Geometria z Algebrą Liniową II*

Arkadiusz Męcel

WYKŁAD 10, 8.04.2021 r.

Twierdzenie

Niech (V, h) będzie przestrzenią dwuliniową nad ciałem charakterystyki różnej od 2. Wówczas (V, h) ma bazę prostopadłą.

Wniosek

Dla każdej macierzy symetrycznej $A \in M_n(K)$, gdzie $\mathrm{char}(K) \neq 2$ istnieje kongruentna do niej macierz diagonalna $D \in M_n(K)$.

Twierdzenie

Niech $(V, \langle\, , \rangle)$ będzie przestrzenią euklidesową. Wówczas (V, h) ma bazę ortonormalną $\mathcal{A}$, to znaczy: $G(\langle\, , \rangle, \mathcal{A}) = I$.

Kryterium Sylvestera

Symetryczna macierz nad $\mathbb{R}$ jest kongruentna z macierzą identycznościową wtedy i tylko wtedy, gdy wszystkie jej wiodące minory główne są dodatnie.

Twierdzenie (Jacobiego)

Niech (V, h) będzie taką przestrzenią dwuliniową, że wiodące minory główne $\Delta_i = A^{(i)}$ macierzy $A = G(h, \mathcal{A})$ są niezerowe, dla pewnej bazy $\mathcal{A}$ przestrzeni V. Wówczas istnieje baza $\mathcal{B}$ przestrzeni V taka, że

$$G(h, \mathcal{B}) = \operatorname{diag}\left(\frac{\Delta_1}{\Delta_0}, \ldots, \frac{\Delta_n}{\Delta_{n-1}}\right), \qquad \text{gdzie } \Delta_0 = 1.$$

Twierdzenie (Jacobiego)

Niech (V, h) będzie taką przestrzenią dwuliniową, że wiodące minory główne $\Delta_i = A^{(i)}$ macierzy $A = G(h, \mathcal{A})$ są niezerowe, dla pewnej bazy $\mathcal{A}$ przestrzeni V. Wówczas istnieje baza $\mathcal{B}$ przestrzeni V taka, że

$$G(h, \mathcal{B}) = \operatorname{diag}\left(\frac{\Delta_1}{\Delta_0}, \ldots, \frac{\Delta_n}{\Delta_{n-1}}\right), \quad \text{gdzie } \Delta_0 = 1.$$

Twierdzenie to pozwala w niektórych sytuacjach stosunkowo łatwo stwierdzać czy macierze są kongruentne nad ciałem K (zwłaszcza jeśli możemy w ciele K rozważać pojęcie „znaku” elementu, o czym będzie dalej).

Uwaga: nie musimy nic zakładać o ciele K (wobec założenia $\Delta_1 \neq 0$ wiemy, że forma h nie jest alternująca, a zatem (V, h) ma zawsze bazę ortogonalną, nawet jeśli ciało K ma charakterystykę 2).

Idea (rozwiniemy ją kiedyś): w zasadzie wykonujemy znowu ortogonalizację G-S.

Twierdzenie (Jacobiego)

Niech (V, h) będzie taką przestrzenią dwuliniową, że wiodące minory główne $\Delta_i = A^{(i)}$ macierzy $A = G(h, \mathcal{A})$ są niezerowe, dla pewnej bazy $\mathcal{A}$ przestrzeni V. Wówczas istnieje baza $\mathcal{B}$ przestrzeni V taka, że

$$G(h, \mathcal{B}) = \operatorname{diag}\left(\frac{\Delta_1}{\Delta_0}, \ldots, \frac{\Delta_n}{\Delta_{n-1}}\right), \quad \text{gdzie } \Delta_0 = 1.$$

Dowód. Indukcja. Załóżmy, że istnieje baza $\mathcal{C} = (\gamma_1, \ldots, \gamma_n)$ przestrzeni V, że:

$$G(h, \mathcal{C}) = \begin{bmatrix} \Delta_1/\Delta_0 & 0 & \ldots & 0 & h(\gamma_1, \gamma_n) \\ 0 & \Delta_2/\Delta_1 & \ldots & 0 & h(\gamma_2, \gamma_n) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & \Delta_{n-1}/\Delta_{n-2} & h(\gamma_{n-1}, \gamma_n) \\ h(\gamma_n, \gamma_1) & h(\gamma_n, \gamma_2) & \ldots & h(\gamma_{n-1}, \gamma_n) & h(\gamma_n, \gamma_n) \end{bmatrix}.$$

Twierdzenie (Jacobiego)

Niech (V, h) będzie taką przestrzenią dwuliniową, że wiodące minory główne $\Delta_i = A^{(i)}$ macierzy $A = G(h, \mathcal{A})$ są niezerowe, dla pewnej bazy $\mathcal{A}$ przestrzeni V. Wówczas istnieje baza $\mathcal{B}$ przestrzeni V taka, że

$$G(h, \mathcal{B}) = \operatorname{diag}\left(\frac{\Delta_1}{\Delta_0}, \dots, \frac{\Delta_n}{\Delta_{n-1}}\right), \qquad \text{gdzie } \Delta_0 = 1.$$

Dowód. Indukcja. Załóżmy, że istnieje baza $\mathcal{C} = (\gamma_1, \dots, \gamma_n)$ przestrzeni V, że:

$$G(h, \mathcal{C}) = \begin{bmatrix} \Delta_1/\Delta_0 & 0 & \dots & 0 & h(\gamma_1, \gamma_n) \\ 0 & \Delta_2/\Delta_1 & \dots & 0 & h(\gamma_2, \gamma_n) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & \Delta_{n-1}/\Delta_{n-2} & h(\gamma_{n-1}, \gamma_n) \\ h(\gamma_n, \gamma_1) & h(\gamma_n, \gamma_2) & \dots & h(\gamma_{n-1}, \gamma_n) & h(\gamma_n, \gamma_n) \end{bmatrix}.$$

Skoro $W = \operatorname{lin}(\gamma_1, \dots, \gamma_{n-1})$ jest nieosobliwa (bo $\Delta_{n-1} \neq 0$) to można przyjąć, że γ_n to niezerowy wektor z $W^\perp$ (mamy wszak $V = W \oplus W^\perp$), czyli...

Twierdzenie (Jacobiego)

Niech (V, h) będzie taką przestrzenią dwuliniową, że wiodące minory główne $\Delta_i = A^{(i)}$ macierzy $A = G(h, \mathcal{A})$ są niezerowe, dla pewnej bazy $\mathcal{A}$ przestrzeni V. Wówczas istnieje baza $\mathcal{B}$ przestrzeni V taka, że

$$G(h, \mathcal{B}) = \operatorname{diag}\left(\frac{\Delta_1}{\Delta_0}, \ldots, \frac{\Delta_n}{\Delta_{n-1}}\right), \qquad \text{gdzie } \Delta_0 = 1.$$

Dowód. Indukcja. Załóżmy, że istnieje baza $\mathcal{C} = (\gamma_1, \ldots, \gamma_n)$ przestrzeni V, że:

$$G(h, \mathcal{C}) = \begin{bmatrix} \Delta_1/\Delta_0 & 0 & \ldots & 0 & 0 \\ 0 & \Delta_2/\Delta_1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & \Delta_{n-1}/\Delta_{n-2} & 0 \\ 0 & 0 & \ldots & 0 & h(\gamma_n, \gamma_n) \end{bmatrix}.$$

Twierdzenie (Jacobiego)

Niech (V, h) będzie taką przestrzenią dwuliniową, że wiodące minory główne $\Delta_i = A^{(i)}$ macierzy $A = G(h, \mathcal{A})$ są niezerowe, dla pewnej bazy $\mathcal{A}$ przestrzeni V. Wówczas istnieje baza $\mathcal{B}$ przestrzeni V taka, że

$$G(h, \mathcal{B}) = \operatorname{diag}\left(\frac{\Delta_1}{\Delta_0}, \ldots, \frac{\Delta_n}{\Delta_{n-1}}\right), \quad \text{gdzie } \Delta_0 = 1.$$

Dowód. Indukcja. Załóżmy, że istnieje baza $\mathcal{C} = (\gamma_1, \ldots, \gamma_n)$ przestrzeni V, że:

$$G(h, \mathcal{C}) = \begin{bmatrix} \Delta_1/\Delta_0 & 0 & \ldots & 0 & 0 \\ 0 & \Delta_2/\Delta_1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & \Delta_{n-1}/\Delta_{n-2} & 0 \\ 0 & 0 & \ldots & 0 & h(\gamma_n, \gamma_n) \end{bmatrix}.$$

Niech $C = M(\mathrm{id})^{\mathcal{A}}_{\mathcal{C}}$ i $\det C = d$. Mamy $C^T \cdot A \cdot C = G(h, \mathcal{C})$ oraz $\det A = \Delta_n$. Zatem $d^2 \cdot \Delta_n = \Delta_{n-1} \cdot h(\gamma_n, \gamma_n)$. Możemy podmienić wektor γ_n przez $d^{-1} \cdot \gamma_n$ dostając:

Twierdzenie (Jacobiego)

Niech (V, h) będzie taką przestrzenią dwuliniową, że wiodące minory główne $\Delta_i = A^{(i)}$ macierzy $A = G(h, \mathcal{A})$ są niezerowe, dla pewnej bazy $\mathcal{A}$ przestrzeni V. Wówczas istnieje baza $\mathcal{B}$ przestrzeni V taka, że

$$G(h, \mathcal{B}) = \operatorname{diag}\left(\frac{\Delta_1}{\Delta_0}, \ldots, \frac{\Delta_n}{\Delta_{n-1}}\right), \qquad \text{gdzie } \Delta_0 = 1.$$

Dowód. Indukcja. Załóżmy, że istnieje baza $\mathcal{C} = (\gamma_1, \ldots, \gamma_n)$ przestrzeni V, że:

$$G(h, \mathcal{C}) = \begin{bmatrix} \Delta_1/\Delta_0 & 0 & \ldots & 0 & 0 \\ 0 & \Delta_2/\Delta_1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & \Delta_{n-1}/\Delta_{n-2} & 0 \\ 0 & 0 & \ldots & 0 & h(\gamma_n, \gamma_n)/d^2 \end{bmatrix}.$$

Twierdzenie (Jacobiego)

Niech (V, h) będzie taką przestrzenią dwuliniową, że wiodące minory główne $\Delta_i = A^{(i)}$ macierzy $A = G(h, \mathcal{A})$ są niezerowe, dla pewnej bazy $\mathcal{A}$ przestrzeni V. Wówczas istnieje baza $\mathcal{B}$ przestrzeni V taka, że

$$G(h, \mathcal{B}) = \operatorname{diag}\left(\frac{\Delta_1}{\Delta_0}, \ldots, \frac{\Delta_n}{\Delta_{n-1}}\right), \quad \text{gdzie } \Delta_0 = 1.$$

Dowód. Indukcja. Załóżmy, że istnieje baza $\mathcal{C} = (\gamma_1, \ldots, \gamma_n)$ przestrzeni V, że:

$$G(h, \mathcal{C}) = \begin{bmatrix} \Delta_1/\Delta_0 & 0 & \ldots & 0 & 0 \\ 0 & \Delta_2/\Delta_1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & \Delta_{n-1}/\Delta_{n-2} & 0 \\ 0 & 0 & \ldots & 0 & h(\gamma_n, \gamma_n)/d^2 \end{bmatrix}.$$

Teraz jednak $\det M(\mathrm{id})_{\mathcal{C}}^{\mathcal{A}} = 1$. Zatem $\Delta_n = \Delta_{n-1} \cdot \frac{h(\gamma_n, \gamma_n)}{d^2}$, co kończy dowód.

Problem

Znaleźć warunki konieczne i dostateczne na to, by dla nad ciałem K zachodziła kongruencja macierzy diagonalnych: $\mathrm{diag}(a_1, \ldots, a_n) \cong \mathrm{diag}(b_1, \ldots, b_n)$.

Problem

Znaleźć warunki konieczne i dostateczne na to, by dla nad ciałem K zachodziła kongruencja macierzy diagonalnych: $\mathrm{diag}(a_1, \dots, a_n) \cong \mathrm{diag}(b_1, \dots, b_n)$.

Trywialna uwaga 1 Jeśli $A = \mathrm{diag}(a_1, \dots, a_n)$ oraz $B = \mathrm{diag}(a_{\sigma(1)}, \dots, a_{\sigma(n)})$, dla pewnej permutacji $\sigma \in S_n$, to jeśli P jest macierzą permutacji σ, to $B = P^T AP$, czyli:

$$\mathrm{diag}(a_1, \dots, a_n) \cong \mathrm{diag}(a_{\sigma(1)}, \dots, a_{\sigma(n)}).$$

Innymi słowy, jeśli $A = G(h, \mathcal{A})$, gdzie $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$, to dla bazy $\mathcal{B} = (\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)})$ mamy $B = G(h, \mathcal{B})$.

Problem

Znaleźć warunki konieczne i dostateczne na to, by dla nad ciałem K zachodziła kongruencja macierzy diagonalnych: $\mathrm{diag}(a_1, \ldots, a_n) \cong \mathrm{diag}(b_1, \ldots, b_n)$.

Trywialna uwaga 1 Jeśli $A = \mathrm{diag}(a_1, \ldots, a_n)$ oraz $B = \mathrm{diag}(a_{\sigma(1)}, \ldots, a_{\sigma(n)})$, dla pewnej permutacji $\sigma \in S_n$, to jeśli P jest macierzą permutacji σ, to $B = P^T AP$, czyli:

$$\mathrm{diag}(a_1, \ldots, a_n) \cong \mathrm{diag}(a_{\sigma(1)}, \ldots, a_{\sigma(n)}).$$

Trywialna uwaga 2 Dla dowolnych $a_1, \ldots, a_n, b_1 \neq 0, \ldots, b_n \neq 0 \in K$ mamy:

$$\mathrm{diag}(a_1, \ldots, a_n) \cong \mathrm{diag}(b_1^2 a_1, \ldots, b_n^2 a_n).$$

Problem

Znaleźć warunki konieczne i dostateczne na to, by dla nad ciałem K zachodziła kongruencja macierzy diagonalnych: $\mathrm{diag}(a_1, \dots, a_n) \cong \mathrm{diag}(b_1, \dots, b_n)$.

Trywialna uwaga 1 Jeśli $A = \mathrm{diag}(a_1, \dots, a_n)$ oraz $B = \mathrm{diag}(a_{\sigma(1)}, \dots, a_{\sigma(n)})$, dla pewnej permutacji $\sigma \in S_n$, to jeśli P jest macierzą permutacji σ, to $B = P^T AP$, czyli:

$$\mathrm{diag}(a_1, \dots, a_n) \cong \mathrm{diag}(a_{\sigma(1)}, \dots, a_{\sigma(n)}).$$

Trywialna uwaga 2 Dla dowolnych $a_1, \dots, a_n, b_1 \neq 0, \dots, b_n \neq 0 \in K$ mamy:

$$\mathrm{diag}(a_1, \dots, a_n) \cong \mathrm{diag}(b_1^2 a_1, \dots, b_n^2 a_n).$$

Definicja

Ciało K nazywamy **kwadratowo domkniętym**, jeśli każdy element K jest kwadratem pewnego elementu z K.

Uwaga

Jeśli K jest ciałem kwadratowo domkniętym oraz jeśli $A = \mathrm{diag}(a_1, \ldots, a_r, 0, \ldots, 0) \in M_n(K)$, gdzie $a_i \neq 0$, to

$$\mathrm{diag}(a_1, \ldots, a_r, 0, \ldots, 0) \simeq \mathrm{diag}(\underbrace{1, \ldots, 1}_{r}, 0, \ldots, 0).$$

Uwaga

Jeśli K jest ciałem kwadratowo domkniętym oraz jeśli $A = \operatorname{diag}(a_1, \dots, a_r, 0, \dots, 0) \in M_n(K)$, gdzie $a_i \neq 0$, to

$$\operatorname{diag}(a_1, \dots, a_r, 0, \dots, 0) \simeq \operatorname{diag}(\underbrace{1, \dots, 1}_{r}, 0, \dots, 0).$$

Dowód. Jeśli $A = \operatorname{diag}(a_1, \dots, a_r, 0, \dots, 0) \in M_n(\mathbb{C})$, gdzie $a_i \neq 0$, jest macierzą formy h na V w bazie $(\alpha_1, \dots, \alpha_n)$, to biorąc bazę $\mathcal{B} = (\beta_1, \dots \beta_n)$ postaci:

$$\beta_j = \begin{cases} \frac{1}{\sqrt{a_i}}\alpha_i, & \text{dla } i \leq r, \\ \alpha_i, & \text{dla } i > r \end{cases}$$

dostajemy: $G(h, \mathcal{B}) = \operatorname{diag}(1, \dots, 1, 0, \dots, 0)$, czyli:

$$\operatorname{diag}(a_1, \dots, a_r, 0, \dots, 0) \simeq \operatorname{diag}(\underbrace{1, \dots, 1}_{r}, 0, \dots, 0).$$

Uwaga

Jeśli K jest ciałem kwadratowo domkniętym oraz jeśli $A = \operatorname{diag}(a_1, \dots, a_r, 0, \dots, 0) \in M_n(K)$, gdzie $a_i \neq 0$, to

$$\operatorname{diag}(a_1, \dots, a_r, 0, \dots, 0) \simeq \operatorname{diag}(\underbrace{1, \dots, 1}_{r}, 0, \dots, 0).$$

Przykłady ciał kwadratowo domkniętych:

- ciała algebraicznie domknięte,
- ciało $\mathbb{Z}_2$ (trudniejszy fakt: dowolne skończone ciało charakterystyki 2).

Uwaga

Jeśli K jest ciałem kwadratowo domkniętym oraz jeśli $A = \operatorname{diag}(a_1, \ldots, a_r, 0, \ldots, 0) \in M_n(K)$, gdzie $a_i \neq 0$, to

$$\operatorname{diag}(a_1, \ldots, a_r, 0, \ldots, 0) \simeq \operatorname{diag}(\underbrace{1, \ldots, 1}_{r}, 0, \ldots, 0).$$

Przykłady ciał kwadratowo domkniętych:

- ciała algebraicznie domknięte,
- ciało $\mathbb{Z}_2$ (trudniejszy fakt: dowolne skończone ciało charakterystyki 2).

Wniosek

Jeśli $A, B \in M_n(K)$, gdzie K jest ciałem kwadratowo domkniętym charakterystyki różnej od 2, to $A \cong B \Leftrightarrow r(A) = r(B)$.

Uwaga

Jeśli K jest ciałem kwadratowo domkniętym oraz jeśli $A = \mathrm{diag}(a_1, \ldots, a_r, 0, \ldots, 0) \in M_n(K)$, gdzie $a_i \neq 0$, to

$$\mathrm{diag}(a_1, \ldots, a_r, 0, \ldots, 0) \simeq \mathrm{diag}(\underbrace{1, \ldots, 1}_{r}, 0, \ldots, 0).$$

Definicja

Na zbiorze $\dot{K}$ niezerowych elementów ciała K definiujemy relację równoważności: $a \sim b$ wtedy i tylko wtedy, gdy ab^{-1} jest kwadratem w K. Zbiór klas abstrakcji $\dot{K}/\dot{K}^2$ ma strukturę grupy z działaniem

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

nazywanej **grupą klas kwadratów ciała** K.

Przykłady i uwagi (informacyjnie)

- Dla ciał kwadratowo domkniętych mamy $|\dot{K}/\dot{K}^2| = 1$.

Przykłady i uwagi (informacyjnie)

- Dla ciał kwadratowo domkniętych mamy $|\dot{K}/\dot{K}^2| = 1$.
- Jeśli $0 \neq a \in \mathbb{R}$, to $a \sim 1$ lub $a \sim -1$, czyli $|\dot{\mathbb{R}}/\dot{\mathbb{R}}^2| = 2$.

Przykłady i uwagi (informacyjnie)

- Dla ciał kwadratowo domkniętych mamy $|\dot{K}/\dot{K}^2| = 1$.
- Jeśli $0 \neq a \in \mathbb{R}$, to $a \sim 1$ lub $a \sim -1$, czyli $|\dot{\mathbb{R}}/\dot{\mathbb{R}}^2| = 2$.
- Jeśli $p, q \in \mathbb{Q}$ są liczbami pierwszymi, to $p \sim q \Leftrightarrow p = q$, czyli $|\dot{\mathbb{Q}}/\dot{\mathbb{Q}}^2| = \infty$.

Przykłady i uwagi (informacyjnie)

- Dla ciał kwadratowo domkniętych mamy $|\dot{K}/\dot{K}^2| = 1$.
- Jeśli $0 \neq a \in \mathbb{R}$, to $a \sim 1$ lub $a \sim -1$, czyli $|\dot{\mathbb{R}}/\dot{\mathbb{R}}^2| = 2$.
- Jeśli $p, q \in \mathbb{Q}$ są liczbami pierwszymi, to $p \sim q \Leftrightarrow p = q$, czyli $|\dot{\mathbb{Q}}/\dot{\mathbb{Q}}^2| = \infty$.
- $(*)$ jeśli $|\dot{K}/\dot{K}^2|$ jest skończona, to ma 2^k elementów, dla pewnego k.

Przykłady i uwagi (informacyjnie)

- Dla ciał kwadratowo domkniętych mamy $|\dot{K}/\dot{K}^2| = 1$.
- Jeśli $0 \neq a \in \mathbb{R}$, to $a \sim 1$ lub $a \sim -1$, czyli $|\dot{\mathbb{R}}/\dot{\mathbb{R}}^2| = 2$.
- Jeśli $p, q \in \mathbb{Q}$ są liczbami pierwszymi, to $p \sim q \Leftrightarrow p = q$, czyli $|\dot{\mathbb{Q}}/\dot{\mathbb{Q}}^2| = \infty$.
- $(*)$ jeśli $|\dot{K}/\dot{K}^2|$ jest skończona, to ma 2^k elementów, dla pewnego k.
- $(*)$ Dla każdego ciała skończonego K charakterystyki $\neq 2$ mamy $|\dot{K}/\dot{K}^2| = 2$.

Przykłady i uwagi (informacyjnie)

- Dla ciał kwadratowo domkniętych mamy $|\dot{K}/\dot{K}^2| = 1$.
- Jeśli $0 \neq a \in \mathbb{R}$, to $a \sim 1$ lub $a \sim -1$, czyli $|\dot{\mathbb{R}}/\dot{\mathbb{R}}^2| = 2$.
- Jeśli $p, q \in \mathbb{Q}$ są liczbami pierwszymi, to $p \sim q \Leftrightarrow p = q$, czyli $|\dot{\mathbb{Q}}/\dot{\mathbb{Q}}^2| = \infty$.
- $(*)$ jeśli $|\dot{K}/\dot{K}^2|$ jest skończona, to ma 2^k elementów, dla pewnego k.
- $(*)$ Dla każdego ciała skończonego K charakterystyki $\neq 2$ mamy $|\dot{K}/\dot{K}^2| = 2$.
- $(*)$ Rozważa się tzw. ciała szeregów formalnych (ilorazy szeregów formalnych) o współczynnikach w ciele K, ozn. $K((x))$. Okazuje się, że
$$|K(\dot{(}x))/K(\dot{(}x))^2| = 2 \cdot |\dot{K}/\dot{K}^2|.$$

Przykłady i uwagi (informacyjnie)

- Dla ciał kwadratowo domkniętych mamy $|\dot{K}/\dot{K}^2| = 1$.
- Jeśli $0 \neq a \in \mathbb{R}$, to $a \sim 1$ lub $a \sim -1$, czyli $|\dot{\mathbb{R}}/\dot{\mathbb{R}}^2| = 2$.
- Jeśli $p, q \in \mathbb{Q}$ są liczbami pierwszymi, to $p \sim q \Leftrightarrow p = q$, czyli $|\dot{\mathbb{Q}}/\dot{\mathbb{Q}}^2| = \infty$.
- $(*)$ jeśli $|\dot{K}/\dot{K}^2|$ jest skończona, to ma 2^k elementów, dla pewnego k.
- $(*)$ Dla każdego ciała skończonego K charakterystyki $\neq 2$ mamy $|\dot{K}/\dot{K}^2| = 2$.
- $(*)$ Rozważa się tzw. ciała szeregów formalnych (ilorazy szeregów formalnych) o współczynnikach w ciele K, ozn. $K((x))$. Okazuje się, że

$$|K((\dot{x}))/K((\dot{x}))^2| = 2 \cdot |\dot{K}/\dot{K}^2|.$$

Nasz cel. Klasyfikacja macierzy kongruentnych nad ciałem K dla $|\dot{K}/\dot{K}^2| = 2$.

Problem

Znaleźć warunki konieczne i dostateczne na to, by dla nad ciałem K zachodziła kongruencja macierzy diagonalnych: $\mathtt{diag}(a_1, \ldots, a_n) \cong \mathtt{diag}(b_1, \ldots, b_n)$.

Uwaga. Jeśli $A = \mathtt{diag}(a_1, \ldots, a_r, 0, \ldots, 0) \in M_n(\mathbb{R})$, gdzie $a_i \neq 0$, jest macierzą formy h na V w bazie $(\alpha_1, \ldots, \alpha_n)$, to biorąc bazę $\mathcal{B} = (\beta_1, \ldots \beta_n)$ postaci:

$$\beta_j = \begin{cases} \frac{1}{\sqrt{|a_i|}}\alpha_i, & \text{dla } i \leq r, \\ \alpha_i, & \text{dla } i > r \end{cases}$$

dostajemy: $h(\beta_i, \beta_i) \in \{-1, 0, 1\}$.

Problem

Znaleźć warunki konieczne i dostateczne na to, by dla nad ciałem K zachodziła kongruencja macierzy diagonalnych: $\operatorname{diag}(a_1, \ldots, a_n) \cong \operatorname{diag}(b_1, \ldots, b_n)$.

Uwaga. Jeśli $A = \operatorname{diag}(a_1, \ldots, a_r, 0, \ldots, 0) \in M_n(\mathbb{R})$, gdzie $a_i \neq 0$, jest macierzą formy h na V w bazie $(\alpha_1, \ldots, \alpha_n)$, to biorąc bazę $\mathcal{B} = (\beta_1, \ldots \beta_n)$ postaci:

$$\beta_j = \begin{cases} \frac{1}{\sqrt{|a_i|}}\alpha_i, & \text{dla } i \leq r, \\ \alpha_i, & \text{dla } i > r \end{cases}$$

dostajemy: $h(\beta_i, \beta_i) \in \{-1, 0, 1\}$.

Wniosek

Każda symetryczna macierz o wyrazach w ciele $\mathbb{R}$ jest kongruentna z macierzą diagonalną mającą na przekątnej pewną liczbę elementów $\{-1, 0, 1\}$.

Nasz cel. Twierdzenie Witta o skracaniu

Niech K będzie ciałem charakterystyki $\neq 2$ oraz niech $a_1, \ldots, a_n$, $b_1, \ldots, b_n$, $c_1 \neq 0, \ldots, c_k \neq 0$ będą elementami K. Wtedy z kongruencji (nad K) macierzy

$$\operatorname{diag}(c_1, \ldots, c_k, a_1, \ldots, a_n) \cong \operatorname{diag}(c_1, \ldots, c_k, b_1, \ldots, b_n)$$

wynika kongruencja (nad K) macierzy diagonalnych

$$\operatorname{diag}(a_1, \ldots, a_n) \cong \operatorname{diag}(b_1, \ldots, b_n).$$

Nasz cel. Twierdzenie o bezwładności (inercji)

Niech $A = \operatorname{diag}(a_1, \ldots, a_n)$, $B = \operatorname{diag}(b_1, \ldots, b_n)$, gdzie $a_i, b_j \in \{-1, 0, 1\}$. Wówczas jeśli macierze A, B są kongruentne nad $\mathbb{R}$, to

$$|\{i : a_i = 1\}| = |\{i : b_i = 1\}|, \quad |\{i : a_i = -1\}| = |\{i : b_i = -1\}|.$$

Definicja

Niech h będzie formą dwuliniową na przestrzeni V oraz niech h' będzie formą dwuliniową na izomorficznej z V przestrzeni W. Izomorfizm $i : V \to W$ nazwiemy **izometrią** przestrzeni (V, h) i (W, h'), jeśli dla każdych $x, y \in U$ mamy:

$$h(x, y) = h'(i(x), i(y)).$$

Definicja

Niech h będzie formą dwuliniową na przestrzeni V oraz niech h' będzie formą dwuliniową na izomorficznej z V przestrzeni W. Izomorfizm $i : V \to W$ nazwiemy **izometrią** przestrzeni (V, h) i (W, h'), jeśli dla każdych $x, y \in U$ mamy:

$$h(x, y) = h'(i(x), i(y)).$$

Jeśli istnieje izometria (V, h) i (W, h'), wówczas przestrzenie/formy te nazywamy **izometrycznymi** lub **równoważnymi**, ozn. $(V, h) \cong (W, h')$.

Definicja

Niech h będzie formą dwuliniową na przestrzeni V oraz niech h' będzie formą dwuliniową na izomorficznej z V przestrzeni W. Izomorfizm $i : V \to W$ nazwiemy **izometrią** przestrzeni (V, h) i (W, h'), jeśli dla każdych $x, y \in U$ mamy:

$$h(x, y) = h'(i(x), i(y)).$$

Jeśli istnieje izometria (V, h) i (W, h'), wówczas przestrzenie/formy te nazywamy **izometrycznymi** lub **równoważnymi**, ozn. $(V, h) \cong (W, h')$.

Przykłady:

- id oraz $-$id,
- obrót w $(\mathbb{R}^2, \langle\, ,\, \rangle_{st})$,
- symetria prostopadła (V, h) względem podprzestrzeni nieosobliwej W,
- złożenie dowolnej liczby izometrii.

Definicja

Niech h będzie formą dwuliniową na przestrzeni V oraz niech h' będzie formą dwuliniową na izomorficznej z V przestrzeni W. Izomorfizm $i : V \to W$ nazwiemy **izometrią** przestrzeni (V, h) i (W, h'), jeśli dla każdych $x, y \in U$ mamy:

$$h(x, y) = h'(i(x), i(y)).$$

Jeśli istnieje izometria (V, h) i (W, h'), wówczas przestrzenie/formy te nazywamy **izometrycznymi** lub **równoważnymi**, ozn. $(V, h) \cong (W, h')$.

Idea: izometria dokonuje „transportu” struktury dwuliniowej z V do W.

Fakt - proszę udowodnić samodzielnie!

Niech (V, h) oraz (W, h') będą skończenie wymiarowe i niech $A = G(h, \mathcal{A})$, $B = G(h', \mathcal{B})$, gdzie $\mathcal{A}, \mathcal{B}$ są jakimikolwiek bazami V, W. Wówczas:

$$(V, h) \cong (W, h') \Leftrightarrow A \cong B.$$

Pierwsza wersja twierdzenia Witta o przedłużaniu izometrii

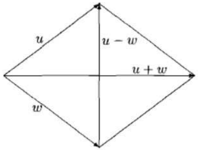
Niech (V, h) będzie przestrzenią dwuliniową nad ciałem charakterystyki $\neq 2$. Jeśli $u, w \in V$ są wektorami nieizotropowymi i $h(u, u) = h(w, w)$, to istnieje taka izometria przestrzeni $i : (V, h) \to (V, h)$, że $i(u) = w$.

Pierwsza wersja twierdzenia Witta o przedłużaniu izometrii

Niech (V, h) będzie przestrzenią dwuliniową nad ciałem charakterystyki $\neq 2$. Jeśli $u, w \in V$ są wektorami nieizotropowymi i $h(u, u) = h(w, w)$, to istnieje taka izometria przestrzeni $i : (V, h) \to (V, h)$, że $i(u) = w$.

Dowód. Gdy $u = w$ teza jest jasna. Niech $u \neq w$.

- Mamy $h(u, u) = h(w, w)$, więc $h(u - w, u + w) = 0$.



Pierwsza wersja twierdzenia Witta o przedłużaniu izometrii

Niech (V, h) będzie przestrzenią dwuliniową nad ciałem charakterystyki $\neq 2$. Jeśli $u, w \in V$ są wektorami nieizotropowymi i $h(u, u) = h(w, w)$, to istnieje taka izometria przestrzeni $i : (V, h) \to (V, h)$, że $i(u) = w$.

Dowód. Gdy $u = w$ teza jest jasna. Niech $u \neq w$.

- Mamy $h(u, u) = h(w, w)$, więc $h(u - w, u + w) = 0$.
- Mamy więc (było) $u = \frac{1}{2}(u - w) + \frac{1}{2}(u + w)$.

Pierwsza wersja twierdzenia Witta o przedłużaniu izometrii

Niech (V, h) będzie przestrzenią dwuliniową nad ciałem charakterystyki $\neq 2$. Jeśli $u, w \in V$ są wektorami nieizotropowymi i $h(u, u) = h(w, w)$, to istnieje taka izometria przestrzeni $i : (V, h) \to (V, h)$, że $i(u) = w$.

Dowód. Gdy $u = w$ teza jest jasna. Niech $u \neq w$.

- Mamy $h(u, u) = h(w, w)$, więc $h(u - w, u + w) = 0$.
- Mamy więc (było) $u = \frac{1}{2}(u - w) + \frac{1}{2}(u + w)$.
- Jeśli $u + w$ jest nieizotropowy, to symetria prostopadła V względem podprzestrzeni nieosobliwej $\mathrm{lin}(u + w)$ przeprowadza $u \mapsto w$.

Pierwsza wersja twierdzenia Witta o przedłużaniu izometrii

Niech (V, h) będzie przestrzenią dwuliniową nad ciałem charakterystyki $\neq 2$. Jeśli $u, w \in V$ są wektorami nieizotropowymi i $h(u, u) = h(w, w)$, to istnieje taka izometria przestrzeni $i : (V, h) \to (V, h)$, że $i(u) = w$.

Dowód. Gdy $u = w$ teza jest jasna. Niech $u \neq w$.

- Mamy $h(u, u) = h(w, w)$, więc $h(u - w, u + w) = 0$.
- Mamy więc (było) $u = \frac{1}{2}(u - w) + \frac{1}{2}(u + w)$.
- Jeśli $u + w$ jest nieizotropowy, to symetria prostopadła V względem podprzestrzeni nieosobliwej $\mathrm{lin}(u + w)$ przeprowadza $u \mapsto w$.
- Jeśli $u - w$ jest nieizotropowy, to symetria prostopadła V względem podprzestrzeni nieosobliwej $\mathrm{lin}(u - w)$ przeprowadza $u \mapsto -w$, a zatem złożenie tej symetrii z $-\mathrm{id}$ to izometria V przeprowadzająca $u \mapsto w$.

Pierwsza wersja twierdzenia Witta o przedłużaniu izometrii

Niech (V, h) będzie przestrzenią dwuliniową nad ciałem charakterystyki $\neq 2$. Jeśli $u, w \in V$ są wektorami nieizotropowymi i $h(u, u) = h(w, w)$, to istnieje taka izometria przestrzeni $i : (V, h) \to (V, h)$, że $i(u) = w$.

Dowód. Gdy $u = w$ teza jest jasna. Niech $u \neq w$.

- Mamy $h(u, u) = h(w, w)$, więc $h(u - w, u + w) = 0$.
- Mamy więc (było) $u = \frac{1}{2}(u - w) + \frac{1}{2}(u + w)$.
- Jeśli $u + w$ jest nieizotropowy, to symetria prostopadła V względem podprzestrzeni nieosobliwej $\mathrm{lin}(u + w)$ przeprowadza $u \mapsto w$.
- Jeśli $u - w$ jest nieizotropowy, to symetria prostopadła V względem podprzestrzeni nieosobliwej $\mathrm{lin}(u - w)$ przeprowadza $u \mapsto -w$, a zatem złożenie tej symetrii z $-\mathrm{id}$ to izometria V przeprowadzająca $u \mapsto w$.
- Skoro u, w są nieizotropowe, to jeden z wektorów $u - w$ lub $u + w$ też, bo:

$$h(u - w, u - w) + h(u + w, u + w) = 2h(u, u) + 2h(w, w) = 4h(u, u) \neq 0.$$

Dowód twierdzenia Witta o skracaniu.

- Zacznijmy od dowodu poniższej implikacji (dla $c \neq 0$):

$$\operatorname{diag}(c, a_1, \dots, a_n) \cong \operatorname{diag}(c, b_1, \dots, b_n) \Rightarrow \operatorname{diag}(a_1, \dots, a_n) \cong \operatorname{diag}(b_1, \dots, b_n).$$

Dowód twierdzenia Witta o skracaniu.

- Zacznijmy od dowodu poniższej implikacji (dla $c \neq 0$):

$$\mathrm{diag}(c, a_1, \ldots, a_n) \cong \mathrm{diag}(c, b_1, \ldots, b_n) \Rightarrow \mathrm{diag}(a_1, \ldots, a_n) \cong \mathrm{diag}(b_1, \ldots, b_n).$$

- Lewa strona powyższej implikacji oznacza, że na K^{n+1} istnieje forma dwuliniowa h oraz bazy ortogonalne $\mathcal{A} = \{\alpha, \alpha_1, \ldots, \alpha_n\}$, $\mathcal{B} = \{\beta, \beta_1, \ldots, \beta_n\}$ takie, że $G(h, \mathcal{A}) = \mathrm{diag}(c, a_1, \ldots, a_n)$, $G(h, \mathcal{B}) = \mathrm{diag}(c, b_1, \ldots, b_n)$.

Dowód twierdzenia Witta o skracaniu.

- Zacznijmy od dowodu poniższej implikacji (dla $c \neq 0$):

$$\mathrm{diag}(c, a_1, \ldots, a_n) \cong \mathrm{diag}(c, b_1, \ldots, b_n) \Rightarrow \mathrm{diag}(a_1, \ldots, a_n) \cong \mathrm{diag}(b_1, \ldots, b_n).$$

- Lewa strona powyższej implikacji oznacza, że na K^{n+1} istnieje forma dwuliniowa h oraz bazy ortogonalne $\mathcal{A} = \{\alpha, \alpha_1, \ldots, \alpha_n\}$, $\mathcal{B} = \{\beta, \beta_1, \ldots, \beta_n\}$ takie, że $G(h, \mathcal{A}) = \mathrm{diag}(c, a_1, \ldots, a_n)$, $G(h, \mathcal{B}) = \mathrm{diag}(c, b_1, \ldots, b_n)$.
- W szczególności $h(\alpha, \alpha) = h(\beta, \beta) = c \neq 0$, czyli z twierdzenie o przedłużaniu izometrii istnieje izometria $i : (K^{n+1}, h) \to (K^{n+1}, h)$, że $i(\alpha) = \beta$.

Dowód twierdzenia Witta o skracaniu.

- Zacznijmy od dowodu poniższej implikacji (dla $c \neq 0$):

$$\operatorname{diag}(c, a_1, \ldots, a_n) \cong \operatorname{diag}(c, b_1, \ldots, b_n) \Rightarrow \operatorname{diag}(a_1, \ldots, a_n) \cong \operatorname{diag}(b_1, \ldots, b_n).$$

- Lewa strona powyższej implikacji oznacza, że na K^{n+1} istnieje forma dwuliniowa h oraz bazy ortogonalne $\mathcal{A} = \{\alpha, \alpha_1, \ldots, \alpha_n\}$, $\mathcal{B} = \{\beta, \beta_1, \ldots, \beta_n\}$ takie, że $G(h, \mathcal{A}) = \operatorname{diag}(c, a_1, \ldots, a_n)$, $G(h, \mathcal{B}) = \operatorname{diag}(c, b_1, \ldots, b_n)$.
- W szczególności $h(\alpha, \alpha) = h(\beta, \beta) = c \neq 0$, czyli z twierdzenie o przedłużaniu izometrii istnieje izometria $i : (K^{n+1}, h) \to (K^{n+1}, h)$, że $i(\alpha) = \beta$.
- Ponieważ i zachowuje prostopadłość wektorów, mamy $i(\operatorname{lin}(\alpha)^{\perp}) = \operatorname{lin}(\beta)^{\perp}$. Zatem $i|_{\operatorname{lin}(\alpha)^{\perp}}$ jest izometrią.

Dowód twierdzenia Witta o skracaniu.

- Zacznijmy od dowodu poniższej implikacji (dla $c \neq 0$):

$$\mathrm{diag}(c, a_1, \ldots, a_n) \cong \mathrm{diag}(c, b_1, \ldots, b_n) \Rightarrow \mathrm{diag}(a_1, \ldots, a_n) \cong \mathrm{diag}(b_1, \ldots, b_n).$$

- Lewa strona powyższej implikacji oznacza, że na K^{n+1} istnieje forma dwuliniowa h oraz bazy ortogonalne $\mathcal{A} = \{\alpha, \alpha_1, \ldots, \alpha_n\}$, $\mathcal{B} = \{\beta, \beta_1, \ldots, \beta_n\}$ takie, że $G(h, \mathcal{A}) = \mathrm{diag}(c, a_1, \ldots, a_n)$, $G(h, \mathcal{B}) = \mathrm{diag}(c, b_1, \ldots, b_n)$.
- W szczególności $h(\alpha, \alpha) = h(\beta, \beta) = c \neq 0$, czyli z twierdzenie o przedłużaniu izometrii istnieje izometria $i : (K^{n+1}, h) \to (K^{n+1}, h)$, że $i(\alpha) = \beta$.
- Ponieważ i zachowuje prostopadłość wektorów, mamy $i(\mathrm{lin}(\alpha)^\perp) = \mathrm{lin}(\beta)^\perp$. Zatem $i|_{\mathrm{lin}(\alpha)^\perp}$ jest izometrią.
- Z drugiej strony $\mathrm{lin}(\alpha)^\perp = \mathrm{lin}(\alpha_1, \ldots, \alpha_n), \mathrm{lin}(\beta)^\perp = \mathrm{lin}(\beta_1, \ldots, \beta_n)$. A zatem mamy bazy prostopadłe izometrycznych przestrzeni, w których odpowiednio obcięte h mają macierze $\mathrm{diag}(a_1, \ldots, a_n) \cong \mathrm{diag}(b_1, \ldots, b_n)$. Dalej indukcja...

Twierdzenie Witta o przedłużaniu izometrii

Niech (V, h) będzie przestrzenią dwuliniową nad ciałem charakterystyki $\neq 2$. Jeśli $U, W \subseteq V$ są nieosobliwymi podprzestrzeniami przestrzeni V oraz jeśli $i_0 : U \to W$ jest izometrią, to istnieje przedłużenie izometrii i_0 do izometrii i na V, tzn. $i|_U \equiv i_0$.

Dowód - ćwiczenie.

Twierdzenie Witta o przedłużaniu izometrii

Niech (V, h) będzie przestrzenią dwuliniową nad ciałem charakterystyki $\neq 2$. Jeśli $U, W \subseteq V$ są nieosobliwymi podprzestrzeniami przestrzeni V oraz jeśli $i_0 : U \to W$ jest izometrią, to istnieje przedłużenie izometrii i_0 do izometrii i na V, tzn. $i|_U \equiv i_0$.

Dowód - ćwiczenie.

Twierdzenia o przedłużaniu rozmaitych przekształceń mają bardzo ważne miejsce w matematyce. Przykłady (będą na dalszych latach).

- (topologia) lemat Tietzego o przedłużaniu przekształcenia ciągłego z podzbioru domkniętego przestrzeni metrycznej,
- (analiza funkcjonalna) twierdzenie Hahna-Banacha o przedłużaniu funkcjonałów ograniczonych na przestrzeni unormowanej,
- (analiza wielowymiarowa) twierdzenie Whitneya (mniej więcej) o przedłużaniu funkcji na zbiorze domkniętym tak, by miała ona z góry zadane pochodne,
- (teoria miary) twierdzenie Carathéodory'ego o konstrukcji miary itd.

Dowód twierdzenia o bezwładności (wersja rzeczywista).

- Niech $A = \mathrm{diag}(a_1, \ldots, a_n)$, $B = \mathrm{diag}(b_1, \ldots, b_n)$ będą kongruentnymi macierzami diagonalnymi nad $\mathbb{R}$. Możemy założyć, że $a_i, b_j \in \{-1, 1\}$.

Dowód twierdzenia o bezwładności (wersja rzeczywista).

- Niech $A = \mathrm{diag}(a_1, \dots, a_n)$, $B = \mathrm{diag}(b_1, \dots, b_n)$ będą kongruentnymi macierzami diagonalnymi nad $\mathbb{R}$. Możemy założyć, że $a_i, b_j \in \{-1, 1\}$.
- Zgodnie z Trywialną Uwagą 1 możemy zakładać, ze jeśli $a_i = 1$ oraz $a_j = -1$, to $i < j$, podobnie dla macierzy B.

Dowód twierdzenia o bezwładności (wersja rzeczywista).

- Niech $A = \mathrm{diag}(a_1, \ldots, a_n)$, $B = \mathrm{diag}(b_1, \ldots, b_n)$ będą kongruentnymi macierzami diagonalnymi nad $\mathbb{R}$. Możemy założyć, że $a_i, b_j \in \{-1, 1\}$.
- Zgodnie z Trywialną Uwagą 1 możemy zakładać, ze jeśli $a_i = 1$ oraz $a_j = -1$, to $i < j$, podobnie dla macierzy B.
- Jeśli $|\{i : a_i = 1\}| \neq 0$, to również $|\{i : b_i = 1\}| \neq 0$. W przeciwnym razie z postaci macierzy B wynika, że $h(u, u) < 0$, dla dowolnego $u \in \mathbb{R}^n$, gdzie $A = G(h, st)$, co prowadzi do sprzeczności.

Dowód twierdzenia o bezwładności (wersja rzeczywista).

- Niech $A = \mathrm{diag}(a_1, \dots, a_n)$, $B = \mathrm{diag}(b_1, \dots, b_n)$ będą kongruentnymi macierzami diagonalnymi nad $\mathbb{R}$. Możemy założyć, że $a_i, b_j \in \{-1, 1\}$.
- Zgodnie z Trywialną Uwagą 1 możemy zakładać, ze jeśli $a_i = 1$ oraz $a_j = -1$, to $i < j$, podobnie dla macierzy B.
- Jeśli $|\{i : a_i = 1\}| \neq 0$, to również $|\{i : b_i = 1\}| \neq 0$. W przeciwnym razie z postaci macierzy B wynika, że $h(u, u) < 0$, dla dowolnego $u \in \mathbb{R}^n$, gdzie $A = G(h, st)$, co prowadzi do sprzeczności.
- Jeśli $|\{i : a_i = 1\}| > |\{i : b_i = 1\}| > 0$, to na mocy twierdzenia Witta o skracaniu istnieją s, r takie, że:

$$\mathrm{diag}(\underbrace{1, \dots, 1}_{s}, \underbrace{-1, \dots, -1}_{r}) \cong \mathrm{diag}(\underbrace{-1, \dots, -1}_{s+r}),$$

co prowadzi do sprzeczności, jak wyżej.

Dowód twierdzenia o bezwładności (wersja rzeczywista).

- Niech $A = \mathrm{diag}(a_1, \ldots, a_n)$, $B = \mathrm{diag}(b_1, \ldots, b_n)$ będą kongruentnymi macierzami diagonalnymi nad $\mathbb{R}$. Możemy założyć, że $a_i, b_j \in \{-1, 1\}$.
- Zgodnie z Trywialną Uwagą 1 możemy zakładać, ze jeśli $a_i = 1$ oraz $a_j = -1$, to $i < j$, podobnie dla macierzy B.
- Jeśli $|\{i : a_i = 1\}| \neq 0$, to również $|\{i : b_i = 1\}| \neq 0$. W przeciwnym razie z postaci macierzy B wynika, że $h(u, u) < 0$, dla dowolnego $u \in \mathbb{R}^n$, gdzie $A = G(h, st)$, co prowadzi do sprzeczności.
- Jeśli $|\{i : a_i = 1\}| > |\{i : b_i = 1\}| > 0$, to na mocy twierdzenia Witta o skracaniu istnieją s, r takie, że:

$$\mathrm{diag}(\underbrace{1, \ldots, 1}_{s}, \underbrace{-1, \ldots, -1}_{r}) \cong \mathrm{diag}(\underbrace{-1, \ldots, -1}_{s+r}),$$

  co prowadzi do sprzeczności, jak wyżej.
- Stąd $|\{i : a_i = 1\}| = |\{i : b_i = 1\}|$ oraz $|\{i : a_i = -1\}| = |\{i : b_i = -1\}|$.

Definicja

Niech (V, h) będzie przestrzenią dwuliniową nad ciałem $\mathbb{R}$. **Sygnaturą przestrzeni** (V, h) (albo formy dwuliniowej h) nazywamy liczbę

$$\underbrace{|\{i : a_i = 1\}|}_{r^+(h)} - \underbrace{|\{i : a_i = -1\}|}_{r^-(h)},$$

gdzie $\mathrm{diag}(a_1, \ldots, a_n)$ jest macierzą h. Sygnaturę oznaczamy $s(V, h)$ lub $s(h)$.

Sygnaturą macierzy symetrycznej $A \in M_n(\mathbb{R})$ nazywamy sygnaturę formy dwuliniowej $h : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ zadanej warunkiem $G(h; st) = A$. Sygnaturę macierzy A oznaczamy $s(A)$. Więc $s(A)$ to liczba dodatnich – liczba ujemnych wyrazów na przekątnej w macierzy diagonalnej kongruentnej do macierzy A.

Definicja

Niech (V, h) będzie przestrzenią dwuliniową nad ciałem $\mathbb{R}$. **Sygnaturą przestrzeni** (V, h) (albo formy dwuliniowej h) nazywamy liczbę

$$\underbrace{|\{i : a_i = 1\}|}_{r^+(h)} - \underbrace{|\{i : a_i = -1\}|}_{r^-(h)},$$

gdzie $\mathrm{diag}(a_1, \ldots, a_n)$ jest macierzą h. Sygnaturę oznaczamy $s(V, h)$ lub $s(h)$.

Sygnaturą macierzy symetrycznej $A \in M_n(\mathbb{R})$ nazywamy sygnaturę formy dwuliniowej $h : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ zadanej warunkiem $G(h; st) = A$. Sygnaturę macierzy A oznaczamy $s(A)$. Więc $s(A)$ to liczba dodatnich – liczba ujemnych wyrazów na przekątnej w macierzy diagonalnej kongruentnej do macierzy A.

Wniosek

Niech $A, B \in M_n(\mathbb{R})$ będą symetryczne. Wówczas $A \cong B$ wtedy i tylko wtedy, gdy $r(A) = r(B)$ oraz $s(A) = s(B)$.

Definicja

Ciało K nazywa się:

- **formalnie rzeczywistym**, jeśli element $-1 \in K$ nie jest sumą kwadratów elementów ciała K,
- **nierzeczywistym**, jeśli K nie jest formalnie rzeczywiste,
- **uporządkowanym**, jeśli na K jest określona relacja $>$, zwana porządkiem, o następujących własnościach, dla każdych $a, b, c \in K$:
  - przechodniość:
    $$a > b \text{ i } b > c \Rightarrow a > c,$$
  - trychotomia
    $$a > b \text{ albo } a = b \text{ albo } b > a,$$
  - zgodność z dodawaniem i mnożeniem:
    $$a > b \Rightarrow a + c > b + c, \qquad a > b \text{ i } c > 0 \Rightarrow ac > bc.$$

Przykłady i uwagi (są to w zasadzie niezbyt trudne ćwiczenia)

- Każde ciało charakterystyki $p \neq 0$ jest nierzeczywiste, bo $-1 = (p-1) \cdot 1^2$.

Przykłady i uwagi (są to w zasadzie niezbyt trudne ćwiczenia)

- Każde ciało charakterystyki $p \neq 0$ jest nierzeczywiste, bo $-1 = (p-1) \cdot 1^2$.
- Każde ciało kwadratowo domknięte jest nierzeczywiste.

Przykłady i uwagi (są to w zasadzie niezbyt trudne ćwiczenia)

- Każde ciało charakterystyki $p \neq 0$ jest nierzeczywiste, bo $-1 = (p-1) \cdot 1^2$.
- Każde ciało kwadratowo domknięte jest nierzeczywiste.
- Jeśli K jest ciałem formalnie rzeczywistym i $|\dot{K}/\dot{K}^2| = 2$, to relacja
$$a > b \Leftrightarrow a - b \in \dot{K}^2$$
zadaje na K strukturę ciała uporządkowanego. Elementy $a > 0$ nazywamy dodatnimi (w porządku $>$), zaś elementy $a < 0$ nazywamy ujemnymi.

Przykłady i uwagi (są to w zasadzie niezbyt trudne ćwiczenia)

- Każde ciało charakterystyki $p \neq 0$ jest nierzeczywiste, bo $-1 = (p-1) \cdot 1^2$.
- Każde ciało kwadratowo domknięte jest nierzeczywiste.
- Jeśli K jest ciałem formalnie rzeczywistym i $|\dot{K}/\dot{K}^2| = 2$, to relacja
$$a > b \Leftrightarrow a - b \in \dot{K}^2$$
zadaje na K strukturę ciała uporządkowanego. Elementy $a > 0$ nazywamy dodatnimi (w porządku $>$), zaś elementy $a < 0$ nazywamy ujemnymi.
- $(*)$ Jeśli K jest ciałem formalnie rzeczywistym i $|\dot{K}/\dot{K}^2| = 2$, to dla macierzy symetrycznych nad tym ciałem zachodzi twierdzenie o bezwładności.

Przykłady i uwagi (są to w zasadzie niezbyt trudne ćwiczenia)

- Każde ciało charakterystyki $p \neq 0$ jest nierzeczywiste, bo $-1 = (p-1) \cdot 1^2$.
- Każde ciało kwadratowo domknięte jest nierzeczywiste.
- Jeśli K jest ciałem formalnie rzeczywistym i $|\dot{K}/\dot{K}^2| = 2$, to relacja
$$a > b \Leftrightarrow a - b \in \dot{K}^2$$
zadaje na K strukturę ciała uporządkowanego. Elementy $a > 0$ nazywamy dodatnimi (w porządku $>$), zaś elementy $a < 0$ nazywamy ujemnymi.
- $(*)$ Jeśli K jest ciałem formalnie rzeczywistym i $|\dot{K}/\dot{K}^2| = 2$, to dla macierzy symetrycznych nad tym ciałem zachodzi twierdzenie o bezwładności.
- $(*)$ Jeśli K jest ciałem nierzeczywistym o charakterystyce $\neq 2$ oraz $|\dot{K}/\dot{K}^2| = 2$ (np. ciało skończone charakterystyki $\neq 2$), to macierze symetryczne nad K są kongruentne wtedy i tylko wtedy, gdy ich rzędy oraz tzw. wyróżniki (wyznaczniki modulo kwadrat z ciała K) są równe.