Uzupełnienie wiadomości z algebry

Krzysztof Gdawiec

UNIWERSYTET ŚLĄSKI
INSTYTUT INFORMATYKI

Ciała

Definicja

Niepusty zbiór K z wyróżnionymi elementami 0 i 1 oraz działaniami $+ : K \times K \to K$ i $\cdot : K \times K \to K$ nazywamy *ciałem* jeśli dla wszystkich $a, b, c \in K$:

1. $a + (b + c) = (a + b) + c$,
2. $a + 0 = 0 + a = a$,
3. dla każdego $a \in K$ istnieje $b \in K$ takie, że $a + b = b + a = 0$,
4. $a + b = b + a$,
5. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$,
6. $a \cdot 1 = 1 \cdot a = a$,
7. $a \cdot b = b \cdot a$,
8. $a \cdot (b + c) = a \cdot b + a \cdot c$,
9. dla każdego $a \in K \setminus \{0\}$ istnieje $b \in K$ takie, że $a \cdot b = 1$.

Przykład

1. Ciałami są: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$, gdzie p jest liczbą pierwszą.
2. Ciałami **nie** są: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}_q$, gdzie q nie jest liczbą pierwszą.

Macierze

Definicja

Macierzą o n kolumnach i m wierszach nad ciałem K nazywamy każdą tablicę postaci

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix},$$

gdzie $a_{ij} \in K$ dla $i = 1, \dots, m$ oraz $j = 1, \dots, n$.
Zbiór macierzy o n kolumnach i m wierszach nad K oznaczamy K_m^n lub $K^{n \times m}$. Macierz, dla której liczba kolumn i wierszy jest taka sama nazywamy macierzą *kwadratową*.

Definicja

Podstawowe działania na macierzach definiujemy następująco:

- Dodawanie $+ : K_m^n \times K_m^n \to K_m^n$
$$A + B = [a_{ij} + b_{ij}],$$
gdzie $A = [a_{ij}], B = [b_{ij}] \in K_m^n$.
- Mnożenie macierzy przez elementy z ciała K czyli $\cdot : K \times K_m^n \to K_m^n$
$$a \cdot A = [aa_{ij}],$$
gdzie $a \in K$ oraz $A = [a_{ij}] \in K_m^n$.

- Mnożenie macierzy $\cdot : K_m^n \times K_n^r \to K_m^r$

$$A \cdot B = \left[\sum_{j=1}^{n} a_{ij} b_{jk}\right] = [c_{ik}],$$

gdzie $A \in K_m^n$, $B \in K_n^r$.
- Transpozycja macierzy $^T : K_m^n \to K_n^m$

$$A^T = [a_{ji}],$$

gdzie $A = [a_{ij}] \in K_m^n$.

Uwaga

Mnożenie macierzy nie jest przemienne.

Definicja

Macierzą *jednostkową* nazywamy macierz kwadratową, która na przekątnej ma jedynki, a poza przekątną zera. Oznaczamy ją przez I.

Definicja

Wyznacznikiem macierzy $A \in K_n^n$ nazywamy liczbę $\det A$ daną wzorem:

- jeśli $A = [a_{11}]$, to $\det A = a_{11}$,
- jeśli $A = [a_{ij}]$ i $n > 1$, to

$$\det A = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det A_{ij},$$

gdzie j to ustalona kolumna, A_{ij} to podmacierz macierzy A powstająca przez skreślenie i-tego wiersza i j-tej kolumny.

Definicja

Niech A będzie macierzą kwadratową stopnia n. Jeśli istnieje macierz A^{-1} taka, że spełnione są warunki

$$A \cdot A^{-1} = A^{-1} \cdot A = I,$$

to mówimy, że macierz A jest *odwracalna*, a macierz A^{-1} nazywamy *macierzą odwrotną* do A.

Twierdzenie

Niech A i B będą macierzami odwracalnymi tego samego stopnia, a $\alpha \neq 0$ będzie liczbą. Wówczas:

1. $\det(A^{-1}) = (\det A)^{-1}$,
2. $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$,
3. $(A^{-1})^{-1} = A$,
4. $(A^T)^{-1} = (A^{-1})^T$,
5. $(\alpha \cdot A)^{-1} = \frac{1}{\alpha} A^{-1}$.

Definicja

Macierz kwadratową A taką, że $\det A \neq 0$ nazywamy macierzą *nieosobliwą*. W przeciwnym przypadku macierz nazywamy *osobliwą*.

Twierdzenie

Macierz kwadratowa jest odwracalna $\iff$ jest nieosobliwa.

Definicja

Niech $A = [a_{ij}]$ będzie macierzą stopnia $n \geqslant 2$. Macierz

$$A^D = \begin{bmatrix} D_{11} & D_{12} & \dots & D_{1n} \\ D_{21} & D_{22} & \dots & D_{2n} \\ \dots & \dots & \dots & \dots \\ D_{n1} & D_{n2} & \dots & D_{nn} \end{bmatrix},$$

gdzie $D_{ij} = (-1)^{i+j} \det A_{ij}$ oraz A_{ij} jest macierzą powstałą przez skreślenie i-tego wiersza i j-tej kolumny, nazywamy *macierzą dopełnień algebraicznych*.

Twierdzenie

Jeśli macierz $A = [a_{ij}]$ *stopnia* n *jest nieosobliwa, to macierz* A^{-1} *wyraża się wzorem:*

$$A^{-1} = \frac{1}{\det A}(A^D)^T.$$

Przestrzenie liniowe

Definicja

Przestrzenią liniową (wektorową) nad ciałem K nazywamy dowolny niepusty zbiór V, na którym określone są działania $+ : V \times V \to V$ i $\cdot : K \times V \to V$, które spełniają następujące aksjomaty dla wszystkich $u, v, w \in V$ i $\alpha, \beta \in K$:

1. $v + w = w + v$,
2. $v + (w + u) = (v + w) + u$,
3. istnieje $0 \in V$ (wektor zerowy) taki, że $0 + v = v + 0 = v$,
4. dla każdego $v \in V$ istnieje $v' \in V$ taki, że $v + v' = v' + v = 0$,
5. $\alpha \cdot (v + w) = \alpha \cdot v + \alpha \cdot w$,
6. $(\alpha + \beta) \cdot v = \alpha \cdot v + \beta \cdot v$,
7. $\alpha \cdot (\beta \cdot v) = (\alpha\beta) \cdot v$,
8. $1 \cdot v = v$.

Przykład

Przestrzeniami liniowymi są:

1. zbiór $\mathbb{R}^n$ ze zwykłymi działaniami dodawania wektorów i mnożenia wektorów przez skalary jest przestrzenią liniową nad ciałem $\mathbb{R}$,
2. zbiór wielomianów jednej zmiennej $\mathbb{R}[X]$ z dodawaniem wielomianów i mnożeniem wielomianu przez skalar jest przestrzenią liniową nad ciałem $\mathbb{R}$,
3. zbiór funkcji ciągłych $C(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} : f \text{ jest ciągła}\}$ z działaniami:

$$(f+g)(x) = f(x) + g(x),$$
$$(\alpha f)(x) = \alpha \cdot f(x),$$

gdzie $f, g \in C(\mathbb{R})$ i $\alpha \in \mathbb{R}$, jest przestrzenią liniową nad ciałem $\mathbb{R}$.

Uwaga

Na zajęciach najważniejszą dla nas przestrzenią liniową, której będziemy używać, jest przestrzeń $\mathbb{R}^n$ nad $\mathbb{R}$.

Definicja

Niepusty podzbiór W przestrzeni liniowej V nad K nazywamy *podprzestrzenią* (liniową) przestrzeni V $\iff$

1. $v + w \in W$ dla każdego $v, w \in W$,
2. $\alpha \cdot v \in W$ dla każdego $\alpha \in K$ i $v \in W$.

Definicja

Kombinacją liniową wektorów $v_1, \ldots, v_m \in V$ nazywamy dowolny wektor postaci:

$$\alpha_1 v_1 + \ldots + \alpha_m v_m,$$

gdzie $\alpha_1, \ldots, \alpha_m \in K$.

Definicja

Dla niepustego zbioru $A = \{v_1, \ldots, v_m\} \subset V$ zbiór wszystkich kombinacji liniowych wektorów z A oznaczamy przez $lin(A)$, tzn.

$$lin(A) = \left\{ \sum_{i=1}^{m} \alpha_i v_i : \alpha_i \in K \wedge v_i \in A \right\}.$$

Definicja

Wektory $v_1, \ldots, v_m \in V$ nazywamy *liniowo niezależnymi* $\iff$

$$\forall_{\alpha_1, \ldots, \alpha_m \in K} \quad (\alpha_1 v_1 + \ldots + \alpha_m v_m = 0 \Rightarrow \alpha_1 = \ldots = \alpha_m = 0).$$

Jeżeli wektory $v_1, \ldots, v_m$ nie są liniowo niezależne, to mówimy, że są one *liniowo zależne*.

Definicja

Bazą przestrzeni liniowej V nazywamy zbiór B tej przestrzeni taki, że

1. B generuje całą przestrzeń, tj. $lin(B) = V$,
2. B składa się z wektorów liniowo niezależnych.

Definicja

Niech zbiór wektorów $\{b_1, \ldots, b_n\}$ będzie bazą przestrzeni liniowej V nad K. Wówczas mówimy, że *wymiar* przestrzeni V wynosi n i piszemy $\dim V = n$.

Twierdzenie

Niech $B = \{b_1, \ldots, b_n\}$ będzie bazą przestrzeni liniowej V nad K. Każdy wektor $v \in V$ jest jednoznaczną kombinacją liniową wektorów z bazy B, tzn.

$$v = \alpha_1 b_1 + \ldots + \alpha_m b_n,$$

gdzie współczynniki $\alpha_1, \ldots, \alpha_n \in K$ są wyznaczone jednoznacznie i nazywamy je współrzędnymi wektora v w bazie B.

Przykład

Wymiar przestrzeni $\mathbb{R}^n$ wynosi n, a wektory

$$\varepsilon_1 = [1, 0, \ldots, 0], \varepsilon_2 = [0, 1, 0, \ldots, 0], \ldots, \varepsilon_n = [0, \ldots, 0, 1]$$

tworzą bazę i nazywamy ją *bazą kanoniczną*.

Definicja

Niech V, W będą przestrzeniami liniowymi nad ciałem K. Funkcja $f : V \longrightarrow W$ jest *przekształceniem liniowym* $\iff$

1. $f(v_1 + v_2) = f(v_1) + f(v_2)$,
2. $f(a \cdot v) = a \cdot f(v)$,

dla każdych $v, v_1, v_2 \in V$ i $a \in K$.

Twierdzenie

Niech $B = \{b_1, \ldots, b_n\}$ będzie bazą przestrzeni V, a $\{v_1, \ldots, v_n\}$ układem wektorów z przestrzeni W. Wówczas istnieje dokładnie jedno przekształcenie liniowe $f : V \longrightarrow W$ takie, że dla każdego $i \in \{1, \ldots, n\}$

$$f(b_i) = v_i.$$

Przestrzenie euklidesowe

Definicja

Niech V będzie przestrzenią liniową nad ciałem K. Przekształcenie $\langle , \rangle : V \times V \to K$ nazywamy *iloczynem skalarnym*, gdy dla każdych $v, v_1, v_2 \in V$ i $a \in K$:

1. $\langle v_1, v_2 \rangle = \langle v_2, v_1 \rangle$,
2. $\langle v_1 + v_2, v \rangle = \langle v_1, v \rangle + \langle v_2, v \rangle$,
3. $\langle a v_1, v_2 \rangle = a \langle v_1, v_2 \rangle$,
4. $\langle v, v \rangle > 0$ dla $v \neq 0$.

Definicja

Przestrzeń liniową z wyróżnionym iloczynem skalarnym $(V, \langle , \rangle)$ nazywamy przestrzenią *euklidesową*.
Normę (długość) wektora $v \in V$ określamy następująco $\|v\| = \sqrt{\langle v, v \rangle}$.
Wektor, którego długość wynosi 1 nazywamy wektorem *unormowanym* (jednostkowym).

Uwaga

Każdy niezerowy wektor w przestrzeni euklidesowej V możemy unormować. Niech $v \in V$ i $v \neq 0$. Wówczas wektor $\frac{v}{\|v\|}$ ma długość 1.

Uwaga

Iloczyn skalarny ma następującą własność:

$$\langle v, w \rangle = \|v\| \|w\| \cos \varphi,$$

gdzie φ jest to kąt pomiędzy v i w.

Przykład

Przestrzeniami euklidesowymi są:

- $(\mathbb{R}^n, \langle , \rangle)$, gdzie $\langle v, w\rangle = \sum_{i=1}^n v_i w_i$ dla $v = [v_1, \ldots, v_n], w = [w_1, \ldots, w_n] \in \mathbb{R}^n$. Wówczas $\|v\| = \sqrt{\sum_{i=1}^n v_i^2}$ dla $v = [v_1, \ldots, v_n]$.
- przestrzeń wielomianów rzeczywistych stopnia co najwyżej n z iloczynem skalarnym $\langle p_1, p_2\rangle = \int_0^1 p_1(t)p_2(t)\,\mathrm{d}t$. Wówczas $\|p\| = \sqrt{\int_0^1 (p(t))^2\,\mathrm{d}t}$.

Definicja

Niech V będzie przestrzenią euklidesową z iloczynem skalarnym $\langle , \rangle$. Wektory $v, w \in V$ nazywamy *prostopadłymi* (ortogonalnymi) jeśli $\langle v, w\rangle = 0$.

Definicja

Ortogonalny układ wektorów niezerowych $\{v_1, \ldots, v_n\}$ przestrzeni euklidesowej $(V, \langle , \rangle)$ rozpinający V nazywamy *bazą ortogonalną* w V. Dodatkowo, jeśli $\|v_i\| = 1$ dla $i \in \{1, \ldots, n\}$ to bazę nazywamy *ortonormalną*.

Twierdzenie (ortogonalizacja Grama-Schmidta)

Niech $\{v_1, \ldots, v_n\}$ będzie liniowo niezależnym układem wektorów przestrzeni euklidesowej $(V, \langle , \rangle)$. Niech wektory $w_1, \ldots, w_n$ będą dane wzorem:

$$\begin{aligned} w_1 &= v_1, \\ w_k &= v_k - \sum_{i=1}^{k-1} \frac{\langle v_k, w_i \rangle}{\langle w_i, w_i \rangle} w_i \ \textit{dla } i = 2, \ldots, n. \end{aligned}$$

Wówczas dla każdych $i, j \in \{1, \ldots, n\}$ takich, że $i \neq j$ wektory w_i i w_j są ortogonalne oraz $lin(v_1, \ldots, v_n) = lin(w_1, \ldots, w_n)$.

Iloczyn wektorowy w $\mathbb{R}^3$

Definicja

Iloczynem wektorowym wektorów
$v = [v_1, v_2, v_3], w = [w_1, w_2, w_3] \in \mathbb{R}^3$ nazywamy wektor:

$$v \times w = \left[\det \begin{bmatrix} v_2 & v_3 \\ w_2 & w_3 \end{bmatrix}, \det \begin{bmatrix} v_3 & v_1 \\ w_3 & w_1 \end{bmatrix}, \det \begin{bmatrix} v_1 & v_2 \\ w_1 & w_2 \end{bmatrix}\right]$$
$$= [v_2 w_3 - v_3 w_2, v_3 w_1 - v_1 w_3, v_1 w_2 - v_2 w_1].$$

Uwaga

Iloczyn wektorowy ma następujące własności:

1. Jeśli $v \times w = 0$, to wektory v i w są równoległe.
2. Jeśli $v \times w \neq 0$, to wektor $v \times w$ jest prostopadły do v i w.
3. $\|v \times w\| = \|v\|\|w\| \sin \varphi$, gdzie φ jest to kąt pomiędzy v i w.
4. $\|v \times w\|$ jest to pole powierzchni równoległoboku, którego bokami są wektory v i w.
5. $v \times w = -w \times v$.
6. $v \times (w_1 + w_2) = v \times w_1 + v \times w_2$.

Przestrzenie afiniczne

Definicja

Przestrzenią afiniczną nad ciałem K nazywamy trójkę $A = (P, V, +)$, gdzie P jest niepustym zbiorem punktów, V jest przestrzenią liniową nad ciałem K, której elementy nazywamy wektorami swobodnymi nad K, a $+ : P \times V \to P$ jest operacją zaczepiania wektorów swobodnych w punktach taką, że

1. $p + 0 = p$ dla $p \in P$,
2. $(p + u) + v = p + (u + v)$ dla $p \in P$ i $u, v \in V$,
3. Dla każdej pary punktów $p, q \in P$ istnieje dokładnie jeden wektor $v \in V$ taki, że $p + v = q$ (będziemy go oznaczać $\overrightarrow{pq}$).

Wymiarem przestrzeni afinicznej będziemy nazywać wymiar jej przestrzeni liniowej, tzn. $\dim A = \dim V$.

Uwaga

Warunek 3 w definicji oznacza, że dla ustalonego $p \in P$ przyporządkowanie wektorowi $v \in V$ punktu $p + v \in P$ ustala wzajemnie jednoznaczną odpowiedniość między P i V. Operacją odwrotną jest przyporządkowanie punktowi q wektora $\overrightarrow{pq}$, punkt początkowy p odpowiada wektorowi zerowemu.

Przykład

Przykładem przestrzeni afinicznej, z której będziemy korzystać na zajęciach, jest: $A = (\mathbb{R}^n, \mathbb{R}^n, +)$, gdzie $+ : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$ dane jest wzorem:

$$(p_1, \ldots, p_n) + [v_1, \ldots, v_n] = (p_1 + v_1, \ldots, p_n + v_n),$$

gdzie $(p_1, \ldots, p_n)$ to punkt, a $[v_1, \ldots, v_n]$ to wektor.

Definicja

Niech $A = (P, V, +)$ będzie przestrzenią afiniczną oraz niech $p \in P$, a $U \subset V$ będzie podprzestrzenią przestrzeni wektorów swobodnych V. Zbiory postaci:

$$p + U = \{p + u : u \in U\}$$

nazywamy *podprzestrzeniami afinicznymi*. Dla tak zdefiniowanej podprzestrzeni afinicznej przestrzenią wektorów swobodnych jest $U = \{\overrightarrow{qr} : q, r \in p + U\}$, a wymiarem jest wymiar przestrzeni $p + U$.

Definicja

Układem bazowym w przestrzeni afinicznej $A = (P, V, +)$ nazywamy układ $(p; v_1, \dots, v_n)$ taki, że $p \in P$, a $\{v_1, \dots, v_n\}$ jest bazą V.

Definicja

Bazą punktową w przestrzeni afinicznej $A = (P, V, +)$ nazywamy układ punktów $(p_0, \dots, p_n)$ taki, że $(p_0; \overrightarrow{p_0 p_1}, \dots, \overrightarrow{p_0 p_n})$ jest układem bazowym w A.

Uwaga

Jeśli $(p_0, \ldots, p_n)$ jest bazą punktową przestrzeni afinicznej $A = (P, V, +)$, to punkt $q \in P$ można jednoznacznie zapisać w układzie bazowym $(p_0; \overrightarrow{p_0 p_1}, \ldots, \overrightarrow{p_0 p_n})$ w postaci:

$$q = p_0 + \sum_{j=1}^{n} \alpha_j \overrightarrow{p_0 p_j},$$

gdzie $\alpha_j \in K$.

Definicja

Niech $(p_0, \ldots, p_n)$ będzie bazą punktową przestrzeni afinicznej $A = (P, V, +)$. Wówczas kombinację postaci:

$$q = \sum_{j=0}^{n} \alpha_j p_j,$$

gdzie $\alpha_j \in K$ dla $j = 0, \ldots, n$ oraz $\sum_{j=0}^{n} \alpha_j = 1$ nazywamy *kombinacją afiniczną*. Wagi $\alpha_0, \ldots, \alpha_n$ nazywamy *współrzędnymi barycentrycznymi* punktu q.

Definicja

Niech $A_1 = (P_1, V_1, +_1)$ oraz $A_2 = (P_2, V_2, +_2)$ będą przestrzeniami afinicznymi nad tym samym ciałem K. Funkcję $f : A_1 \to A_2$ nazywamy *przekształceniem afinicznym* jeśli dla pewnego $p \in P_1$ istnieje przekształcenie liniowe $\overrightarrow{f} : V_1 \to V_2$ (zwane częścią liniową f) spełniające warunek

$$f(p +_1 v) = f(p) +_2 \overrightarrow{f}(v) \quad \text{dla } v \in V_1.$$

Definicja

Przestrzeń afiniczną $A = (P, V, +)$, gdzie V jest przestrzenią euklidesową z iloczynem skalarnym $\langle , \rangle$ nazywamy *afiniczną przestrzenią euklidesową*.

Definicja

Niech $A = (P, V, +)$ będzie afiniczną przestrzenią euklidesową. *Odległość* między punktami $p, q \in P$ definiujemy następująco:

$$d(p, q) = \|\overrightarrow{pq}\| = \sqrt{\langle \overrightarrow{pq}, \overrightarrow{pq} \rangle}.$$