Przekształcenia samosprzężone i twierdzenie spektralne

Wśród przekształceń liniowych przestrzeni euklidesowych szczególnie interesujące są te, które zachowują pewien element struktury euklidesowej. Obok warunku zachowywania iloczynu skalarnego jest wiele innych możliwych warunków, które nakładać można na endomorfizmy przestrzeni (nie tylko) euklidesowych, aby uzyskiwać inne ważne wyniki strukturalne. Dziś powiemy o warunku, który wysłowić można w języku funkcjonałów liniowych.

Zainteresowanych odsyłam do: http://www.math.us.edu.pl/zatl/szymiczek/referaty/AlgebraLiniowa4.pdf.

Fakt 128. *Niech $(V, \langle , \rangle)$ będzie liniową przestrzenią euklidesową wymiaru n. Każdemu wektorowi $v \in V$ przyporządkowujemy funkcjonał $f_v \in V^*$ określony wzorem:*

$$f_v(u) = \langle u, v \rangle, \text{ gdzie } u \in V.$$

Przyporządkowanie $\Phi : V \to V^*$ zadane wzorem

$$\Phi(v) = f_v$$

jest izomorfizmem przestrzeni liniowych. Jeśli $\mathcal{V} = (v_1, \ldots, v_n)$ jest bazą ortonormalną w V, to układ $(f_{v_1}, \ldots, f_{v_n})$ jest dualną do $\mathcal{V}$ bazą V^*.

Dowód. Przekształcenie f_v jest liniowe dla każdego $v \in V$, bo

$$f_v(au) = \langle au, v \rangle = a\langle u, v \rangle = a \cdot f_v(u)$$
$$f_v(u_1 + u_2) = \langle u_1 + u_2, v \rangle = \langle u_1, v \rangle + \langle u_2, v \rangle = f_v(u_1) + f_v(u_2)$$

A zatem rzeczywiście $f_v \in V^*$. Także przyporządkowanie Φ jest liniowe, ponieważ $f_{av}(u) = \langle u, av \rangle = a\langle u, v \rangle = a \cdot f_v(u)$, czyli funkcjonały $\Phi(av)$ oraz $a \cdot \Phi(v)$ są identyczne na V. Także

$$f_{v_1+v_2}(u) = \langle u, v_1 + v_2 \rangle = \langle u, v_1 \rangle + \langle u, v_2 \rangle = f_{v_1}(u) + f_{v_2}(u),$$

czyli funkcjonały $\Phi(v_1 + v_2)$ oraz $\Phi(v_1) + \Phi(v_2)$ są równe. Skoro V oraz V^* są tego samego wymiaru to do wykazania, że Φ jest izomorfizmem wystarczy pokazać, że Φ to monomorfizm. Jeśli mamy $\Phi(v) = 0$, to f_v jest tożsamościowo równe 0. W szczególności $f_v(v) = \langle v, v \rangle = 0$. Zatem $v = 0$. Czyli Φ jest izomorfizmem. Ostatnie stwierdzenie dotyczące baz dualnych jest oczywiste. □

Jaka jest zaleta tego rezultatu? Pozwala on na utożsamianie endomorfizmów V oraz V^*. A zatem: bierzemy taki funkcjonał f_v, wykonujemy na nim ϕ^* i dostajemy znowu funkcjonał z V^*, czyli pewien funkcjonał $f_{v'}$ (bo tak nakazuje Φ). Co mają ze sobą wspólnego v oraz v'? Musimy mieć $\phi^*(f_v) = f_{v'}$, czyli dla każdego $u \in V$ mamy $\phi^*(f_v)(u) = f_v(\phi(u)) = f_{v'}(u)$. A zatem z definicji funkcjonałów f_v oraz $f_{v'}$ mamy:

$$\langle \phi(u), v\rangle = \langle u, v'\rangle.$$

Endomorfizm przestrzeni euklidesowej V przypisujący wektorowi v wektor v' tak, że spełniona jest powyższa równość nazywamy ENDOMORFIZMEM SPRZĘŻONYM do ϕ ze względu na iloczyn skalarny $\langle , \rangle$. Zwyczajowo ten endomorfizm również oznacza się przez ϕ^*, mimo, że jest to (teraz) endomorfizm V. Mamy więc:

$$\langle \phi(u), v\rangle = \langle u, \phi^*(v)\rangle.$$

Czy rozważania te mają jakiś praktyczny skutek? Chodzi tu o to, że spojrzenie na endomorfizmy V jako na pochodzące od endomorfizmów V^* pozwala na wyróżnienie dodatkowych klas endomorfizmów.

Proszę zauważyć, że przyjmując w powyższej równości ϕ^* jako ϕ^{-1} dostajemy dokładnie definicję izometrii. Istotnie, skoro $\langle \phi(u), v\rangle = \langle u, \phi^{-1}(v)\rangle$, to dla $v = \phi(u)$ mamy:

$$\langle \phi(u), \phi(u)\rangle = \langle u, \phi^{-1}(\phi(u))\rangle = \langle u, u\rangle.$$

A zatem ϕ zachowuję normę i jest izomorfizmem (bo istnieje ϕ^{-1}), czyli to izometria. Krótko mówiąc, izometrie to takie przekształcenia, że sprzężone do nich to ich odwrotności. Nie powinno nas to dziwić. Pamiętamy przecież, że macierz przekształcenia sprzężonego w bazach sprzężonych to macierz transponowana. Z drugiej strony macierz M izometrii w bazach ortonormalnych jest ortogonalna, czyli spełnia $M^{-1} = M^T$. Widać jak te rezultaty się ładnie łączą?

Oczywiście jest mnóstwo endomorfizmów ϕ przestrzeni euklidesowych, które nie muszą spełniać $\phi^{-1} = \phi^*$, czyli nie są izometriami. Dziś rozważać będziemy jedną z najważniejszych takich klas, czyli endomorfizmy samosprzężone. Spełniają one warunek postaci $\phi^* = \phi$. Proszę zauważyć, że w języku macierzowym oznacza to, że macierz takiego przekształcenia spełnia $M^T = M$, czyli jest symetryczna (pokażemy to). Macierze izometrii symetryczne być nie muszą.

Definicja 88. *Niech $(V, \langle , \rangle)$ będzie przestrzenią euklidesową liniową. Mówimy, że przekształcenie liniowe $\phi : V \to V$ jest* SAMOSPRZĘŻONE, *jeśli dla każdych $\alpha, \beta \in V$ zachodzi:*

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

Fakt 129. *Niech ϕ będzie endomorfizmem przestrzeni euklidesowej liniowej $(V, \langle , \rangle)$ Dla dowolnej bazy $\mathcal{A} = (\alpha_1, \ldots, \alpha_n)$ następujące warunki są równoważne:*

- *ϕ jest samosprzężone,*
- *dla każdych $1 \leq i, j \leq n$ mamy $\langle \alpha_i, \phi(\alpha_j)\rangle = \langle \phi(\alpha_i), \alpha_j\rangle$.*

Dowód. Jeśli ϕ jest samosprzężone, to oczywiście $\langle \alpha_i, \phi(\alpha_j)\rangle = \langle \phi(\alpha_i), \alpha_j\rangle$, dla każdych i, j. Odwrotnie, jeśli $\langle \alpha_i, \phi(\alpha_j)\rangle = \langle \phi(\alpha_i), \alpha_j\rangle$, dla każdych i, j, to dla każdych wektorów $\alpha = x_1\alpha_1 + \ldots + x_n\alpha_n$ oraz $\beta = y_1\alpha_1 + \ldots + y_n\alpha_n$ mamy:

$$\begin{aligned}
\langle \alpha, \phi(\beta)\rangle &= \langle x_1\alpha_1 + \ldots + x_n\alpha_n, \phi(y_1\alpha_1 + \ldots + y_n\alpha_n)\rangle = \\
&= \langle x_1\alpha_1 + \ldots + x_n\alpha_n, y_1\phi(\alpha_1) + \ldots + y_n\phi(\alpha_n)\rangle = \\
&= \sum_{i,j=1}^{n} x_i y_j \langle \alpha_i, \phi(\alpha_j)\rangle = \\
&= \sum_{i,j=1}^{n} x_i y_j \langle \phi(\alpha_i), \alpha_j\rangle = \\
&= \langle x_1\phi(\alpha_1) + \ldots + x_n\phi(\alpha_n), y_1\alpha_1 + \ldots + y_n\alpha_n\rangle = \\
&= \langle \phi(x_1\alpha_1 + \ldots + x_n\alpha_n), y_1\alpha_1 + \ldots + y_n\alpha_n\rangle = \\
&= \langle \phi(\alpha), \beta\rangle.
\end{aligned}$$

□

Fakt 130. *Niech ϕ będzie endomorfizmem przestrzeni euklidesowej liniowej $(V, \langle , \rangle)$ Jeśli $\mathcal{A}$ jest ortonormalna, to następujące warunki są równoważne:*

- *$\phi : V \to V$ jest samosprzężone,*
- *$M(\phi)^{\mathcal{A}}_{\mathcal{A}}$ jest macierzą symetryczną.*

Dowód. Niech $M(\phi)^{\mathcal{A}}_{\mathcal{A}} = [a_{ij}]$. Dla każdych $i, j = 1, \ldots, n$ element a_{ij} jest i-tą współrzędną wektora $\phi(\alpha_j)$ w bazie ortonormalnej $\mathcal{A}$, czyli ma postać $a_{ij} = \langle \alpha_i, \phi(\alpha_j)\rangle$. W takim razie korzystając z samosprzężoności ϕ i z symetryczności iloczynu skalarnego mamy:

$$a_{ji} = \langle \alpha_j, \phi(\alpha_i)\rangle = \langle \phi(\alpha_j), \alpha_i\rangle = \langle \alpha_i, \phi(\alpha_j)\rangle = a_{ij}.$$

□

Izometrie zachowywały iloczyn skalarny. Przekształcenia samosprzężone zachowują się dobrze ze względu na podprzestrzenie własne i ogólniej – przestrzenie niezmiennicze. Jak się przekonamy, są to w istocie endomorfizmy diagonalizowalne nad $\mathbb{R}$, a baza złożona z wektorów własnych jest ortogonalna. Przygotujemy teraz szereg obserwacji zmierzających do wykazania tego bardzo ważnego rezultatu.

Fakt 131. *Niech ϕ będzie endomorfizmem samosprzężonym przestrzeni $(V, \langle , \rangle)$ i niech $W \subseteq V$ będzie podprzestrzenią ϕ-niezmienniczą, czyli $\phi(W) \subseteq W$. Wówczas $W^\perp$ również jest ϕ-niezmiennicza, czyli $\phi(W^\perp) \subseteq W^\perp$. W szczególności, jeśli $\alpha \in V$ jest wektorem własnym ϕ, to $\phi(\mathrm{lin}(\alpha)^\perp) \subseteq \mathrm{lin}(\alpha)^\perp$.*

Dowód. Niech W będzie ϕ-niezmiennicza i niech $v \in W^\perp$. Wówczas dla dowolnego $w \in W$ mamy

$$0 = \langle v, \phi(w) \rangle = \langle \phi(v), w \rangle,$$

czyli także $\phi(v) \in W^\perp$. □

Fakt 132. *Jeśli α, β są wektorami własnymi przekształcenia samosprzężonego ϕ o różnych wartościach własnych, to $\alpha \perp \beta$.*

Dowód. Niech $\phi(\alpha) = a\alpha$ oraz $\phi(\beta) = b\beta$, dla pewnych $a \neq b$. Wówczas:

$$a\langle \alpha, \beta \rangle = \langle a\alpha, \beta \rangle = \langle \phi(\alpha), \beta \rangle = \langle \alpha, \phi(\beta) \rangle = \langle \alpha, b\beta \rangle = b\langle \alpha, \beta \rangle.$$

Stąd $(a - b)\langle \alpha, \beta \rangle = 0$, czyli $\langle \alpha, \beta \rangle = 0$. □

Podstawową przeszkodą na drodze do ewentualnej diagonalizowalności endomorfizmu przestrzeni rzeczywistej może być brak rzeczywistych wartości własnych (są i inne potencjalne problemy, jak pamiętamy). W przypadku izometrii nietrudno wskazać przykłady obrotów, które nie mają wartości własnych. Wielomian charakterystyczny endomorfizmu nad $\mathbb{R}$ może nie mieć rzeczywistych pierwiastków. Co więcej, do diagonalizowalności nad ciałem $\mathbb{R}$ potrzeba, by wszystkie wartości własne były rzeczywiste (bo suma wymiarów podprzestrzeni własnych $\leq$ suma krotności algebraicznych wartości własnych $\leq$ wymiar, a diagonalizowalność wymaga równości tych wielkości). Okazuje się, że tak właśnie jest w przypadku endomorfizmów samosprzężonych. Zajmijmy się wartościami własnymi macierzy symetrycznej nad $\mathbb{R}$.

Fakt 133. *Niech $A \in M_n(\mathbb{R})$ będzie macierzą symetryczną. Wówczas wielomian charakterystyczny macierzy A rozkłada się nad ciałem $\mathbb{R}$ na iloczyn czynników stopnia 1. Innymi słowy, wielomian ten ma n rzeczywistych pierwiastków.*

Dowód. Traktujemy macierz A jako macierz z przestrzeni $M_n(\mathbb{C})$. Jak to rozumieć? Każdy wyraz a_{ij} tej macierzy jest postaci $x_{ij} + i \cdot y_{ij}$, przy czym wszystkie y_{ij} równe są 0 (bo wyrazy macierzy są w istocie rzeczywiste). Niech $z \in \mathbb{C}^n$ będzie wektorem własnym macierzy A o wartości własnej $c \in \mathbb{C}$. Zatem:

$$A \cdot \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} = \begin{bmatrix} a_{11}z_1 + \ldots + a_{1n}z_n \\ \vdots \\ a_{n1}z_1 + \ldots + a_{nn}z_n \end{bmatrix} = c \cdot \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix},$$

czyli dla $i = 1, 2, \ldots, n$ mamy:

$$a_{i1}z_1 + \ldots + a_{in}z_n = cz_i.$$

Mnożymy i-tą równość (wypisaną wyżej) przez $\overline{z_i}$ i otrzymujemy równości:

$$a_{i1}z_1\overline{z_i} + \ldots + a_{in}z_n\overline{z_i} = cz_i\overline{z_i} = c|z_i|^2.$$

Dodajemy teraz do siebie wszystkie te równości, dla $i = 1, \ldots, n$. Mamy wówczas:

$$\sum_{i,j=1}^{n} a_{ij}z_j\overline{z_i} = c(|z_1|^2 + \ldots + |z_n|^2).$$

Lewą stronę uzyskanej równości przepisać możemy korzystając z założenia $a_{ij} = a_{ij}$ do sumy postaci:

$$a_{11}|z_1|^2 + \ldots + a_{nn}|z_n|^2 + \sum_{i<j} a_{ij}(z_j\overline{z_i} + z_i\overline{z_j}).$$

Występujące w tej sumie wyrażenia $z_j\overline{z_i} + z_i\overline{z_j}$ są liczbami rzeczywistymi, bo są sumami liczb zespolonych i ich sprzężeń. Pozostałe składniki wypisanej sumy też są rzeczywiste, a zatem cała suma jest liczbą rzeczywistą. W szczególności także prawa strona równości, czyli $c(|z_1|^2 + \ldots + |z_n|^2)$ jest liczbą rzeczywistą. Wiemy jednak, że wyrażenie w nawiasie jest liczbą rzeczywistą, a wiec także $c \in \mathbb{R}$.

Nawet fakt, że endomorfizm ma wielomian charakterystyczny rozkładający się na czynniki liniowe nie gwarantuje jeszcze diagonalizowalności, w przypadku gdy wartości własne są wielokrotnymi jego pierwiastkami. W przypadku endomorfizmów samosprzężonych problem ten nie występuje, jak pokazuje poniższe twierdzenie.

Fakt 134 (Twierdzenie spektralne, wersja rzeczywista)**.** *Niech $(V, \langle , \rangle)$ będzie przestrzenią euklidesową liniową i niech $\phi : V \to V$ będzie przekształceniem samosprzężonym. Wówczas istnieje baza ortonormalna przestrzeni $(V, \langle , \rangle)$ złożona z wektorów własnych endomorfizmu ϕ.*

Zobaczmy przykład. Rozważmy przekształcenie samosprzężone $\phi \in \mathrm{End}(\mathbb{R}^3)$, którego macierz w bazach standardowych ma postać:

$$M(\phi)^{st}_{st} = \begin{bmatrix} 14 & -13 & 8 \\ -13 & 14 & 8 \\ 8 & 8 & -7 \end{bmatrix}.$$

Wówczas poniższa baza $\mathcal{A}$ przestrzeni $\mathbb{R}^3$ jest ortonormalna

$$\frac{1}{\sqrt{2}}(1, -1, 0), \quad \frac{1}{\sqrt{3}}(1, 1, 1), \quad \frac{1}{\sqrt{6}}(1, 1, -2)$$

i

$$M(\phi)^{\mathcal{A}}_{\mathcal{A}} = \begin{bmatrix} 27 & 0 & 0 \\ 0 & 9 & 0 \\ 0 & 0 & -15 \end{bmatrix}.$$

Dowód. Dowód jest indukcją po $n = \dim V$. Dla $n = 1$ twierdzenie jest oczywiste. Załóżmy jego prawdziwość dla $n-1$. Niech $\dim V = n$. Niech $\mathcal{B}$ będzie bazą ortonormalną $(V, \langle , \rangle)$. Wiemy, że $M(\phi)^{\mathcal{B}}_{\mathcal{B}}$ jest macierzą symetryczną o wyrazach rzeczywistych, a więc na mocy ostatniej uwagi ma ona rzeczywistą wartość własną c. Niech $\alpha \in V$ będzie wektorem własnym ϕ o wartości własnej c. Pokazaliśmy wcześniej, że $\phi(\mathrm{lin}(\alpha)^{\perp}) \subseteq \mathrm{lin}(\alpha)^{\perp}$ (czyli, że $\mathrm{lin}(\alpha)^{\perp}$ jest podprzestrzenią ϕ-niezmienniczą). Rozpatrzmy obcięcie ϕ do podprzestrzeni $n-1$-wymiarowej $\mathrm{lin}(\alpha)^{\perp}$. Wiemy, że obcięcie endomorfizmu do podprzestrzeni niezmienniczej jest endomorfizmem tej podprzestrzeni. Rozważane obcięcie to przekształcenie samosprzężone $n-1$-wymiarowej przestrzeni euklidesowej $(\mathrm{lin}(\alpha)^{\perp}, \langle , \rangle|_{\mathrm{lin}(\alpha)^{\perp}})$. Z założenia indukcyjnego istnieje zatem baza ortonomalna $\alpha_2, \ldots, \alpha_n$ przestrzeni $\mathrm{lin}(\alpha)^{\perp}$ złożona z wektorów własnych przekształcenia $\phi|_{\mathrm{lin}(\alpha)^{\perp}}$. Oczywiście są to zatem także wektory własne przekształcenia ϕ stanowiące układ ortonormalny. Dopełniamy ten układ prostopadły do bazy ortonormalnej $(V, \langle , \rangle)$ znormalizowanym wektorem $\alpha_1 = \frac{1}{\|\alpha\|}\alpha$. Układ $\alpha_1, \ldots, \alpha_n$ jest bazą ortonormalną $(V, \langle , \rangle)$. □

Fakt 135. *Każda macierz symetryczna $A \in M_n(\mathbb{R})$ jest diagonalizowalna nad $\mathbb{R}$. Co więcej istnieje macierz ortogonalna C taka, że macierz $C^T AC = C^{-1}AC$ jest diagonalna.*

Dowód. Niech $\phi : \mathbb{R}^n \to \mathbb{R}^n$ będzie przekształceniem liniowym zadanym warunkiem $M(\phi)^{st}_{st} = A$. Wówczas ϕ jest przekształceniem samosprzężonym przestrzeni $\mathbb{R}^n$ ze standardowym iloczynem skalarnym, Istnieje więc baza ortonormalna tej przestrzeni złożona z wektorów własnych ϕ. Niech $\mathcal{C} = (\gamma_1, \ldots, \gamma_n)$ będzie taką bazą. Zatem macierz $C = M(id)^{\mathcal{C}}_{st}$ jest ortogonalna i spełnia tezę. □

Twierdzenie o diagonalizowalności rzeczywistej macierzy symetrycznej przy pomocy bazy ortonormalnej, samo w sobie niezwykle istotne w rozmaitych zastosowaniach matematycznych, jest jedynie niby wrota do jaskini pełnej skarbów i rezultatów stanowiących punkt wyjścia do bardzo rozbudowanych teorii o niezliczonych zastosowaniach pozamatematycznych. Odnotujmy kolejny prosty wniosek.

Fakt 136. *Macierz $A \in M_n(\mathbb{R})$ jest diagonalizowalna nad $\mathbb{R}$ wtedy i tylko wtedy, gdy jest podobna do macierzy symetrycznej.*

Uwaga. Twierdzenie spektralne w podanej przez nas wersji nie działa dla macierzy zespolonych. Poniższa symetryczna macierz zespolona nie jest diagonalizowalna:

$$\begin{bmatrix} 1 & i \\ i & -1 \end{bmatrix}$$

(ale następnym razem naprawimy ten problem).

Uzupełnienie. Największa i najmniejsza wartość własna

Jednym z ważnych zastosowań teorii macierzy symetrycznych i twierdzenia o ich diagonalizowalności jest możliwość szacowania wartości własnych tych macierzy. Udowodnimy następujący rezultat.

Fakt 137. *Niech $A \in M_n(\mathbb{R})$ będzie macierzą symetryczną. Dla $\alpha \in \mathbb{R}^n$ niech $\|\alpha\|$ oznacza normę wektora przy standardowym iloczynie skalarnym. Niech wartości własne A to $\lambda_1 \geq \ldots \geq \lambda_n$. Wówczas*

$$\lambda_1 = \max_{\|\alpha\|=1} \alpha^T A\alpha, \quad \lambda_n = \min_{\|\alpha\|=1} \alpha^T A\alpha.$$

Co więcej, jeśli dla pewnego wektora α mamy

$$\alpha^T A\alpha = \lambda_i \|\alpha\|^2,$$

to $A\alpha = \lambda_i\alpha$, gdzie $i = 1, n$.

Dowód. Dowodzimy tezę dla λ_1, dla λ_n – całkowicie analogicznie. Niech $\alpha_1, \ldots, \alpha_n$ będzie bazą ortonormalną $(\mathbb{R}^n, \langle\,,\rangle_{st})$ złożoną z wektorów własnych macierzy symetrycznej $A \in M_n(\mathbb{R})$ odpowiadających $\lambda_1 \geq \ldots \geq \lambda_n$. Niech $\alpha = x_1\alpha_1 + \ldots + x_n\alpha_n$. Wówczas $\|\alpha\|^2 = x_1^2 + \ldots + x_n^2$. Zatem

$$\alpha^T A\alpha = \lambda_1 x_1^2 + \ldots + \lambda_n x_n^2 \leq \lambda_1(x_1^2 + \ldots + x_n^2) = \lambda_1\|\alpha\|^2. \qquad (*)$$

Z drugiej strony $\alpha_1^T A\alpha_1 = \lambda_1\|\alpha_1\|^2$, co daje pierwszą część tezy.

Jeśli natomiast dla pewnego wektora α mamy $\alpha^T A\alpha = \lambda_1\|\alpha\|^2$, to równość w nierówności $(*)$ dostaniemy tylko, gdy $x_{k+1} = \ldots = x_n = 0$, gdzie $\lambda_1 = \ldots = \lambda_k > \lambda_{k+1} \geq \ldots \geq \lambda_n$. Stąd $\alpha = x_1\alpha_1 + \ldots + x_n\alpha_k$ i dostajemy $A\alpha = \lambda_1\alpha$. □

Fakt 138. *Niech $A \in M_n(\mathbb{R})$ będzie macierzą symetryczną o wyrazach nieujemnych i wartościach własnych $\lambda_1 \geq \ldots \geq \lambda_n$. Istnieje wówczas niezerowy wektor $\alpha = (a_1, \ldots, a_n)$ taki, że $A\alpha = \lambda_1\alpha$ oraz $a_i \geq 0$, dla $1 \leq i \leq n$.*

Dowód. Niech $\alpha_1 = (x_1, \ldots, x_n)$ będzie wektorem własnym macierzy symetrycznej A o nieujemnych wyrazach o największej jej wartości własnej λ_1, gdzie $\|\alpha_1\| = 1$. Niech $\alpha = (|x_1|, \ldots, |x_n|)$. Wówczas $\|\alpha\| = \|\alpha_1\|$. Skoro A jest nieujemna, to $\alpha^T A\alpha \geq \alpha_1^T A\alpha_1 = \lambda_1$. Zatem z poprzedniego faktu mamy $\alpha^T A\alpha = \lambda_1$ oraz $A\alpha = \lambda_1\alpha$. □

Rezultaty te mają duże znaczenie na przykład w algebraicznej teorii grafów. Uogólniają się one do tzw. twierdzenia min-max oraz twierdzenia Gershgorina.

Przykładowe zastosowanie: jeśli macierz sąsiedztwa grafu G ma największą wartośc własną mniejszą od 2, wówczas G musi być drzewem.

Dodatek. Promień spektralny i potęgi macierzy

Na wykładziem mówiliśmy o diagonalizowalności rzeczywistych macierzy symetryczych. Jednym z kluczowych powodów, dla którego chcemy diagonalizować macierze jest, jak wiemy, badanie procesów zachodzących w czasie (dyskretnych lub ciągłych) za pomocą wielokrotnego aplikowania macierzy na pewnym wektorze danych startowych. Szereg rezultatów tej teorii wiąże się z twierdzeniem spektralnym.

Definicja 89. *Niech $A \in M_n(\mathbb{R})$. Promieniem spektralnym macierzy A nazwiemy liczbę*

$$\rho(A) = \max\{|\lambda| : \lambda \textit{ jest wartością własną } A.\}Okrelamyrwnie$$

Definicja 90. *Macierz $A \in M_n(\mathbb{R})$ nazywamy nieujemną (odp. dodatnią), jeśli wszystkie jej wyrazy są nieujemne (odp. dodatnie).*

Z uwagi na liczne zas

Formy hermitowskie i przekształcenia unitarne

Na poprzednich wykładach rozważaliśmy strukturę przestrzeni euklidesowej na przestrzeni liniowej nad ciałem liczb rzeczywistych. Ograniczenie się do przestrzeni rzeczywistej V pozwalało na wprowadzenie warunku $\langle v, v\rangle > 0$, dla $v \neq 0$, co z kolei dało możliwość określenia w $(V, \langle , \rangle)$ długości wektora, kąta między wektorami, objętości itd. Podobne konstrukcje można rozważać nad ciałem liczb zespolonych $\mathbb{C}$.

Podstawowa intuicja pochodzi z geometrycznej interpretacji modułu liczby zespolonej $z = a + bi$ jako długości odcinka łączącego punkty 0 oraz $a + bi$ na płaszczyźnie zespolonej. Moduł ten równy jest $\sqrt{a^2 + b^2}$. Myśląc o przestrzeni $\mathbb{C}^2$ możemy uprawiać na niej geometrię euklidesową przez utożsamienie jej z $\mathbb{R}^4$ – każdej parze liczb zespolonych (z_1, z_2) przyporządkowujemy czwórkę (a_1, b_1, a_2, b_2), przy czym mamy $z_1 = a_1 + b_1 i$, $z_2 = a_2 + b_2 i$. Załóżmy, że owa przestrzeń $\mathbb{R}^4$ wyposażona jest w standardowy iloczyn skalarny. Wówczas norma wektora (a_1, b_1, a_2, b_2) wynosi

$$\sqrt{a_1^2 + b_1^2 + a_2^2 + b_2^2}.$$

Powstaje pytanie: czy można przypisać parze $(z_1, z_2) \in \mathbb{C}^2$ jakiś rodzaj „zespolonego iloczynu skalarnego", który dawałby identyczną normę? Innymi słowy pytamy czy nie znając a_1, b_1, a_2, b_2, a jedynie operując na samych liczbach zespolonych z_1, z_2 jesteśmy w stanie odtworzyć wzór na normę wektora (z_1, z_2)? Czy możemy zdefiniować „standardowy iloczyn skalarny" w $\mathbb{C}^2$ wzorem $\langle (z_1, z_2), (z_1', z_2')\rangle = z_1 z_1' + z_2 z_2'$ i przyjąć jako normę wektora o współrzędnych zespolonych pierwiastek z „iloczynu skalarnego" tego wektora ze sobą? Otóż nie możemy, bowiem wówczas „norma" wektora (z_1, z_2) byłaby równa $\sqrt{z_1^2 + z_2^2}$, przy czym pod pierwiastkiem stoi liczba zespolona, a taki pierwiastek nie jest jednoznacznie określony. Co więcej, po rozpisaniu postaci ogólnych liczb z_1, z_2 norma ta (żadna z nich) nie byłaby równa $\sqrt{a_1^2 + b_1^2 + a_2^2 + b_2^2}$, poza szczególnymi (jakimi?) przypadkami. Szukany „iloczyn skalarny" w $\mathbb{C}^2$ uzyskamy natomiast wzorem:

$$\langle (z_1, z_2), (z_1', z_2')\rangle = z_1 \overline{z_1'} + z_2 \overline{z_2'}.$$

Wprawdzie nadal możemy dostać w wyniku $\langle\,,\rangle$ liczbę zespoloną, ale $\langle (z_1,z_2),(z_1,z_2)\rangle$ równe jest teraz liczbie rzeczywistej $z_1\overline{z_1}+z_2\overline{z_2} = |z_1|^2+|z_2|^2$. A zatem „norma zespolona" wektora (z_1,z_2) według zmodyfikowanej definicji wynosi $\sqrt{a_1^2+b_1^2+a_2^2+b_2^2}$, jak wcześniej.

Nowa definicja rodzi jednak pewne problemy. Otóż nowy „iloczyn skalarny" nie jest liniowy ze względu na drugą zmienną, np.

$$\langle (1,1),(1,i+1)\rangle = 1+(1-i) = 2-i, \text{ zaś}$$
$$\langle (1,1),(1,i)\rangle + \langle (1,1),(1,1)\rangle = 1-i+2 = 3-i.$$

Wyjaśnienie przynosi następująca definicja obejmująca wprowadzony wyżej „iloczyn".

Definicja 91. *Niech V będzie przestrzenią liniową nad ciałem $\mathbb{C}$. Funkcjonał $\langle\,,\rangle : V\times V\to\mathbb{C}$ nazywamy* ILOCZYNEM HERMITOWSKIM, *jeśli dla każdych $\alpha,\beta,\gamma,\delta\in V$ i $a,b,c,d\in\mathbb{C}$ zachodzi:*

(1)	$\langle a\alpha+b\beta,\gamma\rangle = a\langle\alpha,\gamma\rangle + b\langle\beta,\gamma\rangle$	*liniowość wzgl. pierwszej zmiennej,*
(2)	$\langle\alpha,c\gamma+d\delta\rangle = \overline{c}\langle\alpha,\gamma\rangle + \overline{d}\langle\alpha,\delta\rangle$	***anty**liniowość wzgl. drugiej zmiennej,*
(3)	$\langle\alpha,\beta\rangle = \overline{\langle\beta,\alpha\rangle}$	*hermitowska symetria,*
(4)	$\alpha\neq 0\Rightarrow\langle\alpha,\alpha\rangle\in\mathbb{R}_+$	*dodatnia określoność.*

Parę $(V,\langle\,,\rangle)$, gdzie V – skończenie wymiarowa przestrzeń liniowa nad $\mathbb{C}$ oraz $\langle\,,\rangle$ – iloczyn hermitowski nazywamy PRZESTRZENIĄ UNITARNĄ.

Podstawowym przykładem iloczynu hermitowskiego jest odpowiednik standardowego iloczynu skalarnego na $\mathbb{R}^n$, czyli tzw. standardowy iloczyn hermitowski na $\mathbb{C}^n$ dany wzorem:

$$\langle (z_1,z_2,\ldots,z_n),(z_1',z_2',\ldots,z_n')\rangle = z_1\overline{z_1'}+z_2\overline{z_2'}+\ldots+z_n\overline{z_n'}.$$

Iloczyn hermitowski ma fundamentalne znaczenie dla mechaniki kwantowej, gdzie – mówiąc bardzo nieprecyzyjnie – opis stanu układu kwantowego dokonuje się w zespolonej przestrzeni wektorowej. Słynna zasada superpozycji mówi o tym, że stany układu w przestrzeni stanów mogą być kombinacjami liniowymi innych stanów. Klasycznym przykładem jest tu słynny eksperyment myślowy Schrödingera, mówiący o kocie znajdującym się w superpozycji dwóch stanów: „kot żywy" i „kot martwy".

Co nas – matematyków interesuje w przestrzeniach unitarnych na obecnym etapie poznawania algebry liniowej? Przede wszystkim – pojęcie prostopadłości i problemy diagonalizowalności endomorfizmów. Mimo, że iloczyn hermitowski nie jest symetryczny, to prostopadłość wektorów taką własność zachowuje.

Fakt 139. *Niech $(V,\langle\,,\rangle)$ będzie przestrzenią unitarną oraz niech $\alpha,\beta\in V$. Wówczas $\langle\alpha,\beta\rangle = 0$ wtedy i tylko wtedy, gdy $\langle\beta,\alpha\rangle = 0$.*

Dowód. Warunek $\langle\alpha,\beta\rangle = 0$ jest równoważny warunkowi $\overline{\langle\beta,\alpha\rangle} = 0$, co jest równoważne warunkowi $\langle\beta,\alpha\rangle = 0$ (sprzężenie liczby zespolonej jest zerem wtedy i tylko wtedy, gdy ona sama jest zerem). □

Wynik ten motywuje wprowadzenie następującej definicji.

Definicja 92. *Niech $(V, \langle , \rangle)$ będzie przestrzenią unitarną. Wektory $\alpha, \beta \in V$ nazywamy* PROSTOPADŁYMI, *gdy $\langle \alpha, \beta \rangle = 0$. Układ wektorów $\alpha_1, \ldots, \alpha_n$ przestrzeni V nazywamy* ORTOGONALNYM, *jeśli $\langle \alpha_i, \alpha_j \rangle = 0$, dla $1 \leq i, j \neq n$, $i \neq j$. Dla podzbioru $S \subseteq V$ przez $S^\perp$ rozumiemy podprzestrzeń liniową złożoną ze wszystkich wektorów przestrzeni V prostopadłych do wszystkich wektorów ze zbioru S.*

Szereg rezultatów dotyczących układów ortogonalnych w przestrzeniach euklidesowych przenosi się bez żadnych zmian na przypadek przestrzeni unitarnych. Czytelnik zechce, śledząc dowody z poprzednich wykładów, sprawdzić (co jest pouczające o tym jakie założenia są tu naprawdę ważne), że:

- układ wektorów ortogonalnych w przestrzeni unitarnej jest liniowo niezależny,
- dla podprzestrzeni $W \subseteq V$ mamy $V = W \oplus W^\perp$ oraz $(W^\perp)^\perp = W$,
- każda przestrzeń unitarna ma bazę ortogonalną,
- współrzędne wektora α w bazie ortogonalnej $(\gamma_1, \ldots, \gamma_n)$ przestrzeni V wynoszą:

$$\frac{\langle \alpha, \gamma_1 \rangle}{\langle \gamma_1, \gamma_1 \rangle}, \frac{\langle \alpha, \gamma_2 \rangle}{\langle \gamma_2, \gamma_2 \rangle}, \quad \ldots, \quad \frac{\langle \alpha, \gamma_n \rangle}{\langle \gamma_n, \gamma_n \rangle}.$$

Ostatni fakt zawiera w sobie pewną istotną delikatność. Liczniki ułamków opisujących współrzędne wektora w bazie ortogonalnej są iloczynami hermitowskimi, a więc istotna jest kolejność. Innymi słowy mamy: $\langle \alpha, \gamma_i \rangle \neq \langle \gamma_i, \alpha \rangle$. To, że w ostatnim wyniku ustalona jest taka właśnie kolejność wynika z przyjętej przez nas definicji iloczynu hermitowskiego, w którym to zachodzi antyliniowość ze względu na drugą, a nie na pierwszą zmienną. Również twierdzenie o ortogonalizacji Grama-Schmidta układu liniowo niezależnego $\alpha_1, \ldots, \alpha_n$ do układu ortogonalnego $\gamma_1, \ldots, \gamma_n$ przenosi się bez zmian, o ile tylko pamiętamy o przyjęciu odpowiedniej kolejności. Wektory γ_i definiujemy w następujący sposób: $\gamma_1 = \alpha_1$ oraz dla $j > 1$:

$$\gamma_j = \alpha_j - \sum_{i=1}^{j-1} \frac{\langle \alpha_j, \gamma_i \rangle}{\langle \gamma_i, \gamma_i \rangle} \gamma_i.$$

Definicja 93. *Niech $(V, \langle , \rangle)$ będzie przestrzenią unitarną.* NORMĄ WEKTORA *$v \in V$ oznaczaną przez $\|v\|$ nazywamy liczbę $\sqrt{\langle v, v \rangle}$.*

Odnotujmy, że $\|v\| = 0$ wtedy i tylko wtedy, gdy $v = 0$. Co więcej, nietrudno widzieć, że $\|av\| = |a| \cdot \|v\|$. Oto dowód:

$$\|av\|^2 = \langle av, av \rangle = a\langle v, av \rangle = a\bar{a}\langle v, v \rangle = |a|^2 \|v\|^2.$$

Pouczające jest również zobaczenie dowodów odpowiedników twierdzenia Pitagorasa, nierówności Schwarza i nierówności trójkąta (stosują się one także do przypadku euklidesowego).

Fakt 140. *Niech $(V, \langle , \rangle)$ będzie przestrzenią unitarną.*

- *(twierdzenie Pitagorasa) Jeśli u, v są prostopadłe, to $\|u+v\|^2 = \|u\|^2 + \|v\|^2$.*
- *(nierówność Schwarza) Jeśli $u, v \in V$, to $|\langle u, v\rangle| \leq \|u\| \cdot \|v\|$.*
- *(nierówność trójkąta) Jeśli $u, v \in V$, to $\|u+w\| \leq \|u\| + \|v\|$.*

Dowód. Dla dowodu twierdzenia Pitagorasa zauważmy, że:

$$\begin{aligned}\|u+v\|^2 &= \langle u+v, u+v\rangle = \\ &= \langle u, 1\cdot u + 1\cdot v\rangle + \langle v, 1\cdot u + 1\cdot v\rangle = \\ &= \overline{1}\langle u, u\rangle + \underbrace{\overline{1}\langle u, v\rangle + \overline{1}\langle v, u\rangle}_{0} + 1\langle v, v\rangle = \\ &= \|u\|^2 + \|v\|^2.\end{aligned}$$

Nierówność Schwarza jest oczywista jeśli u lub v są wektorami zerowymi. Załóżmy przeciwnie. Posłużymy się rozkładem u na wektor będący jego rzutem na $\mathrm{lin}(v)$ oraz pewien wektor z $\mathrm{lin}(v)^\perp$. Dokładniej, określamy $w \in \mathrm{lin}(v)^\perp$ przez:

$$w = u - \frac{\langle u, v\rangle}{\|v\|^2} v$$

Wówczas z twierdzenia Pitagorasa:

$$\begin{aligned}\|u\|^2 &= \left\| \frac{\langle u, v\rangle}{\|v\|^2} v \right\|^2 + \|w\|^2 = \\ &= \langle \frac{\langle u, v\rangle}{\|v\|^2} v, \frac{\langle u, v\rangle}{\|v\|^2} v\rangle + \|w\|^2 = \\ &= \frac{\langle u, v\rangle}{\|v\|^2} \langle v, \frac{\langle u, v\rangle}{\|v\|^2} v\rangle + \|w\|^2 = \\ &= \frac{\langle u, v\rangle}{\|v\|^2} \overline{\frac{\langle u, v\rangle}{\|v\|^2}} \langle v, v\rangle + \|w\|^2 = \\ &= \frac{|\langle u, v\rangle|^2}{\|v\|^4} \cdot \|v\|^2 + \|w\|^2 = \\ &= \frac{|\langle u, v\rangle|^2}{\|v\|^2} + \|w\|^2 \geq \frac{|\langle u, v\rangle|^2}{\|v\|^2}.\end{aligned}$$

Mnożąc strony uzyskanej nierówności przez $\|v\|^2$ i pierwiastkując uzyskujemy nierówność Schwarza.

Wreszcie, nierówność trójkąta wymaga następującej dobrze znanej obserwacji zachodzącej dla każdej liczby zespolonej: $Re(z) \leq |z|$. Mamy podobnie jak wcześniej:

$$\begin{aligned}\|u+v\|^2 &= \langle u+v, u+v\rangle = \\ &= \langle u,u\rangle + \langle u,v\rangle + \langle v,u\rangle + \langle v,v\rangle = \\ &= \|u\|^2 + \|v\|^2 + \langle u,v\rangle + \overline{\langle u,v\rangle} = \\ &= \|u\|^2 + \|v\|^2 + 2Re\langle u,v\rangle \leq \\ &\leq \|u\|^2 + \|v\|^2 + 2|\langle u,v\rangle| \overset{\text{Schwarz}}{\leq} \\ &\leq \|u\|^2 + \|v\|^2 + 2\|u\|\|v\| = (\|u\| + \|v\|)^2.\end{aligned}$$

□

Podobnie jak w przypadku przestrzeni euklidesowych wprowadzić można pojęcie układu i bazy ortonormalnej, a wraz z nim pojęcie macierzy i wyznacznika Grama układu wektorów $\alpha_1, \ldots, \alpha_n$ przestrzeni unitarnej $(V, \langle , \rangle)$ o wyrazach postaci $\langle \alpha_i, \alpha_j\rangle$. Zauważmy jednak, że owa „macierz Grama" iloczynu hermitowskiego nie jest symetryczna. Jej wyrazy a_{ij} spełniają bowiem warunek hermitowskiej symetrii. Prowadzi to do fundamentalnej definicji, stanowiącej uogólnienie pojęć macierzy transponowanej i symetrycznej.

Definicja 94. *Niech $A \in (a_{ij}) \in M_n(\mathbb{C})$. Macierz $A^* \in M_n(\mathbb{C})$ mającą w i-tym wierszu i j-tej kolumnie wyraz $\overline{a_{ji}}$ nazywamy* SPRZĘŻENIEM HERMITOWSKIM *macierzy A. Jeśli macierz $A \in M_n(\mathbb{C})$ spełnia warunek $A^* = A$, wówczas mówimy, że A jest macierzą* HERMITOWSKĄ.

Oczywiście macierz hermitowska ma na przekątnej liczby rzeczywiste. Oto przykład takiej macierzy

$$\begin{bmatrix} -1 & 0 & -2i \\ 0 & 2 & 0 \\ 2i & 0 & -1 \end{bmatrix}.$$

Jak się (nietrudno) okazuje, pozostaje w mocy charakteryzacja układów liniowo niezależnych jako tych, których wyznacznik Grama jest niezerowy. Opis macierzy zespolonych stanowiących macierze Grama przypomina kryterium Sylvestera i dowodzi się w zasadzie analogicznie. Dla przykładu, przywołana wyżej macierz hermitowska w sposób oczywisty nie jest macierzą Grama żadnego iloczynu hermitowskiego.

Ma miejsce również niezwykle istotne twierdzenie o diagonalizowalności macierzy hermitowskich, stanowiące zespolony wariant twierdzenia spektralnego. Aby je sformułować, niezbędne jest określenie odpowiednika izometrii w kontekście przestrzeni unitarnych.

Definicja 95. *Niech* $(V_1, \langle , \rangle_1)$, $(V_2, \langle , \rangle_2)$ *będą przestrzeniami unitarnymi. Izomorfizm* $\phi : V_1 \to V_2$ *nazywamy* PRZEKSZTAŁCENIEM UNITARNYM, *jeżeli zachowuje iloczyn hermitowski, tj. dla każdych wektorów* $\alpha, \beta \in V_1$ *mamy:*

$$\langle \alpha, \beta \rangle_1 = \langle \phi(\alpha), \phi(\beta) \rangle_2.$$

Macierz $M \in M_n(\mathbb{C})$ *nazywamy* UNITARNĄ, *jeśli* $M \cdot \overline{M}^T = I_n$, *gdzie* $\overline{M}$ *powstaje z* M *przez sprzężenie zespolone każdego z wyrazów macierzy* M.

W przypadku przestrzeni euklidesowych dowodziliśmy, że ϕ jest izometrią wtedy i tylko wtedy, gdy jego macierz w pewnych (dowolnych) bazach ortonormalnych jest ortogonalna. Analogicznie pokazuje się, że przekształcenia unitarne przestrzeni unitarnych charakteryzują się posiadaniem w pewnych (dowolnych) bazach ortonormalnych macierzy unitarnej. Naszym celem jest pokazanie diagonalizowalności przekształceń unitarnych. Oznacza ona, że każda macierz unitarna jest podobna (nad $\mathbb{C}$) do macierzy diagonalnej.

Fakt 141. *Endomorfizm* ϕ *przestrzeni unitarnej* $(V, \langle , \rangle)$ *jest przekształceniem unitarnym wtedy i tylko wtedy, gdy zachowuje on normę wektora, to znaczy dla każdego* $v \in V$ *mamy* $\langle v, v \rangle = \langle \phi(v), \phi(v) \rangle$.

Dowód. Konieczność tego warunku jest oczywista, bo przekształcenia unitarne zachowują iloczyn skalarny. Załóżmy, że warunek w tezie jest spełniony dla pewnego endomorfizmu ϕ przestrzeni unitarnej V. Pokażemy, że jest to przekształcenie unitarne. Na mocy założenia dla dowolnych wektorów $u, v \in V$ mamy $\langle u+v, u+v \rangle = \langle \phi(u+v), \phi(u+v) \rangle$. A zatem po rozpisaniu:

$$\begin{aligned}\langle \phi(u+v), \phi(u+v) \rangle &= \langle \phi(u) + \phi(v), \phi(u) + \phi(v) \rangle = \\ &= \langle \phi(u), \phi(u) \rangle + \langle \phi(v), \phi(u) \rangle + \langle \phi(u), \phi(v) \rangle + \langle \phi(v), \phi(v) \rangle = \\ &= \langle u, u \rangle + \langle \phi(v), \phi(u) \rangle + \langle \phi(u), \phi(v) \rangle + \langle v, v \rangle,\end{aligned}$$

czyli $\langle \phi(u), \phi(v) \rangle + \langle \phi(v), \phi(u) \rangle = \langle u, v \rangle + \langle v, u \rangle$. Skoro równość ta jest prawdziwa dla dowolnych u, v, to wstawiając w miejsce v wektor iv i korzystając z $\mathbb{C}$-liniowości ϕ (czyli $\phi(iv) = i\phi(v)$) dostajemy:

$$\begin{aligned}\langle \phi(u), \phi(iv) \rangle + \langle \phi(iv), \phi(u) \rangle &= \langle \phi(u), i\phi(v) \rangle + \langle i\phi(v), \phi(u) \rangle = \\ &= -i\langle \phi(u), \phi(v) \rangle + i\langle \phi(v), \phi(u) \rangle = \\ &= -i\langle u, v \rangle + i\langle v, u \rangle,\end{aligned}$$

czyli po uproszczeniu i mamy

$$-\langle \phi(u), \phi(v) \rangle + \langle \phi(v), \phi(u) \rangle = -\langle u, v \rangle + \langle v, u \rangle.$$

Dodając stronami równości = oraz = dostajemy $\langle \phi(v), \phi(u) \rangle = \langle v, u \rangle$, dla wszystkich $u, v \in V$. Czyli ϕ jest unitarne. □

Naszym celem jest pokazanie, że w przeciwieństwie do izometrii przestrzeni euklidesowych, przekształcenia unitarne przestrzeni unitarnych są zawsze diagonalizowalne.

W rzeczywistości mając trochę czasu na opis tzw. przekształceń normalnych bylibyśmy w stanie przy pomocy zapowiadanego rezultatu pokazać fundamentalny rezultat mówiący, że każda izometria przestrzeni euklidesowej da się przedstawić w pewnej bazie ortonormalnej w postaci macierzy blokowo-diagonalnej o blokach 1x1 lub 2x2, przy czym bloki $2x2$ są macierzami obrotów. Warunek ten charakteryzuje izometrie jeśli dodamy, że bloki 1×1 równe są 1 lub -1. A więc twierdzenia o endomorfizmach przestrzeni nad $\mathbb{C}$ mogą nieść skutki dla opisu izometrii.

Fakt 142. *Niech ϕ będzie endomorfizmem unitarnym przestrzeni $(V, \langle , \rangle)$. Wówczas każda wartość własna $\lambda \in \mathbb{C}$ endomorfizmu ϕ spełnia $|\lambda| = 1$. Wektory własne ϕ odpowiadające parami różnym wartościom własnym są ortogonalne. Istnieje też baza ortogonalna przestrzeni $(V, \langle , \rangle)$ złożona z wektorów własnych ϕ.*

Dowód. Niech λ będzie wartością własną ϕ. Istnieje więc niezerowy wektor v taki, że $\phi(v) = \lambda v$. Wiemy, że przekształcenie unitarne zachowuje normę, a więc mamy $\langle x, x\rangle = \langle \phi(x), \phi(x)\rangle = \lambda\overline{\lambda}\langle x, x\rangle$. Skoro $\langle x, x\rangle \neq 0$, to $|\lambda|^2 = 1$, co dowodzi pierwszą część tezy.

Weźmy teraz $\lambda_1 \neq \lambda_2 \in \mathbb{C}$, dla których istnieją niezerowe wektory x, y, że $\phi(v_1) = \lambda_1 v_1, \phi(v_2) = \lambda_2 v_2$. Przekształcenie unitarne zachowuje iloczyn hermitowski, więc $\langle x, y\rangle = \langle \phi(x), \phi(y)\rangle = \lambda_1\overline{\lambda_2}\langle x, y\rangle$. Skoro wiemy już z poprzedniego punktu tezy, że $|\lambda_2| = 1$, mamy $\overline{\lambda_2} = \lambda_2^{-1}$. A zatem z założenia $\lambda_1 \neq \lambda_2$ widzimy, że $\lambda_1\lambda_2^{-1} \neq 1$. Stąd warunek $\langle x, y\rangle = \langle \phi(x), \phi(y)\rangle = \lambda_1\overline{\lambda_2}\langle x, y\rangle = \lambda_1\lambda_2^{-1}\langle x, y\rangle$, pociąga za sobą $\langle x, y\rangle = 0$, co dowodzi prostopadłości wektorów własnych odpowiadających różnym wartościom własnym przekształcenia unitarnego.

Dowodzimy teraz istnienia bazy $(V, \langle , \rangle)$ złożonej z wektorów własnych ϕ. Dowód jest indukcją ze względu na wymiar n przestrzeni V. Dla $n = 1$ teza jest jasna. Przechodzimy do kroku indukcyjnego. Skoro ϕ jest endomorfizmem przestrzeni zespolonej, to oczywiście ma wartość własną (bo jego wielomian charakterystyczny musi mieć, jako wielomian o współczynnikach w $\mathbb{C}$, pierwiastek), którą oznaczamy λ. Niech x będzie odpowiadającym jej niezerowym wektorem własnym. Rozważmy $\mathrm{lin}(x)^\perp$. Twierdzimy, że $(\mathrm{lin}(x)^\perp, \langle , \rangle|_{\mathrm{lin}(x)^\perp})$ jest przestrzenią unitarną (to jest w zasadzie oczywiste, tak jak dla iloczynów skalarnych, na mocy dodatniej określoności) oraz, że $\mathrm{lin}(x)^\perp$ jest ϕ-niezmiennicza. Istotnie, weźmy $v \in \mathrm{lin}(x)^\perp$. Z faktu, że ϕ zachowuje normę i jest izomorfizmem mamy

$$\langle \phi(v), x\rangle = \langle v, \phi^{-1}(x)\rangle = \langle v, \lambda^{-1}x\rangle = \overline{\lambda^{-1}}\langle v, x\rangle = 0.$$

A zatem ϕ obcięte do $\mathrm{lin}(x)^\perp$ jest endomorfizmem unitarnym przestrzeni wymiaru $n-1$ (już wspominałem, że w przestrzeni unitarnej mamy $V = \mathrm{lin}(x) \oplus \mathrm{lin}(x)^\perp$), a zatem na mocy założenia indukcyjnego jest diagonalizowalny w pewnej bazie $a_1, \ldots, a_{n-1}$. Każdy z wektorów tej bazy jest prostopadły do x. A zatem układ $a_1, \ldots, a_{n-1}, x$ jest bazą ortogonalną V złożoną z wektorów własnych ϕ. □

Przestrzenie dwuliniowe. Macierze kongruentne

Od kilku wykładów zajmujemy się badaniem przestrzeni liniowych V wyposażonych w dodatkową strukturę pochodzącą od pewnych funkcji na przestrzeni $V \times V$ (dotychczas nad $\mathbb{R}$ i $\mathbb{C}$). Celem geometrycznym jest zrozumienie naturalnych obiektów związanych z prostopadłością. Z algebraicznego punktu widzenia interesujące było rozważanie przekształceń liniowych zachowujących dodatkową strukturę i sposobów ich klasyfikowania m.in. za pomocą macierzy ortogonalnych. Celem obecnych rozważań jest omówienie tych zagadnień w ogólnym kontekście, nie ograniczając się do ciał liczb rzeczywistych i zespolonych. Formy dwuliniowe, bo o nich będzie mowa, wywodzą się z badania problemów znacznie starszych niż sama algebra liniowa, m.in. z teorioliczbowych problemów rozkładu liczb całkowitych na sumy (pewnej liczby) kwadratów, geometrycznych problemów klasyfikacji powierzchni opisanych wielomianowymi równaniami stopnia 2 czy analitycznych problemów szukania ekstremów funkcji wielu zmiennych.

Definicja 96. *Niech V będzie przestrzenią liniową nad ciałem K. Funkcję:*

$$h : V \times V \to K$$

nazywamy FORMĄ DWULINIOWĄ *(albo* FUNKCJONAŁEM DWULINIOWYM*) na przestrzeni V, jeśli dla każdych $\alpha, \beta, \gamma, \delta \in V$ i $a, b, c, d \in K$ zachodzi:*

(1) $h(a\alpha + b\beta, \gamma) = a \cdot h(\alpha, \gamma) + b \cdot h(\beta, \gamma)$ *liniowość względem pierwszej zmiennej,*
(2) $h(\alpha, c\gamma + d\delta) = c \cdot h(\alpha, \gamma) + d \cdot h(\alpha, \delta)$ *liniowość względem drugiej zmiennej,*

Jeśli h jest formą dwuliniową na V oraz $W \subseteq V$ jest podprzestrzenią, to formę $h' : W \times W \to K$ określoną dla każdych $u, w \in W$ wzorem

$$h'(u, w) = h(u, w)$$

nazywamy OGRANICZENIEM FORMY *h do W i oznaczamy $h|_W$.*

Definicja ta przypomina definicję iloczynu skalarnego, przy czym opuściliśmy w niej założenie o symetryczności i dodatniej określoności. Oczywiście każdy iloczyn skalarny jest formą dwuliniową. Forma

hermitowska nie jest formą dwuliniową (analogiem są tu tzw. formy półtoraliniowe). Zobaczmy kilka dalszych przykładów.

- Dla $V = \mathbb{R}^3$ funkcja $h : V \times V \to \mathbb{R}$ dana wzorem:

$$h((x_1, x_2, x_3), (y_1, y_2, y_3)) = x_1y_1 + x_2y_2 - 2x_3y_3,$$

- Dla dowolnej pary wektorów $(a_1, a_2), (b_1, b_2) \in K^2$ określamy:

$$h((a_1, a_2), (b_1, b_2)) = \det \begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \end{bmatrix}.$$

- Dla $V = M_n(K)$ oraz dowolnych $A, B \in V$ określamy:

$$h((A, B)) = \mathrm{tr}(AB^T).$$

- Dla $V = F_c[0, 1]$ – funkcji „całkowalnych" z $[0, 1]$ do $\mathbb{R}$, określamy:

$$h(f, g) = \int_0^1 f(x)g(x)dx.$$

- Dla przestrzeni $V = (P(X), \triangle, \emptyset)$ nad $\mathbb{Z}_2$ oraz $A, B \in V$ określamy:

$$h(A, B) = |A \cap B| \pmod 2.$$

Nietrudno widzieć (naśladując dowody z poprzednich wykładów), że każda forma dwuliniowa $h : K^n \times K^n \to K$ na przestrzeni K^n zadana jest wzorem:

$$\begin{aligned} h((x_1, \ldots, x_n), (y_1, \ldots, y_n)) &= h(x_1\epsilon_1 + \ldots + x_n\epsilon_n, y_1\epsilon_1 + \ldots + y_n\epsilon_n) = \\ &= x_1 h(\epsilon_1, y_1\epsilon_1 + \ldots + y_n\epsilon_n) + \ldots + x_n h(\epsilon_n, y_1\epsilon_1 + \ldots + y_n\epsilon_n) = \\ &= \sum_{i,j}^{n} x_i y_i h(\epsilon_i, \epsilon_j), \end{aligned}$$

gdzie $(\epsilon_1, \ldots, \epsilon_n)$ jest bazą standardową K^n. Podobnie można wykazać, że jeśli $(\alpha_1, \ldots, \alpha_n)$ jest bazą przestrzeni V, to wszystkie formy dwuliniowe na V opisane są wzorami:

$$h((x_1\alpha_1 + \ldots + x_n\alpha_n), (y_1\alpha_1 + \ldots + y_n\alpha_n)) = \sum_{i,j}^{n} x_i y_j h(\alpha_i, \alpha_j).$$

Definicja 97. *Niech $h : V \times V \to K$ będzie formą dwuliniową na przestrzeni V i niech $\mathcal{A} = (\alpha_1, \ldots, \alpha_n)$ będzie bazą przestrzeni V.* MACIERZĄ FORMY h W BAZIE $\mathcal{A}$ *nazywamy macierz:*

$$G(h; \mathcal{A}) = [h(\alpha_i, \alpha_j)] \in M_n(K)$$

Pojęcie to jest naturalnym uogólnieniem macierzy Grama bazy przestrzeni euklidesowej. Rozważmy kilka przykładów, uwzględniających między innymi macierze nie spełniające kryterium Sylvestera:

- Niech $h : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}$ dana będzie wzorem

$$h((x_1, x_2, x_3), (y_1, y_2, y_3)) = x_1y_1 + x_2y_2 - x_3y_3.$$

Wówczas:

$$G(h; st) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}.$$

- Niech $h : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$ dana będzie wzorem

$$h((x_1, x_2), (y_1, y_2)) = x_1y_1 - 2x_1y_2 + 3x_2y_1 + 5x_2y_2.$$

Wówczas jeśli $\mathcal{A} = ((1,1),(0,4))$, to

$$G(h; st) = \begin{bmatrix} 1 & -2 \\ 3 & 5 \end{bmatrix}, \quad G(h; \mathcal{A}) = \begin{bmatrix} 7 & 12 \\ 32 & 80 \end{bmatrix}.$$

Przypominamy formułę wynikającą z definicji macierzy formy i wyprowadzaną już na wykładzie o iloczynie skalarnym.

Fakt 143. *Jeśli $h : V \times V \to K$ jest formą dwuliniową, $\mathcal{A} = (\alpha_1, \ldots, \alpha_n)$ jest bazą przestrzeni V oraz $A = G(h; \mathcal{A})$, to dla dowolnych wektorów $\alpha = x_1\alpha_1 + \ldots + x_n\alpha_n, \beta = y_1\alpha_1 + \ldots + y_n\alpha_n$ przestrzeni V zachodzi:*

$$h(\alpha, \beta) = \begin{bmatrix} x_1 & \ldots & x_n \end{bmatrix} \cdot A \cdot \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}.$$

Ważnym wątkiem naszych rozważań będzie badanie macierzy form dwuliniowych w różnych bazach.

Fakt 144. *Niech $h : V \times V \to K$ będzie formą dwuliniową oraz niech $\mathcal{A} = (\alpha_1, \ldots, \alpha_n)$, $\mathcal{B} = (\beta_1, \ldots, \beta_n)$ będą bazami przestrzeni V. Jeśli $A = G(h; \mathcal{A}), \mathcal{B} = G(h; \mathcal{B})$ oraz $C = M(id)^{\mathcal{A}}_{\mathcal{B}}$, to*

$$B = C^T AC.$$

Dowód. Niech $C = [c_{ij}]$. Opiszmy wyraz z i-tego wiersza i j-tej kolumny macierzy $C^T AC$. Nietrudno widzieć (bo tak jest dla dowolnego iloczynu trzech macierzy), że wyraz ten powstaje przez przemnożenie i-tego wiersza macierzy C^T, macierzy A oraz j-tej kolumny macierzy C. Mnożymy więc w rezultacie współrzędne i-tego oraz j-tego elementu bazy $\mathcal{B}$ zapisanych w bazie $\mathcal{A}$ przez macierz formy h w bazie $\mathcal{A}$. A zatem zgodnie z poprzednią uwagą wyraz ten wynosi $h(\beta_i, \beta_j)$. Dokładnie tej samej postaci jest także z definicji wyraz w i-tym wierszu i j-tej kolumnie macierzy $B = G(h; \mathcal{B})$. □

Uwaga ta motywuje wprowadzenie następującego ważnego pojęcia.

Definicja 98. *Mówimy, że macierze $A, B \in M_n(K)$ są* KONGRUENTNE NAD *K jeśli istnieje macierz odwracalna $C \in M_n(K)$ taka, że*

$$B = C^T AC.$$

Przykład. Macierze $A_1, A_2 \in M_3(K)$ postaci

$$A_1 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \quad A_2 = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

są kongruentne nad dowolnym ciałem charakterystyki różnej od 2, ponieważ:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix} = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Fakt 145. *Macierze $A, B \in M_n(K)$ są kongruentne wtedy i tylko wtedy, gdy są macierzami tej samej formy dwuliniowej (w pewnych bazach).*

Dowód. Jeśli istnieje forma dwuliniowa $h : V \times V \to K$ na n wymiarowej przestrzeni liniowej V nad K oraz bazy $\mathcal{A}, \mathcal{B}$ przestrzeni V takie, że $A = G(h, \mathcal{A})$, $B = G(h, \mathcal{B})$, to macierze A, B są kongruentne na mocy uwagi wyżej. Na odwrót, niech $B = C^T AC$, dla pewnej macierzy odwracalnej $C \in M_n(K)$. Niech $A = [a_{ij}]$. Określmy formę dwuliniową $h : K^n \times K^n \to K$ warunkiem $G(h; st) = A$. To znaczy:

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

Niech $B = (\beta_1, \ldots, \beta_n)$ będzie bazą przestrzeni K^n zadaną przez $M(id)_{\mathcal{B}}^{st} = C$. Wówczas z dowodu poprzedniej uwagi wynika natychmiast, że $B = G(h; \mathcal{B})$. □

Kilka dalszych przykładów.

- Dla (rozważanej wcześniej) formy $h : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$ zadanej wzorem

  $$h((x_1, x_2), (y_1, y_2)) = x_1 y_1 - 2x_1 y_2 + 3x_2 y_1 + 5x_2 y_2$$

  wyliczyliśmy

  $$G(h; st) = \begin{bmatrix} 1 & -2 \\ 3 & 5 \end{bmatrix}, \quad G(h; \mathcal{A}) = \begin{bmatrix} 7 & 12 \\ 32 & 80 \end{bmatrix},$$

  więc macierze te są kongruentne nad $\mathbb{R}$. Przestrzeń $(\mathbb{R}^2, h)$ nie jest jednak euklidesowa, bo $G(h; st)$ nie jest nawet symetryczna.

- Niech $(V, \langle , \rangle)$ będzie przestrzenią euklidesową. Wówczas dowolne dwie macierze Grama dla baz $\mathcal{A}$, $\mathcal{B}$ przestrzeni V są kongruentne. W szczególności, skoro dla każdej przestrzeni euklidesowej istnieje baza ortonormalna, to macierz Grama w tej bazie jest identycznością. W szczególności każda macierz Grama bazy n-wymiarowej przestrzeni euklidesowej jest kongruentna do macierzy identyczności I rozmiaru $n \times n$.

Jak wiemy z kryterium Sylvestera, nie każda macierz rozmiaru n nad $\mathbb{R}$ jest macierzą Grama. Istnieją więc macierze, które nie są kongruentne z identycznością.

- Niech ϕ będzie izometrią na przestrzeni euklidesowej V oraz niech A, B będą odpowiednio macierzami tej izometrii w bazach ortonormalnych $\mathcal{A}$ oraz $\mathcal{B}$. Macierz C przejścia pomiędzy bazami ortonormalnymi $\mathcal{A}$ oraz $\mathcal{B}$ jest macierzą ortogonalną (bo to także macierz izometrii – identyczności), to znaczy $C^{-1} = C^T$. W szczególności macierze A oraz B są jednocześnie podobne i kongruentne. Nietrudno jednak wskazać przykłady macierzy kongruentnych, które nie są podobne, i na odwrót.

Kongruentność, podobnie jak podobieństwo, jest relacją równoważności w zbiorze $M_n(K)$. Rzeczywiście:

- zwrotność relacji kongruencji wynika z faktu, że $A = I^T A I$,
- symetryczność relacji kongruencji wynika z tego, że jeśli $A = C^T B C$, dla pewnej macierzy odwracalnej C, to $B = (C^{-1})^T A C^{-1}$,

Mamy oczywiście $(C^{-1})^T = (C^T)^{-1}$.

- przechodniość relacji kongruencji wynika z tego, że jeśli $A = X^T B X, B = Y^T C Y$, to $A = X^T Y^T C Y X = (YX)^T C (YX)$.

Stwierdzenie kiedy macierze są kongruentne może być bardzo trudnym zadaniem. Jednym z celów kolejnego wykładu jest dokonać takiej klasyfikacji dla macierzy symetrycznych nad ciałem liczb rzeczywistych i zespolonych. Sformułujmy teraz kilka warunków koniecznych, aby macierze były kongruentne.

Fakt 146. *Jeśli macierze $A, B \in M_n(K)$ są kongruentne nad K, to:*

- $r(A) = r(B)$,
- $\det(A) \cdot \det(B)$ *jest kwadratem w ciele K.*

Dowód. Skoro istnieje macierz odwracalna C taka, że $B = C^T A C$, to:

$$r(B) = r(C^T A C) = r(A),$$

bo mnożenie przez macierz odwracalną (z dowolnej strony) nie zmienia rzędu. Mamy również:

$$\det(A) \cdot \det(B) = \det(A) \cdot \det(C^T A C) = (\det A \cdot \det C)^2.$$

□

Intuicyjnie mówiąc, problem badania kongruencji macierzy nad K jest tym trudniejszy, im więcej elementów ciała K nie można utożsamić za pomocą kwadratu. Stąd na przykład klasyfikacja macierzy kongruentnych nad ciałem $\mathbb{Q}$ jest bardzo skomplikowana, w porównaniu do ciał $\mathbb{C}$ oraz $\mathbb{R}$. Przede wszystkim jednak, interesuje nas ograniczenie się do badania form i macierzy symetrycznych.

Definicja 99. *Mówimy, że forma dwuliniowa h na przestrzeni V jest* SYMETRYCZNA, *jeśli dla każdych wektorów $\alpha, \beta \in V$ mamy $h(\alpha, \beta) = h(\beta, \alpha)$.*

Fakt 147. *Relacja kongruencji nad ciałem K jest relacją równoważności w zbiorze macierzy symetrycznych rozmiaru n. W szczególności macierz symetryczna nie może być kongruentna do macierzy niesymetrycznej.*

Dowód. Jeśli $A = A^T$ oraz $B = C^T AC$, dla pewnej macierzy A, to oczywiście

$$B^T = (C^T AC)^T = C^T A^T C = C^T AC = B.$$

□

Zobaczmy kilka przykładów zastosowania tych rezultatów:

- Weźmy macierze zespolone

$$A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}.$$

  Macierze te są kongruentne nad $\mathbb{C}$, ponieważ:

$$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{2} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{2} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}.$$

  Nad $\mathbb{R}$ macierze A i B nie będą kongruentne, a nad ciałem $\mathbb{Q}$ także B i C nie są kongruentne.

- Wśród poniższych czterech macierzy rzeczywistych

$$A = \begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix}, \quad B = \begin{bmatrix} -1 & 6 \\ -2 & 6 \end{bmatrix}, \quad C = \begin{bmatrix} 6 & -2 \\ 6 & -1 \end{bmatrix}, \quad D = \begin{bmatrix} 4 & 2 \\ 6 & 3 \end{bmatrix}$$

  kongruentne nad $\mathbb{R}$ są jedynie macierze niesymetryczne B, C. Rzeczywiście, mamy:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} -1 & 6 \\ -2 & 6 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 6 & -2 \\ 6 & -1 \end{bmatrix}.$$

  Widzimy też, że $\det A = -1, \det B = 1, \det C = 2$, co oznacza, że A, B nie mogą być kongruentne nad $\mathbb{R}$, zaś B, C nie mogą być kongruentne nad $\mathbb{Q}$.

Podstawową metodą sprawdzania czy macierze są kongruentne jest próba znalezienia kongruentnej do nich macierzy o szczególnie prostej postaci, np. macierzy diagonalnej. Kiedy macierz formy dwuliniowej jest diagonalna? Czy zawsze musi być diagonalna? Na te pytania odpowiada teoria przestrzeni dwuliniowych, stanowiących uogólnienie przestrzeni euklidesowych.

Definicja 100. *Parę (V,h), gdzie V jest skończenie wymiarową przestrzenią liniową nad ciałem K, zaś $h : V \times V \to K$ jest formą dwuliniową symetryczną nazywamy* PRZESTRZENIĄ DWULINIOWĄ.

Oczywiście każda przestrzeń euklidesowa jest przestrzenią dwuliniową. Podobnie jak w przypadku przestrzeni euklidesowych, jeśli weźmiemy podprzestrzeń W przestrzeni dwuliniowej (V,h) nad K, wówczas obcięcie $h|_W : W \times W \to K$ formy h do W zadaje na W strukturę przestrzeni dwuliniowej $(W, h|_W)$. W przeciwieństwie jednak do przypadku euklidesowego, podprzestrzenie przestrzeni dwuliniowej mogą – jako przestrzenie dwuliniowe z „odziedziczoną formą" – mieć zupełnie inne własności niż wyjściowa przestrzeń. Problemowi temu przyjrzymy się następnym razem. Dziś zakończymy definicją prostopadłości, analogiczną do euklidesowej, odnoszącą się do problemu znajdowania diagonalnych macierzy danej formy dwuliniowej.

Definicja 101. *Niech (V,h) będzie przestrzenią dwuliniową.*

(a) Mówimy, że wektory α, β są PROSTOPADŁE, *jeśli $h(\alpha,\beta) = 0$, ozn. $\alpha \perp \beta$. Jeśli X, Y są podzbiorami V i $\alpha \perp \beta$, dla każdych $\alpha \in X$, $\beta \in Y$, to piszemy $X \perp Y$.*

(b) Jeśli $\mathcal{A} = (\alpha_1, \ldots, \alpha_n)$ jest bazą przestrzeni dwuliniowej (V,h) i $\alpha_i \perp \alpha_j$, dla każdego $i \neq j$, to bazę $\mathcal{A}$ nazywamy BAZĄ PROSTOPADŁĄ *(ortogonalną) przestrzeni dwuliniowej (V,h).*

Problem znajdowania diagonalnej macierzy formy dwuliniowej jest zatem w istocie problemem istnienia i znajdowania bazy prostopadłej przestrzeni dwuliniowej. Na kolejny wykład mamy zatem następujące wyzwania:

- rozstrzygnąć kiedy (i czy) przestrzenie dwuliniowe mają bazy prostopadłe, co by oznaczało, ze każda macierz formy dwuliniowej jest kongruentna do macierzy diagonalnej,
- opisać metody znajdowania baz prostopadłych przestrzeni dwuliniowych, jeśli istnieją,
- rozstrzygnąć kiedy macierze diagonalne są kongruentne nad ciałem K (i jak to zależy od ciała K, bo zależy, i to bardzo).

Baza prostopadła przestrzeni dwuliniowej

Na ostatnim wykładzie poznaliśmy pojęcie przestrzeni dwuliniowej, czyli skończenie wymiarowej przestrzeni nad ciałem K z dodatkową strukturą h zadaną przez symetryczną formę dwuliniową. Opuszczenie obowiązującego w przestrzeniach euklidesowych $(V, \langle , \rangle)$ założenia o dodatniej określoności formy $\langle , \rangle$ sprawia, że przestrzeń dwuliniowa może zawierać wektory prostopadłe do siebie. Ważnym skutkiem tego zjawiska jest, jak się okaże, występowanie podprzestrzeni W przestrzeni dwuliniowej V, które nie mają „dopełnienia ortogonalnego", czyli $V \neq W + W^{\perp}$. Utrudnia to (a czasem wręcz uniemożliwia) skuteczne badanie układów prostopadłych wektorów w przestrzeniach dwuliniowych.

Definicja 102. *Niech (V, h) będzie przestrzenią dwuliniową. Mówimy, że wektory α, β są* PROSTOPADŁE, *jeśli $h(\alpha, \beta) = 0$, ozn. $\alpha \perp \beta$. Zbiór wszystkich wektorów prostopadłych do zbioru $X \subseteq V$ oznaczamy $X^{\perp}$. Wektor $\alpha \in V$ nazywamy* IZOTROPOWYM, *jeśli $h(\alpha, \alpha) = 0$, to znaczy $\alpha \perp \alpha$.*

Rozważmy kilka przykładów.

- W przestrzeniach euklidesowych nie ma niezerowych wektorów izotropowych, bo dla iloczynu skalarnego h w V i każdego niezerowego wektora $\alpha \in V$ mamy $h(\alpha, \alpha) > 0$. Dla każdej podprzestrzeni W przestrzeni euklidesowej V mamy $V = W \oplus W^{\perp}$. W przestrzeni dwuliniowej nie zawsze tak jest.

- Dla formy $h : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$ zadanej wzorem

  $$h((x_1, x_2), (y_1, y_2)) = x_1 y_2 + x_2 y_1$$

  wektory $(1, 0), (0, 1)$ są izotropowe. Przy tym $\mathrm{lin}(1, 0)^{\perp} = \mathrm{lin}(1, 0)$ oraz $\mathrm{lin}(0, 1)^{\perp} = \mathrm{lin}(0, 1)$.

- Dla formy $h : \mathbb{Z}_2^2 \times \mathbb{Z}_2^2 \to \mathbb{Z}_2$ zadanej wzorem

  $$h((x_1, x_2), (y_1, y_2)) = x_1 y_2 + x_2 y_1$$

  każdy wektor jest izotropowy, bo $h((x_1, x_2), (x_1, x_2)) = 2x_1 x_2 = 0$. A jednak jest to przestrzeń nieosobliwa!

Definicja 103. *Niech (V,h) będzie przestrzenią dwuliniową. Układ $\alpha_1,\dots,\alpha_k$ wektorów V nazywamy* PROSTOPADŁYM *(albo* ORTOGONALNYM*), jeśli $\alpha_i \perp \alpha_j$ (czyli $h(\alpha_i,\alpha_j)=0$), dla każdych $i \neq j$.*

Bazę przestrzeni V nazywamy PROSTOPADŁĄ *(albo* ORTOGONALNĄ*), jeśli jest ona układem prostopadłym.*

Przykład. Dla formy $h:\mathbb{R}^2\times\mathbb{R}^2\to\mathbb{R}$ zadanej wzorem

$$h((x_1,x_2),(y_1,y_2)) = x_1y_2 + x_2y_1$$

mamy $\operatorname{lin}(1,0)^\perp = \operatorname{lin}(1,0)$ oraz $\operatorname{lin}(0,1)^\perp = \operatorname{lin}(0,1)$, a zatem wektory $(1,0),(0,1)$ nie tylko nie są prostopadłe, ale nie uda nam się, korzystając z żadnej „dwuliniowej ortogonalizacji" typu Grama-Schmidta, otrzymać bazy prostopadłej z tego układu. To rodzi następujące pytanie: czy w przestrzeni $(\mathbb{R}^2,h)$ istnieje baza ortogonalna? Okazuje się, że tak, wystarczy obrać układ $((1,1),(1,-1))$. Pierwszy układ zawierał wektory izotropowe, drugi ich nie zawiera. Czy zawsze można wybrać bazę z wektorów nieizotropowych?

Same wzory mają sens, bo w każdym ciele K dopuszczalny jest iloraz typu $h(\beta,\alpha)/h(\alpha,\alpha)$, gdzie α – nieizotropowy.

Przykład. W $(\mathbb{Z}_2)^2$ z formą $h:\mathbb{Z}_2\times\mathbb{Z}_2\to\mathbb{Z}_2$ daną wzorem:

$$((x_1,x_2),(y_1,y_2)) = x_1y_2 + x_2y_1$$

nie ma bazy prostopadłej. Istotnie, gdyby α_1,α_2 było taką bazą, to $h(\alpha_1,\alpha_2) = h(\alpha_2,\alpha_1) = 0$. Co więcej, mielibyśmy także

$$h(\alpha_1,\alpha_1) = h(\alpha_2,\alpha_2) = 0,$$

bo każdy wektor w $((\mathbb{Z}_2)^2,h)$ jest izotropowy. To oznacza, że gdyby $\mathcal{A} = (\alpha_1,\alpha_2)$ było bazą, to macierz $G(h;\mathcal{A})$ byłaby zerowa. To by z kolei oznaczało, że h wykonane na dowolnej parze wektorów (v,w) jest zerowe (bo wykonanie h to przemnożenie $G(h;\mathcal{A})$ z obydwu stron przez wektory współrzędnych v,w w bazie $\mathcal{A}$. Mamy natomiast $h((1,0),(0,1)) = 1 \neq 0$. Sprzeczność.

Definicja 104. *Mówimy, że przestrzeń dwuliniowa (V,h) jest* NIEOSOBLIWA*, jeśli dla każdej bazy $\mathcal{A}$ przestrzeni V macierz $G(h,\mathcal{A})$ jest odwracalna. Będziemy wtedy mówić krótko, że h jest formą nieosobliwą oraz, że V jest nieosobliwa. Jeśli macierz $G(h,\mathcal{A})$ nie jest odwracalna, to mówimy, że przestrzeń dwuliniowa (V,h) (krócej: forma h/przestrzeń V) jest* OSOBLIWA*.*

Jeśli $h(v,w)=0$, dla każdych $v,w\in V$, to mówimy, że forma h (przestrzeń V) jest CAŁKOWICIE ZDEGENEROWANA*.*

Przykład: weźmy formę dwuliniową na $\mathbb{R}^4$ zadaną macierzą:

$$G(h;st) = \begin{bmatrix} 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}.$$

Wówczas przestrzeń dwuliniowa (V,h) jest nieosobliwa, ale na podprzestrzeni $W = \mathrm{lin}(\epsilon_1, \epsilon_2, \epsilon_3)$ forma $h|_W$ jest osobliwa. Podprzestrzeń $Z = \mathrm{lin}(\epsilon_1, \epsilon_2)$ jest natomiast całkowicie zdegenerowana względem h.

Fakt 148. *Niech (V,h) będzie przestrzenią dwuliniową. Następujące warunki są równoważne:*

(i) (V,h) jest nieosobliwa,

(ii) dla każdego niezerowego wektora $\alpha \in V$ istnieje wektor $\beta \in V$ taki, że $h(\alpha,\beta) \neq 0$.

Dowód. Załóżmy, że (V,h) jest nieosobliwa. Załóżmy, że dla pewnego niezerowego $\alpha \in V$ mamy $h(\alpha,\beta) = 0$, dla wszystkich $\beta \in V$. Wektor α dopełniamy do bazy $\mathcal{A}$ przestrzeni V postaci $(\alpha, \beta_1, \ldots, \beta_s)$. Wówczas $G(h,\mathcal{A})$ ma zerowy pierwszy wiersz i kolumnę, bo $h(\alpha,\alpha) = 0$ oraz $h(\alpha,\beta_i) = h(\beta_i,\alpha) = 0$, dla $i = 1,\ldots,s$. A zatem $G(h,\mathcal{A})$ jest osobliwa, sprzeczność. Na odwrót: załóżmy, że zachodzi (ii), ale dla pewnej bazy $\mathcal{A} = (\alpha_1,\ldots,\alpha_n)$ macierz $G(h;\mathcal{A})$ jest osobliwa. Oznacza to, że rząd tej macierzy nie jest maksymalny. A zatem kolumny tej macierzy są liniowo zależne, czyli istnieje wektor niezerowy $(x_1,\ldots,x_n) \in K^n$ taki, że:

$$x_1 \begin{bmatrix} h(\alpha_1,\alpha_1) \\ \vdots \\ h(\alpha_1,\alpha_n) \end{bmatrix} + x_2 \begin{bmatrix} h(\alpha_2,\alpha_1) \\ \vdots \\ h(\alpha_2,\alpha_n) \end{bmatrix} + \ldots + x_n \begin{bmatrix} h(\alpha_n,\alpha_1) \\ \vdots \\ h(\alpha_n,\alpha_n) \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Korzystając z liniowości formy dwuliniowej względem pierwszej zmiennej mamy zatem:

$$\begin{bmatrix} h(x_1\alpha_1 + x_2\alpha_2 + \ldots + x_n\alpha_n, \alpha_1) \\ \vdots \\ h(x_1\alpha_1 + x_2\alpha_2 + \ldots + x_n\alpha_n, \alpha_n) \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Niech $\alpha = x_1\alpha_1 + x_2\alpha_2 + \ldots + x_n\alpha_n$. Zauważmy, że skoro $h(\alpha,\alpha_i) = 0$, dla każdego $i = 1,\ldots,n$, to $h(\alpha,\beta) = 0$, dla każdego $\beta \in V$ (bo każde β jest sumą α_i). Skoro w (V,h) zachodzi (ii), to $\alpha = 0$. Ale α to kombinacja wektorów bazowych przestrzeni (V,h) o współczynnikach $x_1,\ldots,x_n$. A zatem $x_1 = \ldots = x_n = 0$, co przeczy wyborowi elementów x_i jako współczynników liniowej zależności kolumn $G(h;\mathcal{A})$. □

Fakt 149. *Każda przestrzeń euklidesowa jest nieosobliwa.*

Fakt 150. *Przestrzeń (V,h) jest osobliwa wtedy i tylko wtedy, gdy istnieje niezerowy wektor $\alpha \in V$ taki, że $h(\alpha,\beta)=0$, dla każdego $\beta \in V$.*

Definicja 105. *Niech (V,h) będzie przestrzenią dwuliniową.* RZĘDEM PRZESTRZENI *(V,h) (albo formy dwuliniowej h) nazywamy rząd macierzy $G(h;\mathcal{A})$ dla dowolnej bazy $\mathcal{A}$, oznaczany $r(V,h)$ lub $r(h)$.*

Fakt 151. *Przestrzeń dwuliniowa (V,h) jest nieosobliwa wtedy i tylko wtedy, gdy $r(V,h)=\dim V$.*

Problemy te są skutkiem poniższego faktu.

Fakt 152. *Niech (V,h) będzie przestrzenią dwuliniową nad ciałem K i niech W będzie podprzestrzenią przestrzeni V. Następujące warunki są równoważne:*

(1) $V = W \oplus W^{\perp}$,

(2) *W jest nieosobliwa.*

Dowód. Załóżmy, że $V = W \oplus W^{\perp}$. Mamy zatem $W \cap W^{\perp} = \{0\}$. Gdyby W była osobliwa to, na mocy wyników z poprzedniego wykładu, istniałby wektor $\alpha \in W$ taki, że dla każdego $\beta \in W$ mielibyśmy $h(\alpha,\beta)=0$. W szczególności $h(\alpha,\alpha)=0$, czyli $\alpha \in W^{\perp}$. A zatem $\alpha \in W \cap W^{\perp}$, sprzeczność.

Na odwrót: przypuśćmy, że przestrzeń W jest nieosobliwa. Mamy wykazać, że $V = W \oplus W^{\perp}$, czyli że dla każdego $\alpha \in V$ istnieją jednoznacznie wyznaczone wektory $\alpha' \in W$ oraz $\alpha'' \in W^{\perp}$ takie, że $\alpha = \alpha' + \alpha''$. Niech $\mathcal{A} = (\alpha_1,\ldots,\alpha_k)$ będzie bazą przestrzeni W. Istnienie i jednoznaczność wektora $\alpha' = x_1\alpha_1 + \ldots + x_k\alpha_k$ spełniającego powyższe warunki jest równoważne istnieniu i jednoznaczności współczynników $x_1,\ldots,x_k \in K$ takich, że $\alpha - (x_1\alpha_1 + \ldots + x_k\alpha_k) \in W^{\perp}$. Sprawdzenie czy jakiś wektor leży w $W^{\perp}$ jest równoważne sprawdzeniu, czy wektor ten jest prostopadły do każdego wektora z bazy W (na mocy liniowości h). A zatem teza (czyli (1)) jest równoważna temu, że zachodzi układ warunków

$$h(\alpha_j, \alpha - x_1\alpha_1 + \ldots + x_k\alpha_k) = 0, \text{ dla każdego } j = 1,\ldots,k,$$

czyli (1) równoważne jest, z liniowości h, istnieniu jednoznacznego rozwiązania $(x_1,\ldots,x_k)$ układu równań

$$\begin{cases} x_1h(\alpha_1,\alpha_1) + x_2h(\alpha_1,\alpha_2) + \ldots + x_kh(\alpha_1,\alpha_k) &= h(\alpha_1,\alpha) \\ x_1h(\alpha_2,\alpha_1) + x_2h(\alpha_2,\alpha_2) + \ldots + x_kh(\alpha_2,\alpha_k) &= h(\alpha_2,\alpha) \\ & \vdots \\ x_1h(\alpha_k,\alpha_1) + x_2h(\alpha_k,\alpha_2) + \ldots + x_kh(\alpha_k,\alpha_k) &= h(\alpha_k,\alpha) \end{cases}.$$

Macierzą współczynników tego (być może niejednorodnego) układu jest macierz $G(h|_W, \mathcal{A})$. Skoro W jest nieosobliwa, to macierz ta jest odwracalna, a zatem jej rząd wynosi k. Także rząd macierzy całego układu (rozmiarów $k \times k+1$) wynosi k, a zatem na mocy Twierdzenia Kroneckera-Capelliego układ ten ma dokładnie jedno rozwiązanie. To kończy dowód istnienia i jednoznaczności wektora α', a więc i α''. □

Układ ortogonalny złożony z dwóch egzemplarzy wektora izotropowego nie jest liniowo niezależny. Okazuje się, że jest to w zasadzie jedyna przeszkoda do tego, aby układy ortogonalne były liniowo niezależne.

Fakt 153. *Każdy układ prostopadły złożony z wektorów nieizotropowych jest liniowo niezależny.*

Dowód. Niech $\alpha_1, \ldots, \alpha_k$ będzie układem prostopadłym złożonym z wektorów nieizotropowych. Przypuśćmy, że dla pewnych $a_1, \ldots, a_k \in K$ mamy: $a_1\alpha_1 + a_2\alpha_2 + \ldots + a_k\alpha_k = 0$. Oczywiście dla każdej formy dwuliniowej na V oraz wektora $v \in V$ mamy $h(0, v) = h(v, 0) = 0$, bo $h(0, v) = 0 \cdot h(v, v) = 0$. A zatem dla każdego $j = 1, \ldots, k$ mamy:

$$\begin{aligned} 0 = h(0, \alpha_j) &= h(a_1\alpha_1 + a_2\alpha_2 + \ldots + a_k\alpha_k, \alpha_j) \\ &= a_1 h(\alpha_1, \alpha_j) + \ldots + a_j h(\alpha_j, \alpha_j) + \ldots + a_k h(\alpha_k, \alpha_j) \\ &= a_j h(\alpha_j, \alpha_j), \end{aligned}$$

bo $h(\alpha_i, \alpha_j) = 0$, dla $i \neq j$. Układ nasz składa się z wektorów nieizotropowych, czyli $h(\alpha_j, \alpha_j) \neq 0$, dla $j = 1, \ldots, k$. Z równości $0 = a_j h(\alpha_j, \alpha_j)$ dostajemy zatem $a_j = 0$, dla $j = 1, \ldots, k$, czyli liniową niezależność układu $\alpha_1, \ldots, \alpha_k$. □

Poprzednia uwaga mówi, że jeśli rozpinający przestrzeń dwuliniową (V, h) układ prostopadły złożony jest z wektorów nieizotropowych, to układ ten jest bazą V. Jest również jasne, że prostopadłość bazy przestrzeni dwuliniowej (V, h) można wyrazić przez macierz $G(h; \mathcal{A})$ formy h w tej bazie. Mianowicie: baza $\mathcal{A}$ jest prostopadła wtedy i tylko wtedy, gdy macierz $G(h; \mathcal{A})$ jest diagonalna.

Fakt 154. *Niech (V, h) będzie przestrzenią dwuliniową nad ciałem charakterystyki różnej od 2. Wówczas (V, h) ma bazę prostopadłą.*

Dowód. Stosujemy indukcję po V. Dla $\dim V = 1$ twierdzenie jest oczywiste. Załóżmy, że twierdzenie jest prawdziwe dla $\dim V = n - 1$. Dowodzimy dla $\dim V = n$.

- Przypadek 1. W przestrzeni V istnieje wektor nieizotropowy.

Niech $\alpha \in V$ będzie wektorem nieizotropowym. Rozpatrzmy przestrzeń $W = \mathrm{lin}(\alpha)$. Skoro α jest nieizotropowy, to W jest przestrzenią nieosobliwą. Stąd $V = W \oplus W^{\perp}$, na mocy wcześniejszego twierdzenia.

Zatem $\dim W^\perp = n-1$. Z założenia indukcyjnego zatem $W^\perp$ ma bazę prostopadłą. Oznaczmy ją przez $(\alpha_2, \ldots, \alpha_n)$. Wówczas $(\alpha, \alpha_2, \ldots, \alpha_n)$ jest bazą prostopadłą przestrzeni V.

- Przypadek 2. Wszystkie wektory przestrzeni V są izotropowe.

Dla każdych $\alpha, \beta \in V$ wektory $\alpha, \beta, \alpha+\beta$ są izotropowe, więc:

$$0 = h(\alpha+\beta, \alpha+\beta) = h(\alpha,\alpha) + 2h(\alpha,\beta) + h(\beta,\beta) = 2h(\alpha,\beta),$$

a stąd $h(\alpha,\beta) = 0$, bo $2 \neq 0$ w K (założenie o charakterystyce). Zatem wszystkie pary wektorów w przestrzeni V są prostopadłe, co oznacza, że każda baza V jest bazą prostopadłą.

□

Poniższe wnioski wprowadzają do dwóch kolejnych wykładów.

Fakt 155. *Nad ciałem charakterystyki różnej od* 2 *każda macierz symetryczna jest kongruentna do macierzy diagonalnej (będącej macierzą odpowiedniej formy w bazie diagonalnej).*

Fakt 156. *Nad ciałem charakterystyki różnej od* 2 *forma dwuliniowa symetryczna h na V wyznaczona jest jednoznacznie przez swoje wartości na parach (v,v), dla $v \in V$.*

Dowód powyższego twierdzenia daje nam także przepis na konstruowanie bazy prostopadłej dowolnej przestrzeni dwuliniowej (V,h) nad ciałem charakterystyki różnej od 2, zgodnie z poniższą procedurą.

- Szukaj w (V,h) wektora nieizotropowego. Jeśli nie ma takiego wektora, to wybierz dowolną bazę V i będzie ona prostopadła (por. Przypadek 2). Jeśli istnieje taki wektor α, to przejdź dalej.
- Podprzestrzeń $\operatorname{lin}(\alpha)$ jest nieosobliwa, więc $V = \operatorname{lin}(\alpha) \oplus \operatorname{lin}(\alpha)^\perp$ (por. Przypadek 1). A zatem dla znalezienia kolejnych wektorów bazy V powtórz wcześniejszy krok dla przestrzeni $\operatorname{lin}(\alpha)^\perp$.

Przykład. Znajdziemy bazę prostopadłą przestrzeni dwuliniowej $(\mathbb{R}^3, h)$, gdzie h jest zadana wzorem:

$$h((x_1,x_2,x_3),(y_1,y_2,y_3)) = x_1y_1 + x_1y_2 + x_2y_1 + 2x_2y_3 + 2x_3y_2 - 4x_3y_3.$$

Szukamy wektora nieizotropowego $\alpha_1 \in \mathbb{R}^3$. Możemy taki wektor zgadnąć, albo zapisać macierz $G(h;st)$ oraz $\alpha_1 = (x_1,x_2,x_3)$. Wówczas bycie wektorem nieizotropowym równoważne jest warunkowi:

$$\begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 2 \\ 0 & 2 & -4 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \neq 0.$$

Warunek ten spełnia na przykład $\alpha_1 = (1,0,0)$, bo $h(\alpha_1,\alpha_1) = 1$. Przechodzimy do kolejnego kroku. Opisujemy przestrzeń $\mathrm{lin}(\alpha_1)^\perp$ i sprawdzamy czy w niej jest jakiś wektor nieizotropowy. Przestrzeń $\mathrm{lin}(\alpha_1)^\perp$ składa się z wektorów $\beta = (y_1,y_2,y_3)$ spełniających równanie $h(\beta,\alpha_1) = 0$, a więc:

$$\mathrm{lin}(\alpha_1)^\perp = \{(y_1,y_2,y_3) \in \mathbb{R}^3 : y_1 + y_2 = 0\}.$$

W przestrzeni tej również istnieje wektor nieizotropowy, na przykład $\alpha_2 = (1,-1,0)$, bo $h(\alpha_2,\alpha_2) = -1$. A zatem przechodzimy do kolejnego kroku. Układ (α_1,α_2) chcemy dopełnić do bazy prostopadłej $\mathbb{R}^3$. Przestrzeń $\mathrm{lin}(\alpha_1,\alpha_2)^\perp$ opisujemy przez układ warunków (prostopadłość do α_1 oraz do α_2:

$$\mathrm{lin}(\alpha_1,\alpha_2)^\perp = \{(z_1,z_2,z_3) : z_1+z_2 = 0, z_2-2z_3 = 0\} = \mathrm{lin}((2,-2,-1)).$$

Wektor $(2,-2,1)$ jest izotropowy, a więc każdy wektor w $\mathrm{lin}(\alpha_1,\alpha_2)^\perp$ jest izotropowy. A zatem dowolny układ liniowo niezależny z tej przestrzeni dopełnia (α_1,α_2) do bazy $\mathbb{R}^3$. Tutaj potrzebowaliśmy tylko jednego wektora, ale teoretycznie już w poprzednim kroku mogliśmy trafić na przestrzeń mającą jedynie wektory izotropowe. A zatem bazą prostopadłą w $(\mathbb{R}^3,h)$ jest układ $((1,0,0),(1,-1,0),(2,-2,-1))$.

Powyższa procedura oparta była na dobieraniu do pojedynczego wektora nieizotropowego pewnego układu ortogonalnego. Nietrudno pokazać, że dowolny układ wektorów nieizotropowych przestrzeni dwuliniowej (V,h) można dopełnić do bazy ortogonalnej, o ile charakterystyka ciała bazowego nie jest równa 2.

Fakt 157. *Niech (V,h) będzie przestrzenią dwuliniową nad ciałem charakterystyki różnej od 2 wymiaru n. Niech $((\alpha_1,\ldots,\alpha_k))$ będzie układem prostopadłym złożonym z wektorów nieizotropowych, gdzie $k < n$. Wówczas istnieją w V wektory $\alpha_{k+1},\ldots,\alpha_n$ takie, że układ $(\alpha_1,\ldots,\alpha_n)$ jest bazą ortogonalną V.*

Dowód. Rozważmy przestrzeń $W = \mathrm{lin}(\alpha_1,\ldots,\alpha_k)$. Układ prostopadły $\mathcal{A} = (\alpha_1,\ldots,\alpha_k)$ złożony jest z wektorów nieizotropowych, a zatem jest to baza W. Macierz $G(h|_W,\mathcal{A})$ jest zatem diagonalna i na jej przekątnej stoją elementy niezerowe $h(\alpha_i,\alpha_i)$, dla $i = 1,\ldots,k$. Zatem macierz ta ma niezerowy wyznacznik. W szczególności W jest nieosobliwa i mamy rozkład $V = W \oplus W^\perp$. Na mocy poprzedniego twierdzenia, istnieje baza ortogonalna $W^\perp$ złożona z pewnych wektorów $\alpha_{k+1},\ldots,\alpha_n$. Układ $(\alpha_1,\ldots,\alpha_n)$ jest zatem bazą ortogonalną V. □

Na kolejnym wykładzie rozstrzygniemy problem kongruencji macierzy diagonalnych nad $\mathbb{R}$ i $\mathbb{C}$, co pozwoli na pełen opis macierzy symetrycznych (nad tymi ciałami) z dokładnością do kongruencji.

Kongruentność macierzy nad $\mathbb{R}$ oraz $\mathbb{C}$

Poprzedni wykład dotyczył znajdowania baz prostopadłych w przestrzeniach dwuliniowych. Kluczowy rezultat zapewnia istnienie takiej bazy dla każdej przestrzeni dwuliniowej nad ciałem charakterystyki różnej od 2. Wynik ten ma bardzo istotne skutki dla problemu znajdowania macierzy danej symetrycznej dwuliniowej formy h. Jeśli dodamy informację, że macierze kwadratowe $A, B \in M_n(K)$ są kongruentne tylko wtedy, gdy są macierzami pewnej formy dwuliniowej, otrzymamy kluczowy wniosek.

Fakt 158. *Nad ciałem charakterystyki $\neq 2$ każda macierz symetryczna jest kongruentna do macierzy diagonalnej.*

Naszym celem jest klasyfikacja symetrycznych macierzy nad ciałem K (na razie zakładamy tylko, że $\operatorname{char} K \neq 2$), które znajdują się w tej samej klasie kongruencji (nad K). Wiemy już, że każda macierz symetryczna jest w tej relacji z pewną macierzą diagonalną. Nad ciałami $\mathbb{R}$ oraz $\mathbb{C}$ możemy doprecyzować to twierdzenie do następującej postaci.

Fakt 159. *Niech (V, h) będzie przestrzenią dwuliniową nad ciałem K.*

(a) Jeśli $K = \mathbb{C}$, to istnieje taka baza prostopadła $(\alpha_1, \ldots, \alpha_n)$ przestrzeni V, że:

$$h(\alpha_i, \alpha_i) \in \{0, 1\}, \text{ dla } i = 1, \ldots, n.$$

Zatem dla $i, j = 1, \ldots, n$ mamy:

$$h(\alpha_i, \alpha_j) = \begin{cases} 0 \text{ lub } 1 & \text{gdy } i = j \\ 0 & \text{gdy } i \neq j. \end{cases}$$

(b) Jeśli $K = \mathbb{R}$, to istnieje taka baza prostopadła $(\alpha_1, \ldots, \alpha_n)$ przestrzeni V, że:

$$h(\alpha_i, \alpha_i) \in \{0, 1, -1\}, \text{ dla } i = 1, \ldots, n.$$

Zatem dla $i, j = 1, \ldots, n$ mamy:

$$h(\alpha_i, \alpha_j) = \begin{cases} 0, 1 \text{ lub } -1 & \text{gdy } i = j \\ 0 & \text{gdy } i \neq j. \end{cases}$$

Dowód. Zarówno w (a), jak i (b) mamy ciała charakterystyki różnej od 2, a zatem na mocy znanych nam już wyników istnieje baza prostopadła przestrzeni V, nazwijmy ją $(\beta_1, \ldots, \beta_n)$. Definiujemy następnie bazę $(\alpha_1, \ldots, \alpha_n)$ przestrzeni V przy pomocy warunków:

- $\alpha_i = \beta_i$, dla $h(\beta_i, \beta_i) = 0$,
- $\alpha_i = \frac{1}{a_i}\beta_i$, dla $h(\beta_i, \beta_i) \neq 0$,

przy czym dla $i = 1, \ldots, n$ element $a_i \in K$ jest:

- dowolną liczbą spełniającą $a_i^2 = h(\beta_i, \beta_i)$, dla $K = \mathbb{C}$,
- taki, że $a_i^2 = |h(\beta_i, \beta_i)|$, gdy $K \in \mathbb{R}$.

Wówczas w przypadku $h(\beta_i, \beta_i) \neq 0$ mamy

$$h(\alpha_i, \alpha_i) = h\left(\frac{1}{a_i}\beta_i, \frac{1}{a_i}\beta_i\right) = \frac{1}{a_i^2}h(\beta_i, \beta_i) = \begin{cases} 1, & \text{gdy } K = \mathbb{C}, \\ 1, -1 & \text{gdy } K = \mathbb{R}. \end{cases}$$

□

Fakt 160. *Każda niezerowa macierz symetryczna $A \in M_n(\mathbb{C})$ jest kongruentna (nad $\mathbb{C}$) do macierzy diagonalnej D_A, która ma na przekątnej k jedynek, potem $n - k$ zer, gdzie $k = r(A)$ czyli*

$$D_A = \begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{bmatrix}$$

Każda niezerowa macierz symetryczna $A \in M_n(\mathbb{R})$ jest kongruentna (nad $\mathbb{R}$) do takiej macierzy diagonalnej D_A, która ma na przekątnej k jedynek, potem s minus jedynek i wreszcie $n - k - s$ zer, gdzie $k + s = r(A)$, czyli

$$D_A = \begin{bmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & -1 & & & & \\ & & & & \ddots & & & \\ & & & & & -1 & & \\ & & & & & & 0 & \\ & & & & & & & \ddots \\ & & & & & & & & 0 \end{bmatrix}$$

Fakt 161. *Symetryczne macierze $A, B \in M_n(\mathbb{C})$ są kongruentne wtedy i tylko wtedy, gdy mają ten sam rząd. Istnieje więc $n+1$ klas kongruencji symetrycznych macierzy zespolonych $n \times n$.*

Dowód. Wykazaliśmy, że każda symetryczna macierz zespolona A jest kongruentna nad $\mathbb{C}$ do macierzy D_A mającej postać z Wniosku 1. Przy tym liczba jedynek występującej na przekątnej macierzy D_A równa jest $r(D_A)$, czyli też $r(A)$, bo macierze kongruentne muszą mieć identyczny rząd (jest to rząd odpowiadającej im formy). Zatem jeśli macierze symetryczne $A, B \in M_n(\mathbb{C})$ mają ten sam rząd k, to obie są kongruentne do tej samej macierzy 0-1-kowej z Wniosku 1. Stąd, z przechodniości relacji kongruencji, macierze A i B są kongruentne nad $\mathbb{C}$. Macierzy $n \times n$ postaci D_A opisanej we Wniosku 1 jest $n+1$, przy czym parami różne nie są kongruentne, bo mają różny rząd. Wynika stąd, że jest $n+1$ klas kongruencji symetrycznych macierzy zespolonych $n \times n$. □

Czego zatem dowiedzieliśmy się o każdej zespolonej symetrycznej formie dwuliniowej h na przestrzeni V? Otóż można do niej dobrać bazę prostopadłą V taką, że forma h obcięta do podprzestrzeni rozpiętej przez pierwszych $r(h)$ wektorów tej bazy jest dodatnio określona. Zachowuje się ona na tej podprzestrzeni „w zasadzie jak" iloczyn skalarny. Jesteśmy wprawdzie nad $\mathbb{C}$, ale dla tej podprzestrzeni te $r(h)$ wektorów rozpinających to jest właściwie „baza ortonormalna", której nie da się w przestrzeniach dwuliniowych często wyznaczyć (co innego z bazą ortogonalną). Na prostopadłej podprzestrzeni rozpiętej przez pozostałe $\dim V - r(h)$ wektorów (izotropowych) forma jest całkowicie zdegenerowana – zabija wszystko. A więc symetryczne formy dwuliniowe nad $\mathbb{C}$ można oglądać „lokalnie" obcinając je do dwóch podprzestrzeni. Patrząc na każde obcięcie z osobna całkowicie rozumiemy co się w podprzestrzeni dzieje (z formą) i w łatwy sposób umiemy „skleić" obcięcia do pełnego opisu. Ta sama idea, tylko dotycząca „sklejania" endomorfizmu z jego obcięć do podprzestrzeni niezmienniczych leży u podstaw twierdzenia Jordana.

Fakt 162 (Twierdzenie Sylvestera o bezwładności)**.** *Niech $\mathcal{A} = (\alpha_1, \ldots, \alpha_n)$ oraz $\mathcal{B} = (\beta_1, \ldots, \beta_n)$ będą bazami prostopadłymi przestrzeni dwuliniowej (V, h) nad ciałem $\mathbb{R}$. Oznaczmy:*

- $r_+(\mathcal{A}) =$ *liczba takich* $1 \leq i \leq n$, *że* $h(\alpha_i, \alpha_i) > 0$,
- $r_-(\mathcal{A}) =$ *liczba takich* $1 \leq i \leq n$, *że* $h(\alpha_i, \alpha_i) < 0$,
- $r_+(\mathcal{B}) =$ *liczba takich* $1 \leq i \leq n$, *że* $h(\beta_i, \beta_i) > 0$,
- $r_-(\mathcal{B}) =$ *liczba takich* $1 \leq i \leq n$, *że* $h(\beta_i, \beta_i) < 0$.

Wówczas

$$r_+(\mathcal{A}) = r_+(\mathcal{B}) \quad \text{oraz} \quad r_-(\mathcal{A}) = r_-(\mathcal{B}).$$

Ponadto $r_+(\mathcal{A}) + r_-(\mathcal{A}) = r(h) = r_+(\mathcal{B}) + r_-(\mathcal{B})$.

Dowód. Definiujemy następujące trójki podprzestrzeni V rozpiętych przez elementy bazowe z $\mathcal{A}$, $\mathcal{B}$:

$$\begin{aligned} V_+ &= \operatorname{lin}(\alpha_i \,|\, h(\alpha_i,\alpha_i) > 0), \quad W_+ = \operatorname{lin}(\beta_i \,|\, h(\beta_i,\beta_i) > 0),\\ V_- &= \operatorname{lin}(\alpha_i \,|\, h(\alpha_i,\alpha_i) < 0), \quad V_0 = \operatorname{lin}(\alpha_i \,|\, h(\alpha_i,\alpha_i) = 0),\\ W_- &= \operatorname{lin}(\beta_i \,|\, h(\beta_i,\beta_i) < 0), \quad W_0 = \operatorname{lin}(\beta_i \,|\, h(\beta_i,\beta_i) = 0). \end{aligned}$$

Jest jasne, że

$$r_+(\mathcal{A}) = \dim V_+, r_-(\mathcal{A}) = \dim V_-, r_+(\mathcal{B}) = \dim W_+, r_-(\mathcal{B}) = \dim W_-.$$

Co więcej

$$V_+ \oplus V_- \oplus V_0 = V = W_+ \oplus W_- \oplus W_0,$$

skąd

$$\dim V_+ + \dim V_- + \dim V_0 = \dim V = \dim W_+ + \dim W_- + \dim W_0.$$

Przy tym

$$\dim V_+ + \dim V_- = r(h) = \dim W_+ + \dim W_-,$$

co daje

$$r_+(\mathcal{A}) + r_-(\mathcal{A}) = r(h) = r_+(\mathcal{B}) + r_-(\mathcal{B}),$$

co stanowi drugą część tezy.

Po prostu wektor przestrzeni V jest kombinacją liniową wektorów z V_+, V_-, V_0, a przestrzenie te nie tylko mają zerowe przecięcie, ale każda z nich przecina się jedynie na zerze z sumą dwóch pozostałych. Stąd też wynika natychmiast, że wymiar sumy prostej trzech podprzestrzeni równy jest sumie wymiarów poszczególnych składników. Analogicznie dla rozkładu $V = W_+ \oplus W_- \oplus W_0$.

Dowodzimy, że $r_+(\mathcal{A}) = r_+(\mathcal{B})$. Zaczniemy od pokazania tego, że $V_+ \cap (W_- + W_0) = \{0\}$. Otóż

- dla każdego niezerowego wektora $\alpha \in V_+$ mamy
$$h(\alpha,\alpha) = h(\sum a_i\alpha_i, \sum a_i\alpha_i) = \sum a_i^2 h(\alpha_i,\alpha_i) > 0,$$
- dla każdego wektora $\beta \in W_-$ mamy
$$h(\beta,\beta) = h(\sum b_i\beta_i, \sum b_i\beta_i) = \sum b_i^2 h(\beta_i,\beta_i) \leq 0.$$

A zatem dla każdego $\delta = \beta + \gamma$, gdzie $\beta \in W_-, \gamma \in W_0$ zachodzi:

$$h(\delta,\delta) = h(\beta+\gamma,\beta+\gamma) = h(\beta,\beta) + 2h(\beta,\gamma) + h(\gamma,\gamma) = h(\beta,\beta) + 0 + 0 \leq 0.$$

A zatem $V_+ \cap (W_- + W_0) = \{0\}$, a stąd

$$\dim V_+ + \dim(W_- + W_0) = \dim(V_+ + W_- + W_0) \leq \dim V.$$

Korzystając z $\dim(W_- + W_0) = \dim W_- + \dim W_0 = \dim V - \dim V_+$, możemy powyższą nierówność przepisać w postaci

$$\dim V_+ + \dim V - \dim W_+ \leq \dim V.$$

W rezultacie dostajemy $\dim V_+ \leq \dim W_+$. Tak samo dowodzimy, że $\dim W_+ \leq \dim V_+$, co daje łącznie $\dim V_+ = \dim W_+$. Korzystając z tej równości i równości udowodnionej w pierwszej części tezy mamy też $\dim V_- = \dim W_-$. Dowód jest zakończony. □

Definicja 106. *Niech (V,h) będzie przestrzenią dwuliniową nad ciałem $\mathbb{R}$.* SYGNATURĄ PRZESTRZENI *(V,h) (albo formy dwuliniowej h) nazywamy liczbę $r_+(\mathcal{A}) - r_-(\mathcal{A})$ z poprzedniego twierdzenia. Sygnaturę oznaczamy $s(V,h)$ lub $s(h)$. Twierdzenie pokazuje, że jest ona dobrze określona (nie zależy od wyboru bazy prostopadłej $\mathcal{A}$).*

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 macierzą $G(h;st) = A$. Sygnaturę macierzy A oznaczamy $s(A)$. Więc $s(A)$ równa jest różnicy liczby dodatnich oraz liczby ujemnych wyrazów na przekątnej w macierzy diagonalnej kongruentnej (nad $\mathbb{R}$) do macierzy A.*

Przed nami kluczowy wniosek określający postaci kanoniczne kongruencji (nad $\mathbb{R}$) w zbiorze $M_n(\mathbb{R})$.

Fakt 163. *Symetryczne macierze $A, B \in M_n(\mathbb{R})$ są kongruentne (nad $\mathbb{R}$) wtedy i tylko wtedy, gdy mają równe rzędy i sygnatury, tzn. $r(A) = r(B)$ oraz $s(A) = s(B)$. Istnieje $(n+1)(n+2)/2$ klas kongruencji symetrycznych macierzy rzeczywistych $n \times n$.*

Dowód. Rozumowanie jest takie samo jak w przypadku analogicznej charakteryzacji kongruencji symetrycznych macierzy zespolonych. Każda rzeczywista macierz symetryczna A jest kongruentna nad $\mathbb{R}$ do macierzy diagonalnej D_A opisanej we Wniosku 2. Macierzy takich jest $(n+1)(n+2)/2$ przy czym parami różne z nich nie są kongruentne nad $\mathbb{R}$, bo mają różne rzędy lub sygnatury. □

Dokonaliśmy klasyfikacji macierzy kongruentnych dla macierzy nad ciałami $\mathbb{C}$ i $\mathbb{R}$. Dla jakich ciał istnieją analogiczne klasyfikacje? Nietrudno zobaczyć, że można zamienić $\mathbb{C}$ na dowolne ciało algebraicznie domknięte. Ciało $\mathbb{R}$ można zamienić na tzw. ciało kwadratowo domknięte (musimy umieć wyciągać pierwiastki kwadratowe z każdego elementu), w którym każda liczba jest, modulo pewien kwadrat, elementem 1 lub -1. w dodatku pokażemy analog kryterium Sylvestera, które pozwala w wielu sytuacjach określać macierz diagonalną kongruentną do danej za pomocą głównych minorów wiodących.

Twierdzenie Sylvestera o bezwładności jest punktem wyjścia do mówienia o określoności form kwadratowych. Temat ten, niezwykle istotny dla zastosowań, omówimy następnym razem, zamykając tym samym teorię przestrzeni liniowych na tym wykładzie. Teoria wymiernych form dwuliniowych jest znacznie bardziej skomplikowana i przekracza ramy tego wykładu.

Uzupełnienie. Twierdzenie Jacobiego

W niektórych sytuacjach możliwe jest określenie (nad dowolnym ciałem) macierzy diagonalnej, do której kongruentna jest dana macierz.

Fakt 164 (Twierdzenie Jacobiego)**.** *Niech (V,h) będzie taką przestrzenią dwuliniową nad ciałem charakterystyki różnej od 2, 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*

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

Założenie o charakterystyce nie jest potrzebne – to twierdzenie jest prawdziwe nad każdym ciałem. W dowodzie korzystamy jednak z rozkładu $V = W \oplus W^{\perp}$, dla podprzestrzeni nieosobliwej V.

Dowód. Rozumowanie jest indukcją ze względu na n. Załóżmy, że istnieje baza $\mathcal{C} = (\gamma_1,\ldots,\gamma_n)$ przestrzeni V, że:

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

Skoro $W = \operatorname{lin}(\gamma_1,\ldots,\gamma_{n-1})$ 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 istnieje baza $\mathcal{B}$ przestrzeni V taka, 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 $C = M(\mathrm{id})_{\mathcal{C}}^{\mathcal{A}}$ 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, że istnieje baza $\mathcal{C} = (\gamma_1,\ldots,\gamma_n)$ przestrzeni V, że:

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

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

Trivia. Sygnatura, a geometria elementarna

W 1866 roku G. Darboux zdefiniował potęgę pary okręgów C_1, C_2, czyli:

$$C_1 * C_2 = d^2 - r_1^2 - r_2^2,$$

gdzie r_1, r_2 to promienie okręgów C_1, C_2, a d to odległość pomiędzy ich środkami. Jeśli okręgi się przecinają, wówczas $C_1 * C_2 = r_1 r_2 \cos\theta$, gdzie θ jest kątem pomiędzy okręgami. Jeśli okręgi są rozłączne, wówczas $C_1 * C_2$ równy jest kwadratowi długości odcinka narysowanego niżej.

Źródło: J. Kocik, *A theorem on circle configurations*.

Zbiór punktów na okręgu o promieniu r i środku (f, g) ma postać:

$$x^2 + y^2 - 2fx - 2gy + k = 0 \qquad (\spadesuit)$$

gdzie $k = f^2 + g^2 - r^2$. W roku 1883 H. Cox zapisał produkt Darboux dwóch okręgów o środkach (f_1, g_1), (f_2, g_2) i promieniach r_1, r_2, odpowiednio, w języku współczynników równań ($\spadesuit$):

$$C_1 * C_2 = k_1 + k_2 - 2f_1 f_2 - 2g_1 g_2.$$

W 1970 roku D. Pedoe zorientował się, że powyższą równość można interpretować jako... formę dwuliniową $\langle\ ,\ \rangle$ w przestrzeni $\mathbb{R}^4$. Pomysł jest *rzutowy* w naturze: równanie ($\spadesuit$) można przeskalować do równania postaci: $a(x^2 + y^2) - 2bx - 2cy + d = 0$ i określić (dla tak opisanych okręgów):

$$\langle C_1, C_2 \rangle = b_1 b_2 + c_1 c_2 - \frac{d_1 a_1 + d_2 a_2}{2}.$$

O co tu chodzi? Każdemu okręgowi opisanemu w $\mathbb{R}^2$ równaniem:

$$a(x^2 + y^2) - 2bx - 2cy + d = 0, \quad a \neq 0.$$

przypisujemy wektor $C(a, b, c, d) \in \mathbb{R}^4$. Każda niezerowa wielokrotność tego wektora reprezentuje ten sam okrąg , a więc możemy ograniczyć się do znormalizowanego równania opisującego C:

$$x^2 + y^2 - 2fx - 2gy + k = 0$$

i związanego z nim wektora współrzędnych $C(1, f, g, k)$.

Na $\mathbb{R}^4$ wprowadzamy strukturę przestrzeni dwuliniowej Minkowskiego (o wielkim znaczeniu w fizyce) poprzez zadanie formy dwuliniowej $\langle\ ,\ \rangle$ danej macierzą:

$$G(\langle,\rangle, st) = \begin{bmatrix} 0 & 0 & 0 & -\frac{1}{2} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -\frac{1}{2} & 0 & 0 & 0 \end{bmatrix},$$

i widzimy, że teraz rzeczywiście dla okręgów opisanych równaniami

$$a(x^2 + y^2) - 2bx - 2cy + d = 0$$

określić można wektory $(a, b, c, d) \in \mathbb{R}^4$ i wtedy

$$\langle C_1, C_2\rangle = b_1b_2 + c_1c_2 - \frac{d_1a_2 + d_2a_1}{2}$$

Zauważmy też, że sens geometryczny mają także wektory (a, b, c, d), gdzie $a = 0$:

• jeśli $a = 0$ oraz $b^2 + c^2 > 0$, to równanie *okręgu* opisuje prostą na płaszczyźnie, której można przypisać wektor

$$L(0, b, c, d),$$

• dla $a = b = c = 0$ praz $d \neq 0$ żadne punkty nie spełniają tego równania i można utożsamić je z prostą niewłaściwą o współrzędnych

$$E(0, 0, 0, d).$$

Następujące fakty są prostymi ćwiczeniami:

(i) $\langle C_1, C_1\rangle = r_1^2$,

(ii) $\langle C_1, C_2\rangle = 0$ wtedy i tylko wtedy, gdy okręgi C_1, C_2 są ortogonalne.

(iii) $\langle C_1, C_2\rangle \pm r_1r_2$ wtedy i tylko wtedy, gdy C_1, C_2 są styczne,

(iv) Jeśli C_1 jest punktem, czyli $r_1^2 = 0$, to $\langle C_1, C_2\rangle$ równe jest minus potędze punktu C_1 względem okręgu C_2,

(v) punkt C_1 leży na okręgu C_2 wtedy i tylko wtedy, gdy $\langle C_1, C_2\rangle = 0$,

(vi) jeśli C_1, C_2 są punktami, to $\langle C_1, C_2\rangle = -d^2/2$, gdzie $d = \rho(C_1, C_2)$,

(vii) $\langle C_1, L_2\rangle = -D$ jest skierowaną odległością od środka C_1 do L_2,

(viii) prosta L_2 przechodzi przez środek C_1 wtedy i tylko wtedy, gdy $\langle L_2, C_1\rangle = 0$,

(ix) jeśli E to prosta w nieskończoności, to $\langle C_1, E\rangle = -1/2$,

(x) wszystkie proste właściwe są prostopadłe do prostej w nieskończoności (zwanej też prostą niewłaściwą).

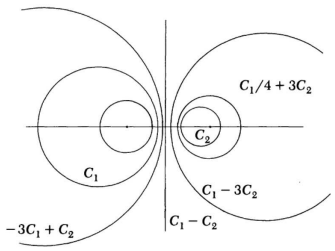
Niech $C_1(1, f_1, g_1, k_1), C_2(1, f_2, g_2, k_2)$ będą dwoma okręgami. Dla dowolnych $a_1, a_2 \in \mathbb{R}$, $a_1 + a_2 \neq 0$, określamy: $C = a_1C_1 + a_2C_2/(a_1 + a_2)$, czyli okrąg o środku:

$$\left(\frac{a_1f_1 + a_2f_2}{a_1 + a_2}, \frac{a_1g_1 + a_2g_2}{a_1 + a_2}\right).$$

Jeśli $a_1 + a_2 = 0$, to zbiór $C = a_1C_1 + a_2C_2$ jest prostą, zwaną **prostą potęgową** okręgów C_1, C_2, zaś zbiór okręgów

$$C = a_1C_1 + a_2C_2$$

(gdzie $a_1 \neq 0$ lub $a_2 \neq 0$) nazywamy **współosiowym pękiem okręgów**. Zbiór ten odpowiada $\text{lin}(C_1, C_2)$ w przestrzeni $\mathbb{R}^4$.

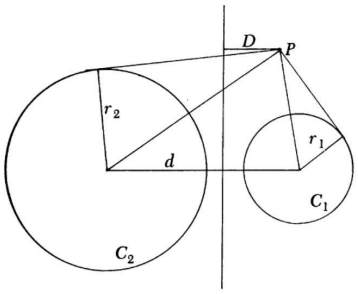


Źródło rysunków: R. Pfiefer, C. Van Hook, *Circles, Vectors, and Linear Algebra.*

Fakt 165. *Dla każdego punktu P oraz okręgów C_1, C_2 niech D będzie odległością od P do osi potęgowej $C_1 - C_2$ i niech d będzie odległością pomiędzy środkami C_1, C_2. Wówczas:*

$$2Dd = (d_1^2 - r_1^2) - (d_2^2 - r_2^2),$$

jest różnicą potęg punktu P względem C_1 i C_2.



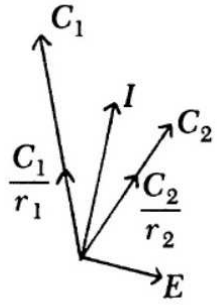
Dowód. Na mocy własności (vii) oraz (iv) mamy:

$$-D = \langle P, \frac{C_1 - C_2}{d}\rangle = (\langle P, C_1\rangle - \langle P, C_2\rangle)/d = (-(d_1^2 - r_1^2) + (d_2^2 - r_2^2))/2d.$$

Dwusieczne. Skoro $\langle C, C\rangle = r^2$, to dla okręgów C_1, C_2 o promieniach r_1, r_2 można określić wektory jednostkowe $C_1/r_1, C_2/r_2$. Przez analogię do zwykłych wektorów w przestrzeni euklidesowej można określić

$$I = C_1/r_1 + C_2/r_2, \quad E = C_1/r_1 - C_2/r_2.$$

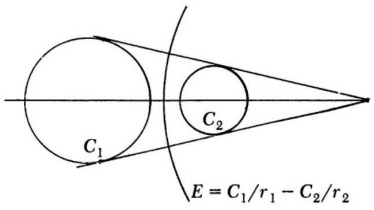
jako nazywane **wewnętrznym i zewnętrznym okręgiem antypodobieństwa** okręgów C_1, C_2. Z punktów (viii), (ix) dowodzi się łatwo, że środki I oraz E leżą w punktach, w których przecinają się odpowiednio wewnętrzne i zewnętrzne wspólne styczne do C_1, C_2 (dla prostych są to: **dwusieczna wewnętrzna i zewnętrzna**!).



Inwersja. W przestrzeni dwuliniowej odbicie u' wektora U względem V (lub równolegle do V) dane jest formułą:

$$U' = \pm\frac{2\langle U, V\rangle}{\langle V, V\rangle}V \mp U.$$

i jak się okazuje w języku rozważanego iloczynu skalarnego U' jest obrazem inwersyjnym okręgu U względem okręgu V. Dla przykładu, odbicie wektora C_1 względem wektorów I, E daje wektory $C_2, -C_2$ (z dokładnością do skalarnej wielokrotności), więc inwersja C_1 w okręgach I, E daje okrąg C_2.



Liniowa niezależność. Okręgi C_i są liniowo niezależne jeśli

$$\sum x_i C_i = 0$$

wtedy i tylko wtedy, gdy $x_i = 0$, dla wszystkich i. W szczególności trzy okręgi są liniowo niezależne jeśli żaden nie leży w pęku współosiowym pozostałych dwóch.

Fakt 166 (Tw. Menelaosa)**.** *Dane są trzy liniowo niezależne okręgi C_1, C_2, C_3. Jeśli*

$$D_1 = a_1 C_2 + b_1 C_3, \quad D_2 = a_2 C_3 + b_2 C_1, \quad D_3 = a_3 C_1 + b_3 C_2,$$

wówczas D_1, D_2, D_3 są zależne (w tym samym pęku współosiowym) wtedy i tylko wtedy, gdy

$$a_1 a_2 a_3 = -b_1 b_2 b_3.$$

Dowód. Istnieją niezerowe x_i spełniające $\sum x_i D_i = 0$ wtedy i tylko wtedy, gdy poniższy układ ma niezerowe rozwiązanie:

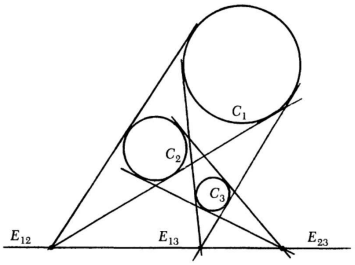
$$\begin{bmatrix} 0 & b_2 & a_3 \\ a_1 & 0 & b_3 \\ b_1 & a_2 & 0 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

□

Fakt 167 (Tw. Monge'a)**.** *Niech C_1, C_2, C_3 będą liniowo niezależnymi okręgami i niech I_{ij}, E_{ij} będą wewnętrznymi i zewnętrznymi okręgami antypodobieństwa dla C_i oraz C_j. Wówczas każdy z czterech układów okręgów jest liniowo zależny (czyli współpękowy):*

$$\{E_{12}, E_{23}, E_{31}\}, \{E_{12}, I_{23}, I_{31}\}, \{I_{12}, E_{23}, I_{31}\}, \{I_{12}, I_{23}, E_{31}\}.$$

W szczególności środki okręgów w każdym układzie są współliniowe.

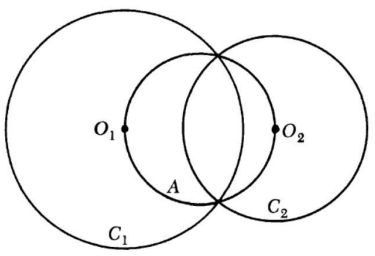


Fakt 168. *Niech C_1 będzie ortogonalny do C_2 i niech okręgi te mają środki O_1, O_2. Rozważmy **okrąg średni** postaci:*

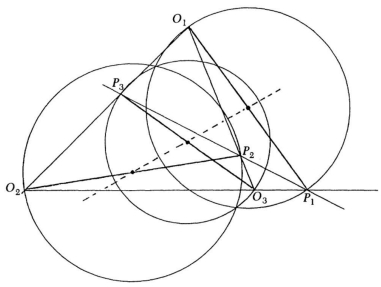
$$A = \frac{C_1 + C_2}{2}.$$

Wówczas O_1O_2 to średnica A, ponieważ (patrz (ix)):

$$\langle O_i, C_i \rangle = r_i^2/2, \quad \langle O_i, C_j \rangle = -r_i^2/2 \quad \Rightarrow \langle O_i, A \rangle = 0.$$



Fakt 169. *Niech C_1, C_2, C_3 będą trzema wzajemnie prostopadłymi okręgami o środkach O_1, O_2, O_3. Załóżmy, że (znormalizowane) okręgi D_1, D_2, D_3 zdefiniowane jak w twierdzeniu Menelaosa, o środkach P_1, P_2, P_3 są zależne i niech A_i będą średnimi okręgami okręgów C_i oraz D_i. Wówczas okręgi A_1, A_2, A_3 są zależne (uzyskujemy m.in. tw. Gaussa-Bodenmillera czy tw. Newtona).*



Dysponując liniowo zależnym układem wektorów $\sum x_i V_i = 0$ i biorąc formę $\langle\ ,\ \rangle$ z każdym z wektorów W_i widzimy, że istnieje niezerowe rozwiązanie układu:

$$\begin{bmatrix} \langle W_1, V_1\rangle & \dots & \langle W_1, V_1\rangle \\ \vdots & & \vdots \\ \langle W_n, V_n\rangle & \dots & \langle W_n, V_n\rangle \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Dla $W_i = V_i$ widzimy, że wyznacznik Grama tego układu jest zerowy.

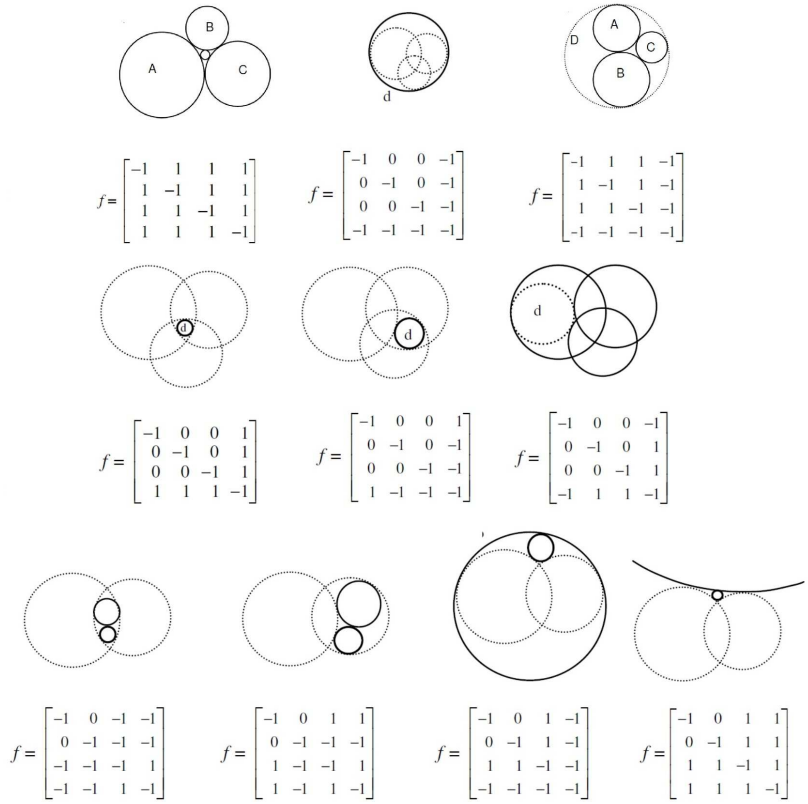
• **Wniosek 1.** Nie istnieją cztery parami prostopadłe okręgi na płaszczyźnie - twierdzenie o bezwładności!

• **Wniosek 2**. Biorąc układ czterech parami stycznych zewnętrznie okręgów $C_1, .C_2, C_3, C_4$ o promieniach r_1, r_2, r_3, r_4 oraz $C_5 = E$ warunek $W(C_i) = 0$ implikuje słynne twierdzenie Kartezjusza o okręgach:

$$\frac{1}{r_1^2} + \frac{1}{r_2^2} + \frac{1}{r_3^2} + \frac{1}{r_4^2} = \frac{1}{r_1 r_2} + \frac{1}{r_1 r_3} + \frac{1}{r_1 r_4} + \frac{1}{r_2 r_3} + \frac{1}{r_2 r_4} + \frac{1}{r_3 r_4}.$$

Macierze Grama układów okręgów stycznych w różnych dopuszczalnych konfiguracjach.

W cytowanej pracy iloczyn skalarny jest z przeciwnym znakiem niż u nas, czyli $\langle C_1, C_2\rangle = (d_1 a_1 + d_2 a_2)/2 - b_1 b_2 - c_1 c_2$ i rozważa się go jedynie na czwórkach wektorów jednostkowych (można, po odpowiednim przeskalowaniu).



Formy kwadratowe

Definicja 107. *Niech V będzie przestrzenią liniową nad ciałem K. Funkcję $q : V \to K$ nazywamy* FORMĄ KWADRATOWĄ NA PRZESTRZENI *V, jeśli istnieje forma dwuliniowa $h : V \times V \to K$ taka, że dla każdego $\alpha \in V$ zachodzi*

$$q(\alpha) = h(\alpha, \alpha).$$

Fakt 170. *Niech V będzie skończenie wymiarową przestrzenią liniową nad K i niech $(\alpha_1, \ldots, \alpha_n)$ będzie bazą przestrzeni V. Następujące warunki są równoważne.*

- *funkcja $q : V \to K$ jest formą kwadratową na przestrzeni V,*
- *istnieją elementy $a_{ij} \in K$, dla $i, j = 1, \ldots, n$ takie, że dla każdych skalarów $x_1, \ldots, x_n$ z ciała K zachodzi równość:*

$$q(x_1\alpha_1 + \ldots + x_n\alpha_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j.$$

Dowód. Niech $q(\alpha) = h(\alpha, \alpha)$, dla pewnej formy dwuliniowej h na V. Niech $a_{ij} = h(\alpha_i, \alpha_j)$, dla $i, j = 1, \ldots, n$. Dla $x_1, \ldots, x_n$, $y_1, \ldots, y_n \in K$ mamy:

$$h(x_1\alpha_1 + \ldots + x_n\alpha_n, y_1\alpha_1 + \ldots + y_n\alpha_n) = \sum_{i,j=1}^{n} a_{ij}x_iy_j,$$

a więc w szczególności $q(x_1\alpha_1 + \ldots + x_n\alpha_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j$.

Na odwrót: mając $q(x_1\alpha_1 + \ldots + x_n\alpha_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j$. dla każdych $x_1, \ldots, x_n \in K$ zadajemy formę dwuliniową h wzorem

$$h(x_1\alpha_1 + \ldots + x_n\alpha_n, y_1\alpha_1 + \ldots + y_n\alpha_n) = \sum_{i,j=1}^{n} a_{ij}x_iy_j.$$

Wówczas dla każdego $\alpha = x_1\alpha_1 + \ldots + x_n\alpha_n$ mamy $h(\alpha, \alpha) = q(\alpha)$. □

Przyjmując $b_{ii} = a_{ii}$ dla $i = 1, \ldots, n$ oraz $b_{ij} = a_{ij} + a_{ji}$ dla $1 \leq i, j \leq n$ w powyższej uwadze możemy ją przeformułować następująco.

Fakt 171. *Niech V będzie skończenie wymiarową przestrzenią liniową nad K i niech $(\alpha_1, \ldots, \alpha_n)$ będzie bazą przestrzeni V. Wówczas funkcja $q : V \to K$ jest formą kwadratową na przestrzeni V wtedy i tylko wtedy, gdy istnieją elementy $b_{ij} \in K$, dla $i, j = 1, \ldots, n$ takie, że dla każdych $x_1, \ldots, x_n \in K$:*

$$q(x_1\alpha_1 + \ldots + x_n\alpha_n) = \sum_{1 \leq i \leq j \leq n} b_{ij} x_i x_j.$$

Rozważmy kilka przykładów.

- Każda forma kwadratowa na przestrzeni K^n jest postaci:

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

na przykład

$$q_1((x_1, x_2)) = 2x_1^2 + 3x_1x_2 - 5x_3^2$$
$$q_2((x_1, x_2, x_3)) = x_1^2 + 4x_1x_2 + 7x_2^2 - 6x_2x_3 + 3x_3^2.$$

- Jeśli $q : V \to K$ jest formą kwadratową na przestrzeni V, to dla każdej podprzestrzeni liniowej $W \subseteq V$ funkcja $q|_W : W \to K$, zadana jako $q|_W(\alpha) = q(w)$ dla każdego $\alpha \in W$, jest formą kwadratową na przestrzeni W.

Definicja 108. *Niech $q : V \to K$ będzie formą kwadratową.* Postacią diagonalną formy kwadratowej *q nazwiemy przedstawienie jej w formie:*

$$q(x_1\alpha_1 + \ldots + x_n\alpha_n) = a_1x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2,$$

gdzie $(\alpha_1, \ldots, \alpha_n)$ jest pewną bazą przestrzeni V oraz $a_1, \ldots, a_n \in K$.

Przykład. Niech

$$q((x_1, x_2, x_3, x_4)) = x_1^2 + 8x_1x_2 + 7x_2^2 + 2x_3x_4.$$

Forma q określona jest na $\mathbb{R}^4$, a zapisany wzór oparty jest o współrzędne wektora w bazie standardowej. Rozważmy bazę $\alpha_1 = (1, 0, 0, 0)$, $\alpha_2 = (4, -1, 0, 0)$, $\alpha_3 = (0, 0, 1, 1)$, $\alpha_4 = (0, 0, 1, -1)$. Jest to baza ortogonalna w $(\mathbb{R}^4, h)$, gdzie h jest symetryczna i $h(\alpha, \alpha) = q(\alpha)$, dla każdego α (to wyjaśnię niżej). Wówczas forma q zapisywać się będzie wzorem:

$$q((y_1\alpha_1 + y_2\alpha_2 + y_3\alpha_3 + y_4\alpha_4)) = y_1^2 - 9y_2^2 + 2y_3^2 - 2y_4^2.$$

Chcemy mieć narzędzia do rozróżniania określoności (zawsze diagonalizowalnych) form rzeczywistych, a dla dowolnego ciała – do diagonalizacji form kwadratowych i do stwierdzania kiedy ta ostatnia jest możliwa. Dla ciał charakterystyki różnej od 2 istnieje bardzo bliski związek pomiędzy formami kwadratowymi i symetrycznymi formami dwuliniowymi. Mówi o tym następujące stwierdzenie.

Fakt 172. *Niech V będzie przestrzenią liniową nad ciałem K charakterystyki różnej od 2. Jeśli $q : V \to K$ jest formą kwadratową, to istnieje dokładnie jedna forma dwuliniowa symetryczna $h : V \to K$ taka, że dla każdego $\alpha \in V$ zachodzi $q(\alpha) = h(\alpha, \alpha)$. Dokładniej, dla ciała charakterystyki różnej od 2 przyporządkowania:*

- $h \mapsto q$, *gdzie* $q(\alpha) = h(\alpha, \alpha)$, *dla każdego* $\alpha \in V$,
- $q \mapsto h$, *gdzie* $h(\alpha, \beta) = \frac{1}{2}\left(q(\alpha + \beta) - q(\alpha) - q(\beta)\right)$

zadają bijekcje pomiędzy formami dwuliniowymi symetrycznymi na przestrzeni V a formami kwadratowymi na przestrzeni V.

Zanim zobaczymy dowód zobaczmy krótki przykład. Weźmy formę kwadratową $q : \mathbb{R}^2 \to \mathbb{R}$ daną wzorem

$$q((x_1, x_2)) = 3x_1^2 - 4x_2^2 + 6x_1x_2.$$

Istnieje naturalnie wiele form dwuliniowych $h : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$ takich, że $q(\alpha) = h(\alpha, \alpha)$, dla każdego $\alpha \in V$, na przykład

$$h((x_1, x_2), (y_1, y_2)) = 3x_1y_1 + 2x_1y_2 + 4x_2y_1 - 4x_2y_2$$

lub

$$h((x_1, x_2), (y_1, y_2)) = 3x_1y_1 + 6x_1y_2 - 4x_2y_2.$$

ale istnieje wśród nich tylko jedna forma dwuliniowa symetryczna, mianowicie

$$h((x_1, x_2), (y_1, y_2)) = 3x_1y_1 + 3x_1y_2 + 3x_2y_1 - 4x_2y_2.$$

Dowód. Niech $h' : V \times V \to K$ będzie dowolną formą dwuliniową taką, że dla każdego $\alpha \in V$ zachodzi $q(\alpha) = h'(\alpha, \alpha)$. Wówczas funkcja $h : V \times V \to K$ zadana warunkami $h(\alpha, \beta) = \frac{1}{2}(h'(\alpha, \beta) + h'(\beta, \alpha))$ jest formą dwuliniową symetryczną na przestrzeni V i mamy równość $q(\alpha) = h'(\alpha, \alpha) = h(\alpha, \alpha)$, dla każdego $\alpha \in V$. To dowodzi istnienia żądanej formy dwuliniowej symetrycznej h. Aby wykazać jej jednoznaczność zauważmy, że jeśli h jest formą dwuliniową symetryczną spełniającą $q(\alpha) = h(\alpha, \alpha)$ dla każdego $\alpha \in V$, to dla każdych $\alpha, \beta \in V$ mamy

$$\frac{1}{2}(q(\alpha+\beta) - q(\alpha) - q(\beta)) = \frac{1}{2}\left(h(\alpha + \beta, \alpha + \beta) - h(\alpha, \alpha) - h(\beta, \beta)\right) = h(\alpha, \beta),$$

czyli h jest wyznaczona jednoznacznie przez q. □

Odtąd, aż do końca wykładu zakładamy, że ciało K jest charakterystyki różnej od 2.

Definicja 109. *Niech $q : V \to K$ będzie formą kwadratową na skończenie wymiarowej przestrzeni liniowej.* MACIERZĄ FORMY KWADRATOWEJ *q w bazie $\mathcal{A}$ przestrzeni V nazywamy macierz formy dwuliniowej symetrycznej odpowiadającej formie q. Macierz formy kwadratowej q w bazie $\mathcal{A}$ oznaczamy $G(q;\mathcal{A})$.*

Zatem $G(q;\mathcal{A}) = G(h;\mathcal{A})$ gdzie $h : V \times V \to K$ jest formą dwuliniową symetryczną spełniającą $q(\alpha) = h(\alpha,\alpha)$, dla każdego $\alpha \in V$.

Przykład. Dla formy $q : K^n \to K$ zadanej wzorem $q((x_1,\ldots,x_n)) = x_1^2 + \ldots + x_n^2$ mamy $G(q;st) = I$. Dla formy $q : \mathbb{R}^2 \to \mathbb{R}$ zadanej wzorem

$$q((x_1,x_2)) = x_1^2 + 3x_1x_2 + 7x_2^2$$

mamy

$$G(q;st) = \begin{bmatrix} 1 & \frac{3}{2} \\ \frac{3}{2} & 7 \end{bmatrix},$$

a w bazie $\mathcal{A} = ((1,1),(1,-1))$ mamy $G(q;\mathcal{A}) = \begin{bmatrix} 11 & -6 \\ -6 & 5 \end{bmatrix}$.

Opis form kwadratowych w języku form dwuliniowych symetrycznych uruchamia całą maszynerię i rezultaty uzyskane wcześniej. W szczególności mamy następujące własności macierzy form kwadratowych.

Fakt 173. *Jeśli $A = [a_{ij}]$ jest macierzą formy kwadratowej q w bazie $\mathcal{A} = (\alpha_1,\ldots,\alpha_n)$, to dla dowolnych elementów $x_1,\ldots,x_n \in K$ zachodzi równość $q(x_1\alpha_1 + \ldots + x_n\alpha_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j$.*

Fakt 174. *Jeśli A, B są macierzami formy kwadratowej q w bazach $\mathcal{A}$, $\mathcal{B}$ odpowiednio, to $B = C^TAC$, gdzie $C = M(\mathrm{id})_{\mathcal{B}}^{\mathcal{A}}$.*

Fakt 175. *Dla każdej formy kwadratowej q na skończenie wymiarowej przestrzeni V (gdzie* $\operatorname{char} K \neq 2$*) istnieje taka baza, w której macierz q ma macierz diagonalną, czyli taka baza $\mathcal{A} = (\alpha_1,\ldots,\alpha_n)$ przestrzeni V, że zachodzi równość $q(x_1\alpha_1 + \ldots + x_n\alpha_n) = a_1x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2$.*

Na ćwiczeniach będziecie Państwo stosować różne sposoby na diagonalizację formy q. Trzy podstawowe metody to:

- szukanie bazy prostopadłej przestrzeni dwuliniowej (V,h), gdzie h jest formą symetryczną odpowiadającą formie kwadratowej q,
- szukanie bazy ortonormalnej złożonej z wektorów własnych rzeczywistej macierzy symetrycznej $A = G(h;st)$ w przestrzeni euklidesowej ze standardowym iloczynem skalarnym (tutaj $K = \mathbb{R}$),
- intuicyjna metoda uzupełniania do kwadratów (jest ona opisana w skrypcie i na pewno będzie wspomniana na ćwiczeniach, choć powyższe dwie w zupełności wystarczają do diagonalizacji).

Definicja 110. *Mówimy, że forma kwadratowa kwadratowej) $q : V \to \mathbb{R}$ jest*

- DODATNIO OKREŚLONA, *jeśli $q(\alpha) > 0$, dla każdego niezerowego $\alpha \in V$,*
- UJEMNIE OKREŚLONA, *jeśli $q(\alpha) < 0$, dla każdego niezerowego $\alpha \in V$,*
- DODATNIO PÓŁOKREŚLONA, *jeśli $q(\alpha) \geq 0$, dla każdego wektora $\alpha \in V$,*
- UJEMNIE PÓŁOKREŚLONA, *jeśli $q(\alpha) \leq 0$, dla każdego wektora $\alpha \in V$,*
- NIEOKREŚLONA, *jeśli istnieją $\alpha, \beta \in V$ takie, że $q(\alpha) > 0$ oraz $q(\beta) < 0$.*

Definicje te mają ogromne znaczenie w zastosowaniach, zwłaszcza w analizie. Powyższym pojęciom odpowiadają analogiczne dotyczące macierzy form.

Definicja 111. *Mówimy, że macierz kwadratowa $A \in M_n(\mathbb{R})$ jest*

- DODATNIO OKREŚLONA, *jeśli $v^T Av > 0$, dla każdego $v \in \mathbb{R}^n \setminus \{0\}$,*
- UJEMNIE OKREŚLONA, *jeśli $v^T Av < 0$, dla każdego $v \in \mathbb{R}^n \setminus \{0\}$,*
- DODATNIO PÓŁOKREŚLONA, *jeśli $v^T Av \geq 0$, dla każdego $v \in \mathbb{R}^n$,*
- UJEMNIE PÓŁOKREŚLONA, *jeśli $v^T Av \leq 0$, dla każdego $v \in \mathbb{R}^n$,*
- NIEOKREŚLONA, *jeśli istnieją $v, w \in \mathbb{R}^n$, takie, że $v^T Av > 0$ oraz $w^T Aw < 0$.*

Określoność formy ma duży związek z jej postacią diagonalną.

Fakt 176. *Jeśli rzeczywista forma kwadratowa q ma w bazie $\mathcal{A} = (\alpha_1, \ldots, \alpha_n)$ postać diagonalną daną wzorem*

$$q(x_1\alpha_1 + \ldots + x_n\alpha_n) = a_1x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2,$$

dla pewnych $a_1, \ldots, a_n \in \mathbb{R}$, to forma q jest:

- DODATNIO OKREŚLONA $\iff a_i > 0$, *dla $i = 1, \ldots, n$.*
- UJEMNIE OKREŚLONA $\iff a_i < 0$, *dla $i = 1, \ldots, n$.*
- DODATNIO PÓŁOKREŚLONA $\iff a_i \geq 0$, *dla $i = 1, \ldots, n$.*
- UJEMNIE PÓŁOKREŚLONA $\iff a_i \leq 0$, *dla $i = 1, \ldots, n$.*
- NIEOKREŚLONA $\iff$ *istnieją $1 \leq i, j \leq n$ takie, że $a_i > 0$ oraz $a_j < 0$.*

Badanie określoności rzeczywistej formy kwadratowej opiera się na kryterium Sylvestera.

Fakt 177. *Niech $q : V \to \mathbb{R}$ będzie rzeczywistą formą kwadratową mającą w bazie $\mathcal{A}$ przestrzeni V macierz $G(q; \mathcal{A}) = A \in M_{n\times n}(\mathbb{R})$. Wówczas forma q jest:*

- DODATNIO OKREŚLONA $\iff \det A^{(i)} > 0$, *dla $i = 1, \ldots, n$.*
- UJEMNIE OKREŚLONA $\iff (-1)^i \det A^{(i)} > 0$, *dla $i = 1, \ldots, n$.*

Na koniec odnotujmy jak twierdzenia klasyfikacyjne dla form dwuliniowych i macierzy symetrycznych przenoszą się na formy kwadratowe.

Definicja 112. RZĘDEM FORMY KWADRATOWEJ *(odpowiednio:* SYGNATURĄ*, w przypadku ciała* $\mathbb{R}$*)* *nazywamy rząd (sygnaturę) odpowiadającej jej formy dwuliniowej symetrycznej. Mówimy, że formy kwadratowe* $q_1 : V_1 \to K, q_2 : V_2 \to K$ *są* równoważne*, jeśli istnieją bazy* $\mathcal{A}_1$ *przestrzeni* V_1 *oraz* $\mathcal{A}_2$ *przestrzeni* V_2 *takie, że* $G(q_1; \mathcal{A}_1) = G(q_2; \mathcal{A}_2)$*.*

Fakt 178. *Formy kwadratowe* $q_1 : V_1 \to K$ *oraz* $q_2 : V_2 \to K$ *są równoważne wtedy i tylko wtedy, gdy dla każdej bazy* $\mathcal{A}_1$ *przestrzeni* V_1 *oraz każdej bazy* $\mathcal{A}_2$ *przestrzeni* V_2 *macierze* $G(q_1; \mathcal{A}_1)$*,* $G(q_2; \mathcal{A}_2)$ *są kongruentne nad* K*.*

Fakt 179. *Każda forma kwadratowa na* n *wymiarowej przestrzeni liniowej nad* $\mathbb{C}$ *jest równoważna formie* $q : \mathbb{C}^n \to \mathbb{C}$ *postaci*

$$q((x_1, \ldots, x_n)) = x_1^2 + \ldots + x_r^2,$$

dla pewnego $0 \leq r \leq n$*. Formy kwadratowe* $q_1 : \mathbb{C}^n \to \mathbb{C}$*,* $q_2 : \mathbb{C}^n \to \mathbb{C}$ *są równoważne wtedy i tylko wtedy, gdy mają równe rzędy.*

Fakt 180. *Każda forma kwadratowa na* n *wymiarowej przestrzeni liniowej nad* $\mathbb{R}$ *jest równoważna formie* $q : \mathbb{R}^n \to \mathbb{R}$ *postaci*

$$q((x_1, \ldots, x_n)) = x_1^2 + \ldots + x_r^2 - x_{r+1}^2 - \ldots - x_{r+s}^2,$$

dla pewnych $r, s \geq 0$*,* $r + s \leq n$*. Formy kwadratowe* $q_1 : \mathbb{R}^n \to \mathbb{R}$*,* $q_2 : \mathbb{R}^n \to \mathbb{R}$ *są równoważne wtedy i tylko wtedy, gdy mają równe rzędy i sygnatury.*

Na tym kończy się część wykładu dotycząca wprowadzania dodatkowej struktury na przestrzeni liniowej, pozwalającej przede wszystkim na rozważanie pojęcia ortogonalności wektorów, a w przypadku rzeczywistym także na mówienie o kątach, miarach, orientacji itd.

Teoria ta pozwoliła nam na wyrobienie wstępnych intuicji geometrycznych niezbędnych do pracy w przestrzeniach afinicznych. Dała nam też posmak zjawiska, które będziecie Państwo często obserwować – zamiast rozważać czysto algebraiczne struktury typu przestrzenie liniowe czy przekształcenia między nimi uczyć się Państwo będziecie o ich szczególnych typach, wyposażonych w dodatkowe struktury algebraiczne (jak iloczyn skalarny), metryczne (jak choćby izometrie), i wiele innych.

Konkluzją wykładu będzie badanie zbiorów opisanych (niekoniecznie liniowymi) równaniami algebraicznymi w przestrzeni afinicznej.

Uzupełnienie. Minima i maksima

Możliwość diagonalizacji formy kwadratowej ma olbrzymie znaczenie w teorii liczb i geometrii, a także w wielu innych działach matematyki. Przyjrzymy się teraz prostemu zastosowaniu, mającemu dalej istotne zastosowania analityczne.

Zainteresowanych odsyłam do wykładu z Analizy II, np. do notatek dr. M. Krycha: Lokalne ekstrema, formy kwadratowe: https://www.mimuw.edu.pl/~krych/matematyka/AM2skrypt/am2cz06L.pdf.

Formy kwadratowe służą w analizie np. do określania kryteriów osiągania lub nie ekstremów lokalnych. Są to wyniki analogiczne jak dla funkcji różniczkowalnej jednej zmiennej, gdzie np. minimum lokalne osiągane jest w punkcie zerowania się pochodnej, pod warunkiem, że druga pochodna jest dodatnia. Dla funkcji wielu zmiennych zamiast pochodnych odpowiednich stopni mamy różniczki, przy czym pierwsza różniczka jest przekształceniem liniowym, a druga – symetryczną formą dwuliniową. Jeśli np. różniczkowalna w pewnym punkcie funkcja dwóch zmiennych ma zerową różniczkę oraz jej druga różniczka jest dodatnio określona to w punkcie tym jest minimum lokalne. Patrz też: http://smurf.mimuw.edu.pl/node/244.

Fakt 181. *Niech $(\mathbb{R}^n, \langle\,,\rangle)$ będzie przestrzenią euklidesową ze standardowym iloczynem skalarnym oraz niech $q : V \to \mathbb{R}$ będzie formą kwadratową, którą w pewnej bazie $(\alpha_1, \ldots, \alpha_n)$ można przedstawić w postaci diagonalnej*

$$q(x_1\alpha_1 + \ldots + x_n\alpha_n) = a_1x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2,$$

przy czym $a_1 \geq a_2 \geq \ldots \geq a_n$. Niech $I \subseteq (\mathbb{R}^n, \langle\,,\rangle)$ oznacza zbiór wektorów o normie 1. Wówczas na zbiorze I forma q ma największą wartość równą $q(\alpha_1/\|\alpha_1\|) = a_1$, a najmniejszą wartość równą $q(\alpha_n/\|\alpha_n\|) = a_n$.

Co to twierdzenie oznacza? Mówi ono, że przedstawienie formy kwadratowej w postaci diagonalnej, a więc w „nowym układzie prostopadłym" pozwala odczytać kierunki „najszybszego" jej wzrostu i „najszybszego" jej spadku.

Przykład. Wyznaczymy największą i najmniejszą wartość funkcji dwóch zmiennych $f : \mathbb{R}^2 \to \mathbb{R}$ postaci $f((x_1, x_2)) = x_1^2 + x_2^2 + 4x_1x_2$ na okręgu zadanym równaniem $x_1^2 + x_2^2 = 1$. Wykresem naszej funkcji jest pewna powierzchnia w $\mathbb{R}^3$. Wkrótce dowiemy się więcej na temat tego jak ona w zasadzie wygląda.

Otóż w bazie $(\alpha_1, \alpha_2) = ((1,1),(1,-1))$ (ortogonalnej w $(\mathbb{R}^2, \langle\,,\rangle_{st})$) funkcja f „traktowana jako" forma kwadratowa może być zapisana w postaci $f(y_1\alpha_1 + y_2\alpha_2) = 3y_1^2 - y_2^2$. Twierdzenie mówi, że po wzięciu kierunków powyższych wektorów o normie 1, czyli

$$\left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right) \quad \text{oraz} \quad \left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\right)$$

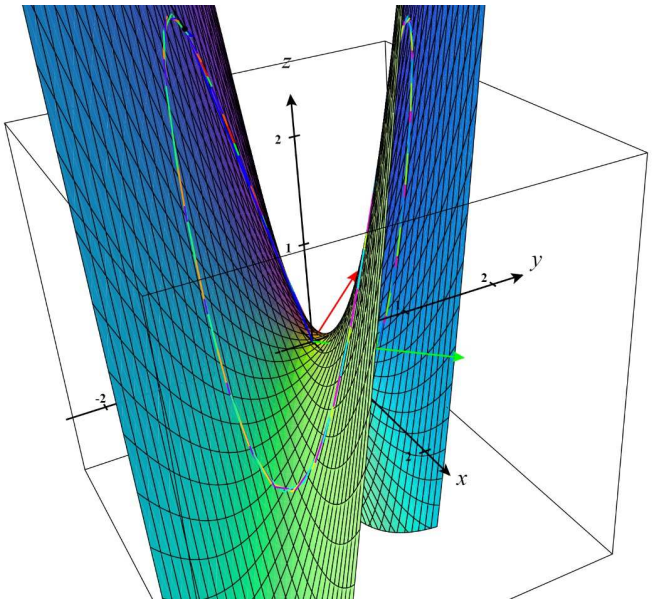
uzyskamy, że największa i najmniejsza wartość naszej funkcji na zbiorze I wynoszą odpowiednio

$$f\left(\left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right)\right) = 3 \quad \text{oraz} \quad f\left(\left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\right)\right) = -1.$$

Co ciekawe, moglibyśmy też wziąć wektory

$$\left(-\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\right) \quad \text{oraz} \quad \left(-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right)$$

i również dla nich dostaniemy odpowiednio największą w zbiorze I wartość f czyli 3 oraz najmniejszą wartość równą -1. Poniżej poglądowy obrazek.



Obrazek wygenerowany online: https://www.monroecc.edu/faculty/paulseeburger/calcnsf/CalcPlot3D/

Pozostał nam dowód wyjściowego faktu. Niech h będzie formą dwuliniową symetryczną na $\mathbb{R}^n$ odpowiadającą formie kwadratowej q. Na mocy twierdzenia o diagonalizowalności macierzy symetrycznych rzeczywistych wiemy, że istnieje baza ortonormalna w $(\mathbb{R}^n, \langle\,,\rangle_{st})$ złożona z wektorów własnych macierzy $A = G(h; st)$. Niech $(\alpha_1, \ldots, \alpha_n)$ będzie tą bazą przy czym $A\alpha_i = \lambda_i$, dla $i - 1, \ldots, n$. Załóżmy też, że $\lambda_1 \geq \ldots \geq \lambda_n$. Dla każdego $\alpha \in \mathbb{R}^n$ mamy rozkłady wektorów α oraz $A\alpha$ w bazie ortonormalnej postaci:

$$\alpha = \langle \alpha, \alpha_1\rangle\alpha_1 + \ldots + \langle \alpha, \alpha_n\rangle\alpha_n, \quad A\alpha = \lambda_1\langle \alpha, \alpha_1\rangle\alpha_1 + \ldots + \lambda_n\langle \alpha, \alpha_n\rangle\alpha_n.$$

Jeśli założymy, że $\|\alpha\| = 1$, to mamy też $\langle \alpha, \alpha_1\rangle^2 + \ldots + \langle \alpha, \alpha_n\rangle^2 = 1$, a także

$$\langle \alpha, A\alpha\rangle = \lambda_1\langle \alpha, \alpha_1\rangle^2 + \ldots + \lambda_n\langle \alpha, \alpha_n\rangle^2.$$

A zatem dla α o normie 1 mamy (proszę dokładnie przemyśleć zwłaszcza trzecią równość):

$$\begin{aligned} q(\alpha) = h(\alpha, \alpha) = \alpha^T A\alpha = \langle \alpha, A\alpha\rangle &= \lambda_1\langle \alpha, \alpha_1\rangle^2 + \ldots + \lambda_n\langle \alpha, \alpha_n\rangle^2 \\ &\leq \lambda_1\langle \alpha, \alpha_1\rangle^2 + \ldots + \lambda_1\langle \alpha, \alpha_n\rangle^2 = \lambda_1. \end{aligned}$$

Analogicznie pokazujemy, że $q(\alpha) \geq \lambda_n$, dla $\|\alpha\| = 1$. Jeśli teraz α jest wektorem własnym A odpowiadającym λ_1 oraz $\|\alpha\| = 1$, to

$$q(\alpha) = h(\alpha, \alpha) = \langle \alpha, A\alpha\rangle = \langle \alpha, \lambda_1\alpha\rangle = \lambda_1\|\alpha\|^2 = \lambda_1.$$

Podobnie $q(\alpha) = \lambda_n$, jeśli $\|\alpha\| = 1$ oraz α jest wektorem własnym A odpowiadającym wartości własnej λ_n. Dowód jest zatem zakończony.

Dodatek. Twierdzenie Hasse-Minkowskiego

Załóżmy, że chcecie Państwo rozwiązać w liczbach całkowitych równanie $x^3 - 2x + 17 = 0$. Oczywiście znamy rezultat szkolny, który mówi jak to robić, ale on ukrywa meritum sprawy. To równanie nie ma rozwiązań w $\mathbb{Z}$ (ani w $\mathbb{Q}$), bo jeśli „zajrzymy z nim" do małego świata ciała pięcioelementowego $\mathbb{Z}_5$, to ma ono postać $x^3 + 3x + 2 = 0$ i nie ma w tym ciele rozwiązań. Stąd i wyjściowe równanie nad $\mathbb{Z}$ ich nie ma. Pytanie: czy z każdym równaniem wielomianowym o współczynnikach całkowitych wystarczy „zajrzeć" do pewnych ciał skończonych, aby dowiedzieć się czy rozwiązanie w $\mathbb{Z}$ istnieje? O tym mówi i owo twierdzenie szkolne, i wynik Hasse-Minkowskiego, o którym chcemy powiedzieć tu kilka zdań. Aby zrozumieć wysłowienie tego faktu odsyłam do jednego z wcześniejszych dodatków dotyczących ciał p-adycznych, a także do notatek z wykładu gwiazdkowego/

Wykłady https://mimuw.edu.pl/~amecel/2021l/gal21/GAL2+_AM_w16.pdf, https://mimuw.edu.pl/~amecel/2021l/gal21/GAL2+_AM_w17.pdf.

Na czym polega problem z rozwiązaniem równania wyżej? Niestety, gdybyśmy znaleźli rozwiązanie powyższego równania w $\mathbb{Z}_5$, to nie mielibyśmy pewności, że istnieje ono nad $\mathbb{Z}$ czy też $\mathbb{Q}$. Zacznijmy od zacytowania następującego rezultatu.

Fakt 182 (https://arxiv.org/pdf/2102.08379.pdf)**.** *Dana jest liczba całkowita $n \neq 1$ spełniająca warunki:*

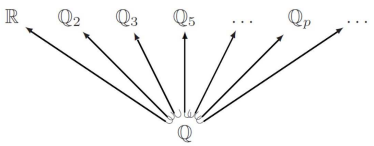
- *n jest niepodzielna przez sześcian liczby pierwszej,*
- *$n \equiv 1$ (mod 9),*
- *jeśli liczba pierwsza q dzieli n, to $q \equiv 1$ (mod 3).*

Wówczas wielomian:

$$(x^3 - n)(x^2 + 3) = 0$$

nie ma pierwiastków wymiernych, choć ma rozwiązania w ciele $\mathbb{Z}_p$.

Istnienie wielomianów o współczynnikach w $\mathbb{Z}$ takich jak powyższe przeczy prawdziwości *zasady lokalno-globalnej* dla dowolnego równania $f = 0$, $f \in \mathbb{Q}[x]$. Pytanie: czy po ograniczeniu do pewnych klas równań zasada ta może działać (i jak ją dokładnie sformułować)? To jedno z centralnych zagadnień teorii liczb. Poniższy rezultat to jedno z ważniejszych twierdzeń teorii form kwadratowych początku XX stulecia, otwierające nowy rozdział jej rozwoju.



Oczywiście $\mathbb{Q}_p \subseteq Q_p$, więc rozważanie formy q_p ma sens. Więcej o tym twierdzeniu można przeczytać w tekście http://www.math.union.edu/hatleyj/Capstone.pdf.

Fakt 183 (Zasada lokalno-globalna (Hasse-Minkowski), 1921)**.** *Niech q będzie formą kwadratową na skończenie wymiarowej przestrzeni nad ciałem $\mathbb{Q}$ oraz niech q_p oznacza formę q rozważaną nad ciałem liczb p-adycznych $\mathbb{Q}_p$, gdzie $p \in \mathbb{P}$ lub $p = \infty$ (konwencja: $\mathbb{Q}_\infty = \mathbb{R}$). Wówczas równanie $q(x) = 0$ ma rozwiązanie wtedy i tylko wtedy, gdy równania $q_p = 0$ mają rozwiązania dla każdego $p \in \mathbb{P} \cup \{\infty\}$.*

Notka historyczna. Sumy kwadratów

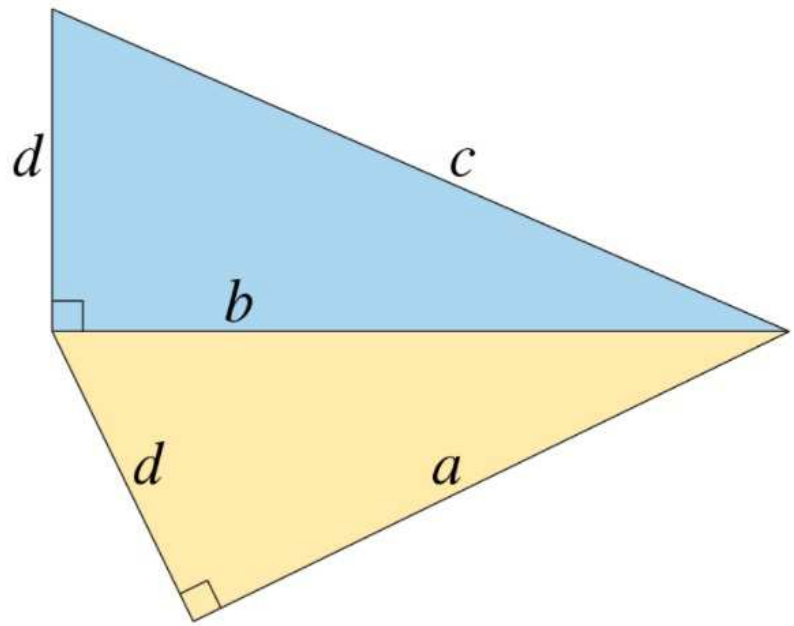
Wyrażeniami i równaniami typu kwadratowego zajmowano się już w starożytnym Babilonie. W starożytnej Grecji, a później w Afryce Północnej i Europie badano je także w kontekście geometrycznym (twierdzenie Pitagorasa, układ współrzędnych, stożkowe...) Najważniejszym czysto matematycznym źródłem była jednak teoria liczb. Punktem wyjścia był Problem 8 z Księgi II starożytnego traktatu *Arithmetica* Diofantosa z III wieku: daną liczbę wymierną przedstawić jako sumę kwadratów liczb wymiernych. Liczne przeformułowania były źródłami wielu słynnych problemów matematycznych stawianych najpierw przez uczonych arabskich w IX wieku, później przez czerpiącego z dorobku arabskiego Fibonacciego walczącego w XIII wieku z problemem CONGRUUM.

Fibonacci (1170-1250), a właściwie Leonardo (z Pizy) zasłynął przez upowszechnienie w początkach XIII wieku notacji arabskiej opartej na cyfrach $0-9$ pochodzącej z tekstu al-Khwārizmiego z 825 roku (od którego nazwę bierze algebra). Nikogo by to nie interesowało gdyby nie fakt, że *Liber Abbaci* (Księga Liczydła), obok wprowadzenia słynnego dziś ciągu jako rozwiązania problemu rozmnażania się królików, zawierała istotne praktyczne wskazówki dotyczące używania ułamków i rozwiązywania rachunkowych problemów powstających przy... wymianie dóbr, zwłaszcza różnych walut. To było wtedy ważne.

W 1225 roku Pizę odwiedził cesarz Fryderyk II (syn Barbarossy). Znając reputację Leonardo cesarz uznał, że warto poddać ją próbie przez... zorganizowanie turnieju (typowe w tamtych czasach). Zawodnicy zadawali sobie nawzajem pytania. Drużynę cesarza stanowili Jan z Palermo i Mistrz Teodor, zaś drużynę Leonarda stanowił on sam. Pytanie mu postawione brzmiało: znaleźć kwadrat liczby wymiernej, który pozostaje kwadratem liczby wymiernej zarówno gdy dodamy do niego 5, jak i gdy odejmiemy od niego 5. Innymi (naszymi) słowy oczekiwano przykładu, że 5 stanowi *congruum*, czyli różnicę w ciągu arytmetycznym trzech kwadratów liczb wymiernych. Najmniejszy przykład rozwiązania problemu turniejowego to $1681/144$ – co Leonardo wykrył (choć przed nim inni). W swoim ważnym dziele *Liber quadratorum* Fibonacci atakował ogólny problem congruum próbując zastąpić liczbę 5 innymi, w tym kwadratami liczb całkowitych (np. 1), dla których nie umiał go rozwiązać. Zrobił to dopiero Fermat, co wymagało prostego pomysłu zakładającego, że z istnienia „najmniejszej realizacji kwadratowego congruum" wywieść można istnienie jeszcze mniejszej realizacji (i dostać sprzeczność). Jest to *technika nieskończonego schodzenia*.

Do 1915 roku znano wszystkie congrua mniejsze niż 100. W 1986 roku – mniejsze niż 2000 (komputer). Ogólne rozwiązanie problemu congruum nie jest znane.

Fermat w 1670 roku rozwiązał problem Fibonacciego pokazując, ze jeśli różnice pewnych dwóch par kwadratów liczb całkowitych (lub ogólniej: liczb wymiernych) są identyczne, to nie mogą być one kwadratami. Innymi słowy, w poniższej konfiguracji trójkątów prostokątnych jedna z długości a, b, c, d musi być liczbą niewymierną.



Jeśli $d^2 = b^2 - a^2 = c^2 - b^2$, to jedna z liczb a, b, c, d jest niewymierna. Źródło: Wikipedia. Fermat's right triangle theorem.

Fermat zajmował się między innymi badaniem możliwości rozkładania liczb na sumy kwadratów. Aby opowiedzieć nieco o historii tego znanego zagadnienia przejdźmy do języka form kwadratowych. W notce tej zajmiemy się niezwykle ważnym i ciekawym problemem reprezentowalności formy kwadratowej o współczynnikach całkowitych. Interesuje nas jakie wartości całkowite przyjmować może ta forma. Zaczniemy od ogólnej definicji.

Definicja 113. *Niech q będzie formą kwadratową na przestrzeni n wymiarowej V nad ciałem K. Element niezerowy $a \in K$* JEST REPREZENTOWANY PRZEZ *q nad ciałem K, jeśli istnieją $x_1, \ldots, x_n$ takie, że $f(x_1, \ldots, x_n) = a$.*

- *Zbiór niezerowych elementów ciała K reprezentowanych przez formę q nazywamy* ZBIOREM WARTOŚCI *tej formy, ozn. $D_K(q)$.*
- *Formę q nazywamy* IZOTROPOWĄ, *jeśli istnieje $x \neq 0$ należący do V, że $q(x) = 0$. Formę q nazywamy* ANIZOTROPOWĄ, *jeśli $q(x) = 0 \Rightarrow x = 0$.*
- *Formę q nazywamy* UNIWERSALNĄ, *jeśli $D_K(q) = K \setminus \{0\}$.*

Interesuje nas odpowiedź na pytanie **jakie liczby całkowite mogą być reprezentowane przez formy kwadratowe o wyrazach całkowitych**?

Kiedy formy te mają zbiór wartości $\mathbb{Z}_+$, co określamy mianem **całkowitej formy uniwersalnej**?

Zobaczmy kilka przykładów.

- Równanie $x^2 - xy + y^2 = 2$ nie ma całkowitych rozwiązań.

Można argumentować modulo 3, ale można też zauważyć, że:

$$x^2 - xy + y^2 = (x - \frac{1}{2}y)^2 + \frac{3}{4}y^2 = 2 \Rightarrow \frac{3}{4}y^2 \leq 3 \Rightarrow |y| < 2,$$

czyli $y \in \{-1, 0, 1\}$, a przez symetrię $x \in \{-1, 0, 1\}$.

- Ile jest całkowitoliczbowych rozwiązań równania $x^2 - 3xy + y^2 = 1$?

Rozwiązaniami są np. $(x, y) = \pm(1, 0), \pm(0, 1)$, ale też $(x, y) = (8, 3)$. Pomnóżmy jednak strony wyjściowego równania przez 2 i zapiszmy:

$$\begin{aligned} 2x^2 - 6xy + 2y^2 &= \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} 2 & -3 \\ -3 & 2 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} \\ &= \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} -3 & -1 \\ 8 & 3 \end{bmatrix} \cdot \begin{bmatrix} 2 & -3 \\ -3 & 2 \end{bmatrix} \cdot \begin{bmatrix} -3 & 8 \\ -1 & 3 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} = 2. \end{aligned}$$

Więc jeśli $\begin{bmatrix} x \\ y \end{bmatrix}$ jest rozwiązaniem, to jest nim także

$$\begin{bmatrix} -3 & 8 \\ -1 & 3 \end{bmatrix}^n \cdot \begin{bmatrix} x \\ y \end{bmatrix}, \quad \text{dla} \quad n \geq 1,$$

czyli rozważane równanie ma nieskończenie wiele rozwiązań.

Problem reprezentowalności form kwadratowych znany jest (pod różnymi nazwami) od wieków. Oto kilka przykładów znanych rezultatów.

- **Euklides, -300.** Opis trójek liczb całkowitych, na których zeruje się forma całkowita (tzw. trójki pitagorejskie)

$$q(x_1, x_2, x_3) = x_1^2 + x_2^2 - x_3^2.$$

- **Fermat, 1640.** Forma kwadratowa na $\mathbb{Z}^2$ postaci

$$q(x_1, x_2) = x_1^2 + x_2^2$$

reprezentuje liczbę pierwszą p wtedy i tylko wtedy, gdy $p = 1 \bmod 4$.

- **Lagrange, 1772.** Forma kwadratowa na $\mathbb{Z}^4$ postaci

$$q(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

reprezentuje każdą liczbę całkowitą nieujemną.

- **Legendre, 1798.** Forma kwadratowa na $\mathbb{Z}^3$ postaci

$$q(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2$$

reprezentuje wszystkie liczby całkowite nieujemne, które nie mają postaci $4^a(8k+7)$, dla pewnych $a, k \in \mathbb{Z}$.

- **Liouville 1859-60.** Forma całkowita

$$x_1^2 + x_2^2 + 2x_3^2 + 2x_4^2$$

jest uniwersalna, zaś forma całkowita

$$x_1^2 + x_2^2 + 5x_3^2 + 5x_4^2$$

nie reprezentuje jedynie 3. Natomiast

$$x_1^2 + x_2^2 + 4x_3^2 + 4x_4^2$$

nie reprezentuje tylko liczb dających resztę 3 modulo 4.

- **Ramanujan, 1917.** Jest dokładnie 55 uniwersalnych form całkowitych postaci $q(x_1, x_2, x_3, x_4) = ax_1^2 + bx_2^2 + cx_3^2 + dx_4^2$.

- **Dickson, 1926.** Ramanujan nie ma racji, są tylko 54 uniwersalne formy całkowite o czterech zmiennych. Jest nieskończenie wiele całkowitych form uniwersalnych, dla każdej liczby zmiennych większej niż 4 (co wynika z twierdzenia o czterech kwadratach Lagrange'a), ale też żadna forma postaci

$$ax_1^2 + bx_2^2 + cx_3^2$$

nie jest uniwersalna (fajne ćwiczenie dla $a \leq b \leq c$).

- **Halmos, 1938.** Jeśli $a, b, c, d \in \mathbb{Z}_+$, to forma

$$ax_1^2 + bx_2^2 + cx_3^2 + dx_4^2$$

jest uniwersalna wtedy i tylko wtedy, gdy reprezentuje pierwsze 15 dodatnich liczb całkowitych (tak naprawdę wystarczy 9 liczb: $\{1, 2, 3, 5, 6, 7, 10, 14, 15\}$).

- **Conway, Schneeberger, 1993 (15-theorem).** Wynik Halmosa jest prawdziwy dla dowolnej formy

$$q(x_1, \ldots, x_n) = a_1x_1^2 + \ldots + a_nx_n^2$$

na $\mathbb{Z}^n$, gdzie $a_i \in \mathbb{Z}_+$. Hipoteza: jeśli nie założymy, że a_i są dodatnie, ale tylko, że q jest dodatnio określona (czyli $q(x) > 0$, dla $x \neq 0$, $x \in \mathbb{Z}^n$), to uniwersalność q zapewnia *już* reprezentowalność pierwszych 290 liczb całkowitych dodatnich.

- **Bhargava, 2000.** Wynik Halmosa działa dla dowolnej liczby zmiennych w mocniejszej wersji (9 liczb). Dowód jest elementarny, warto przeczytać pracę ze znakomitym wstępem Conwaya (który wywołał całe to *zamieszanie*): http://www.fen.bilkent.edu.tr/~franz/mat/15.pdf.

• **Bhargava, Hanke 2011.** Hipoteza Conwaya z 1993 roku jest prawdziwa. Do uniwersalności dodatnio określonej całkowitej formy kwadratowej potrzeba i wystarcza sprawdzenie reprezentowalności 27 liczb:

$$1, 2, 3, 5, 6, 7, 10, 13, 14, 15, 17, 19, 21, 22, 23, 26, 29, 30, 31, 34, 35, 37, 42, 58, 93, 110, 145, 203, 290.$$

Takich form jest 6436 (to już policzono komputerowo).

Przykład problemu otwartego: forma ternarna Ramanujana.

Więcej: K. Williams: *A "Four Integers" Theorem and a "Five Integers" Theorem*, The American Mathematical Monthly , Vol. 122, No. 6 (June–July 2015), pp. 528- 536, pod adresem (wymagane zalogowanie przez BUW): https://www.jstor.org/stable/10.4169/amer.math.monthly.122.6.528.

• **Ramanujan 1916.** Forma

$$x^2 + y^2 + 10z^2$$

nie reprezentuje liczb parzystych postaci

$$4^a(16b + 6),$$

dla $a, b \in \mathbb{Z}_+$ oraz liczb nieparzystych:

$$3, 7, 31, 33, 33, 43, 67, 79, 87, 133, 217, 219, 223, 253, 307, 391.$$

• **Gupta, 1941** Forma $x^2 + y^2 + 10z^2$ nie reprezentuje też 2719.

• **Ono, Sonudararajan 2011.** Hipoteza. Forma $x^2 + y^2 + 10z^2$ nie reprezentuje innych liczb nieparzystych, niż wypisane wyżej. Jeśli jednak zachodzi uogólniona Hipoteza Riemanna, to hipoteza jest prawdziwa!

Ważny problem: jakie liczby pierwsze reprezentowane są przez formy

$$x^2 + ay^2?$$

Zagadnienie to było motywem przewodnim rozwoju teorii liczb.

• Fermat (dowody dał Euler, dając początki prawu wzajemności)

– forma $x^2 + y^2$ reprezentuje liczby pierwsze $p = 1 \bmod 4$,

– forma $x^2 + 2y^2$ reprezentuje liczby pierwsze $p = 1, 3 \bmod 8$,

– forma $x^2 + 3y^2$ reprezentuje $p = 3$ oraz $p = 1 \bmod 3$.

• Hipotezy Eulera (nie umiał ich udowodnić, zrobił to Gauss)

– forma $x^2 + 5y^2$ repr. liczby pierwsze $p = 3, 7 \bmod 20$,

– forma $x^2 + 14y^2$ repr. liczby pierwsze $p = 1, 9, 15, 23, 25, 39 \bmod 56$,

– forma $x^2 + 27y^2$ repr. $p = 1 \bmod 3$ gdzie 2 jest resztą sześcienną mod p,

– forma $x^2 + 64y^2$ repr. $p = 1 \bmod 4$ gdzie 2 jest resztą dwukwadratową mod p.

- Lagrange, Legendre, Gauss wnieśli do teorii zagadnienia takie, jak równoważność form, początki teorii genusu, użycie wyróżnika, teoria kompozycji form, wyższe prawa wzajemności.
- Dedekind, Kronecker, Minkowski, Dirichlet, Hilbert rozważali całkowite formy kwadratowe w kontekście algebraicznej teorii liczb i prapoczątków geometrii algebraicznej.

Na koniec przytoczmy **bardzo trudne pytanie**. Czy istnieje nieskończenie wiele liczb pierwszych postaci

$$x^2 + 1,$$

dla $x \in \mathbb{Z}$? To jeden z czterech problemów zestawionych w 1912 roku przez E. Landau na Międzynarodowym Kongresie Matematycznym.

Pozostałe *problemy Landau* to: hipoteza Goldbacha, hipoteza liczb bliźniaczych i hipoteza Legendre'a o istnieniu liczby pierwszej pomiędzy $n^2 > 1$ a $(n+1)^2$.

Fundamentalny wkład w badanie wspomnianego problemu ma Profesor Henryk Iwaniec, Absolwent Wydziału MIM UW (żyje i pracuje w USA), pochodzący z Elbląga. W 1978 roku Profesor Iwaniec uzyskał wybitny rezultat: istnieje nieskończenie wiele liczb postaci $x^2 + 1$, które są iloczynami co najwyżej dwóch liczb pierwszych. Natomiast w 1997 Profesor udowodnił wraz z Friendlanderem, że istnieje nieskończenie wiele liczb pierwszych postaci $x^2 + y^4$.

Za wkład w rozwiązanie tej hipotezy prof. Iwaniec otrzymał (wraz z Peterem Sarnakiem i Richardem Taylorem) w 2001 roku nagrodę Ostrowskiego (w 1995 otrzymał ją A. Wiles za dowód Wielkiego Twierdzenia Fermata, a w 2005 r. – Ben Green i Terrence Tao za twierdzenie o ciągach arytmetycznych w zbiorze liczb pierwszych). W 2015 roku. Profesor otrzymał Nagrodę Shawa (razem z Gerdem Faltingsem). Osoby zainteresowane sylwetką najbardziej utytułowanego obecnie matematyka z Polski zachęcam między innymi do lektury wywiadu „Matematyka to moja miłość" (https://www.cultureave.com/matematyka-to-moja-milosc/), gdzie można dowiedzieć się więcej o życiu Profesora i Jego matematycznych osiągnięciach.

Literatura dotycząca zacytowanych wyżej zagadnień jest bardzo szeroka. Na elementarnym poziomie można o niektórych z nich poczytać w znakomitych tekstach Keitha Conrada (https://kconrad.math.uconn.edu/blurbs/), np. Pythagorean triples, Sums of two squares and lattices, Fermat's method of descent, Congruent number problem, Quadratic residue patterns modulo a prime, i wielu innych. Zainteresowanych – gorąco zachęcam.