty$, to

$$\dim V = \dim(\ker A) + \dim(\operatorname{im} A)$$

<u>Macierz odwzorowania liniowego</u>

Niech V, W będą skończenie wymiarowe oraz

$$A \in L(V, W) \text{ (liniowe pomiędzy } V \text{ i } W)$$

Niech $e = (e_i)_{i=1,\dots,m}$ będzie bazą V oraz $f = (f_j)_{j=1,\dots,m}$ będzie bazą W.

Wówczas dla dowolnego $i = 1, \dots, m$ mamy

$$A(e) = \sum_{k=1}^{m} a_i^k f_k$$

Połóżmy $A_{e,f} = [a_i^k]_{\substack{i=1,\dots,m \\ k=1,\dots,m}} \in M(m, n)$

Maierz odwzorowania liniowego

$A_{e,f}$ nazywamy macierzą odwzorowania liniowego A w bazach e i f.

Niech $v \in V$. Mamy

$$v = \sum_{s=1}^{n} v^s e_s$$

oraz połóżmy

$$C_e(v) = \begin{bmatrix} v^1 \\ v^2 \\ \vdots \\ v^n \end{bmatrix}$$ (wektor współrzędnych wektora v w bazie e)

Zbadajmy relację pomiędzy odwzorowaniem, a macierzą odwzorowania $A_{e,f}$ oraz wektorem współrzędnych $C_e(v)$

Mamy:

$$A(v) = A\left(\sum_{s=1}^{n} v^s e_s\right) = \sum_{s=1}^{n} v^s A(e_s) = \sum_{s=1}^{n} v^s \sum_{k=1}^{m} a_s^k f_k =$$

$$= \sum_{k=1}^{n}\left(\sum_{s=1}^{m} a_s^k v^s\right) f_k \iff C_f(A(v)) = A_{e,f}\, C_e(v)$$

Innymi słowy, jeśli działanie odwzorowania na wektor można utożsamić (przy ustalonych bazach) z mnożeniem macierzy odwzorowania przez wektor współrzędnych.

Analogicznie rachunek pokazuje, że:
Jeśli: $A \in L(V, W)$, $B \in L(W, U)$
oraz e, f, g są bazami przestrzeni V, W, U to
$B \circ A \in L(V, U)$ oraz
$(B \circ A)_{e,g} = B_{f,g} \cdot A_{e,f}$

Maierz odwzorowania liniowego CDN

Inaczej słowy:

1. Złożenie dwóch odwzorowań liniowych jest odwzor. liniow.
2. Składanie odwzor. lini. można utożsamić z mnożeniem macierzy tych odwzorowań.
3. Jeżeli odwzor. liniow. jest odwracalne to jego macierz jest również macierzą odwracalną.
   Co więcej odwzorowanie odwrotne do odwzorowania liniowego jest również odwzorowaniem odwrotnym a jego macierz jest macierzą odwrotną do macierzy odwzorowania.

Odwzorowanie liniowe w przestrzeni Euklisdesowej

Odwzorowanie liniowe w przestrzeni Euklidesowej

$A: \mathbb{R}^n \to \mathbb{R}^m$

$v = [x_1, x_2, \dots, x_n] \in \mathbb{R}^n$

$A(v) = A(x_1, \dots, x_n) = [y_1, y_2, \dots, y_m]$

$A \in L(\mathbb{R}^n, L^m) \Leftrightarrow \forall_{j=1,\dots,m}$

$y_j = a_1 x_1 + a_2 x_2 + \dots + a_n x_n$ (gdy $a_i \in \mathbb{R}$ są zależne od j)

Czy A jest odwzorowaniem liniowym?

$A(x,y) = (3x + y \;\; 1 \cdot x + 0y \;\; 7x - y)$ TAK

$A(x,y,z) = 7x + z = 7x + 0 \cdot y + 1 \cdot z =$ TAK

$A(x,y,z) = 2x + y + 3z + 1$ NIE

$A(x,y) = 0 = 0x + 0y$ TAK

$A(x,y,z) = x + yz$ NIE

Zadanie

Niech $A: \mathbb{R}^2 \to \mathbb{R}^3$, $A \in L(\mathbb{R}^2, \mathbb{R}^3)$

Wyznacz macierz odwzorowania A w bazie kanonicznej.

$A(1,0) = (3, 1, 7)$

$A(0,1) = (1, 0, -1)$

$$A = \begin{bmatrix} 3 & 1 \\ 1 & 0 \\ 7 & -1 \end{bmatrix}$$

Odwzorowanie liniowe w przestrzeni Euklisdesowej

Wyznacz:

$A: \mathbb{R}^3 \to \mathbb{R}^3$

$A(x,y,z) = (6x+z,\ 5x-9y+7z,\ 3x-y+4z)$

$A(1,0,0) = (6,5,3)$

$A(0,1,0) = (0,-9,-1)$

$A(0,0,1) = (1,7,4)$

$$\mathcal{A} = \begin{bmatrix} 6 & 0 & 1 \\ 5 & -9 & 7 \\ 3 & -1 & 4 \end{bmatrix}$$