Jacek Cichoń
Katedra Informatyki
Wydział Podstawowych Problemów Techniki Politechniki Wrocławskiej

MAP3045: Algebra z Geometrią Analityczną

Wykład przeznaczony jest dla studentów I roku I stopnia Informatyki na WPPT. Odbywa się w poniedziałki w godz. 9:15 - 11:00 w sali 1.30 (C-13) oraz w środy w godz. 13:15-15:00 w sali 1.30 (C-13).

Na stronie tej znajdziesz informacje o zasadach zaliczenia, realizowanym materiale, literaturze oraz listę zadań.

Ćwiczenia do wykładu prowadzą: mgr D. Bojko, dr P. Kubiak, dr K. Majcher.

Zasady zaliczania kursu

Na ćwiczeniach odbędą się trzy 30 minutowe kolokwia. Na każdym z nich dostaniecie do zrobienia 3 zadania. Za każde z nich będziecie mogli otrzymać do 5 punktów. Za aktywność można uzyskać dodatkowo do 15 punktów. Ocena końcowa z ćwiczeń będzie wystawiana za pomocą następującej tabelki:

Pkt.	0...14	15..20	21..26	27..32	33..39	40..45	46..60
C	2.0	3.0	3.5	4.0	4.5	5.0	5.5

Literatura

- Podstawowa
  1. A. Białynicki-Birula, Algebra, PWN 1971.
  2. B. Gleichgewicht, Algebra, GiS 2002
  3. Mostowski, M. Stark, Elementy algebry wyższej, PWN 1970
- Pomocnicza
  1. Victor Shoup, **A Computational Introduction to Number Theory and Algebra (Version 2)**
  2. Linda Gilbert, Jimmie Gilbert, Elements of Modern Algebra, Brooks/Cole, Cengage Learning, 2009
  3. T. Banchoff, J. Wermer, Linear Algebra Throught Geometry, Springer Verlag, 1983
  4. M. Zakrzewski, Markowe Wykłady z Matematyki: algebra z geometrią, GIS 2015
- Lista zadań: **Algebra1_2015.pdf**
- Przykładowe zadania na pierwsze kolokwium: **Algebra1_2015_K1.pdf**
- Pytania do mnie związane z kursem: **QandA**

Omówione zagadnienia

[05-10-2015] Struktury algebraiczne

1. Działania binarne; łączność: $x \cdot (y \cdot z) = (x \cdot y) \cdot z$, przemienność: $x \cdot y = y \cdot x$
2. Pojęcie grupy
3. Grupa $_n$ = $(\{0, 1, \ldots, n-1\}, +_n)$, gdzie $a +_n b$ = $(a + b)$ modulo n
4. Tw. W każdej grupie jest dokładnie jeden element neutralny.
5. Tw. W każdej grupie element odwrotny do danego elementu jest wyznaczony jednoznacznie.
6. Grupa Sym(n): grupa permutacji zbioru $\{1, 2, \ldots, n\}$ z działaniem określonym jako złożenie funkcji. Sym(3) jest przykładem grupy nieprzemiennej; np.

   $$\begin{matrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{matrix} \circ \begin{matrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{matrix} = \begin{matrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{matrix}$$

   oraz

   $$\begin{matrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{matrix} \circ \begin{matrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{matrix} = \begin{matrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{matrix}$$

7. Tw. $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$

[07-10-2015] Struktury algebraiczne - II

1. Pojęcie izomorfizmu grup.
2. Tw. Dowolne dwie jednoelementowe grupy są izomorficzne.
3. Tw. Dowolne dwie dwu-elementowe grupy są izomorficzne.
4. Tw. (bez dowodu) Jeśli jest grupą która ma p elementów i p jest liczbą pierwszą, to jest izomorficzna z grupą $_n$.
5. Pojęcie pierścienia.
6. W dowolnym pierścieniu $(R, +, \cdot)$ mamy $0 \cdot x = 0$
7. W dowolnym pierścieniu przemiennym mamy: $(a+b)^2 = a^2 + 2a \cdot b + b^2$, $(a+b) \cdot (a-b) = a^2 - b^2$,$(a+b)^3 = a^3 + 3a^2 \cdot b + 3a \cdot b^2 + b^3$
8. Pojęcie ciała.
9. Tw. (bez dowodu) Jeśli p jest liczbą pierwszą, to struktura $_p = (\{0, 1, \ldots, p-1\}, +, \cdot)$ (z działaniami "modulo p") jest ciałem.
10. Obliczenia w ciele $_5$: równania jednej zmiennej, układ dwóch równań liniowych dwóch zmiennych, równania kwadratowe.

[12-10-2015] Liczby całkowite

1. Różne warianty indukcji matematycznej:

   W1: $(\forall A \subseteq \quad)(A \neq \emptyset \to (\exists a \in A)(\forall x \in A)(a \leq x))$.

   W2: Jeśli $A \subseteq \quad$, $a \in A$ oraz $(\forall n)(n \in A \to n+1 \in A)$ to $(\forall x \in \quad)(a \leq x \to x \in A)$.

   W3: Jeśli $A \subseteq \quad$, $0 \in A$ oraz $(\forall n)(\{0, 1, \ldots, n\} \subseteq A \to n+1 \in A)$ to $A = \quad$.

   Uwaga: równoważności tych warunków nie dowodziliśmy; będzie to zrobione na wykładzie z Logiki i Struktur Formalnych.
2. Twierdzenie o dzieleniu z resztą: jeżeli $a, b \in \quad$ i $b > 0$, to istnieją $q, r \in \quad$ takie, że $a = qb + r$ oraz $0 \leq r < b$.
3. Relacja podzielności w liczbach całkowitych; $(a|b) \wedge (a|c) \to a|(b+c)$
4. Największy wspólny dzielnik i algorytm Euklidesa: $a > b \to NWD(a, b) = NWD(a-b, b)$, jeśli $a = qb + r$, to

$NWD(a,b) = NWD(r,b)$.

5. Tw. $NWD(a,b) = \min(\{aX + bY : X, Y \in \quad\} \cap (\quad \setminus \{0\}))$.
6. Tw: Jeśli $NWD(a,b) = 1$ oraz $a|bc$ to $a|c$.
7. Tw. $\ _n$ jest ciałem wtedy i tylko wtedy, gdy n jest liczbą pierwszą.

[14-10-2015] Liczby całkowite i liczby zespolone

1. Tw. $(\forall n \geq 2)(\exists p \in \mathrm{PRIME})(p|n)$.
2. Tw [Euklides] Istnieje nieskończenie wiele liczb pierwszych.
3. Tw. Każda liczba naturalna $n \geq 2$ jest iloczynem liczb pierwszych.
4. Tw. Rozkład liczby na czynniki pierwsze jest jednoznaczny.
5. Tw. Jeśli $p_1 < p_2 < \ldots < p_n$ są pierwsze, $a = {}_{i=1}^{n} p_i^{k_i}$ i $a = {}_{i=1}^{n} p_i^{l_i}$ to $NWD(a,b) = {}_{i=1}^{n} p_i^{\min(k_i,l_i)}$
6. Def. $NWW(a,b) = \min\{k \in \quad : a|k \wedge b|k\}$
7. Tw. Jeśli $p_1 < p_2 < \ldots < p_n$ są pierwsze, $a = {}_{i=1}^{n} p_i^{k_i}$ i $a = {}_{i=1}^{n} p_i^{l_i}$ to $NWW(a,b) = {}_{i=1}^{n} p_i^{\max(k_i,l_i)}$
8. Wniosek: $NWD(a,b) \cdot NWW(a,b) = a \cdot b$

Liczby zespolone

1. Liczby zespolone ( ): wyrażenia postaci $a + b \cdot i$, gdzie $a, b \in \quad$ zaś i jest takim symbolem, że $i^2 = -1$.

   Dodawanie: $(a + b \cdot i) + (c + d \cdot i) = (a + b) + (c + d) \cdot i$ (patrz **aplet**).

   Mnożenie: $(a + b \cdot i) \cdot (c + d \cdot i) = (ac - bd) + (ad + bc) \cdot i$

   Element neutralny dodawania: $0 + 0 \cdot i$

   Element neutralny mnożenia: $1 + 0 \cdot i$
2. Element odwrotny:
$$\frac{1}{a + b \cdot i} = \frac{1}{a + b \cdot i} \frac{a - b \cdot i}{a - b \cdot i} = \frac{a - b \cdot i}{a^2 + b^2} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2} \cdot i\,.$$
3. Wniosek: Struktura $(\quad, +, \cdot)$ jest ciałem
4. Dzielenie: $\frac{z_1}{z_2} = z_1 \cdot z_2^{-1}$
5. Interpretacja graficzna liczb zespolonych
6. Def. $\overline{a + b \cdot i} = a - b \cdot i$ (sprzężenie liczby zespolonej)
7. Def. $|a + b \cdot i| = \sqrt{a^2 + b^2}$ (moduł liczby zespolonej) (patrz **aplet**)
8. Fakt. $z\bar{z} = |z|^2$.
9. Wniosek: $\frac{z_1}{z_2} = \frac{z_1 \bar{z}_2}{|z_2|^2}$.

Liczby zespolone: II

1. Formalna konstrukcja.

   $\quad = \quad^2$

   Dodawanie: $(a,b) + (c,d) = (a + c, b + d)$

   Mnożenie: $(a,b) \cdot (c,d) = (ac - bd, ad + bc)$

2. Podstawowe funkcje: $\mathrm{Re}(a+bi)=a$, $\mathrm{Im}(a+bi)=b$, $\overline{a+bi}=a-bi$, $|a+bi|=\sqrt{a^2+b^2}$
3. Tw. $|z_1 z_2| = |z_1|\cdot|z_2|$
4. Tw. $|z_1+z_2| \leq |z_1|+|z_2|$
5. Interpretacja: $|z_1-z_2|$ = odległość z_1 od z_2
6. Przykład: $\overline{\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i} = \pm\frac{1}{2}(\ \overline{2+\sqrt{2}}+\ \overline{2-\sqrt{2}}\cdot i)$
7. Dla każdej liczby zespolonej $z\neq 0$ istnieje α taka, że $z=|z|(\cos(\alpha)+i\sin(\alpha))$.
8. Wzór Eulera:
9. $$(\forall t\in\quad)\ \ e^{it}=\cos(t)+i\sin(t)$$

Liczby zespolone: III

1. Najpiękniejszy wzór matematyczny:
2. $$e^{\pi i}=-1$$
3. Mnożenie liczb zespolonych
4. $$r_1(\cos(\alpha)+i\sin(\alpha))\cdot r_2(\cos(\beta)+i\sin(\beta))$$ $$=(r_1r_2)(\cos(\alpha+\beta)+i\sin(\alpha+\beta))$$
5. Wzór de Moivre'a:
6. $$(r(\cos(\alpha)+i\sin(\alpha)))^n = r^n(\cos(n\alpha)+i\sin(\alpha))$$
7. Pierwiastki z jedności:
8. $$\sqrt[n]{1}=\{\epsilon_{n,k}:k=0,\ldots,n-1\},\quad gdzie\quad \epsilon_{n,k}=e^{\frac{2\pi}{n}k}$$
9. Jeśli $u=r(\cos\alpha+i\sin\alpha)$, gdzie $r>0$ oraz $n\geq 2$ to
10. $$\sqrt[n]{u}=\{\sqrt[n]{r}(\cos\frac{\alpha}{n}+i\sin\frac{\alpha}{n})\cdot\epsilon_{n,k}:k=0,\ldots,n-1$$
11. Tw. W dowolym ciele K, jeśli $x\neq 1$, to $1+x+\ldots x^n=\frac{x^{n+1}-1}{x-1}$.
12. Wniosek: ${}^{n-1}_{k=0}\,\epsilon_{n,k}=0$

13. Obserwacja: Struktura $(\{z \in \quad : |z| = 1\}, \cdot)$ jest grupą.

Pojęcie homomorfizmu

1. Pojęcie homomorfizmu grup: $f(x+y) = f(x) \cdot f(y)$
2. Pojęcie podgrupy
3. Jądro homomorfizmu: $ker(f) = \{x : f(x) = e\}$
4. Tw: Jądro homomorfizmu grup jest podgrupą
5. Def: Dziedzina całkowitości: przemienny pierścien z jednością, bez dzielników zera

Wielomiany

1. Dla pierścienia przemiennego z jednością $(R, +, \cdot)$ określamy

$$R[X] = \quad {}_{n=0}^{\infty} a_n X^n : (\forall n)(a_n \in R) \wedge (\exists N)(\forall n > N)(a_n = 0) \quad .$$

2. Równość: ${}_{n=0}^{\infty} a_n X^n = {}_{n=0}^{\infty} b_n X^n \equiv (\forall n)(a_n = b_n)$
3. W ${}_3$ rozważamy wielomian $w(X) = X^3 + 2X$. Mamy: $w(0) = w(1) = w(2) = 0$, ale $w \neq 0$
4. Dodawanie: ${}_{n=0}^{\infty} a_n X^n + {}_{n=0}^{\infty} b_n X^n = {}_{n=0}^{\infty}(a_n + b_n) X^n$
5. Mnożenie: ${}_{n=0}^{\infty} a_n X^n \cdot {}_{n=0}^{\infty} b_n X^n = {}_{n=0}^{\infty} c_n X^n$ gdzie $c_n = {}_{k+l=n} a_k b_l$.
6. Tw. Jeśli R jest pierścieniem przemiennym z jednością, to $R[X]$ jest również pierścieniem przemiennym z jednością.
7. Def: Dla $w \in R[X]$ określamy

$$deg(w) = \begin{matrix} \max\{k : a_k \neq 0\} & : & w \neq 0 \\ -\infty & : & w = 0 \end{matrix}$$

8. Jeśli R jest dziedziną całkowitości i $w, v \in R[X]$, to $deg(w \cdot v) = deg(w) + deg(v)$
9. Jeśli R jest dziedziną całkowitości i $w, v \in R[X]$, to $deg(w + v) \leq \max\{deg(w), deg(v)\}$

Wielomiany na ciałami

1. Tw (O dzielenie z resztą). Niech K będzie ciałem, $w, v \in K[x]$, $deg(v) > 0$. Istnieją wtedy wielomiany $q, r \in K[x]$ takie, że $w = q \cdot v + r$ oraz $deg(r) < deg(v)$.
2. Wniosek (Tw. Bezout): Jeśli K jest ciałem, $a \in K$, $w \in K[x]$ oraz $w(a) = 0$, to $w(x) = (x-a)\alpha(x)$ dla pewnego $\alpha \in K[x]$.
3. Wniosek: Jeśli K jest ciałem, $a \in K$, $w \in K[x]$ to istnieje wielomian α taki, że $w(x) = \alpha(x) \cdot (x-a) + w(a)$
4. Wniosek: Jeśli K jest ciałem, $a_1, \ldots, a_n \in K$ są parami różne, $w \in K[x]$ oraz $w(a_1) = w(a_2) = \ldots w(a_n) = 0$, to $w(x) = (x-a_1) \cdot \ldots (x-a_n)\alpha(x)$ dla pewnego $\alpha \in K[x]$.
5. Schemat Hornera
6. Zasadnicze Twierdzenie Algebry

7. Jeśli $w \in$ $[x]$ i $deg(w) > 0$ to istnieje takie $a \in$, że $w(a) = 0$.

8. Wniosek: Jeśli $w \in$ $[x]$ i $deg(w) = n > 0$ to istnieją $a_1, a_2, \ldots, a_n \in$ oraz $c \in$ takie, że $w(x) = c \cdot (x - a_1) \cdot \ldots (x - a_n)$.
9. Fakt: Jeśli $w \in$ $[x]$, a oraz $w(a) = 0$ to $w(\overline{a}) = 0$
10. Tw. Jeśli $w \in$ $[x]$ i $deg(w) > 0$ to istnieją takie wielomiany $v_1, \ldots, v_k$ takie, że
    1. $w = v_1 \cdot v_2 \cdot \ldots \cdot v_k$
    2. $deg(v_i) \in \{1, 2\}$ dla i = 1,2,...,k
    3. Jeśli $deg(v_i) = 2$ to v_i jest dwumianem o wyróżniku ujemnym
11. Każdy wielomian $w \in$ $[x]$ stopnia trzeciego ma pierwiastek rzeczywisty.

Wielomiany na ciałami - II

1. Fakt: Jeśli $p, q \in K[x]$, $p|q$ i $q|p$ to $p = aq$ dla pewnego $a \in K$.
2. Def. p jest wielomianem pierwszym, jeśli $deg(p) \geq 1$ oraz nie istnieją wielomiany a, b takie, że $p = a \cdot b$ oraz $deg(a), deg(b) < deg(p)$
3. Tw. Każdy wielomian jest iloczynem wielomianów pierwszych
4. Def. Wielomian $p(x) = a_0 + a_1 x + \ldots + a_n x^n$ jest moniczny, jeśli $a_n = 1$
5. Def. $NWD(p, q) = r$ jeśli r jest moniczny, $r|p$, $r|q$ oraz dla dowolnego wielomianu s, jesli $s|p$ i $s|q$ to $s|r$
6. Tw. Jeśli $p \neq 0$ lub $q \neq 0$ to istnieje $NWD(p, q)$. Co więcej, istnieją takie wielomiany a, b takie, że $NWD(p, q) = a \cdot b + b \cdot q$
7. Algorytm Euklidesa dla wielomianów nad ciałem
8. Tw. Rozkład wielomianu na iloczyn wielomianów pierwszych jest jednoznaczny

Przykład. Wielomian $w(x) = x^2 + x + 1$ jest pierwszy w $_2[x]$. Na zbiorze $K = \{a + bx : a, b \in {}_2[x]\}$ określamy działanie

$$p \star q = \text{reszta z dzielenia } p \cdot q \text{ przez wielomian } x^2 + x + 1$$

Mamy, między innymi, $x^2 = 1 \cdot (x^2 + x + 1) + x + 1$, więc $x \star x = 1 + x$

Wielomiany

1. Konstrukcja ciała 4 elementowego za pomocą wielomianu pierwszego $w(x) = x^2 + x + 1$ nad ciałem $_2$.
2. Tw. Jeśli $w(x) = a_0 + a_1 x + \ldots a_n x^n \in$ $[x]$, $NDW(p, q) = 1$ oraz $w(\frac{p}{q}) = 0$ to $q|a_n$ oraz $p|a_0$
3. Def. Zawartością wielomianu $w(x) = a_0 + a_1 x + \ldots a_n x^n \in$ $[x]$ nazywamy liczbę $z(w) = NWD(a_0, \ldots, a_n)$.
4. Lemat: Jeśli $z(w) = z(v) = 1$ to $z(w \cdot v) = 1$.
5. Tw (Gauss). Wielomian $w \in$ $[x]$ jest nierozkładalny w $[x]$ wtedy i tylko wtedy, gdy jest nierozkładalny w $[x]$.
6. Rozwiązywanie równań stopnia trzeciego w ciele liczb zespolonych.

Wielomiany - c.d.

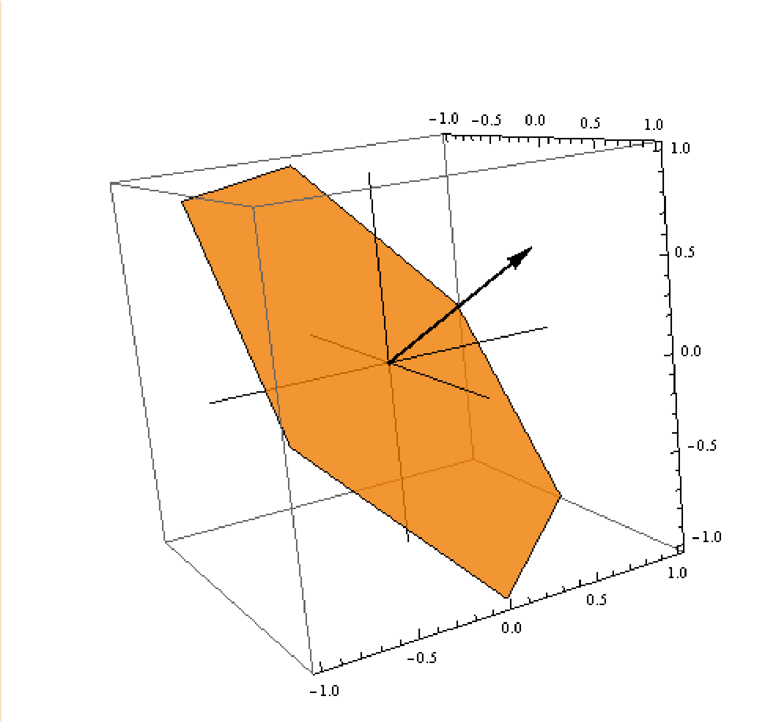
1. Charakterystyka ciała
2. Formalne różniczkowanie wielomianów
3. Tw. (dla ciał o charakterystyce 0) Jeśli $w(a) = w^{(1)}(a) = w^{(2)}(a) = \ldots(x) = w^{(n-1)}(a) = 0$ i $w^{(n)}(a) \neq 0$ to a jest pierwiastkiem krotności n wielomianu w.
4. Tw. $(f \cdot g)' = f' \cdot g + f \cdot g'$

Przestrzeń ^n

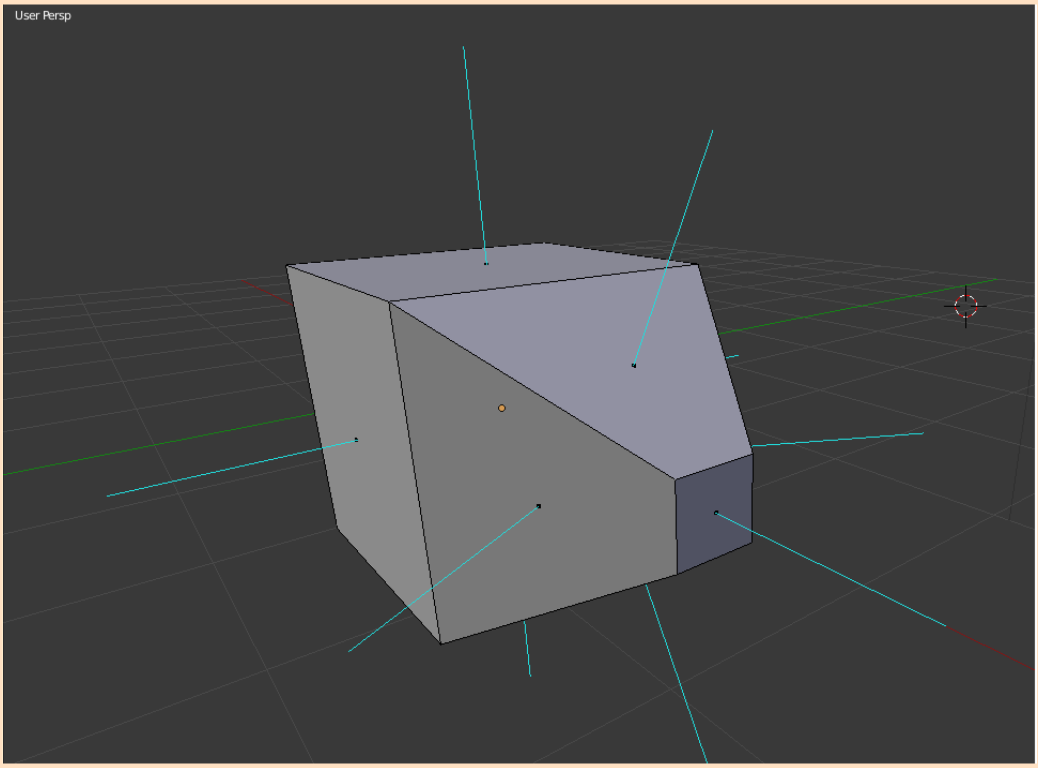
1. Def. $<\vec{x},\vec{y}>= \;{}^{n}_{k=1} x_i y_i$
2. Def. $||\vec{x}|| = \;\overline{<\vec{x},\vec{x}>}$
3. Tw. $|<\vec{x},\vec{y}>| \leq ||\vec{x}|| \cdot ||\vec{y}||$
4. Def. $d(\vec{x},\vec{y}) = ||x-y||$
5. Tw. (nierówność trójkąta) $d(x,z) \leq d(x,y) + d(y,z)$
6. Tw. $<\vec{x},\vec{y}>= ||x|| \cdot ||y|| \cdot \cos(\alpha)$

Przestrzeń ^n

1. Def. $(x \perp y) \equiv (<\vec{x},\vec{y}>= 0)$
2. Twierdzenie Pitagorasa: jeśli $x \perp y$ to $\|x+y\|^2 = \|x\|^2 + \|y\|^2$
3. Równanie parametryczne prostej: $X_t = \vec{P} + t\vec{a}$, $t \in \;$.
4. Hiperpłaczyzna wyznaczona przez parametry $A_1, \ldots, A_n$, B (zakładamy, że $A_1^2 + \ldots A_n^2 > 0$): zbiór tych $(x_1, \ldots, x_n) \in \;{}^n$, że
$$A_1 x_1 + \ldots A_n x_n + B = 0\,.$$
5. Własności: wektor $(A_1, \ldots, A_n)$ jest prostopadły do hiperpłaszczyzny zadanej powyższym równaniem.
6. Odległość punktu $P = (p_1, \ldots, p_n)$ od hiperpłaszczyzny zadanje wzorem $A_1 x_1 + \ldots A_n x_n + B = 0$ wyraża się wzorem
$$d(P,\Pi) = \frac{|A_1 p_1 + \ldots A_n p_n + B|}{\overline{A_1^2 + \ldots A_n^2}}$$
7. Wektor normalny do hiperpłaszczyzny: wektor długości 1, prostopadły do tej hiperpłaszczyzny.



Normalne ścian w programie Blender:



Przestrzenie wektorowe

1. Definicja przestrzeni wektorowej nad ciałem K.
2. Def. Liniowa kombinacja wektorów $f_1, \ldots, f_n$: dowolny wektor postaci

$$\lambda_1 f_1 + \ldots + \lambda_n f_n \ ,$$

   gdzie $\lambda_1, \ldots, \lambda_n \in K$.
3. Def. Liniowa otoczka zbioru $E \subseteq V$: zbiór

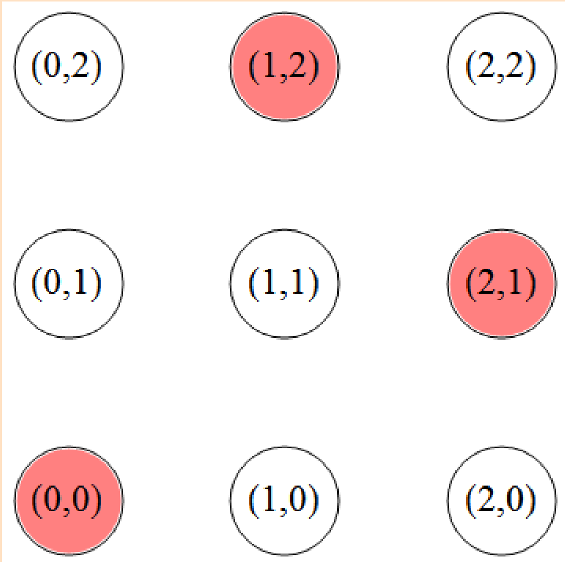
$$Lin(E) = \{ \overset{n}{\underset{k=1}{}} \lambda_k f_k : n \in \quad , \lambda_1, \ldots, \lambda_n \in K, f_1, \ldots, f_n \in E \}$$

4. **Def**: Wektory $f_1, \ldots, f_n \in V$ są **liniowo niezależne** jeśli dla dowolnych $\lambda_1, \ldots, \lambda_n \in K$ mamy

$$(\lambda_1 f_1 + \ldots + \lambda_n f_n = 0) \quad \to \quad (\lambda_1 = \ldots = \lambda_n = 0)\ .$$

5. W przestrzeni wektorowej $(\ \ _3)^2$:

$$Lin(\{(2,1)\}) = \{(0,0),(2,1),(1,2)\}\ .$$



Liniowa niezależność

1. Tw. Zbiór E jest liniowo niezależny wtedy i tylko wtedy, gdy dla dowolnego $e \in E$ mamy $e \notin Lin(E \setminus \{e\})$.
2. Tw. Jeśli $f_1, \ldots, f_n$są liniowo niezależne oraz

$$\lambda_1 f_1 + \ldots + \lambda_n f_n = \mu_1 f_1 + \ldots + \mu_n f_n,$$

to $\lambda_1 = \mu_1, \ldots, \lambda_n = \mu_n$.

3. Def. Bazą przestrzeni wektorowej V nazywamy dowolny taki liniowo niezależny podzbiór $B \subseteq V$, że $Lin(B) = V$.
4. Tw (bez dowodu, bo był on wykładzie z Logiki i Struktur Formalych) W każdej przestrzeni wektorowej $V \neq \{0\}$ istnieje baza
5. Tw. Liniowo podzbiór B przestrzeni wektorowej V jest bazą wtedy i tylko wtedy, jest maksymalnym, liniowo niezależnym podzbiorem przestrzeni V.
6. Tw. Jeśli $k < n$ to układ równań

$$(\forall i \in \{1, \ldots, k\}) \mathop{\ }_{j=1}^{n} \alpha_{i,j} x_j = 0$$

ma nietrywialne rozwiązanie.

7. Tw. Jeśli B jest bazą przestrzeni V, $F \subseteq V$ oraz $|B| < |F|$ to F jest liniowo zależny.

Podprzestrzenie liniowe i odwzorowania liniowe

1. Tw. Jeśli B_1 i B_2 są bazami przestrzeni V to $|B_1| = |B_2|$.
2. Def:

$$dim(V) = \begin{matrix} 0 & : & V = \{0\} \\ |B| & : & B \text{ jest bazą V} \end{matrix}$$

3. Def. Niepusty zbiór $H \subseteq V$ jest podprzestrzenią liniową przetrzeni V jeśli
$$(\forall x, y \in H)(\forall \alpha, \beta \in K)(\alpha x + \beta y \in H)\ .$$
4. Def. Funkcja $F : V_1 \to V_2$ jest odwzorowaniem liniowym jeśli
$$(\forall x, y \in H)(\forall \alpha, \beta \in K)(F(\alpha x + \beta y) = \alpha F(x) + \beta F(y))\ .$$
5. Opis odwzorowań liniowych z ^{2} w ^{2}:
$$F \begin{matrix} x_1 \\ x_2 \end{matrix} = \begin{matrix} a_{11}x_1 + a_{12}x_2 \\ a_{21}x_1 + a_{22}x_2 \end{matrix}$$
dla pewnych $a_{11}, a_{12}, a_{21}, a_{22} \in$.
6. Def. Jeśli $F : V_1 \to V_2$ jest odwzorowaniem liniowym, to $ker(F) = \{x \in V_1 : F(x) = 0\}$.
7. Tw. Jeśli $F : V_1 \to V_2$ jest odwzorowaniem liniowym, to $ker(F)$ jest podprzestrzenią liniową przestrzeni V_1.
8. Tw. Jeśli $F : V_1 \to V_2$ jest odwzorowaniem liniowym, to $rng(F)$ jest podprzestrzenią liniową przestrzeni V_2.
9. Tw. Jeśli $F : V_1 \to V_2$ jest odwzorowaniem liniowym, to
10. $$dim(V_1) = dim(ker(F)) + dim(rng(F))$$

Odwzorowania liniowe

1. Jeśli $F : V \to H$ jest liniowe, $B = \{e_1, \ldots, e_n\}$ jest bazą V oraz $C = \{f_1, \ldots, f_m\}$ jest bazą H to macierzą F w bazach B i C nazywamy macierz $M_{C,B}(F)$ rozmiaru $m \times n$ o wyrazach $(a_{i,j})$ jeśli
$$F(e_i) = \overset{m}{\underset{j=1}{}} f_j a_{ji}$$
2. Mnożenie macierzy przez wektor:
3. $$\begin{matrix} a_{11} & \cdots & a_{1n} \\ \vdots & \cdots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{matrix} \cdot \begin{matrix} x_1 \\ \vdots \\ x_n \end{matrix} = \begin{matrix} \overset{n}{\underset{j=1}{}} a_{1j}x_j \\ \overset{n}{\underset{j=1}{}} a_{2j}x_j \\ \vdots \\ \overset{n}{\underset{j=1}{}} a_{mj}x_j \end{matrix}$$
4. Jeśli $M_{C,B}(F) = (a_{ij})_{i=1\ldots m; j=1\ldots n}$ oraz

$$\begin{matrix} a_{11} & \dots & a_{1n} \\ \vdots & \dots & \vdots \\ a_{m1} & \dots & a_{mn} \end{matrix} \cdot \begin{matrix} x_1 \\ \vdots \\ x_n \end{matrix} = \begin{matrix} y_1 \\ \vdots \\ y_m \end{matrix}$$

to $F({}_{j=1}^{n} x_j e_j) = {}_{j=1}^{n} y_j f_j$, czyli $F([x_1, \dots, x_n]_B) = [y_1, \dots, y_m]_C$.

5. Przykłady odwzorowań liniowych $F : {}^2 \to {}^2$
   1. Identyczność: $Id = \begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix}$
   2. Odwzorowanie zerowe: $\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix}$
   3. Skalowanie : $S_{a,b} = \begin{matrix} a & 0 \\ 0 & b \end{matrix}$
   4. Ścięcie: $S_r = \begin{matrix} 1 & r \\ 0 & 1 \end{matrix}$
   5. Obrót: $O_\alpha = \begin{matrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{matrix}$
6. Def. $det \begin{matrix} a & b \\ c & d \end{matrix} = ad - bc$
7. Tw. Jeśli $F : {}^2 \to {}^2$ jesy liniowe oraz A jest macierzą F w standardowej bazie oraz $S \subseteq {}^2$ to $pow(F[S]) = pow(S) \cdot det(A)$.

Odwzorowania liniowe - c.d.

1. Jeśli $B = (b_1, \dots, b_n)$ jest upoządkowaną bazą, to $[x]_B = [x_1, \dots, x_n]^T$ jeśli $x = {}_{k=1}^{n} x_i b_i$
2. Suma macierzy tych samych rozmiarów: $(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})$
3. Tw. Jeśli $F, G : V \to H$ są liniowe, to $F + G$ też jest liniowe. Jesli B, C są bazami uporządkowanymi przetrzeni V i H, to
$$M_{C,B}(F+G) = M_{C,B}(F) + M_{C,B}(G)$$
4. Iloczyn macierzy: $(a_{ij})_{i=1\dots r; j=1\dots m} \cdot (b_{jk})_{j=1\dots m; k=1\dots n} = (c_{ik})_{i=1\dots r; k=1\dots n}$, gdzie
$$c_{ik} = {}_{j=1}^{m} a_{ij} bjk$$
(patrz: **YouTube**).
5. Jeśli $F : V_1 \to V_2$, $G : V_2 \to V_3$ są liniowe, to $G \circ F : V_1 \to V_3$ jest liniowe. Jesli B, C, D są bazami uporządkowanymi przetrzeni V_1 i V_2, V_3 to
$$M_{D,B}(G \circ F) = M_{D,C}(G) \cdot M_{C,B}(F)$$
6. Przykład: Rozważamy odwzorowanie $F : {}^2 \to {}^2$ zadane wzorem
$$F(x, y) = \begin{matrix} \frac{3}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{3}{2} \end{matrix} \begin{matrix} x \\ y \end{matrix}$$
W bazie $C = \{(1,1), (-1,1)\}$ ma ono macierz

$$M = \begin{matrix} 2 & 0 \\ 0 & 1 \end{matrix}$$

Pokazaliśmy, że $M^n = \begin{matrix} 2^n & 0 \\ 0 & 1 \end{matrix}$

7. Macierz przejścia z bazy $B = (b_1, \ldots, b_n)$ do bazy $C = (c_1, \ldots, c_n)$:

$$T_{B,C} = [[c_1]_B, \ldots, [c_n]_B] \; .$$

8. Jeśli T jest macierzą przejścia z B do C to $[x]_B = T \cdot [x]_C$.
9. Jeśli T jest macierzą przejścia z B do C to $[x]_C = T^{-1} \cdot [x]_B$.
10. Jeśli $M = \begin{matrix} a & b \\ c & d \end{matrix}$ oraz $det(M) \neq 0$, to
11. $$M^{-1} = \frac{1}{det(M)} \begin{matrix} d & -b \\ -c & a \end{matrix}$$

(wrócimy do tego na nastepnym wykładzie).

Odwzorowania afiniczne płaszczyzny

1. Def. Odwzorowaniem afinicznym płaszczyzny nazywamy odwzorownie postaci

$$F(x, y) = \begin{matrix} a & b \\ c & d \end{matrix} \begin{matrix} x \\ y \end{matrix} + \begin{matrix} e \\ f \end{matrix}$$

2. Reprezentacja odwzorowań afinicznych:

$$\begin{matrix} a & b & e \\ c & d & f \\ 0 & 0 & 1 \end{matrix} \begin{matrix} x \\ y \\ 1 \end{matrix}$$

3. Przykłady: translacja: $\begin{matrix} 1 & 0 & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{matrix} \begin{matrix} x \\ y \\ 1 \end{matrix}$, obrót: $\begin{matrix} \cos\alpha & -\sin\alpha & 0 \\ \sin\alpha & \cos\alpha & 0 \\ 0 & 0 & 1 \end{matrix} \begin{matrix} x \\ y \\ 1 \end{matrix}$

Znak permutacji

1. Def. $Inv((a_i)_{i=1\ldots n}) = card(\{(i,j) : 1 \leq i < j \leq n \wedge a_i > a_j\})$.
2. Def. Jeśli $\vec{a} = (a_i)_{i=1\ldots n}$ to $sgn(\vec{a}) = (-1)^{Inv(\vec{a})}$.
3. Tw. Jeśli $T_{i,j}$ jest transpozycją dwóch elementów to $sqn(T_{i,j}) = -1$.
4. Tw. Jesli $\sigma, \pi \in S_n$ to $sqn(\pi \circ \sigma) = sqn(\pi) \cdot sqn(\sigma)$.

Wyznacznik

1. Def. Jeśli $A = (a_{i,j})_{i,j=1,\ldots,n}$ to

2. $$det(A) = {}_{\sigma\in S_n} sgn(\sigma) \; {}_{i=1}^{n} \; a_{i,\sigma(i)} \, .$$

Wyznaczniki

1. Wyznacznik macierzy 3×3: **YouTube**
2. Tw. Niech $(G, \cdot)$ będzie grupą oraz $a \in G$ Wtedy funkcje $f(x) = x^{-1}$ oraz $g(x) = x \cdot a$ są bijekcjami G.
3. Tw. $det(A) = {}_{\sigma\in S_n} sgn(\sigma) \; {}_{i=1}^{n} a_{\sigma(i),i}$
4. Def. $[a_{i,j}]^T = [a_{j,i}]$
5. Wniosek. $det(A^T) = det(A)$
6. Tw (o mnożeniu kolumny przez stałą) $det([k_1, \ldots, k_{i-2}, \;\cdot\;, k_{i+1}, \ldots, k_n]) = \;\cdot\, det([k_1, \ldots, k_{i-2}, \;, k_{i+1}, \ldots, k_n])$
7. Tw.(o sumie dwóch kolumn) $det([k_1, \ldots, k_{i-2}, \;, k_{i+1}, \ldots, k_n]) = det([k_1, \ldots, k_{i-2}, \;, k_{i+1}, \ldots, k_n])$ $+ \, det([k_1, \ldots, k_{i-2}, \;, k_{i+1}, \ldots, k_n])$
8. Tw. (o zamianie kolumn) $det([k_1, \ldots, k_{i-2}, \;, k_{i+1}, \ldots, k_{j-1}, \;, k_{j+1} k_n]) = -det([k_1, \ldots, k_{i-2}, \;, k_{i+1}, \ldots, k_{j-1}, \;, k_{j+1} k_n]$
9. **Wniosek.** Wyznacznik macierzy o dwoch takich samych kolumnach (lub dwóch takich samych wierszach) jest równy zero.
10. Tw.(o dodawaniu kolumn) Jeśli $1 \leq i < j \leq n$ to $det([k_1, \ldots, \;, \ldots, \;, \ldots, k_n]) = det([k_1, \ldots, k_{i-2}, \;, k_{i+1}, \ldots, k_{j-1}, \;\cdot\;, \ldots, k_n])$
11. Algorytm obliczania wyznacznika o złożoności obliczeniowej $O(n^3)$.

Wyznaczniki

1. Def. Niech $A \in M_{n\times}$. Minorem $M_{i,j}$ maciezry A nazywamy wyznacznik macierzy która powstaje z A po skreśleniu i-tego wiersza oraz j-tej kolumny.
2. Def. Niech $A \in M_{n\times}$. Algebraicznym dopełnieniem elementu $a_{i,j}$ nazywamy liczbę $A_{i,j} = (-1)^{i+j} M_{i,j}$.
3. Tw. (Laplace) Niech $1 \leq r, s \leq n$. Wtedy
$${}_{j=1}^{n} \; a_{r,j} A_{s,j} = det(A)\delta_{r,s}$$
gdzie $\delta_{r,s} = \begin{matrix} 1 & : r = s \\ 0 & : r \neq s \end{matrix}$.
4. Tw. Jeśli $A \in M_{n\times}$ oraz $det(A) \neq 0$, to istnieje taka macierz A^{-1}, że $A \cdot A^{-1} = A^{-1} \cdot A = I_n$. Ponadto

5. $$A^{-1} = \frac{1}{det(A)} [A_{i,j}]^T \, .$$

6. **Wzory Cramera**: Rozważamy układ równań liniowych:

$$\begin{aligned} a_{1,1}x_1 + a_{1,2}x_2 + \dots a_{1,n}x_n &= b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + \dots a_{2,n}x_n &= b_2 \\ \dots &= \vdots \\ a_{n,1}x_1 + a_{n,2}x_2 + \dots a_{n,n}x_n &= b_n \end{aligned}$$

(mamy n równań oraz n zmiennych). Oznaczamy $A[a_{i,j}]_{i,j=1,\dots,n}$. Rozważany układ ten jest równoważny następującemu równaniu:

$$A \cdot \vec{x} = \vec{b}$$

gdzie $\vec{x} = \begin{matrix} x_1 \\ \vdots \\ x_n \end{matrix}$ oraz $\vec{b} = \begin{matrix} b_1 \\ \vdots \\ b_n \end{matrix}$.

Załóżmy, że $det(A) \neq 0$. Wtedy $\vec{x} = A^{-1}\vec{b}$. Po rozpisaniu tego, otrzymujemy wzory na rozwiązanie:

$$x_k = \frac{\det \ A_{k,\vec{b}}}{det(A)} ,$$

gdzie $A_{k,\vec{b}}$ jest macierzą, którą otrzymujemy z macierzy A przez zastąpienie k-tej kolumny wektorem $\vec{b}$.

Wyznaczniki

1. Tw. $det(A \cdot B) = det(A) \cdot det(B)$
2. Def. $rank([k_1, \dots, k_n]) = dim(Lin(\{k_1, \dots, k_n\}))$.
3. Tw. $rank(A)$ jest równy największemu stopniu niezerowego minora macierzy A
4. Układ równań liniowych

$$\begin{aligned} a_{11}x_1 + \dots + a_{1,n}x_n &= b_1 \\ \dots &= \vdots \\ a_{m1}x_1 + \dots + a_{m,n}x_n &= b_m \end{aligned}$$

jest równoważny równaniu

$$\begin{matrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & \dots & \vdots \\ a_{m,1} & \dots & a_{m,n} \end{matrix} \cdot \begin{matrix} x_1 \\ \vdots \\ x_n \end{matrix} = \begin{matrix} b_1 \\ \vdots \\ b_m \end{matrix}$$

Istnienie rozwiązania tego układu jest równoważne zdaniu

$$\begin{matrix} b_1 \\ \vdots \\ b_m \end{matrix} \in \mathrm{rng}(F_A) ,$$

gdzie $F_A \begin{matrix} x_1 \\ \vdots \\ x_n \end{matrix} = A \cdot \begin{matrix} x_1 \\ \vdots \\ x_n \end{matrix}$, a $A = \begin{matrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & \dots & \vdots \\ a_{m,1} & \dots & a_{m,n} \end{matrix}$.

5. Niech $A = [k_1, \dots, k_n]$. Wtedy

$$6. \quad \vec{b} \in \operatorname{rng}(F_A) \quad \leftrightarrow \quad rank([k_1, \dots, k_n]) = rank([k_1, \dots, k_n, \vec{b}]) \quad .$$

Metoda eliminacji Gaussa-Jordana

1. Tw. Jeśli $a \neq 0$ to $dim(lin(\{w_1, w_2, \dots, w_n\})) = dim(lin(\{w_1, aw_1 + w_2, w_3, \dots, w_n\}))$
2. Metoda eliminacji Gausa-Jordana: **YouTube**
3. Zastosowanie metody eliminacji do wyznaczania macierzy odwrotnej. **YouTube**
4. Def. $H_1 + H_2 = \{x + y : x \in H_1 \wedge y \in H_2\}$.
5. Tw. $dim(H_1 + H_2) = dim(H_1) + dim(H_2) - dim(H_1 \cap H_2)$
6. Def. $H = H_1 \oplus H_2$ jeśli $H = H_1 + H_2 \wedge H_1 \cap H_2 = \{0\}$.
7. Jeśli $H = H_1 \oplus H_2$ to przestrzeń $H_1 + H_2$ jest izomorficzna z przetrzenią $H_1 \times H_2$

Podprzestrzenie niezmiennicze.

1. Def. Podprzestrzeń $H \subseteq V$ jest podprzestrzenią niezmieniiczą odwzorowania $F : V \to V$ jeśli $F[H] \subseteq H$
2. Def. Wartość własna macierzy A: taka λ, że istnieje niezerowy wektor $\vec{x}$ taki, że $A \cdot \vec{x}^T = \lambda \vec{x}^T$
3. Def. Wektor własny odpowiadający wartości własnej λ: taki $\vec{x}$ że $\vec{x} \neq \vec{0}$ oraz $A \cdot \vec{x}^T = \lambda \vec{x}^T$
4. Def. Wielomian charakterystyczony macierzy kwadratowej A:

$$p_A(\lambda) = \det(A - \lambda I)$$

5. Tw. λ jest wartością własną macierzy A wtedy i tylko wtedy, gdy $p_A(\lambda) = 0$
6. Liczby Fibonacciego: $F_0 = F_1 = 1$, $F_{n+2} = F_n + F_{n+1}$.
   1. $\begin{matrix} 0 & 1 \\ 1 & 1 \end{matrix}^n \begin{matrix} 1 \\ 1 \end{matrix} = \begin{matrix} F_n \\ F_{n+1} \end{matrix}$
   2. $p(\lambda) = \det(\begin{matrix} -\lambda & 1 \\ 1 & 1-\lambda \end{matrix}) = \lambda^2 - \lambda - 1$
   3. Równanie $p(\lambda) = 0$ ma dwa pierwiastki: $\lambda_1 = \frac{1}{2}(1 - \sqrt{5})$, $\lambda_2 = \frac{1}{2}(1 + \sqrt{5})$
   4. Wiemy, że są takie stałe a i b, że $F_n = a\lambda_1^n + b\lambda_2^n$
   5. Korzystając z tego, że znamy F_0 i F_1$ liczymy trochę i po kilku uproszczeniach otrzymujemy

6. $$F_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^{n+1} + (-1)^n \left(\frac{\sqrt{5}-1}{2}\right)^{n+1}$$

Wielomian charakterystyczny

1. Def: Spektrum macierzy A: spec(A) = \{\lambda: p_A(\lambda) = 0\}$
2. Tw. Jeśli T jest macierzą przejścia z bazy do bazy i A jest dowolną macierzą kwadratową to $p_{TAT^{-1}}(\lambda) = p_A(\lambda)$.
3. Tw. Jeśli A jest macierzą kwadratową rozmiaru $n \times N$ oraz $p_A(\lambda) = c_0 + c_1\lambda + c_1\lambda + c_n\lambda^n$ to
   1. $c_n = (-1)^n$
   2. $c_{n-1} = (-1)^{n+1}\mathrm{Tr}(A)$
   3. $c_0 = \det(A)$
4. Przykład: Jeśli $A \in M_{2\times 2}(K)$ to $p_A(\lambda) = \lambda^2 - \mathrm{tr}(A)\lambda + \mathrm{det}(A)
5. Tw(Cayley-Hamilton) Jeśli A jest macierzą kwadratową, to $p_A(A) = 0$

Macierze ortogonalne

1. Proces ortogonalizacji Grama-Schmidta : $g_1 = f_1$,

$$g_{k+1} = f_k - \sum_{i=1}^{k} \frac{< f_i, g_i >}{< g_i, g_i >} g_u$$

2. Def: A jest macierzą ortogonalną jeśli A jest macierzą złożoną z kolumn ortonormalnych.
3. Tw. Jeśli A jest macierzą ortogonalną, to $AA^T = I$.
4. Wniosek: Jeśli A jest ortogonalna, to $A^{-1} = A^T$
5. Tw. A jest macierzą ortogonalną wtedy i tylko wtedy, gdy $< Ax, Ay >$ = $< x, y >$ dla dowolnych wektorów x i y.
6. Wniosek: Jeśli A jest ortogonalna, to A^{-1} też jest ortogonalna
7. Wniosek: Jeśli A, B są ortogonalne, to AB też jest ortogonalna
8. Wniosek: Zbiór macierzy ortogonalnych tworzy grupę, ze względu na składanie macierzy. Oznacza się ją przez $O(n)$

Singular value decomposition

1. Tw. Załóżmy, że A jes macierzą rzeczywistą i symetryczną. Istnieją wtedy macierze V i Σ takie, że V jest ortogonalna, Σ jest diagonalna oraz

$$A = V\Sigma V^T .$$

2. Twierdzenie [O rozkładzie SVD] Niech $A \in M_{m\times n}(R)$. Istnieją wtedy macierze $Q \in M_{m\times m}(R)$, $\Sigma \in M_{m\times n}(R)$ oraz $R \in M_{n\times n}(R)$ taki, że
   1. Q i R są ortogonalne
   2. tylko elementy na głównej przekątnej macierzy Σ są niezerowej

oraz

$$A = Q\Sigma R^T\ .$$