1. Wykład 2 (1 III)

Suma, produkt, przestrzeń ilorazowa.

Definicja 1. Suma i produkt przestrzeni wektorowych.

Stwierdzenie 2. *Jeśli I jest skończony, to $\bigoplus_{i\in I} V_i \cong \prod_{i\in I} V_i$. Jeśli nie, jest nietrywialne zawieranie $\bigoplus_{i\in I} V_i \subsetneq \prod_{i\in I} V_i$*

Definicja 3. Naturalne włożenia i rzutowania.

Stwierdzenie 4. *Własność uniwersalna sumy i produktu.*

Stwierdzenie 5. *Niech V_i będą przestrzeniami wektorowymi i niech $\mathcal{B}_i$ będzie bazą V_i. Wówczas $\sum_{i\in I} \mathcal{B}_i$ jest bazą $\bigoplus_{i\in I} V_i$.*

Uwaga. W przypadku nieskończonego produktu nie ma dobrego opisu bazy.

Definicja 6. Niech $W \subseteq V$ będzie podprzestrzenią wektorową. Na V wprowadzamy relację $\alpha \sim \beta$ jeśli $\alpha - \beta \in W$. Jest to relacja równoważności. Klasę równoważności tej relacji nazywamy *warstwą* i oznaczamy $\alpha + W$. Zbiór warstw ma określoną strukturę przestrzeni wektorowej; nazywamy ją *przestrzenią ilorazową* i oznaczamy V/W.

Definicja 7. Homomorfizm rzutowania $p : V \to V/W$.

Uwaga (*). Ciąg $0 \to W \to V \to V/W \to 0$ jest dokładny, tj. obraz poprzedniego przekształcenia jest jądrem kolejnego.

Przykład 1. $V/V = 0$, $V/0 \cong V$, $V \oplus W/V \cong W$.

Stwierdzenie 8. *Własność uniwersalna przestrzeni ilorazowej: dla każdego homomorfizmu $f : V \to Y$ takiego, że $f|_W = 0$ istnieje dokładnie jedno $f' : V/W \to Y$ takie, że $f' \circ p = f$. Inaczej:*

$$\mathrm{Hom}(V/W, Y) \cong \ker\left(\mathrm{Hom}(V, Y) \xrightarrow{(W\subseteq V)^*} \mathrm{Hom}(W, Y)\right).$$

2. Wykład 3 (3 III)

Definicja 9. Niech $f : V \to W$ będzie homomorfizmem.

- *Jądro* f to $\ker(f) = \{\alpha \in V :\ f(\alpha) = 0\}$
- *Obraz* f to $\mathrm{im}(f) = \{\beta \in W :\ \exists_{\alpha\in V}\ f(\alpha) = \beta\}$
- *Kojądro* f to $\mathrm{coker}(f) = W/\mathrm{im}(f)$
- *Koobraz* f to $\mathrm{coim}(f) = V/\ker(f)$.

Stwierdzenie 10. *Obraz i koobraz są naturalnie izomorficzne.*

Stwierdzenie 11. *Dla $f : V \to W$ istnieją naturalnie ciągi*

$$V \to \mathrm{im}(f) \to W$$

oraz

$$0 \to \ker(f) \to V \xrightarrow{f} W \to \mathrm{coker}(f) \to 0.$$

Stwierdzenie 12. *Własność uniwersalna jądra i kojądra.*

Kategorie(*).

Definicja 13. *Kategoria* $\mathcal{C}$ składa się z:

- rodziny obiektów $Ob(\mathcal{C})$ (niekoniecznie jest to zbiór),
- dla każdej pary obiektów $a, b \in Ob(\mathcal{C})$ dany jest zbiór $Mor_{\mathcal{C}}(a, b)$ zwany *zbiorem morfizmów z a do b*,
- dla każdej trójki $a, b, c \in Ob(\mathcal{C})$ dane jest działanie

  $$Mor_{\mathcal{C}}(a, b) \times Mor_{\mathcal{C}}(b, c) \ni (f, g) \mapsto gf \in Mor_{\mathcal{C}}(a, c)$$

  zwane składaniem morfizmów.

Spełnione są następujące aksjomaty:

- dla każdego obiektu a istnieje morfizm $\mathrm{id}_a : a \to a$, tzn. $\mathrm{id}_a \in Mor_{\mathcal{C}}(a,a)$ taki, że $f\,\mathrm{id}_a = f$, $\mathrm{id}_a\, g = g$.
- składanie jest łączne.

Przykład 2. Przykłady kategorii:

- Kategoria zbiorów **Set**.
- Kategoria przestrzeni wektorowych nad K $\mathbf{Vect}_K$.
- Kategoria grup **Gr**.
- Jeśli $\mathcal{C}$ jest kategorią, to dla podrodziny obiektów $X \subseteq Ob(\mathcal{C})$ można zdefiniować podkategorię pełną (obiekty: X, morfizmy: takie jak w $\mathcal{C}$).
- Kategoria odwrotna $\mathcal{C}^{op}$: $Ob(\mathcal{C}^{op}) = Ob(\mathcal{C})$, $Mor_{\mathcal{C}^{op}}(a,b) = Mor_{\mathcal{C}}(b,a)$.
- Kategorie z jednym obiektem.
- Małe kategorie.

Definicja 14. *Obiekt początkowy i końcowy.*

Definicja 15. *Funktor* z $\mathcal{C}$ do $\mathcal{D}$ to:

- Dla każdego obiektu $a \in \mathcal{C}$ określony jest pewien obiekt $F(a) \in \mathcal{D}$.
- Dla każdego morfizmu $f : a \to a'$ określony jest morfizm $F(f) : F(a) \to F(a')$.

spełniające następujące warunki:

- $\forall_{a\in\mathcal{C}}\ F(\mathrm{id}_a) = \mathrm{id}_{F(a)}$,
- dla każdej pary składalnych morfizmów f, g w $\mathcal{C}$ mamy $F(gf) = F(g)F(f)$.

Przykład 3.

(a) Funktor zapominania $\mathbf{Vect}_K \to \mathbf{Set}$.
(b) Funktor wolny $\mathbf{Set} \to \mathbf{Vect}_K$.
(c) Przestrzeń sprzężona $\mathbf{Vect}_K \to \mathbf{Vect}_K^{op}$.
(d) Suma prosta $\mathbf{Vect}_K \times \mathbf{Vect}_K \to \mathbf{Vect}_K$.
(e) $Hom : \mathbf{Vect}_K^{op} \times \mathbf{Vect}_K \to \mathbf{Vect}_K$

Definicja 16. Diagram w kategorii $\mathcal{C}$ o kształcie $\mathcal{D}$ to funktor $\mathcal{D} \to \mathcal{C}$.

Przykład 4.

(a) Kategorie z jednym obiektem.
(b) $\bullet \to \bullet$
(c) Push-out i pull-back.
(d) $\mathbb{N}$

3. Wykład 4 (8 III)

3.1. Granice w kategoriach.

Definicja 17. Niech $\mathcal{D}$ będzie małą kategorią, $\mathcal{C}$ dowolną kategorią, a $F : \mathcal{D} \to \mathcal{C}$ funktorem. *Stożkiem* nad F nazywamy obiekt $x \in \mathrm{Ob}(\mathcal{C})$ wraz z rodziną morfizmów $\{f_a \in \mathcal{C}[x, F(a)]\}_{a\in\mathrm{Ob}(\mathcal{D})}$ takich, że dla każdego morfizmu $\psi \in \mathcal{D}[a,a']$ zachodzi $f_{a'} = F(\psi)f_a$. *Kostożkiem* nad F nazywamy obiekt $y \in \mathrm{Ob}(\mathcal{C})$ wraz z rodziną morfizmów $\{g_a \in \mathcal{C}[F(a), y]\}_{a\in\mathrm{Ob}(\mathcal{D})}$ takich, że dla każdego morfizmu $\psi \in \mathcal{D}[a,a']$ zachodzi $g_a = g_{a'}F(\psi)$.

Definicja 18. Załóżmy, że $\mathcal{D}$ jest małą kategorią, $\mathcal{C}$ dowolną kategorią a $F : \mathcal{D} \to \mathcal{C}$ funktorem. *Granica* F (granica odwrotna), oznaczana $\lim(F)$, to stożek $(x, \{f_a\})$ nad F o następującej własności: dla każdego stożka $(x', \{f'_a\})$ nad F istnieje dokładnie jeden morfizm $u \in \mathcal{C}[x', x]$ taki, że $f'_a = f_a u$ dla $a \in \mathrm{Ob}(\mathcal{D})$. *Kogranica* (granica prosta) F to kostożek $(y, \{g_a\}_{a\in\mathrm{Ob}(\mathcal{D})})$ nad F o następującej własności: dla każdego kostożka $(y', \{g'_a\})$ nad F istnieje dokładnie jeden morfizm $v \in \mathcal{C}[y, y']$ taki, że $g'_a = v g_a$ dla każdego $a \in \mathrm{Ob}(\mathcal{D})$.

Przykład 5. Suma prosta, produkt, jądro, kojądro.

3.2. **Endomorfizmy.** Niech K będzie ustalonym ciałem, a V przestrzenią wektorową nad K o wymiarze n. Oznaczmy $\mathrm{End}(V) := \mathrm{Hom}(V, V)$.

Definicja 19. Macierzą endomorfizmu $\varphi : V \to V$ z bazie $\mathcal{A}$ nazywamy macierz $\mathcal{M}(\varphi)^{\mathcal{A}}_{\mathcal{A}}$.

Dany endomorfizm może mieć różne macierze w różnych bazach. Jeśli $\mathcal{A}, \mathcal{B}$ — bazy V, $\varphi \in \mathrm{End}(V)$ to

$$\mathcal{M}(\varphi)^{\mathcal{B}}_{\mathcal{B}} = \mathcal{M}(\mathrm{id}_V)^{\mathcal{A}}_{\mathcal{B}} \cdot \mathcal{M}(\varphi)^{\mathcal{A}}_{\mathcal{A}} \cdot \mathcal{M}(\mathrm{id}_V)^{\mathcal{B}}_{\mathcal{A}} = (\mathcal{M}(\mathrm{id}_V)^{\mathcal{B}}_{\mathcal{A}})^{-1} \cdot \mathcal{M}(\varphi)^{\mathcal{A}}_{\mathcal{A}} \cdot \mathcal{M}(\mathrm{id}_V)^{\mathcal{B}}_{\mathcal{A}}$$

Definicja 20. Macierze $A, B \in M_{n\times n}(K)$ są *podobne* jeśli istnieje macierz odwracalna $C \in M_{n\times n}(K)$ taka, że $A = C^{-1}BC$. Endomorfizmy $f, g \in \mathrm{End}(V)$ są *sprzężone*, jeśli istnieje automorfizm h taki, że $f = h^{-1}gh$.

Stwierdzenie 21. *Macierze są podobne wtedy i tylko wtedy, gdy są macierzami tego samego endomorfizmu. Endomorfizmy są sprzężone, jeśli w pewnych bazach mają tą samą macierz.*

Cel: sklasyfikować endomorfizmy z dokładnością do sprzężenia, lub równoważnie, macierze z dokładnością do podobieństwa.

3.3. **Niezmienniki endomorfizmów.**

Definicja 22. Funkcję $M_{n\times n}(K) \to X$ nazywamy niezmiennikiem endomorfizmu jeśli jej wartości są takie same na macierzach podobnych. Każdy niezmiennik endomorfizmu zadaje funkcję na $\mathrm{End}(V)$, która nie zależy od klasy sprzężoności endomorfizmu.

Definicja 23. Rząd.

Definicja 24. Wyznacznik.

Definicja 25. *Śladem* macierzy $A = (a_{ij}) \in M_{n\times n}(K)$ nazywamy liczbę $\mathrm{tr}\, A = a_{11} + \cdots + a_{nn}$.

Stwierdzenie 26. *Dla* $A, B \in M_{n\times n}$ *zachodzi* $\mathrm{tr}\, AB = \mathrm{tr}\, BA$.

Wniosek. Ślad jest niezmiennikiem endomorfizmu.

4. Wykład 5 (10 III)

4.1. **Wektory własne i wartości własne.** Niech V będzie n-wymiarową przestrzenią liniową nad ciałem K, a $\varphi : V \to V$ endomorfizmem.

Definicja 27. Niezerowy wektor $\alpha \in V$ nazywamy *wektorem własnym* endomorfizmu φ, jeśli $\varphi(\alpha) = \lambda \cdot \alpha$ dla pewnej wartości $\lambda \in K$. Element λ nazywamy *wartością własną* wektora własnego α.

Definicja 28. Element $\lambda \in K$ nazywamy *wartością własną* endomorfizmu jeśli istnieje wektor własny z wartością własną λ. Przestrzeń

$$V_{(\lambda)} := \{\alpha \in V : \ \varphi(\alpha) = \lambda \cdot \alpha\}$$

nazywamy *podprzestrzenią własna* endomorfizmu φ odpowiadająca wartości własnej λ.

4.2. **Jak znajdować wektory własne i wartości własne? — wielomian charakterystyczny.** Niech A będzie macierzą φ w pewnej bazie.

Stwierdzenie 29. *Następujące warunku są równoważne:*
- $\lambda \in K$ *jest wartością własną* φ,
- $\mathrm{rk}(A - \lambda \cdot I) < n$,
- $\det(A - \lambda \cdot I) = 0$.

Definicja 30. *Wielomianem charakterystycznym macierzy* $A \in M_{n\times n}(K)$ *nazywamy wielomian*

$$w_A(\lambda) = \det(A - \lambda \cdot I).$$

Stwierdzenie 31. *Wielomian charakterystyczny jest niezmiennikiem endomorfizmu.*

Stwierdzenie 32. *Liczba* $\lambda \in K$ *jest wartością własną* φ *wtedy i tylko wtedy, gdy* λ *jest pierwiastkiem wielomianu charakterystycznego.*

Stwierdzenie 33. *Jeśli* K *jest ciałem algebraicznie domkniętym, to każdy endomorfizm przestrzeni* V *posiada wektor własny.*

4.3. **Wartości własne i wektory własne — przykłady.** W poniższych przykładach V jest przestrzenią wymiaru n nad ciałem K, a $A \in M_{n\times n}(K)$ jest macierzą endomorfizmu $\varphi : V \to V$ w pewnej bazie $\mathcal{B}$ przestrzeni V.

Przykład 6. Niech $K = \mathbb{R}$, $A = \begin{pmatrix} 1 & 2 \\ -1 & 4 \end{pmatrix}$. Wówczas

$$w_A(\lambda) = \det \begin{pmatrix} 1-\lambda & 2 \\ -1 & 4-\lambda \end{pmatrix} = (1-\lambda)(4-\lambda) + 2 = \lambda^2 - 5\lambda + 6 = (\lambda-2)(\lambda-3).$$

Wobec tego wartościami własnymi macierzy A są liczby 2 i 3. Żeby znaleźć wektory własne rozwiązujemy jednorodne układy równań $(A-2I)\mathbf{x} = 0$ i $(A-3I)\mathbf{x} = 0$. Otrzymujemy

$$\begin{pmatrix} 1-2 & 2 \\ -1 & 4-2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} -1 & 2 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = 0 \quad \Leftrightarrow \quad (x_1, x_2) \in \operatorname{lin}\{(2,1)\}$$

oraz

$$\begin{pmatrix} 1-3 & 2 \\ -1 & 4-3 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} -2 & 2 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = 0 \quad \Leftrightarrow \quad (x_1, x_2) \in \operatorname{lin}\{(1,1)\}.$$

Wobec tego $V_{(2)} = \operatorname{lin}\{(2,1)\}$ oraz $V_{(3)} = \operatorname{lin}\{(1,1)\}$.

Przykład 7. Niech $K = \mathbb{R}$, $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Wówczas

$$w_A(\lambda) = \det \begin{pmatrix} -\lambda & -1 \\ 1 & -\lambda \end{pmatrix} = \lambda^2 + 1.$$

Wielomian charakterystyczny nie ma peirwiastków, więc A nie ma wektorów ani wartości własnych.

Przykład 8. Niech A będzie tą samą macierzą co w powyższym przykładzie, ale dla $K = \mathbb{C}$. Wówczas $w_A(\lambda) = \lambda^2 + 1$ ma dwa pierwiastki, więc dwie warotści własne: i oraz $-i$. Ponadto $V_{(i)} = \operatorname{lin}\{(1, -i)\}$, $V_{(-i)} = \operatorname{lin}\{(1, i)\}$.

Przykład 9. Niech $K = \mathbb{R}$, $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Wówczas $w_A(\lambda) = \lambda^2$ ma jeden pierwiastek podwójny: 0, a $V_{(0)} = \operatorname{lin}\{(1,0)\}$.

4.4. **Wielomian charakterystyczny — własności.**

Stwierdzenie 34. *Jeśli macierze A, B są podobne, to ich wielomiany charakterystyczne są równe.*

Dowód.

$$w_A(\lambda) = \det(A - \lambda I) = \det(C^{-1}BC - \lambda I) = \det(C^{-1}BC - C^{-1}(\lambda I)C) =$$
$$\det(C^{-1}(B - \lambda I)C) = \det(B - \lambda I) = w_B(\lambda). \quad \square$$

Wielomian charakterystyczny jest więc niezmiennikiem homomorfizmu.

Stwierdzenie 35. *Niech $A \in M_{n\times n}(K)$ i niech*

$$w_A(\lambda) = c_n\lambda^n + c_{n-1}\lambda^{n-1} + \cdots + c_1\lambda_1 + c_0$$

będzie wielomianem charakterystycznym. Wówczas

- $c_n = (-1)^n$,
- $c_{n-1} = (-1)^{n-1}\operatorname{tr}(A)$,
- $c_0 = \det(A)$.

Wniosek. Wielomian charakterystyczny jest niezmiennikiem silniejszym (tj. odróżnia więcej endomorfizmów) niż ślad i wyznacznik. Nie jest jednak silniejszy niż rząd endomorfizmu (patrz ostatni przykład).

4.5. **Macierze diagonalizowalne.** Zakładamy, że V jest n-wymiarową przestrzenią nad K, φ jest endomorfizmem V, a A jest macierzą A w bazie $\mathcal{B}$.

Definicja 36. Macierz $A = (a_{ij}) \in M_{n\times n}(K)$ jest *diagonalna* jeśli $a_{ij} = 0$ dla $i \neq j$. Macierz A jest *diagonalizowalna* jeśli jest podobna do macierzy diagonalnej.

Stwierdzenie 37. *Macierz A jest diagonalna wtedy i tylko wtedy, gdy $\mathcal{B}$ składa się z wektorów własnych endomorfizmu φ. Macierz A jest diagonalizowalna wtedy i tylko wtedy, gdy istnieje baza V składająca się z wektorów własnych φ.*

Stwierdzenie 38. *Jeśli $\alpha_1, \ldots, \alpha_k \in V$ są wektorami własnymi o parami różnych wartościach własnych $\lambda_1, \ldots, \lambda_k$, to układ (α_i) jest liniowo niezależny.*

Dowód. Indukcja po k. Jesli $k = 1$ to jasne. Załóżmy, że $c_1\alpha_1 + \cdots + c_k\alpha_k = 0$. Mamy

$$\varphi(c_1\alpha_1 + \cdots + c_k\alpha_k) = \lambda_1 c_1\alpha_1 + \cdots + \lambda_k c_k\alpha_k$$

i zarazem

$$\varphi(c_1\alpha_1 + \cdots + c_k\alpha_k) = \lambda_k c_1\alpha_1 + \cdots + \lambda_k c_k\alpha_k$$

bo $c_1\alpha_1 + \cdots + c_{k-1}\alpha_{k-1} = -c_k\alpha_k$ jest wektorem własnym z wartością własną λ_k (lub zerem). Po odjęciu dostajemy

$$(\lambda_1 - \lambda_k)c_1\alpha_1 + \cdots + (\lambda_{k-1} - \lambda_k)c_{k-1}\alpha_{k-1} = 0,$$

stąd z założenia indukcyjnego $c_1 = \cdots = c_{k-1} = 0$. □

Stwierdzenie 39. *Niech $V' \subseteq V$ będzie podprzestrzenią rozpiętą przez wszystkie wektory własne endomorfizmu φ i niech $\{\lambda_1, \ldots, \lambda_k\}$ będzie zbiorem wartości własnych endomorfizmu φ. Wówczas*

$$V' = V_{(\lambda_1)} \oplus \cdots \oplus V_{(\lambda_k)}.$$

Stwierdzenie 40. *Niech $\lambda_1, \ldots, \lambda_k$ będą parami różnymi wartościami własnymi φ. Wówczas macierz A jest diagonalizowalna wtedy i tylko wtedy, gdy*

$$n = \dim(V_{(\lambda_1)}) + \dim(V_{(\lambda_2)}) + \cdots + \dim(V_{(\lambda_k)}).$$

Stwierdzenie 41. *Jeśli endomorfizm φ ma n różnych wartości własnych, to jego macierz jest diagonalizowalna.*

Stwierdzenie 42. *Macierz jest diagonalizowalna wtedy i tylko wtedy, gdy jej wymiar jest sumą wymiarów podprzestrzeni własnych.*

Przykład 10. Zdiagonalizować macierz $A = \begin{pmatrix} -1 & 1 & 1 \\ 2 & 0 & -1 \\ -4 & 2 & 3 \end{pmatrix}$.

5. Wykład 6 (15 III)

5.1. **Wielomiany a macierze.**

Stwierdzenie 43. *Dla dowolnej macierzy $A \in M_{n\times n}(K)$ istnieje dokładnie jeden unormowany wielomian $\mu_A(x) \in K[x]$, zwany* wielomianem minimalnym, *taki, że jeśli $w(A) = 0$, to μ_A dzieli w.*

Dowód. Jeśli $w(A) = v(A) = 0$ i $r(x)$ jest resztą z dzielenia w przez v, to $r(A) = 0$. □

Twierdzenie 44 (Cayley-Hamilton)**.** *Dla każdej macierzy $A \in M_{n\times n}(K)$ zachodzi $w_A(A) = 0$.*

Definicja 45. *Macierz dołączona* macierzy $A \in M_{n\times n}(K)$ to macierz $B = (b_{ij}) \in M_{n\times n(K)}$ taka, że $b_{ij} = (-1)^{i+j}\det(A_{ji})$, gdzie A_{ij} jest macierzą powstała przez usunięcie i-tego wiersza i j-tej kolumny z macierzy A.

Stwierdzenie 46. *Jeśli B jest dołączona do A, to $AB = BA = \det(A) \cdot I$.*

Dowód tw. C-H. Niech $B \in M_{n\times n}(K[\lambda])$ będzie macierzą dołączoną do $\lambda I - A$ (o współczynnikach w $K[\lambda]$). Mamy

$$(\lambda I - A)B = \det(\lambda I - A)I = \pm w_A(\lambda)I.$$

Ponieważ stopnie wielomianów w B nie przekraczają $n-1$, mamy przedstawienie

$$B = \sum_{i=0}^{n-1} \lambda^i B_i,$$

gdzie $B_i \in M_{n\times n}(K)$. Mamy

$$\begin{aligned} w_A(\lambda)I = (\lambda I - A)B = (\lambda I - A)\sum_{i=0}^{n-1}\lambda^i B_i = \sum_{i=0}^{n-1}\lambda^{i+1}B_i - \sum_{i=0}^{n-1}\lambda^i AB_i \\ = \lambda^n B_{n-1} + \sum_{i=1}^{n-1}\lambda^i(B_{i-1} - AB_i) - AB_0. \end{aligned}$$

Oznaczmy $\pm w_A(\lambda)I = \lambda^n I + \lambda^{n-1}c_{n-1}I + \cdots + \lambda c_1 I + c_0 I$. Wobec tego $B_{n-1} = I$, $-AB_0 = c_0 I$ oraz

$$B_{i-1} - AB_i = c_i I$$

dla $i \in \{1,\ldots,n-1\}$. Ostatecznie

$$\pm w_A(A) = A^n B_{n-1} + A^{n-1}(B_{n-2} - AB_{n-1}) + A^{n-2}(B_{n-3} - AB_{n-2}) + \cdots + A(B_0 - AB_1) - AB_0 = 0.$$

□

Stwierdzenie 47. *Wielomian minimalny dzieli wielomian charakterystyczny.*

5.2. **Podprzestrzenie niezmiennicze.** Niech f będzie endomorfizmem przestrzeni V wymiaru n nad ciałem K.

Definicja 48. Podprzestrzeń $W \subseteq V$ jest *f-niezmiennicza* jeśli $\varphi(W) \subseteq W$. W szczególności $f|_W$ jest endomorfizmem przestrzeni W.

Definicja 49. Rozkład $V = W_1 \oplus \cdots \oplus W_k$ jest *f-niezmienniczy* jeśli wszystkie podprzestrzenie W_i są f-niezmiennicze.

Stwierdzenie 50. *Jeśli $W \subseteq V$ jest f-niezmiennicza. Niech $\mathcal{B} = (\beta_1,\ldots,\beta_n)$ będzie bazą V taką, że $(\beta_1,\ldots,\beta_m)$ jest bazą przestrzeni W. Wówczas*

$$M(\varphi)^{\mathcal{B}}_{\mathcal{B}} = \begin{pmatrix} L & M \\ 0 & N \end{pmatrix},$$

gdzie L jest macierzą $f|_W$ w bazie $(\beta_1,\ldots,\beta_m)$.

Stwierdzenie 51. *Jeśli rozkład $V = W_1 \oplus \cdots \oplus W_k$ jest f-niezmienniczy, a $\mathcal{B} = (\beta_1,\ldots,\beta_n)$ jest sumą baz przestrzeni W_i, to $M(\varphi)^{\mathcal{B}}_{\mathcal{B}}$ jest diagonalna.*

Definicja 52. Mówimy, że V jest *f-nierozkładalna* jeśli nie istnieje nietrywialny rozkład f-niezmienniczy przestrzeni V.

Stwierdzenie 53. *Niech $\varphi \in \mathrm{End}(V)$. Wówczas istnieje φ-niezmienniczy rozkład*

$$V = W_1 \oplus \cdots \oplus W_k$$

taki, że W_i jest $f|_{W_i}$-nierozkładalna.

Definicja 54. *Podprzestrzenią pierwiastkową* endomorfizmu $f \in \mathrm{End}(V)$ wartości własnej $\lambda \in K$ nazywamy przestrzeń

$$V_\lambda = \bigcup_{n>0} \ker(f - \lambda\,\mathrm{id})^n.$$

6. Wykład 7 (17 III)

6.1. Twierdzenie Jordana.

Twierdzenie 55. *Niech*

- *K będzie ciałem algebraicznie domkniętym,*
- *V będzie n-wymiarową przestrzenią liniową nad K,*
- *$f \in \operatorname{End}(V)$.*

Jeśli V jest f-nierozkładalna, to $f = g + \lambda \cdot \mathrm{id}_V$, gdzie $g : V \to V$ jest endomorfizmem takim, że $g^{n-1} \neq 0$, $g^n = 0$.

Stwierdzenie 56. *Jeśli $g \in \operatorname{End}(V)$ spełnia warunki $g^{n-1} \neq 0$, $g^n = 0$, gdzie $n = \dim(V)$, to*

- *V jest g-nierozkładalna,*
- *istnieje baza V w której g jest zadane macierzą*

$$J = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & 0 & \dots & 0 & 0 \end{pmatrix}.$$

Dowód. Zauważmy, że $\operatorname{im}(g^k) \subseteq \operatorname{im}(g^{k-1})$. Jeśli $\dim(\operatorname{im} g^k) = \dim(\operatorname{im} g^{k-1})$, to $\operatorname{im} g^k = \operatorname{im} g^{k-1}$ i wówczas $\operatorname{im} g^l = \operatorname{im} g^k$ dla $l \geqslant k$. Oznaczmy $Z_k = \operatorname{im} g^k$; mamy $\dim(Z_k) = n - k$ dla $k \leqslant n$. Niech β_1 będzie wektorem rozpinającym Z_{n-1}. Istnieje β_2 takie, że $g(\beta_2) = \beta_1$, itd. Tak konstruujemy bazę (β_i), łatwo sprawdzić, że macierz w bazie jest odpowiednia. Teraz załóżmy, że $V = W_1 \oplus W_2$ jest g-niezmienniczym rozkładem. Jedna z nich musi zawierać wektor postaci $\beta_n + \sum_{i<n} c_i \beta_i$, więc musi być równa V. □

Definicja 57. *Suma prosta macierzy.*

Definicja 58. *Klatką Jordana* nazywamy macierz postaci $J + \lambda \cdot I$. *Macierzą Jordana* nazywamy macierz, która jest sumą prostą klatek Jordana. *Bazą Jordana* endomorfizmu $f \in \operatorname{End}(V)$ nazywamy bazę, w której macierz f jest macierzą Jordana.

Twierdzenie 59 (Jordan raz jeszcze)**.** *Dla każdego endomorfizmu przestrzeni wektorowej nad ciałem algebraicznie istnieje baza Jordana.*

6.2. Dowód tw. Jordana.

Lemat 60 (N)**.** *Niech $V \in \mathbf{Vect}_K$, $f \in \operatorname{End}(V)$, $\alpha \in V$. Załóżmy, że $f^n(\alpha) = 0$ i $f^{n-1}(\alpha) \neq 0$. Wówczas układ $(\alpha, f(\alpha), \dots, f^{n-1}(\alpha))$ jest liniowo niezależny.*

Dowód. Indukcja ze względu do n. Jeśli $n = 1$, to z założenia $\alpha = f^0(\alpha) \neq 0$, więc (α) jest układem liniowo niezależnym. Załóżmy, że $n > 1$ oraz że $c_0\alpha + c_1 f(\alpha) + \dots + c_{n-1} f^{n-1}(\alpha) = 0$ dla pewnego ciągu liczb $c_0 \dots, c_{n-1} \in K$. Mamy

$$\begin{aligned} 0 = f(0) = f(c_0\alpha + c_1 f(\alpha) + \dots + c_{n-1} f^{n-1}(\alpha)) &= c_0 f(\alpha) + c_1 f^2(\alpha) + \dots + c_{n-1} f^n(\alpha) \\ &= c_0 f(\alpha) + c_1 f^2(\alpha) + \dots + c_{n-2} f^{n-1}(\alpha) \end{aligned}$$

więc z założenia indukcyjnego dla wektora $f(\alpha)$ dostajemy $c_0 = \dots = c_{n-2} = 0$. Ale stąd $c_{n-1} f^{n-1}(\alpha) = 0$, więc również c_{n-1}. □

Lemat 61 (K)**.** *Niech $V \in \mathbf{Vect}_K$, $f \in \operatorname{End}(V)$. Załóżmy, że $\dim(V) = n$, $f^n = 0$, $f^{n-1} \neq 0$. Wówczas w pewnej bazie macierzą f jest klatka Jordana typu $(0, n)$; w szczególności $\dim\ker(f) = 1$.*

Dowód. Istnieje $\alpha \in V$ takie, że $f^{n-1}(\alpha) \neq 0$ (i oczywiście $f^n(\alpha) = 0$). Z powyższego lematu $(\alpha, \dots, f^{n-1}(\alpha))$ jest bazą V. Łatwo zauważyć, że macierz f w tej bazie to klatka Jordana typu $(0, n)$. □

Lemat 62 (S)**.** *Niech $V \in \mathbf{Vect}_K$, $f \in \operatorname{End}(V)$. Jeśli $V = V_1 \oplus \dots \oplus V_k$ jest f-niezmienniczym rozkładem, to*

$$\ker f = (V_1 \cap \ker(f)) \oplus \dots \oplus (V_k \cap \ker(f)).$$

Dowód. Zawieranie $\supseteq$ jest jasne. W drugą stronę — korzystamy z niezmienniczości rozkładu. $\square$

Twierdzenie 63. *Niech K — ciało algebraicznie domknięte, $V \in \mathbf{Vect}_K$, $\dim(V) = n$, $f \in \mathrm{End}(V)$. Załóżmy, że*

- *V jest f-nierozkładalna,*
- *0 jest wartością własną f.*

Wówczas $f^n = 0$, $f^{n-1}(0)$.

Dowód. A. Indukcja ze względu na n. Dla $n = 1$ mamy $f = 0$, bo 0 jest wartością własną, więc teza jest spełniona.

B. Załóżmy, że $n > 1$. Ponieważ $\ker(f) \neq 0$, to $\dim(\mathrm{im}(f)) < n$. Niech

$$\mathrm{im}(f) = V_1 \oplus \cdots \oplus V_k$$

będzie f-niezmienniczym rozkładem na składniki f-nierozkładalne. Oznaczmy $n_i = \dim(V_i)$.

C. Po przenumerowaniu składników możemy zakładać, że 0 jest wartością własną składników $V_1, \ldots, V_s$, a nie jest wartością własną składników $V_{s+1}, \ldots, V_k$.

D. Dla każdego $i = 1, \ldots, s$ wybierzmy wektor $\alpha_i \in V_i$ taki, że $f^{n_i}(\alpha_i) = 0$ oraz $f^{n_i-1}(\alpha_i) \neq 0$ — istnieje on z założenia indukcyjnego dla przestrzeni V_i. Następnie wybierzmy wektor $\beta_i \in V$ taki, że $f(\beta_i) = \alpha_i$ (istnieje, bo $\alpha_i \in \mathrm{im}(f)$). Oznaczmy $V_i' = \mathrm{lin}(V_i \cup \{\beta_i\})$. Oczywiście $f(V_i') \subseteq V_i \subseteq V_i'$, więc V_i' jest f-niezmiennicza.

E. Niech $W \subseteq V$ będzie podprzestrzenią taką, że

$$\ker(f) = (\ker(f) \cap \mathrm{im}(f)) \oplus W.$$

Oczywiście W jest f-niezmiennicza (bo $W \subseteq \ker(f)$).

F. Udowodnimy, że $V = \mathrm{lin}(V_1' \cup \cdots \cup V_s' \cup V_{s+1} \cup \cdots \cup V_k \cup W)$. Niech $\alpha \in V$. Wówczas $f(\alpha)$ ma jednoznaczny rozkład

$$f(\alpha) = \gamma_1 + \cdots + \gamma_k,$$

gdzie $\gamma_i \in V_i$. Dla $i \leqslant s$ mamy przestawienie $\gamma_i = c_i\alpha_i + f(\delta_i)$, gdzie $\delta_i \in V_i$ (korzystamy z faktu, że $(\alpha_i, f(\alpha_i), \ldots, f^{n_i-1}(\alpha_i))$ jest bazą V_i). Niech teraz

$$\alpha' := (c_1\beta_1 + \delta_1) + \cdots + (c_s\beta_s + \delta_s) + (f|_{V_{s+1}})^{-1}(\gamma_{s+1}) + \cdots + (f|_{V_k})^{-1}(\gamma_k).$$

Jest to dobra definicja, bo z założenia $f|_{V_i}$ jest odwracalne. Ponadto mamy

$$f(\alpha') = \sum_{i=1}^{s}(f(c_i\beta_i) + f(\delta_i)) + \sum_{i=s+1}^{k} f((f|_{V_i})^{-1}(\gamma_i)) = \sum_{i=1}^{s}(c_i\alpha_i + f(\delta_i)) + \sum_{i=s+1}^{k}\gamma_i = f(\alpha)$$

Wobec tego $f(\alpha - \alpha') = 0$, czyli $\alpha \in \mathrm{lin}(\{\alpha'\} \cup \ker(f))$. Ostatecznie

$$\alpha \in \mathrm{lin}(\bigcup_{i \leqslant s} V_i' \cup \bigcup_{i>s} V_i \cup \mathrm{im}(f) \cup W).$$

G. Zauważmy, że

$$\sum_{i \leqslant s}\dim(V_i') + \sum_{i>s}\dim(V_i) + \dim(W) = \dim(\mathrm{im}(f)) + s + \dim(\ker(f)) - \dim(\ker(f) \cap \mathrm{im}(f)).$$

Z lematu (S) powyżej mamy

$$\mathrm{im}(f) \cup \ker(f) = (V_1 \cap \ker(f)) \cap \cdots \cap (V_k \cap \ker(f)).$$

Ponadto $\dim(V_i \cap \ker(f)) = 1$ dla $i \leqslant s$ (z lematu (K)) i $\dim(V_i \cap \ker(f)) = 0$ dla $i > s$ (bo $f|_{V_i}$ jest izomorfizmem). Wobec tego $\dim(\ker(f) \cap \mathrm{im}(f)) = s$. Ostatecznie

$$\sum_{i \leqslant s}\dim(V_i') + \sum_{i>s}\dim(V_i) + \dim(W) = \dim(\mathrm{im}(f)) + \dim(\ker(f)) = n.$$

Z poprzedniego punktu możemy więc wywnioskować, że istnieje f-niezminniczy rozkład.

$$V = V_1' \oplus \cdots \oplus V_s' \oplus V_{s+1} \oplus \cdots \oplus V_k \oplus W.$$

H. Wobec założenia, że V jest f-nierozkładalna tylko jeden ze składników jest niezerowy. Mamy trzy przypadki:

- $V = W$. Ale wtedy $\dim(W) > 1$ i $f|_W = 0$, więc $W = V$ nie byłaby nierozkładalna.
- $V = V_i$. Ale wtedy 0 nie jest wartością własną V.
- $V = V_i' = \operatorname{lin}(V_i \cup \{\beta_i\})$. Wtedy $f^n = 0$ i $f^{n-1}(\beta_i) = f^{n-2}(\alpha_i) \neq 0$. Teza indukcyjna jest więc spełniona. □

7. Wykład 8 (22 III)

7.1. Wnioski z tw. Jordana.

Stwierdzenie 64. *Niech K — ciało algebraicznie domknięte, $V \in \mathbf{Vect}_K$, $\dim(V) = n$, $f \in \operatorname{End}(V)$. Załóżmy, że V jest f-nierozkładalna. Wówczas istnieje baza, w której macierz f jest klatką Jordana.*

Dowód. Niech $\lambda \in K$ będzie wartością własną f. Wówczas 0 jest wartością własną $g = f - \lambda \cdot \mathrm{id}$. Łatwo zauważyć, że f-nierozkładaność i g-nierozkładalność są równoważne, więc V jest g-nierozkładalna. Wobec tego $g^n = 0$, $g^{n-1} \neq 0$, a więc macierzą g w pewnej bazie jest klatka Jordana typu $(0, n)$. W tej samej bazie macierzą f jest klatka Jordana typu (λ, n). □

Wniosek. Jeśli K jest ciałem algebraicznie domkniętym, V przestrzenią nad K, a $f : V \to V$ endomorfizmem. Wówczas w pewnej bazie macierz f jest macierzą Jordana.

Twierdzenie 65. *Niech $V \in \mathbf{Vect}_K$, K — dowolne ciało, $f \in \operatorname{End}(V)$. Jeśli w_f rokłada się na iloczyn czynników liniowych, to V ma bazę Jordana.*

Dowód jest analogiczny do dowodu tw. Jordana dla ciała algebraicznie domkniętego. Należy zauważyć, że założenie rozkładalności wielomianu charakterystycznego implikuje istnienie wartości własnej oraz skorzystać z poniższego lematu, który gwarantuje działanie indukcji:

Lemat 66. *Wielomian w_f dzieli się przez $w_{f|_{\operatorname{im}(f)}}$.*

Dowód. Niech $\beta_1, \dots, \beta_n$ będzie bazą V taką, że $\beta_1, \dots, \beta_s$ jest bazą $\operatorname{im}(f)$. Wówczas macierz f w bazie $\mathcal{B}$ ma postać

$$\begin{pmatrix} A & B \\ 0 & 0 \end{pmatrix},$$

więc $w_f = w_A w_C$, gdzie w_A jest macierzą $f_{\operatorname{im}(f)}$. □

Podobieństwo macierzy Jordana.

Stwierdzenie 67. *Niech f będzie endomorfizmem przestrzeni liniowej V, którego macierz w pewnej bazie jest macierzą Jordana. Wówczas liczba klatek typu (λ, k) w tej macierzy wynosi*

$$\dim(\ker((f - \lambda \cdot \mathrm{id})^k)) - \dim(\ker((f - \lambda \cdot \mathrm{id})^{k-1})).$$

Dowód. Wystarczy sprawdzić, że jeśli macierzą f jest klatka Jordana typu (μ, n), to

$$\dim(\ker((f - \lambda \cdot \mathrm{id})^k)) = \begin{cases} 0 & \text{jeśli } \lambda \neq \mu, \\ k & \text{jeśli } \lambda = \mu \text{ i } k \leqslant n, \\ n & \text{jeśli } \lambda = \mu \text{ i } k \geqslant n. \end{cases}$$

Wniosek. Macierze Jordana A i B są podobne wtedy i tylko wtedy, gdy dla każdego $\lambda \in K$ i $k > 0$ obie macierze zawierają tą samą ilość klatek Jordana typu (λ, k).

Dowód. Jeśli macierze zawierają taką samą ilość klatek danego typu, można uzyskać jedną z drugiej przez przenumerowanie bazy. Jeśli ilości są różne, wartości wyrażeń powyżej są różne, a są one niezmiennikami endomorfizmu. □

7.2. **Podprzestrzenie pierwiastkowe.** Niech V będzie przestrzenią liniową nad ciałem K wymiaru n, a f endomorfizmem V.

Definicja 68. *Podprzestrzenią pierwiastkową* endomorfizmu f dla wartości własnej $\lambda \in K$ nazywamy podprzestrzeń

$$V^{\infty}_{(\lambda)} := \bigcup_{k \geqslant 1} \ker((f - \lambda \cdot \mathrm{id})^k).$$

Stwierdzenie 69. *Załóżmy, że ciało K jest algebraicznie domknięte, i że $\lambda_1, \dots, \lambda_s \in K$ są różnymi wartościami własnymi. Wówczas istnieje rozkład*

$$V = V^{\infty}_{(\lambda_1)} \oplus \cdots \oplus V^{\infty}_{(\lambda_s)}.$$

Dowód. Przez macierz Jordana. □

Twierdzenie Jordana dla $\mathbb{R}$.

Definicja 70. *Uogólnioną klatką Jordana* nazywamy macierz

$$\begin{pmatrix} A & I & 0 & \dots & 0 & 0 \\ 0 & A & I & \dots & 0 & 0 \\ 0 & 0 & A & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & A & I \\ 0 & 0 & 0 & \dots & 0 & A \end{pmatrix},$$

gdzie $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $I = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, $a, b \in \mathbb{R}$.

Twierdzenie 71. *Jeśli V jest f-nierozkładalną przestrzenią liniową nad $\mathbb{R}$, to macierz f jest w pewnej bazie klatką Jordana — zwykłą lub uogólnioną.*

7.3. **Zastosowanie twierdzenia Jordana — liczenie potęg macierzy.**

8. Wykład 9 (31 III)

8.1. **Przestrzenie afiniczne.**

Definicja 72. *Przestrzenią afiniczną* nad ciałem K nazywamy trójkę $(A, T_A, +)$, gdzie

- A jest niepustym zbiorem,
- T_A jest przestrzenią liniową nad ciałem K,
- $+$ jest działaniem $A \times T_A \ni (p, \alpha) \mapsto p + \alpha \in A$,

i spełnione są następujące warunki:

- $p + 0 = p$ dla $p \in A$,
- $(p + \alpha) + \beta = p + (\alpha + \beta)$ dla $p \in A$, $\alpha, \beta \in T_A$,
- dla każdych $p, q \in A$ istnieje dokładnie jeden wektor $\alpha \in T_A$ taki, że $p + \alpha = q$.

Elementy A nazywamy *punktami*, elementy T_A *wektorami*, a przestrzeń T_A *przestrzenią styczną* do przestrzeni afinicznej A. Ostatni aksjomat pozwala na zdefiniowanie działania $- : A \times A \to T_A$, które parze punktów p, q przyporządkowuje dokładnie jeden wektor $(p - q)$ taki, że $q + (p - q) = p$.

Stwierdzenie 73. *Niech A będzie przestrzenią afiniczną i niech $p, q, r \in A$, $\alpha \in T_A$. Wówczas*

- $(p - q) = -(q - p)$,
- $(q - p) + (r - q) = (r - p)$,
- $(p + \alpha) - q = \alpha + (p - q) = p - (q + (-\alpha))$.

8.2. **Przykłady przestrzeni afinicznych.**

Przykład 11. Niech V będzie przestrzenią liniową. Przestrzeń afiniczną $(V, V, +)$ nazywamy *kanoniczną przestrzenią afiniczną nad* V. Szczególny przypadek: przestrzeń kartezjańska K^n.

Przykład 12. Niech $V \in \mathbf{Vect}_K$, $W \subseteq V$, $[\alpha] \in V/W$. Przestrzeń $(\alpha + W, W, +)$ jest przestrzeni afiniczną.

Przykład 13. Niech R będzie układem równań liniowych, niekoniecznie jednorodnym. Wówczas przestrzeń $(S_R, V_R, +)$, gdzie

- S_R jest zbiorem rozwiązań układu R,
- V_R jest przestrzenią rozwiązań układu jednorodnego odpowiadającego R

jest przestrzenią afiniczną rozwiązań układu R.

Definicja 74. Niech $A \in \mathbf{Aff}_K$, $p \in A$. Odwzorowanie

$$\kappa_p : T_A \ni \alpha \mapsto p + \alpha \in A$$

nazywamy *mapą* o środku w punkcie p; z definicji jest to bijekcja.

8.3. **Podprzestrzenie afiniczne.**

Definicja 75. *Podprzestrzenią afiniczną* przestrzeni afinicznej A nazywamy przestrzeń afiniczną B taką, że $B \subseteq A$ oraz $T_B \subseteq T_A$.

Uwaga. Przestrzeń styczna T_B jest wyznaczona jednoznacznie przez zbiór punktów B — dokładniej $T_B = \{q - p : \ p, q \in B\}$.

Przykład 14. Niech A będzie przestrzenią afiniczną, $p \in A$ oraz $V \subseteq T_A$ podprzestrzenią liniową. Wówczas $(p + V, V, +|_{p+V})$, gdzie $p + V = \{p + \alpha : \ \alpha \in V\}$ jest podprzestrzenią afiniczną A. Każda podprzestrzeń afiniczna jest tej postaci.

Stwierdzenie 76. *Jeśli $B, C \subseteq A$ są podprzestrzeniami afinicznymi, to $B \cap C$ jest albo zbiorem pustym, albo podprzestrzenią afiniczną A. Ponadto $T_{B\cap C} = T_B \cap T_C$.*

8.4. **Przekształcenia afiniczne.**

Definicja 77. Niech A, B będą przestrzeniami afinicznymi. *Przekształceniem afinicznym* z A do B nazywamy parę (f, T_f), gdzie $f : A \to B$ jest funkcją, $T_f : T_A \to T_B$ przekształceniem liniowym i spełniony jest warunek $f(p + \alpha) = f(p) + T_f(\alpha)$ dla $p \in A$, $\alpha \in T_A$.

Definicja 78. Niech $f : A \to B$ będzie przekształceniem afinicznym.

- *Obrazem* f nazywamy przestrzeń afiniczną $\mathrm{im}(f) = f(A)$, gdzie $T_{\mathrm{im}(f)} = \mathrm{im}(T_f)$.
- *Przeciwobrazem punktu* $q \in \mathrm{im}(f)$ nazywamy przestrzeń afiniczną $f^{-1}(q)$, gdzie $T_{f^{-1}(q)} = \ker(T_f)$.

8.5. **Kombinacje afiniczne.**

Stwierdzenie 79. *Niech $p_i \in A$, $c_i \in K$ dla $1 \leqslant i \leqslant k$. Jeśli $\sum c_i = 1$, to wyrażenie*

$$p + \sum_{i=1}^{k} c_i(p_i - p)$$

nie zależy od wyboru punktu $p \in A$.

Dowód. Niech $q \in A$, $\alpha = \sum c_i(p_i - p)$, $\beta = \sum c_i(p_i - q)$. Trzeba pokazać, że $p + \alpha = q + \beta$, czyli $p + \alpha - \beta = q$, czyli $q - p = \alpha - \beta$. Mamy

$$\alpha - \beta = \sum_{i=1}^{k} c_i(p_i - p) - \sum_{i=1}^{k} c_i(p_i - q) = \sum_{i=1}^{k} c_i((p_i - p) - (p_i - q)) = \sum_{i=1}^{k} c_i(q - p) = q - p. \qquad \square$$

Definicja 80. *Kombinacją afiniczną punktów* $p_1, \ldots, p_k$ w przestrzeni afinicznej A o współczynnikach $c_1, \ldots, c_k$, $c_i \in K$, $\sum c_i = 1$ nazywamy wyrażenie

$$c_1 p_1 + \cdots + c_k p_k := p + (c_1(p_1 - p) + \cdots + c_k(p_k - p)) \in A.$$

8.6. **Przestrzeń rozpięta.**

Definicja 81. Niech A będzie przestrzenią afiniczną i $X \subseteq A$ dowolnym podzbiorem. *Przestrzenią rozpiętą* przez zbiór X nazywamy podprzestrzeń afiniczną A daną przez

$$\mathrm{af}(X) = \left\{ \sum_{i=1}^{k} c_i p_i \in A : \ c_i \in K, \ p_i \in X, \ \sum_{i=1}^{k} c_i = 1 \right\}.$$

$$T_{\mathrm{af}(X)} = \mathrm{lin}\{q - p : \ p, q \in X\}.$$

Stwierdzenie 82. *Powyższa definicja jest poprawna.*

Dowód. Wystarczy pokazać, że dla każdych $p, q \in \mathrm{af}(X)$ istnieje $\alpha \in T_{\mathrm{af}(X)}$ takie, że $p + \alpha = q$ (jednoznaczność wynika bezposrednio z definicji). Mamy $p = \sum_i c_i p_i$ i $q = \sum_j d_j q_j$, gdzie $p_i \in X$, $q_j \in X$. Wybierzmy $r \in X$. Mamy

$$p + \sum_i c_i(r - p_i) + \sum_j d_j(q_j - r) = r + \sum_j d_j(q_j - r) = q. \qquad \square$$

Stwierdzenie 83. $\mathrm{af}(X)$ *jest przecięciem wszystkich przestrzeni liniowych zawierających* X.

9. Wykład 10 (5 IV)

9.1. **Afiniczna niezależność.**

Definicja 84. Układ punktów $p_0, \ldots, p_k \in A$ nazywamy *afinicznie zależnym*, jeśli istnieje $0 \leqslant i \leqslant k$ takie, że p_i jest kombinacją afiniczną punktów $p_0, \ldots, p_{i-1}, p_{i+1}, \ldots, p_k$. Układ nazywamy *afinicznie niezależnym*, jeśli nie jest afinicznie zależny.

Stwierdzenie 85. *Niech $A \in \mathbf{Aff}_K$, $p_0, \ldots, p_k \in A$. Wówczas układ $(p_0, \ldots, p_k)$ jest afinicznie niezależny wttw układ $(p_1 - p_0, p_2 - p_0, \ldots, p_k - p_0)$ jest liniowo niezależny.*

Dowód. Załóżmy, że $p_0, \ldots, p_k$ jest afinicznie zależny. Wówczas

$$p_s = \sum_{i \neq s} c_i p_i = p_s + \sum_{i \neq s} c_i(p_i - p_s)$$

więc

$$0 = \sum_{i \neq s} c_i(p_i - p_s) = \sum_{i \neq s} c_i(p_i - p_0) - c_i(p_s - p_0) = -(p_s - p_0) + \sum_{i \neq 0,s} c_i(p_i - p_0),$$

mamy więc kombinację liniową z niezerowym współczynnikiem (-1 lub c_i). Jeśli układ $(p_i - p_0)$ jest liniowo zależny, to

$$\sum_{i=1}^{k} c_i(p_i - p_0) = 0$$

dla pewnych $c_1, \ldots, c_k$ nie wszystkich równych 0. Jeśli $0 \neq s = \sum_{i=1}^{k} c_i$, to mamy

$$p_0 = p_0 + \sum_{i=1}^{k} \frac{c_i}{s}(p_i - p_0) = \sum_{i=1}^{k} \frac{c_i}{s} p_i,$$

czyli punkt p_0 jest kombinacją afiniczną pozostałych punktów. Jeśli $\sum_{i=1}^{k} c_i = 0$, to wybierzmy $j \in \{1, \ldots, k\}$ takie, że $c_j \neq 0$. W tym przypadku

$$\sum_{i \neq j} -\frac{c_i}{c_j} = 1, \qquad (p_j - p_0) = \sum_{i \neq j} -\frac{c_i}{c_j}(p_i - p_0)$$

więc mamy

$$p_j = p_0 + (p_j - p_0) = p_0 + \sum_{i \neq j} -\frac{c_i}{c_j}(p_i - p_0) = \sum_{i \neq j} -\frac{c_i}{c_j} p_i. \qquad \square$$

Stwierdzenie 86. *Niech $A \in \mathbf{Aff}_K$ i niech $p_0, \dots, p_k \in A$ będzie układem afinicznie niezależnym. Wówczas jeśli*

$$p = \sum_{i=0}^{k} c_i p_i = \sum_{i=0}^{k} d_i p_i$$

dla $\sum c_i = \sum d_i = 1$, to $c_i = d_i$ dla każdego $i \in \{0, \dots, k\}$.

Dowód. Mamy

$$p = p_0 + \sum_{i=1}^{k} c_k(p_i - p_0) = p_0 + \sum_{i=1}^{k} d_k(p_i - p_0).$$

Z liniowej niezależności mamy $c_i = d_i$. $\square$

9.2. **Baza wektorowa.**

Definicja 87. *Bazą wektorową* przestrzeni afinicznej A nazywamy ciąg $(o; \beta_1, \dots, \beta_n)$, gdzie $o \in A$ oraz $(\beta_i)_{i=1}^n$ jest bazą T_A.

Stwierdzenie 88. *Jeśli $(o; \beta_1, \dots, \beta_n)$ jest bazą A, to każdy punkt $p \in A$ można jednoznacznie zapisać w postaci $o + \sum c_i(p)\beta_i$. Łatwo zauważyć, że $c_i(p) = \beta_i^*(\kappa_o^{-1}(p))$ — funkcje c_i nazywamy* współrzędnymi *punktu p w bazie $(o; \beta_1, \dots, \beta_n)$.*

Stwierdzenie 89. *Istnieje jednoznaczna odpowiedniość pomiędzy bazami wektorowymi A a izomorfizmami $f : K^n \to A$.*

Dowód. Baza $(o; \beta_1, \dots, \beta_n)$ wyznacza przekształcenie dane wzorem $(x_1, \dots, x_n) \mapsto o + x_1\beta_1 + \dots + x_n\beta_n$, a izomorfizm $f : K^n \to A$ bazę $(f(0); f(e_1) - f(0), \dots, f(e_n) - f(0))$. $\square$

Wniosek. Każda skończenie wymiarowa przestrzeń afiniczna jest izomorficzna z przestrzenią kartezjańską.

9.3. **Baza punktowa.**

Definicja 90. Ciąg punktów $(p_0, \dots, p_n)$ nazywamy *bazą punktową* jeśli jest afinicznie niezależny oraz zachodzi $\mathrm{af}(\{p_0, \dots, p_n\}) = A$.

Stwierdzenie 91. *Następujące warunki są równoważne:*

- *$(p_0, \dots, p_n)$ jest bazą,*
- *jest maksymalnym zbiorem afinicznie niezależnym,*
- *jest minimalnym zbiorem rozpinającym.*

Stwierdzenie 92. *Jeśli $(p_0, \dots, p_n)$ jest bazą punktową A, to każdy punkt $p \in A$ można jednoznacznie zapisać jako $\sum t_i p_i$, $\sum t_i = 1$.*

Dowód. Istnienie wynika z rozpinania, a jednoznaczność ze stwierdzenia powyżej, bo jeśli $p \in A$ oraz

$$p = \sum_{i=0}^{n} t_i p_i = \sum_{i=0}^{n} t_i' p_i,$$

to

$$p_0 + \sum_{i=1}^{n} t_i(p_i - p_0) = p_0 + \sum_{i=1}^{n} t_i'(p_i - p_0)$$

więc $t_i = t_i'$ z niezależności układów $(p_i - p_0)$, $i = 1, \dots, n$. $\square$

Stwierdzenie 93. *Istnieje jednoznaczna odpowiedniość pomiędzy bazami punktowymi n-wymiarowej przestrzeni afinicznej A, a izomorfizmami afinicznymi $S^n \to A$, gdzie*

$$S^n = \{(t_0, \dots, t_n) \in K^{n+1} : \sum_{i=0}^{n} t_i = 1\}.$$

Dowód. Jeśli $f : S^n \to A$ jest izomorfizmem, to odpowiada mu baza $p_i = f(0, \dots, 0, 1, 0, \dots, 0)$, gdzie jedynka jest na i-tym miejscu. Bazie (p_i) odpowiada przekształcenie afiniczne $f((t_0, \dots, t_n)) = t_0p_0 + \dots + t_np_n$. $\square$

Stwierdzenie 94. *Każdej bazie wektorowej odpowiada baza punktowa i na odwrót:*

$$\mathcal{B} = (o; \beta_1, \ldots, \beta_n) \mapsto (o, o + \beta_1, \ldots, o + \beta_n) = \mathcal{P}$$

$$(p_0, p_1, \ldots, p_n) \mapsto (p_0; p_1 - p_0, \ldots, p_n - p_0).$$

Łatwo zauważyć, że jeśli punkt w bazie wektorowej $\mathcal{B}$ ma współrzędne $(c_1, \ldots, c_n)$, to jego współrzędne w bazie punktowej $\mathcal{P}$ to $(1 - \sum c_i, c_1, \ldots, c_n)$. Na odwrót, punkt $(t_0, t_1, \ldots, t_n)$ ma współrzędne $(t_1, \ldots, t_n)$.

10. Wykład 11 (7 IV)

10.1. Opis przekształceń afinicznych.

Stwierdzenie 95. *Niech A będzie przestrzenią afiniczną z bazą wektorową $(o; \alpha_1, \ldots, \alpha_n)$, a B bazę $(o'; \beta_1, \ldots, \beta_m)$. Wówczas każde przekształcenie afiniczne $f : A \to B$ ma postać*

$$\mathbf{x} \mapsto A\mathbf{x} + \mathbf{b},$$

gdzie $A = M(T_f)^{(\beta_1,\ldots,\beta_m)}_{(\alpha_1,\ldots,\alpha_n)} \in M_{m\times n}(K)$, $\mathbf{b} = f(o)^{(\beta_1,\ldots,\beta_m)} \in M_{m\times 1}(K)$.

Stwierdzenie 96. *Niech A, B mają bazy punktowe $(p_0, \ldots, p_n)$, $(q_0, \ldots, q_m)$ odpowiednio. Wówczas dowolne przekształcenie $f : A \to B$ dane jest wzorem*

$$\mathbf{t} \mapsto A\mathbf{t}$$

gdzie $A \in M_{(m+1)\times(n+1)}(K)$ oraz $\sum_{i=1}^{m+1} a_{ij} = 1$.

Definicja 97. Niech A, B będą przestrzeniami afinicznymi nad ciałem K. *Przestrzeń przekształceń afinicznych* z A do B to trójka $(\mathit{Aff}(A, B), \mathit{Aff}(A, T_B), +)$, gdzie

- $\mathit{Aff}(A, B)$ jest zbiorem przekształceń afinicznych $A \to B$,
- $\mathit{Aff}(A, T_B)$ jest zbiorem przekształceń afinicznych $T_A \to B$. Ma on naturalną strukturę przestrzeni wektorowej,
- dodawanie jest dodawaniem funkcji.

Oczywiście $\dim(\mathit{Aff}(A, B)) = (\dim(A) + 1) \dim(B)$.

10.2. Opis podprzestrzeni afinicznych.

Niech $B \subseteq A$ będzie podprzestrzenią afiniczną. Istnieją dwa podstawowe sposoby opisu B:

- przez parametryzację — według bazy punktowej lub wektorowej, tj. jako obraz przekształcenia afinicznego.
- przez przez układ równań (być może niejednorodny), tj. jako przeciwobraz pewnego punktu przy przekształceniu afinicznym.

10.3. Geometria.

Zakładamy, że $K = \mathbb{R}$.

Definicja 98. Mówimy, że dwie podprzestrzenie afiniczne $B_1, B_2 \subseteq A$ są *równoległe* jeśli $T_{B_1} \subseteq T_{B_2}$ lub $T_{B_2} \subseteq T_{B_1}$. Przestrzenie B_1 i B_2 są *silnie równoległe*, jeśli $T_{B_1} = T_{B_2}$.

Twierdzenie 99 (Tales)**.** *Załóżmy, że $b - o = \lambda(a - o)$ oraz $d - o = \mu(c - o)$. Wówczas $\mathrm{lin}\{a - c\} = \mathrm{lin}\{b - d\}$ wtedy i tylko wtedy, gdy $\lambda = \mu$ lub gdy o, a, b, c, d leżą na wspólnej prostej.*

Twierdzenie 100 (Menelaos)**.** *Niech $a, b, c \in A$ będą niewspółliniowymi punktami. Wybierzmy punkty p, q, r leżące odpowiednio na prostych $\mathrm{af}(b, c)$, $\mathrm{af}(c, a)$ i $\mathrm{af}(a, b)$. Istnieją jednoznaczne przedstawienia*

$$p = tb + (1 - t)c, q = uc + (1 - u)a, r = va + (1 - v)b.$$

Wówczas punkty p, q, r są współliniowe wtedy i tylko wtedy, gdy $tuv = -(1 - t)(1 - u)(1 - v)$.

Dowód. Każdą prostą w $\mathrm{af}(a, b, c)$ można opisać równaniem

$$L = \{(s_1 a + s_2 b + s_3 c) \in A : \ c_1 s_1 + c_2 s_2 + c_3 s_3 = 0\},$$

gdzie $c_1, c_2, c_3 \in \mathbb{R}$ są nie wszystkie równe zeru. Jeśli prosta L przechodzi przez punkty p, q, r, to liczby c_1, c_2, c_3 muszą spełniać układ równań

$$\begin{cases} & & tc_2 & + & (1-t)c_3 & = & 0 \\ (1-u)c_1 & & & + & uc_3 & = & 0 \\ vc_1 & + & (1-v)c_2 & & & = & 0, \end{cases}$$

który ma niezerowe rozwiązanie wtedy i tylko wtedy, gdy wyznacznik jego macierzy jest niezerowy, a więc gdy $tuv + (1-t)(1-u)(1-v) = 0$. ☐

11. Wykład 13 (19 IV)

11.1. **Zbiory wypukłe.** Niech A będzie przestrzenią afiniczną nad ciałem $\mathbb{R}$.

Definicja 101. Podzbiór $X \subseteq A$ jest *wypukły* jeśli zachodzi warunek:

$$\forall x, y \in X \quad \forall t \in [0,1] \quad tx + (1-t)y \in X.$$

Równoważnie można wymagać, że każda kombinacja wypukła (tj. afiniczna ze współczynnikami pomiędzy 0 a 1) punktów z X należy do X.

Stwierdzenie 102. *Przecięcie dowolnej rodziny zbiorów wypukłych jest zbiorem wypukłym.*

Definicja 103. Niech $Y \subseteq A$ będzie dowolnym podzbiorem. Najmniejszy zbiór wypukły zawierający Y nazywamy *uwypukleniem* zbioru Y i oznaczamy $\operatorname{conv}(Y)$.

Stwierdzenie 104. *Niech $Y \subseteq A$. Następujące warunki są równoważne:*
- $X = \operatorname{conv}(Y)$,
- $X = \bigcap\{Z : Y \subseteq Z \text{ i } Z \text{ jest wypukły}\}$,
- $X = \{t_0 y_0 + \dots + t_k y_k \in A : y_i \in Y, t_i \in [0,1] \text{ oraz } \sum t_i = 1\}$.

Stwierdzenie 105. *Obrazy i przeciwobrazy zbiorów wypukłych przy przekształceniach afinicznych są wypukłe.*

Przykład 15. Podprzestrzeń afiniczna.

Przykład 16. *Półprzestrzenią* w A nazywamy dowolny zbiór postaci $f^{-1}([0,+\infty))$, gdzie $f : A \to \mathbb{R}$ jest niestałym przekształceniem afinicznym.

Definicja 106. *k-wymiarowym sympleksem* nazywamy uwypuklenie $(k+1)$ punktów afinicznie niezależnych.

Stwierdzenie 107. *Wszystkie k-wymiarowe sympleksy są afinicznie równoważne.*

Stwierdzenie 108. *Niech $(p_0, \dots, p_k)$ będzie sympleksem w $\mathbb{R}^n$ i niech $(p_{k+1}, \dots, p_n)$ będzie uzupełnieniem do bazy punktowej. Wówczas*

$$\Delta[p_0, \dots, p_k] = \left\{ \sum_{i=0}^{n} t_i p_i : t_0, \dots, t_k \in [0,1],\ t_{k+1} = \dots = t_n = 0 \right\}.$$

Wszystkie przestrzenie afiniczne są skończenie wymiarowe nad ciałem $\mathbb{R}$.

Twierdzenie 109. $\operatorname{conv}(Y)$ *jest sumą sympleksów o wierzchołkach w Y.*

Lemat 110. *Niech A będzie n-wymiarową przestrzenią afiniczną nad $\mathbb{R}$, $\Delta = \Delta[P] \subseteq A$ sympleksem o wierzchołkach $P = \{p_0, \dots, p_n\}$, a $B \subseteq A$ podprzestrzenią afiniczną wymiaru k. Załóżmy, że $\Delta \cap B \neq \emptyset$. Wówczas istnieje podzbiór $(n+1-k)$–elementowy podzbiór $Q \subseteq P$ taki, że $\Delta[Q] \cap B \neq \emptyset$.*

Dowód. Jeśli $k = 0$, to stwierdzenie jest trywialne, więc założymy, że $k > 0$. Indukcja po n. Jeśli $n = 1$, to Δ jest odcinkiem, $k = 1$ implikuje $B = A$, więc B zawiera zarówno p_0 jak i p_1. Załóżmy, że $n > 1$. Niech $L \subseteq B$ będzie dowolną prostą taką, że $L \cap \Delta \neq \emptyset$. Zbiór $L \cap \Delta$ jest wypukły, domknięty i ograniczony, a więc jest punktem lub odcinkiem. Niech p będzie końcem tego odcinka (lub punktem). Wówczas

$$p = \sum_{i=0}^{n} t_i p_i,$$

gdzie $t_i \in [0,1]$, $\sum t_i = 1$. Ponieważ p leży na brzegu sympleksu, któraś ze współrzędnych t_i jest zerowa. Niech

$$P' = \{i \in \{0, \dots, n\} : p_i \neq 0\}.$$

Oznaczmy przez $(m+1)$ będzie liczbę elementów zbioru P'. Wówczas:
- $p \in \Delta'$, gdzie $\Delta' = \Delta[P']$,
- $B' = B \cap \operatorname{af}(P')$ jest podprzestrzenią wymiaru $d \geqslant k + m - n$.

- $B' \cap \Delta' \neq \emptyset$.

Z założenia indukcyjnego dla sympleksu Δ' i podprzestrzeni B' w przestrzeni $\mathrm{af}(P')$ istnieje $(m+1-d)$-elementowy podzbiór $Q' \subseteq P'$ taki, że $\Delta[Q'] \cap B' \neq \emptyset$. Ponieważ

$$m + 1 - d \leqslant m + 1 - (k + m - n) = n + 1 - k$$

możemy uzupełnić Q' do $(n+1-k)$-elementowego zbioru Q, dla którego również zachodzi $\Delta[Q] \cap B' \neq \emptyset$, a więc również $\Delta[Q] \cap B \neq \emptyset$. □

Stwierdzenie 111. *Załóżmy, że $C = \mathrm{af}(p_0, \dots, p_n)$, $p \in \mathrm{conv}(p_0, \dots, p_n)$ i $\dim(C) = n - k$. Wówczas p można zapisać jako kombinację wypukłą nie więcej niż $(n-k+1)$ spośród punktów $p_0, \dots, p_n$.*

Dowód. Można założyć, że $k > n$. Niech A będzie przestrzenią afiniczną o bazie punktowej $q_0, \dots, q_n$ i niech $f : A \to C$ będzie przekształceniem afinicznym zadanym przez wartości na bazie punktowej: $f(q_i) = p_i$. Oznaczmy $B = f^{-1}(p)$ oraz $\Delta = \Delta[\{q_0, \dots, q_n\}] \subseteq A$. Wówczas:

- $\dim(B) = n - (n-k) = k$ (bo f jest na),
- $B \cap \Delta \neq \emptyset$ (bo jeśli $p = \sum t_i p_i$ i $t_i \in [0,1]$, to $f(\sum t_i q_i) = p$).

Ze stwierdzenia powyżej istnieje $(n+1-k)$-elementowy podzbiór $J \subseteq \{0, \dots, n\}$ taki, że $q \in \Delta[\{q_i\}_{i \in J}] \cap B$. Stąd

$$p = f(q) = f(\sum_{i \in J} t_i q_i) = \sum_{i \in J} t_i f(q_i) = \sum_{i \in J} t_i p_i.$$

jest przedstawieniem p w postaci kombinacji $(n+1-k)$ punktów p_i. □

Stwierdzenie 112. *Niech $Y \subseteq A$, $p \in \mathrm{conv}(Y)$. Wówczas $p \in \mathrm{conv}(Y')$ dla pewnego afinicznie niezależnego podzbioru $Y' \subseteq Y$.*

Dowód. Indukcja ze względu na wymiar A. Dla $\dim(A) = 1$ stwierdzenie zachodzi. Niech $p = \sum_{i=0}^{n} t_i p_i$, $p_i \in Y$ będzie kombinacją wypukłą dla której n jest możliwie najmniejsze. Niech $m = \dim(\mathrm{af}(p_0, \dots, p_n))$. Z powyższego stwierdzenia dla $C = \mathrm{af}(p_0, \dots, p_n)$ wynika, że p można przedstawić jako kombinację afiniczną $m+1$ punktów spośród $p_0, \dots, p_n$. Z minimalności przedstawienia $m = n$, a więc zbiór $\{p_0, \dots, p_n\}$ jest afinicznie niezależny. □

Wniosek. $\mathrm{conv}(Y) = \bigcup_{k \in \mathbb{N}} \bigcup_{p_0, \dots, p_k \in X} \Delta[\{p_0, \dots, p_k\}]$.

Dowód. Zawieranie $\supseteq$ jest oczywiste, a $\subseteq$ wynika ze Stwierdzenia. □

Stwierdzenie 113. *Niech $X \subseteq A$ będzie podzbiorem domkniętym, wypukłym i ograniczonym. Wówczas X jest częścią wspólną podprzestrzeni zawierających Y.*

Dowód. Można założyć, że $A = \mathbb{R}^n$. Wystarczy wykazać, że dla każdego $y = (y_1, \dots, y_n) \notin X$ istnieje funkcja afiniczna $f : \mathbb{R}^n \to \mathbb{R}$ taka, że $f(y) < 0$ oraz $f(X) \geqslant 0$. Przez przesunięcie można założyć, że $y = 0$. Niech $d : \mathbb{R}^n \to \mathbb{R}$ będzie funkcją daną wzorem $d(x_1, \dots, x_n) = \sum_{i=1}^{n} x_i^2$. Ponieważ d jest ciągła to osiąga wartość najmniejszą w pewnym punkcie $a = (a_1, \dots, a_n)$. Niech $f(x_1, \dots, x_n) = \sum_{k=1}^{n} a_i x_i - \sum_{i=1}^{n} a_i^2$. Oczywiście $f(0) < 0$ oraz $f(a) = 0$. Załóżmy, że $b \in X$ takie, że $f(b) < 0$. Ale odcinek $[a, b]$ zawiera się w X i posiada punkt bliższy 0 niż a. □

Definicja 114. Punkt $x \in X$ należący do zbioru wypukłego nazywamy *wierzchołkiem* X jeśli $x \notin \mathrm{conv}(X \setminus \{x\})$.

Stwierdzenie 115. *Domkniety i ograniczony zbiór wypukły jest uwypukleniem zbioru swoich wierzchołków.*

Dowód. Bez dowodu. Indukcja po wymiarach. Wystarczy udowodnić, że punkt brzegowy należy do podprzestrzeni podpierającej. □

12. Wykład 14 (21 IV)

12.1. **Wielościany.**

Definicja 116. *Wielościanem* nazywamy uwypuklenie skończonego zbioru punktów.

Definicja 117. *Wielościanem* nazywamy ograniczone przecięcie skończonej liczby półprzestrzeni.

Uwaga. Równoważność tych definicji — elementarne, ale nie całkiem łatwe.

Definicja 118. *Wymiarem wielościanu* W nazywamy wymiar przestrzeni $\mathrm{af}(W)$.

Definicja 119. Niech $W \subseteq A$ będzie wielościanem. *Ścianą* wielościanu W nazywamy wielościan $P = W \cap f^{-1}(0)$ o ile $f : A \to \mathbb{R}$ jest funkcją afiniczną taką, że $W \subseteq f^{-1}([0,\infty))$.

Stwierdzenie 120. *Zbiór ścian posiada częściowy porządek przez zawieranie.*

Przykład 17. Przykłady wielościanów:

- Wielościan 0-wymiarowy to punkt, 1-wymiarowy to odcinek.
- Wielościan 2-wymiarowy to n-kąt.
- Sympleks.
- Sześcian i uogólnienia.
- Ośmiościan i uogólnienia.
- Ostrosłup.
- Granastosłup.
- Wielościan funkcyjny.

Stwierdzenie 121 (Własności wielościanów)**.**

- *Część wspólna wielościanu i podprzestrzeni afinicznej jest wielościanem.*
- *Część wspólna dwóch wielościanów jest wielościanem.*
- *Suma Minkowskiego dwóch wielościanów jest wielościanem.*
- *Obraz wielościanu przy przekształceniu afinicznym jest wielościanem.*
- *Produkt wielościanów.*

Definicja 122. Niech $0 \in W \subseteq \mathbb{R}^d$ będzie wielościanem. *Wielościan dualny* P^* definiujemy przez

$$P^* = \{\mathbf{x} \in (\mathbb{R}^d)^* : \mathbf{x}(P) \leqslant 1\} \subseteq (\mathbb{R}^d)^*.$$

Przykład 18. Dualność sześcianu i ośmiościanu.

12.2. **Funkcjonały i przestrzenie sprzężone.**

Niech K będzie ustalonym ciałem.

Definicja 123. *Funkcjonałem liniowym* na przestrzeni liniowej V nazywamy homomorfizm $f : V \to K$. Zbiór wszystkich funkcjonałów tworzy przestrzeń liniową nazywaną *przestrzenią sprzężoną* do V i oznaczaną V^*.

Stwierdzenie 124. *Jeśli* $\dim(V) < \infty$*, to* $\dim(V^*) = \dim(V)$*. W szczególności przestrzenie* V *i* V^* *są izomorficzne.*

Definicja 125. Niech $(\beta_i)_{i\in I}$ będzie bazą V. Wówczas dla każdego $i \in I$ istnieje dokładnie jeden funkcjonał $\beta_i^* \in V^*$ taki, że $\beta_i^*(\beta_i) = 1$, $\beta_i^*(\beta_j) = 0$ dla $i \neq j$. Układ $(\beta_i^*)_{i\in I} \in V^*$ nazywamy układem sprzężonym.

Stwierdzenie 126. *Układ sprzężony jest liniowo niezależny.*

Dowód. Załóżmy, że $\sum_{i\in I} c_i\beta_i^* = 0$ (oczywiście prawie wszystkie c_i są zerowe). Waluacja na wektorach bazowych pokazuje, że wszystkie współczynniki są zerowe. □

Stwierdzenie 127. *Jeśli wymiar* V *jest nieskończony, to wymiar* V^* *również jest nieskończony ale układ sprzężony do bazy nie jest bazą (a nawet* V *i* V^* *nie są izomorficzne).*

Stwierdzenie 128 (Baza sprzężona to układ współrzędnych)**.** *Niech* $\alpha \in V$ *i niech* $(\beta_i)_{i\in I}$ *będzie bazą* V*. Wówczas*

$$\alpha = \sum_{i\in I} \beta_i^*(\alpha) \cdot \beta_i.$$

Dowód. Niech $\alpha = \sum_{j\in I} c_j\beta_j$. Mamy

$$\sum_{i\in I} \beta_i^*(\alpha)\cdot\beta_i = \sum_{i\in I}\beta_i^*\left(\sum_{j\in I} c_j\beta_j\right)\cdot\beta_i = \sum_{i\in I}\beta_i^*(c_i\beta_i)\cdot\beta_i = \sum_{i\in I} c_i\beta_i = \alpha. \qquad \square$$

Definicja 129. *Homomorfizmem sprzężonym* do homomorfizmu $F : V \to W$ nazywamy homomorfizm $F^* : W^* \to V^*$ dany wzorem

$$F^*(f)(\alpha) = f(F(\alpha)).$$

dla $\alpha \in V$. Inaczej: $F^*(f) = f \circ F$.

Stwierdzenie 130. *Jeśli $F : V \to W$ jest monomorfizmem, to F^* jest epimorfizmem. Jeśli $F : V \to W$ jest epimorfizmem, to F^* jest monomorfizmem.*

Dowód. Niech F będzie monomorfizmem i niech $f \in V^*$. Wybierzmy bazę $\{\alpha_i\}_{i\in I}$ przestrzeni V. Układ $\{F(\alpha_i)\}_{i\in I}$ jest liniowo niezależny, więc można go rozszerzyć wektorami $\{\beta_j\}_{j\in J}$ do bazy W. Niech $g(F(\alpha_i)) = f(\alpha_i)$ i niech $g(\beta_j) = 0$. Wówczas $F^*(g) = f$. Jeśli F jest epimorfizmem i $g \in W^*$ niezerowym funkcjonałem, to istnieje $\beta \in W$ takie, że $g(\beta) = 0$, oraz $\alpha \in V$ takie, że $F(\alpha) = \beta$. Więc $F^*(g)(\alpha) = g(F(\alpha)) \neq 0$. $\square$

Stwierdzenie 131. *Jeśli $F : V \to W$ i $G : W \to X$ homomorfizmy, to $(G\circ F)^* = F^* \circ G^*$.*

Dowód. Niech $h \in X^*$. Mamy

$$(F^*\circ G^*)(h) = F^*(G^*(h)) = F^*(h\circ G) = h\circ G\circ F = (G\circ F)^*(h). \qquad \square$$

Stwierdzenie 132. *Niech $(\beta_i)_{i=1}^n$ będzie bazą przestrzeni V. Wówczas $f \in V^*$ ma w bazie $(\beta_i^*)_{i=1}^n$ współrzędne $(f(\beta_i))_{i=1}^n$.*

Dowód. Trzeba pokazać, że $f = \sum_{i=1}^n f(\beta_i)\beta_i^*$. Dla każdego wektora bazowego β_i mamy

$$\left(\sum_{j=1}^n f(\beta_j)\beta_j^*\right)(\beta_i) = f(\beta_i). \qquad \square$$

Stwierdzenie 133. *Niech $V \in \mathbf{Vect}_K$. Homomorfizm $I : V \to V^{**}$ dany wzorem $I(\alpha)(f) = f(\alpha)$ jest monomorfizmem, a jeśli $\dim(V) < \infty$ to nawet izomorfizmem.*

Dowód. Wystarczy zauważyć, że dla $0 \neq \alpha \in V$ istnieje $f \in V^*$ takie, że $f(\alpha) \neq 0$. $\square$

Stwierdzenie 134. *Niech $\dim(V) < \infty$, niech $(\beta_i)_{i=1}^n$ będzie bazą V, a (β_i^{**}) jej podwójnym sprzężeniem. Wówczas $\beta_i^{**} = I(\beta_i)$.*

Dowód. A definicji $I(\beta_i)(\beta_j^*) = \beta_j^*(\beta_i) = \delta_i^j = \beta_i^{**}(\beta_j^*)$. $\square$

Stwierdzenie 135. *Niech $F \in \mathrm{Hom}(V, W)$ i niech $\mathcal{A} = (\alpha_i)_{i=1}^n$, $\mathcal{B}(\beta_j)_{j=1}^m$ będą bazami V i W odpowiednio. Oznaczmy $\mathcal{A}^* = (\alpha_i^*)_{i=1}^n$, $\mathcal{B}^* = (\beta_i^*)_{j=1}^m$. Wówczas*

$$\mathbf{M}(F^*)_{\mathcal{B}^*}^{\mathcal{A}^*} = \mathbf{M}(F)_{\mathcal{A}}^{\mathcal{B}}.$$

Dowód. Niech $\mathbf{M}(F)_{\mathcal{A}}^{\mathcal{B}} = (m_{ij})$, $\mathbf{M}(F^*)_{\mathcal{B}^*}^{\mathcal{A}^*} = (m_{ji}^*)$. Mamy $m_{ij} = \beta_i^*(\alpha_j)$ oraz

$$m_{ji}^* = \alpha_j^{**}(\beta_i^*) = I(\alpha_j)(\beta_i^*) = \beta_i^*(\alpha_j) = m_{ij}. \qquad \square$$

Definicja 136. Niech $V \in \mathbf{Vect}_K$. *Waluacją* nazywamy przekształcenie

$$V \times V^* \ni (\alpha, f) \mapsto f(\alpha) \in K.$$

Jest to szczególny przypadek przekształcenia

$$ev : V \times \mathrm{Hom}(V, W) \to W.$$

Przekształcenie to nie jest liniowe.

13. Wykład 15 (26 IV)

13.1. **Przekształcenia dwuliniowe.**

Definicja 137. Niech $V, W, X \in \mathbf{Vect}_K$. Przekształcenie $f : V \times W \to X$ nazywamy *dwuliniowym*, jeśli:

- Dla każdego $\alpha \in V$ przekształcenie $W \ni \beta \mapsto f(\alpha, \beta) \in X$ jest liniowe.
- Dla każdego $\beta \in W$ przekształcenie $V \ni \alpha \mapsto f(\alpha, \beta) \in X$ jest liniowe.

Ogólnie: jeśli $\{V_i\}_{i\in I}$ jest rodziną przestrzeni liniowych (zakładamy, że I jest skończony) i $X \in \mathbf{Vect}_K$, to przekształcenie $f : \prod_{i\in I} V_i \to X$ jest *wieloliniowe*, jeśli dla każdego $j \in I$ i dla każdych $\alpha_i \in V_i$, $i \in I \setminus \{j\}$ przekształcenie

$$V_j \ni \alpha_j \mapsto f\left((\alpha_i)_{i\in I}\right) \in X$$

jest liniowe.

Przykład 19 (Przykłady przekształceń dwuliniowych)**.**

(1) Mnożenie $K \times V \to V$.
(2) Jeśli $V \in \mathbf{Vect}_K$, to waluacja $V \times V^* \to K$ jest dwuliniowa.
(3) Jeśli $V, W \in \mathbf{Vect}_K$, to waluacja $V \times \mathrm{Hom}(V, W) \to W$ jest dwuliniowa.
(4) Jeśli $V, W, X \in \mathbf{Vect}_K$, to przekształenie złożenia $\mathrm{Hom}(V, W) \times \mathrm{Hom}(W, X) \to \mathrm{Hom}(V, X)$ jest dwuliniowe.
(5) Jeśli $V, W \in \mathbf{Vect}_K$, to przekształcenie
$$V^* \times W \ni (f, \alpha) \mapsto (\beta \mapsto f(\beta)\alpha) \in \mathrm{Hom}(V, W)$$
jest dwuliniowe.
(6) Iloczyn skalarny.
(7) Iloczyn wektorowy
$$\mathbb{R}^3 \times \mathbb{R}^3 \ni (x_1, y_1, z_1) \times (x_2, y_2, z_2) \mapsto (y_1z_2 - y_2z_1, z_1x_2 - z_2x_1, x_1y_2 - x_2y_1).$$

Stwierdzenie 138. *Niech $(\alpha_i)_{i\in I}$ będzie bazą V, a $(\beta_j)_{j\in J}$ bazą W. Wówczas dla każdego układu wektorów $(\gamma_{i,j})$ przestrzeni X istnieje dokładnie jedno przekształcenie dwuliniowe $f : V \times W \to X$ takie, że $f(\alpha_i, \beta_j) = \gamma_{i,j}$.*

13.2. **Iloczyn tensorowy.**

Stwierdzenie 139 (Własność uniwersalna iloczynu tensorowego)**.** *Niech $V, W \in \mathbf{Vect}_K$. Istnieje przestrzeń wektorowa $V \otimes W$ oraz przekształcenie dwuliniowe $\mu : V \times W \to V \otimes W$ o własności uniwersalnej: dla każdego przekształcenia dwuliniowego $f : V \times W \to X$ istnieje dokładnie jedno przekształcenie liniowe $\tilde{f} : V \otimes W \to X$ takie, że $f = \tilde{f} \circ \mu$.*

Dowód. Konstrukcja: niech Z będzie przestrzenią o bazie $V \times W$. Zdefiniujmy zbiór $R \subseteq Z$

$$\begin{aligned} R =& \{(\alpha_1 + \alpha_2, \beta) - (\alpha_1, \beta) - (\alpha_2, \beta)\}_{\alpha_i\in V, \beta\in W} \cup \{(c\alpha, \beta) - c(\alpha, \beta)\}_{c\in K, \alpha\in V, \beta\in W} \\ &\cup \{(\alpha, \beta_1 + \beta_2) - (\alpha, \beta_1) - (\alpha, \beta_2)\}_{\alpha\in V, \beta_j\in W} \cup \{(\alpha, c\beta) - c(\alpha, \beta)\}_{c\in K, \alpha\in V, \beta\in W}. \end{aligned}$$

Niech teraz $V \otimes W := Z/\operatorname{lin}(R)$ i niech $\mu(\alpha, \beta) = (\alpha, \beta) \cdot \operatorname{lin}(R)$. Jeśli $f : V \times W \to X$ jest przekształceniem dwuliniowym, to niech $f' : Z \to X$ będzie dane wzorem $f'((\alpha, \beta)) = f(\alpha, \beta)$ — jest to jedyne przekształcenie takie, że $f = f' \circ (V \times W \subseteq Z)$. Oczywiście $f|_R = 0$ (z dwuliniowości), więc otrzymujemy dokładnie jedno przekształcenie ilorazowe

$$\tilde{f} : V \otimes W \ni (\alpha, \beta) \cdot \operatorname{lin}(R) \mapsto f(\alpha, \beta) \in X.$$

□

Definicja 140. Przestrzeń $V \otimes W$ nazywamy *iloczynem tensorowym* przestrzeni V i W, a element $(\alpha, \beta) \cdot \operatorname{lin}(R)$ oznaczamy przez $\alpha \otimes \beta$.

Stwierdzenie 141. *Dla $\alpha, \alpha_1, \alpha_2 \in V$, $\beta, \beta_1, \beta_2 \in W$ oraz $c \in K$ mamy*

$$(\alpha_1 + \alpha_2) \otimes \beta = \alpha_1 \otimes \beta + \alpha_2 \otimes \beta, \quad (c\alpha) \otimes \beta = c(\alpha \otimes \beta)$$
$$\alpha \otimes (\beta_1 + \beta_2) = \alpha \otimes \beta_1 + \alpha \otimes \beta_2, \quad \alpha \otimes \beta_1 + \alpha \otimes \beta_2.$$

Dowód. Równości zachodzą w Z z dokładnością do R. □

Stwierdzenie 142. *Niech $V, W \in \mathbf{Vect}_K$. Jeśli $(\alpha_i)_{i\in I}$ jest bazą V, a $(\beta_j)_{j\in J}$ bazą W, to $(\alpha_i \otimes \beta_j)_{i\in I, j\in J}$ jest bazą $V \otimes W$.*

Dowód. Niech $i \in I$, $j \in J$ i rozważmy przekształcenie dwuliniowe

$$f_{ij} : V \times W \ni (\alpha, \beta) \mapsto \alpha_i^*(\alpha) \cdot \beta_j^*(\beta) \in K.$$

Niech $\tilde{f}_{ij} : V \otimes W \to K$ będzie odpowiednim homomorfizmem $V \otimes W \to K$. Oczywiście

$$\tilde{f}_{ij}(\alpha_k \otimes \beta_l) = \begin{cases} 1 & \text{dla } i = k,\ j = l, \\ 0 & \text{w przeciwnym przypadku.} \end{cases}$$

Wobec tego $\alpha_i \otimes \beta_j$ nie jest kombinacją liniową pozostałych wektorów, czyli układ $(\alpha_i \otimes \beta_j)_{i\in I, j\in J}$ jest liniowo niezależny. Z drugiej strony, $V \otimes W = \operatorname{lin}\{\alpha \otimes \beta : \ \alpha \in V,\ \beta \in W\}$. Jeśli $\alpha = \sum_{i\in I} c_i\alpha_i$, $\beta = \sum_{j\in J} d_j\beta_j$, to

$$\alpha \otimes \beta = \left(\sum_{i\in I} c_i\alpha_i\right) \otimes \left(\sum_{j\in J} d_j\beta_j\right) = \sum_{i\in I}\sum_{j\in J} c_i d_j (\alpha_i \otimes \beta_j).$$ □

14. Wykład 16 (28 IV)

14.1. Własności iloczynu tensorowego.

Stwierdzenie 143. *Niech $V, W, X \in \mathbf{Vect}_K$.*
(a) $K \otimes V \cong V$,
(b) $V \otimes W \cong W \otimes V$,
(c) $V \otimes (W \otimes X) \cong (V \otimes W) \otimes X$,
(d) $V \otimes (W \oplus X) \cong (V \otimes W) \oplus (V \otimes X)$.

Dowód. Niech

$$F : K \otimes V \ni c \otimes \alpha \mapsto c\alpha \in V,$$
$$G : V \ni \alpha \mapsto 1 \otimes \alpha \in K \otimes V.$$

Przekształcenie F jest liniowe, bo

$$F((c + c') \otimes \alpha) = (c + c')\alpha = c\alpha + c'\alpha = F(c \otimes \alpha) + F(c' \otimes \alpha),$$
$$F(dc \otimes \alpha) = (dc)\alpha = d(c\alpha) = dF(c \otimes \alpha),$$

podobnie dla drugiej współrzędnej i dla G. Złożenia: $F(G(\alpha)) = F(1 \otimes \alpha) = \alpha$,

$$G(F(c \otimes \alpha)) = G(c\alpha) = 1 \otimes c\alpha = c(1 \otimes \alpha) = c \otimes \alpha.$$

Podobnie dla pozostałych tożsamości. Alternatywnie — rachunek na bazach. □

Stwierdzenie 144. *Jeśli $V, W \in \mathbf{Vect}_K^{fin}$, to $(V \otimes W)^* \cong V^* \otimes W^*$.*

Dowód. Jeśli $(\alpha_i)_{i\in I}$, $(\beta_j)_{j\in J}$ bazy V i W odpowiednio, to jest odpowiedniość $(\alpha_i \otimes \beta_j)^* \cong \alpha_i^* \otimes \beta_j^*$. □

Stwierdzenie 145. *Niech $V, W \in \mathbf{Vect}_K$. Przekształcenie $\Phi : V^* \otimes W \to \operatorname{Hom}(V, W)$ dane wzorem*

$$\Phi(f \otimes \beta)(\alpha) = f(\alpha)\beta$$

jest monomorfizmem. Jeśli W jest skończenie wymiarowa, to Φ jest izomorfizmem.

Dowód. Niech $\omega \in V^* \otimes W$ będzie niezerowym elementem i niech $(\beta_j)_{j\in J}$ będzie bazą W. Istnieje jednoznaczne przedstawienie $\omega = \sum_{j\in J} f_j \otimes \beta_j$ i pewien element $f_k \in V^*$ jest niezerowy. Niech $\alpha \in V$ będzie takie, że $f_k(\alpha) \neq 0$. Wtedy

$$\Phi(\omega)(\alpha) = \Phi(\sum_{j\in J} f_j \otimes \beta_j)(\alpha) = \sum_{j\in J} f_j(\alpha)\beta_j \neq 0,$$

bo na k-tej współrzędnej współczynnik jest niezerowy.

Teraz załóżmy, że J jest skończony i zdefiniujmy przekształcenie

$$\Psi : \operatorname{Hom}(V, W) \ni F \mapsto \sum_{j\in J} (\beta_j^* \circ F) \otimes \beta_j \in V^* \otimes W.$$

Dla $\alpha \in V$ mamy

$$\Phi(\Psi(f))(\alpha) = \Psi\left(\sum_{j\in J}(\beta_j^* \circ F) \otimes \beta_j\right)(\alpha) = \sum_{j\in J}\Psi((\beta_j^* \circ F) \otimes \beta_j)(\alpha) = \sum_{j\in J}\beta_j^*(F(\alpha)) \cdot \beta_j = F(\alpha),$$

więc $\Phi(\Psi(F)) = F$, więc Φ jest epimorfizmem. □

Stwierdzenie 146. *Niech $V, W \in \mathbf{Vect}_K^{fin}$, $(\alpha_i)_{i=1}^m$, $(\beta_j)_{j=1}^n$ — bazy V i W odpowiednio, $F \in \mathrm{Hom}(V, W)$. Wówczas jeśli $M(F)_{\mathcal{A}}^{\mathcal{B}} = (m_{ij})$, to F odpowiada element*

$$\sum_{i=1}^m \sum_{j=1}^n m_{ji}(\alpha_i^* \otimes \beta_j) \in V^* \otimes W.$$

Dowód. Niech Ψ będzie odwrotnością z poprzedniego dowodu. Mamy

$$\Psi(F) = \sum_{j=1}^n(\beta_j^* \circ F) \otimes \beta_j = \sum_{j=1}^n\sum_{i=1}^m((\beta_j^* \circ F)(\alpha_i) \cdot \alpha_i^*) \otimes \beta_j = \sum_{j=1}^n\sum_{i=1}^m(m_{ji} \cdot \alpha_i^*) \otimes \beta_j.$$ □

Definicja 147. Jeśli $F : V \to W$ i $G : V' \to W'$ są liniowe, to przekształcenie

$$F \otimes G : V \otimes V' \to W \otimes W'$$

dane wzorem

$$(F \otimes G)(\alpha \otimes \beta) = F(\alpha) \otimes G(\beta)$$

jest liniowe. Nazywamy je *iloczynem tensorowym przekształceń F i G*.

15. Wykład 17 (5 V)

15.1. Iloczyn skalarny.

Niech $K = \mathbb{R}$.

Definicja 148. Iloczynem skalarnym na przestrzeni liniowej V nazywamy przekształcenie

$$\langle -, - \rangle : V \times V \to \mathbb{R}$$

które jest:
- dwuliniowe,
- symetryczne, tj. $\langle \alpha, \beta \rangle = \langle \beta, \alpha \rangle$,
- dodatnio określone, tj. $\langle \alpha, \alpha \rangle > 0$ dla $\alpha \neq 0$.

Przykład 20. Dla $V = \mathbb{R}^n$

$$\langle (x_1, \ldots, x_n), (y_1, \ldots, y_n) \rangle = x_1y_1 + \cdots + x_ny_n$$

jest iloczynem skalarnym. Ogólniej

$$\langle (x_1, \ldots, x_n), (y_1, \ldots, y_n) \rangle = c_1x_1y_1 + \cdots + c_nx_ny_n$$

jest iloczynem skalarnym jeśli $c_i > 0$.

Stwierdzenie 149. *Każdy iloczyn skalarny na $\mathbb{R}^n$ jest postaci*

$$\langle (x_1, \ldots, x_n), (y_1, \ldots, y_n) \rangle = \sum_{i,j} c_{ij}x_iy_j,$$

gdzie $c_{ij} \in \mathbb{R}$, $c_{ij} = c_{ji}$, ale nie każdy układ liczb c_{ij} wyznacza iloczyn skalarny.

Definicja 150. Przestrzeń liniową z ustalonym iloczynem skalarnym nazywamy *przestrzenią unitarną*.

Definicja 151. *Długością* wektora $\alpha \in V$ nazywamy $\|\alpha\| := \sqrt{\langle \alpha, \alpha \rangle}$.

Definicja 152. Mówimy, że wektory α, β są *prostopadłe*, jeśli $\langle \alpha, \beta \rangle = 0$.

Stwierdzenie 153. *W przestrzeni unitarnej zachodzą*
- $\langle \alpha, \beta \rangle \leqslant \|\alpha\| \cdot \|\beta\|$ *(nierówność Schwartza),*
- $\|\alpha + \beta\| \leqslant \|\alpha\| + \|\beta\|$ *(nierówność trójkąta),*
- $\|\alpha\|^2 + \|\beta\|^2 = \|\alpha + \beta\|^2$ *(twierdzenie Pitagorasa).*

Dowód. Mamy

$$0 \leqslant \langle t\alpha+\beta, t\alpha+\beta\rangle = \|\alpha\|^2 t^2 + 2\langle\alpha,\beta\rangle t + \|\beta\|^2$$

więc

$$0 \geqslant \Delta = 4\langle\alpha,\beta\rangle^2 - 4\|\alpha\|^2 \cdot \|\beta\|^2,$$

co dowodzi nierówności Schwartza. Dalej

$$\|\alpha+\beta\|^2 = \langle\alpha+\beta,\alpha+\beta\rangle = \|\alpha\|^2 + 2\langle\alpha,\beta\rangle + \|\beta\|^2 \leqslant \|\alpha\|^2 + 2\|\alpha\|\cdot\|\beta\| + \|\beta\|^2 = (\|\alpha\|+\|\beta\|)^2$$

dowodzi nierówności trójkąta. Twierdzenie Pitagorasa jest oczywiste. □

Definicja 154. *Kątem* pomiędzy wektorami $\alpha, \beta \in V$ nazywamy liczbę $\theta \in [0,\pi]$ taką, że

$$\cos\theta = \frac{\langle\alpha,\beta\rangle}{\|\alpha\|\cdot\|\beta\|}.$$

Definicja jest poprawna, bo nierówność Schwartza gwarantuje, że iloraz należy do przedziału $[-1, 1]$.

15.2. **Bazy ortogonalne i ortonormalne.** Niech V będzie przestrzenią unitarną wymiaru n.

Definicja 155. Układ wektorów $\alpha_1,\dots,\alpha_k \in V$ jest *prostopadły* jeśli $\alpha_i \perp \alpha_j$ dla $i \neq j$. Bazę złożoną z wektorów prostopadłych nazywamy *bazą ortogonalną*.

Stwierdzenie 156. *Prostopadły układ niezerowych wektorów jest liniowo niezależny.*

Dowód. Załóżmy, że $\alpha_1 = \sum_{i=2}^k c_i\alpha_i$. Wówczas

$$0 \neq \langle\alpha_1,\alpha_1\rangle = \langle\alpha_1, \sum_{i=2}^k c_i\alpha_i\rangle = 0,$$

więc α_1 nie może być kombinacją liniową pozostałych wektorów. □

Definicja 157. Bazę $(\beta_1,\dots,\beta_n)$ przestrzeni V nazywamy:

- *bazą ortogonalną*, jesli $\alpha_i \perp \alpha_j$ dla $i \neq j$,
- *bazą ortonormalną*, jeśli dodatkowo $\|\alpha_i\| = 1$ dla $1 \leqslant i \leqslant n$.

Stwierdzenie 158. *Jeśli $(\beta_i)_{i=1}^n$ jest bazą ortogonalną, to*

$$\alpha = \sum_{i=1}^n \frac{\langle\alpha,\beta_i\rangle}{\langle\beta_i,\beta_i\rangle}\beta_i.$$

Dla bazy ortonormalnej równość upraszcza się do $\alpha = \sum_{i=1}^n \langle\alpha,\beta_i\rangle\beta_i$.

Dowód. Niech $\alpha = \sum_{i=1}^n c_i\beta_i$. Mamy

$$\langle\alpha,\beta_k\rangle = \langle\sum_{i=1}^n c_i\beta_i,\beta_k\rangle = \sum_{i=1}^n c_i\langle\beta_i,\beta_k\rangle = c_k\langle\beta_k,\beta_k\rangle.$$ □

Stwierdzenie 159. *Niech $(\beta_i)_{i=1}^n$ będzie bazą ortonormalną V. Wówczas, dla $\alpha,\alpha' \in V$ mamy*

$$\langle\alpha,\alpha'\rangle = \sum_{i=1}^n \langle\alpha,\beta_i\rangle\cdot\langle\alpha',\beta_i\rangle$$

Dowód. Mamy

$$\langle\alpha,\alpha'\rangle = \langle\sum_{i=1}^n\langle\alpha,\beta_i\rangle\beta_i, \sum_{j=1}^n\langle\alpha',\beta_j\rangle\beta_j\rangle = \sum_{i=1}^n\sum_{j=1}^n\langle\langle\alpha,\beta_i\rangle\beta_i,\langle\alpha',\beta_j\rangle\beta_j\rangle$$

$$= \sum_{i=1}^n\sum_{j=1}^n\langle\alpha,\beta_i\rangle\langle\alpha',\beta_j\rangle\langle\beta_i,\beta_j\rangle = \sum_{i=1}^n\langle\alpha,\beta_i\rangle\langle\alpha',\beta_j\rangle.$$ □

Twierdzenie 160 (Ortogormalizacja Grama-Schmidta)**.** *Niech $(\beta_i)_{i=1}^n$ będzie bazą V. Wówczas układ wektorów $(\gamma_i)_{i=1}^n$ zadany wzorem indukcyjnym*

$$\gamma_k = \beta_k - \sum_{i=1}^{k-1} \frac{\langle \beta_k, \gamma_i \rangle}{\langle \gamma_i, \gamma_i \rangle} \gamma_i$$

jest bazą ortogonalną przestrzeni V. Co więcej, dla każdego k układ $(\gamma_i)_{i=1}^k$ jest bazą ortogonalną przestrzeni $V_k := \mathrm{lin}(\{\beta_i\}_{i=1}^k)$.

Dowód. Dowód przez indukcję. Dla $k = 1$ teza jest oczywista. Dla $k > 1$ mamy

$$\mathrm{lin}(\{\gamma_i\}_{i=1}^k) = \mathrm{lin}(V_{k-1} \cup \{\gamma_k\}) = \mathrm{lin}(V_{k-1} \cup \{\beta_k\}) = V_k,$$

co dowodzi, że $(\gamma_i)_{i=1}^k$ jest bazą V_k. Ponadto, dla dowolnego $j < k$ mamy

$$\langle \gamma_k, \gamma_j \rangle = \langle \beta_k - \sum_{i=1}^{k-1} \frac{\langle \beta_k, \gamma_i \rangle}{\langle \gamma_i, \gamma_i \rangle} \gamma_i, \gamma_j \rangle = \langle \beta_k, \gamma_j \rangle - \sum_{i=1}^{k-1} \frac{\langle \beta_k, \gamma_i \rangle}{\langle \gamma_i, \gamma_i \rangle} \langle \gamma_i, \gamma_j \rangle = \langle \beta_k, \gamma_j \rangle - \frac{\langle \beta_k, \gamma_j \rangle}{\langle \gamma_j, \gamma_j \rangle} \langle \gamma_j, \gamma_j \rangle = 0,$$

więc ta baza jest ortogonalna. □

Uwaga. Przez przeskalowanie wektorów możemy uzyskać bazę ortonormalną.

Wniosek. Każda skończenie wektorowa przestrzeń unitarna posiada bazą ortonormalną.

Stwierdzenie 161. *Niech V, V' będą przestrzeniami unitarnym wymiaru n. Wówczas istnieje izomorfizm $V \to V'$, który zachowuje iloczyn skalarny.*

Dowód. Wystarczy wybrać bazy ortonormalne i izomorfizm, który przeprowadza jedną na drugą. □

15.3. **Podprzestrzenie prostopadłe.**

Definicja 162. Niech $X \subseteq V$ będzie dowolnym podzbiorem. *Podprzestrzeń prostopadła do X* to

$$X^\perp := \{\alpha \in V : \forall_{\beta \in X} \ \langle \alpha, \beta \rangle = 0\}.$$

Łatwo sprawdzić, że jest to podprzestrzeń wektorowa.

Stwierdzenie 163. *Dla podzbioru $X \subseteq V$ mamy $X^\perp = \mathrm{lin}(X)^\perp$.*

Stwierdzenie 164. *Niech $W \subseteq V$ będzie podprzestrzenią. Wówczas*

- $W \oplus W^\perp = V$,
- $W = (W^\perp)^\perp$.

Dowód. Jeśli $\alpha \in W \cap W^\perp$, to $\langle \alpha, \alpha \rangle = 0$, więc $\alpha = 0$. Stąd $W \cap W^\perp = \{0\}$. Niech $(\beta_i)_{i=1}^m$ będzie bazą ortonormalną W. Wówczas dla dowolnego $\alpha \in V$ niech

$$\alpha' = \sum_{i=1}^m \langle \alpha, \beta_i \rangle \beta_i.$$

Oczywiście $\alpha' \in W$, ponadto dla każdego $1 \leqslant j \leqslant m$ mamy

$$\langle \alpha - \alpha', \beta_j \rangle = \langle \alpha, \beta_j \rangle - \langle \sum_{i=1}^m \langle \alpha, \beta_i \rangle \beta_i, \beta_j \rangle = \langle \alpha, \beta_j \rangle - \langle \langle \alpha, \beta_j \rangle \beta_j, \beta_j \rangle = 0,$$

więc $\alpha - \alpha' \in (\{\beta_i\}_{i=1}^k)^\perp = W^\perp$. Stąd $\alpha = \alpha' + (\alpha - \alpha') \in W + W^\perp$, a więc $V = W \oplus W'$. Jeśli $\alpha \in W$, to dla każdego $\beta \in W^\perp$ mamy $\langle \alpha, \beta \rangle = 0$, więc $W \subseteq (W^\perp)^\perp$. Z drugiej strony,

$$\dim((W^\perp)^\perp) = \dim(V) - \dim(W^\perp) = \dim(V) - (\dim(V) - \dim(W)) = \dim(W),$$

więc musi zachodzić równość. □

Definicja 165. *Rzutem prostopadłym na W* nazywamy rzut na W wzdłuż $W^\perp$. Podobnie *symetrią prostopadłą względem W* nazywamy symetrię względem W wzdłuż $W^\perp$.

16. Wykład 18 (10 V)

16.1. **Wyznacznik Grama.** Niech V będzie przestrzenią unitarną wymiaru n, $K = \mathbb{R}$.

Definicja 166. Niech $(\alpha_i)_{i=1}^k$ będzie układem wektorów w przestrzeni unitarnej V. *Macierzą Grama* układu (α_i) nazywamy macierz $G(\alpha_1, \ldots, \alpha_k) = g_{ij}$, gdzie $g_{ij} = \langle \alpha_i, \alpha_j \rangle$. *Wyznacznikiem Grama* tego układu nazywamy liczbę

$$W(\alpha_1, \ldots, \alpha_k) = \det G(\alpha_1, \ldots, \alpha_k).$$

Stwierdzenie 167. *Niech $(\beta_j)_{j=1}^n$ będzie bazą ortonormalną V i niech $(\alpha_i)_{i=1}^k$ bedzie układem wektorów. Wówczas*

$$G(\alpha_1, \ldots, \alpha_k) = A^T A,$$

gdzie $A = (a_{ji}) \in M_{n\times k}(\mathbb{R})$, $a_{ji} = \beta_j^*(\alpha_i) = \langle \beta_j, \alpha_i \rangle$.

Dowód. Niech $A^T A = [c_{rs}]_{r,s=1,\ldots,k}$. Mamy

$$c_{rs} = \sum_{t=1}^n a_{rt} a_{ts} = \sum_{t=1}^n \langle \beta_t, \alpha_r \rangle \cdot \langle \beta_t, \alpha_s \rangle = \langle \alpha_r, \alpha_s \rangle.$$ □

Stwierdzenie 168. *Niech $(\beta_i)_{i=1}^n$ będzie bazą przestrzeni V. Wówczas*

$$\langle \alpha, \beta \rangle = \mathbf{x}^T G(\beta_1, \ldots, \beta_n)\mathbf{y},$$

gdzie $\mathbf{x} = (x_1, \ldots, x_n)^T$, $\mathbf{y} = (y_1, \ldots, y_n)^T$ są współczynnikami wektorów α, α' w bazie (β_i).

Dowód. Oznaczmy $G(\beta_1, \ldots, \beta_n) = (g_{ij})$. Mamy

$$\langle \alpha, \alpha' \rangle = \langle \sum_{i=1}^n x_i \beta_i, \sum_{j=1}^n y_j \beta_j \rangle = \sum_{i=1}^n \sum_{j=1}^n x_i y_j \langle \beta_i, \beta_j \rangle = \sum_{i=1}^n \sum_{j=1}^n x_i g_{ij} y_j = \mathbf{x}^T G(\beta_1, \ldots, \beta_n)\mathbf{y}.$$ □

Stwierdzenie 169. *Baza jest ortogonalna wtedy i tylko wtedy, gdy jej macierz Grama jest diagonalna. Baza jest ortonormalna wtedy i tylko wtedy, gdy jej macierz Grama jest jednostkowa.* □

Stwierdzenie 170. *Niech $\mathcal{B} = (\beta_i))i = 1^n$, $\mathcal{B}' = (\beta_i'))i = 1^n$ będą bazami przestrzeni unitarnej V. Wówczas*

$$G(\beta_1, \ldots, \beta_n) = (M(id)_{\mathcal{B}}^{\mathcal{B}'})^T G(\beta_1', \ldots, \beta_n') M(id)_{\mathcal{B}}^{\mathcal{B}'}.$$

Dowód. Niech $\alpha, \alpha' \in V$ i niech $\mathbf{x}, \mathbf{x}'$ będą przedstawieniami α i α' w bazie $\mathcal{B}$. Oczywiście $M(id)_{\mathcal{B}}^{\mathcal{B}'}\mathbf{x}$, $M(id)_{\mathcal{B}}^{\mathcal{B}'}\mathbf{x}'$ są przedstawieniami α i α' w bazie $\mathcal{B}'$. Mamy

$$\langle \alpha, \alpha' \rangle = \mathbf{x}^T G(\beta_1, \ldots, \beta_n)\mathbf{x}$$

i jednocześnie

$$\langle \alpha, \alpha' \rangle = (M(id)_{\mathcal{B}}^{\mathcal{B}'}\mathbf{x})^T G(\beta_1', \ldots, \beta_n') M(id)_{\mathcal{B}}^{\mathcal{B}'}\mathbf{x} = \mathbf{x}^T (M(id)_{\mathcal{B}}^{\mathcal{B}'})^T G(\beta_1', \ldots, \beta_n') M(id)_{\mathcal{B}}^{\mathcal{B}'}\mathbf{x},$$

co dowodzi tezy. □

Stwierdzenie 171. *Macierz $A \in M_{n\times n}(\mathbb{R})$ jest macierzą Grama pewnej bazy wtedy i tylko wtedy, gdy $A = B^T B$ dla pewnej macierzy odwracalnej $B \in M_{n\times n}(\mathbb{R})$.*

Dowód. Niech $\mathcal{B} = (\beta_i)_{i=1}^n$ będzie bazą ortonormalną. Jeśli A jest macierzą Grama bazy $\mathcal{A} = (\alpha_1, \ldots, \alpha_n)$, to

$$A = G(\alpha_1, \ldots, \alpha_n) = (M(id)_{\mathcal{A}}^{\mathcal{B}})^T M(id)_{\mathcal{A}}^{\mathcal{B}}.$$

Jeśli $A = B^T B$, to A jest macierzą Grama bazy $(B^{-1}\beta_1, \ldots, B^{-1}\beta_n)$. □

Stwierdzenie 172. *Dla dowolnego układu wektorów $(\alpha_1, \ldots, \alpha_k)$ jego wyznacznik Grama jest nieujemny, przy czym $G(\alpha_1, \ldots, \alpha_k) > 0$ wtedy i tylko wtedy, gdy układ jest liniowo niezależny.*

Dowód. Jeśli $k = n$, to

$$G(\alpha_1, \ldots, \alpha_k) = \det(A^T A) = \det(A)^2,$$

gdzie A jest macierzą wpółrzędnych wektorów α_i. W ogólnym przypadku rozpatrujemy układ wektorów na przestrzeni $\mathrm{lin}(\alpha_1, \ldots, \alpha_k)$. □

Definicja 173. *k-tym wiodącym minorem głównym* macierzy A nazywamy macierz $A^{(k)} \in M_{k\times k}(\mathbb{R})$ powstałą z A przez skreślenie ostatnich wierszy i kolumn.

Twierdzenie 174 (Kryterium Sylvestera)**.** *Macierz A jest macierzą Grama pewnego liniowo niezależnego układu wektorów wtedy i tylko wtedy, gdy:*

- *jest symetryczna,*
- *wszystkie wiodące minory główne mają dodatnie wyznaczniki.*

Dowód. Warunki są konieczne, bo jeśli $A = G(\alpha_1, \dots, \alpha_k)$, to $A^{(j)} = G(\alpha_1, \dots, \alpha_j)$. Załóżmy, że $A = (a_{ij})$ jest symetryczną macierzą o dodatnich wyznacznikach minorów wiodących. Dowód indukcyjny po k — liczbie wektorów w układzie. Jeśli $k = 1$ — prosto, więc załóżmy, że $k > 1$. Z założenia indukcyjnego $A^{(k-1)}$ jest macierzą Grama pewnego układu wektorów $(\alpha_1, \dots, \alpha_{k-1})$, więc istnieje macierz $B \in M_{(k-1)\times(k-1)}(\mathbb{R})$ taka, że $A^{(k-1)} = B^T B$. Rozważmy macierz $C = (\bar{B}^{-1})^T A \bar{B}^{-1}$, gdzie

$$\bar{B} = \begin{pmatrix} B & 0 \\ 0 & 1 \end{pmatrix}.$$

Zauważmy, że C jest postaci

$$C = \begin{pmatrix} & & & c_1 \\ & I & & \vdots \\ & & & c_{k-1} \\ c_1 & \dots & c_{k-1} & c_k \end{pmatrix}$$

oraz $\det(C) = c_k - c_1^2 - \dots - c_{k-1}^2$. Oznaczmy

$$\mathbf{c} = \begin{pmatrix} c_1 \\ \vdots \\ c_{k-1} \end{pmatrix}, \qquad D = \begin{pmatrix} I & -\mathbf{c} \\ 0 & 1 \end{pmatrix}.$$

Wtedy

$$D^T C D = \begin{pmatrix} I & 0 \\ -\mathbf{c}^T & 1 \end{pmatrix} \begin{pmatrix} I & \mathbf{c} \\ \mathbf{c}^T & c_k \end{pmatrix} \begin{pmatrix} I & \mathbf{c} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & c_k - \|\mathbf{c}\|^2 \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & \det(C) \end{pmatrix}.$$

Ostatecznie

$$A = \bar{B}^T C \bar{B} = \bar{B}^T (D^{-1})^T K^T K D^{-1} \bar{B} = (K D^{-1} \bar{B})^T (K D^{-1} \bar{B}),$$

gdzie

$$K = \begin{pmatrix} I & 0 \\ 0 & \sqrt{\det(C)} \end{pmatrix}.$$ □

16.2. **Izometrie i macierze ortogonalne.**

Definicja 175. Niech V, W będą przestrzeniami unitarnymi. Mówimy, że homomorfizm $f : V \to W$ *zachowuje iloczyn skalarny* (lub równoważnie, jest *homomorfizmem unitarnym*) jeśli

$$\forall_{\alpha,\beta\in V}\ \langle \alpha, \beta \rangle_V = \langle f(\alpha), f(\beta) \rangle_W.$$

Izomorfizm, który jest homomorfizmem unitarnym nazywamy *automorfizmem unitarnym* lub *izometrią.*

Stwierdzenie 176. *Jeśli homomorfizm $f : V \to W$ zachowuje długość wektorów (tzn. $\|\alpha\|_V = \|f(\alpha)\|_W$ dla $\alpha \in V$), to jest homomorfizmem unitarnym.*

Dowód. Mamy

$$\langle \alpha, \beta \rangle = \tfrac{1}{2}(\|\alpha + \beta\|^2 - \|\alpha\|^2 - \|\beta\|^2) = \tfrac{1}{2}(\|f(\alpha) + f(\beta)\|^2 - \|f(\alpha)\|^2 - \|f(\beta)\|^2) = \langle f(\alpha), f(\beta) \rangle.$$ □

Uwaga. Każdy homomorfizm unitarny jest monomorfizmem.

Stwierdzenie 177. *Automorfizm $f : V \to V$ jest izometrią wtedy i tylko wtedy, gdy przeprowadza pewną (lub każdą) bazę ortonormalną na bazę ortonormalną.* □

Definicja 178. Macierz $A \in M_{n\times n}(\mathbb{R})$ jest *ortogonalna* jeśli $A^T A = I$.

Stwierdzenie 179. *Automorfizm $f : V \to V$ jest izometrią wtedy i tylko wtedy, gdy jego macierz A w bazie ortonormalnej jest ortogonalna.*

Dowód. Niech $\alpha, \beta \in V$, $\mathbf{x}, \mathbf{y}$ — przedstawienia w bazie. Mamy

$$\langle f(\alpha), f(\beta)\rangle = (A\mathbf{x})^T IA\mathbf{y} = \mathbf{x}^T A^T A\mathbf{y}, \qquad \langle \alpha, \beta\rangle = \mathbf{x}^T y,$$

i powyższe wyrażenia są równe dla wszystkich α, β jeśli $A^T A = I$. □

Stwierdzenie 180. *Niech $A \in M_{n\times n}(\mathbb{R})$ będzie macierzą ortogonalną i niech $\mathbf{x}^1, \ldots, \mathbf{x}^n$ będą wektorami stojącymi w kolumnach. Wówczas $(\mathbf{x}^i)^T \mathbf{x}_j = \delta_i^j$.*

Dowód. Wystarczy obliczyć $\mathbf{e}_i A^T A \mathbf{e}_j$. □

Przykład 21 (Przykłady izometrii)**.** Symetria prostopadła, obrót.

Stwierdzenie 181. *Każda izometria $\mathbb{R}^2$ jest albo symetrią prostopadłą, albo obrotem.*

Dowód. Macierz

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

jest ortogonalna wtedy i tylko wtedy, gdy

$$A^T A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2+c^2 & ab+cd \\ ab+cd & b^2 d^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

mamy więc $a^2 + c^2 = b^2 + d^2 = 1$, $ab + cd = 0$. Z pierwszego równania istnieją $\alpha, \beta \in \mathbb{R}$ takie, że $a = \cos\alpha$, $c = \sin\alpha$, $d = \cos\beta$, $b = \sin\beta$. Z drugiego równania

$$ab + cd = \cos\alpha \sin\beta + \sin\alpha\cos\beta = \sin(\alpha+\beta) = 0,$$

więc $\alpha + \beta \equiv 0 \mod \pi$. Jeśli $\alpha + \beta \equiv 0 \mod 2\pi$, to $b = \sin\beta = -c$, $d = a$, a jeśli $\alpha + \beta \equiv \pi \mod 2\pi$, to $b = c$ i $d = -a$. Wobec tego

$$A = \begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix}, \quad \text{lub} \quad A = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}.$$

Druga macierz jest macierzą obrotu o kąt α. Macierz symetrii względem prostej generowanej przez wektor $(\cos\beta, \sin\beta)$ to

$$\begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} \cos\beta & \sin\beta \\ -\sin\beta & \cos\beta \end{pmatrix} = \begin{pmatrix} \cos^2\beta - \sin^2\beta & -2\sin\beta\cos\beta \\ -2\sin\beta\cos\beta & -\cos^2\beta - \sin^\beta \end{pmatrix} = \begin{pmatrix} \cos 2\beta & -\sin\beta \\ -\sin(-\beta) & -\cos(2\beta) \end{pmatrix},$$

więc dla $\alpha = -2\beta$ otrzymujemy pierwszą macierz. □

Stwierdzenie 182. *Jeśli $f : V \to V$ jest izometrią i $f(W) = W$ dla pewnej podprzestrzeni, to $f(W^\perp) = W^\perp$, a więc $f = f|_W \oplus f_{W^\perp}$.*

Dowód. f zachowuje iloczyn skalarny, więc też przestrzeń prostopadłą. □

Stwierdzenie 183. *Każdą izometrię V, $\dim(V) = n$, można zapisać jako złożenie co najwyżej n symetrii względem podprzestrzeni kowymiaru 1.*

Dowód. Dowód indukcyjny. Dla $n = 1$ istnieją tylko dwie izometrie — identyczność i $v \mapsto -v$. Niech $n > 1$ i niech $\alpha \in V$ będzie dowolnym wektorem. Jeśli $f(\alpha) = \alpha$, to oznaczmy $W = \{\alpha\}^\perp$, $W^\perp = \mathrm{lin}(\alpha)$. Na mocy założenia indukcyjnego $f|_W = s_1 \circ s_k$, gdzie s_i są symetriami względem podprzestrzeni $W_1, \ldots, W_k$, więc f jest złożeniem symetrii względem $W_i + \mathrm{lin}(\alpha)$. Jeśli $f(\alpha) \neq \alpha$, to niech g będzie złożeniem symetrii prostopadłej względem $\mathrm{lin}(\alpha - f(\alpha))^\perp$. Wtedy $g(\alpha) = \alpha$, więc g jest złożeniem co najwyżej $n-1$ symetrii, a więc f jest złożeniem co najwyżej n symetrii. □

Definicja 184. Zbiór G z działaniem $G \times G \ni (g,h) \mapsto gh \in G$ nazywamy grupą, jeśli:

- $\forall_{g,h,k\in G}\ (gh)k = g(hk)$ (łączność)
- $\exists_{e\in G}\forall_{g\in G}\ eg = g = ge$ (element neutralny)
- $\forall g \in G \exists_{h\in G}\ gh = hg = e$ (element odwrotny).

Stwierdzenie 185. *Macierze odwracalne $n \times n$ nad ciałem K z działaniem mnożenia stanowią grupę $GL(n,K)$. Macierze unitarne $n \times n$ nad $\mathbb{R}$ stanowią grupę $O(n)$.*

17. Wykład 19 (12 V)

17.1. **Przekształcenia samosprzężone.** Niech V będzie przestrzenią unitarną wymiaru n.

Definicja 186. Automorfizm $f : V \to V$ nazywamy *samosprzężonym*, jeśli dla dowolnych $\alpha, \beta \in V$ mamy

$$\langle \alpha, f(\beta)\rangle = \langle f(\alpha), \beta\rangle.$$

Stwierdzenie 187. *Niech $\mathcal{B}$ będzie bazą ortonormalną. Automorfizm $f : V \to V$ jest samosprzężony wtedy i tylko wtedy, gdy jego macierz w bazie $\mathcal{B}$ jest symetryczna.*

Dowód. Jeśli A — macierz f i $\mathbf{x}, \mathbf{y} \in M_{n\times 1}(\mathbb{R})$, to

$$\mathbf{x}^T(A\mathbf{y}) = (A\mathbf{x})^T\mathbf{y} = \mathbf{x}^T A^T \mathbf{y}.$$ □

Stwierdzenie 188. *Niech $f : V \to V$ będzie automorfizmem samosprzężonym. Wówczas*

- *jeśli $\alpha \in V$ jest wektorem własnym, to $f(\{\alpha\}^\perp) \subseteq \{\alpha\}^\perp$,*
- *jeśli $\alpha, \beta \in V$ są wektorami własnymi o różnych wartościach własnych, to $\alpha \perp \beta$.*

Dowód. Jeśli $\langle \alpha, \beta\rangle = 0$, to

$$\langle \alpha, f(\beta)\rangle = \langle f(\alpha), \beta\rangle = \langle \lambda\alpha, \beta\rangle = 0.$$

Jeśli $f(\alpha) = \lambda\alpha$, $f(\beta) = \mu\beta$ i $\lambda \neq \mu$, to

$$\lambda\langle \alpha, \beta\rangle = \langle f(\alpha), \beta\rangle = \langle \alpha, f(\beta)\rangle = \mu\langle \alpha, \beta\rangle,$$

a więc $\langle \alpha, \beta\rangle = 0$. □

Stwierdzenie 189. *Wszystkie wartości własne automorfizmu samospreżonego są rzeczywiste.*

Dowód. Niech $A = (a_{ij})$ będzie macierzą symetryczną o współczynnikach rzeczywistych i niech $\mathbf{z} = (z_1, \ldots, z_n)$ będzie zespolonym wektorem własnym o wartości własnej $c \in \mathbb{C}$. Mamy $A\mathbf{z} = c\mathbf{z}$, a więc dla każdego j

$$\sum_{i=1}^n a_{ij} z_i = c z_j \quad\Rightarrow\quad \sum_{i=1}^n a_{ij} z_i \bar{z}_j = c|z_j|^2 \quad\Rightarrow\quad \sum_{j=1}^n\sum_{i=1}^n a_{ij} z_i \bar{z}_j = \sum_{j=1}^n c|z_j|^2 \quad\Rightarrow$$

$$\sum_{i=1}^n a_{ii} z_i \bar{z}_i + \sum_{i<j} a_{ij}(z_i\bar{z}_j + \bar{z}_j z_j) = c\sum_{j=1}^n |z_j|^2 \quad\Rightarrow\quad c = \left(\sum_{i=1}^n a_{ii} z_i\bar{z}_i + \sum_{i<j} a_{ij}(z_i\bar{z}_j + \bar{z}_j z_j)\right)\left(\sum_{j=1}^n |z_j|^2\right)^{-1} \in \mathbb{R}.$$ □

Stwierdzenie 190. *Jeśli f jest samosprzężonym automorfizmem V, to istnieje baza ortonormalna V złożona z wektorów własnych.*

Dowód. Automorfizm f posiada wektor własny α z rzeczywistą wartością własną. Ponadto podprzestrzeń $\{\alpha\}^\perp$ jest f-niezmiennicza i $f_{\{\alpha\}^\perp}$ jest samosprzężonym automorfizmem $\{\alpha\}^\perp$. Z założenia indukcyjnego posiada bazę ortonormalną $\beta_1, \ldots, \beta_{n-1}$ złożoną z wektorów własnych. Wobec tego $(\alpha\|\alpha\|^{-1}, \beta_1, \ldots, \beta_{n-1})$ jest szukaną bazą. □

Wniosek. Rzeczywista macierz symetryczna jest diagonalizowalna.

Przestrzenie euklidesowe.

Definicja 191. *Przestrzenią euklidesową* nazywamy przestrzeń afiniczną A nad $\mathbb{R}$ z iloczynem skalarnym na T_A.

Niech A będzie przestrzenią euklidesową.

Definicja 192. *Odległość* punktów $x, y \in A$ to $\varrho(x, y) = \|y - x\|$.

Definicja 193. *Przestrzenią metryczną* nazywamy zbiór X z określoną funkcją $\varrho : X \times X \to \mathbb{R}_{\geqslant 0}$ taką, że:

- $x = y \iff \varrho(x, y) = 0$,
- $\varrho(x, y) = \varrho(y, x)$,
- $\varrho(x, z) \leqslant \varrho(x, y) + \varrho(y, z)$.

$\varrho(x, y)$ nazywamy odległością punktów x, y.

Stwierdzenie 194. *Przestrzeń euklidesowa jest przestrzenią metryczną.*

Definicja 195. Niech $B \subseteq A$ będzie podprzestrzenią afiniczną.

- *Rzutem prostopadłym na* B nazywamy przekształcenie afiniczne $\pi_B : A \to A$ takie, że $\pi_B(x) \in B$ oraz $(\pi_b(x) - x) \perp T_B$.
- *Symetrią prostopadłą względem* B nazywamy przekształcenie afiniczne $\sigma_B : A \to A$ takie, że $\frac{1}{2}(x + \pi_B(x)) \in B$ oraz $(\sigma_b(x) - x) \perp T_B$.

Definicja 196. *Układem bazowym ortogonalnym* (odpowiednio: *ortogonalnym*) nazywamy ciąg $(p; \beta_1, \ldots, \beta_n)$, gdzie $p \in A$ oraz $(\beta_1, \ldots, \beta_n)$ jest bazą ortogonalną (odpowiednio: ortogonalną) przestrzeni T_A

Stwierdzenie 197. *Wzory na symetrię i rzut w bazie ortogonalnej.*

Definicja 198. Niech $x \in A$ i niech $B \subseteq A$ będzie podprzestrzenią. *Odległością punktu x od podprzestrzeni B* nazywamy odległość rzutu $\pi_B(x)$ od x.

Stwierdzenie 199. *Jeśli $y \in B$, to $\varrho(x, y) \geqslant \varrho(x, B)$.*

Dowód. Z tw. Pitagorasa. □

18. Wykład 20 (17 V)

18.1. Miara pewnych podzbiorów przestrzeni euklidesowych.

Definicja 200. Niech $S(p_0, \ldots, p_n)$ oznacza sympleks o wierzchołkach p_i. *Miarą sympleksu* (n-wymiarową) nazywamy

$$\mu_n(S(p_0, \ldots, p_n)) = \frac{1}{n!}\sqrt{\det G(p_1 - p_0, \ldots, p_n - p_0)}.$$

Niech $R(p; \alpha_1, \ldots, \alpha_n)$ będzie równoległościanem. *Miarą równoległościanu* nazywamy

$$\mu_n(R(p; \alpha_1, \ldots, \alpha_n)) = \sqrt{\det G(\alpha_1, \ldots, \alpha_n)}.$$

Stwierdzenie 201. *Niech $R(p; \alpha_1, \ldots, \alpha_n)$ będzie równoległościanem i niech γ będzie rzutem α_n na $\{\alpha_1, \ldots \alpha_{n-1}\}^\perp$. Wówczas*

$$\mu_n(R(p; \alpha_1, \ldots, \alpha_n)) = \|\gamma\| \mu_n(R(p; \alpha_1, \ldots, \alpha_{n-1})).$$

Dowód. Zapisujemy $\alpha_n = \gamma + \beta$ i liczymy wyznacznik. □

Stwierdzenie 202. *Niech $p_0, \ldots, p_n$ będzie układem punktów w przestrzeni euklidesowej. Wówczas*

$$\mu_n(S(p_0, \ldots, p_{n-1}, p_n)) = \frac{1}{n}\|\gamma\| \cdot \mu_{n-1}(S(p_0, \ldots, p_{n-1}))$$

Orientacja i iloczyn wektorowy.

Definicja 203. Mówimy, że dwie bazy $\mathcal{B}$ i $\mathcal{B}'$ w przestrzeni wektorowej nad $\mathbb{R}$ są

- *zgodnie zorientowane* jeśli $\det M(id)_{\mathcal{B}}^{\mathcal{B}'} > 0$,
- *przeciwnie zorientowane* jeśli $\det M(id)_{\mathcal{B}}^{\mathcal{B}'} < 0$.

Stwierdzenie 204. *Zgodna orientacja jest relacją równoważności na zbiorze wszystkich baz. Posiada ona dwie klasy abstrakcji.*

Definicja 205.

- *Orientacją* przestrzeni wektorowej nad $\mathbb{R}$ nazywamy klasy równoważności baz zorientowanych.
- Mówimy, że przestrzeń jest *zorientowana*, jeśli została wybrana jej orientacja.
- Baza przestrzeni zorientowanej jest *zorientowana dodatnio* jeśli należy do wybranej klasy równoważności, a jest *zorientowana ujemnie* w przeciwnym przypadku.
- Izomorfizm przestrzeni zorientowanych *zachowuje orientację* jeśli przeprowadza bazy dodatnio zorientowane na bazy dodatnio zorientowane.

Definicja 206. Niech V będzie przestrzenią unitarną zorientowaną wymiaru n. Iloczynem wektorowym układu wektorów $\alpha_1, \ldots, \alpha_{n-1}$ nazywamy wektor $\beta \in V$ taki, że:

- Jeśli układ $(\alpha_1, \ldots, \alpha_{n-1})$ jest liniowo zależny, to $\beta = 0$.
- Jeśli układ $(\alpha_1, \ldots, \alpha_{n-1})$ jest liniowo niezależny, to
  - $\beta \in \operatorname{lin}(\alpha_1, \ldots, \alpha_{n-1})^\perp$,
  - $\|\beta\| = \sqrt{\det G(\alpha_1, \ldots, \alpha_{n-1})}$

– Baza $(\alpha_1, \dots, \alpha_{n-1}, \beta)$ jest dodatnio zorientowana.

Oznaczamy $\beta = \alpha_1 \times \dots \times \alpha_{n-1}$.

Stwierdzenie 207. *Iloczyn wektorowy jest odwzorowaniem antysymetrycznym $(n-1)$-liniowym.*

Dowód. Sprawdzimy liniowość na $(n-1)$-szej współrzędnej. Ustalamy $\alpha_1, \dots, \alpha_{n-2} \in V$; trzeba pokazać, że funkcja $f : V \to V$,

$$f(\gamma) = \alpha_1 \times \dots \times \alpha_{n-2} \times \gamma$$

jest przekształceniem liniowym. Oznaczmy $W = \mathrm{lin}(\alpha_1, \dots, \alpha_{n-2})$. Jeśli $\dim(W) < n-2$, to $f(\gamma) = 0$ dla każdego $\gamma \in V$, załóżmy więc, że $\dim(W) = n-2$. Niech (β_1, β_2) będzie bazą ortonormalną $W^\perp$ taką, że $(\alpha_1, \dots, \alpha_{n-1}, \beta_1, \beta_2)$ jest dodatnio zorientowana. Wówczas $f(\beta_1) = r\beta_2$, gdzie

$$r = \sqrt{\det G(\alpha_1, \dots, \alpha_{n-2}, \beta_1)} = \|\beta_1\| \sqrt{\det G(\alpha_1, \dots, \alpha_{n-2})} = \sqrt{\det G(\alpha_1, \dots, \alpha_{n-2})},$$

oraz $f(\beta_2) = -r\beta_1$, bo

$$\sqrt{\det G(\alpha_1, \dots, \alpha_{n-2}, \beta_1)} = \sqrt{\det G(\alpha_1, \dots, \alpha_{n-2}, \beta_2)} = |r|$$

oraz bazy $(\alpha_1, \dots, \alpha_{n-2}, \beta_1, \beta_2)$ i $(\alpha_1, \dots, \alpha_{n-2}, \beta_2, \beta_1)$ mają przeciwną orientację. Dowolny wektor $\gamma \in V$ można zapisać w postaci $\gamma = \delta + c_1\beta_1 + c_2\beta_2$, gdzie $\delta \in W$. Pozostaje sprawdzić, że

$$f(\delta + c_1\beta_1 + c_2\beta_2) = -rc_2\beta_1 + rc_1\beta_2.$$

Wektor $-c_2\beta_1 + c_1\beta_2$ jest prostopadły do W oraz do $\delta + rc_1\beta_1 + rc_2\beta_2$. Ponadto

$$\sqrt{\det G(\alpha_1, \dots, \alpha_{n-2}, \delta + c_1\beta_1 + c_2\beta_2)} = \|c_1\beta_1 + c_2\beta_2\| \sqrt{\det G(\alpha_1, \dots, \alpha_{n-2})} = r\sqrt{c_1^2 + c_2^2} = \|-rc_2\beta_1 + rc_1\beta_2\|,$$

czyli długość wektora jest odpowiednia. Macierz zmiany bazy z $(\alpha_1, \dots, \alpha_{n-2}, \beta_1, \beta_2)$ do bazy $(\alpha_1, \dots, \alpha_{n-2}, \delta + c_1\beta_1 + c_2\beta_2, -rc_2\beta_1 + rc_1\beta_2)$ ma postać

$$\begin{pmatrix} & & & \delta_1 & 0 \\ & I & & \vdots & \vdots \\ & & & \delta_{n-2} & 0 \\ 0 & \dots & 0 & c_1 & -rc_2 \\ 0 & \dots & 0 & c_2 & rc_1 \end{pmatrix}$$

Jej wyznacznik jest równy $r(c_1^2 + c_2^2)$, a więc dodatni. □

Stwierdzenie 208. *Jeśli (a, b, c) i (a', b', c') to współrzędne wektorów α, α' w bazie ortonormalnej, to*

$$\alpha \times \alpha' = (bc' - b'c, ca' - c'a, ab' - a'b).$$

Dowód. Wystaczy obliczyć $e_i \times e_j$ dla wektorów bazowych. □

19. Wykład 21 (19 V)

19.1. **Przestrzenie unitarne zespolone.** Niech V będzie przestrzenią wektorową nad $\mathbb{C}$ wymiaru n.

Definicja 209. *Formą hermitowską* na V nazywamy funkcję $\langle -, - \rangle : V \times V \to \mathbb{C}$ spełniającą następujące warunki:

- $\langle \alpha, \beta \rangle = \overline{\langle \beta, \alpha \rangle}$ (skośnie symetryczna),
- $\langle c\alpha, \beta \rangle = c\langle \alpha, \beta \rangle$,
- $\langle \alpha_1 + \alpha_2, \beta \rangle = \langle \alpha_1, \beta \rangle + \langle \alpha_2, \beta \rangle$ (liniowość na pierwszej współrzędnej),
- $\langle \alpha, \alpha \rangle = 0$ wttw $\alpha = 0$ (niezdegenowanie),
- $\langle \alpha, \alpha \rangle \in \mathbb{R}_+$ (dodatnia określoność).

Stwierdzenie 210. *Forma hermitowska jest półtoraliniowa, tj. liniowa na pierwszej współrzędnej i antyliniowa na drugiej:*

$$\langle \alpha, c\beta \rangle = \overline{\langle c\beta, \alpha \rangle} = \bar{c}\overline{\langle \beta, \alpha \rangle} = \bar{c}\langle \alpha, \beta \rangle.$$

Przykład 22 (Standardowa forma hermitowska na $\mathbb{C}^n$)**.** Określmy na $\mathbb{C}^n$ formę wzorem

$$\langle (z_1, \dots, z_n), (z'_1, \dots, z'_n) \rangle = z_1\bar{z}'_1 + \dots + z_n\bar{z}'_n.$$

Stwierdzenie 211. *Każda forma hermitowska na $\mathbb{C}^n$ jest dana wzorem*

$$\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x}^T A \bar{\mathbf{y}},$$

gdzie $A \in M_{n\times n}(\mathbb{C})$ jest macierzą taką, że $A^T = \bar{A}$.

Definicja 212. Macierz $A \in M_{n\times n}(\mathbb{C})$ taką, że $A^T = \bar{A}$ nazywamy *macierzą hermitowską.*

Definicja 213. *Przestrzenią unitarną zespoloną* nazywamy przestrzeń wektorową nad ciałem $\mathbb{C}$ z zadaną formą hermitowską.

Definicja 214. Niech V będzie przestrzenią unitarną zespoloną.
- *Długość wektora* $\alpha \in V$ to $\|\alpha\| := \sqrt{\langle \alpha, \alpha \rangle}$.
- Kąta pomiędzy wektorami nie definiujemy.
- Wektory α, β są prostopadłe ($\alpha \perp \beta$) jeśli $\langle \alpha, \beta \rangle$.
- Jeśli $W \subseteq V$, to $W^\perp = \{\alpha \in V : \forall_{\beta \in W}\ \alpha \perp \beta\}$ jest podprzestrzenią wektorową zwaną *ortogonalnym dopełnieniem* W.
- Bazę $(\beta_1, \ldots, \beta_n)$ przestrzeni V nazywamy *ortogonalną*, jeśli $\langle \beta_i, \beta_j \rangle = 0$ dla $i \neq j$.
- Bazę $(\beta_1, \ldots, \beta_n)$ przestrzeni V nazywamy *ortonormalną*, jeśli $\langle \beta_i, \beta_j \rangle = \delta_i^j$.

Stwierdzenie 215. *Jeśli $(\beta_1, \ldots, \beta_n)$ to baza ortonormalna V, to dla $\alpha \in V$ mamy*

$$\alpha = \sum_{i=1}^{n} \langle \alpha, \beta_i \rangle \beta_i.$$

Uwaga. Kolejność w iloczynie skalarnym we wzorze powyżej jest istotna.

Stwierdzenie 216 (Ortonormalizacja Grama-Schidta)**.** *Jeśli $(\beta_1, \ldots, \beta_n)$ jest bazą V, to $(\gamma_1, \ldots, \gamma_n)$ zadane wzorem indukcyjnym*

$$\beta_k' = \beta_k - \sum_{i=1}^{k-1} \langle \beta_k, \gamma_i \rangle, \qquad \gamma_k = \frac{\beta_k'}{\|\beta_k'\|}$$

jest bazą ortonormalną.

Definicja 217. Odwzorowanie $f : V \to W$, gdzie $V, W \in \mathbf{Vect}_{\mathbb{C}}$ nazywamy *antyhomomorfizmem* jeśli
- $f(\alpha + \beta) = f(\alpha) + f(\beta)$ dla $\alpha, \beta \in V$,
- $f(c\alpha) = \bar{c} f(\alpha)$ dla $c \in \mathbb{C}$, $\alpha \in V$.

Definicja 218. Odwzorowanie $F : V \to V^*$ zadane wzorem

$$F(\alpha)(\beta) = \langle \beta, \alpha \rangle$$

jest nazywane antyizomorfizmem Frecheta-Riesza.

19.2. **Odwzorowania unitarne.** Niech V będzie przestrzenią unitarną zespoloną wymiaru n.

Definicja 219. Homomorfizm $f : V \to W$ nazywamy *homomorfizmem unitarnym* jeśli $\langle f(\alpha), f(\beta) \rangle = \langle \alpha, \beta \rangle$ dla $\alpha, \beta \in V$.

Stwierdzenie 220. *Każdy homomorfizm unitarny jest monomorfizmem.*

Definicja 221. Macierz $A \in M_{n\times n}(\mathbb{C})$ nazywamy macierzą unitarną jeśli $A^T \bar{A} = I$.

Stwierdzenie 222.

(a) Macierz automorfizmu unitarnego w bazie ortonormalnej jest macierzą unitarną.
(b) Jeśli A, B są macierzami unitarnymi, to A^{-1}, $\bar{A}$, AB też są unitarne.
(c) Wyznacznik macierzy unitarnej ma moduł 1.
(d) Wiersze (kolumny) macierzy unitarnej stanowią bazę ortonormalną.

Stwierdzenie 223. *Jesli $A \in M_{2\times 2}(\mathbb{C})$ jest macierzą unitarną, to*

$$A = k \begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix}$$

dla pewnych liczb a, b, $|a|^2 + |b|^2 = 1$, $k \in \mathbb{C}$, $|k| = 1$.

Dowód. Bezpośredni rachunek. Załóżmy, że $\det A = 1$. Niech

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

Wektor (a, b) ma długość 1, więc $a^2 + b^2 = 1$. Wektory (a, b) i (c, d) są prostopadłe, więc

$$\langle (c, d), (a, b) \rangle = \bar{a}c + \bar{b}d = 0.$$

To równanie ma rozwiązania postaci $c = -\bar{b}z$, $d = \bar{a}z$ dla $z \in \mathbb{C}$. Ponadto

$$1 = ad - bc = a\bar{a}z + b\bar{b}z = z,$$

więc $z = 1$. W ogólnym przypadku rozważamy macierz $k^{-1}A$, gdzie k jest pierwiastkiem z wyznacznika A. □

Definicja 224. *Grupą unitarną rangi n $U(n)$* nazywamy grupę macierzy unitarnych $n \times n$. *Specjalną grupą unitarną $SU(n)$* nazywamy grupę macierzy unitarnych o wyznaczniku 1.

Ćwiczenie: znaleźć przekształcenie $SU(2) \to SO(3)$ które zachowuje mnożenie i nie jest identycznością.

20. Wykład 22 (24 V)

20.1. **Formy dwuliniowe.**

Niech K będzie ciałem charakterystyki różnej od 2, a V przestrzenią wektorową nad K wymiaru n.

Definicja 225. *Formą dwuliniową* nad V nazywamy odwzorowanie dwuliniowe $V \times V \to K$, tzn. takie, że $f(\alpha, -)$ i $f(-, \alpha)$ to funkcjonały liniowe. Formy dwuliniowe tworzą przestrzeń wektorową.

Uwaga. Forma dwuliniowa to przekształcenie liniowe $V \to V^*$ lub $V \otimes V \to K$ lub element $V^* \otimes V^*$.

Stwierdzenie 226. *Każda forma dwuliniowa na K^n ma postać*

$$f((x_1, \ldots, x_n), (y_1, \ldots, y_n)) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} x_i y_j,$$

gdzie $a_{ij} \in K$. Równoważnie,

$$f(\mathbf{x}, \mathbf{y}) = \mathbf{x}^T A \mathbf{y}$$

dla $A = (a_{ij}) \in M_{n \times n}(K)$. Macierz A nazywana jest też macierzą Grama *formy f.*

Stwierdzenie 227. *Jeśli A jest macierzą formy f w bazie $\mathcal{B}$, to $(M(id)^{\mathcal{B}}_{\mathcal{B}'})^T A M(id)^{\mathcal{B}}_{\mathcal{B}'}$ jest macierzą formy f w bazie $\mathcal{B}'$.*

Definicja 228. Mówimy, że macierze A, B są kongruentne jeśli istnieje macierz odwracalna C taka, że $A = C^T BC$.

Definicja 229. Mówimy, że forma f jest *nieosobliwa* (lub *niezdegenerowana*) jeśli spełniony jest jeden z równoważnych warunków:

- macierz formy jest odwracalna (to nie zależy od bazy),
- dla każdego $0 \neq \alpha \in V$ istnieje $\beta \in V$ takie, że $f(\alpha, \beta) \neq 0$,
- stowarzyszone przekształcenie $V \to V^*$ jest odwracalne.

Definicja 230. *Rzędem* formy dwuliniowej f oznaczanym $\mathrm{rk}(f)$ nazywamy:

- Rząd macierzy formy.
- Rząd przekształcenia $V \to V^*$.

Forma jest nieosobliwa wttw jej rząd jest równy wymiarowi macierzy.

20.2. **Formy symetryczne i antysymetryczne.**

Definicja 231. Formę dwuliniową nazywamy

- *symetryczną* jeśli $f(\alpha, \beta) = f(\beta, \alpha)$,
- *antysymetryczną* jeśli $f(\alpha, \beta) = f(\beta, \alpha)$.

Stwierdzenie 232. *Każda forma dwuliniowa jest sumą formy symetrycznej i antysymetrycznej.*

Dowód. Mamy $f(\alpha, \beta) = s(\alpha, \beta) + t(\alpha, \beta)$, gdzie

$$s(\alpha, \beta) = \tfrac{1}{2}(f(\alpha, \beta) + f(\beta, \alpha)) + \tfrac{1}{2}(f(\alpha, \beta) - f(\beta, \alpha)).$$

Analogiczny argument z przedstawieniem macierzy w postaci sumy macierzy symetrycznej i antysymetrycznej. $\square$

Definicja 233. Funkcję $q : V \to K$ nazywamy *formą kwadratową* jeśli istnieje forma dwuliniowa f taka, że $q(\alpha) = f(\alpha, \alpha)$.

Stwierdzenie 234. *Jeśli q jest formą kwadratową, to istnieje dokładnie jedna forma symetryczna f taka, że $q(\alpha) = f(\alpha, \alpha)$.*

Dowód. Z dwuliniowości

$$q(\alpha + \beta) = f(\alpha + \beta, \alpha + \beta) = q(\alpha) + q(\beta) + 2f(\alpha, \beta),$$

więc f jest wyznaczone przez q. $\square$

Niech teraz V będzie przestrzenią z określoną formą symetryczną f.

Definicja 235. Wektor α nazywamy *izotropowym* jeśli $f(\alpha, \alpha) = 0$.

Definicja 236. *Przestrzeń prostopadła* do $W \subseteq V$ to

$$W^\perp := \{\alpha \in V : \forall_{\beta \in W}\ f(\alpha, \beta) = 0\}.$$

Definicja 237. Podprzestrzeń dualna $W^d \subseteq V^*$ do podprzestrzeni $W \subseteq V$ to

$$W^d = \{\omega \in V^* : \omega(W) = 0\}.$$

Jeśli $\dim W = k$, to $\dim W^d = n - k$.

Stwierdzenie 238. *Niech $\bar{f} : V \to V^*$ będzie homomorfizmem stowarzyszonym z formą f. Wówczas*

$$W^\perp = (\bar{f})^{-1}(W^d).$$

Dowód. Mamy

$$\alpha \in W^\perp \Leftrightarrow \forall_{\beta \in W}\ f(\alpha, \beta) = 0 \Leftrightarrow \forall_{\beta \in W}\ \bar{f}(\alpha)(\beta) = 0 \Leftrightarrow \bar{f}(\alpha) \in W^d \Leftrightarrow \alpha \in (\bar{f})^{-1}(W^d).$$ $\square$

Stwierdzenie 239. *Niech $W \subseteq V$ będzie podprzestrzenią. Wówczas $f|_W$ jest nieosobliwa, wtedy i tylko wtedy, gdy $W \oplus W^\perp = V$.*

Dowód. Zauważyć, że jeśli $f|_W$ jest osobliwa, to istnieje $\alpha \in W \cap W^\perp$. Jeśli $f|_W$ jest nieosobliwa, to $\bar{f}|_W : W \to V^*$ jest monomorfizmem i $W^d \cap \bar{f}(W) = 0$ (bo inaczej $f|_W$ byłaby osobliwa), więc z porównania wymiarów wynika, że $V^* = \bar{f}(W) \oplus W^d$. Przekształcenie

$$g : V \xrightarrow{\bar{f}} V^* \cong \bar{f}(W) \oplus W^d \xrightarrow{p_1} \bar{f}(W)$$

jest epimorfizmem, więc $n - k = \dim(\ker(g)) = \dim((\bar{f})^{-1}(W^d)) = \dim(W^\perp)$. Więc $V = W \oplus W^d$. $\square$

Stwierdzenie 240. *Każdy ortogonalny układ nieizotropowych wektorów jest liniowo niezależny.*

Dowód. Liczymy wartości formy na kombinacji nieizotropowych wektorów i pewnym wektorze z tego układu. $\square$

Twierdzenie 241. *Każda forma symetryczna ma bazę prostopadłą.*

Dowód. Indukcja po wymiarze. Dla $n = 1$ oczywiste. Jeśli f ma wektor nieizotropowy α (tj. $f(\alpha, \alpha) \neq 0$) to mamy rozkład $\mathrm{lin}(\alpha) \oplus \mathrm{lin}(\alpha)^\perp$. Jeśli wszystkie wektory są izotropowe, to $f = 0$. $\square$

Wniosek. Każda forma symetryczna jest określona w pewnej bazie macierzą diagonalną.

Stwierdzenie 242. *Jeśli $K = \mathbb{C}$, to macierz formy w pewnej bazie dana jest macierzą $diag(1, \ldots, 1, 0, \ldots, 0)$. Jeśli $K = \mathbb{R}$, to macierz formy jest w pewnej bazie macierzą*

$$diag(1, \ldots, 1, -1, \ldots, -1, 0, \ldots, 0).$$

Stwierdzenie 243. *Rząd formy jest niezmiennikiem izomorfizmu. Wniosek: istnieje $n+1$ nieizomorfizmych form kwadratowych na $\mathbb{C}^n$, istnieje $n+1$ klas kongruencji macierzy $M_{n\times n}(\mathbb{C})$.*

Definicja 244. Niech $K = \mathbb{R}$. *Sygnaturą* formy symetrycznej nazywamy sumę elementów na przekątnej w postaci 0, 1, -1.

Twierdzenie 245 (Sylvestera o bezwładności)**.** *Sygnatura jest niezmiennikiem izomorfizmu.*

Dowód. Niech V, V' będą rzeczywistymi przestrzeniami wektorowymi nad $\mathbb{R}$ z formami symetrycznymi $f : V \otimes V \to \mathbb{R}$, $f' : V' \otimes V' \to \mathbb{R}$ oraz izomorfizm $F : V \to V'$ zachowujący formy symetryczne. Wybierzmy bazy prostopadłe $(\beta_i)_{i=1}^n$, $(\beta_i')_{i=1}^n$ na V i V' odpowiednio i niech $V = L_0 \oplus L_+ \oplus L_-$, $V' = L_0' \oplus L_+' \oplus L_-'$ będą rozkładami na podprzestrzenie generowane przez odpowiednio izotropowe, dodatnie i ujemne wektory baz. Wiemy, że $\dim(L_0) = \dim(L_0')$ (bo rzędy są równe). Załóżmy, że $\dim(L_+) > \dim(L_+')$. Przekształcenie

$$L_+ \subseteq V \xrightarrow{F} V' \cong L_0' \oplus L_+' \oplus L_-' \xrightarrow{proj} L_+'$$

ma nietrywialne jądro, więc istnieje niezerowy element $\alpha \in L_+$ taki, że $F(\alpha) \in L_0 \oplus L_-$. Ostatecznie $f(\alpha, \alpha) > 0$ i $f'(F(\alpha), F(\alpha)) \leqslant 0$ — sprzeczność. □

Stwierdzenie 246. *Każda forma symetryczna nad $\mathbb{R}$ jest wyznaczona jednoznacznie przez rząd i sygnaturę.*

Twierdzenie 247. *Twierdzenie Witta.*

21. Wykład 23 (31 V)

21.1. **Przestrzenie symplektyczne.** Niech V będzie przestrzenią wektorową z zadaną formą antysymetryczną.

Przykład 23. Jeśli $\dim(V) = 1$, to $f = 0$. Jeśli $\dim(V) = 2$, to $f = 0$ lub ma postać

$$f((x_1, x_2), (y_1, y_2)) = x_1 y_2 - x_2 y_1.$$

Stwierdzenie 248. *Niech V będzie przestrzenią z formą antysymetryczną. Istnieje baza w której forma ma postać*

$$\begin{pmatrix} 0 & I & 0 \\ -I & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Dowód. Dowód przez indukcję. Jeśli istnieje wektor $\alpha \in V$ taki, że $f(\alpha, V) = 0$, to wybieramy podprzestrzeń $W \subseteq V$ taką, że $W \oplus \mathrm{lin}(\alpha)$ i niech β_i będzie bazą symplektyczną W. Wtedy $(\beta_i) \cup \{\alpha\}$ jest bazą symplektyczną V. Jeśli zdegenerowany wektor α nie istnieje, wybierzmy dowolne $\alpha \neq 0$ i α' takie, że $f(\alpha, \alpha') = 1$. Oczywiście α, α' nie są współliniowe, więc $\dim(\alpha, \alpha') = 2$. Niech $\alpha^\perp$, $(\alpha')^\perp$ — są to podprzestrzenie wymiaru $n-1$ i nie są sobie równe, więc $\dim(W) = n-2$, gdzie $W = \alpha^\perp \cap (\alpha')^\perp$. Łatwo sprawdzić, że $W \cap \mathrm{lin}(\alpha, \alpha')$. Możemy więc wziąć bazę symplektyczną W i dołączyć α i α'. □

Definicja 249. Przestrzeń wektorową V z zadaną niezdegenerowaną formą dwuliniową antysymetryczną $f : V \otimes V \to K$ nazywamy przestrzenią symplektyczną.

21.2. **Diagonalizacja form kwadratowych.** Niech $f : V \otimes V \to K$ będzie formą symetryczną, a $q : V \to K$ odpowiadającą jej formą kwadratową. Wybierzmy bazę $(\beta_i)_{i=1}^n$ i niech $A = (a_{ij})$ będzie macierzą Grama formy f.

Stwierdzenie 250. *Jeśli $\mathcal{B} = (\beta_i)_{i=1}^n$ jest bazą ortogonalną złożoną z wektorów własnych przekształcenia zadanego macierzą A, to macierz Grama w bazie $\mathcal{B}$ jest diagonalna.*

Dowód. Wiemy, że β_i są wektorami własnymi przekształcenia

$$V \xrightarrow{\bar{f}} V^* \xrightarrow{\beta_i^* \mapsto \beta_i} V,$$

więc $f(\beta_i, \beta_j) = \bar{f}(\beta_i)(\beta_j) = c\beta_i^*(\beta_j) = 0$ dla $i \neq j$. □

Stwierdzenie 251 (Ortogonalizacja G-S)**.** *Niech $(\beta_i)_{i=1}^n$ będzie bazą. Niech γ_i będzie bazą zadaną wzorem indukcyjnym*

$$\gamma_k = \beta_k - \sum_{i=1}^{k-1} f(\beta_k, \gamma_i) f(\gamma_i, \gamma_i)^{-1} \gamma_i.$$

Wówczas w bazie γ_i forma ma macierz diagonalną — o ile nie zdarzy się, że $q(\gamma_i) = 0$. W ogólności należy zadbać o to, aby najpierw brać wektory nieizotropowe.

Stwierdzenie 252 (Sprowadzenie formy kwadratowej do sumy kwadratów)**.** *Załóżmy, że q dane jest wzorem*

$$q(x_1, \ldots, x_n) = \sum_{i=1}^n \sum_{j=1}^n a_{ij} x_i x_j$$

Istnieje podstawienie $y_i = h_i(x_1, \ldots, x_n)$ takie, że

$$q(y_1, \ldots, y_n) = \sum_{i=1}^n b_i y_i^2.$$

Dowód. Dowód indukcyjny. Rozważamy dwa przypadki. Jeśli pewna wartość na przekątnej jest niezerowa, możemy założyć, że $a_{11} \neq 0$. Mamy

$$q(x_1, \ldots, x_n) = a_{11} x_1^2 + 2x_1(a_{12}x_2 + \cdots + a_{1n}x_n) + q'(x_2, \ldots, x_n),$$

gdzie q' jest pewną formą kwadratową od $n-1$ zmiennych. Dalej

$$q(x_1, \ldots, q_n) = a_{11} \left(x_1 + \frac{a_{12}}{a_{11}} x_2 + \cdots + \frac{a_{1n}}{a_{11}} x_n \right)^2 + q''(x_2, \ldots, x_n)$$

dla pewnej innej formy q''. Po podstawieniu

$$y_1 = x_1 + \frac{1}{a_{11}}(a_{12}x_2 + \cdots + a_{1n}x_n), \quad y_2 = x_2, \ldots, y_n = x_n$$

mamy $q(y_1, \ldots, y_n) = a_{11} y_1^2 + q''(y_2, \ldots, y_n)$. Następnie stosujemy analogiczną redukcję dla formy q''.

Drugi przypadek: wszystkie a_{ii} są równe 0. Wtedy albo $A = 0$ i można wybrać dowolną bazę, albo można założyć, że $a_{12} = a_{21} \neq 0$, $a_{11} = a_{22} = 0$. Wtedy

$$q(x_1, \ldots, x_n) = 2a_{12}x_1x_2 + x_1 l_1(x_3, \ldots, x_n) + x_2 l_2(x_3, \ldots, x_n) + q'(x_3, \ldots, x_n)$$

Podstawiamy $x_1 = y_1 + y_2$, $x_2 = y_1 - y_2$, $x_i = y_i$ dla $i \geqslant 3$. Wtedy

$$q(y_1, \ldots, y_n) = 2a_{12} y_1^2 - 2a_{12} y_2^2 + q''(y_1, \ldots, y_n),$$

przy czym w q'' nie występują y_1^2 ani y_2^2. Można więc do tej formy zastosować sposób 1. □

22. Wykład 24 (2 VI)

22.1. **Potęgi symetryczne i zewnętrzne.**

Niech K — ciało charaktektystyki różnej od 2.

Stwierdzenie 253. *Niech f będzie formą dwuliniową na V. Wówczas f można traktować jak homomorfizm $f : V \otimes V \to K$.*

- *Jeśli forma f jest symetryczna wttw $f(\alpha \otimes \beta - \beta \otimes \alpha) = 0$ dla $\alpha, \beta \in V$.*
- *Jeśli forma f jest antysymetryczna wttw $f(\alpha \otimes \alpha) = 0$ dla $\alpha \in V$.*

Definicja 254. *Potęgą symetryczną* (drugą) przestrzeni V nazywamy przestrzeń

$$S^2(V) = V \otimes V / \operatorname{lin}\{\alpha \otimes \beta - \beta \otimes \alpha\}.$$

Potęgą zewnętrzną (drugą) przestrzeni V nazywamy przestrzeń

$$\Lambda^2(V) = V \otimes V / \operatorname{lin}\{\alpha \otimes \alpha\}.$$

Stwierdzenie 255. *Formy symetryczne na V odpowiadają homomorfizmom $S^2(V) \to K$, a formy antysymetryczne homomorfizmom $\Lambda^2(V) \to K$.*

Stwierdzenie 256. *Jeśli $(\beta_i)_{i=1}^n$ jest bazą V, to*

- *Bazę $S^2(V)$ stanowią tensory $\beta_i \otimes \beta_i$ oraz $\beta_i \otimes \beta_j + \beta_j \otimes \beta_i$ dla $i < j$, a więc $\dim(S^2(V)) = \frac{n(n+1)}{2}$.*
- *Bazę $\Lambda^2(V)$ stanowią tensory $\beta_i \otimes \beta_j - \beta_j \otimes \beta_i$ dla $i < j$, a więc $\dim(\Lambda^2(V)) = \frac{(n-1)n}{2}$.*
- *Mamy rozkład $V \otimes V \cong S^2(V) \oplus \Lambda^2(V)$.*

22.2. **Formy wieloliniowe.** Załóżmy, że K jest ciałem charakterystyki 0.

Definicja 257. *Formą k-liniową* nazywamy przekształcenie $f : V^{\otimes k} \to K$.

Definicja 258. Forma k-liniowa jest *symetryczna* jeśli zachodza równoważne warunki:

- $f(x_1, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_{j-1}, x_j, x_{j+1}, \dots, x_k) = f(x_1, \dots, x_{i-1}, x_j, x_{i+1}, \dots, x_{j-1}, x_i, x_{j+1}, \dots, x_k)$
- $f(x_1, \dots, x_k) = f(x_{\sigma(1)}, \dots, x_{\sigma(k)})$ dla dowolnej permutacji $\sigma \in \Sigma_n$.

Definicja 259. Forma k-liniowa f jest *antysymetryczna* jeśli zachodza równoważne warunki:

- $f(x_1, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_{j-1}, x_j, x_{j+1}, \dots, x_k) = -f(x_1, \dots, x_{i-1}, x_j, x_{i+1}, \dots, x_{j-1}, x_i, x_{j+1}, \dots, x_k)$
- $f(x_1, \dots, x_k) = |\sigma| \cdot f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$ dla dowolnej permutacji $\sigma \in \Sigma_k$.
- $f(x_1, \dots, x_k) = 0$ jeśli $x_i = x_j$ dla $i \neq j$.

Stwierdzenie 260. *Jeśli f jest symetryczna, to*

$$f(x_1 \otimes \dots \otimes x_i \otimes \dots \otimes x_j \otimes \dots \otimes x_k - x_1 \otimes \dots \otimes x_j \otimes \dots \otimes x_i \otimes \dots \otimes x_k) = 0.$$

Jeśli f jest antysymetryczna, to

$$f(x_1 \otimes \dots \otimes x_i \otimes \dots \otimes x_i \otimes \dots \otimes x_k) = 0.$$

Definicja 261. *k-tą potęgą symetryczną V* nazywamy

$$S^k(V) = V^{\otimes k}/\text{tensory z zamienionymi współrzędnymi.}$$

n-tą potęgą zewnętrzną V nazywamy

$$\Lambda^k(V) = V^{\otimes k}/\text{tensory z powtórzeniami.}$$

Stwierdzenie 262. *Formy k-liniowe symetryczne to funkcjonały na $S^k(V)$. Formy k-liniowe antysymetryczne to funkcjonały na $\Lambda^k(V)$.*

Definicja 263. Symetryzacja $s : V^{\otimes k} \to S^k(V)$

$$s(\alpha_1 \otimes \dots \otimes \alpha_k) = \frac{1}{k!} \sum_{\sigma \in \Sigma_k} \alpha_{\sigma(1)} \otimes \dots \otimes \alpha_{\sigma(k)}$$

Stwierdzenie 264. *Niech (β_i) będzie bazą przestrzeni V. Przestrzeń $S^n(V)$ jest generowana przez tensory postaci*

$$\beta_{i_1} \otimes \dots \otimes \beta_{i_k}$$

dla $i_1 \leqslant \dots \leqslant i_k$. Przestrzeń $\Lambda^n(V)$ jest generowana przez tensory

$$\beta_{i_1} \otimes \dots \otimes \beta_{i_k}$$

dla $i_1 < \dots < i_k$.

Uwaga. Oznaczenie — tensory w potędze zewnętrznej oznaczamy

$$\alpha_1 \wedge \dots \wedge \alpha_k,$$

a przestawienie dwóch współrzędnych powoduje zmianę znaku.

Wniosek. Jeśli $\dim(V) = n$, to

- $\dim(S^k(V)) = \binom{n+k-1}{k}$,
- $\dim(\Lambda^k(V)) = \binom{n}{k}$.

22.3. **Przykłady form k-liniowych.**

Przykład 24. Iloczyn wektorowy: $\Lambda^{n-1}(V) \to V$.

Przykład 25. Wyznacznik: $\Lambda^n(V) \to K$.

23. Wykład 25 (7 VI)

23.1. **Wielomiany.** Niech K będzie dowolnym ciałem.

Definicja 265. *Wielomianem* na zmiennych $x_1, \ldots, x_n$ nazywamy wyrażenie postaci

$$\sum_{i_1,\ldots,i_n \geqslant 0} a_{i_1,\ldots,i_n} x_1^{i_1} \ldots x_n^{i_n},$$

gdzie $a_{i_1,\ldots,i_n}$ są elementami K prawie wszystkimi równymi 0.

Definicja 266. *Suma i iloczyn wielomianów.*

Definicja 267. Oznaczenie: $K[x_1, \ldots, x_n]$.

Definicja 268. *Stopień wielomianu.*

Definicja 269. *Funkcja wielomianowa* zadana przez wielomian.

Stwierdzenie 270. *Jeśli ciało jest nieskończone, to funkcja wielomianowa jest wyznaczona jednoznacznie przez wielomian.*

Dowód. Wystarczy wykazać, że jeśli $W(c_1, \ldots, c_n) = 0$ dla wszystkich $(c_1, \ldots, c_n) \in K^n$, to $W = 0$. Dla $n = 1$ z twierdzenia Bezout, dalej indukcja z wyodrębnieniem zmiennej. □

Algebry.

Definicja 271. *Algebrą* nad ciałem K nazywamy przestrzeń wektorową A nad K wraz z zadanym mnożeniem

$$\mu : A \times A \to A$$

które jest łączne, tzn.

$$\mu(\alpha \otimes \mu(\beta \otimes \gamma)) = \mu(\mu(\alpha \otimes \beta) \otimes \gamma).$$

Można to zapisać jako równość $\mu(\mu \otimes id) = \mu(id \otimes \mu)$.

Będziemy zapisywać $\mu(\alpha \otimes \beta) = \alpha \cdot \beta$.

Definicja 272. Mówimy, że algebra A ma jedynkę, jeśli istnieje element $1 \in A$ taki, że $1 \cdot \alpha = \alpha = \alpha \cdot 1$.

Definicja 273. Algebra A jest przemienna jeśli zachodzi jeden z równoważnych warunków:

- $\forall_{\alpha,\beta \in A}\ \alpha \cdot \beta = \beta \cdot \alpha$,
- $\forall_{\alpha,\beta \in A}\ \mu(\alpha \otimes \beta) = \mu(\beta \otimes \alpha)$,
- $\mu\tau = \tau\mu : A \otimes A \to A$, gdzie $\tau : A \otimes A \to A \otimes A$ zamienia kolejność.

Przykład 26. Rozszerzenia ciał.

Przykład 27. $K[x_1, \ldots, x_n]$.

Przykład 28. $\mathrm{End}(V) \simeq M_{n \times n}(K)$.

Definicja 274. *Monoidem* nazywamy zbiór z łącznym działaniem i jedynką. Monoid jest przemienny, jeśli to działanie jest przemienne.

Definicja 275. Jeśli M jest monoidem, to

$$K[M] = \{f : M \to K : \ f \text{ prawie wszędzie równa } 0\}$$

z dodawaniem $(f + g)(m) = f(m) + g(m)$ i mnożeniem

$$(f \cdot g)(m) = \sum_{m_1 m_2 = m} f(m_1) g(m_2)$$

jest algebrą nad K (przemienną o ile M jest przemienny).

Przykład 29. Dla monoidu $\mathbb{N}^n$ otrzymujemy pierścień wielomianów of n zmiennych.

23.2. **Wielomiany symetryczne.**

Definicja 276. Wielomian $W(x_1, \ldots, x_n)$ jest *symetryczny* jeśli dla dowolnej permutacji $\sigma \in \Sigma_n$ mamy

$$W(x_1, \ldots, x_n) = W(x_{\sigma(1)}, \ldots, \sigma_n).$$

Definicja 277. Elementarnym wielomianem symetrycznym stopnia k od n zmiennych nazywamy wielomian

$$\sigma_n^k = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} x_{i_1} \ldots x_{i_k}.$$

Przykład 30. Elementarne wielomiany symetryczne dla małych n.

Twierdzenie 278. *Jeśli W jest wielomianem symetrycznym od n zmiennych, to istnieje wielomian P taki, że*

$$W(x_1, \ldots, x_n) = P(\sigma_n^1, \ldots, \sigma_n^n).$$

Dowód. Indukcja według pary (n, s), gdzie n jest liczbą zmiennych, a s jest stopniem wielomianu. Jeśli $n = 1$ to twierdzenie jest oczywiste. Załóżmy, że twierdzenie zachodzi dla dowolnych wielomianów, które mają mniej zmiennych niż n lub n zmiennych, ale stopień mniejszy niż s. Z założenia indukcyjnego mamy przedstawienie

$$W(x_1, \ldots, x_{n-1}, 0) = Q(\sigma_{n-1}^1, \ldots, \sigma_{n-1}^{n-1}).$$

Zdefinijmy $P_1 := P - Q(\sigma_n^1, \ldots, \sigma_n^{n-1})$. Można sprawdzić, że $P_1(x_1, \ldots, x_{n-1}, 0) = 0$. Z twierdzenia Darboux P_1 dzieli się przez x_n, a ponieważ jest symetryczny, to dzieli się przez σ_n^n. Wobec tego istnieje wielomian P_2 taki, że

$$P = \sigma_n^n P_2 + Q(\sigma_n^1, \ldots, \sigma_n^{n-1}).$$

Wielomian P_2 ma mniejszy stopień niż n , więc można go przedstawić jako wielomian od wielomianów symetrycznych. □

Twierdzenie 279. *Jeśli $Q(\sigma_n^1, \ldots, \sigma_n^n) = 0$, to $Q = 0$.*

Dowód. Bez dowodu. □

23.3. **Wielomiany jednorodne.**

Definicja 280. Wielomian $w(x_1, \ldots, x_n) = \sum a_{i_1, \ldots, i_n} x_1^{a_1} \ldots x_n^{a_n}$ nazywamy wielomianem jednorodnym stopnia k, jeśli

$$a_{i_1, \ldots, i_n} \neq 0 \;\Rightarrow\; \sum_{j=1}^n i_j = k.$$

Każdy wielomian można zapisać jednoznacznie jako sumę

$$w(x_1, \ldots, x_k) = \sum_{k=0}^{\infty} w_k(x_1, \ldots, x_n),$$

gdzie w_k jest wielomianem jednorodnym stopnia k.

Stwierdzenie 281. *Niech $P_k \subseteq K[x_1, \ldots, x_n]$ to podprzestrzeń wielomianów jednorodnych stopnia k. Wówczas P_k jest podprzestrzenią wektorową. Ponadto:*

- $P_0 \simeq K$,
- *P_1 to przestrzeń funkcjonałów liniowych na K^n (tj. $P_1 \cong (K^n)^*$),*
- *P_2 to przestrzeń form kwadratowych na K^n ($P_2 \cong (S^2(K^n))^* \cong S^2((K^n)^*)$).*

Stwierdzenie 282. *Niech V będzie skończenie wymiarową przestrzenią wektorową z bazą $(\beta_1, \ldots, \beta_n)$. Wówczas istnieje izomorfizm*

$$F : P_k \ni x_1^{i_1} \ldots x_n^{i_n} \mapsto \overbrace{\beta_1^* \otimes \cdots \otimes \beta_1^*}^{i_1 \ razy} \otimes \cdots \otimes \overbrace{\beta_n^* \otimes \cdots \otimes \beta_n^*}^{i_n \ razy} \in S^k(V^*)$$

23.4. **Funkcje wielomianowe.**

Definicja 283. Niech V będzie przestrzenią wektorową z bazą $(\beta_1, \ldots, \beta_n)$. Wówczas wielomian $w \in K[x_1, \ldots, x_n]$ zadaje funkcję wielomianową

$$f_w : V \ni \alpha \mapsto w(\beta_1^*(\alpha), \ldots, \beta_n^*(\alpha)) \in K.$$

Zadaje to homomorfizm $K[x_1, \ldots, x_n] \to C(V, K)$, który jest monomorfizmem jeśli ciało K jest nieskończone.

Niech A będzie przestrzenią afiniczną.

Definicja 284. Funkcję $f : A \to K$ nazywamy *funkcją wielomianową*, jeśli dla wybranego układu bazowego $(p; \beta_1, \ldots, \beta_n)$ istnieje wielomian $w(x_1, \ldots, x_n)$ taki, że

$$f\left(p + \sum c_i \beta_i\right) = w(c_1, \ldots, c_n).$$

Stopniem funkcji wielomianowej nazywamy najmniejszy możliwy stopień wielomianu w.

Definicja 285. Podzbiór $X \subseteq A$ nazywamy *hiperpowierzchnią*, jeśli jest zbiorem zer pewnej funkcji wielomianowej. Podzbiór jest *algebraiczny* jeśli jest przecięciem hiperpowierzchni.

23.5. **Klasyfikacja hiperpowierzchni stopnia $\leqslant 2$.** Niech A będzie przestrzenią afiniczną wymiaru n.

Stwierdzenie 286. *Hiperpowierzchnia stopnia* 0 *na* A *to albo cała przestrzeń, albo zbiór pusty.*

Stwierdzenie 287. *Hiperpowierzchnia stopnia* 1 *to hiperpłaszczyzna, zadana z pewnej bazie równaniem* $x_1 = 0$.

Stwierdzenie 288. *Każda hiperpowierzchnia stopnia* 2 *(kwadryka) na* $\mathbb{R}^2$ *jest afinicznie równoważna jednemu z poniższych zbiorów:*

- *zbiór pusty* $x^2 + y^2 + 1 = 0$,
- *okrąg (elipsa)* $x^2 + y^2 - 1 = 0$,
- *punkt* $x^2 + y^2 = 0$,
- *hiperbola* $x^2 - y^2 + 1 = 0$,
- *dwie proste przecinające się* $x^2 - y^2 = 0$,
- *parabola* $x^2 + y = 0$,
- *dwie proste równoległe* $x^2 = 1$,
- *prosta* $x^2 = 0$.

Dowód. Mamy

$$P = \{(x, y) \in \mathbb{R}^2 :\ w(x, y) = ax^2 + bxy + cy^2 + dx + ey + f = 0\}$$

Rozpatrzmy trzy przypadki:

- $a \neq 0$ lub $c \neq 0$. Możemy założyć, że $a \neq 0$. Wykonujemy postawienie $x = x - \frac{b}{2a}y$ i dostajemy wielomian, w którym współczynnik przy xy jest równy 0.
- $a = c = 0$, ale $b \neq 0$. Podstawiając $x = bx$ można założyć, że

  $$w(x, y) = xy + dx + ey + f.$$

  Podstawiamy $x = u + v$, $y = u - v$ i dostajemy wielomian, którego część 2-jednorodna nie zawiera uv.

Ostatecznie można założyć, że w jest postaci

$$w(x, y) = ax^2 + cy^2 + dx + ey + f.$$

Podstawiając $x = lx$, $y = my$ możemy uzyskać $a, c \in \{1, 0, -1\}$. Jeśli $a \neq 0$, to przy pomocy postawienia $x = x - \frac{d}{2a}$ dostajemy $d = 0$. Analogicznie, jeśli $c \neq 0$, to możemy skasować e. Można też unormować wyraz wolny — doprowadzić do stanu w którym $f \in \{-1, 0, 1\}$. Ostatecznie pozostają przypadki jak wyżej. $\square$

24. Wykład 26 (14 VI)

Stwierdzenie 289. *Każdą hiperpowierzchnię stopnia 2 na K^n można opisać w pewnej bazie równianiem*
$$a_1x_1^2 + \cdots + a_rx_r^2 + x_n = 0$$
lub
$$a_1x_1^2 + \cdots + a_rx_r^2 + c = 0$$
gdzie $a_1, \dots, a_r \neq 0$.

Dowód. Mamy
$$w(x_1, \dots, x_n) = q(x_1, \dots, x_n) + l(x_1, \dots, x_n) + c = 0,$$
gdzie q jest formą kwadratową (wielomianem jednorodnym stopnia 2), a l funkcjonałem (wielomianem jednorodnym stopnia 1). Ponieważ każdą formę można zdiagonalizować, można założyć, że $q(x_1, \dots, x_n) = a_1x_1^2 + \cdots + a_rx_r^2$. Po dokonaniu podstawień $x_i = x_i - \frac{a_i}{2b_i}$, gdzie b_i są współczynnikami nowo uzyskanej formy l możemy wyzerować zmienne w części liniowej. Otrzymujemy
$$w(x_1, \dots, x_n) = a_1x_1^2 + \cdots + a_rx_r^2 + b_{r+1}x_{r+1} + \cdots + b_nx_n + c = 0.$$
Jeśli część liniowa się zeruje, to otrzymaliśmy przypadek drugi, a jeśli nie to podstawiamy $x_n = b_{r+1}x_{r+1} + \cdots + b_nx_n + c$, a zmienne $x_{r+1}, \dots, x_{n-1}$ dowolnie i dostajemy przypadek pierwszy. □

Wniosek. Każdą hiperpowierzchnię stopnia 2 na $\mathbb{C}^n$ można opisać jednym z równań
$$x_1^2 + \cdots + x_r^2 = 0$$
$$x_1^2 + \cdots + x_r^2 + x_n = 0$$
$$x_1^2 + \cdots + x_r^2 + 1 = 0$$
Każdą hiperpowierzchnię stopnia 2 na $\mathbb{R}^n$ można opisać jednym z równań
$$x_1^2 + \cdots + x_r^2 - x_{r+1}^2 - \cdots - x_{r+s}^2 = 0$$
$$x_1^2 + \cdots + x_r^2 - x_{r+1}^2 - \cdots - x_{r+s}^2 + x_n = 0$$
$$x_1^2 + \cdots + x_r^2 - x_{r+1}^2 - \cdots - x_{r+s}^2 + 1 = 0$$

Stwierdzenie 290 (Klasyfikacja kwadryk na $\mathbb{C}^2$)**.** *Każda kwadryka na $\mathbb{C}^2$ jest opisana jednym z równań:*
- $x^2 + y^2 + 1$. *Odpowiadają jej trzy kwadryki rzeczywiste:*
  - $x^2 + y^2 + 1$ *(elipsa urojona),*
  - $x^2 + y^2 - 1$ *(elipsa),*
  - $x^2 - y^2 + 1$ *(hiperbola).*
- $x^2 + y^2$. *Odpowiadają jej dwie kwadryki rzeczywiste:*
  - $x^2 + y^2$ *(punkt),*
  - $x^2 - y^2$ *(para prostych przecinających się)*
- $x^2 + y$ *(parabola)*
- $x^2 + 1$. *Odpowiadają jej dwie kwadryki rzeczywiste:*
  - $x^2 + 1$ *(para prostych równoległych urojonych)*
  - $x^2 - 1$ *(para prostych równoległych)*
- $x^2 = 0$ *(prosta)*

Stwierdzenie 291 (Klasyfikacja kwadryk na $\mathbb{C}^3$)**.** *Każda kwadryka na $\mathbb{C}^2$ jest opisana jednym z równań:*
- $x^2 + y^2 + z^2 + 1$. *Odpowiadają jej następujące kwadryki rzeczywiste:*
  - $x^2 + y^2 + z^2 + 1$ *(elipsa urojona),*
  - $x^2 + y^2 + z^2 - 1$ *(elipsa),*
  - $x^2 + y^2 - z^2 + 1$ *(hiperboloida dwupowłokowa),*
  - $x^2 + y^2 - z^2 - 1$ *(hiperboloida jednopowłokowa),*
- $x^2 + y^2 + z^2$. *Odpowiadają jej następujące kwadryki rzeczywiste:*
  - $x^2 + y^2 + z^2$ *(punkt)*
  - $x^2 + y^2 - z^2$ *(stożek)*
- $x^2 + y^2 + z$. *Odpowiadają jej następujące kwadryki rzeczywiste:*
  - $x^2 + y^2 + z$ *(paraboloida eliptyczna)*

   - $x^2 - y^2 + z$ *(paraboloida hiperboliczna)*
- $x^2 + y^2 + 1$. *Odpowiadają jej następujące kwadryki rzeczywiste:*
   - $x^2 + y^2 + 1$ *(walec urojony)*
   - $x^2 + y^2 - 1$ *(walec eliptyczny)*
   - $x^2 - y^2 + 1$ *(walec hiperboliczny)*
- $x^2 + y^2$. *Odpowiadają jej następujące kwadryki rzeczywiste:*
   - $x^2 + y^2$ *(prosta)*
   - $x^2 - y^2$ *(para płaszczyzn przecinających się)*
- $x^2 + y$.*(walec paraboliczny)*
- $x^2 + 1$. *Odpowiadają jej następujące kwadryki rzeczywiste:*
   - $x^2 + 1$ *(prosta płaszczyzn równoległych urojona)*
   - $x^2 - 1$ *(para płaszczyzn równoległych)*
- $x^2 = 0$. *(płaszczyzna)*

Definicja 292. Punkt $p \in A$ nazywamy *środkiem symetrii* podzbioru przestrzeni afinicznej $X \subseteq A$ jeśli

$$p + \alpha \in X \;\Leftrightarrow\; p - \alpha \in X.$$

Stwierdzenie 293. *Jeśli $f : A \to A$ jest automorfizmem afinicznym zachowującym zbiór $X \subseteq A$ i p jest środkiem symetrii, to $f(p)$ też jest środkiem symetrii.*

Stwierdzenie 294. *Niech K będzie nieskończonym ciałem charakterystyki różnej od 2. Załóżmy, że hiperpowierzchnia $X \subseteq A$ nie jest zawarta w żadnej właściwej podprzestrzeni. Jeśli*

$$X = \{a_1x_1^2 + \dots a_rx_r^2 + c = 0\},$$

i $(s_1, \dots, s_n)$ jest środkiem symetrii X, to $s_1 = \dots = s_r = 0$. Jeśli

$$X = \{a_1x_1^2 + \dots a_rx_r^2 + x_n = 0\},$$

to X nie ma środka symetrii.

Dowód. Istnienie jest oczywiste. Załóżmy, że zachodzi przypadek 1 i $(s_1, \dots, s_n)$ jest środkiem symetrii. Jeśli $(x_i) \in X$, to

$$\sum_{i=1}^r a_ix_i^2 = -c = \sum_{i=1}^r a_i(2s_i - x_i)^2$$

więc

$$\sum_{i=1}^r a_i(4s_i^2 - 4s_ix_i) = 0$$

czyli współrzędne (x_i) muszą spełniać pewną tożsamość liniową która jest nietrywialna jeśli $s_i \neq 0$ dla pewnego $s_i \in \{1, \dots, r\}$.

W przypadku 2 niech $\mathbf{s} = (s_1, \dots, s_n)$ będzie środkiem symetrii. Jeśli $\mathbf{s} \in X$, to

$$\sum_{i=1}^r a_is_i^2 + s_n = 0.$$

Sprawdzamy, że $(-s_1, s_2, \dots, s_n) \in X$ skąd wynika, że $(3s_1, s_2, \dots, s_n) \in X$, więc $8s_1^2 = 0$. Analogicznie pokazujemy, że $s_1 = \dots = s_r = 0$, a więc również $s_n = 0$. Ale to nie jest środek symetrii. Jeśli $(s_1, \dots, s_n) \notin X$, to $(s_1, \dots, s_{n-1}, -a_1s_1^2 - \dots - a_rs_r^2) \in X$, ale punkt symetryczny ma współrzędne

$$(s_1, \dots, s_{n-1}, a_1s_1^2 + \dots + a_rs_r^2 + 2s_n)$$

i jak można sprawdzić nie należy do X. □

24.1. **Stożkowe.** Niech $K = \mathbb{R}$.

Stwierdzenie 295. *Dla każdej nieosobliwej hiperpowierzchni $X \subseteq \mathbb{R}^2$ stopnia 2 istnieje włożenie afiniczne $\mathbb{R}^2 \to \mathbb{R}^3$ takie, że X jest przeciwobrazem standardowego stożka $x^2 + y^2 - z^2 = 0$.*

Od tego momentu rozpatrujemy metrykę na $\mathbb{R}^2$.

Definicja 296. Niech $a \in \mathbb{R}^2$, $K \subseteq \mathbb{R}$ będzie prostą i $e > 0$. *Stożkową* o ognisku a, kierownicy K i mimośrodzie e nazywamy zbiór

$$S(a, K, e) = \{p \in \mathbb{R}^2 : \ \varrho(p, a) = e \cdot \varrho(p, K)\}.$$

Stwierdzenie 297. *Dla $a \in K$ stożkowa jest zbiorem pustym dla $e < 1$, prostą dla $e = 1$ i sumą dwóch prostych dla $e > 1$.*

Stwierdzenie 298. *Dla $a \notin K$, to stożkowa jest elipsą, jeśli $e < 1$, parabolą dla $e = 1$ i hiperbolą dla $e > 1$. Okrąg jest zdegenerowanym przypadkiem elipsy — dla kierownicy w nieskończoności.*

Definicja 299. Kanoniczne równanie elipsy (a, b — osie):

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1.$$

Kanoniczne równanie hiperboli (a — oś rzeczywista, b — oś urojona):

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1.$$

Kanoniczne równanie paraboli:

$$x^2 = 2dy.$$

Stwierdzenie 300. *Każdą stożkową można zapisać w postaci kanonicznej w pewnym metrycznie równoważnym układzie współrzędnych.*

Dowód. Bez straty ogólności możemy założyć, że $K = \{(u, y) : \ y \in \mathbb{R}\}$, $a = (v, 0)$, gdzie $r = u - v$ jest odległością pomiędzy ogniskiem a kierownicą. Wówczas $S(a, K, e)$ dana jest równaniem

$$(x - v)^2 + y^2 = e^2(x - u)^2$$

czyli

$$x^2(1 - e^2) + x(-2v + 2e^2u) + y^2 = (e^2u^2 - v^2).$$

Załóżmy, że $e \neq 1$. Wówczas możemy dobrać u, v tak, aby $v = e^2u$ przy zachowaniu r. Konkretnie

$$u = \frac{1}{1 - e^2} r, \quad v = \frac{e^2}{1 - e^2} r.$$

Dostajemy wtedy równanie

$$x^2(1 - e^2) + y^2 = r^2 \left(e^2 \frac{1}{(1 - e^2)^2} - \frac{e^4}{(1 - e^2)^2} \right) = r^2 \frac{e^2}{1 - e^2}.$$

Po podzieleniu przez prawą stronę otrzymujemy

$$x^2 \left(\frac{1 - e^2}{re} \right)^2 \pm y^2 \left(\frac{\sqrt{|1 - e^2|}}{re} \right)^2 = 1,$$

przy czym znak przy y jest dodatni dla $e < 1$ i ujemny dla $e > 1$. Otrzymujemy równanie elipsy (hiperboli) o osiach

$$a = r \frac{e}{1 - e^2}, \quad b = r \frac{e}{\sqrt{|1 - e^2|}}.$$

Dla $e = 1$ przyjmujemy $u = -\frac{r}{2}$, $v = \frac{r}{2}$ i dostajemy równanie

$$y^2 = 2rx. \qquad \square$$

Stwierdzenie 301. *Każdą formę kwadratową na przestrzeni unitarnej $\mathbb{R}^2$ można zdiagonalizować przy pomocy unitarnej zmainy bazy.*

Stwierdzenie 302. *Każda hiperpowierzchnia stopnia 2 jest izometryczna z pewną stożkową w postaci kanonicznej.*