

Algebra liniowa 4
Endomorfizmy przestrzeni euklidesowych i unitarnych

Wykład monograficzny 2009

Kazimierz Szymiczek

12.06.2009

Spis treści

Przedmowa	iii
1 Endomorfizmy przestrzeni wektorowych	1
1.1 Podstawowe pojęcia	1
1.2 Homomorfizmy	3
1.3 Endomorfizmy i macierze	4
1.4 Wielomian minimalny endomorfizmu	7
1.5 Podprzestrzenie niezmiennicze	9
1.6 Podobieństwo	12
1.7 Triangularyzacja i diagonalizacja	14
2 Funkcjonały dwuliniowe	17
2.1 Przestrzenie dwuliniowe	17
2.2 Przestrzenie dwuliniowe i kongruencja macierzy	19
2.3 Izometrie przestrzeni dwuliniowych	21
2.4 Nieosobliwość przestrzeni dwuliniowych	23
2.5 Twierdzenie o rzucie prostopadłym	25
2.6 Bazy ortogonalne przestrzeni dwuliniowych	26
3 Przestrzenie euklidesowe	29
3.1 Norma, odległość i kąt między wektorami	29
3.2 Bazy ortonormalne	31
3.3 Przykłady	33
3.4 Najlepsza aproksymacja	35
4 Endomorfizmy przestrzeni euklidesowych	37
4.1 Endomorfizmy sprzężone	37
4.2 Macierze endomorfizmów sprzężonych	39
4.3 Endomorfizmy samosprężone przestrzeni euklidesowych	40
4.4 Przemienne zbiory endomorfizmów samosprężonych	42
4.5 Izometrie przestrzeni dwuliniowych	44
4.6 Symetrie przestrzeni dwuliniowych	45
4.7 Macierzowa reprezentacja grupy izometrii	47
4.8 Grupa ortogonalna	51
5 Funkcjonały półtoraliniowe	57
5.1 Przestrzenie hermitowskie	57
5.2 Przestrzenie hermitowskie i kongruencja macierzy	59
5.3 Izometrie przestrzeni hermitowskich	59
5.4 Nieosobliwość przestrzeni hermitowskich	60
5.5 Twierdzenie o rzucie prostopadłym	62

5.6	Bazy ortogonalne przestrzeni hermitowskich	63
6	Przestrzenie unitarne	65
6.1	Norma wektora i odległość między wektorami	65
6.2	Bazy ortonormalne	66
6.3	Przykłady	67
6.4	Dodatnio określone funkcjonały hermitowskie	68
6.5	Najlepsza aproksymacja	69
7	Endomorfizmy przestrzeni unitarnych	71
7.1	Endomorfizmy sprzężone	71
7.2	Endomorfizmy samosprężone przestrzeni unitarnych	74
7.3	Przemienne zbiory endomorfizmów samosprężonych	76
7.4	Endomorfizmy normalne	76
7.4.1	Charakteryzacja endomorfizmów normalnych	78
7.4.2	Przemienne zbiory endomorfizmów normalnych	80
7.5	Endomorfizmy unitarne	83
7.6	Symetrie i grupa unitarna	85
7.7	Rozkład biegunowy	86
8	Ciała rzeczywiste domknięte	89
8.1	Ciała formalnie rzeczywiste	89
8.2	Ciała uporządkowane	93
8.3	Rzeczywiste domknięcie ciała uporządkowanego	98
9	Ogólne przestrzenie euklidesowe i unitarne	101
	Bibliografia	103

Przedmowa

Linear algebra, like motherhood,
has become a sacred cow.
Irving Kaplansky

Algebrę liniową wykłada się dla wszystkich specjalności matematycznych studiów uniwersyteckich. Jednakże usytuowanie tych wykładów na pierwszych semestrach studiów nie pozwala na omówienie bardziej zaawansowanych tematów, które są kluczowe dla zastosowań algebry liniowej w matematyce i poza nią. W szczególności, centralny problem istnienia postaci kanonicznych endomorfizmów przestrzeni wektorowych jest zwykle zaledwie muśnięty wzmianką o diagonalizowalności endomorfizmów samosprzężonych przestrzeni euklidesowych.

Niniejszy skrypt jest zapisem wykładu monograficznego z algebry liniowej w Uniwersytecie Śląskim w semestrze letnim roku akademickiego 2008/2009. Koncentruje się on na przestrzeniach euklidesowych i unitarnych i postaciach kanonicznych macierzy endomorfizmów samosprzężonych i normalnych. Przedstawiamy także nieco ogólniejszą wersję tej teorii zastępując ciało liczb zespolonych dowolnym ciałem algebraicznie domkniętym K o charakterystyce zero oraz ciało liczb rzeczywistych ciałem rzeczywście domkniętym R takim, że K jest kwadratowym rozszerzeniem R . W rozdziale ósmym przedstawiamy zarys teorii ciał rzeczywście domkniętych i w rozdziale dziewiątym opisujemy uogólnienia przestrzeni euklidesowych i unitarnych do kontekstu ciał rzeczywście domkniętych i ich algebraicznych domknięć.

Kazimierz Szymiczek

Rozdział 1

Endomorfizmy przestrzeni wektorowych

Ostatnie zmiany 17.02.2007 r.

W tym rozdziale przypomnimy podstawowe pojęcia i fakty o endomorfizmach przestrzeni wektorowych nad dowolnymi ciałami. Zakładamy, że są one znane z kursowego wykładu algebry liniowej.

1.1 Podstawowe pojęcia

Niech K będzie dowolnym ciałem i niech $(V, +, \theta)$ będzie addytywną grupą abelową. Grupę V nazywamy *przestrzenią wektorową* nad ciałem K lub K -przestrzenią wektorową, jeśli na grupie V określone jest *działanie zewnętrzne* z ciałem skalarów K :

$$K \times V \rightarrow V, \quad (a, v) \mapsto av$$

i ma ono następujące własności:

$$\begin{aligned} a(v_1 + v_2) &= av_1 + av_2 \\ (a_1 + a_2)v &= a_1v + a_2v \\ (a_1a_2)v &= a_1(a_2v) \\ 1v &= v \end{aligned}$$

dla wszystkich $a, a_1, a_2 \in K$, $v_1, v_2, v \in V$. Elementy przestrzeni V nazywamy *wektorami*. Mówimy, że wektory $v_1, \dots, v_m \in V$ są *liniowo zależne*, jeśli istnieją $a_1, \dots, a_m \in K$ nie wszystkie równe zero takie, że

$$a_1v_1 + \dots + a_mv_m = \theta.$$

Wektory $v_1, \dots, v_m \in V$, które nie są liniowo zależne nazywają się *liniowo niezależne*. Mówimy, że podzbiór $B \subset V$ przestrzeni V jest *liniowo niezależny* jeśli każdy skończony podzbiór zbioru B jest liniowo niezależny. Mówimy, że podzbiór $B \subset V$ przestrzeni V *rozpina* przestrzeń V jeśli każdy wektor $v \in V$ można przedstawić w postaci kombinacji liniowej wektorów zbioru B ,

$$v = a_1v_1 + \dots + a_mv_m$$

dla pewnych $a_1, \dots, a_m \in K$ oraz $v_1, \dots, v_m \in B$. Piszemy wtedy $V = \text{lin}\{B\}$. Podzbiór B przestrzeni V nazywa się *bazą* przestrzeni V jeśli jest liniowo niezależny

i rozpina przestrzeń V . Można udowodnić, że każda przestrzeń wektorowa ma bazę i ponadto, każde dwie bazy przestrzeni V są zbiorami równolicznymi. Wobec tego moc jakiejkolwiek bazy przestrzeni V nazywa się *wymiarem* przestrzeni V i oznacza $\dim V$ lub $\dim_K V$, jeśli chcemy zaznaczyć, że traktujemy V jako przestrzeń wektorową nad ciałem K (a nie nad jakimś podciałem ciała K).

Podgrupę $(U, +, \theta)$ addytywnej grupy $(V, +, \theta)$ przestrzeni wektorowej V nad ciałem K nazywa się *podprzestrzenią* przestrzeni V jeśli U jest zbiorem zamkniętym ze względu na mnożenie przez skalary z ciała K , to znaczy dla każdych $a \in K$ oraz $u \in U$ także $au \in U$. Wtedy U jest także przestrzenią wektorową nad ciałem K .

Jeśli U i W są podprzestrzeniami przestrzeni V to zbiór

$$U + W = \{u + w \in V : u \in U, w \in W\}$$

także jest podprzestrzenią przestrzeni V . Podprzestrzeń $U + W$ nazywamy *sumą* lub *sumą zwykłą* podprzestrzeni U i W . Zauważmy, że $U + W = V$ oznacza iż zbiór $U \cup W$ rozpina przestrzeń V .

Mówimy, że przestrzeń V jest *sumą prostą* podprzestrzeni U i W gdy

$$U + W = V \quad \text{oraz} \quad U \cap W = \{\theta\}.$$

Piszemy wtedy $V = U \oplus W$. Łatwo dowodzi się, że $V = U \oplus W$ wtedy i tylko wtedy gdy każdy wektor $v \in V$ ma *dokładnie jedno* przedstawienie w postaci $v = u + w$ gdzie $u \in U$ oraz $w \in W$.

Pojęcia sumy i sumy prostej dwóch podprzestrzeni są szczególnymi przypadkami ogólniejszych pojęć sumy i sumy prostej dowolnej (niekoniecznie skończonej) rodziny podprzestrzeni przestrzeni V . Sformułujemy odpowiednie definicje w przypadku skończonej rodziny podprzestrzeni.

Niech $U_1, \dots, U_m$ będzie dowolną skończoną rodziną podprzestrzeni przestrzeni wektorowej V . *Sumą* tej rodziny podprzestrzeni nazywamy zbiór wszystkich wektorów $v \in V$, które można przedstawić w postaci

$$v = u_1 + \dots + u_m \quad \text{gdzie} \quad u_i \in U_i. \quad (1.1)$$

Suma podprzestrzeni $U_1, \dots, U_m$ jest podprzestrzenią przestrzeni V . Oznaczamy ją $U_1 + \dots + U_m$ lub krótko $\sum_{i=1}^m U_i$.

Mówimy, że przestrzeń V jest *sumą prostą* rodziny podprzestrzeni $U_1, \dots, U_m$ jeśli

$$\sum_{i=1}^m U_i = V \quad \text{oraz} \quad U_j \cap \sum_{\substack{i=1 \\ i \neq j}}^m U_i = \{\theta\} \quad \text{dla każdego} \quad j \in \{1, \dots, m\}.$$

Piszemy wtedy $V = \bigoplus_{i=1}^m U_i$. W szczególności więc przestrzeń V jest sumą prostą swoich trzech podprzestrzeni U_1, U_2, U_3 , jeśli

$$U_1 + U_2 + U_3 = V \quad \text{oraz} \quad U_1 \cap (U_2 + U_3) = U_2 \cap (U_1 + U_3) = U_3 \cap (U_1 + U_2) = \{\theta\}.$$

Podobnie jak w przypadku dwóch podprzestrzeni, $V = \bigoplus_{i=1}^m U_i$ wtedy i tylko wtedy gdy każdy wektor $v \in V$ ma *dokładnie jedno* przedstawienie w postaci (1.1). W szczególności, jeśli przestrzeń V ma bazę $v_1, \dots, v_n$ oraz $U_i = Kv_i$ są jednowymiarowymi podprzestrzeniami rozpiętymi na wektorach bazowych, to

$$V = U_1 \oplus \dots \oplus U_n.$$

Niech U będzie podprzestrzenią przestrzeni V . Wtedy $(U, +, \theta)$ jest podgrupą addytywnej grupy abelowej $(V, +, \theta)$ i wobec tego można rozpatrywać grupę ilorazową V/U , której elementami są warstwy $v + U$ grupy V względem podgrupy (normalnej) U i dodawanie warstw jest określone następująco:

$$(v_1 + U) + (v_2 + U) = v_1 + v_2 + U.$$

Grupa ilorazowa V/U jest grupą abelową i można na niej określić działanie zewnętrzne

$$K \times V/U \rightarrow V/U, \quad (a, v + U) \mapsto av + U,$$

które wyposaża grupę abelową V/U w strukturę przestrzeni wektorowej nad ciałem K . Nazywamy ją *przestrzenią ilorazową* przestrzeni V względem podprzestrzeni U .

Jeśli $\dim V < \infty$, to znaczy jeśli V ma skończoną bazę, to wymiar przestrzeni ilorazowej V/U jest wyznaczony następująco:

$$\dim V/U = \dim V - \dim U.$$

Jeśli bowiem $\{v_1, \dots, v_k\}$ jest dowolną bazą podprzestrzeni U , to uzupełniamy ją do bazy $\{v_1, \dots, v_k, u_1, \dots, u_m\}$ przestrzeni V i łatwo dowodzimy, że warstwy $u_1 + U, \dots, u_m + U$ tworzą bazę przestrzeni ilorazowej V/U .

1.2 Homomorfizmy

Niech teraz V i W będą przestrzeniami wektorowymi nad ciałem K . *Homomorfizmem* przestrzeni V w przestrzeń W nazywamy odwzorowanie $\varphi : V \rightarrow W$, które jest homomorfizmem addytywnej grupy V w addytywną grupę W i zachowuje mnożenie wektorów przez skalary. A więc

$$\varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2) \quad \text{oraz} \quad \varphi(av) = a\varphi(v)$$

dla wszystkich $v_1, v_2, v \in V$ oraz $a \in K$. Homomorfizm $\varphi : V \rightarrow W$ nazywa się *monomorfizmem*, *epimorfizmem*, *izomorfizmem* jeśli φ jest odpowiednio odwzorowaniem iniektywnym, surjektywnym, bijektywnym. Jeśli homomorfizm $\varphi : V \rightarrow W$ jest izomorfizmem, to przestrzenie V i W nazywamy izomorficznymi i piszemy $V \cong W$. Łatwo sprawdza się, że izomorfizm $\varphi : V \rightarrow W$ przeprowadza bazę przestrzeni V na bazę przestrzeni W i wobec tego

$$V \cong W \quad \Rightarrow \quad \dim V = \dim W.$$

Jeśli znamy jakąś bazę przestrzeni V , to istnieje bardzo prosty i wygodny sposób określania homomorfizmów $\varphi : V \rightarrow W$ w dowolną przestrzeń wektorową W (nad tym samym ciałem). Jeśli, na przykład, przestrzeń V jest skończenie wymiarowa i ma bazę $\{v_1, \dots, v_n\}$ to dla każdego układu $\{w_1, \dots, w_n\}$ wektorów przestrzeni W istnieje dokładnie jeden homomorfizm $\varphi : V \rightarrow W$ taki, że $\varphi(v_i) = w_i$ dla $i = 1, \dots, n$. Homomorfizm ten działa na wektorach przestrzeni V (które są kombinacjami liniowymi wektorów bazowych) następująco:

$$\varphi(a_1v_1 + \dots + a_nv_n) = a_1w_1 + \dots + a_nw_n.$$

Zatem dla określenia homomorfizmu φ na przestrzeni wektorowej V wystarczy wskazać obrazy poprzez φ wektorów bazowych przestrzeni V .

Jądro homomorfizmu $\varphi : V \rightarrow W$ przestrzeni wektorowych nazywa się *jądro* homomorfizmu $\varphi : V \rightarrow W$ grupy abelowej V w grupę abelową W . Jądro φ oznacza się $\ker \varphi$. A więc $\ker \varphi = \{v \in V : \varphi(v) = \theta_W\}$. Specjalną rolę odgrywa *homomorfizm kanoniczny*

$\kappa_U : V \rightarrow V/U$ przestrzeni V w przestrzeń ilorazową V/U względem (dowolnej) podprzestrzeni U . Z definicji mamy $\kappa_U(v) = v + U$. Łatwo zauważyć, że $\ker \kappa_U = U$. Ważne twierdzenie o homomorfizmach przestrzeni wektorowych mówi, że jeśli $\varphi : V \rightarrow W$ jest epimorfizmem przestrzeni wektorowych, to

$$V/\ker \varphi \cong W.$$

Jako proste zastosowanie twierdzenia o homomorfizmach otrzymamy formułę dla wymiaru sumy skończenie wymiarowych podprzestrzeni U i W przestrzeni V :

$$\dim(U + W) = \dim U + \dim W - \dim(U \cap W).$$

Ten rezultat wynika stąd, że epimorfizm

$$U \rightarrow (U + W)/W, \quad u \mapsto u + W$$

ma jądro $U \cap W$. Zatem $U/(U \cap W) \cong (U + W)/W$, skąd porównując wymiary izomorficznych przestrzeni otrzymujemy formułę dla $\dim(U + W)$.

Dla ustalonych przestrzeni wektorowych V, W nad ciałem K zbiór wszystkich homomorfizmów $\varphi : V \rightarrow W$ oznacza się symbolem $\text{Hom}(V, W)$ lub $\text{Hom}_K(V, W)$. Zbiór $\text{Hom}(V, W)$ jest grupą abelową ze względu na zwykłe dodawanie funkcji i grupę tę wyposażamy w strukturę przestrzeni wektorowej nad ciałem K definiując mnożenie homomorfizmów przez skalary następująco: dla $\varphi \in \text{Hom}(V, W)$ i dla $a \in K$ określamy $a\varphi : V \rightarrow W$ następująco:

$$(a\varphi)(v) = a\varphi(v) \quad \text{dla } v \in V.$$

Łatwo sprawdza się, że faktycznie $a\varphi \in \text{Hom}(V, W)$. W ten sposób możemy rozpatrywać *przestrzeń homomorfizmów* $\text{Hom}(V, W)$.

Jeśli $\{v_1, \dots, v_n\}$ oraz $\{w_1, \dots, w_m\}$ są bazami przestrzeni V i W , to definiujemy nm homomorfizmów $\tau_{ij} : V \rightarrow W$ takich, że

$$\tau_{ij}(v_k) = \delta_{jk} w_i$$

dla $1 \leq i \leq m$, $1 \leq j \leq n$. Tutaj $\delta_{jk} = 0$ gdy $j \neq k$ oraz $\delta_{jj} = 1$. Dowodzi się, że tworzą one bazę przestrzeni $\text{Hom}(V, W)$. Zatem dla przestrzeni skończenie wymiarowych mamy

$$\dim \text{Hom}(V, W) = \dim V \cdot \dim W. \quad (1.2)$$

1.3 Endomorfizmy i macierze

Homomorfizm $\tau : V \rightarrow V$ przestrzeni wektorowej V w siebie nazywa się *endomorfizmem* przestrzeni wektorowej V . Endomorfizm $\tau : V \rightarrow V$, który jest izomorfizmem nazywa się *automorfizmem* przestrzeni wektorowej V . Inaczej mówiąc, automorfizm przestrzeni V jest endomorfizmem odwracalnym tej przestrzeni. Przestrzeń endomorfizmów $\text{Hom}(V, V)$ oznacza się $\text{End } V$ lub $\text{End}_K V$. Jeśli $\dim_K V = n < \infty$, to na podstawie (1.2) otrzymujemy $\dim_K \text{End}_K V = n^2$. Dla uproszczenia, od tego miejsca wektor zerowy przestrzeni V będziemy oznaczać 0 zamiast θ lub θ_V .

Wyróżnimy *endomorfizm zerowy* $0_V : V \rightarrow V$ taki, że $0_V(u) = 0$ dla każdego $u \in V$, oraz *endomorfizm identycznościowy* $1_V : V \rightarrow V$ taki, że $1_V(u) = u$ dla każdego $u \in V$.

Działania dodawania endomorfizmów i mnożenia endomorfizmów przez skalary określone są następująco: dla $\sigma, \tau \in \text{End } V$

$$\sigma + \tau : V \rightarrow V, \quad (\sigma + \tau)(u) = \sigma(u) + \tau(u),$$

oraz dla $a \in K$ i $\tau \in \text{End } V$

$$a\tau : V \rightarrow V, \quad (a\tau)(u) = a\tau(u)$$

dla każdego $u \in V$. Ponadto określamy działanie *mnożenia* endomorfizmów, jako złożenie odwzorowań:

$$\sigma \cdot \tau : V \rightarrow V, \quad (\sigma \cdot \tau)(u) = \sigma(\tau(u)).$$

Rutynowe rachunki pokazują, że $\text{End}_K V$ z dodawaniem i mnożeniem endomorfizmów jako działaniami jest pierścieniem.

Należy jeszcze zauważyć, że mnożenie endomorfizmów w $\text{End } V$ oraz mnożenie endomorfizmów przez skalary są związane następującą własnością:

$$a(\sigma \cdot \tau) = a\sigma \cdot \tau = \sigma \cdot a\tau$$

dla dowolnych $\sigma, \tau \in \text{End } V$ oraz $a \in K$. W ten sposób pierścień $\text{End}_K V$ jest K -*algebrą*. Nazywamy ją *algebrą endomorfizmów przestrzeni wektorowej* V .

Przypomnimy teraz fundamentalne pojęcie macierzy endomorfizmu względem bazy przestrzeni.

DEFINICJA 1.3.1. Niech $\mathcal{B} = \{v_1, \dots, v_n\}$ będzie uporządkowaną bazą przestrzeni wektorowej V i niech $\tau \in \text{End}_K V$. Każdy wektor $\tau(v_j)$ przedstawiamy jako kombinację liniową wektorów bazy $\mathcal{B}$:

$$\tau(v_j) = \sum_{i=1}^n b_{ij}v_i,$$

gdzie b_{ij} są jednoznacznie określonymi elementami ciała K .

Macierz $\mathbf{m}(\tau, \mathcal{B}) := [b_{ij}] \in M_n(K)$ nazywa się *macierzą endomorfizmu* τ w bazie $\mathcal{B}$.

Macierz $\mathbf{m}(\tau, \mathcal{B})$ można więc opisać jako macierz, której j -tą kolumnę tworzą współrzędne wektora $\tau(v_j)$ w bazie $\mathcal{B}$.

Niech $M_n(K)$ będzie zbiorem wszystkich $n \times n$ macierzy (macierzy o n kolumnach i n wierszach) o elementach z ciała K . Jak wiadomo $M_n(K)$ jest przestrzenią wektorową nad ciałem K z działaniem zewnętrznym i dodawaniem macierzy określonymi następująco:

$$a \cdot [a_{ij}] := [aa_{ij}], \quad [a_{ij}] + [b_{ij}] := [a_{ij} + b_{ij}],$$

gdzie $a \in K$.

Zbiór macierzy

$$\{E_{ij} \in M_n(K) : 1 \leq i, j \leq n\}$$

gdzie E_{ij} jest macierzą, która w i -tym wierszu i j -tej kolumnie ma 1 a na pozostałych miejscach zera, jest bazą algebry $M_n(K)$. Rzeczywiście, macierze te rozpinają przestrzeń $M_n(K)$, co wynika z równości

$$[a_{ij}] = \sum_{1 \leq i, j \leq n} a_{ij}E_{ij},$$

oraz są liniowo niezależne, co łatwo otrzymuje się przy pomocy tej samej równości. Zatem

$$\dim_K M_n(K) = n^2.$$

W $M_n(K)$ jest także określone wewnętrzne działanie mnożenia macierzy

$$[a_{ij}] \cdot [b_{ij}] := [c_{ij}], \quad c_{ij} = a_{i1}b_{1j} + \dots + a_{in}b_{nj}.$$

To mnożenie jest łączne i rozdzielne względem dodawania oraz macierz jednostkowa $I \in M_n(K)$ jest jedyneką mnożenia: $I \cdot A = A \cdot I = A$ dla każdej macierzy $A \in M_n(K)$. Tak więc $M_n(K)$ jest pierścieniem. Ponadto mnożenie macierzy w $M_n(K)$ oraz mnożenie macierzy przez skalary są związane następującą własnością:

$$a(A \cdot B) = aA \cdot B = A \cdot aB$$

dla dowolnych $A, B \in M_n(K)$ oraz $a \in K$.

A więc $M_n(K)$ jest K -algebrą. Łatwo stwierdzić, że dla $n > 1$ algebra $M_n(K)$ jest nieprzemienne.

Okazuje się, że każda uporządkowana baza $\mathcal{B}$ przestrzeni V wyznacza przyporządkowanie

$$\mu : \text{End}_K V \longrightarrow M_n(K), \quad \mu(\tau) = \mathbf{m}(\tau, \mathcal{B}),$$

które jest izomorfizmem K -algebr. Rutynowy argument pozwala bowiem stwierdzić, że odwzorowanie μ jest bijekcją, a ponadto dla dowolnych $\sigma, \tau \in \text{End}_K V$ oraz dowolnego $a \in K$ mamy

$$\begin{aligned} \mathbf{m}(\sigma + \tau, \mathcal{B}) &= \mathbf{m}(\sigma, \mathcal{B}) + \mathbf{m}(\tau, \mathcal{B}), \\ \mathbf{m}(a\tau, \mathcal{B}) &= a \mathbf{m}(\tau, \mathcal{B}), \\ \mathbf{m}(\sigma \cdot \tau, \mathcal{B}) &= \mathbf{m}(\sigma, \mathcal{B}) \cdot \mathbf{m}(\tau, \mathcal{B}). \end{aligned}$$

Jeśli bowiem $\mathcal{B} = \{v_1, \dots, v_n\}$ jest bazą V i

$$\sigma(v_j) = \sum_{i=1}^n a_{ij} v_i, \quad \tau(v_j) = \sum_{i=1}^n b_{ij} v_i$$

to

$$(\sigma + \tau)(v_j) = \sum_{i=1}^n (a_{ij} + b_{ij}) v_i,$$

oraz

$$a\tau(v_j) = \sum_{i=1}^n ab_{ij} v_i$$

co oznacza, że $\mathbf{m}(\sigma + \tau, \mathcal{B}) = \mathbf{m}(\sigma, \mathcal{B}) + \mathbf{m}(\tau, \mathcal{B})$ oraz $\mathbf{m}(a\tau, \mathcal{B}) = a \mathbf{m}(\tau, \mathcal{B})$. Dalej,

$$\begin{aligned} (\sigma \cdot \tau)(v_j) &= \sigma(\tau(v_j)) = \sigma\left(\sum_{i=1}^n b_{ij} v_i\right) = \sum_{i=1}^n b_{ij} \sigma(v_i) = \sum_{i=1}^n b_{ij} \sum_{k=1}^n a_{ki} v_k \\ &= \sum_{k=1}^n \left(\sum_{i=1}^n a_{ki} b_{ij}\right) v_k, \end{aligned}$$

skąd wynika, że element c_{kj} macierzy endomorfizmu $\sigma \cdot \tau$ w bazie $\mathcal{B}$ ma postać

$$c_{kj} = \sum_{i=1}^n a_{ki} b_{ij}.$$

Jest to więc element k -tego wiersza i j -tej kolumny iloczynu macierzy $[a_{ij}] \cdot [b_{ij}]$. Stąd otrzymujemy $\mathbf{m}(\sigma \cdot \tau, \mathcal{B}) = \mathbf{m}(\sigma, \mathcal{B}) \cdot \mathbf{m}(\tau, \mathcal{B})$.

A więc bijektywne odwzorowanie

$$\mu : \text{End}_K V \longrightarrow M_n(K), \quad \mu(\tau) = \mathbf{m}(\tau, \mathcal{B})$$

ma następujące własności

$$\begin{aligned}\mu(\sigma + \tau) &= \mu(\sigma) + \mu(\tau), \\ \mu(\sigma \cdot \tau) &= \mu(\sigma) \cdot \mu(\tau), \\ \mu(a\tau) &= a\mu(\tau) \\ \mu(1_V) &= I,\end{aligned}$$

dla dowolnych $\sigma, \tau \in \text{End}_K V$ oraz dowolnego $a \in K$. Odwzorowanie to jest więc izomorfizmem K -algebr.

1.4 Wielomian minimalny endomorfizmu

Rozpatrzmy ważny przykład homomorfizmu pierścienia $K[X]$ wielomianów jednej zmiennej nad ciałem K w pierścień endomorfizmów $\text{End}_K V$ przestrzeni wektorowej V . Homomorfizm ten sprowadza się do operacji podstawiania endomorfizmu w miejsce zmiennej wielomianu.

Niech $f = a_0 + a_1X + \dots + a_nX^n$ będzie wielomianem o współczynnikach z ciała K i niech $\tau \in \text{End}_K V$ będzie dowolnym endomorfizmem przestrzeni V . Wtedy określamy

$$f(\tau) := a_0 1_V + a_1 \tau + \dots + a_n \tau^n,$$

gdzie 1_V oznacza endomorfizm identycznościowy na V , to znaczy $1_V(v) = v$ dla każdego $v \in V$. Oczywiście dla dowolnego wielomianu $f \in K[X]$ oraz $\tau \in \text{End}_K V$ mamy $f(\tau) \in \text{End}_K V$. Ponadto, przy ustalonym $\tau \in \text{End}_K V$, odwzorowanie

$$\varphi_\tau : K[X] \rightarrow \text{End}_K V, \quad \varphi_\tau(f) = f(\tau)$$

jest homomorfizmem pierścieni. Dla dowolnych wielomianów $f, g \in K[X]$ mamy bowiem

$$(f + g)(\tau) = f(\tau) + g(\tau), \quad (fg)(\tau) = f(\tau) \cdot g(\tau),$$

oraz dla jedynki 1 pierścienia $K[X]$ mamy $\varphi_\tau(1) = 1_A$. Ponadto,

$$\varphi_\tau(af) = (af)(\tau) = af(\tau) = a\varphi_\tau(\tau)$$

dla każdego $a \in K$. Oznacza to, że $\varphi_\tau : K[X] \rightarrow \text{End}_K V$ jest faktycznie homomorfizmem K -algebr.

Ważną konsekwencją tego, że φ_τ jest homomorfizmem pierścieni jest następujący fakt:

TWIERDZENIE 1.4.1. *Dla każdego endomorfizmu $\tau \in \text{End}_K V$ i dla dowolnych wielomianów $f, g \in K[X]$ endomorfizmy $f(\tau)$ i $g(\tau)$ są przemienne:*

$$f(\tau) \cdot g(\tau) = g(\tau) \cdot f(\tau).$$

Dowód. Mamy bowiem $f(\tau) \cdot g(\tau) = \varphi_\tau(fg) = \varphi_\tau(gf) = g(\tau) \cdot f(\tau)$. □

Zauważmy, że przestrzeń wektorowa $K[X]$ jest nieskończenie wymiarowa natomiast $\dim \text{End}_K V = n^2$, gdzie $n = \dim V$. W związku z tym żaden homomorfizm K -algebr $K[X] \rightarrow \text{End}_K V$ nie może być monomorfizmem, w szczególności więc dla żadnego endomorfizmu $\tau \in \text{End}_K V$ homomorfizm φ_τ nie jest monomorfizmem. Nieco dokładniejszą informację podaje następujące twierdzenie.

Twierdzenie 1.4.2. *Jeśli V jest przestrzenią n -wymiarową nad ciałem K , to każdy endomorfizm $\tau \in \text{End}_K V$ jest zerem pewnego niezerowego wielomianu o współczynnikach z ciała K stopnia niewiększego od n^2 .*

Dowód. Jak wiemy $\dim_K \text{End}_K V = n^2$. Zatem w przestrzeni wektorowej $\text{End}_K V$ każdy układ $n^2 + 1$ elementów jest liniowo zależny. Dla każdego $\tau \in \text{End}_K V$ istnieją więc skalary $a_0, a_1, \dots, a_{n^2} \in K$, nie wszystkie równe zero, takie, że

$$a_0 1_V + a_1 \tau + \dots + a_{n^2} \tau^{n^2} = 0_V.$$

Oznacza to, że dla wielomianu $g = a_0 + a_1 X + \dots + a_{n^2} X^{n^2} \in K[X]$ mamy $g \neq 0$ oraz $g(\tau) = 0_V$. $\square$

Wniosek 1.4.1. *Dla każdego endomorfizmu $\tau \in \text{End}_K V$ skończenie wymiarowej przestrzeni wektorowej V jądro homomorfizmu $\varphi_\tau : K[X] \rightarrow \text{End}_K V$ jest niezerowym ideałem w pierścieniu wielomianów $K[X]$.*

Wiemy, że w pierścieniu wielomianów $K[X]$ każdy ideał jest główny. W szczególności $\ker \varphi_\tau = (p)$ jest ideałem głównym generowanym przez pewien wielomian $p \in K[X]$. Prowadzi to do następującej definicji *wielomianu minimalnego* endomorfizmu τ .

Definicja 1.4.1. Niech τ będzie endomorfizmem skończenie wymiarowej przestrzeni wektorowej V nad ciałem K . *Wielomianem minimalnym p_τ endomorfizmu τ nazywamy unormowany generator p_τ ideału $\ker \varphi_\tau$ pierścienia $K[X]$.*

A więc $p_\tau \in K[X]$ jest wielomianem minimalnym endomorfizmu $\tau \in \text{End}_K V$ wtedy i tylko wtedy, gdy p_τ jest wielomianem unormowanym (to znaczy, najwyższy współczynnik wielomianu p_τ jest równy 1) oraz $\ker \varphi_\tau = (p_\tau)$.

Definicję wielomianu minimalnego endomorfizmu można więc sformułować także następująco.

Wielomian $p_\tau \in K[X]$ jest wielomianem minimalnym endomorfizmu τ jeśli

- p_τ jest wielomianem unormowanym,
- $p_\tau(\tau) = 0_V$,
- p_τ dzieli każdy wielomian $f \in K[X]$ taki, że $f(\tau) = 0_V$.

Przykład 1.4.1. Wielomianem minimalnym endomorfizmu zerowego $0_V \in \text{End}_K V$ jest wielomian $p_{0_V} = X \in K[X]$, natomiast wielomianem minimalnym endomorfizmu identycznościowego 1_V przestrzeni V jest wielomian $p_{1_V} = X - 1 \in K[X]$.

W podstawowym wykładzie algebry liniowej rozpatruje się *wielomian charakterystyczny* F_τ endomorfizmu τ . Jeśli $\mathcal{B}$ jest bazą przestrzeni V i $A = \mathbf{m}(\tau, \mathcal{B})$, to

$$F_\tau = F_A = \det(XI - A) \in K[X].$$

Dowodzi się, że wielomian F_τ nie zależy od wyboru bazy $\mathcal{B}$ przestrzeni V . Dowodzi się także, że $F_A(A) = 0 \in M_n(K)$ i wobec tego także $F_\tau(\tau) = 0_V \in \text{End}_K V$. Jest to tak zwane twierdzenie Cayleya-Hamiltona. Wobec tego wielomian minimalny endomorfizmu τ dzieli wielomian charakterystyczny endomorfizmu τ : $p_\tau \mid F_\tau$.

Uwaga 1.4.1. Podobnie jak w przypadku endomorfizmów skończenie wymiarowych przestrzeni wektorowych także dla macierzy kwadratowych można mówić o wielomianach minimalnych. Punktem wyjścia są homomorfizmy K -algebr

$$\varphi_A : K[X] \rightarrow M_n(K), \quad f \mapsto f(A)$$

określone dla każdej macierzy $A \in M_n(K)$. Unormowany generator p_A jądra takiego homomorfizmu φ_A nazywa się wielomianem minimalnym macierzy A .

A więc wielomian $p_A \in K[X]$ jest wielomianem minimalnym macierzy $A \in M_n(K)$ jeśli

- p_A jest wielomianem unormowanym,
- $p_A(A) = 0$,
- p_A dzieli każdy wielomian $f \in K[X]$ taki, że $f(A) = 0$.

W szczególności, na podstawie twierdzenia Cayleya-Hamiltona, wielomian minimalny macierzy A dzieli wielomian charakterystyczny macierzy A : $p_A \mid F_A$.

Innym faktem, ważnym dla praktycznego wyznaczania wielomianu minimalnego endomorfizmu, jest następujące twierdzenie.

TWIERDZENIE 1.4.3. *Niech $\tau \in \text{End}_K V$ i niech $A \in M_n(K)$ będzie macierzą endomorfizmu τ w jakiegokolwiek bazie przestrzeni V . Wtedy $p_\tau = p_A$.*

Dowód. Niech $\mu : \text{End}_K V \rightarrow M_n(K)$ będzie izomorfizmem K -algebr, który endomorfizmowi τ przyporządkowuje macierz A . Wtedy z równości $p_\tau(\tau) = 0$ wynika, że

$$0 = \mu(0) = \mu(p_\tau(\tau)) = p_\tau(\mu(\tau)) = p_\tau(A),$$

skąd wynika, że $p_A \mid p_\tau$. Podobnie, rozpatrując izomorfizm odwrotny $\mu^{-1} : M_n(K) \rightarrow \text{End}_K V$, z równości $p_A(A) = 0$ otrzymamy $p_A(\tau) = 0$. Zatem $p_\tau \mid p_A$. Ponieważ wielomiany p_τ i p_A są unormowane wynika stąd, że $p_\tau = p_A$. $\square$

Dla wyznaczenia wielomianu minimalnego p_A macierzy $A \in M_n(K)$ rozpatrujemy następujące układy n^2 równań liniowych o niewiadomych $x_0, x_1, \dots$:

$$A + x_0 I = 0, \quad A^2 + x_1 A + x_0 I = 0, \quad \dots, \quad A^k + x_{k-1} A^{k-1} + \dots + x_1 A + x_0 I = 0, \dots$$

Jeśli k jest najmniejszą liczbą naturalną, dla której układ równań liniowych

$$A^k + x_{k-1} A^{k-1} + \dots + x_1 A + x_0 I = 0$$

o niewiadomych $x_{k-1}, \dots, x_1, x_0$ ma rozwiązanie w ciele K , to

$$p_A = X^k + x_{k-1} X^{k-1} + \dots + x_1 X + x_0.$$

1.5 Podprzestrzenie niezmiennicze

DEFINICJA 1.5.1. Podprzestrzeń U przestrzeni V nazywamy podprzestrzenią *niezmienniczą* endomorfizmu $\tau \in \text{End}_K V$ lub τ -niezmienniczą, jeśli $\tau(U) \subseteq U$, to znaczy, jeśli dla każdego $u \in U$ także $\tau(u) \in U$.

Szczególnie ważny jest przypadek, gdy podprzestrzeń niezmiennicza ma wymiar 1. Jeśli dla $v \neq 0$ podprzestrzeń $U = Kv$ jest τ -niezmiennicza, to $\tau(v) \in Kv$, zatem istnieje taki skalar $a \in K$, że $\tau(v) = av$. Wtedy też $(\tau - a1_V)(v) = 0$, to znaczy endomorfizm $\tau - a1_V$ ma niezerowe jądro i jest wobec tego osobliwy.

DEFINICJA 1.5.2. Element $a \in K$ nazywa się *wartością własną endomorfizmu τ przestrzeni wektorowej V* , jeśli endomorfizm $\tau - a1_V$ jest osobliwy.

TWIERDZENIE 1.5.1. *Element $a \in K$ jest wartością własną endomorfizmu τ przestrzeni wektorowej V wtedy i tylko wtedy gdy istnieje wektor $v \in V$ taki, że $v \neq 0$ oraz $\tau(v) = av$.*

Dowód. Endomorfizm $\tau - a1_V$ jest osobliwy wtedy i tylko wtedy gdy istnieje niezerowy wektor $v \in V$ taki, że $(\tau - a1_V)(v) = 0$, a więc taki, że $\tau(v) = av$. $\square$

DEFINICJA 1.5.3. Niech $a \in K$ będzie wartością własną endomorfizmu τ . *Wektorem własnym* endomorfizmu τ *należącym do wartości własnej* a nazywamy każdy wektor $v \in V$ taki, że

$$v \neq 0 \quad \text{i} \quad \tau(v) = av.$$

LEMAT 1.5.1. Niech $\tau \in \text{End}_K V$, $a \in K$, $0 \neq v \in V$ i niech $g \in K[X]$ będzie dowolnym wielomianem. Wtedy

$$\tau(v) = av \quad \Rightarrow \quad g(\tau)(v) = g(a)v.$$

Dowód. Zauważmy najpierw, że dla każdej liczby naturalnej k ,

jeśli v jest wektorem własnym endomorfizmu τ należącym do wartości własnej a , to v jest wektorem własnym endomorfizmu τ^k należącym do wartości własnej a^k .

Rzeczywiście, jeśli $\tau(v) = av$ dla pewnego niezerowego wektora $v \in V$, to $\tau^2(v) = \tau(\tau(v)) = \tau(av) = a\tau(v) = a^2v$ i łatwa indukcja pokazuje, że $\tau^k(v) = a^k v$.

Stąd dla wielomianu $g = c_0X^m + c_1X^{m-1} + \dots + c_m$ mamy

$$\begin{aligned} g(\tau)(v) &= c_0\tau^m(v) + c_1\tau^{m-1}(v) + \dots + c_m1_V(v) \\ &= c_0a^m v + c_1a^{m-1}v + \dots + c_mv \\ &= g(a)v. \end{aligned}$$

A więc $g(a)$ jest wartością własną endomorfizmu $g(\tau)$ oraz v jest wektorem własnym należącym do wartości własnej $g(a)$. $\square$

TWIERDZENIE 1.5.2. Dla $a \in K$ i dla endomorfizmu $\tau \in \text{End}_K V$ następujące warunki są równoważne.

- (a) a jest wartością własną endomorfizmu τ .
- (b) a jest pierwiastkiem wielomianu minimalnego p_τ endomorfizmu τ .

Dowód. (a) $\Rightarrow$ (b) Niech $v \in V$ będzie wektorem własnym należącym do wartości własnej a . Zatem $\tau(v) = av$ oraz $v \neq 0$. Na podstawie lematu 1.5.1 mamy $p_\tau(\tau)(v) = p_\tau(a)v$. Ponieważ $p_\tau(\tau) = 0_V$, więc wynika stąd, że $p_\tau(a)v = 0$. Ponieważ zaś wektor v jest niezerowy, otrzymujemy $p_\tau(a) = 0$.

(b) $\Rightarrow$ (a) Jeśli $p_\tau(a) = 0$ oraz $a \in K$, to istnieje wielomian $q \in K[X]$ taki, że $p_\tau = (X - a)q$. Wtedy wobec $p_\tau(\tau) = 0_V$, endomorfizm $(\tau - a1_V)q(\tau)$ jest endomorfizmem zerowym, ale $q(\tau)$ nie jest endomorfizmem zerowym (gdyż stopień wielomianu q jest mniejszy od stopnia wielomianu minimalnego p_τ). Istnieje więc wektor $v \in V$ taki, że $u := q(\tau)(v) \neq 0$. Wtedy

$$(\tau - a1_V)(u) = (\tau - a1_V)q(\tau)(v) = p_\tau(\tau)(v) = 0,$$

a więc a jest wartością własną endomorfizmu τ . $\square$

WNIOSEK 1.5.1. Każdy endomorfizm τ ma tylko skończoną liczbę wartości własnych.

Dowód. Wielomian minimalny p_τ ma tylko skończoną liczbę pierwiastków. $\square$

Uwaga 1.5.1. W podstawowym wykładzie algebry liniowej dowodzi się, że w twierdzeniu 1.5.2 można zamienić wielomian minimalny p_τ wielomianem charakterystycznym F_τ endomorfizmu τ . A więc element a ciała K jest wartością własną endomorfizmu $\tau \in \text{End}_K V$ wtedy i tylko wtedy gdy a jest pierwiastkiem wielomianu charakterystycznego endomorfizmu τ : $F_\tau(a) = 0$.

Twierdzenie 1.5.3. *Jeśli $a_1, \dots, a_k \in K$ są różnymi wartościami własnymi endomorfizmu τ oraz $v_1, \dots, v_k \in V$ są wektorami własnymi endomorfizmu τ należącymi odpowiednio do wartości własnych $a_1, \dots, a_k$, to wektory $v_1, \dots, v_k$ są liniowo niezależne w przestrzeni V .*

Dowód. Jeśli $v_1, \dots, v_k$ są liniowo zależne, to istnieją skalary $c_1, \dots, c_k$ nie wszystkie równe zero takie, że

$$c_1 v_1 + \dots + c_k v_k = 0. \quad (1.3)$$

Biorąc wartości endomorfizmu τ po obydwu stronach otrzymujemy

$$c_1 a_1 v_1 + \dots + c_k a_k v_k = 0.$$

Mnożąc pierwszą z tych równości przez a_1 i odejmując od niej drugą równość otrzymamy

$$c_2(a_1 - a_2)v_2 + \dots + c_k(a_1 - a_k)v_k = 0.$$

Równość ta pokazuje liniową zależność wektorów $v_2, \dots, v_k$ (gdyż jeśli $c_i \neq 0$, to $c_i(a_1 - a_i) \neq 0$). Podobnie z liniowej zależności wektorów $v_2, \dots, v_k$ wydedukujemy liniową zależność wektorów $v_3, \dots, v_k$. Kontynuując dochodzimy do wniosku, że układ jednoelementowy złożony z wektora v_k jest liniowo zależny, sprzeczność (gdyż $v_k \neq 0$). $\square$

Wniosek 1.5.2. *Każdy endomorfizm τ przestrzeni n -wymiarowej ma co najwyżej n różnych wartości własnych.*

Dowód. Wektory własne należące do różnych wartości własnych endomorfizmu τ są liniowo niezależne, ich liczba nie może więc przekraczać wymiaru przestrzeni. $\square$

Wniosek 1.5.3. *Jeśli $\dim_K V = n$ i endomorfizm τ ma n różnych wartości własnych, to istnieje baza przestrzeni V złożona z wektorów własnych endomorfizmu τ .*

Dowód. Na podstawie twierdzenia 1.5.3 endomorfizm τ ma n liniowo niezależnych wektorów własnych. $\square$

Istnienie podprzestrzeni τ -niezmienniczych i wektorów własnych endomorfizmu ma decydujący wpływ na możliwość znalezienia bazy przestrzeni, względem której endomorfizm ma macierz opisującą w przejrzysty sposób działanie endomorfizmu na wektorach przestrzeni.

Twierdzenie 1.5.4. *Jeśli $\dim_K V = n$ oraz endomorfizm τ ma n różnych wartości własnych, to istnieje baza przestrzeni V , względem której endomorfizm τ ma macierz diagonalną.*

Dowód. Niech $a_1, \dots, a_n$ będą wartościami własnymi endomorfizmu τ . Dla każdej wartości własnej a_j wybieramy wektor własny v_j należący do a_j . Na podstawie wniosku 1.5.3, wektory własne $v_1, \dots, v_n$ tworzą bazę $\mathcal{B}$ przestrzeni V . Zatem z równości $\tau(v_j) = a_j v_j$ wynika, że

$$m(\tau, \mathcal{B}) = \begin{bmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ & & \ddots & \\ 0 & 0 & \dots & a_n \end{bmatrix}.$$

A więc macierz endomorfizmu τ w bazie $\mathcal{B}$ jest diagonalna. $\square$

Założmy teraz, że endomorfizm τ przestrzeni V ma podprzestrzeń niezmienniczą U . Wtedy zacieśnienie $\tau_1 = \tau|_U$ endomorfizmu τ do podprzestrzeni U jest endomorfizmem podprzestrzeni U . Obieramy jakąkolwiek uporządkowaną bazę $\mathcal{B}_1 = \{v_1, \dots, v_r\}$ podprzestrzeni U i rozpatrujemy macierz $A = m(\tau_1, \mathcal{B}_1)$ endomorfizmu $\tau_1 = \tau|_U$ podprzestrzeni U . Bazę $\mathcal{B}_1$ uzupełniamy następnie do uporządkowanej bazy $\mathcal{B}$ przestrzeni V , a więc

$$\mathcal{B} = \{v_1, \dots, v_r, v_{r+1}, \dots, v_n\}.$$

Macierz $m(\tau, \mathcal{B})$ ma wtedy postać

$$m(\tau, \mathcal{B}) = \begin{bmatrix} A & B \\ 0 & C \end{bmatrix}$$

gdzie B i C są pewnymi macierzami. A więc niezmienniczość podprzestrzeni U względem τ pozwala znaleźć bazę przestrzeni V względem której macierz endomorfizmu τ ma klatkę zer w lewym dolnym rogu o rozmiarach $(n - r) \times r$.

Macierz endomorfizmu τ ma jeszcze prostszą postać, gdy przestrzeń V jest *sumą prostą* dwóch podprzestrzeni niezmienniczych U i W . Obieramy wtedy jakąkolwiek bazę $\mathcal{B}_1 = \{v_1, \dots, v_r\}$ podprzestrzeni U oraz jakąkolwiek bazę $\mathcal{B}_2 = \{v_{r+1}, \dots, v_n\}$ podprzestrzeni W i wobec $V = U \oplus W$ otrzymujemy, że $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ jest bazą przestrzeni V . Ponieważ $\tau(U) \subseteq U$ oraz $\tau(W) \subseteq W$, więc dla $j = 1, \dots, r$ oraz $i = 1, \dots, n - r$ mamy

$$\tau(v_j) \in \text{lin}\{\mathcal{B}_1\} \quad \text{oraz} \quad \tau(v_{r+i}) \in \text{lin}\{\mathcal{B}_2\}.$$

Zatem macierz endomorfizmu τ w bazie $\mathcal{B}$ ma postać macierzy klatkowej

$$m(\tau, \mathcal{B}) = \begin{bmatrix} A & 0 \\ 0 & C \end{bmatrix},$$

gdzie $A = m(\tau|_U, \mathcal{B}_1)$ oraz $C = m(\tau|_W, \mathcal{B}_2)$.

1.6 Podobieństwo

Przypomnimy teraz związek między macierzami $m(\tau, \mathcal{A})$ oraz $m(\tau, \mathcal{B})$ endomorfizmu τ w dwóch różnych uporządkowanych bazach $\mathcal{A}$ i $\mathcal{B}$ przestrzeni V . Niech więc $\mathcal{A} = \{u_1, \dots, u_n\}$ i $\mathcal{B} = \{v_1, \dots, v_n\}$ będą uporządkowanymi bazami przestrzeni V i niech $m(\tau, \mathcal{A}) = [a_{ij}] =: A$ oraz $m(\tau, \mathcal{B}) = [b_{ij}] =: B$. Zatem

$$\tau(u_j) = \sum_{i=1}^n a_{ij} u_i, \quad \tau(v_j) = \sum_{i=1}^n b_{ij} v_i$$

dla $j = 1, \dots, n$. Obieramy endomorfizm $\sigma \in \text{End}_K V$ taki, że

$$\sigma(u_j) = v_j, \quad j = 1, \dots, n.$$

Wtedy σ przeprowadza bazę przestrzeni V na bazę V , zatem jest automorfizmem przestrzeni V oraz

$$\tau\sigma(u_j) = \tau(v_j) = \sum_{i=1}^n b_{ij} v_i = \sum_{i=1}^n b_{ij} \sigma(u_i) = \sigma\left(\sum_{i=1}^n b_{ij} u_i\right).$$

Wynika stąd, że

$$\sigma^{-1}\tau\sigma(u_j) = \sum_{i=1}^n b_{ij} u_i,$$

dla $j = 1, \dots, n$. Równości te pokazują, że endomorfizm $\sigma^{-1}\tau\sigma$ ma w bazie $\mathcal{A}$ macierz B , to znaczy, $\mathbf{m}(\sigma^{-1}\tau\sigma, \mathcal{A}) = B$. Niech $S := \mathbf{m}(\sigma, \mathcal{A})$. Wtedy

$$B = \mathbf{m}(\sigma^{-1}\tau\sigma, \mathcal{A}) = \mathbf{m}(\sigma^{-1}, \mathcal{A}) \mathbf{m}(\tau, \mathcal{A}) \mathbf{m}(\sigma, \mathcal{A}) = S^{-1}AS.$$

Udowodniliśmy więc następujące twierdzenie.

Twierdzenie 1.6.1. *Jeśli A i B są macierzami endomorfizmu τ w uporządkowanych bazach $\mathcal{A}$ i $\mathcal{B}$ przestrzeni V i jeśli $S = \mathbf{m}(\sigma, \mathcal{A})$ jest macierzą endomorfizmu σ przeprowadzającego bazę $\mathcal{A}$ na bazę $\mathcal{B}$, to $B = S^{-1}AS$, to znaczy*

$$\mathbf{m}(\tau, \mathcal{B}) = \mathbf{m}(\sigma, \mathcal{A})^{-1} \cdot \mathbf{m}(\tau, \mathcal{A}) \cdot \mathbf{m}(\sigma, \mathcal{A}).$$

Uwaga 1.6.1. Macierz $S = \mathbf{m}(\sigma, \mathcal{A})$ można także interpretować jako *macierz przejścia* od bazy $\mathcal{A}$ do bazy $\mathcal{B}$. Jeśli bowiem $S = [s_{ij}]$, to

$$v_j = \sigma(u_j) = \sum_{i=1}^n s_{ij}u_i, \quad j = 1, \dots, n.$$

Definicja 1.6.1. Macierze $A, B \in M_n(K)$ nazywamy *podobnymi* lub *sprzężonymi*, jeśli istnieje macierz odwracalna $S \in M_n(K)$ taka, że

$$B = S^{-1}AS.$$

Podobieństwo macierzy jest relacją równoważnościową w algebrze macierzy $M_n(K)$. Twierdzenie 1.6.1 orzeka, że macierze endomorfizmu τ w różnych bazach przestrzeni V są podobne.

Definicja 1.6.2. Endomorfizmy ρ i τ przestrzeni V nazywamy endomorfizmami *podobnymi* lub *sprzężonymi*, jeśli istnieje automorfizm σ przestrzeni V taki, że

$$\rho = \sigma^{-1}\tau\sigma.$$

Łatwo sprawdzić, że relacja podobieństwa endomorfizmów jest relacją równoważności w algebrze $\text{End}_K V$.

Twierdzenie 1.6.2. *Dla endomorfizmów ρ i τ przestrzeni V następujące warunki są równoważne:*

- (a) ρ i τ są podobne.
- (b) Dla każdej uporządkowanej bazy $\mathcal{A}$ przestrzeni V macierze $\mathbf{m}(\rho, \mathcal{A})$ i $\mathbf{m}(\tau, \mathcal{A})$ są podobne.
- (c) Dla każdej uporządkowanej bazy $\mathcal{A}$ przestrzeni V istnieje uporządkowana baza $\mathcal{B}$ przestrzeni V taka, że

$$\mathbf{m}(\rho, \mathcal{A}) = \mathbf{m}(\tau, \mathcal{B}).$$

Dowód. (a) $\Rightarrow$ (b) Niech $\rho = \sigma^{-1}\tau\sigma$, gdzie $\sigma \in \text{Aut } V$ i niech $\mathcal{A}$ będzie dowolną bazą przestrzeni V . Wtedy

$$\mathbf{m}(\rho, \mathcal{A}) = \mathbf{m}(\sigma^{-1}\tau\sigma, \mathcal{A}) = S^{-1} \cdot \mathbf{m}(\tau, \mathcal{A}) \cdot S,$$

gdzie $S = \mathbf{m}(\sigma, \mathcal{A})$. A więc macierze $\mathbf{m}(\rho, \mathcal{A})$ i $\mathbf{m}(\tau, \mathcal{A})$ są podobne.

(b) $\Rightarrow$ (c) Niech $\mathbf{m}(\rho, \mathcal{A}) = S^{-1} \cdot \mathbf{m}(\tau, \mathcal{A}) \cdot S$, gdzie S jest macierzą odwracalną. Obieramy automorfizm σ przestrzeni V taki, że $S = \mathbf{m}(\sigma, \mathcal{A})$. Niech $\mathcal{B} = \sigma(\mathcal{A})$. Wtedy $\mathcal{B}$ jest bazą przestrzeni V i na podstawie twierdzenia 1.6.1 mamy $S^{-1}\mathbf{m}(\tau, \mathcal{A})S = \mathbf{m}(\tau, \mathcal{B})$. A więc

$$m(\rho, \mathcal{A}) = m(\tau, \mathcal{B}).$$

(c) $\Rightarrow$ (a) Niech σ będzie automorfizmem przestrzeni V przeprowadzającym bazę $\mathcal{A}$ na bazę $\mathcal{B}$. Wtedy na podstawie (c) i twierdzenia 1.6.1 mamy

$$m(\rho, \mathcal{A}) = m(\tau, \mathcal{B}) = m(\sigma, \mathcal{A})^{-1} \cdot m(\tau, \mathcal{A}) \cdot m(\sigma, \mathcal{A}) = m(\sigma^{-1}\tau\sigma, \mathcal{A}).$$

Endomorfizmy ρ i $\sigma^{-1}\tau\sigma$ mają więc równe macierze w bazie $\mathcal{A}$ skąd wynika, że $\rho = \sigma^{-1}\tau\sigma$. A więc (c) $\Rightarrow$ (a). $\square$

Jak widzimy, endomorfizmy podobne mają wiele wspólnych własności. Naturalnym problemem jest więc klasyfikacja endomorfizmów przestrzeni V ze względu na podobieństwo endomorfizmów. Problem ten jest ściśle związany z klasyfikacją macierzy w $M_n(K)$ ze względu na podobieństwo macierzy.

Jeśli bowiem ustalimy uporządkowaną bazę $\mathcal{A}$ przestrzeni V i każdemu endomorfizmowi τ przestrzeni V przyporządkujemy macierz $\mu(\tau) = A = m(\tau, \mathcal{A})$ endomorfizmu τ względem bazy $\mathcal{A}$, to jak wiemy, otrzymujemy izomorfizm K -algebr

$$\mu : \text{End}_K V \rightarrow M_n(K).$$

Ten izomorfizm przeprowadza klasy endomorfizmów podobnych na klasy macierzy podobnych:

$$\mu\{\sigma^{-1}\tau\sigma : \sigma \in \text{Aut } V\} = \{S^{-1}AS : S \in \mathbf{GL}(n, K)\},$$

gdzie $\mu(\sigma) = S$ dla $\sigma \in \text{Aut } V$. Tutaj $\text{Aut } V$ oznacza grupę automorfizmów przestrzeni V natomiast $\mathbf{GL}(n, K)$ oznacza grupę macierzy odwracalnych w $M_n(K)$. A więc μ przeprowadza klasę endomorfizmów podobnych do τ na zbiór macierzy endomorfizmu τ we wszystkich bazach przestrzeni V (lub równoważnie, na zbiór macierzy wszystkich endomorfizmów podobnych do τ , w ustalonej bazie $\mathcal{A}$ przestrzeni V).

Ta obserwacja jest podstawą klasyfikacji endomorfizmów przestrzeni wektorowej i poszukiwania postaci kanonicznych macierzy endomorfizmów. Z każdym endomorfizmem τ przestrzeni V wiążemy klasę macierzy tego endomorfizmu we wszystkich bazach przestrzeni V i znajdujemy w tej klasie macierze szczególnych postaci, które opisują przejrzyście działanie endomorfizmu τ na odpowiadających tym macierzom bazach przestrzeni wektorowej V . Są to tak zwane postaci kanoniczne macierzy endomorfizmu τ .

1.7 Triangularyzacja i diagonalizacja

Przytoczymy tu bez dowodu twierdzenia wskazujące warunki konieczne i wystarczające na to by dla danego endomorfizmu τ przestrzeni wektorowej V istniała baza V względem której macierz τ jest trójkątna lub diagonalna.

Macierz $A = [a_{ij}] \in M_n(K)$ nazywamy macierzą *diagonalną*, jeśli $a_{ij} = 0$ dla $i \neq j$. Piszemy wówczas $A = \text{diag}(a_{11}, a_{22}, \dots, a_{nn})$.

Macierz $A = [a_{ij}] \in M_n(K)$ nazywamy macierzą *trójkątną*, jeśli wszystkie elementy pod główną przekątną są równe zero (to znaczy, jeśli $a_{ij} = 0$ dla $i > j$), lub gdy wszystkie elementy nad główną przekątną są równe zero (to znaczy, $a_{ij} = 0$ dla $i < j$). W pierwszym przypadku mówimy, że A jest górna trójkątna, w drugim, że jest dolna trójkątna.

TWIERDZENIE 1.7.1. *Endomorfizm $\tau \in \text{End}_K V$ ma macierz trójkątną w pewnej bazie przestrzeni V wtedy i tylko wtedy, gdy wielomian minimalny p_τ endomorfizmu τ rozkłada się nad ciałem K na iloczyn czynników liniowych:*

$$p_\tau = (X - b_1) \cdots (X - b_k), \quad b_1, \dots, b_k \in K.$$

Twierdzenie 1.7.2. Niech endomorfizm $\tau \in \text{End}_K V$ ma macierz trójkątną $A = [a_{ij}]$ w pewnej bazie przestrzeni V . Wtedy

(a) Wielomian minimalny p_τ endomorfizmu τ jest dzielnikiem wielomianu

$$(X - a_{11}) \cdots (X - a_{nn}).$$

(b) Każda wartość własna endomorfizmu τ występuje przynajmniej jeden raz wśród elementów diagonalnych a_{jj} macierzy A .

(c) Każdy element diagonalny a_{jj} macierzy A jest wartością własną endomorfizmu τ .

A oto odpowiednie twierdzenia o endomorfizmach diagonalizowalnych.

Twierdzenie 1.7.3. Endomorfizm $\tau \in \text{End}_K V$ ma macierz diagonalną w pewnej bazie przestrzeni V wtedy i tylko wtedy, gdy wielomian minimalny p_τ endomorfizmu τ rozkłada się nad ciałem K na iloczyn parami różnych czynników liniowych:

$$p_\tau = (X - b_1) \cdots (X - b_k), \quad b_1, \dots, b_k \in K, \quad b_i \neq b_j \quad \text{dla} \quad i \neq j.$$

Twierdzenie 1.7.4. Jeśli endomorfizm $\tau \in \text{End}_K V$ ma macierz diagonalną w pewnej bazie przestrzeni V oraz $b_1, \dots, b_k \in K$ są wszystkimi parami różnymi elementami ciała K występującymi na przekątnej macierzy diagonalnej endomorfizmu τ , to wielomian minimalny p_τ ma postać

$$p_\tau = (X - b_1) \cdots (X - b_k).$$

Rozdział 2

Funkcjonały dwuliniowe

Ostatnie zmiany 19.04.2009 r.

2.1 Przestrzenie dwuliniowe

DEFINICJA 2.1.1. *Przestrzenią dwuliniową nad ciałem K nazywamy parę (V, β) , gdzie V jest skończone wymiarową przestrzenią wektorową nad ciałem K oraz*

$$\beta : V \times V \rightarrow K$$

jest funkcjonalem dwuliniowym na przestrzeni V .

To ostatnie oznacza, że β spełnia

$$\beta(ax + by, z) = a\beta(x, z) + b\beta(y, z),$$

$$\beta(x, ay + bz) = a\beta(x, y) + b\beta(x, z),$$

dla wszystkich $x, y, z \in V$ i wszystkich $a, b \in K$.

Jeśli U jest podprzestrzenią przestrzeni wektorowej V , to zacieśnienie $\alpha = \beta|_{U \times U}$ funkcjonala β do podprzestrzeni U jest oczywiście funkcjonalem dwuliniowym na przestrzeni U . Parę (U, α) nazywamy *podprzestrzenią* przestrzeni dwuliniowej (V, β) .

Będziemy stale stosować następujące uproszczenia w oznaczeniach.

Po pierwsze, zamiast pisać (V, β) będziemy także używać symbolu V dla oznaczenia przestrzeni dwuliniowej.

Po drugie, zamiast $\beta(x, y)$ piszemy często po prostu (x, y) .

Po trzecie, dla dowolnego wektora $x \in V$ wprowadzamy oznaczenie $q(x) := (x, x)$. Określona w ten sposób funkcja

$$q : V \rightarrow K$$

ma następujące własności:

$$q(ax) = a^2q(x), \quad q(x + y) - q(x) - q(y) = (x, y) + (y, x)$$

dla dowolnych $a \in K, x, y \in V$. Funkcję q nazywamy funkcjonalem *kwadratowym* stowarzyszonym z funkcjonalem dwuliniowym $(\ , \)$.

DEFINICJA 2.1.2. Niech V będzie przestrzenią dwuliniową z funkcjonalem dwuliniowym $(\ , \)$ i stowarzyszonym funkcjonalem kwadratowym q .

1. Wektor $x \in V$ nazywa się *izotropowy*, jeśli $x \neq 0$ i $q(x) = 0$. Jeśli $q(x) \neq 0$, to x nazywa się *nieizotropowy*.

2. Przestrzeń V nazywa się *izotropowa*, jeśli zawiera wektor izotropowy. W przeciwnym przypadku przestrzeń nazywa się *nieizotropowa*.
3. Przestrzeń V nazywa się *symetryczna* jeśli funkcjonal $(\ , \)$ jest symetryczny, to znaczy jeśli

$$(x, y) = (y, x) \quad \text{dla wszystkich } x, y \in V.$$

4. Jeśli V jest przestrzenią symetryczną, to mówimy, że wektory $x, y \in V$ są *ortogonalne* lub *prostopadłe* jeśli $(x, y) = 0$.

Zauważmy, że pojęcie prostopadłości wektorów wprowadzamy jedynie dla przestrzeni symetrycznych. Dzięki temu relacja prostopadłości wektorów jest symetryczna: jeśli $(x, y) = 0$, to także $(y, x) = 0$. Ponadto, w przestrzeni symetrycznej, dla każdych $x, y \in V$ mamy

$$q(x + y) - q(x) - q(y) = 2(x, y).$$

Przykład 2.1.1. *Przestrzenią euklidesową* nazywamy symetryczną przestrzeń dwuliniową V nad ciałem $\mathbb{R}$ liczb rzeczywistych, w której $q(x) > 0$ dla każdego niezerowego wektora $x \in V$. Przestrzeń euklidesowa jest więc nieizotropowa. Standardowym przykładem n -wymiarowej przestrzeni euklidesowej jest przestrzeń współrzędnych $\mathbb{R}^n$ z funkcjonalem dwuliniowym $(\ , \)$ określonym formułą

$$((x_1, \dots, x_n), (y_1, \dots, y_n)) = x_1 y_1 + \dots + x_n y_n.$$

Dla wektora $x = (x_1, \dots, x_n) \in \mathbb{R}^n$ mamy

$$q(x) = x_1^2 + \dots + x_n^2.$$

Jest to zawsze nieujemna liczba rzeczywista. W związku z tym *długością* lub *normą* wektora x przestrzeni euklidesowej nazywa się liczbę $\|x\| = \sqrt{q(x)}$.

Przykład 2.1.2. Przestrzeń dwuliniowa (V, θ) , gdzie θ jest funkcjonalem zerowym (to znaczy, $\theta(x, y) = 0$ dla wszystkich $x, y \in V$) nazywa się *totalnie izotropowa*. Tutaj każdy niezerowy wektor jest izotropowy i każde dwa wektory są ortogonalne.

Przykład 2.1.3. Niech $V = K^2$ będzie 2-wymiarową przestrzenią współrzędnych nad dowolnym ciałem K . Definiujemy funkcjonal Δ na przestrzeni V kładąc

$$\Delta : K^2 \times K^2 \rightarrow K,$$

$$\Delta((x_1, x_2), (y_1, y_2)) := \det \begin{bmatrix} x_1 & y_1 \\ x_2 & y_2 \end{bmatrix}.$$

Z dobrze znanych własności wyznaczników macierzy otrzymujemy

1. Δ jest funkcjonalem dwuliniowym na przestrzeni K^2 .
2. Każdy niezerowy wektor przestrzeni dwuliniowej (K^2, Δ) jest izotropowy:

$$q(x) = \Delta(x, x) = 0 \quad \text{dla wszystkich } x \in K^2.$$

3. Dwa wektory x, y są ortogonalne, $\Delta(x, y) = 0$, wtedy i tylko wtedy gdy są proporcjonalne (to znaczy gdy są równoległe!).

Przykład 2.1.4. Rozpatrzmy teraz przestrzeń współrzędnych $\mathbb{C}^n$ nad ciałem liczb zespolonych $\mathbb{C}$ i określmy funkcjonał

$$\chi : \mathbb{C}^n \times \mathbb{C}^n \rightarrow \mathbb{C},$$

$$\chi((x_1, \dots, x_n), (y_1, \dots, y_n)) = x_1 \bar{y}_1 + \dots + x_n \bar{y}_n,$$

gdzie $\bar{a}$ oznacza liczbę sprzężoną z $a \in \mathbb{C}$. Łatwo sprawdzić, że χ jest funkcjonałem liniowym ze względu na pierwszą zmienną i jest addytywny ze względu na drugą zmienną:

$$\chi(ax + by, z) = a\chi(x, z) + b\chi(y, z),$$

$$\chi(x, y + z) = \chi(x, y) + \chi(x, z),$$

dla wszystkich $x, y, z \in \mathbb{C}^n$ i wszystkich $a, b \in \mathbb{C}$. Jednakże χ *nie jest* funkcjonałem liniowym ze względu na drugą zmienną. Mamy natomiast

$$\chi(x, ay) = \bar{a}\chi(x, y).$$

Tak więc, zgodnie z definicją 2.1.1, $(\mathbb{C}^n, \chi)$ nie jest przestrzenią dwuliniową. Nazywamy ją przestrzenią półtoraliniową (lub hermitowską lub unitarną).

Prawie wszystko co powiedzieliśmy powyżej o przestrzeniach euklidesowych przenosi się na przestrzenie unitarne. Funkcjonał χ jest bardzo bliski symetrii ma bowiem własność

$$\chi(x, y) = \overline{\chi(y, x)}.$$

Ponadto, $q(x) = \chi(x, x)$ dla dowolnego wektora $x \in \mathbb{C}^n$, jest dodatnią liczbą rzeczywistą co wynika natychmiast z definicji:

$$q(x) = x_1 \bar{x}_1 + \dots + x_n \bar{x}_n = |x_1|^2 + \dots + |x_n|^2$$

dla $x = (x_1, \dots, x_n) \in \mathbb{C}^n$. Tak więc przestrzeń unitarna jest nieizotropowa i możemy wprowadzić długość wektora $x \in \mathbb{C}^n$ używając tej samej formuły $\sqrt{q(x)}$, której użyliśmy w przypadku przestrzeni euklidesowej.

2.2 Przestrzenie dwuliniowe i kongruencja macierzy

Niech V będzie przestrzenią dwuliniową nad ciałem K i niech $\mathcal{B} = \{v_1, \dots, v_n\}$ będzie pewną bazą przestrzeni wektorowej V . Macierz

$$A := [(v_i, v_j)]$$

nazywamy macierzą przestrzeni dwuliniowej V względem bazy $\mathcal{B}$. Piszemy

$$V \cong A \text{ w bazie } \mathcal{B}$$

gdy A jest macierzą V względem bazy $\mathcal{B}$, a także

$$V \cong A$$

gdy A jest macierzą V względem jakiejś bazy przestrzeni V .

Zauważmy, że działanie funkcjonału dwuliniowego $(\ , \)$ na przestrzeni V jest opisane w

sposób kompletny poprzez macierz A przestrzeni V .

Rzeczywiście, dla $x, y \in V$, gdzie $x = \sum_i x_i v_i$, $y = \sum_j y_j v_j$, $x_i, y_j \in K$, mamy

$$(x, y) = \sum_i \sum_j x_i y_j (v_i, v_j), \quad (2.1)$$

a także

$$q(x) = (x, x) = \sum_i \sum_j x_i x_j (v_i, v_j). \quad (2.2)$$

Znając macierz $A = [(v_i, v_j)]$ oraz współrzędne wektorów x, y w bazie $\mathcal{B}$ możemy znaleźć wartość funkcjonału dwuliniowego (x, y) a także normę $q(x)$ posługując się formułami (2.1) i (2.2).

Spróbujemy teraz opisać zbiór $\text{Bil } V$ *wszystkich* funkcjonałów dwuliniowych, jakie można określić na przestrzeni wektorowej V nad ciałem K . Zauważyliśmy już, że jeśli obierzemy bazę $\mathcal{B}$ przestrzeni V , to każdy funkcjonał dwuliniowy na V wyznacza macierz kwadratową zależną od bazy $\mathcal{B}$ i jest jednoznacznie wyznaczony przez tę macierz. Tak więc przy ustalonej bazie $\mathcal{B} = \{v_1, \dots, v_n\}$ przestrzeni V mamy odwzorowanie

$$\begin{aligned} \text{Bil } V &\rightarrow M_n(K) \\ \beta &\mapsto [\beta(v_i, v_j)], \end{aligned} \quad (2.3)$$

gdzie $M_n(K)$ jest zbiorem wszystkich $n \times n$ macierzy o elementach z ciała K . To odwzorowanie jest injektywne, gdyż z (2.1) wynika, że dwa funkcjonały dwuliniowe mające tę samą macierz względem bazy $\mathcal{B}$ są równe. Można także łatwo pokazać, że odwzorowanie (2.3) jest surjektywne.¹ Tak więc funkcjonały dwuliniowe na przestrzeni V są we wzajemnie jednoznacznej odpowiedniości z macierzami kwadratowymi stopnia $n = \dim V$. Zauważmy, że w tej odpowiedniości *symetrycznym* funkcjonałom dwuliniowym odpowiadają macierze *symetryczne*.

Zbadamy teraz, w jaki sposób odwzorowanie (2.3) zależy od wyboru bazy $\mathcal{B}$ przestrzeni wektorowej V . Niech więc $\mathcal{B} = \{v_1, \dots, v_n\}$ oraz $\mathcal{B}' = \{w_1, \dots, w_n\}$ będą bazami przestrzeni V i niech

$$V \cong A = [a_{ij}] \text{ w bazie } \mathcal{B} \text{ oraz } V \cong C = [c_{ij}] \text{ w bazie } \mathcal{B}'. \quad (2.4)$$

Każdy wektor w_j bazy $\mathcal{B}'$ przedstawiamy jako kombinację liniową wektorów bazy $\mathcal{B}$,

$$\begin{aligned} w_1 &= p_{11}v_1 + p_{12}v_2 + \dots + p_{1n}v_n, \\ &\vdots \\ w_n &= p_{n1}v_1 + p_{n2}v_2 + \dots + p_{nn}v_n. \end{aligned} \quad (2.5)$$

Macierz $P := [p_{ij}]$ nazywa się *macierzą przejścia* od bazy $\mathcal{B}$ do bazy $\mathcal{B}'$. Z kursowego wykładu algebry liniowej wiemy, że macierz przejścia P jest macierzą nieosobliwą. Wobec (2.4) i (2.5) otrzymujemy

$$\begin{aligned} c_{ij} = (w_i, w_j) &= \left(\sum_s p_{is} v_s, \sum_t p_{jt} v_t \right) \\ &= \sum_s \sum_t p_{is} (v_s, v_t) p_{jt} \\ &= \sum_t \sum_s p_{is} a_{st} p_{jt}. \end{aligned}$$

Tutaj $d_{it} := \sum_s p_{is} a_{st}$ jest elementem i -tego wiersza i t -tej kolumny macierzy $P \cdot A$, natomiast $c_{ij} = \sum_t d_{it} p_{jt}$ jest elementem i -tego wiersza i j -tej kolumny macierzy $PA \cdot P^t$. A więc $C = PAP^t$.

¹Zob. K. Szymiczek, *Wykłady z algebry dwuliniowej*, Skrypt UŚ 1991, str. 24.

DEFINICJA 2.2.1. Macierze $A, C \in M_n(K)$ nazywamy *kongruentnymi*, jeśli istnieje macierz nieosobliwa $P \in M_n(K)$ taka, że $C = PAP^t$. Piszemy wtedy $A \cong C$.

Podsumujemy naszą analizę zależności odwzorowania (2.3) od wyboru bazy w przestrzeni V następująco.

TWIERDZENIE 2.2.1. Niech V będzie przestrzenią dwuliniową i niech $\mathcal{B}$ oraz $\mathcal{B}'$ będą bazami przestrzeni V . Jeśli

$$V \cong A \text{ w bazie } \mathcal{B} \text{ oraz } V \cong C \text{ w bazie } \mathcal{B}',$$

to A i C są macierzami kongruentnymi: $A \cong C$. Dokładniej, jeśli P jest macierzą przejścia od bazy $\mathcal{B}$ do bazy $\mathcal{B}'$, to

$$C = PAP^t.$$

Okazuje się, że kongruentność macierzy A i C jest nie tylko warunkiem koniecznym, ale także wystarczającym na to, by A i C były macierzami tej samej przestrzeni dwuliniowej.

TWIERDZENIE 2.2.2. Niech V będzie przestrzenią dwuliniową z bazą $\mathcal{B}$. Załóżmy, że $V \cong A$ w bazie $\mathcal{B}$. Wtedy macierz C jest macierzą przestrzeni dwuliniowej V względem pewnej bazy $\mathcal{B}'$ przestrzeni V wtedy i tylko wtedy gdy $A \cong C$.

Dowód. Pozostaje pokazać, że $V \cong A$ i $A \cong C \Rightarrow V \cong C$.

Założmy więc, że $V \cong A$ w bazie $\mathcal{B} = \{v_1, \dots, v_n\}$ i założmy, że istnieje macierz nieosobliwa P taka, że $C = PAP^t$. Obieramy wektory $w_1, \dots, w_n$ spełniające (2.5). Nieosobliwość P pociąga, że wektory te tworzą bazę przestrzeni V . Oznaczmy tę nową bazę przez $\mathcal{B}'$. Wtedy P jest macierzą przejścia od $\mathcal{B}$ do $\mathcal{B}'$. Odwracając teraz kolejność argumentów użytych do wyznaczenia elementów c_{ij} w dowodzie twierdzenia 2.2.1 stwierdzamy, że równość $C = PAP^t$ pociąga $c_{ij} = (w_i, w_j)$. Tak więc C jest macierzą przestrzeni dwuliniowej V względem bazy $\mathcal{B}'$. $\square$

Z twierdzenia 2.2.1 wynika, że wyznacznik macierzy przestrzeni dwuliniowej V zależy od wyboru bazy przestrzeni V . Jeśli bowiem A i C są macierzami tej samej przestrzeni dwuliniowej V względem baz $\mathcal{B}$ i $\mathcal{B}'$, to

$$\det C = (\det P)^2 \cdot \det A, \tag{2.6}$$

gdzie P jest macierzą przejścia od bazy $\mathcal{B}$ do bazy $\mathcal{B}'$. Wyznaczniki A i C różnią się więc czynnikiem, który jest kwadratem pewnego niezerowego elementu ciała K .

2.3 Izometrie przestrzeni dwuliniowych

DEFINICJA 2.3.1. Niech (U, α) i (V, β) będą przestrzeniami dwuliniowymi nad tym samym ciałem K . Izomorfizm $i : U \rightarrow V$ przestrzeni wektorowych U i V nazywamy *izometrią* przestrzeni dwuliniowych (U, α) i (V, β) jeśli zachowuje on funkcjonały dwuliniowe α i β , to znaczy, jeśli

$$\alpha(x, y) = \beta(i(x), i(y)) \text{ dla wszystkich } x, y \in U.$$

Jeśli istnieje izometria i między (U, α) i (V, β) , to mówimy, że przestrzenie te są *izometryczne* i piszemy

$$(U, \alpha) \cong (V, \beta).$$

Dla zaznaczenia, że odwzorowanie i jest izometrią piszemy

$$i : (U, \alpha) \cong (V, \beta).$$

Zauważmy, że jeśli $i : (U, \alpha) \cong (V, \beta)$, to

$$\alpha(x, y) = 0 \Leftrightarrow \beta(i(x), i(y)) = 0,$$

a więc izometria i zachowuje ortogonalność wektorów,

$$q_\alpha(x) := \alpha(x, x) = \beta(i(x), i(x)) =: q_\beta(i(x)),$$

a więc izometria i zachowuje funkcjonały kwadratowe stowarzyszone z funkcjonałami dwuliniowymi α, β , a także

$$q_\alpha(x) = 0 \Leftrightarrow q_\beta(i(x)) = 0,$$

to znaczy izometria i zachowuje izotropowość wektorów (i przestrzeni).

Przykład 2.3.1. Jeśli (U, α) jest przestrzenią euklidesową oraz $(U, \alpha) \cong (V, \beta)$, to (V, β) także jest przestrzenią euklidesową, gdyż izometria zachowuje funkcjonały kwadratowe, a zatem także ich dodatniość.

Pokażemy teraz, że problem klasyfikacji n -wymiarowych przestrzeni dwuliniowych nad ciałem K ze względu na izometrię jest równoważny klasyfikacji $n \times n$ macierzy o elementach z ciała K ze względu na kongruencję macierzy.

TWIERDZENIE 2.3.1. Niech (U, α) i (V, β) będą przestrzeniami dwuliniowymi nad ciałem K . Załóżmy, że A i B są macierzami (U, α) i (V, β) względem jakichkolwiek baz przestrzeni U i V :

$$(U, \alpha) \cong A \quad \text{ i } \quad (V, \beta) \cong B.$$

Wtedy

$$(U, \alpha) \cong (V, \beta) \Leftrightarrow A \cong B.$$

Dowód. Niech $\{u_1, \dots, u_n\}$ i $\{v_1, \dots, v_n\}$ będą bazami U i V takimi, że

$$(U, \alpha) \cong A \quad \text{ w bazie } \{u_1, \dots, u_n\},$$

$$(V, \beta) \cong B \quad \text{ w bazie } \{v_1, \dots, v_n\}.$$

Jeśli $i : U \rightarrow V$ jest izometrią, to $\{i(u_1), \dots, i(u_n)\}$ jest bazą przestrzeni V oraz $[\beta(i(u_k), i(u_l))] = [\alpha(u_k, u_l)] = A$, zatem

$$(V, \beta) \cong A \quad \text{ w bazie } \{i(u_1), \dots, i(u_n)\}.$$

Niech P będzie macierzą przejścia od bazy $\{i(u_1), \dots, i(u_n)\}$ przestrzeni V do bazy $\{v_1, \dots, v_n\}$. Wtedy $B = PAP^t$ na podstawie twierdzenia 2.2.1 czyli $A \cong B$.

Założmy teraz, że $B = PAP^t$, gdzie P jest macierzą nieosobliwą. Rozpatrzmy bazę $\{u'_1, \dots, u'_n\}$ przestrzeni U otrzymaną z bazy $\{u_1, \dots, u_n\}$ przy pomocy macierzy przejścia P . Wtedy na podstawie twierdzenia 2.2.1 mamy

$$[\alpha(u'_k, u'_l)] = PAP^t = B.$$

A więc przestrzenie (U, α) i (V, β) mają tę samą macierz B względem odpowiednio dobranych baz. Pokażemy iż wynika stąd, że przestrzenie U i V są izometryczne.

Niech $i : U \rightarrow V$ będzie jedynym izomorfizmem przestrzeni wektorowych spełniającym $i(u'_k) = v_k$ dla $k = 1, \dots, n$.

Wtedy dla dowolnych wektorów $x = \sum_k x_k u'_k$, $y = \sum_l y_l u'_l$ przestrzeni U mamy

$$\alpha(x, y) = \sum_k \sum_l x_k y_l \alpha(u'_k, u'_l) = \sum_k \sum_l x_k y_l \beta(v_k, v_l) = \beta(i(x), i(y)).$$

Zatem i jest izometrią. □

2.4 Nieosobliwość przestrzeni dwuliniowych

W dalszym ciągu zajmujemy się wyłącznie *symetrycznymi* przestrzeniami dwuliniowymi. Od tego miejsca termin *przestrzeń dwuliniowa* jest skrótem dla *symetrycznej przestrzeni dwuliniowej*.

DEFINICJA 2.4.1. Niech V będzie przestrzenią dwuliniową nad dowolnym ciałem K . Zbiór

$$\text{rad}V := \{v \in V : (v, x) = 0 \text{ dla wszystkich } x \in V\}$$

nazywamy *radykałem* przestrzeni dwuliniowej V .

Łatwo sprawdzić, że radykał $\text{rad}V$ jest podprzestrzenią przestrzeni wektorowej V . Jest to totalnie izotropowa podprzestrzeń przestrzeni dwuliniowej V . Zauważmy, że założenie iż funkcjonal dwuliniowy jest symetryczny uwalnia nas od konieczności rozróżniania lewo- i prawostronnych radykałów.

DEFINICJA 2.4.2. Przestrzeń dwuliniowa V nazywa się *nieosobliwa* jeśli $\text{rad}V = 0$. W przeciwnym przypadku przestrzeń V nazywa się *osobliwa*.

Zauważmy, że zgodnie z tą definicją przestrzeń zerowa (składająca się tylko z wektora zerowego) jest nieosobliwa. W dalszym ciągu milcząco zakładamy, że rozpatrywane przestrzenie są niezerowe. Zauważmy także, że każda przestrzeń euklidesowa jest nieosobliwa. Rzeczywiście, jeśli $v \neq 0$, to $(v, v) > 0$, a więc v nie należy do $\text{rad}V$. Ogólniej, każda przestrzeń nieizotropowa jest nieosobliwa.

W szczególności, jeśli $v \in V$ jest wektorem nieizotropowym, to jednowymiarowa podprzestrzeń $S = Kv$ jest nieizotropowa (bo dla niezerowego wektora $av \in S$, gdzie $0 \neq a \in K$, mamy $(av, av) = a^2(v, v) \neq 0$), zatem jest nieosobliwa.

Pokażemy teraz, że wyznaczenie radykału przestrzeni dwuliniowej sprowadza się do rozwiązania pewnego układu równań liniowych.

STWIERDZENIE 2.4.1. Niech $\{v_1, \dots, v_n\}$ będzie bazą przestrzeni dwuliniowej V i niech $v \in V$. Wtedy

$$v \in \text{rad}V \Leftrightarrow (v, v_k) = 0 \text{ dla } k = 1, \dots, n.$$

Dowód. Konieczność tych warunków jest oczywista. Z drugiej strony, jeśli $(v, v_k) = 0$ dla $k = 1, \dots, n$, to dla każdego wektora $x = x_1v_1 + \dots + x_nv_n$ przestrzeni V mamy

$$(v, x) = x_1(v, v_1) + \dots + x_n(v, v_n) = 0,$$

zatem $v \in \text{rad}V$. □

Na podstawie stwierdzenia 2.4.1 wektor $v = x_1v_1 + \dots + x_nv_n$ należy do radykału przestrzeni V wtedy i tylko wtedy gdy

$$x_1(v_1, v_k) + \dots + x_n(v_n, v_k) = 0 \text{ dla } k = 1, \dots, n,$$

to znaczy wtedy i tylko wtedy gdy współrzędne wektora v spełniają układ równań liniowych jednorodnych, którego macierzą współczynników przy niewiadomych jest macierz $[(v_i, v_k)]$ przestrzeni dwuliniowej V w pewnej bazie tej przestrzeni. Przestrzeń V jest więc nieosobliwa wtedy i tylko wtedy gdy ten układ równań ma tylko rozwiązanie zerowe. Udowodniliśmy więc następujące kryterium nieosobliwości przestrzeni dwuliniowej.

TWIERDZENIE 2.4.1. Niech V będzie niezerową przestrzenią dwuliniową nad dowolnym ciałem K i niech A będzie macierzą przestrzeni V względem jakiejkolwiek bazy przestrzeni V . Przestrzeń V jest nieosobliwa wtedy i tylko wtedy gdy $\det A \neq 0$.

Z tego twierdzenia łatwo wynika, że przestrzeń nieosobliwa nie musi być nieizotropowa. Na przykład, dwuwymiarowa przestrzeń dwuliniowa z bazą $\{u, v\}$, względem której funkcjonał dwuliniowy ma macierz

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

jest nieosobliwa (gdyż $\det A \neq 0$), natomiast zawiera wektor izotropowy $u + v$.

Przystępujemy teraz do interpretacji nieosobliwości przestrzeni dwuliniowej przy pomocy pojęcia przestrzeni dualnej do danej przestrzeni wektorowej. Dla przestrzeni wektorowej V nad ciałem K *przestrzenią dualną* V^* nazywamy przestrzeń

$$V^* := \text{Hom}(V, K)$$

wszystkich *funkcjonałów liniowych* $\lambda : V \rightarrow K$, czyli homomorfizmów przestrzeni V nad ciałem K w jednowymiarową przestrzeń K nad K . Dodawanie funkcjonałów i mnożenie przez skalary z ciała K są zwykłymi działaniami dodawania funkcji i mnożenia funkcji przez skalar. A więc dla $\lambda, \mu \in V^*$ oraz dowolnego $a \in K$ mamy

$$\lambda + \mu : V \rightarrow K, \quad (\lambda + \mu)(v) = \lambda(v) + \mu(v), \quad a\lambda : V \rightarrow K, \quad (a\lambda)(v) = a \cdot \lambda(v)$$

dla każdego wektora $v \in V$.

Jeśli przestrzeń V jest skończenie wymiarowa, to $\dim V = \dim V^*$. Rzeczywiście, jeśli $v_1, \dots, v_n$ jest bazą przestrzeni V , to konstruujemy n funkcjonałów liniowych $v_1^*, \dots, v_n^*$ na przestrzeni V kładąc

$$v_i^*(v_j) = 0 \quad \text{gdy} \quad i \neq j \quad \text{oraz} \quad v_i^*(v_i) = 1$$

dla wszystkich $i = 1, 2, \dots, n$. Łatwo sprawdzić, że funkcjonały te są liniowo niezależne i rozpinają przestrzeń V^* . Jeśli bowiem $a_1 v_1^* + \dots + a_n v_n^* = 0 \in V^*$, to biorąc obraz wektora v_i poprzez funkcjonał $a_1 v_1^* + \dots + a_n v_n^*$ otrzymujemy $a_i = 0$. Z drugiej strony, jeśli $\lambda \in V^*$ jest dowolnym funkcjonałem oraz $\lambda(v_i) = a_i \in K$, to $a_1 v_1^* + \dots + a_n v_n^*$ oraz λ przyjmują równe wartości na wektorach bazy $v_1, \dots, v_n$ przestrzeni V , są zatem równe: $\lambda = a_1 v_1^* + \dots + a_n v_n^*$. Pokazaliśmy więc, że funkcjonały $v_1^*, \dots, v_n^*$ tworzą bazę przestrzeni dualnej V^* . Stąd $\dim V = \dim V^*$.

Gdy V jest przestrzenią dwuliniową istnieje bardzo prosty sposób konstruowania funkcjonałów liniowych na przestrzeni V . Ustalamy wektor $v \in V$ i wiążemy z nim odwzorowanie

$$\lambda_v : V \rightarrow K, \quad \lambda_v(x) = (x, v) \quad \text{dla} \quad x \in V.$$

Z liniowości $(\ , \)$ względem pierwszej zmiennej wynika natychmiast, że λ_v jest funkcjonałem liniowym na V , a więc jest elementem przestrzeni dualnej V^* . Okazuje się, że dla *nieosobliwego* funkcjonału dwuliniowego $(\ , \)$ ta konstrukcja daje *wszystkie* funkcjonały liniowe na V . Dla ustalenia tego faktu rozpatrzmy odwzorowanie

$$\Lambda_V : V \rightarrow V^*, \quad \Lambda_V(v) = \lambda_v.$$

LEMAT 2.4.1. *Niech V będzie przestrzenią dwuliniową nad dowolnym ciałem K . Wtedy*

- (a) Λ_V jest homomorfizmem przestrzeni wektorowych.
- (b) $\ker \Lambda_V = \text{rad} V$.

Dowód. (a) pozostawiamy jako łatwe ćwiczenie dla czytelnika.

(b) Wykorzystując jedynie definicje otrzymujemy

$$\begin{aligned}\ker \Lambda_V &= \{v \in V : \Lambda_V(v) = 0 \in V^*\} \\ &= \{v \in V : (x, v) = 0 \text{ dla wszystkich } x \in V\} \\ &= \text{rad}V.\end{aligned}$$

□

Twierdzenie 2.4.2. *Przestrzeń dwuliniowa V jest nieosobliwa wtedy i tylko wtedy gdy homomorfizm $\Lambda_V : V \rightarrow V^*$ jest izomorfizmem przestrzeni wektorowych.*

Dowód. Wykorzystamy następujący elementarny fakt z algebry liniowej. Jeśli V i U są skończone wymiarowymi przestrzeniami wektorowymi nad tym samym ciałem K oraz $\dim V = \dim U$, to homomorfizm $\chi : V \rightarrow U$ jest izomorfizmem przestrzeni wektorowych wtedy i tylko wtedy gdy χ jest injektywny (to znaczy, gdy $\ker \chi = 0$). Rzeczywiście, jeśli χ jest injektywny, to $\dim \chi(V) = \dim V = \dim U$, zatem $\chi(V) \subseteq U$ pociąga $\chi(V) = U$.

Rozpatrzmy teraz homomorfizm Λ_V przestrzeni wektorowej V w przestrzeń dualną V^* . Przestrzeń V ma skończony wymiar i jak wiemy $\dim V = \dim V^*$. Na podstawie powyższej uwagi wnioskujemy, że Λ_V jest izomorfizmem wtedy i tylko wtedy gdy Λ_V jest injektywny, to znaczy gdy $\ker \Lambda_V = 0$. Na podstawie lematu 2.4.1 jest to równoważne warunkowi $\text{rad}V = 0$, a więc nieosobliwości przestrzeni dwuliniowej V . □

Zauważmy jeszcze, że z twierdzenia 2.4.2 wynika rezultat znany jako twierdzenie Riesa o reprezentacji. Twierdzenie to mówi, że dla każdego funkcjonału liniowego $\lambda : V \rightarrow K$ na skończone wymiarowej nieosobliwej przestrzeni dwuliniowej V istnieje dokładnie jeden wektor $v \in V$ taki, że

$$\lambda(x) = (x, v)$$

dla wszystkich $x \in V$.

2.5 Twierdzenie o rzucie prostopadłym

Niezerowy wektor nieosobliwej przestrzeni dwuliniowej V nie może być prostopadły do całej przestrzeni V . Może się jednak zdarzyć, że niezerowy wektor przestrzeni nieosobliwej jest prostopadły do niezerowej podprzestrzeni przestrzeni V . Na przykład, w przestrzeni euklidesowej $\mathbb{R}^n$ każdy wektor bazy standardowej jest prostopadły do podprzestrzeni rozpiętej na wszystkich pozostałych wektorach bazy standardowej.

Definicja 2.5.1. Niech S będzie podprzestrzenią przestrzeni dwuliniowej V . Zbiór

$$S^\perp := \{v \in V : (v, x) = 0 \text{ dla wszystkich } x \in S\}$$

nazywamy *ortogonalnym dopełnieniem* podprzestrzeni S .

Uwaga 2.5.1. $V^\perp = \text{rad} V$ oraz $0^\perp = V$. Ponadto, $S^\perp$ jest podprzestrzenią przestrzeni V . Rzeczywiście, jeśli $u, v \in S^\perp$ oraz $a, b \in K$, to dla każdego wektora $x \in S$ mamy

$$(au + bv, x) = a(u, x) + b(v, x) = 0,$$

i wobec tego $au + bv \in S^\perp$.

Uwaga 2.5.2. Dla podprzestrzeni S przestrzeni dwuliniowej V mamy

$$\begin{aligned} S \cap S^\perp &= \{v \in S : (v, x) = 0 \text{ dla wszystkich } x \in S\} \\ &= \text{rad } S. \end{aligned}$$

Stąd wynika, że podprzestrzeń S jest nieosobliwa wtedy i tylko wtedy gdy $S \cap S^\perp = 0$.

Twierdzenie 2.5.1. (Twierdzenie o rzucie prostopadłym.) *Jeśli S jest nieosobliwą podprzestrzenią przestrzeni dwuliniowej V , to*

$$V = S \oplus S^\perp.$$

Dowód. Na podstawie uwagi 2.5.2 nieosobliwość S pociąga $S \cap S^\perp = \text{rad } S = 0$, zatem $S + S^\perp = S \oplus S^\perp$. Pozostaje zatem udowodnić, że $V = S + S^\perp$.

Niech $v \in V$. Rozpatrzmy funkcjonal liniowy μ_v na podprzestrzeni S określony następująco:

$$\mu_v : S \rightarrow K, \quad \mu_v(s) = (s, v).$$

Ponieważ S jest nieosobliwą przestrzenią dwuliniową, na podstawie twierdzenia 2.4.2 homomorfizm $\Lambda_S : S \rightarrow S^*$ jest izomorfizmem przestrzeni wektorowych. Zatem istnieje wektor $t \in S$ taki, że $\mu_v = \Lambda_S(t) = \lambda_t$, gdzie

$$\lambda_t : S \rightarrow K, \quad \lambda_t(s) = (s, t).$$

Tak więc dla każdego $s \in S$ mamy

$$(s, v) = \mu_v(s) = \lambda_t(s) = (s, t),$$

skąd wynika, że $(s, v - t) = 0$ dla każdego $s \in S$. Oznacza to, że $v - t \in S^\perp$. Wobec tego dla każdego $v \in V$ mamy

$$v = t + (v - t), \quad t \in S, \quad v - t \in S^\perp,$$

skąd $V = S + S^\perp$. □

2.6 Bazy ortogonalne przestrzeni dwuliniowych

Głównym zastosowaniem twierdzenia o rzucie prostopadłym jest twierdzenie o istnieniu baz prostopadłych w przestrzeniach dwuliniowych.

Definicja 2.6.1. Baza $\{v_1, \dots, v_n\}$ przestrzeni dwuliniowej V nazywa się *prostopadłą* lub *ortogonalną* jeśli wektory tej bazy są parami prostopadłe to znaczy, $(v_i, v_j) = 0$ dla $i \neq j$.

Inaczej mówiąc, jeśli $A = [(v_i, v_j)]$ jest macierzą przestrzeni dwuliniowej V względem bazy $\{v_1, \dots, v_n\}$, to baza ta jest ortogonalna wtedy i tylko wtedy gdy macierz A jest diagonalna:

$$A = ((v_1, v_1), \dots, (v_n, v_n)) = (q(v_1), \dots, q(v_n)).$$

Twierdzenie 2.6.1. *Każda przestrzeń dwuliniowa V nad ciałem K o charakterystyce $\neq 2$ ma bazę ortogonalną. Ponadto, dla każdego wektora nieizotropowego $v \in V$ istnieje baza ortogonalna przestrzeni V zawierająca wektor v .*

Dowód. Indukcja ze względu na wymiar przestrzeni V . Jeśli $\dim V = 1$, to każdy niezerowy wektor przestrzeni tworzy bazę ortogonalną. Załóżmy więc, że $\dim V > 1$ i że przestrzenie dwuliniowe o wymiarze mniejszym niż $\dim V$ mają bazy ortogonalne.

Rozpatrzmy dwa przypadki. Najpierw przypuśćmy, że wszystkie niezerowe wektory przestrzeni V są izotropowe. Wtedy dla wszystkich $x, y \in V$ mamy

$$0 = (x + y, x + y) = (x, x) + 2(x, y) + (y, y) = 2(x, y).$$

Ponieważ charakterystyka ciała K nie jest równa 2, wynika stąd, że $(x, y) = 0$ dla wszystkich $x, y \in V$. Zatem w tym przypadku przestrzeń V jest *totalnie* izotropowa. Wtedy jednak *każda* baza przestrzeni V jest ortogonalna.

Teraz załóżmy, że przestrzeń V zawiera wektor nieizotropowy v . Rozpatrzmy 1-wymiarową podprzestrzeń $S := Kv$ rozpiętą na wektorze v . Ponieważ v jest nieizotropowy, podprzestrzeń S jest nieosobliwa. Zatem na podstawie twierdzenia 2.5.1 o rzucie prostym mamy rozkład

$$V = S \oplus S^\perp.$$

Tutaj $\dim S^\perp < \dim V$ i wobec tego na podstawie założenia indukcyjnego $S^\perp$ ma bazę ortogonalną $\{v_2, \dots, v_n\}$. Wtedy $\{v, v_2, \dots, v_n\}$ jest bazą ortogonalną przestrzeni V . $\square$

Twierdzenie 2.6.1 o istnieniu baz ortogonalnych ma następującą interpretację macierzową.

WNIOSEK 2.6.1. *Niech A będzie dowolną macierzą symetryczną o elementach z ciała K o charakterystyce $\neq 2$. Wtedy istnieje macierz nieosobliwa P o elementach z ciała K taka, że*

$$PAP^t$$

jest macierzą diagonalną.

W standardowej przestrzeni euklidesowej $\mathbb{R}^n$ wektory jednostkowe $e_1, \dots, e_n$ tworzą bazę ortogonalną.

Twierdzenie 2.6.1 nie obejmuje przestrzeni dwuliniowych nad ciałami o charakterystyce 2. Okazuje się, że istnieją przestrzenie dwuliniowe nad ciałami o charakterystyce 2, które nie mają baz ortogonalnych. Najprostszym przykładem jest dwuwymiarowa przestrzeń dwuliniowa V nad ciałem $\mathbb{F}_2$, która w pewnej bazie u, v ma macierz

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Przestrzeń V jest nieosobliwa, gdyż jej macierz w bazie u, v ma wyznacznik różny od zera. Gdyby przestrzeń ta miała bazę ortogonalną x, y , to jej macierz w tej bazie byłaby macierzą diagonalną $(q(x), q(y))$. Tymczasem jednak norma $q(x)$ każdego wektora przestrzeni V jest równa zero. Rzeczywiście, jeśli $x = au + bv$ gdzie $a, b \in \mathbb{F}_2$, to

$$q(x) = (au + bv, au + bv) = a^2(u, u) + 2ab(u, v) + b^2(v, v) = 0,$$

gdyż $(u, u) = (v, v) = 0$ oraz $2ab = 0$ w ciele $\mathbb{F}_2$. Zatem przestrzeń V w bazie ortogonalnej miałaby macierz zerową wbrew temu, że jest przestrzenią nieosobliwą.

Ogólniej można powiedzieć, że nad ciałami o charakterystyce 2 baz ortogonalnych nie mają *przestrzenie symplektyczne*. Są to dwuliniowe przestrzenie symetryczne V , w których każdy wektor ma normę zero: $(x, x) = 0$ dla każdego $x \in V$.

Można udowodnić, że jeśli przestrzeń dwuliniowa symetryczna V nad ciałem o charakterystyce 2 nie jest symplektyczna, to ma bazę ortogonalną.²

²Zob. K. Szymiczek, *Wykłady z algebry dwuliniowej*, Skrypt UŚ 1991, str. 57.

Na zakończenie przedstawimy jeszcze jedną metodę dowodu twierdzenia 2.6.1, która w odróżnieniu od przyjętego w tym rozdziale podejścia jest w pełni efektywna i nadaje się do konstrukcji bazy ortogonalnej. Jest to tak zwana metoda ortogonalizacji Grama-Schmidta. Jedynym ograniczeniem stosowalności tej metody jest założenie, że rozpatrywana przestrzeń dwuliniowa jest nieizotropowa.

Twierdzenie 2.6.2. *Niech V będzie nieizotropową przestrzenią dwuliniową nad dowolnym ciałem K . Niech $\mathcal{B} = \{v_1, \dots, v_k\}$ będzie zbiorem liniowo niezależnych wektorów przestrzeni V . Wtedy istnieje zbiór parami ortogonalnych wektorów $\mathcal{B}' = \{u_1, \dots, u_k\}$ taki, że*

$$\text{lin}\{\mathcal{B}\} = \text{lin}\{\mathcal{B}'\}.$$

W szczególności, jeśli $\mathcal{B}$ jest bazą przestrzeni V , to $\mathcal{B}'$ jest bazą ortogonalną przestrzeni V .

Dowód. Przeprowadzimy dowód indukcyjny ze względu na liczbę k wektorów w zbiorze $\mathcal{B}$. Jeśli $k = 1$, to obieramy $u_1 = v_1$ i wtedy oczywiście $\text{lin}\{\mathcal{B}\} = \text{lin}\{\mathcal{B}'\}$. Niech $1 \leq \ell < k$ i założmy, że twierdzenie jest prawdziwe dla ℓ -elementowych zbiorów liniowo niezależnych. Niech $\mathcal{B} = \{v_1, \dots, v_\ell, v_{\ell+1}\}$ będzie zbiorem liniowo niezależnym i niech $u_1, \dots, u_\ell$ będą parami prostopadłymi wektorami takimi, że

$$\text{lin}\{v_1, \dots, v_\ell\} = \text{lin}\{u_1, \dots, u_\ell\}.$$

Wskażemy jak znaleźć wektor $u_{\ell+1}$ prostopadły do wszystkich wektorów $u_1, \dots, u_\ell$ i taki, że

$$\text{lin}\{\mathcal{B}\} = \text{lin}\{u_1, \dots, u_\ell, u_{\ell+1}\}. \quad (2.7)$$

Okazuje się, że przy odpowiednio dobranych skalarach $x_1, \dots, x_\ell$ wektor

$$u_{\ell+1} = v_{\ell+1} + x_1 u_1 + \dots + x_\ell u_\ell \quad (2.8)$$

jest prostopadły do każdego z wektorów $u_1, \dots, u_\ell$ i spełnia (2.7). Rzeczywiście, dla $i \leq \ell$ mamy

$$(u_{\ell+1}, u_i) = (v_{\ell+1} + x_1 u_1 + \dots + x_\ell u_\ell, u_i) = (v_{\ell+1}, u_i) + x_i (u_i, u_i).$$

Zatem $(u_{\ell+1}, u_i) = 0$ wtedy i tylko wtedy gdy

$$x_i = -\frac{(v_{\ell+1}, u_i)}{(u_i, u_i)}$$

(wykorzystujemy tu nieizotropowość przestrzeni V). Ten wybór skalarów x_i gwarantuje więc, że wektor $u_{\ell+1}$ postaci (2.8) jest prostopadły do każdego z wektorów $u_1, \dots, u_\ell$. Ponadto,

$$\text{lin}\{\mathcal{B}\} = \text{lin}\{v_1, \dots, v_\ell\} + \text{lin}\{v_{\ell+1}\} = \text{lin}\{u_1, \dots, u_\ell\} + \text{lin}\{u_{\ell+1}\} = \text{lin}\{u_1, \dots, u_\ell, u_{\ell+1}\},$$

gdzie środkowa równość wynika z (2.8). □

Rozdział 3

Przestrzenie euklidesowe

Ostatnie zmiany 20.04.2009 r.

DEFINICJA 3.0.2. Przestrzenią *euklidesową* nazywamy skończenie wymiarową przestrzeń dwuliniową V nad ciałem $\mathbb{R}$ liczb rzeczywistych z dodatnio określonym symetrycznym funkcjonałem dwuliniowym

$$(\cdot, \cdot) : V \times V \rightarrow \mathbb{R}$$

zwanym *iloczynem skalarnym* na przestrzeni V .

Dodatnia określoność funkcjonału dwuliniowego oznacza, że dla każdego niezerowego wektora $v \in V$ mamy $q(v) = (v, v) > 0$. Tak więc funkcjonał dwuliniowy $(\cdot, \cdot)$ jest dodatnio określony gdy stowarzyszony z nim funkcjonał kwadratowy q przyjmuje dodatnie wartości na niezerowych wektorach przestrzeni V . Mówimy wtedy także, że q jest dodatnio określonym funkcjonałem kwadratowym.

Wobec dodatniej określoności iloczynu skalarnego przestrzeń euklidesowa jest nieizotropowa i zatem także nieosobliwa. Jeśli U jest podprzestrzenią przestrzeni euklidesowej V , to iloczyn skalarny zacieśniony do U jest oczywiście także dodatnio określony. Wobec tego każda podprzestrzeń przestrzeni euklidesowej jest także przestrzenią euklidesową. W szczególności, każda podprzestrzeń przestrzeni euklidesowej jest podprzestrzenią *nieosobliwą*.

3.1 Norma, odległość i kąt między wektorami

Ponieważ dla każdego wektora v przestrzeni euklidesowej mamy $(v, v) \geq 0$, liczba (v, v) jest kwadratem pewnej liczby rzeczywistej d , $(v, v) = d^2$, przy czym możemy wziąć $d \geq 0$. Tę nieujemną liczbę rzeczywistą d nazywamy *długością* lub *normą* wektora v i oznaczamy $\|v\|$. A więc

$$\|v\| = \sqrt{(v, v)} = \sqrt{q(v)} \quad \text{dla każdego wektora } v \in V.$$

Zauważmy, że dla dowolnej liczby rzeczywistej a i dowolnego wektora $v \in V$ mamy

$$\|av\| = \sqrt{(av, av)} = \sqrt{a^2(v, v)} = |a| \|v\|.$$

W szczególności, $\|-v\| = \|v\|$.

Z pojęciem długości wektora przestrzeni euklidesowej V związane są następujące cztery twierdzenia. Dowody dwóch pierwszych (wraz z interpretacją geometryczną tych twierdzeń) pozostawiamy jako ćwiczenia dla Czytelnika.

Twierdzenie Pitagorasa: Jeśli $u, v \in V$ są prostopadłe, to

$$\|u + v\|^2 = \|u\|^2 + \|v\|^2.$$

Twierdzenie o równoległoboku: Dla dowolnych $u, v \in V$,

$$\|u + v\|^2 + \|u - v\|^2 = 2(\|u\|^2 + \|v\|^2).$$

Nierówność Cauchy'ego-Schwarza: Dla dowolnych $u, v \in V$,

$$|(u, v)| \leq \|u\| \cdot \|v\|,$$

przy czym równość zachodzi tylko wtedy gdy wektory u, v są liniowo zależne.

Nierówność trójkąta: Dla dowolnych $u, v \in V$,

$$\|u + v\| \leq \|u\| + \|v\|,$$

przy czym równość zachodzi tylko wtedy gdy wektory u, v są liniowo zależne oraz $(u, v) > 0$.

Dla dowodu nierówności Cauchy'ego-Schwarza można założyć, że wektory u i v są niezerowe, gdyż w przeciwnym wypadku nierówność jest prawdziwa. Dla dowolnej liczby $x \in \mathbb{R}$ mamy

$$\|u - xv\|^2 = (u - xv, u - xv) = (u, u) - 2x(u, v) + x^2(v, v)$$

skąd wobec nieujemności $\|u - xv\|^2$ wynika, że trójmian kwadratowy $(u, u) - 2x(u, v) + x^2(v, v)$ dla każdego $x \in \mathbb{R}$ przyjmuje wartości nieujemne. Zatem jego wyróżnik jest nie-dodatni,

$$4(u, v)^2 - 4(u, u)(v, v) \leq 0,$$

skąd otrzymujemy nierówność Cauchy'ego-Schwarza. Ponadto, z jednej strony $\|u - xv\|^2 = 0$ wtedy i tylko wtedy gdy $u - xv = 0$, czyli gdy wektory u i v są liniowo zależne, z drugiej zaś strony $\|u - xv\|^2 = 0$ wtedy i tylko wtedy gdy $(u, u) - 2x(u, v) + x^2(v, v) = 0$. Wobec niedodatniości wyróżnika ma to miejsce tylko wtedy gdy $4(u, v)^2 - 4(u, u)(v, v) = 0$ czyli tylko wtedy gdy $|(u, v)| = \|u\| \cdot \|v\|$.

Dla dowodu nierówności trójkąta wykorzystamy nierówność Cauchy'ego-Schwarza w następującym rachunku:

$$\|u + v\|^2 = (u + v, u + v) = \|u\|^2 + 2(u, v) + \|v\|^2 \leq \|u\|^2 + 2\|u\|\|v\| + \|v\|^2 = (\|u\| + \|v\|)^2.$$

Stąd wynika już nierówność trójkąta, przy czym widzimy, że w nierówności trójkąta zachodzi równość wtedy i tylko wtedy, gdy $(u, v) = \|u\|\|v\|$ a więc wtedy i tylko wtedy gdy zachodzi równość w nierówności Cauchy'ego-Schwarza oraz $(u, v) \geq 0$.

Z nierówności Cauchy'ego-Schwarza wynika, że dla dowolnych niezerowych wektorów u i v przestrzeni euklidesowej mamy

$$-1 \leq \frac{(u, v)}{\|u\| \cdot \|v\|} \leq 1.$$

W związku z tym w przedziale $[0, \pi]$ istnieje dokładnie jedna liczba α taka, że

$$\cos \alpha = \frac{(u, v)}{\|u\| \cdot \|v\|}.$$

Tę liczbę α nazywamy miarą kąta pomiędzy wektorami u i v przestrzeni euklidesowej. W szczególności, jeśli wektory są prostopadłe, $(u, v) = 0$, to kąt między nimi ma miarę $\frac{1}{2}\pi$. Zauważmy, że nie zdefiniowaliśmy pojęcia kąta między wektorami, lecz pojęcie *miary*

kąta między wektorami.

W przestrzeni euklidesowej V można określić *odległość* $d(u, v)$ pomiędzy wektorami $u, v \in V$,

$$d(u, v) = \|u - v\|. \quad (3.1)$$

Tak określona funkcja $d : V \times V \rightarrow \mathbb{R}$ ma wszystkie własności wymagane od metryki przestrzeni metrycznej:

- $d(u, v) \geq 0$ oraz $d(u, v) = 0$ wtedy i tylko wtedy gdy $u = v$,
- $d(u, v) = d(v, u)$,
- $d(u, v) \leq d(u, w) + d(w, v)$,

dla dowolnych wektorów $u, v, w \in V$. Pierwsza własność odległości wynika z dodatniej określoności iloczynu skalarnego, druga wynika z $\|u - v\| = \|-(u - v)\|$, trzecia jest konsekwencją nierówności trójkąta:

$$d(u, v) = \|u - v\| = \|(u - w) + (w - v)\| \leq \|u - w\| + \|w - v\| = d(u, w) + d(w, v).$$

A więc każda przestrzeń euklidesowa jest przestrzenią metryczną z metryką określoną wzorem (3.1). Tak jak w każdej przestrzeni metrycznej określa się pojęcie granicy ciągu wektorów przestrzeni euklidesowej i ciągłości endomorfizmów i funkcjonałów liniowych na przestrzeni euklidesowej. Rozpatruje się też takie pojęcia jak domkniętość zbiorów wektorów czy zupełność przestrzeni. W przestrzeniach euklidesowych wszystkie te pojęcia zachowują się bardzo regularnie: wszystkie endomorfizmy i funkcjonały są ciągłe, wszystkie podprzestrzenie są domknięte, przestrzeń euklidesowa jest zupełna. Istnieją jednak ważne przykłady nieskończone wymiarowe przestrzeni dwuliniowych nad $\mathbb{R}$ z dodatnio określonymi funkcjonałami dwuliniowymi (takie jak w przykładzie 3.3.2), w których analiza i topologia są znacznie bardziej skomplikowane. Jest to problematyka *analizy funkcjonalnej*, którą w tym skrypcie nie będziemy się zajmować. Przeciwnie, naszym zamiarem jest studiowanie *algebraicznych* aspektów przestrzeni euklidesowych i pokazanie, że wszystkie rozpatrywane przez nas pojęcia i fakty uogólniają się na przestrzenie euklidesowe nad ciałami rzeczywiście domkniętymi.

3.2 Bazy ortonormalne

Na podstawie twierdzenia 2.6.1 każda przestrzeń euklidesowa ma bazę ortogonalną. Jeśli $\mathcal{B} = \{v_1, \dots, v_n\}$ jest bazą ortogonalną przestrzeni euklidesowej V , to wektory

$$e_1 = \frac{1}{\|v_1\|} v_1, \dots, e_n = \frac{1}{\|v_n\|} v_n$$

tworzą bazę *ortonormalną* tej przestrzeni euklidesowej. Oznacza to, że są one parami prostopadłe i mają długości równe 1. Dla dowolnych skalarów $a, b \in \mathbb{R}$ mamy bowiem $(av_i, bv_j) = ab(v_i, v_j) = 0$ oraz $(av_i, av_i) = a^2(v_i, v_i) = a^2\|v_i\|^2$. Zatem obierając $a = \|v_i\|^{-1}$, $b = \|v_j\|^{-1}$ otrzymujemy ortonormalność bazy $e_1, \dots, e_n$.

Tak więc każda przestrzeń euklidesowa ma bazę ortonormalną. Przejście od bazy ortogonalnej $\mathcal{B}$ do bazy ortonormalnej $\{e_1, \dots, e_n\}$ nazywa się *normalizacją* bazy ortogonalnej $\mathcal{B}$. Przypomnijmy, że dysponujemy także efektywną metodą konstrukcji bazy ortogonalnej przestrzeni euklidesowej. Jeśli dana jest jakakolwiek baza przestrzeni euklidesowej, to zastosowanie metody ortogonalizacji Grama-Schmidta, opisanej w twierdzeniu 2.6.2, prowadzi do konstrukcji bazy ortogonalnej tej przestrzeni.

Bazy ortonormalne prowadzą do istotnych uproszczeń rachunków w przestrzeniach euklidesowych. Jeśli $\mathcal{E} = \{e_1, \dots, e_n\}$ jest bazą ortonormalną przestrzeni V oraz $u = \sum_{i=1}^n x_i e_i, v = \sum_{i=1}^n y_i e_i$ są dowolnymi wektorami tej przestrzeni, to z dwuliniowości iloczynu skalarnego i ortonormalności bazy $\mathcal{E}$ otrzymujemy następujące, bardzo proste formuły dla iloczynu skalarnego wektorów u i v i dla normy wektora u :

$$(u, v) = x_1 y_1 + x_2 y_2 + \dots + x_n y_n, \quad \|u\|^2 = x_1^2 + x_2^2 + \dots + x_n^2.$$

Jak to zauważyliśmy już wcześniej, z twierdzenia 2.2.1 wynika, że jeśli A i C są macierzami tej samej przestrzeni dwuliniowej V względem baz $\mathcal{B} = \{v_1, \dots, v_n\}$ i $\mathcal{B}' = \{w_1, \dots, w_n\}$, to

$$\det C = (\det P)^2 \cdot \det A, \quad (3.2)$$

gdzie P jest macierzą przejścia od bazy $\mathcal{B}$ do bazy $\mathcal{B}'$. Jeśli V jest przestrzenią euklidesową, to V ma bazę ortonormalną $\mathcal{B}$ i w tej bazie przestrzeni V ma macierz jednostkową $A = I = [(v_i, v_j)]$. Jeśli $\mathcal{B}'$ jest także bazą ortonormalną V , to także macierz $C = [(w_i, w_j)]$ jest macierzą jednostkową i wobec tego z równości (3.2) wynika, że dla macierzy przejścia P od bazy $\mathcal{B}$ do bazy $\mathcal{B}'$ mamy $(\det P)^2 = 1$. Następujące twierdzenie podaje znacznie dokładniejszy rezultat.

Twierdzenie 3.2.1. *Niech $\mathcal{B}$ będzie bazą ortonormalną przestrzeni euklidesowej V i niech $\mathcal{B}'$ będzie bazą V . Niech P będzie macierzą przejścia od bazy ortonormalnej $\mathcal{B}$ do bazy $\mathcal{B}'$. Baza $\mathcal{B}'$ jest ortonormalna wtedy i tylko wtedy gdy P jest macierzą ortogonalną, to znaczy $P^{-1} = P^T$.*

Dowód. Niech najpierw $\mathcal{B} = \{v_1, \dots, v_n\}$ oraz $\mathcal{B}' = \{w_1, \dots, w_n\}$ będą bazami ortonormalnymi przestrzeni euklidesowej V i niech

$$\begin{aligned} w_1 &= p_{11}v_1 + p_{12}v_2 + \dots + p_{1n}v_n, \\ &\vdots \\ w_n &= p_{n1}v_1 + p_{n2}v_2 + \dots + p_{nn}v_n. \end{aligned} \quad (3.3)$$

Macierz $P := [p_{ij}]$ jest więc macierzą przejścia od bazy $\mathcal{B}$ do bazy $\mathcal{B}'$. Wiersze macierzy P traktujemy jako wektory standardowej przestrzeni euklidesowej $\mathbb{R}^n$. Wtedy z ortonormalności baz $\mathcal{B}$ i $\mathcal{B}'$ wynika, że

$$0 = (w_i, w_j) = p_{i1}p_{j1} + p_{i2}p_{j2} + \dots + p_{in}p_{jn} = ((p_{i1}, p_{i2}, \dots, p_{in}), (p_{j1}, p_{j2}, \dots, p_{jn})),$$

$$1 = (w_i, w_i) = p_{i1}^2 + p_{i2}^2 + \dots + p_{in}^2 = ((p_{i1}, p_{i2}, \dots, p_{in}), (p_{i1}, p_{i2}, \dots, p_{in}))$$

dla wszystkich $i \neq j, 1 \leq i, j \leq n$. A więc wiersze macierzy P tworzą układ ortonormalny (faktycznie bazę ortonormalną) przestrzeni $\mathbb{R}^n$. Stąd otrzymujemy, że iloczyn macierzy $P \cdot P^T$ jest macierzą jednostkową I_n . Macierz P^T jest więc prawostronnie odwrotna do macierzy P . Ponieważ jednak w każdej grupie każdy element ma tylko jeden element prawostronnie odwrotny, zatem $P^T = P^{-1}$ (w grupie macierzy nieosobliwych $\mathbf{GL}(n, \mathbb{R})$).

Załóżmy teraz, że $\mathcal{B}$ jest bazą ortonormalną V oraz macierz przejścia $P = [p_{ij}]$ od bazy $\mathcal{B}$ do bazy $\mathcal{B}' = \{w_1, \dots, w_n\}$ jest ortogonalna. Mamy więc równości (3.3). Podobnie jak powyżej wiersze macierzy P traktujemy jako wektory standardowej przestrzeni euklidesowej $\mathbb{R}^n$. Z ortogonalności macierzy P wynika, że wiersze macierzy P tworzą bazę ortonormalną przestrzeni $\mathbb{R}^n$. A więc dla $i \neq j$ mamy

$$((p_{i1}, p_{i2}, \dots, p_{in}), (p_{j1}, p_{j2}, \dots, p_{jn})) = 0$$

oraz

$$((p_{i1}, p_{i2}, \dots, p_{in}), (p_{i1}, p_{i2}, \dots, p_{in})) = 1$$

dla każdego $i \leq n$. Ponieważ $\mathcal{B} = \{v_1, \dots, v_n\}$ jest bazą ortonormalną, więc z równości (3.3) otrzymujemy

$$(w_i, w_j) = p_{i1}p_{j1} + p_{i2}p_{j2} + \dots + p_{in}p_{jn} = ((p_{i1}, p_{i2}, \dots, p_{in}), (p_{j1}, p_{j2}, \dots, p_{jn}))$$

i wobec tego $(w_i, w_j) = 0$ dla $i \neq j$ oraz $(w_i, w_i) = 1$ dla $i \leq n$. A więc baza $\mathcal{B}' = \{w_1, \dots, w_n\}$ jest ortonormalna. $\square$

3.3 Przykłady

Przykład 3.3.1. Jak zauważyliśmy w przykładzie 2.1.1, dla każdej liczby naturalnej n funkcjonal dwuliniowy określony na przestrzeni współrzędnych $\mathbb{R}^n$ formułą

$$((x_1, \dots, x_n), (y_1, \dots, y_n)) = x_1y_1 + \dots + x_ny_n$$

jest iloczynem skalarnym na $\mathbb{R}^n$. Zatem $\mathbb{R}^n$ z tak określonym funkcjonalem dwuliniowym jest przestrzenią euklidesową. Nazywamy ją *standardową* przestrzenią euklidesową. Dla wektorów $u = (x_1, \dots, x_n)$, $v = (y_1, \dots, y_n)$ przestrzeni $\mathbb{R}^n$ mamy

$$\|u\| = \sqrt{x_1^2 + \dots + x_n^2}, \quad d(u, v) = \sqrt{(x_1 - y_1)^2 + \dots + (x_n - y_n)^2}.$$

Przestrzeń $\mathbb{R}^n$ ma *standardową* bazę ortonormalną $e_1, \dots, e_n$ złożoną z wektorów jednostkowych $e_i = (x_1, \dots, x_n)$, gdzie $x_i = 1$ oraz $x_j = 0$ dla $j \neq i$.

Przykład 3.3.2. Niech $V = C[a, b]$ będzie przestrzenią wszystkich funkcji ciągłych $f : [a, b] \rightarrow \mathbb{R}$ określonych na przedziale domkniętym $[a, b] \subset \mathbb{R}$. Jest to nieskończenie wymiarowa przestrzeń wektorowa nad ciałem $\mathbb{R}$ (na przykład, funkcje wielomianowe $f_i(x) = x^i$, $i \in \mathbb{N}$, są liniowo niezależne). Na przestrzeni tej określa się funkcjonal $(\ , \) : V \times V \rightarrow \mathbb{R}$ wzorem

$$(f, g) = \int_a^b f(x)g(x)dx.$$

Standardowe własności całki oznaczonej pokazują, że $(\ , \)$ jest dodatnio określonym funkcjonalem dwuliniowym. W ten sposób przestrzeń funkcji ciągłych na przedziale domkniętym ma wszystkie własności przestrzeni euklidesowej z wyjątkiem skończoności wymiaru.

Innym przykładem tego typu jest przestrzeń $V = \ell^2$ wszystkich ciągów (a_i) liczb rzeczywistych spełniających warunek $\sum_{i=0}^{\infty} |a_i| < \infty$. Tutaj funkcjonal dwuliniowy określa się następująco:

$$((a_i), (b_i)) = \sum_{i=0}^{\infty} a_i b_i.$$

Szereg po prawej stronie jest zbieżny gdyż

$$0 \leq (|a_i| - |b_i|)^2 = |a_i|^2 - 2|a_i||b_i| + |b_i|^2$$

i wobec tego $2|a_i b_i| \leq |a_i|^2 + |b_i|^2$ skąd otrzymujemy

$$2 \left| \sum_{i=0}^{\infty} a_i b_i \right| \leq \sum_{i=0}^{\infty} |a_i|^2 + \sum_{i=0}^{\infty} |b_i|^2 < \infty.$$

Twierdzenie 3.3.1. *Każda n -wymiarowa przestrzeń euklidesowa jest izometryczna ze standardową przestrzenią euklidesową $\mathbb{R}^n$.*

Dowód. Niech V będzie n -wymiarową przestrzenią euklidesową z iloczynem skalarnym $(\cdot, \cdot)_V$ i niech $\mathcal{B} = \{v_1, \dots, v_n\}$ będzie bazą ortonormalną przestrzeni V . Z drugiej strony weźmy standardową przestrzeń euklidesową $\mathbb{R}^n$ ze standardową bazą ortonormalną $\{e_1, \dots, e_n\}$. Rozpatrzmy macierze przestrzeni dwuliniowych V i $\mathbb{R}^n$ w tych bazach:

$$[(v_i, v_j)_V] = I_n = [(e_i, e_j)],$$

gdzie I_n jest macierzą jednostkową stopnia n . Przestrzenie dwuliniowe V i $\mathbb{R}^n$ mają identyczne (a więc także kongruentne) macierze w odpowiednich bazach, zatem przestrzenie te są izometryczne na podstawie twierdzenia 2.3.1. $\square$

Twierdzenie 3.3.1 pozwala zawęzić rozpatrywanie przestrzeni euklidesowych do standardowych przestrzeni euklidesowych $\mathbb{R}^n$. Tym niemniej, jeśli przestrzeń dwuliniowa nad $\mathbb{R}$ jest zadana poprzez swoją macierz względem pewnej bazy tej przestrzeni, pozostaje otwarte pytanie jak rozpoznać, czy przestrzeń ta jest euklidesowa. Na to pytanie istnieje klasyczna odpowiedź zawarta w następującym twierdzeniu udowodnionym w 1894 roku przez G. Frobeniusa.

Twierdzenie 3.3.2. *Niech V będzie n -wymiarową przestrzenią wektorową nad ciałem $\mathbb{R}$ i niech $A = [a_{ij}]$ będzie macierzą funkcjonału dwuliniowego $(\cdot, \cdot)$ na przestrzeni V w bazie $\mathcal{B} = \{v_1, \dots, v_n\}$ tej przestrzeni. Dla $k \leq n$, niech $A_k = [a_{ij}]_{1 \leq i, j \leq k}$ będzie macierzą funkcjonału $(\cdot, \cdot)$ zacieśnionego do podprzestrzeni $V_k = \text{lin}\{v_1, \dots, v_k\}$ w bazie $\mathcal{B}_k = \{v_1, \dots, v_k\}$. Przestrzeń V jest euklidesowa wtedy i tylko wtedy, gdy*

$$\det A_k > 0 \quad \text{dla każdego } k = 1, 2, \dots, n.$$

Dowód. Jeśli przestrzeń V jest euklidesowa, to także wszystkie podprzestrzenie V_k są euklidesowe i wobec tego wystarczy pokazać, że wyznacznik macierzy dowolnej przestrzeni euklidesowej w dowolnej bazie tej przestrzeni jest dodatnią liczbą rzeczywistą. Jak już zauważyliśmy, przestrzeń euklidesowa V ma bazę ortonormalną i jeśli P jest macierzą przejścia od bazy $\mathcal{B}$ do bazy ortonormalnej, to $I = PAP^T$ na podstawie twierdzenia 2.2.1. Zatem $1 = (\det P)^2 \cdot \det A$ skąd wynika, że $\det A > 0$.

Założmy teraz, że $\det A_k > 0$ dla każdego $k = 1, 2, \dots, n$. Jeśli $n = 1$, to $A = A_1$ i jedyny element macierzy A jest dodatnią liczbą rzeczywistą, skąd wynika, że funkcjonał dwuliniowy jest dodatnio określony i wobec tego V jest przestrzenią euklidesową. Założmy teraz, że $n > 1$ i twierdzenie jest prawdziwe dla przestrzeni o wymiarze $n - 1$. Rozpatrzmy podprzestrzeń $V_{n-1} = \text{lin}\{v_1, \dots, v_{n-1}\}$ przestrzeni V . Na podstawie założenia indukcyjnego V_{n-1} jest przestrzenią euklidesową, w szczególności jest ona nieosobliwą podprzestrzenią przestrzeni V i wobec tego na podstawie twierdzenia o rzucie prostopadłym mamy

$$V = V_{n-1} \oplus V_{n-1}^\perp.$$

Tutaj $\dim V_{n-1}^\perp = \dim V - \dim V_{n-1} = 1$ i wobec tego $V_{n-1}^\perp = \text{lin}\{w\}$ dla pewnego $w \in V$. Jeśli $(w, w) = a$, to wobec $w \in V_{n-1}^\perp$ mamy

$$V \cong A_{n-1} \oplus [a] \quad \text{w bazie } \mathcal{B}_{n-1} \cup \{w\},$$

gdzie $A_{n-1} \oplus [a]$ oznacza macierz A_{n-1} z dołączoną jedną kolumną i jednym wierszem, których wszystkie elementy są równe 0 z wyjątkiem ostatniego równego a . Ponieważ jednak równocześnie mamy

$$V \cong A \quad \text{w bazie } \mathcal{B},$$

więc jeśli Q jest macierzą przejścia od bazy $\mathcal{B}$ do bazy $\mathcal{B}_{n-1} \cup \{w\}$ przestrzeni V , to

$$A_{n-1} \oplus [a] = QAQ^T.$$

Biorąc wyznaczniki po obu stronach otrzymujemy $a \det A_{n-1} = (\det Q)^2 \det A$ skąd wynika, że $a > 0$. Teraz już łatwo zauważyć, że funkcjonal dwuliniowy na V jest dodatnio określony. Każdy wektor $v \in V$ ma jednoznaczne przedstawienie w postaci $v = u + cw$, gdzie $u \in V_{n-1}$, $c \in \mathbb{R}$ oraz

$$q(v) = (v, v) = (u + cw, u + cw) = (u, u) + c^2(w, w) = q(u) + c^2a \geq 0,$$

gdyż V_{n-1} jest przestrzenią euklidesową i wobec tego $q(u) \geq 0$ oraz $c^2a \geq 0$. Ponadto, jeśli $v \neq 0$, to $u \neq 0$ lub $c \neq 0$ i wobec tego $q(v) > 0$. $\square$

3.4 Najlepsza aproksymacja

W przestrzeni euklidesowej twierdzenie 2.5.1 o rzucie prostopadłym prowadzi do następującego twierdzenia o *najlepszej aproksymacji*.

TWIERDZENIE 3.4.1. *Niech S będzie podprzestrzenią przestrzeni euklidesowej V i niech $v \in V$. Jeśli $v = s + s^\perp$, gdzie $s \in S$ oraz $s^\perp \in S^\perp$, to*

$$\|v - s\| \leq \|v - t\| \quad \text{dla każdego wektora } t \in S.$$

Wektor s jest więc najlepszym przybliżeniem wektora v w podprzestrzeni S .

Dowód. Dla $t \in S$ mamy $s - t \in S$. Ponieważ $v - s = s^\perp \in S^\perp$, więc wektory $s - t$, $v - s$ są prostopadłe i wobec tego na podstawie twierdzenia Pitagorasa mamy

$$\|v - t\|^2 = \|v - s + s - t\|^2 = \|v - s\|^2 + \|s - t\|^2 \geq \|v - s\|^2.$$

Stąd $\|v - t\| \geq \|v - s\|$ dla każdego $t \in S$. $\square$

Rozdział 4

Endomorfizmy przestrzeni euklidesowych

Ostatnie zmiany 12.06.2009 r.

W tym rozdziale rozpatrujemy endomorfizmy przestrzeni euklidesowych, które spełniają pewne dodatkowe warunki wyrażone w języku iloczynu skalarnego. Dwoma typowymi przykładami, które będziemy analizować, są endomorfizmy samosprężone i izometrie przestrzeni euklidesowych. Przypomnijmy, że endomorfizm τ przestrzeni euklidesowej V nazywa się samosprężony jeśli $(\tau(v), u) = (v, \tau(u))$ dla wszystkich $u, v \in V$. Natomiast endomorfizm τ jest izometrią, jeśli jest bijektywny oraz $(\tau(u), \tau(v)) = (u, v)$ dla wszystkich $u, v \in V$. Dla endomorfizmów samosprężonych głównym problemem jest istnienie baz ortonormalnych złożonych z wektorów własnych, natomiast dla izometrii podamy pewne informacje o strukturze grupy izometrii przestrzeni euklidesowej.

W §4.1 i §4.2 rozpatrujemy nieco ogólniejszą sytuację, gdyż endomorfizmy sprzężone i endomorfizmy samosprężone można zdefiniować w dowolnej nieosobliwej symetrycznej przestrzeni dwuliniowej.

4.1 Endomorfizmy sprzężone

Zakładamy, że V jest przestrzenią wektorową nad ciałem K , z nieosobliwym funkcjonałem dwuliniowym $(\ , \)$. Oznacza to, że odwzorowanie

$$\Lambda_V : V \rightarrow V^*, \quad \Lambda_V(v) = \lambda_v$$

jest izomorfizmem przestrzeni wektorowych. Tutaj dla ustalonego wektora $v \in V$

$$\lambda_v : V \rightarrow K, \quad \lambda_v(x) = (v, x) \quad \text{dla } x \in V.$$

Inna interpretacja nieosobliwości przestrzeni dwuliniowej V pozwala stwierdzić, że jeśli dla $v, w \in V$ mamy $(u, v) = (u, w)$ dla każdego wektora $u \in V$, to $v = w$. Rzeczywiście, $(u, v) = (u, w)$ dla każdego $u \in V$ pociąga $v - w \in \text{rad } V = 0$.

TWIERDZENIE 4.1.1. *Dla każdego endomorfizmu τ nieosobliwej przestrzeni dwuliniowej V istnieje dokładnie jeden endomorfizm τ^* przestrzeni V spełniający warunek*

$$(\tau(v), u) = (v, \tau^*(u)) \quad \text{dla wszystkich } u, v \in V.$$

Dowód. Niech $u \in V$. Wektor u i endomorfizm τ przestrzeni V wyznaczają odwzorowanie

$$\lambda : V \rightarrow K, \quad \lambda(v) = (\tau(v), u).$$

Oczywiście λ jest funkcjonałem liniowym na przestrzeni V . Wobec nieosobliwości przestrzeni V istnieje dokładnie jeden wektor $w \in V$ taki, że $\lambda = \Lambda_V(w) = \lambda_w$. W ten sposób każdemu wektorowi $u \in V$ przyporządkujemy jednoznacznie wektor $w \in V$ taki, że

$$(v, w) = \lambda_w(v) = \lambda(v) = (\tau(v), u)$$

dla każdego $v \in V$. Wektor w będziemy oznaczać $w =: \tau^*(u)$. Ma on więc następującą własność:

$$(\tau(v), u) = (v, \tau^*(u)) \quad \text{dla wszystkich } u, v \in V. \quad (4.1)$$

τ^* jest odwzorowaniem $\tau^* : V \rightarrow V$. Z definicji τ^* wynika, że jest to jedyne odwzorowanie $\tau^* : V \rightarrow V$ spełniające warunek (4.1). Pozostaje zatem wykazać, że τ^* jest endomorfizmem przestrzeni V .

Weźmy dowolne $v, x, y \in V$ oraz $a, b \in K$. Wtedy

$$\begin{aligned} (v, \tau^*(ax + by)) &= (\tau(v), ax + by) = a(\tau(v), x) + b(\tau(v), y) \\ &= a(v, \tau^*(x)) + b(v, \tau^*(y)) = (v, a\tau^*(x) + b\tau^*(y)). \end{aligned}$$

Stąd wobec nieosobliwości przestrzeni V wynika, że $\tau^*(ax + by) = a\tau^*(x) + b\tau^*(y)$. $\square$

DEFINICJA 4.1.1. Niech τ będzie endomorfizmem nieosobliwej przestrzeni dwuliniowej V .

(a) Endomorfizm τ^* przestrzeni V , spełniający warunek (4.1), nazywamy *endomorfizmem sprzężonym* z endomorfizmem τ .

(b) Endomorfizm τ przestrzeni V nazywa się *samosprzężony* jeśli $\tau = \tau^*$, to znaczy, jeśli

$$(\tau(v), u) = (v, \tau(u)) \quad \text{dla wszystkich } u, v \in V.$$

TWIERDZENIE 4.1.2. Dla nieosobliwej przestrzeni dwuliniowej V odwzorowanie

$$\text{End}_K V \rightarrow \text{End}_K V, \quad \tau \mapsto \tau^*$$

ma następujące własności

$$(\sigma + \tau)^* = \sigma^* + \tau^*, \quad (\sigma\tau)^* = \tau^*\sigma^*, \quad (a\tau)^* = a\tau^*,$$

dla każdego endomorfizmu σ, τ przestrzeni V i dla każdego skalaru $a \in K$, a także

$$\mathbf{1}_V^* = \mathbf{1}_V, \quad (\tau^*)^* = \tau.$$

Dowód. Wykorzystujemy własność (4.1) definiującą endomorfizm sprzężony i nieosobliwość przestrzeni. A więc dla każdego $u, v \in V$ mamy

$$\begin{aligned} (u, (\sigma + \tau)^*(v)) &= ((\sigma + \tau)(u), v) = (\sigma(u), v) + (\tau(u), v) = (u, \sigma^*(v)) + (u, \tau^*(v)) \\ &= (u, (\sigma^* + \tau^*)(v)), \end{aligned}$$

skąd wynika, że $(\sigma + \tau)^*(v) = (\sigma^* + \tau^*)(v)$ dla każdego $v \in V$. Podobnie

$$(u, (\sigma\tau)^*(v)) = (\sigma\tau(u), v) = (\tau(u), \sigma^*(v)) = (u, \tau^*\sigma^*(v)),$$

oraz

$$(u, (a\tau)^*(v)) = ((a\tau)(u), v) = a(\tau(u), v) = a(u, \tau^*(v)) = (u, a\tau^*(v))$$

dowodzą dwóch następnych własności. Dla dowodu dwóch ostatnich własności zauważmy, że dla dowolnych $u, v \in V$, mamy

$$(u, \mathbf{1}^*(v)) = (\mathbf{1}(u), v) = (u, v) = (u, \mathbf{1}(v)),$$

oraz

$$(u, (\tau^*)^*(v)) = (\tau^*(u), v) = (v, \tau^*(u)) = (\tau(v), u) = (u, \tau(v)).$$

Wobec tego $\mathbf{1}^*(v) = \mathbf{1}(v)$ oraz $(\tau^*)^*(v) = \tau(v)$ dla każdego $v \in V$. $\square$

4.2 Macierze endomorfizmów sprzężonych

Niech V będzie nieosobliwą przestrzenią dwuliniową nad ciałem K . Niech $\mathcal{B} = \{v_1, \dots, v_n\}$ będzie uporządkowaną bazą przestrzeni wektorowej V i niech $\tau \in \text{End}_K V$. Niech $\mathbf{m}(\tau, \mathcal{B}) := B = [b_{ij}] \in M_n(K)$ będzie macierzą endomorfizmu τ w bazie $\mathcal{B}$. Zatem dla $j = 1, \dots, n$,

$$\tau(v_j) = \sum_{i=1}^n b_{ij} v_i.$$

Założmy także, że endomorfizm τ^* sprzężony z τ ma w bazie $\mathcal{B}$ macierz $\mathbf{m}(\tau^*, \mathcal{B}) := C = [c_{ij}] \in M_n(K)$.

LEMAT 4.2.1. *Jeśli baza $\mathcal{B}$ jest ortogonalna, to*

$$b_{ij}(v_i, v_i) = c_{ji}(v_j, v_j)$$

dla $i, j = 1, \dots, n$.

Dowód. Lemat wynika z następującego rachunku

$$\begin{aligned} (v_i, \tau(v_j)) &= (v_i, \sum_{s=1}^n b_{sj} v_s) = \sum_{s=1}^n b_{sj} (v_i, v_s) = b_{ij} (v_i, v_i), \\ (\tau^*(v_i), v_j) &= (\sum_{s=1}^n c_{si} v_s, v_j) = \sum_{s=1}^n c_{si} (v_s, v_j) = c_{ji} (v_j, v_j) \end{aligned}$$

oraz stąd, że $(v_i, \tau(v_j)) = (\tau^*(v_i), v_j)$. □

Związek pomiędzy macierzami B i C staje się jeszcze prostszy jeśli baza ortogonalna $\mathcal{B}$ jest *ortonormalna*, to znaczy dodatkowo $(v_i, v_i) = 1$ dla każdego $i = 1, \dots, n$. Wtedy z lematu 4.2.1 otrzymujemy $b_{ij} = c_{ji}$, to znaczy $C = B^T$. Zanotujmy ten rezultat jako następujące twierdzenie.

TWIERDZENIE 4.2.1. *Niech $\mathcal{B}$ będzie bazą ortonormalną nieosobliwej przestrzeni dwuliniowej V i niech τ będzie endomorfizmem przestrzeni wektorowej V . Wtedy*

$$\mathbf{m}(\tau^*, \mathcal{B}) = \mathbf{m}(\tau, \mathcal{B})^T.$$

W szczególności, jeśli endomorfizm τ jest samosprzężony, to $\mathbf{m}(\tau, \mathcal{B})$ jest macierzą symetryczną.

Zauważmy, że mamy teraz prosty macierzowy argument dla dowodu twierdzenia 4.1.2. Na przykład, udowodnimy jeszcze raz, że $(\sigma\tau)^* = \tau^* \sigma^*$. Niech $\mathcal{B}$ będzie bazą ortonormalną przestrzeni V . Wtedy na podstawie twierdzenia 4.2.1 mamy

$$\begin{aligned} \mathbf{m}((\sigma\tau)^*, \mathcal{B}) &= \mathbf{m}(\sigma\tau, \mathcal{B})^T = (\mathbf{m}(\sigma, \mathcal{B}) \cdot \mathbf{m}(\tau, \mathcal{B}))^T = \mathbf{m}(\tau, \mathcal{B})^T \cdot \mathbf{m}(\sigma, \mathcal{B})^T = \mathbf{m}(\tau^*, \mathcal{B}) \cdot \mathbf{m}(\sigma^*, \mathcal{B}) \\ &= \mathbf{m}(\tau^* \cdot \sigma^*, \mathcal{B}). \end{aligned}$$

Endomorfizmy $(\sigma\tau)^*$ oraz $\tau^* \cdot \sigma^*$ mają więc równe macierze w bazie $\mathcal{B}$, zatem są równe.

TWIERDZENIE 4.2.2. *Niech τ będzie endomorfizmem nieosobliwej przestrzeni dwuliniowej V . Następujące warunki są równoważne.*

- (a) *Endomorfizm τ jest samosprzężony.*
- (b) *Dla każdej bazy ortonormalnej $\mathcal{B}$ macierz endomorfizmu τ względem bazy $\mathcal{B}$ jest symetryczna.*
- (c) *Istnieje baza ortonormalna $\mathcal{B}$ taka, że macierz endomorfizmu τ względem bazy $\mathcal{B}$ jest symetryczna.*

Dowód. (a) $\Rightarrow$ (b). Jeśli τ jest samosprężony, to już zauważyliśmy, że jego macierz względem dowolnej bazy ortonormalnej $\mathcal{B}$ jest symetryczna na podstawie twierdzenia 4.2.1.

(b) $\Rightarrow$ (c) jest oczywiste.

(c) $\Rightarrow$ (a). Jeśli macierz $[b_{ij}]$ endomorfizmu τ względem bazy $\mathcal{B}$ jest symetryczna, to z rachunku przeprowadzonego w dowodzie lematu 4.2.1 otrzymujemy

$$(v_i, \tau(v_j)) = b_{ij} = b_{ji} = (v_j, \tau(v_i)) = (\tau(v_i), v_j)$$

dla każdych dwóch wektorów v_i, v_j bazy ortonormalnej $\mathcal{B}$. Stąd, wykorzystując dwuliniowość $(\cdot, \cdot)$ oraz liniowość τ otrzymujemy dla dowolnych skalarów x_i, y_j

$$\left(\sum_i x_i v_i, \tau\left(\sum_j y_j v_j\right)\right) = \sum_i \sum_j (v_i, \tau(v_j)) = \sum_i \sum_j (\tau(v_i), v_j) = \left(\tau\left(\sum_i x_i v_i\right), \sum_j y_j v_j\right).$$

A więc τ jest endomorfizmem samosprężonym. $\square$

4.3 Endomorfizmy samosprężone przestrzeni euklidesowych

Najprostszym typem endomorfizmów przestrzeni euklidesowych są endomorfizmy diagonalizowalne w bazie ortonormalnej przestrzeni. Jeśli τ jest takim endomorfizmem przestrzeni euklidesowej V , to istnieje baza ortonormalna $\{v_1, \dots, v_n\}$ przestrzeni V złożona z wektorów własnych endomorfizmu τ . Jeśli wektor własny v_i należy do wartości własnej $a_i \in R$, to $\tau(v_i) = a_i v_i$ i dla dowolnego wektora $v = x_1 v_1 + \dots + x_n v_n \in V$, gdzie $x_i \in R$, mamy

$$\tau(v) = \sum_{i=1}^n x_i \tau(v_i) = x_1 a_1 v_1 + \dots + x_n a_n v_n.$$

Otrzymujemy więc bardzo prosty i geometrycznie przejrzysty opis sposobu działania endomorfizmu τ na wektorach przestrzeni euklidesowej V . W związku z tym naturalnym zagadnieniem staje się znalezienie warunków koniecznych i wystarczających na to by endomorfizm przestrzeni euklidesowej był diagonalizowalny w bazie ortonormalnej przestrzeni. Zauważymy najpierw następujący oczywisty warunek konieczny.

TWIERDZENIE 4.3.1. *Jeśli τ jest endomorfizmem przestrzeni euklidesowej diagonalizowalnym w pewnej bazie ortonormalnej tej przestrzeni, to τ jest endomorfizmem samosprężonym.*

Dowód. Endomorfizm diagonalizowalny w bazie ortonormalnej ma w tej bazie macierz diagonalną, a więc symetryczną i wobec tego jest samosprężony na podstawie twierdzenia 4.2.2. $\square$

Główne twierdzenie tego rozdziału (twierdzenie spektralne 4.3.2) orzeka, że zauważony w twierdzeniu 4.3.1 warunek konieczny diagonalizowalności endomorfizmu w bazie ortonormalnej jest także warunkiem wystarczającym. Rozpocniemy od uniwersalnego lematu o istnieniu podprzestrzeni niezmienniczych endomorfizmów dowolnych (niekoniecznie euklidesowych) przestrzeni wektorowych nad ciałem liczb rzeczywistych.

LEMAT 4.3.1. *Każdy endomorfizm τ dowolnej przestrzeni wektorowej nad ciałem liczb rzeczywistych ma podprzestrzeń niezmienniczą o wymiarze 1 lub 2.*

Dowód. Niech p_τ będzie wielomianem minimalnym endomorfizmu τ . Jest to wielomian o współczynnikach w ciele $\mathbb{R}$. Nad ciałem $\mathbb{R}$ jedynymi wielomianami nierozkładalnymi są wielomiany stopnia 1 i wielomiany stopnia 2 z ujemnym wyróżnikiem. Jeśli wielomian p_τ ma w swoim rozkładzie na czynniki nierozkładalne czynnik stopnia 1, to ma w ciele $\mathbb{R}$ pierwiastek i na podstawie twierdzenia 1.5.2 pierwiastek ten jest wartością własną endomorfizmu τ . Zatem τ ma jednowymiarową podprzestrzeń niezmienniczą. Jeśli wielomian p_τ w swoim rozkładzie na iloczyn czynników nierozkładalnych nie ma czynnika liniowego, to rozkład ten ma postać

$$p_\tau = f_1 \cdots f_k,$$

gdzie wielomiany f_i są trójmianami kwadratowymi z ujemnymi wyróżnikami. Zauważmy, że

$$0 = p_\tau(\tau) = f_1(\tau) \cdots f_k(\tau)$$

i wobec tego co najmniej jeden z endomorfizmów $f_i(\tau)$ jest osobliwy (gdyby wszystkie były nieosobliwe, to ich iloczyn byłby także nieosobliwy, podczas gdy jest endomorfizmem zerowym). Jeśli $f_i = X^2 - aX - b$, gdzie $a, b \in \mathbb{R}$, oraz $v \in V$ jest niezerowym wektorem takim, że $f_i(\tau)(v) = 0$, to podprzestrzeń $U = \text{lin}\{v, \tau(v)\}$ jest τ -niezmiennicza. Rzeczywiście,

$$\tau(U) = \text{lin}\{\tau(v), \tau^2(v)\} = \text{lin}\{\tau(v), a\tau(v) + bv\} \subseteq U.$$

Oczywiście $\dim U \leq 2$ i wobec tego lemat jest udowodniony. $\square$

LEMAT 4.3.2. *Każdy endomorfizm samosprężony przestrzeni euklidesowej ma wektor własny, zatem także podprzestrzeń niezmienniczą o wymiarze 1.*

Dowód. Na podstawie poprzedniego lematu wystarczy jedynie udowodnić, że jeśli τ ma podprzestrzeń niezmienniczą o wymiarze 2, to ma także podprzestrzeń niezmienniczą o wymiarze 1. Przypuśćmy zatem, że U jest τ -niezmiennicza i ma wymiar 2. Możemy zatem traktować τ jako endomorfizm przestrzeni (płaszczyzny) euklidesowej U . Endomorfizm τ po zacieśnieniu do U jest także endomorfizmem samosprężonym przestrzeni U , gdyż $(u, \tau(v)) = (\tau(u), v)$ dla wszystkich $u, v \in V$ i tym bardziej dla wszystkich $u, v \in U$. Wobec tego τ ma w bazie ortonormalnej przestrzeni U macierz symetryczną, powiedzmy

$$\begin{bmatrix} a & b \\ b & c \end{bmatrix}.$$

Wielomian charakterystyczny tej macierzy jest równy

$$X^2 - (a + c)X + ac - b^2$$

a jego wyróżnik

$$(a + c)^2 - 4(ac - b^2) = (a - c)^2 + 4b^2$$

jest sumą kwadratów w ciele $\mathbb{R}$, a zatem jest kwadratem liczby rzeczywistej. Wobec tego wielomian charakterystyczny endomorfizmu τ ma pierwiastek w ciele $\mathbb{R}$, a zatem także wartość własną w ciele $\mathbb{R}$. Stąd wynika, że τ ma wektor własny, który rozpina jednowymiarową podprzestrzeń niezmienniczą. $\square$

LEMAT 4.3.3. *Jeśli τ jest endomorfizmem samosprężonym przestrzeni dwuliniowej V oraz U jest podprzestrzenią τ -niezmienniczą, to ortogonalne dopełnienie $U^\perp$ podprzestrzeni U jest także podprzestrzenią τ -niezmienniczą.*

Dowód. Pokażemy, że jeśli $w \in U^\perp$, to także $\tau(w) \in U^\perp$. Niech $w \in U^\perp$. Wtedy dla każdego $u \in U$ mamy $\tau(u) \in U$ (gdyż U jest podprzestrzenią τ -niezmienniczą) oraz $(w, \tau(u)) = 0$ (gdyż $w \in U^\perp$). Zatem, wobec samosprężoności endomorfizmu τ mamy

$$(\tau(w), u) = (w, \tau(u)) = 0$$

dla każdego $u \in U$. Stąd wynika, że $\tau(w) \in U^\perp$. $\square$

TWIERDZENIE 4.3.2 (Twierdzenie spektralne - przypadek symetryczny). *Niech τ będzie endomorfizmem samosprężonym przestrzeni euklidesowej V . Wtedy istnieje baza ortonormalna przestrzeni V złożona z wektorów własnych endomorfizmu τ .*

Dowód. Indukcja ze względu na wymiar przestrzeni V . Niech $n = \dim V > 1$ i niech U będzie 1-wymiarową podprzestrzenią niezmienniczą endomorfizmu τ . Wtedy na podstawie lematu 4.3.3 podprzestrzeń $U^\perp$ jest także τ -niezmiennicza oraz

$$V = U \oplus U^\perp$$

na podstawie twierdzenia 2.5.1 o rzucie prostopadłym. Na podstawie założenia indukcyjnego istnieje baza ortonormalna podprzestrzeni $U^\perp$ złożona z wektorów własnych endomorfizmu τ . Dołączając do niej wektor $u_1 \in U$ o długości 1 otrzymamy bazę ortonormalną przestrzeni V złożoną z wektorów własnych endomorfizmu τ . $\square$

Zauważmy, że twierdzenia 4.3.1 i 4.3.2 dają warunek konieczny i wystarczający diagonalizowalności endomorfizmu przestrzeni euklidesowej w bazie ortonormalnej: *Endomorfizm przestrzeni euklidesowej jest diagonalizowalny w bazie ortonormalnej tej przestrzeni wtedy i tylko wtedy gdy jest samosprężony.*

TWIERDZENIE 4.3.3. *Niech A będzie macierzą symetryczną o elementach rzeczywistych. Wtedy istnieje macierz ortogonalna P o elementach z ciała $\mathbb{R}$ taka, że $P^{-1}AP$ jest macierzą diagonalną.*

Dowód. Macierz A traktujemy jako macierz endomorfizmu samosprężonego przestrzeni euklidesowej $\mathbb{R}^n$ w bazie standardowej. Na podstawie twierdzenia spektralnego istnieje baza ortonormalna $\mathcal{B}$ przestrzeni $\mathbb{R}^n$, w której endomorfizm ten ma macierz diagonalną D . Jeśli P jest macierzą przejścia od bazy standardowej do bazy $\mathcal{B}$, to $D = P^{-1}AP$ na podstawie twierdzenia 1.6.1. $\square$

Ostatnie twierdzenie mówi, że każda macierz symetryczna nad ciałem liczb rzeczywistych jest *ortogonalnie podobna* do macierzy diagonalnej.

4.4 Przemienne zbiory endomorfizmów samosprężonych

Na podstawie twierdzenia spektralnego każdy endomorfizm samosprężony przestrzeni euklidesowej jest diagonalizowalny w pewnej bazie ortonormalnej tej przestrzeni. Jeśli więc weźmiemy dwa endomorfizmy samosprężone σ i τ przestrzeni euklidesowej V , to dla każdego z nich istnieje baza ortonormalna złożona z wektorów własnych tego endomorfizmu. Nasuwa się naturalne pytanie, czy istnieje taka baza ortonormalna przestrzeni V , której każdy wektor jest wektorem własnym zarówno σ jak i τ ? Następujące twierdzenie wskazuje warunek konieczny jaki spełniać muszą endomorfizmy samosprężone σ i τ diagonalizowalne w tej samej bazie ortonormalnej przestrzeni euklidesowej.

Twierdzenie 4.4.1. *Niech σ i τ będą endomorfizmami samosprężonymi przestrzeni euklidesowej V . Jeśli istnieje baza przestrzeni V złożona z wektorów własnych obydwu endomorfizmów σ i τ , to endomorfizmy te są przemienne:*

$$\sigma\tau = \tau\sigma.$$

Dowód. Niech $\{v_1, \dots, v_n\}$ będzie bazą przestrzeni V taką, że $\sigma(v_i) = a_i v_i$, $\tau(v_i) = b_i v_i$ dla pewnych skalarów $a_i, b_i \in R$. Wtedy

$$(\sigma\tau)(v_i) = \sigma(b_i v_i) = b_i a_i v_i = \tau(a_i v_i) = (\tau\sigma)(v_i), \quad i = 1, \dots, n.$$

Endomorfizmy $\sigma\tau$ oraz $\tau\sigma$ przyjmują te same wartości na wektorach bazy przestrzeni V i wobec tego przyjmują te same wartości na wszystkich wektorach przestrzeni V : $\sigma\tau = \tau\sigma$. $\square$

Naszym celem jest udowodnić, że przemienność endomorfizmów samosprężonych jest także warunkiem wystarczającym na ich diagonalizowalność w tej samej bazie ortonormalnej przestrzeni euklidesowej. Faktycznie nie ma potrzeby ograniczać się do dwóch endomorfizmów samosprężonych. Będziemy rozpatrywać dowolny zbiór $\mathcal{T}$ endomorfizmów samosprężonych przestrzeni euklidesowej V . Z twierdzenia 4.4.1 otrzymujemy natychmiast, że jeśli istnieje baza przestrzeni V złożona z wektorów własnych wszystkich endomorfizmów zbioru $\mathcal{T}$, to $\mathcal{T}$ jest *przemiennym zbiorem endomorfizmów* przestrzeni V , to znaczy, $\tau\sigma = \sigma\tau$ dla każdego $\tau, \sigma \in \mathcal{T}$. Przystępujemy do dowodu twierdzenia odwrotnego.

Lemat 4.4.1. *Niech $\mathcal{T}$ będzie przemiennym zbiorem endomorfizmów samosprężonych przestrzeni euklidesowej V . Wtedy istnieje wspólny wektor własny dla wszystkich endomorfizmów zbioru $\mathcal{T}$ (to znaczy taki wektor $v \in V$, że $v \neq 0$ oraz dla każdego $\tau \in \mathcal{T}$ mamy $\tau(v) \in Rv$).*

Dowód. Najpierw rozpatrzmy (trywialny) przypadek, gdy wszystkie endomorfizmy w zbiorze $\mathcal{T}$ są skalarne, a więc postaci $\tau = a\mathbf{1}_V$, gdzie $a \in R$ zaś $\mathbf{1}_V$ jest identycznością na V . Dla endomorfizmu skalarnego każdy niezerowy wektor przestrzeni V jest wektorem własnym. W związku z tym, jeśli wszystkie endomorfizmy w zbiorze $\mathcal{T}$ są skalarne, to każdy niezerowy wektor przestrzeni V jest wspólnym wektorem własnym wszystkich endomorfizmów zbioru $\mathcal{T}$. W szczególności, jeśli $\dim V = 1$, to wszystkie endomorfizmy są skalarne i wobec tego lemat jest prawdziwy. Przeprowadzimy dowód indukcyjny ze względu na wymiar przestrzeni V . Niech więc $\dim V > 1$. Jeśli $\tau \in \mathcal{T}$ nie jest skalarny, to τ ma wartość własną a i wektor własny $v \in V$ należący do a . Niech

$$U = \{u \in V : \tau(u) = au\}.$$

Jest to podprzestrzeń τ -niezmiennicza, a także, $U \neq 0$ oraz $U \neq V$ (bo τ nie jest skalarny). Ponadto, U jest σ -niezmiennicza dla każdego $\sigma \in \mathcal{T}$. Rzeczywiście, dla $u \in U$ mamy

$$\tau(\sigma(u)) = \sigma(\tau(u)) = \sigma(au) = a\sigma(u),$$

zatem $\sigma(u) \in U$. Zacieśnienia endomorfizmów $\sigma \in \mathcal{T}$ do podprzestrzeni U tworzą więc przemienne zbiory endomorfizmów samosprężonych przestrzeni U i wobec $\dim U < \dim V$ na podstawie założenia indukcyjnego endomorfizmy zbioru $\mathcal{T}$ mają wspólny wektor własny w podprzestrzeni U . $\square$

Twierdzenie 4.4.2. *Jeśli $\mathcal{T}$ jest przemiennym zbiorem endomorfizmów samosprężonych przestrzeni euklidesowej V , to V ma bazę ortonormalną $\{v_1, \dots, v_n\}$ taką, że każdy wektor v_i jest wektorem własnym wszystkich endomorfizmów zbioru $\mathcal{T}$.*

Dowód. Przeprowadzimy dowód indukcyjny ze względu na wymiar n przestrzeni V . Twierdzenie jest oczywiście prawdziwe dla $n = 1$. Niech więc $n > 1$. Na podstawie lematu 4.4.1 istnieje wspólny wektor własny $v \in V$ dla wszystkich endomorfizmów $\tau \in \mathcal{T}$. Możemy zakładać, że $\|v\| = 1$, gdyż w przeciwnym razie zamiast wektora v weźmiemy wektor $\frac{1}{\|v\|}v$. Niech $U = \mathbb{R}v$. Jest to więc podprzestrzeń τ –niezmiennicza dla każdego endomorfizmu $\tau \in \mathcal{T}$. Na podstawie lematu 4.3.3 ortogonalne dopełnienie $U^\perp$ podprzestrzeni U jest podprzestrzenią τ –niezmienniczą dla każdego endomorfizmu $\tau \in \mathcal{T}$. Ponieważ $\dim U^\perp < \dim V$, na podstawie założenia indukcyjnego podprzestrzeń $U^\perp$ ma bazę ortonormalną $v_2, \dots, v_n$ złożoną z wektorów własnych wszystkich endomorfizmów $\tau \in \mathcal{T}$. Wtedy $\{v, v_2, \dots, v_n\}$ jest bazą ortonormalną przestrzeni V złożoną z wektorów własnych wszystkich endomorfizmów $\tau \in \mathcal{T}$. $\square$

Twierdzenia 4.4.1 i 4.4.2 podają warunek konieczny i wystarczający równoczesnej diagonalizowalności zbioru endomorfizmów samosprzężonych przestrzeni euklidesowej w bazie ortonormalnej tej przestrzeni: *Dla zbioru $\mathcal{T}$ endomorfizmów samosprzężonych przestrzeni euklidesowej istnieje baza ortonormalna przestrzeni złożona z wektorów własnych wszystkich endomorfizmów zbioru $\mathcal{T}$ wtedy i tylko wtedy gdy każde dwa endomorfizmy zbioru $\mathcal{T}$ są przemienne.*

4.5 Izometrie przestrzeni dwuliniowych

Wprawdzie interesują nas przede wszystkim endomorfizmy przestrzeni euklidesowych, ale własności, które będziemy omawiać, mają znacznie szerszy zakres i w związku z tym nie będziemy ograniczać się do przestrzeni euklidesowych. Właściwym kontekstem są tutaj przestrzenie dwuliniowe nad dowolnym ciałem i takie też będziemy przeważnie czynić założenie. Izometrią przestrzeni dwuliniowej V nazywamy bijektywny endomorfizm $\tau : V \rightarrow V$ taki, że $(\tau(u), \tau(v)) = (u, v)$ dla wszystkich $u, v \in V$. Okazuje się, że jeśli przestrzeń V jest nieosobliwa, to bijektywność τ jest konsekwencją pozostałych założeń.

LEMAT 4.5.1. *Niech τ będzie endomorfizmem nieosobliwej przestrzeni dwuliniowej V . Jeśli endomorfizm τ spełnia warunek:*

$$(\tau(u), \tau(v)) = (u, v) \quad \text{dla wszystkich } u, v \in V,$$

to τ jest bijektywny, czyli jest automorfizmem przestrzeni wektorowej V .

Dowód. Przypuśćmy, że $\tau(v) = 0$ dla pewnego $v \in V$. Wtedy $0 = (\tau(u), \tau(v)) = (u, v)$ dla każdego wektora $u \in V$. Stąd $v \in \text{rad } V$ i wobec nieosobliwości przestrzeni V otrzymujemy $v = 0$. A więc $\ker \tau = 0$, τ jest injektywny, a więc także surjektywny. $\square$

Zauważmy także, że jeśli τ jest izometrią nieizotropowej przestrzeni dwuliniowej V i τ ma wartość własną a , to koniecznie $a = \pm 1$. Rzeczywiście, jeśli a jest wartością własną τ i wektor własny v należy do wartości własnej a , to $\tau(v) = av$ oraz $(v, v) = (\tau(v), \tau(v)) = (av, av) = a^2(v, v)$, skąd wobec nieizotropowości przestrzeni V wynika, że $a^2 = 1$.

Z drugiej strony, izometrie mogą w ogóle nie mieć wartości własnych. Na przykład, obrót na płaszczyźnie euklidesowej $\mathbb{R}^2$ o kąt różny od zerowego i półpełnego nie ma oczywiście wartości własnych (bo nie ma wektorów własnych).

4.6 Symetrie przestrzeni dwuliniowych

In this chapter¹ we will consider the isometries of a bilinear space V . This is of great importance for revealing the structure and deeper properties of a bilinear space V .

Thus we consider bijective linear maps $i : V \rightarrow V$ preserving the bilinear functional on the space V :

$$(x, y) = (i(x), i(y)) \quad \text{for all } x, y \in V.$$

The set of all isometries of the space V is denoted $\mathbf{Isom} V$. It is nonempty, since the identity map id_V , leaving every vector of V fixed, is an isometry of V . The identity map will be also written 1_V . There is also the negative -1_V of 1_V which reverses every vector in V , that is, $-1_V(x) = -x$ for all $x \in V$. This is also an isometry of V .

Now we will show that the set $\mathbf{Isom} V$ is, in fact, a group with respect to the composition of maps. The best we can do is to show that $\mathbf{Isom} V$ is a subgroup of the automorphism group $\mathbf{Aut} V$ of bijective linear maps of the vector space V onto V . Thus we are to check that $\mathbf{Isom} V$ is closed with respect to composition of maps, and closed with respect to taking inverses. So let $i, j \in \mathbf{Isom} V$. Then $i \circ j : V \rightarrow V$ is a linear automorphism, and it is an isometry of V , since we have

$$(x, y) = (j(x), j(y)) = (i(j(x)), i(j(y))) = ((i \circ j)(x), (i \circ j)(y))$$

for all $x, y \in V$. It follows that $i \circ j \in \mathbf{Isom} V$. Further, if $i \in \mathbf{Isom} V$, then also $i^{-1} \in \mathbf{Isom} V$, since for $x = i(u)$, $y = i(v)$, $u, v \in V$, we have

$$(x, y) = (i(u), i(v)) = (u, v) = (i^{-1}(x), i^{-1}(y)).$$

Thus $\mathbf{Isom} V$ is a group, and we call it the *isometry group* of the bilinear space V .

DEFINICJA 4.6.1. For a nonsingular symmetric bilinear space V the group $\mathbf{Isom} V$ is said to be the *orthogonal group* of V and is denoted $O(V)$.

We will study the group $O(V)$ in §4.8. Here we only point out some important examples of isometries called *symmetries*.

The motivating example comes from the geometry of Euclidean space $\mathbb{R}^3$. If U is a line in the space $\mathbb{R}^3$, and $U^\perp$ is the plane orthogonal to U , then the ‘mirror’ reflection about the plane $U^\perp$ is a nontrivial isometry of the Euclidean space $\mathbb{R}^3$. It reverses the vectors of the line U and leaves the vectors of the plane $U^\perp$ pointwise fixed.

Now we define symmetries in arbitrary bilinear space V . Let U be a nonsingular subspace of V . Then, according to the orthogonal complement theorem, we have

$$V = U \oplus U^\perp.$$

DEFINICJA 4.6.2. A symmetry of the space V with respect to the nonsingular subspace U is the map $\sigma_U : V \rightarrow V$, defined as follows

$$\sigma_U(u + w) = -u + w, \quad \text{for } u \in U, w \in U^\perp.$$

Thus the symmetry σ_U reverses each vector $u \in U$,

$$\sigma_U(u) = -u \quad \text{for all } u \in U,$$

¹Fragmentsy tekstu w języku angielskim pochodzą z mojej książki *Bilinear Algebra*, Gordon and Breach Science Publishers, Amsterdam 1997.

and leaves the orthogonal complement $U^\perp$ of U pointwise fixed:

$$\sigma_U(w) = w \text{ for all } w \in U^\perp.$$

We leave it to the reader to check that σ_U is a linear automorphism of the vector space V . Given this we show that σ_U is an isometry of the bilinear space V .

For, if $u, u' \in U$, $w, w' \in U^\perp$, then

$$\begin{aligned} (\sigma_U(u + w), \sigma_U(u' + w')) &= (-u + w, -u' + w') \\ &= (u, u') + (w, w') \\ &= (u + w, u' + w'). \end{aligned}$$

Thus for each nonsingular subspace U of V , we have $\sigma_U \in \mathbf{Isom} V$. Choosing the subspace U properly we find nontrivial elements of the isometry group $\mathbf{Isom} V$. The following two particular choices for U are noteworthy.

Przykład 4.6.1. Let V be a nonsingular space and put $U = V$. Then $V^\perp = 0$, and

$$\sigma_V(v) = -v \text{ for all } v \in V.$$

Thus with this choice of U , we have $\sigma_V = -1_V$.

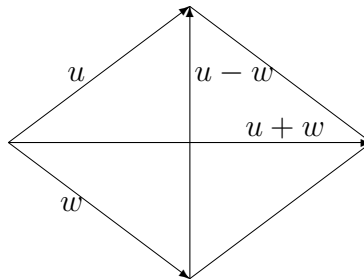
Przykład 4.6.2. Let V be a bilinear space and let $u \in V$ be an anisotropic vector. Then the 1-dimensional subspace $U = Ku$ is nonsingular and we can take the symmetry σ_U with respect to the line $U = Ku$. We write σ_u instead of σ_U and call it the symmetry with respect to the anisotropic vector u . Its action on V is defined by the equation

$$\sigma_u(au + w) = -au + w,$$

for all $a \in K$ and all vectors w orthogonal to u .

Twierdzenie 4.6.1. (Witt's prolongation theorem - first version.) *Let V be a symmetric space over a field K of characteristic $\neq 2$. For each pair of anisotropic vectors u and w with equal norms, there is an isometry of the space V carrying u to w .*

Dowód. We can assume that $u \neq w$, since otherwise the identity 1_V takes u to w . We will use the picture below to direct our intuition but the proof will run independently of any intuitive arguments. So u and w , having equal norms, span a rhombus with the diagonals $u + w$ and $u - w$.



These diagonals are orthogonal (as they should be in a rhombus), since we have $(u - w, u + w) = (u, u) + (u, w) + (-w, u) + (-w, w) = 0$. Moreover, $u = \frac{1}{2}(u - w) + \frac{1}{2}(u + w)$, that is, u is the sum of two orthogonal vectors.

Now if the vector $u - w$ is anisotropic, we can take the symmetry σ_{u-w} in the nonsingular line $K(u - w)$ and then we get

$$\sigma_{u-w}(u) = -\frac{1}{2}(u - w) + \frac{1}{2}(u + w) = w.$$

Hence the isometry σ_{u-w} carries u to w .

Similarly, if the vector $u + w$ is anisotropic, we take the symmetry σ_{u+w} and observe that

$$\sigma_{u+w}(u) = \frac{1}{2}(u - w) - \frac{1}{2}(u + w) = -w.$$

This time the composition $-1_V \circ \sigma_{u+w}$ takes u to w . Alternatively, the composition of two symmetries $\sigma_w \circ \sigma_{u+w}$ also sends u to w .

Thus if at least one of the vectors $u - w$ and $u + w$ is anisotropic, then we are through. It remains to show that one of the vectors $u - w$ and $u + w$ has to be anisotropic. So assume that $(u - w, u - w) = (u + w, u + w) = 0$. Then we would have

$$0 = (u - w, u - w) + (u + w, u + w) = 2((u, u) + (w, w)) = 4(u, u),$$

contrary to the assumptions that $(u, u) \neq 0$ and $\text{char } K \neq 2$. $\square$

Before going on we draw a corollary which states precisely what has been proved.

WNIOSEK 4.6.1. *Retain the hypotheses from Theorem 4.6.1. Then either $u - w$ is anisotropic and the symmetry σ_{u-w} takes u to w , or, $u + w$ is anisotropic and the composition $\sigma_w \circ \sigma_{u+w}$ takes u to w .*

4.7 Macierzowa reprezentacja grupy izometrii

Let V be a bilinear space over an arbitrary field K . The isometry group $\text{Isom } V$ of the bilinear space V is a subgroup of the automorphism group $\text{Aut } V$ of the vector space V :

$$\text{Isom } V \subseteq \text{Aut } V.$$

Now $\text{Aut } V$ is known to be isomorphic with the linear group $\mathbf{GL}(n, K)$, where $n = \dim V$. Recall that $\mathbf{GL}(n, K)$ is the group of all invertible $n \times n$ matrices with entries in K . We fix an isomorphism

$$\mu : \text{Aut } V \rightarrow \mathbf{GL}(n, K),$$

and will find the subgroup $\mu(\text{Isom } V)$ of $\mathbf{GL}(n, K)$ which corresponds to the isometry subgroup $\text{Isom } V$ of the group $\text{Aut } V$. As is known from a basic linear algebra course, the isomorphism μ is defined as follows. We choose a basis $\mathcal{B} = \{v_1, \dots, v_n\}$ for the vector space V and for each linear automorphism $\sigma \in \text{Aut } V$ and each basis vector v_i we write $\sigma(v_i)$ as a linear combination of the basis vectors:

$$\begin{aligned} \sigma(v_1) &= s_{11}v_1 + s_{21}v_2 + \dots + s_{n1}v_n, \\ &\vdots \\ \sigma(v_n) &= s_{1n}v_1 + s_{2n}v_2 + \dots + s_{nn}v_n. \end{aligned} \tag{4.2}$$

This gives the matrix

$$S = [s_{ij}] = \begin{bmatrix} s_{11} & s_{12} & \dots & s_{1n} \\ s_{21} & s_{22} & \dots & s_{2n} \\ \vdots & \vdots & \dots & \vdots \\ s_{n1} & s_{n2} & \dots & s_{nn} \end{bmatrix},$$

whose i -th column consists of coordinates of the vector $\sigma(v_i)$ in the basis $\mathcal{B}$. In linear algebra course one shows that the mapping

$$\mu : \text{Aut } V \rightarrow \mathbf{GL}(n, K), \quad \mu(\sigma) = S$$

is a group isomorphism. Let us emphasize that the isomorphism μ depends on the choice of the basis $\mathcal{B}$. Two different bases for V always determine two distinct isomorphisms $\text{Aut } V \rightarrow \mathbf{GL}(n, K)$.

Now we come to the point of interest to us. Assume that the automorphism σ of V is an isometry of the bilinear space V . What can be said about the matrix $S = \mu(\sigma)$?

TWIERDZENIE 4.7.1. *Let V be an n -dimensional bilinear space over a field K . Let $\mathcal{B} = \{v_1, \dots, v_n\}$ be a basis for V and let $A = [(v_i, v_j)]$ be the matrix of V relative to the basis $\mathcal{B}$.*

(a) *An automorphism σ of the vector space V is an isometry of the bilinear space V if and only if the matrix $S = \mu(\sigma)$ of the automorphism σ relative to the basis $\mathcal{B}$ satisfies the condition*

$$S^t A S = A.$$

(b) *The group $\text{Isom } V$ of isometries of bilinear space V is isomorphic to the subgroup*

$$\{S \in \mathbf{GL}(n, K) : S^t A S = A\}$$

of the matrix group $\mathbf{GL}(n, K)$.

Dowód. (a) The equalities (4.2) show that S^t is the transition matrix from the basis $\mathcal{B} = \{v_1, \dots, v_n\}$ to the basis $\sigma(\mathcal{B}) = \{\sigma(v_1), \dots, \sigma(v_n)\}$ of the space V . Hence, by Theorem 2.2.1,

$$[(\sigma(v_i), \sigma(v_j))] = S^t A (S^t)^t = S^t A S.$$

On the other hand, σ is an isometry if and only if $(\sigma(v_i), \sigma(v_j)) = (v_i, v_j)$ for all $i, j \leq n$, that is, if and only if $S^t A S = A$.

(b) is just a restatement of (a). □

As an example we now consider the isometry group of the hyperbolic plane $\mathbf{H}$ over a field K of characteristic $\neq 2$. So we assume that $\{u, v\}$ is a hyperbolic pair spanning $\mathbf{H}$:

$$\mathbf{H} \cong \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{in } \{u, v\}.$$

Let $\sigma \in \text{Isom } \mathbf{H}$ be an isometry of the hyperbolic plane and let $S = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ be the matrix of σ with respect to the basis $\{u, v\}$. By Theorem 4.7.1,

$$S^t \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} S = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Multiplying through we get

$$\begin{bmatrix} 2ab & ad + bc \\ ad + bc & 2cd \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

The four entries of the matrix S are to satisfy the system of equations

$$ab = 0, \quad ad + bc = 1, \quad cd = 0,$$

and we require additionally that $\det S = ad - bc \neq 0$, since S is an invertible matrix. This system has two series of solutions:

I. $b = 0, \quad c = 0, \quad d = a^{-1}, \quad a$ - an arbitrary element of K .

II. $a = 0$, $d = 0$, $c = b^{-1}$, b - an arbitrary element of $\dot{K}$.

Thus we have two types of isometries σ of the hyperbolic plane $\mathbf{H}$:

$$\text{Type I : } S = \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}; \quad \sigma(u) = au, \quad \sigma(v) = a^{-1}v,$$

$$\text{Type II : } S = \begin{bmatrix} 0 & b^{-1} \\ b & 0 \end{bmatrix}; \quad \sigma(u) = bv, \quad \sigma(v) = b^{-1}u.$$

It is useful to observe that isometries of type I leave the isotropic lines Ku and Kv fixed (but not elementwise!), while isometries of the type II interchange the two isotropic lines of the plane $\mathbf{H}$.

Now we will show that every isometry σ of type II is, in fact, the symmetry σ_{u-bv} in the nonsingular line $K(u - bv)$. First we have

$$(u - bv, u - bv) = -2b(u, v) = -2b \neq 0,$$

and so $u - bv$ is an anisotropic vector. We also have

$$(u - bv, u + bv) = (u - \sigma(u), u + \sigma(u)) = 0,$$

so that $u - bv, u + bv$ form an orthogonal basis for $\mathbf{H}$. Now we check that σ and σ_{u-bv} assume equal values on the basis of $\mathbf{H}$:

$$\sigma(u - bv) = \sigma(u) - b\sigma(v) = bv - u = \sigma_{u-bv}(u - bv),$$

$$\sigma(u + bv) = \sigma(u) + b\sigma(v) = bv + u = \sigma_{u-bv}(u + bv).$$

It follows that $\sigma = \sigma_{u-bv}$.

Now we show that every isometry of type I is the product of two symmetries: $\sigma = \sigma_{u-v} \circ \sigma_{u-av}$. We start with the observation that, as shown above, for each $b \in \dot{K}$, the symmetry σ_{u-bv} is an isometry of type II, hence for $b = a$ and $b = 1$, we have

$$\sigma_{u-av}(u) = av, \quad \sigma_{u-av}(v) = a^{-1}u, \quad \sigma_{u-v}(u) = v, \quad \sigma_{u-v} = u.$$

This is what we need to compute the images of basis vectors u and v under the composition $\sigma_{u-v} \circ \sigma_{u-av}$:

$$\sigma_{u-v} \circ \sigma_{u-av}(u) = \sigma_{u-v}(av) = au = \sigma(u),$$

$$\sigma_{u-v} \circ \sigma_{u-av}(v) = \sigma_{u-v}(a^{-1}u) = a^{-1}v = \sigma(v).$$

Thus the isometries $\sigma_{u-v} \circ \sigma_{u-av}$ and σ act in the same way on the basis $\{u, v\}$ of the plane $\mathbf{H}$, hence they act in the same way on the whole hyperbolic plane $\mathbf{H}$. We have obtained the following explicit description of the isometry group of hyperbolic plane.

TWIERDZENIE 4.7.2. *Let K be a field of characteristic different from 2.*

(a) *Every isometry σ of the hyperbolic plane $\mathbf{H}$ over K is either a symmetry or the product of two symmetries in anisotropic lines of the plane $\mathbf{H}$.*

(b) *The set of matrices*

$$\left\{ \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} : a \in \dot{K} \right\} \cup \left\{ \begin{bmatrix} 0 & b^{-1} \\ b & 0 \end{bmatrix} : b \in \dot{K} \right\}$$

is a subgroup of $\mathbf{GL}(2, K)$ isomorphic to the isometry group $\mathbf{Isom} \mathbf{H}$ of the hyperbolic plane $\mathbf{H}$ over the field K .

The determinants of matrices in the theorem above are all 1 or -1 . This is more than a coincidence. Recall that given any automorphism σ of the vector space V , the determinant $\det \sigma$ of σ is defined to be the determinant of the matrix S of σ relative to any basis $\mathcal{B}$ of the space V . It is well known that $\det S$ does not depend on the choice of the basis $\mathcal{B}$. Taking the determinant of automorphism of V defines a group homomorphism

$$\det : \text{Aut } V \rightarrow \dot{K},$$

which can also be viewed as the composition

$$\text{Aut } V \xrightarrow{\mu} \mathbf{GL}(n, K) \xrightarrow{\det} \dot{K}.$$

TWIERDZENIE 4.7.3. *Let V be a nonsingular bilinear space over a field K . Then every isometry of V has determinant ± 1 , i.e.,*

$$\det(\text{Isom } V) \subseteq \{1, -1\} \subseteq \dot{K}.$$

Dowód. Let $\sigma \in \text{Isom } V$. We choose a basis $\mathcal{B}$ for V and take the matrix S of σ relative to $\mathcal{B}$ and the matrix A of V relative to $\mathcal{B}$. Then by Theorem 4.7.1, $S^t A S = A$, hence taking determinants we get $(\det S)^2 \det A = \det A$. Since V is nonsingular, we have $\det A \neq 0$, and so $(\det S)^2 = 1$. Thus $\det \sigma = \det S = \pm 1$, as required. $\square$

DEFINICJA 4.7.1. An isometry σ of the bilinear space V is said to be a *rotation* of the space V , if $\det \sigma = 1$, and is said to be a *reflection* of V , if $\det \sigma = -1$.

Przykład 4.7.1. Rotations of the hyperbolic plane $\mathbf{H}$ are the isometries of type I, i.e., those with diagonal matrices relative to the hyperbolic pair spanning $\mathbf{H}$, and reflections are the isometries of type II.

It is clear that rotations of a bilinear space V form a subgroup in the isometry group $\text{Isom } V$. We will give some more details on the rotation groups in the next section. Here we discuss another subgroup of the isometry group called the center of the group. The center $Z(G)$ of a group G is the set of elements of G which commute with every element of the group G . Thus the center of the isometry group is defined to be

$$Z(\text{Isom } V) := \{\sigma \in \text{Isom } V : \sigma \circ \tau = \tau \circ \sigma \text{ for all } \tau \in \text{Isom } V\}.$$

Clearly $1_V \in Z(\text{Isom } V)$, and it is also easy to check that $-1_V \in Z(\text{Isom } V)$. We will show in the next section that these two isometries are, in general, the only central elements of the isometry group. As a preparation we now prove a geometric characterization of the isometries $\pm 1_V$. The geometric property of an isometry σ we are going to use is that σ leaves every line of the space V fixed. This amounts to satisfying the condition

$$\sigma(Kv) = Kv$$

for each nonzero vector $v \in V$, that is, for each line Kv of V . Clearly, 1_V and -1_V leave every line of V fixed, and we are going to prove that no other isometry does.

TWIERDZENIE 4.7.4. *Let V be a non-totally isotropic bilinear space over a field K . An isometry $\sigma \in \text{Isom } V$ leaves every line of V fixed if and only if $\sigma = 1_V$ or $\sigma = -1_V$.*

Dowód. Suppose v is a nonzero vector in V and an isometry σ leaves the line Kv fixed. Then $\sigma(v) = av$ for some $a \in \dot{K}$. If u is an arbitrary vector of the line Kv , then $u = bv$, where $b \in K$, and we have

$$\sigma(u) = \sigma(bv) = b\sigma(v) = abv = au = a \cdot 1_{Kv}(u).$$

This shows that, if an isometry σ leaves the line Kv fixed, then its restriction $\sigma|_{Kv}$ to the line Kv is a scalar multiple of the identity isometry of the line:

$$\sigma|_{Kv} = a \cdot 1_{Kv}.$$

Now assume that $\dim V \geq 2$ and σ leaves every line of V fixed. Then for any two linearly independent vectors $v, w \in V$ there are $a, b, c \in K$ such that

$$\sigma|_{Kv} = a \cdot 1_{Kv}, \quad \sigma|_{Kw} = b \cdot 1_{Kw}, \quad \sigma|_{K(v+w)} = c \cdot 1_{K(v+w)}.$$

Hence

$$c(v+w) = \sigma(v+w) = \sigma(v) + \sigma(w) = av + bw.$$

Now linear independence of v and w implies

$$a = c = b.$$

We have proved that, if σ leaves every line of V fixed, then there is an element $a \in K$ such that $\sigma(v) = av$ for all $v \in V$. It remains to show that $a = \pm 1$. Since V is not totally isotropic, there are $u, v \in V$ with $(u, v) \neq 0$. Then

$$(u, v) = (\sigma(u), \sigma(v)) = (au, av) = a^2(u, v).$$

Hence $a^2 = 1$ and $a = \pm 1$, as required. $\square$

4.8 Grupa ortogonalna

In this section we assume throughout that V is a *symmetric* bilinear space. According to Definition 4.6.1, the isometry group $\text{Isom } V$ of a nonsingular symmetric space V is said to be the *orthogonal group* of V and is denoted $O(V)$. If V is an n -dimensional symmetric space over K and A is the matrix of V relative to a basis of V , then

$$O(V) \cong \{S \in \mathbf{GL}(n, K) : S^t A S = A\},$$

in view of Theorem 4.7.1. We begin our discussion of the orthogonal group with a result on the determinant homomorphism $\det : O(V) \rightarrow \{\pm 1\}$. If the characteristic of the field K is 2, then $-1 = 1$, and so $\det$ is obviously a surjective homomorphism. In other words, when $\text{char } K = 2$, then every isometry in $O(V)$ is a rotation. When $\text{char } K \neq 2$, then the determinant homomorphism is also surjective, as the following theorem shows, but this time the conclusion is that not all isometries in $O(V)$ are rotations.

TWIERDZENIE 4.8.1. *For every nonsingular symmetric space V over a field K of characteristic $\neq 2$, the determinant homomorphism*

$$\det : O(V) \rightarrow \{\pm 1\} \tag{4.3}$$

is a surjective map.

Dowód. It is sufficient to point out a reflection in the group $O(V)$. The space V is diagonalizable by Theorem 2.6.1, so we can assume that $\mathcal{B} = \{v_1, \dots, v_n\}$ is an orthogonal basis for V . By nonsingularity of V , all the basis vectors are anisotropic, and so it makes sense to consider the symmetry $\sigma := \sigma_{v_1}$. Since σ reverses v_1 and leaves fixed all the other basis vectors in $\mathcal{B}$, the matrix of σ in the basis $\mathcal{B}$ is the diagonal matrix $S = (-1, 1, \dots, 1)$. Now from

$$-1 = \det S = \det \sigma \in \det(O(V)),$$

it follows that σ is a reflection, as required. $\square$

The group of rotations of a symmetric space V is usually denoted $O^+(V)$. Thus

$$O^+(V) = \{\sigma \in O(V) : \det \sigma = 1\}$$

is the kernel of the determinant homomorphism (4.3). As such it is a normal subgroup of the orthogonal group, and if $\text{char } K \neq 2$, then the index of the rotation group $O^+(V)$ in $O(V)$ is 2. In the latter case, each symmetry σ_v in an anisotropic line Kv is a reflection and we get the following coset decomposition of the orthogonal group:

$$O(V) = O^+(V) \cup \sigma_v O^+(V).$$

Przykład 4.8.1. Consider orthogonal group $O(\mathbf{H})$ of the hyperbolic plane $\mathbf{H}$ over a field of characteristic $\neq 2$. The rotation group $O^+(\mathbf{H})$ is isomorphic to the matrix group

$$\left\{ \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} : a \in K \right\}.$$

This follows immediately from Theorem 4.7.2.

Now we are going to discuss generating sets for the orthogonal group. We have observed in the proof of Theorem 4.8.1 that every symmetry σ_v with respect to an anisotropic line Kv is a reflection. Hence a product

$$\sigma_{v_1} \circ \cdots \circ \sigma_{v_k}$$

of symmetries is a rotation if k is even, and a reflection, if k is odd. Thus products of symmetries produce both rotations and reflections and it is a natural question to ask whether the symmetries actually generate the entire orthogonal group $O(V)$. This makes sense only when $\text{char } K \neq 2$, since otherwise $\sigma_v = 1_V$ for every anisotropic $v \in V$. We will answer the question in the affirmative but first we consider some special cases.

Przykład 4.8.2. Let V be a nonsingular symmetric space over a field of characteristic $\neq 2$. If $\dim V = 1$, then it is easy to show that $O(V) = \{1_V, -1_V\}$, and moreover, -1_V is a symmetry. Then also $1_V = -1_V \circ -1_V$ is a product of two symmetries. If $\dim V = n \geq 2$, then V has an orthogonal basis $\{v_1, \dots, v_n\}$ and we have

$$1_V = \sigma_{v_1} \circ \sigma_{v_1} \quad \text{and} \quad -1_V = \sigma_{v_1} \circ \cdots \circ \sigma_{v_n}.$$

These follow from determining the action of the given products of symmetries on the basis vectors $v_1, \dots, v_n$. For instance,

$$\sigma_{v_1} \circ \cdots \circ \sigma_{v_n}(v_k) = \sigma_{v_1} \circ \cdots \circ \sigma_{v_k}(v_k) = \sigma_{v_1} \circ \cdots \circ \sigma_{v_{k-1}}(-v_k) = -v_k,$$

for $k = 1, \dots, n$. Thus we have shown that, if $\dim V = n$, then the isometry -1_V is a product of n symmetries.

Przykład 4.8.3. We will prove here a result complementary to Theorem 4.7.2. We consider an *anisotropic* plane V over a field K of characteristic $\neq 2$ and claim that *every isometry of V is either a symmetry or the product of two symmetries*.

We fix an orthogonal basis $\{u, v\}$ for V and consider an arbitrary isometry $\sigma \in O(V)$. There are two cases.

I. $\sigma(u) = u$.

Suppose $\sigma(v) = au + bv$ for some $a, b \in K$. Then we have

$$0 = (u, v) = (\sigma(u), \sigma(v)) = (u, au + bv) = a(u, u),$$

whence $a = 0$. Thus $\sigma(v) = bv$ and the computation $(v, v) = (\sigma(v), \sigma(v)) = b^2(v, v)$ shows that $b^2 = 1$. If $b = 1$, then $\sigma(u) = u$, $\sigma(v) = v$, hence $\sigma = 1_V$ and this is the product of two symmetries (in fact, a square $\sigma_w \circ \sigma_w$ of any symmetry σ_w). If $b = -1$, then $\sigma(u) = u$, $\sigma(v) = -v$, hence $\sigma = \sigma_v$ is a symmetry.

II. $\sigma(u) \neq u$.

The vector $\sigma(u) - u \neq 0$ is anisotropic and orthogonal to $\sigma(u) + u$, as a simple calculation shows. Hence we have

$$\begin{aligned}\sigma_{\sigma(u)-u}(\sigma(u)) &= \sigma_{\sigma(u)-u}\left(\frac{1}{2}(\sigma(u) - u) + \frac{1}{2}(\sigma(u) + u)\right) \\ &= -\frac{1}{2}(\sigma(u) - u) + \frac{1}{2}(\sigma(u) + u) \\ &= u.\end{aligned}$$

Thus the isometry $\sigma_{\sigma(u)-u} \circ \sigma$ leaves the vector u fixed, and so the case I applies and gives

$$\sigma_{\sigma(u)-u} \circ \sigma = 1_V \quad \text{or} \quad \sigma_v.$$

So we get $\sigma = \sigma_{\sigma(u)-u}$ or $\sigma = \sigma_{\sigma(u)-u} \circ \sigma_v$, which proves our claim.

TWIERDZENIE 4.8.2. *Let V be a nonsingular symmetric space over a field K of characteristic $\neq 2$. Then the orthogonal group $O(V)$ is generated by the set of all symmetries σ_v with respect to anisotropic vectors $v \in V$.*

Dowód. We will induct on $n = \dim V$. The case when $n = 1$ has been considered in Example 4.8.2, so we can assume that $n \geq 2$. Let σ be an arbitrary isometry of the space V . We choose an orthogonal basis $\{v_1, \dots, v_n\}$ for V , each v_i being anisotropic by nonsingularity of V . Consider the vectors $\sigma(v_1)$ and v_1 . They have equal norms and are anisotropic, hence by Witt's prolongation theorem 4.6.1, there is an isometry $\tau \in O(V)$ taking $\sigma(v_1)$ to v_1 , i.e.,

$$\tau(\sigma(v_1)) = v_1.$$

We know also from Corollary 4.6.1 that τ can be chosen to be either a symmetry or the product of two symmetries, and this fact will be used later in the proof. Now consider the isometry $\tau \circ \sigma$. It leaves v_1 fixed, hence it also leaves fixed the orthogonal complement of Kv_1 :

$$(\tau \circ \sigma)((Kv_1)^\perp) = (Kv_1)^\perp.$$

The space $U := (Kv_1)^\perp$ has dimension $n - 1$ and the restriction $(\tau \circ \sigma)|_U$ is an isometry of U . Hence, by induction hypothesis, there are symmetries $\sigma_{u_1}, \dots, \sigma_{u_r} \in O(U)$ such that

$$(\tau \circ \sigma)|_U = \sigma_{u_1} \circ \dots \circ \sigma_{u_r}. \tag{4.4}$$

By the orthogonal complement theorem 2.5.1,

$$V = Kv_1 \oplus U,$$

and this allows us to extend the symmetries σ_{u_k} of U to the symmetries of V by setting

$$\sigma_{u_k}(v_1) = v_1, \quad k = 1, \dots, r,$$

and extending by linearity to the whole space V .

Now the product $\sigma_{u_1} \circ \dots \circ \sigma_{u_r}$ of symmetries of V agrees with $\tau \circ \sigma$ not only on U but also on the complementary direct summand Kv_1 , and so the two agree on the whole space V . Thus from (4.4) we get

$$\tau \circ \sigma = \sigma_{u_1} \circ \dots \circ \sigma_{u_r},$$

an equality in the group $O(V)$. Recall that here τ is either a symmetry or a product of two symmetries. In the first case, if $\tau = \sigma_v$, say, we get

$$\sigma = \sigma_v \circ \sigma_{u_1} \circ \cdots \circ \sigma_{u_r},$$

a product of $r + 1$ symmetries, and in the second case, when $\tau = \sigma_w \circ \sigma_v$, we get

$$\sigma = \sigma_v \circ \sigma_w \circ \sigma_{u_1} \circ \cdots \circ \sigma_{u_r},$$

a product of $r + 2$ symmetries of the space V . This proves that the group $O(V)$ is generated by symmetries. $\square$

Uwaga 4.8.1. From the above proof and from our earlier results in Theorem 4.7.2 and Example 4.8.3 it is easy to obtain a stronger result saying that if $\dim V = n > 1$, then every isometry $\sigma \in O(V)$ can be written as the product of at most $2n - 2$ symmetries. We propose this as an exercise for the reader. However, it turns out that this is not the strongest statement possible. One can prove that if $\dim V = n > 1$, then every isometry $\sigma \in O(V)$ is the product of at most n symmetries. Our computation of the orthogonal group of hyperbolic plane in Theorem 4.7.2 and the result in Example 4.8.3 confirm this stronger result when $n = 2$. On the other hand, there are isometries in $O(V)$ which are not the products of less than n symmetries, an explicit example being -1_V . This improved version of the theorem on generation of the orthogonal group by symmetries is known as the Cartan-Dieudonné's theorem. Its proof can be found in more advanced texts (see E. Artin [1], Theorem 3.20, T. Y. Lam [2], p. 27, or O. T. O'Meara [3], 43:12a).

Uwaga 4.8.2. W szczególnie interesującym nas przypadku grupy ortogonalnej przestrzeni euklidesowej tę dokładniejszą wersję twierdzenia o generowaniu grupy ortogonalnej przez symetrie można uzyskać bez jakiegokolwiek dodatkowego wysiłku. Jeśli u jest niezerowym wektorem przestrzeni euklidesowej V , to na podstawie twierdzenia 2.5.1 mamy rozkład

$$V = \text{lin}\{u\} \oplus \text{lin}\{u\}^\perp$$

i możemy rozpatrzyć symetrię σ_u przestrzeni V , która działa następująco:

$$\sigma_u(u) = -u, \quad \sigma_u(w) = w \quad \text{dla każdego } w \in \text{lin}\{u\}^\perp.$$

Bardzo łatwo otrzymujemy następujący odpowiednik twierdzenia 4.6.1 o przedłużaniu izometrii.

TWIERDZENIE 4.8.3. *Dla każdej pary różnych wektorów u i w w przestrzeni euklidesowej V takich, że $\|u\| = \|w\|$ istnieje symetria przestrzeni V przeprowadzająca u na w .*

Dowód. Wobec $\|u\| = \|w\|$ mamy $(u, u) = (w, w)$ i stąd $(u - w, u + w) = (u, u) + (u, w) + (-w, u) + (-w, w) = 0$. Wobec tego

$$\sigma_{u-w}(u) = \sigma_{u-w}\left(\frac{1}{2}(u - w) + \frac{1}{2}(u + w)\right) = -\frac{1}{2}(u - w) + \frac{1}{2}(u + w) = w.$$

$\square$

Teraz łatwo otrzymujemy

TWIERDZENIE 4.8.4. *Grupa ortogonalna $O(V)$ przestrzeni euklidesowej V jest generowana przez symetrie. Dokładniej, jeśli $n = \dim V > 1$, to każda izometria przestrzeni euklidesowej V jest iloczynem co najwyżej n symetrii.*

Dowód. Postępujemy jak w dowodzie twierdzenia 4.8.2 z tym, że teraz sytuacja jest prostsza, gdyż na podstawie twierdzenia 4.8.3 wektory o równych normach można przeprowadzić na siebie przez jedną symetrię a nie przez jedną lub iloczyn dwóch symetrii, jak to mieliśmy w dowodzie twierdzenia 4.8.2. Stąd też wynika dokładniejsza wersja twierdzenia 4.8.4. $\square$

We end this section with a discussion of commutativity questions in orthogonal groups. It will become clear that orthogonal groups are highly noncommutative. The only exception is the rotation group $O^+(V)$ of a plane V and we discuss this first. We assume that the characteristic of the ground field K is not 2. Then every nonsingular symmetric space V of dimension 2 over K is either anisotropic or else hyperbolic. This is not quite trivial observation since it amounts to saying that every isotropic plane is hyperbolic, and this holds only when $\text{char } K \neq 2$. We postpone the discussion of these matters to the next chapter and will assume here that nonsingular planes are either anisotropic or hyperbolic. With this assumption Theorem 4.7.2 and Example 4.8.3 cover all nonsingular planes and yield the following result.

WNIOSEK 4.8.1. *Let V be a nonsingular symmetric plane over a field of characteristic $\neq 2$. Then every rotation in the orthogonal group $O(V)$ is the product of two symmetries, and every reflection in $O(V)$ is a symmetry.*

Dowód. Every isometry in $O(V)$ is either a symmetry or the product of two symmetries. Every symmetry is a reflection and every product of two symmetries is a rotation. Hence the result follows. $\square$

Now we can prove commutativity of the rotation group of a plane.

TWIERDZENIE 4.8.5. *Let V be a nonsingular symmetric plane over a field of characteristic $\neq 2$. Then the rotation group $O^+(V)$ is an Abelian group.*

Dowód. Let ρ be a rotation in $O^+(V)$ and let σ be a symmetry in $O(V)$. Then $\sigma_1 := \sigma \circ \rho$ is a reflection (its determinant is -1), hence a symmetry, by Corollary 4.8.1. But the square of a symmetry in the orthogonal group $O(V)$ is equal to the identity map 1_V , hence $\sigma \circ \rho \circ \sigma \circ \rho = 1_V$, and so

$$\sigma \circ \rho \circ \sigma = \rho^{-1} \tag{4.5}$$

for all rotations ρ and all symmetries σ .

Now we will prove the commutativity of the group $O^+(V)$. So let ρ and ρ_1 be two rotations and let σ be an arbitrary symmetry. Then $\sigma_1 := \sigma \circ \rho$ is a symmetry, and we also have $\rho = \sigma \circ \sigma_1$. This will now be used in computing the commutator of ρ and ρ_1 :

$$\begin{aligned} \rho \circ \rho_1 \circ \rho^{-1} \circ \rho_1^{-1} &= \sigma \circ (\sigma_1 \circ \rho_1 \circ \sigma_1) \circ \sigma \circ \rho_1^{-1} \\ &= (\sigma \circ \rho_1^{-1} \circ \sigma) \circ \rho_1^{-1} \\ &= (\rho_1^{-1})^{-1} \circ \rho_1^{-1} = 1_V, \end{aligned}$$

where we have used twice the relation (4.5) to substitute for the expressions in parentheses. Thus $\rho \circ \rho_1 = \rho_1 \circ \rho$, as required. $\square$

Uwaga 4.8.3. The rotation group $O^+(V)$ for spaces V of dimension ≥ 3 is always non-Abelian (see O. T. O'Meara [3], 43:12b). The orthogonal group $O(V)$ is Abelian only in the two cases: when $\dim V = 1$, and when V is a hyperbolic plane over the field $\mathbb{F}_3$ (see O. T. O'Meara [3], 43:12a).

Finally, we determine the center of the orthogonal group of an anisotropic space.

Twierdzenie 4.8.6. *If V is an anisotropic symmetric space over a field of characteristic $\neq 2$, then*

$$Z(O(V)) = \{1_V, -1_V\}.$$

Dowód. Let $\sigma \in Z(O(V))$. To show that $\sigma = \pm 1_V$ it is sufficient to prove that σ leaves every line of V fixed (see Theorem 4.7.4). So let $0 \neq v \in V$. In the anisotropic space V the vector v is anisotropic, hence we can form the symmetry σ_v . Since σ is in the center of the orthogonal group, we have $\sigma \circ \sigma_v = \sigma_v \circ \sigma$, hence also

$$\sigma \circ \sigma_v \circ \sigma^{-1} = \sigma_v.$$

On the other hand, it is easy to check that for every isometry σ ,

$$\sigma \circ \sigma_v \circ \sigma^{-1} = \sigma_{\sigma(v)}.$$

Thus if $\sigma \in Z(O(V))$, then $\sigma_v = \sigma_{\sigma(v)}$ for each nonzero vector $v \in V$. Equal symmetries have the same hyperplanes of fixed vectors, hence the same anisotropic lines, where they reverse vectors. Hence $Kv = K\sigma(v)$ for all $v \in V$, and since $K\sigma(v) = \sigma(Kv)$, we get $\sigma(Kv) = Kv$ for all $v \in V$. Thus the symmetry σ in the center of the group $O(V)$ leaves every line in V fixed, hence $\sigma = 1_V$ or $\sigma = -1_V$, by Theorem 4.7.4. $\square$

Uwaga 4.8.4. We have determined the center of the orthogonal group for an *anisotropic* space V but the same result holds for every nonsingular symmetric space over a field of characteristic $\neq 2$ with the exception of hyperbolic plane over the field $\mathbb{F}_3$ (see O. T. O'Meara [3], 43:12). As to the rotation subgroup $O^+(V)$, it is non-Abelian in dimensions ≥ 3 . Its center is then trivial, that is, contains only 1_V , or is equal to $\{1_V, -1_V\}$, if -1_V is a rotation (see O. T. O'Meara [3], 43:13a).

Uwaga 4.8.5. There is an extensive literature about the structure of orthogonal groups. We cite only one important classical result. If V is a Euclidean space of odd dimension $n \geq 3$, then the rotation group $O^+(V)$ is *simple*, that is, it does not contain proper normal subgroups. If the dimension is an even number ≥ 6 , then the factor group $O^+(V)/\{1_V, -1_V\}$ is a simple group (see E. Artin [1], Theorem 5.3).

Literatura cytowana

- [1] E. Artin. *Geometric Algebra*. Interscience, New York, 1957.
- [2] T. Y. Lam. *The Algebraic Theory of Quadratic Forms*. W. A. Benjamin, Addison-Wesley, Reading, Mass., 1973. Second printing with revisions, 1980.
- [3] O. T. O'Meara. *Introduction to Quadratic Forms*, volume 117 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, Berlin Göttingen Heidelberg, second, corrected edition, 1971.

Rozdział 5

Funkcjonały półtoraliniowe

Ostatnie zmiany 22.04.2009 r.

Pojęcie długości wektora wprowadziliśmy jak dotąd jedynie dla wektorów przestrzeni euklidesowych. Formuła definiująca długość wektora $\|v\| = \sqrt{(v, v)}$ istotnie wykorzystuje dodatnią określoność iloczynu skalarnego $(\cdot, \cdot)$. Okazuje się, że istnieje analogon pojęcia przestrzeni euklidesowej, w którym ciałem podstawowym jest ciało $\mathbb{C}$ liczb zespolonych a funkcyjonał dwuliniowy jest zastąpiony ogólniejszym typem funkcyjonału zwanym *półtoraliniowym*. W tej nowej sytuacji można otrzymać odpowiedniki dość znacznej części teorii przestrzeni euklidesowych poprzez użycie dokładnie tych samych technik, które znamy już z teorii przestrzeni euklidesowych.

W tym rozdziale rozpatrujemy funkcyjonały półtoraliniowe i przestrzenie hermitowskie jako odpowiedniki funkcyjonałów dwuliniowych i symetrycznych przestrzeni dwuliniowych. W następnym rozdziale omawiamy przestrzenie unitarne jako odpowiednik przestrzeni euklidesowych i w końcu w rozdziale 7 dyskutujemy endomorfizmy przestrzeni unitarnych w zakresie podobnym do przedstawionych w rozdziale 4 własności endomorfizmów przestrzeni euklidesowych.

5.1 Przestrzenie hermitowskie

Każda liczba zespolona ma jednoznaczne przedstawienie w postaci $r + si$, gdzie $r, s \in \mathbb{R}$. Ciało $\mathbb{C}$ ma automorfizm $\sigma : \mathbb{C} \rightarrow \mathbb{C}$ taki, że $\sigma(r + si) = r - si$. Dla $a \in \mathbb{C}$ będziemy na ogół pisać $\bar{a}$ zamiast $\sigma(a)$. Zauważmy, że $\bar{\bar{a}} = a$ dla każdego $a \in \mathbb{C}$. Zauważmy też, że jeśli dla $a \in \mathbb{C}$ mamy $a = \bar{a}$, to $a \in \mathbb{R}$.

Niech V będzie przestrzenią wektorową nad ciałem $\mathbb{C}$. Funkcyjonałem *półtoraliniowym* na przestrzeni V nazywamy odwzorowanie

$$\beta : V \times V \rightarrow \mathbb{C}$$

które jest liniowe ze względu na pierwszą zmienną i półliniowe ze względu na drugą zmienną. Oznacza to, że β spełnia warunki

$$\beta(au + bv, w) = a\beta(u, w) + b\beta(v, w),$$

$$\beta(u, av + bw) = \bar{a}\beta(u, v) + \bar{b}\beta(u, w),$$

dla wszystkich $u, v, w \in V$ i wszystkich $a, b \in \mathbb{C}$.

W przypadku funkcyjonałów dwuliniowych rozpatrywaliśmy wyłącznie *symetryczne* funkcyjonały dwuliniowe. Dla funkcyjonałów półtoraliniowych symetria nie jest możliwa,

gdyż wymuszałyby ona liniowość funkcjonału ze względu na drugą zmienną. Natomiast współgra z półtoraliniowością następujący warunek *hermitowskiej symetrii*:

$$\beta(u, v) = \overline{\beta(v, u)} \quad \text{dla wszystkich } u, v \in V.$$

DEFINICJA 5.1.1. Funkcjonał półtoraliniowy spełniający warunek hermitowskiej symetrii nazywamy *hermitowskim*. Skończenie wymiarowa przestrzeń wektorowa V nad $\mathbb{C}$ z określonym na niej funkcjonałem hermitowskim nazywa się *przestrzenią hermitowską*.

W przestrzeni hermitowskiej możemy już wprowadzić pojęcie prostopadłości (ortogonalności) wektorów u, v poprzez warunek $\beta(u, v) = 0$. Ze względu na hermitowską symetrię funkcjonału hermitowskiego relacja ortogonalności wektorów jest symetryczna:

$$\beta(u, v) = 0 \iff \overline{\beta(u, v)} = 0 \iff \beta(v, u) = 0.$$

Tak jak w przestrzeniach dwuliniowych, dla dowolnego wektora $v \in V$ wprowadzamy oznaczenie $q(v) := \beta(v, v)$. Określona w ten sposób funkcja

$$q : V \rightarrow \mathbb{C}$$

ma następujące własności:

$$q(av) = |a|^2 q(v), \quad q(u + v) - q(u) - q(v) = \beta(u, v) + \beta(v, u)$$

dla dowolnych $a \in \mathbb{C}, u, v \in V$. Funkcję q nazywamy funkcjonałem *kwadratowym* stowarzyszonym z funkcjonałem półtoraliniowym β . Zauważmy, że z warunku hermitowskiej symetrii otrzymujemy $\beta(v, v) = \overline{\beta(v, v)}$, zatem dla każdego wektora $v \in V$ wartość funkcjonału kwadratowego $q(v) = \beta(v, v)$ jest liczbą rzeczywistą. A więc q jest funkcją

$$q : V \rightarrow \mathbb{R}, \quad q(v) = (v, v).$$

Wektor niezerowy $v \in V$ nazywa się *izotropowy*, jeśli $q(v) = \beta(v, v) = 0$. Podobnie jak w przestrzeniach dwuliniowych wprowadzamy pojęcia przestrzeni izotropowej i nieizotropowej.

Jeśli $\mathcal{B} = \{v_1, \dots, v_n\}$ jest bazą przestrzeni hermitowskiej V , to macierz

$$A := [\beta(v_i, v_j)]$$

nazywamy macierzą przestrzeni hermitowskiej V względem bazy $\mathcal{B}$. Piszemy wtedy

$$V \cong A \quad \text{w bazie } \mathcal{B}.$$

Oznaczmy $a_{ij} := \beta(v_i, v_j)$. Wtedy

$$a_{ij} = \beta(v_i, v_j) = \overline{\beta(v_j, v_i)} = \overline{a_{ji}}.$$

Tak więc $A = \overline{A^T}$, gdzie dla macierzy $Q = [q_{ij}] \in M_n(\mathbb{C})$ symbolem $\overline{Q}$ oznaczamy macierz sprzężoną z Q , to znaczy $\overline{Q} = [\overline{q_{ij}}]$. Macierz A o własności $A = \overline{A^T}$ nazywamy macierzą hermitowską. Macierz przestrzeni hermitowskiej względem dowolnej bazy tej przestrzeni jest więc macierzą hermitowską.

Dla $u, v \in V$, gdzie $u = \sum_i x_i v_i$, $v = \sum_j y_j v_j$, mamy

$$\beta(u, v) = \sum_i \sum_j a_{ij} x_i \overline{y_j} \tag{5.1}$$

oraz

$$q(u) = \beta(u, u) = \sum_i \sum_j a_{ij} x_i \overline{x_j}.$$

Macierz $[a_{ij}]$ przestrzeni hermitowskiej V względem dowolnej bazy tej przestrzeni wyznacza zatem w zupełności zarówno funkcjonał hermitowski β jak również stowarzyszony z nim funkcjonał kwadratowy q .

Przykład 5.1.1. Rozpatrzmy sygnalizowany już w rozdziale 2 przykład standardowej przestrzeni hermitowskiej (przykład 2.1.4). Niech V będzie przestrzenią współrzędnych $\mathbb{C}^n$ nad ciałem liczb zespolonych $\mathbb{C}$ z funkcjonałem

$$\chi : \mathbb{C}^n \times \mathbb{C}^n \rightarrow \mathbb{C},$$

$$\chi((x_1, \dots, x_n), (y_1, \dots, y_n)) = x_1 \bar{y}_1 + \dots + x_n \bar{y}_n.$$

Łatwo sprawdzić, że χ jest funkcjonałem hermitowskim. Dla $v = (x_1, \dots, x_n)$ wartość funkcjonału kwadratowego $q(v) = |x_1|^2 + \dots + |x_n|^2$ jest *nieujemną* liczbą rzeczywistą i $q(v) > 0$ dla $v \neq 0$. W związku z tym przestrzeń ta jest nieizotropowa. Macierzą funkcjonału χ w bazie standardowej jest macierz jednostkowa.

Przykład 5.1.2. Jeśli $A \in M_n(\mathbb{R})$ jest macierzą *symetryczną*, to A traktowana jako macierz nad ciałem $\mathbb{C}$ jest oczywiście macierzą hermitowską i wobec tego wyznacza na n -wymiarowej przestrzeni wektorowej V nad ciałem $\mathbb{C}$ funkcjonał hermitowski zadany formułą (5.1). Zatem każda symetryczna przestrzeń dwuliniowa nad ciałem $\mathbb{R}$ wyznacza przestrzeń hermitowską nad ciałem $\mathbb{C}$.

Dla przestrzeni hermitowskich istnieją odpowiedniki wszystkich twierdzeń rozdziału 2 o przestrzeniach dwuliniowych. Sformułujemy je tutaj w tej samej kolejności pomijając przeważnie dowody, które otrzymujemy z dowodów odpowiednich twierdzeń o przestrzeniach dwuliniowych poprzez nieznaczne modyfikacje.

5.2 Przestrzenie hermitowskie i kongruencja macierzy

DEFINICJA 5.2.1. Macierze $A, C \in M_n(\mathbb{C})$ nazywamy *hermitowsko kongruentnymi*, jeśli istnieje macierz nieosobliwa $P \in M_n(\mathbb{C})$ taka, że $C = P A \bar{P}^t$. Piszemy wtedy $A \cong^h C$.

TWIERDZENIE 5.2.1. Niech V będzie przestrzenią hermitowską i niech $\mathcal{B}$ oraz $\mathcal{B}'$ będą bazami przestrzeni V . Jeśli

$$V \cong A \text{ w bazie } \mathcal{B} \text{ oraz } V \cong C \text{ w bazie } \mathcal{B}',$$

to A i C są macierzami hermitowsko kongruentnymi: $A \cong^h C$. Dokładniej, jeśli P jest macierzą przejścia od bazy $\mathcal{B}$ do bazy $\mathcal{B}'$, to

$$C = P A \bar{P}^t.$$

Zauważmy, że $C = P A \bar{P}^t$ pociąga

$$\det C = \det A \cdot \det P \cdot \det \bar{P}^t = \det A \cdot \det P \cdot \overline{\det P} = \det A \cdot |\det P|^2.$$

5.3 Izometrie przestrzeni hermitowskich

DEFINICJA 5.3.1. Niech (U, α) i (V, β) będą przestrzeniami hermitowskimi. Izomorfizm $h : U \rightarrow V$ przestrzeni wektorowych U i V nazywamy *izometrią* przestrzeni hermitowskich (U, α) i (V, β) jeśli zachowuje on funkcjonały hermitowskie α i β , to znaczy, jeśli

$$\alpha(u, w) = \beta(h(u), h(w)) \text{ dla wszystkich } u, w \in U.$$

Jeśli istnieje izometria przestrzeni hermitowskich (U, α) i (V, β) , to przestrzenie te nazywamy *izometrycznymi* i piszemy $(U, \alpha) \cong (V, \beta)$.

Zauważmy, że izometria h zachowuje ortogonalność wektorów a także funkcjonały kwadratowe stowarzyszone z funkcjonałami hermitowskimi α i β . Rzeczywiście, dla każdego $u \in U$ mamy

$$q_\alpha(u) = \alpha(u, u) = \beta(h(u), h(u)) = q_\beta(h(u)).$$

TWIERDZENIE 5.3.1. *Niech (U, α) i (V, β) będą przestrzeniami hermitowskimi. Załóżmy, że A i B są macierzami (U, α) i (V, β) względem jakichkolwiek baz przestrzeni U i V :*

$$(U, \alpha) \cong A \quad \text{ i } \quad (V, \beta) \cong B.$$

Wtedy

$$(U, \alpha) \cong (V, \beta) \quad \Leftrightarrow \quad A \cong^h B.$$

5.4 Nieosobliwość przestrzeni hermitowskich

Dla uproszczenia oznaczeń zamiast $\beta(u, v)$ będziemy pisać po prostu (u, v) . Tak jak w przypadku przestrzeni dwuliniowych definiujemy radykał $\text{rad } V$ przestrzeni hermitowskiej jako zbiór wszystkich wektorów ortogonalnych do całej przestrzeni:

$$\text{rad } V = \{v \in V : (v, w) = 0 \quad \forall w \in V\}.$$

Z liniowości funkcjonału hermitowskiego względem pierwszej zmiennej wynika natychmiast, że $\text{rad } V$ jest podprzestrzenią przestrzeni wektorowej V .

DEFINICJA 5.4.1. Niech S będzie podprzestrzenią przestrzeni hermitowskiej V . Zbiór

$$S^\perp := \{v \in V : (v, w) = 0 \quad \text{dla wszystkich } w \in S\}$$

nazywamy *ortogonalnym dopełnieniem* podprzestrzeni S .

Uwaga 5.4.1. $V^\perp = \text{rad } V$ oraz $0^\perp = V$. Ponadto, $S^\perp$ jest podprzestrzenią przestrzeni V . Rzeczywiście, jeśli $u, v \in S^\perp$ oraz $x, y \in \mathbb{C}$, to, wykorzystując liniowość funkcjonału hermitowskiego względem pierwszej zmiennej, dla każdego wektora $w \in S$ mamy

$$(xu + yv, w) = x(u, w) + y(v, w) = 0,$$

i wobec tego $xu + yv \in S^\perp$.

Zauważmy jeszcze, że jeśli S jest podprzestrzenią właściwą, to $S^\perp \neq 0$. Rzeczywiście, niech $v_1, \dots, v_k$ będzie bazą S i niech $v_1, \dots, v_k, v_{k+1}, \dots, v_n$ będzie bazą V . Mamy

$$\begin{aligned} v = \sum_{i=1}^n x_i v_i \in S^\perp &\iff (v, v_1) = \dots = (v, v_k) = 0 \\ &\iff x_1(v_1, v_j) + \dots + x_n(v_n, v_j) = 0 \quad \text{dla } j = 1, \dots, k. \end{aligned}$$

A więc wektor v należy do $S^\perp$ wtedy i tylko wtedy gdy jego współrzędne spełniają układ k równań liniowych jednorodnych o n niewiadomych. Ponieważ $k < n$, taki układ ma rozwiązanie niezerowe.

Przestrzeń hermitowską nazywamy *nieosobliwą* jeśli jej radykał jest zerowy. Podobnie jak w przypadku przestrzeni dwuliniowych dowodzimy, że *przestrzeń hermitowska jest nieosobliwa wtedy i tylko wtedy gdy wyznacznik macierzy tej przestrzeni względem dowolnej bazy jest różny od zera*.

Rzeczywiście, jeśli $v_1, \dots, v_n$ tworzą bazę V , to wektor $v = x_1v_1 + \dots + x_nv_n \in V$ należy do radykału przestrzeni V wtedy i tylko wtedy gdy

$$x_1(v_1, v_k) + \dots + x_n(v_n, v_k) = 0 \quad \text{dla } k = 1, \dots, n,$$

to znaczy wtedy i tylko wtedy gdy współrzędne wektora v spełniają układ równań liniowych jednorodnych, którego macierzą współczynników przy niewiadomych jest macierz $[(v_i, v_k)]$ przestrzeni hermitowskiej V w pewnej bazie tej przestrzeni. Przestrzeń V jest więc nieosobliwa wtedy i tylko wtedy gdy ten układ równań ma tylko rozwiązanie zerowe a to ma miejsce tylko wtedy gdy $\det[(v_i, v_k)] \neq 0$.

Uwaga 5.4.2. *Każda nieizotropowa przestrzeń hermitowska jest nieosobliwa.* Rzeczywiście, jeśli V jest nieizotropowa i $v \in \text{rad } V$, to $(v, v) = 0$, skąd wobec nieizotropowości V otrzymujemy $v = 0$. Zatem $\text{rad } V = 0$ i przestrzeń jest nieosobliwa. W dalszym ciągu zajmować się będziemy przede wszystkim nieizotropowymi przestrzeniami hermitowskimi, które są, jak widzimy, nieosobliwe. Natomiast istnieją oczywiście izotropowe przestrzenie hermitowskie, które także są nieosobliwe. Na przykład, na podstawie przykładu 5.1.2 macierz

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

wyznacza przestrzeń hermitowską i jest to przestrzeń nieosobliwa, gdyż wyznacznik tej macierzy jest różny od zera, natomiast przestrzeń ta jest oczywiście izotropowa.

Przystępujemy teraz do interpretacji nieosobliwości przestrzeni hermitowskiej przy pomocy pojęcia przestrzeni dualnej do danej przestrzeni wektorowej,

$$V^* := \text{Hom}(V, \mathbb{C}).$$

Tak jak w przypadku przestrzeni dwuliniowej istnieje bardzo prosty sposób konstruowania funkcyjałów liniowych na przestrzeni hermitowskiej V . Ustalamy wektor $v \in V$ i wiążemy z nim odwzorowanie

$$\lambda_v : V \rightarrow \mathbb{C}, \quad \lambda_v(x) = (x, v) \quad \text{dla } x \in V.$$

Z liniowości $(\ , \)$ względem pierwszej zmiennej wynika natychmiast, że λ_v jest funkcyjałem liniowym na V , a więc jest elementem przestrzeni dualnej V^* . Okazuje się, że dla *nieizotropowego* funkcyjału hermitowskiego $(\ , \)$ ta konstrukcja daje *wszystkie* funkcyjały liniowe na V . Dla ustalenia tego faktu rozpatrzmy odwzorowanie

$$\Lambda_V : V \rightarrow V^*, \quad \Lambda_V(v) = \lambda_v.$$

LEMAT 5.4.1. *Niech V będzie przestrzenią hermitowską. Wtedy*

(a) Λ_V *jest homomorfizmem grup addytywnych.*

(b) $\ker \Lambda_V = \text{rad } V$.

Dowód. (a) pozostawiamy jako łatwe ćwiczenie dla czytelnika. Zauważmy, że Λ_V nie jest homomorfizmem przestrzeni wektorowych, gdyż $\Lambda_V(av) = \bar{a}\Lambda_V(v)$. Rzeczywiście,

$$\lambda_{av}(x) = (x, av) = \bar{a}(x, v) = \bar{a}\lambda_v(x)$$

dla każdego $x \in V$.

(b) Wykorzystując jedynie definicje otrzymujemy

$$\begin{aligned} \ker \Lambda_V &= \{v \in V : \Lambda_V(v) = 0 \in V^*\} \\ &= \{v \in V : (x, v) = 0 \text{ dla wszystkich } x \in V\} \\ &= \text{rad } V. \end{aligned}$$

□

Twierdzenie 5.4.1. *Jeśli przestrzeń hermitowska V jest nieizotropowa, to homomorfizm Λ_V jest izomorfizmem addytywnych grup abelowych.*

Dowód. Jeśli przestrzeń V jest nieizotropowa, to $\text{rad } V = 0$ i na podstawie lematu 5.4.1 homomorfizm Λ_V jest iniektywny. Należy więc pokazać, że jeśli V jest nieizotropowa, to homomorfizm Λ_V jest suriektywny.

Weźmy dowolny funkcjonał liniowy $\mu \in V^*$. Udowodnimy, że istnieje $v \in V$ taki, że $\lambda_v = \Lambda_V(v) = \mu$, to znaczy,

$$\text{istnieje } v \in V \text{ taki, że } (x, v) = \lambda_v(x) = \mu(x) \text{ dla każdego } x \in V. \quad (5.2)$$

Możemy założyć, że $\mu \neq 0$, gdyż dla $\mu = 0$ można wziąć $v = 0$. Ponieważ $\mu \neq 0$, więc $\ker \mu \neq V$. Faktycznie, jeśli $\dim V = n$, to $\dim \ker \mu = n - 1$, gdyż $n = \dim \ker \mu + \dim \text{im } \mu$ oraz $\text{im } \mu = \mathbb{C}$. Wobec tego $(\ker \mu)^\perp \neq 0$ (na podstawie uwagi 5.4.1).

Jeśli $v \in \ker \mu \cap (\ker \mu)^\perp$, to $(v, v) = 0$, skąd wobec nieizotropowości V wynika, że $v = 0$. Zatem dla każdego niezerowego wektora $v_0 \in (\ker \mu)^\perp$ mamy

$$V = \ker \mu \oplus \mathbb{C}v_0.$$

Każdy wektor $v \in V$ możemy więc przedstawić jednoznacznie w postaci $v = u + cv_0$, gdzie $u \in \ker \mu$ oraz $c \in \mathbb{C}$. Jeśli wektor v spełnia (5.2), to w szczególności dla $x = u$ mamy

$$(u, u + cv_0) = \mu(u) = 0$$

skąd wynika, że $(u, u) + \bar{c}(u, v_0) = 0$, skąd wobec $(u, v_0) = 0$ wynika, że $(u, u) = 0$. Wobec nieizotropowości przestrzeni V oznacza to, że $u = 0$. A więc jeśli wektor $v = u + cv_0$ spełniający (5.2) istnieje, to $u = 0$, czyli $v = cv_0$ gdzie $c \in \mathbb{C}$ oraz $v_0 \in (\ker \mu)^\perp$.

Znajdziemy teraz warunek konieczny i wystarczający jaki spełniać musi liczba c aby wektor $v = cv_0$ spełniał (5.2). Niech x będzie dowolnym wektorem przestrzeni V . Wtedy mamy przedstawienie

$$x = w + dv_0, \quad w \in \ker \mu, \quad d \in \mathbb{C}.$$

Warunek (5.2) jest spełniony przez wektor $v = cv_0$ wtedy i tylko wtedy gdy dla każdego $w \in \ker \mu$, $d \in \mathbb{C}$ zachodzi

$$d\bar{c}(v_0, v_0) = (dv_0, cv_0) = (w + dv_0, cv_0) = (x, cv_0) = \mu(x) = \mu(w + dv_0) = \mu(dv_0) = d\mu(v_0),$$

a więc wtedy i tylko wtedy gdy

$$c = \frac{\overline{\mu(v_0)}}{(v_0, v_0)}.$$

Tak więc dla $v = \frac{\overline{\mu(v_0)}}{(v_0, v_0)}v_0$ mamy $\Lambda_V(v) = \mu$ i Λ_V jest odwzorowaniem suriektywnym. $\square$

WNIOSEK 5.4.1 (Twierdzenie Riesa o reprezentacji). *Jeśli V jest nieizotropową przestrzenią hermitowską, to dla każdego funkcjonatu liniowego $\mu : V \rightarrow \mathbb{C}$ istnieje dokładnie jeden wektor $v \in V$ taki, że*

$$\mu(x) = (x, v) \quad \text{dla każdego } x \in V.$$

5.5 Twierdzenie o rzucie prostopadłym

Tutaj można dosłownie przepisać definicje, twierdzenia i dowody, które przedstawiliśmy w przypadku przestrzeni dwuliniowych.

Uwaga 5.5.1. Dla podprzestrzeni S przestrzeni hermitowskiej V mamy

$$\begin{aligned} S \cap S^\perp &= \{v \in S : (v, x) = 0 \text{ dla wszystkich } x \in S\} \\ &= \text{rad } S. \end{aligned}$$

Stąd wynika, że podprzestrzeń S jest nieosobliwa wtedy i tylko wtedy gdy $S \cap S^\perp = 0$.

Twierdzenie 5.5.1. (Twierdzenie o rzucie prostopadłym.) *Jeśli S jest nieizotropową podprzestrzenią przestrzeni hermitowskiej V , to*

$$V = S \oplus S^\perp.$$

Dowód. Na podstawie uwagi 5.5.1 nieizotropowość S pociąga $S \cap S^\perp = \text{rad } S = 0$, zatem $S + S^\perp = S \oplus S^\perp$. Pozostaje zatem udowodnić, że $V = S + S^\perp$.

Niech $v \in V$. Rozpatrzmy funkcjonal liniowy μ_v na podprzestrzeni S określony następująco:

$$\mu_v : S \rightarrow \mathbb{C}, \quad \mu_v(s) = (s, v).$$

Ponieważ S jest nieizotropową przestrzenią hermitowską, na podstawie twierdzenia 5.4.1 istnieje wektor $t \in S$ taki, że $\mu_v = \Lambda_S(t) = \lambda_t$, gdzie

$$\lambda_t : S \rightarrow \mathbb{C}, \quad \lambda_t(s) = (s, t).$$

Tak więc dla każdego $s \in S$ mamy

$$(s, v) = \mu_v(s) = \lambda_t(s) = (s, t),$$

skąd wynika, że $(s, v - t) = 0$ dla każdego $s \in S$. Oznacza to, że $v - t \in S^\perp$. Wobec tego dla każdego $v \in V$ mamy

$$v = t + (v - t), \quad t \in S, \quad v - t \in S^\perp,$$

skąd $V = S + S^\perp$. □

5.6 Bazy ortogonalne przestrzeni hermitowskich

Tak jak w przypadku przestrzeni dwuliniowych głównym zastosowaniem twierdzenia o rzucie prostopadłym jest twierdzenie o istnieniu baz prostopadłych w przestrzeniach hermitowskich. Dowód jest taki sam jak w przypadku dwuliniowym, a nawet prostszy, gdyż ciało podstawowe ma charakterystykę zero.

Twierdzenie 5.6.1. *Każda nieizotropowa przestrzeń hermitowska ma bazę ortogonalną. Ponadto, dla każdego wektora niezerowego $v \in V$ istnieje baza ortogonalna przestrzeni V zawierająca wektor v .*

Dowód. Weźmy dowolny wektor niezerowy $v \in V$. Jeśli przestrzeń ma wymiar 1, to wektor v tworzy bazę ortogonalną przestrzeni V . Załóżmy, że $\dim V = n > 1$ i twierdzenie jest prawdziwe dla przestrzeni o wymiarze mniejszym niż n . Rozpatrzmy 1-wymiarową podprzestrzeń $S := \mathbb{C}v$ rozpiętą na wektorze v . Ponieważ v jest nieizotropowy, podprzestrzeń S jest nieosobliwa. Zatem na podstawie twierdzenia 5.5.1 o rzucie prostopadłym mamy rozkład

$$V = S \oplus S^\perp.$$

Tutaj $\dim S^\perp < \dim V$ i wobec tego na podstawie założenia indukcyjnego $S^\perp$ ma bazę ortogonalną $\{v_2, \dots, v_n\}$. Wtedy $\{v, v_2, \dots, v_n\}$ jest bazą ortogonalną przestrzeni V . □

Także dla przestrzeni hermitowskich funkcjonuje metoda *ortogonalizacji Grama-Schmidta*. Następujące twierdzenie ma dokładnie taki sam dowód jak twierdzenie 2.6.2.

Twierdzenie 5.6.2. *Niech V będzie nieizotropową przestrzenią hermitowską. Niech $\mathcal{B} = \{v_1, \dots, v_k\}$ będzie zbiorem liniowo niezależnych wektorów przestrzeni V . Wtedy zbiór $\mathcal{B}' = \{u_1, \dots, u_k\}$ określony następująco:*

$$u_1 = v_1, \quad u_{\ell+1} = v_{\ell+1} + x_1 u_1 + \dots + x_\ell u_\ell \quad \text{gdzie} \quad x_i = -\frac{(v_{\ell+1}, u_i)}{(u_i, u_i)}$$

składa się z parami ortogonalnych wektorów oraz

$$\text{lin}\{\mathcal{B}\} = \text{lin}\{\mathcal{B}'\}.$$

W szczególności, jeśli $\mathcal{B}$ jest bazą przestrzeni V , to $\mathcal{B}'$ jest bazą ortogonalną przestrzeni V .

Rozdział 6

Przestrzenie unitarne

Ostatnie zmiany 22.04.2009 r.

DEFINICJA 6.0.1. Przestrzenią *unitarną* nazywamy skończenie wymiarową przestrzeń hermitowską V nad ciałem $\mathbb{C}$ liczb zespolonych z *dodatnio* określonym funkcjonałem hermitowskim

$$(\cdot, \cdot) : V \times V \rightarrow \mathbb{C}$$

zwanym *iloczynem skalarnym*.

Przypomnijmy, że z warunku hermitowskiej symetrii mamy $(v, v) = \overline{(v, v)}$ i wobec tego $(v, v) \in \mathbb{R}$. Funkcjonał półtoraliniowy na przestrzeni unitarnej obok warunku hermitowskiej symetrii spełnia jeszcze warunek *dodatniej określoności*, który oznacza, że

$$(v, v) > 0 \quad \text{dla każdego niezerowego wektora } v \in V.$$

A więc na przestrzeni unitarnej V funkcjonał kwadratowy $q : V \rightarrow \mathbb{R}$ przyjmuje tylko wartości nieujemne, przy czym $q(v) = 0$ tylko dla $v = 0$.

6.1 Norma wektora i odległość między wektorami

Warunek dodatniej określoności iloczynu skalarnego w przestrzeni unitarnej oznacza, że dla każdego wektora $v \in V$ wartość funkcjonału kwadratowego $q(v) = (v, v)$ jest kwadratem pewnej liczby rzeczywistej $d \in \mathbb{R}$:

$$(v, v) = d^2.$$

Z dwóch liczb d i $-d$ wybieramy tę, która jest nieujemna i nazywamy ją *długością* lub *normą* wektora v i oznaczamy $\|v\|$. Zatem

$$\|v\| = \sqrt{(v, v)} = \sqrt{q(v)} \quad \text{dla każdego wektora } v \in V.$$

Zauważmy, że dla dowolnej liczby zespolonej a i dowolnego wektora $v \in V$ mamy

$$\|av\| = \sqrt{(av, av)} = \sqrt{|a|^2(v, v)} = |a| \|v\|.$$

W szczególności, $\|-v\| = \|v\| = \|\pm iv\|$.

Z pojęciem długości wektora przestrzeni unitarnej V związane są następujące cztery twierdzenia, których dowody (wraz z interpretacją geometryczną tych twierdzeń) pozostawiamy jako ćwiczenia dla Czytelnika.

Twierdzenie Pitagorasa: Jeśli $u, v \in V$ są prostopadłe, to

$$\|u + v\|^2 = \|u\|^2 + \|v\|^2.$$

Twierdzenie o równoległoboku: Dla dowolnych $u, v \in V$,

$$\|u + v\|^2 + \|u - v\|^2 = 2(\|u\|^2 + \|v\|^2).$$

Nierówność Cauchy'ego-Schwarza: Dla dowolnych $u, v \in V$,

$$|(u, v)| \leq \|u\| \cdot \|v\|,$$

przy czym równość zachodzi tylko wtedy gdy wektory u, v są liniowo zależne.

Nierówność trójkąta: Dla dowolnych $u, v \in V$,

$$\|u + v\| \leq \|u\| + \|v\|,$$

przy czym równość zachodzi tylko wtedy gdy wektory u, v są liniowo zależne, $(u, v) \in \mathbb{R}$ oraz $(u, v) \geq 0$.

W przestrzeni unitarnej nie możemy wprowadzić (miary) kąta między wektorami tak jak zrobiliśmy to w przestrzeni euklidesowej gdyż $\frac{(u,v)}{\|u\| \cdot \|v\|}$ nie jest na ogół liczbą rzeczywistą. Możemy natomiast dokładnie tak jak w przestrzeni euklidesowej określić *odległość* $d(u, v)$ pomiędzy wektorami $u, v \in V$,

$$d(u, v) = \|u - v\|.$$

Tak określona funkcja $d : V \times V \rightarrow \mathbb{R}$ ma wszystkie własności wymagane od metryki przestrzeni metrycznej. Każda przestrzeń unitarna V jest więc przestrzenią metryczną z metryką d .

Ważną konsekwencją dodatniej określoności iloczynu skalarnego w przestrzeni unitarnej jest następujący fakt.

TWIERDZENIE 6.1.1. *Każda przestrzeń unitarna jest nieizotropową, zatem także nieosobliwą, przestrzenią hermitowską.*

Dowód. Warunek dodatniej określoności iloczynu skalarnego pociąga oczywiście nieizotropowość przestrzeni unitarnej. Stąd też wynika nieosobliwość przestrzeni unitarnej (zobacz uwagę 5.4.2). $\square$

Każda podprzestrzeń S przestrzeni unitarnej V jest oczywiście także przestrzenią unitarną i wobec tego jest nieosobliwa.

6.2 Bazy ortonormalne

Ponieważ dla niezerowego wektora $v \in V$ długość $d = \|v\|$ jest dodatnią liczbą rzeczywistą, więc $\left\|\frac{1}{d}v\right\| = \frac{1}{d}\|v\| = 1$. Przejście od wektora v do $\frac{1}{\|v\|}v$ nazywa się *normalizacją* wektora v . Wektor o długości 1 nazywa się *unormowany*. Baza $\{v_1, \dots, v_n\}$ przestrzeni unitarnej nazywa się bazą *ortonormalną* gdy jest to baza ortogonalna i długość każdego wektora tej bazy jest równa 1.

TWIERDZENIE 6.2.1. *Każda przestrzeń unitarna ma bazę ortonormalną.*

Dowód. Na podstawie twierdzeń 5.6.1, 5.6.2, przestrzeń unitarna ma bazę ortogonalną. Po znormalizowaniu każdego wektora takiej bazy otrzymujemy bazę ortonormalną. $\square$

Bazy ortonormalne prowadzą do istotnych uproszczeń rachunków w przestrzeniach unitarnych. Jeśli $\mathcal{E} = \{e_1, \dots, e_n\}$ jest bazą ortonormalną przestrzeni V oraz

$$u = x_1 e_1 + \dots + x_n e_n, \quad v = y_1 e_1 + \dots + y_n e_n$$

są dowolnymi wektorami tej przestrzeni, to z półtoraliniowości iloczynu skalarnego i ortonormalności bazy $\mathcal{E}$ otrzymujemy następujące, bardzo proste formuły dla iloczynu skalarnego wektorów u i v i dla normy wektora u :

$$(u, v) = x_1 \overline{y_1} + \dots + x_n \overline{y_n}, \quad \|u\|^2 = |x_1|^2 + \dots + |x_n|^2,$$

przy czym pierwszą z nich można także zapisać jako następującą *równość Parsevala*:

$$(u, v) = (u, e_1)(e_1, v) + \dots + (u, e_n)(e_n, v).$$

Jak to już zauważyliśmy, z twierdzenia 5.2.1 wynika, że jeśli A i C są macierzami tej samej przestrzeni hermitowskiej V względem baz $\mathcal{B} = \{v_1, \dots, v_n\}$ i $\mathcal{B}' = \{w_1, \dots, w_n\}$, to

$$\det C = |\det P|^2 \cdot \det A, \quad (6.1)$$

gdzie P jest macierzą przejścia od bazy $\mathcal{B}$ do bazy $\mathcal{B}'$. Jeśli V jest przestrzenią unitarną, to V ma bazę ortonormalną $\mathcal{B}$ i w tej bazie przestrzeń V ma macierz jednostkową $A = I = [(v_i, v_j)]$. Jeśli $\mathcal{B}'$ jest także bazą ortonormalną V , to także macierz $C = [(w_i, w_j)]$ jest macierzą jednostkową i wobec tego z równości (6.1) wynika, że dla macierzy przejścia P od bazy $\mathcal{B}$ do bazy $\mathcal{B}'$ mamy $|\det P|^2 = 1$. Następujące twierdzenie podaje znacznie dokładniejszy rezultat.

Twierdzenie 6.2.2. *Niech $\mathcal{B}$ będzie bazą ortonormalną przestrzeni unitarnej V i niech $\mathcal{B}'$ będzie bazą V . Niech P będzie macierzą przejścia od bazy ortonormalnej $\mathcal{B}$ do bazy $\mathcal{B}'$. Baza $\mathcal{B}'$ jest ortonormalna wtedy i tylko wtedy gdy P jest macierzą unitarną, to znaczy $P^{-1} = \overline{P}^T$.*

Dowód. Łatwa modyfikacja dowodu twierdzenia 3.2.1. $\square$

6.3 Przykłady

Przykład 6.3.1. W przykładzie 2.1.4 rozpatrywaliśmy przestrzeń współrzędnych $\mathbb{C}^n$ z funkcjonalem półtoraliniowym

$$(\cdot, \cdot) : \mathbb{C}^n \times \mathbb{C}^n \rightarrow \mathbb{C},$$

$$((x_1, \dots, x_n), (y_1, \dots, y_n)) = x_1 \overline{y_1} + \dots + x_n \overline{y_n}.$$

Jest to n -wymiarowa przestrzeń unitarna, którą nazywamy *standardową* przestrzenią unitarną. W bazie $\{e_1, \dots, e_n\}$ złożonej z wektorów jednostkowych przestrzeń ta ma macierz jednostkową. Jeśli V jest jakąkolwiek n -wymiarową przestrzenią unitarną, to V ma bazę ortonormalną $\mathcal{B}$ i w tej bazie V ma macierz jednostkową. Tak więc V i $\mathbb{C}^n$ mają identyczne macierze w odpowiednich bazach i wobec tego, na podstawie twierdzenia 5.3.1 są izometryczne. A więc, *każda n -wymiarowa przestrzeń unitarna jest izometryczna ze standardową n -wymiarową przestrzenią unitarną $\mathbb{C}^n$.*

Także przykłady nieskończenie wymiarowych przestrzeni rzeczywistych z dodatnio określonymi funkcjonalami dwuliniowymi rozpatrywane w przykładzie 3.3.2 mają swoje odpowiedniki hermitowskie.

Przykład 6.3.2. Niech $V = C[a, b]$ będzie przestrzenią wszystkich funkcji ciągłych $f : [a, b] \rightarrow \mathbb{C}$ określonych na przedziale domkniętym $[a, b] \subset \mathbb{R}$. Jest to nieskończenie wymiarowa przestrzeń wektorowa nad ciałem $\mathbb{C}$. Na przestrzeni tej określa się funkcjonal $(\cdot, \cdot) : V \times V \rightarrow \mathbb{C}$ wzorem

$$(f, g) = \int_a^b f(x) \overline{g(x)} dx.$$

Standardowe własności całki oznaczonej pokazują, że $(\cdot, \cdot)$ jest dodatnio określonym funkcjonalem hermitowskim. A więc przestrzeń zespolonych funkcji ciągłych na przedziale domkniętym ma wszystkie własności przestrzeni unitarnej z wyjątkiem skończoności wymiaru.

Również na przestrzeni $V = \ell^2$ wszystkich ciągów (a_i) liczb zespolonych spełniających warunek $\sum_{i=0}^{\infty} |a_i|^2 < \infty$ można określić dodatni funkcjonal hermitowski następująco:

$$((a_i), (b_i)) = \sum_{i=0}^{\infty} a_i \overline{b_i}.$$

Szereg po prawej stronie jest zbieżny gdyż

$$0 \leq (|a_i| - |b_i|)^2 = |a_i|^2 - 2|a_i||b_i| + |b_i|^2$$

i wobec tego $2|a_i b_i| \leq |a_i|^2 + |b_i|^2$ skąd otrzymujemy

$$2 \left| \sum_{i=0}^{\infty} a_i \overline{b_i} \right| \leq 2 \sum_{i=0}^{\infty} |a_i b_i| \leq \sum_{i=0}^{\infty} |a_i|^2 + \sum_{i=0}^{\infty} |b_i|^2 < \infty.$$

6.4 Dodatnio określone funkcjonały hermitowskie

Zauważona w przykładzie 6.3.1 izometria przestrzeni unitarnych ze standardowymi przestrzeniami unitarnymi pozwala zawęzić rozpatrywanie przestrzeni unitarnych do standardowych przestrzeni unitarnych $\mathbb{C}^n$. Podobnie jak w przypadku przestrzeni euklidesowych powstaje pytanie jak rozpoznać, czy przestrzeń hermitowska zadana poprzez swoją macierz względem pewnej bazy tej przestrzeni jest unitarna. Klasyczną odpowiedź w przypadku przestrzeni euklidesowych znamy już z twierdzenia Frobeniusa 3.3.2. Dokładnie ten sam argument rozstrzyga tę kwestię w przypadku przestrzeni unitarnych.

Twierdzenie 6.4.1. Niech V będzie n -wymiarową przestrzenią wektorową nad ciałem $\mathbb{C}$ i niech $A = [a_{ij}]$ będzie macierzą funkcjonala hermitowskiego $(\cdot, \cdot)$ na przestrzeni V w bazie $\mathcal{B} = \{v_1, \dots, v_n\}$ tej przestrzeni. Dla $k \leq n$, niech $A_k = [a_{ij}]_{1 \leq i, j \leq k}$ będzie macierzą funkcjonala $(\cdot, \cdot)$ zacieśnionego do podprzestrzeni $V_k = \text{lin}\{v_1, \dots, v_k\}$ w bazie $\mathcal{B}_k = \{v_1, \dots, v_k\}$. Przestrzeń V jest unitarna wtedy i tylko wtedy, gdy

$$\det A_k > 0 \quad \text{dla każdego } k = 1, 2, \dots, n.$$

Dowód. Jeśli przestrzeń V jest unitarna, to także wszystkie podprzestrzenie V_k są unitarne i wobec tego wystarczy pokazać, że wyznacznik macierzy dowolnej przestrzeni unitarnej w dowolnej bazie tej przestrzeni jest dodatnią liczbą rzeczywistą. Jak już zauważyliśmy, przestrzeń unitarna V ma bazę ortonormalną i jeśli P jest macierzą przejścia od bazy $\mathcal{B}$ do bazy ortonormalnej, to $I = PAP^T$ na podstawie twierdzenia 5.2.1. Zatem $1 = |\det P|^2 \cdot \det A$ skąd wynika, że $\det A$ jest liczbą rzeczywistą i $\det A > 0$.

Założmy teraz, że $\det A_k > 0$ dla każdego $k = 1, 2, \dots, n$. Jeśli $n = 1$, to $A = A_1$ i jedyny element macierzy A jest dodatnią liczbą rzeczywistą, skąd wynika, że funkcjonal hermitowski jest dodatnio określony i wobec tego V jest przestrzenią unitarną. Założmy teraz, że $n > 1$ i twierdzenie jest prawdziwe dla przestrzeni o wymiarze $n - 1$. Rozpatrzmy podprzestrzeń $V_{n-1} = \text{lin}\{v_1, \dots, v_{n-1}\}$ przestrzeni V . Na podstawie twierdzenia o rzucie prostopadłym mamy

$$V = V_{n-1} \oplus V_{n-1}^\perp.$$

Tutaj $\dim V_{n-1}^\perp = \dim V - \dim V_{n-1} = 1$ i wobec tego $V_{n-1}^\perp = \text{lin}\{w\}$ dla pewnego $w \in V$. Jeśli $(w, w) = a$, to wobec $w \in V_{n-1}^\perp$ mamy

$$V \cong A_{n-1} \oplus [a] \quad \text{w bazie} \quad \mathcal{B}_{n-1} \cup \{w\},$$

gdzie $A_{n-1} \oplus [a]$ oznacza macierz A_{n-1} z dołączoną jedną kolumną i jednym wierszem, których wszystkie elementy są równe 0 z wyjątkiem ostatniego równego a . Ponieważ jednak równocześnie mamy

$$V \cong A \quad \text{w bazie} \quad \mathcal{B},$$

więc jeśli Q jest macierzą przejścia od bazy $\mathcal{B}$ do bazy $\mathcal{B}_{n-1} \cup \{w\}$ przestrzeni V , to

$$A_{n-1} \oplus [a] = QA\overline{Q}^T.$$

Biorąc wyznaczniki po obu stronach otrzymujemy $a \det A_{n-1} = |\det Q|^2 \det A$ skąd wynika, że $a > 0$. Teraz już łatwo zauważyć, że funkcjonal hermitowski na V jest dodatnio określony. Każdy wektor $v \in V$ ma jednoznaczne przedstawienie w postaci $v = u + cw$, gdzie $u \in V_{n-1}$, $c \in \mathbb{C}$ oraz

$$q(v) = (v, v) = (u + cw, u + cw) = (u, u) + |c|^2(w, w) = q(u) + |c|^2a \geq 0,$$

gdyż V_{n-1} jest przestrzenią unitarną i wobec tego $q(u) \geq 0$ oraz $|c|^2a \geq 0$. Ponadto, jeśli $v \neq 0$, to $u \neq 0$ lub $c \neq 0$ i wobec tego $q(v) > 0$. $\square$

6.5 Najlepsza aproksymacja

Także twierdzenie 3.4.1 o najlepszej aproksymacji w przestrzeni euklidesowej ma swój odpowiednik w przestrzeniach unitarnych. Dowód jest taki sam jak w przypadku euklidesowym.

TWIERDZENIE 6.5.1. *Niech S będzie podprzestrzenią przestrzeni unitarnej V i niech $v \in V$. Jeśli $v = s + s^\perp$, gdzie $s \in S$ oraz $s^\perp \in S^\perp$, to*

$$\|v - s\| \leq \|v - t\| \quad \text{dla każdego wektora} \quad t \in S.$$

Wektor s jest więc najlepszym przybliżeniem wektora v w podprzestrzeni S .

Rozdział 7

Endomorfizmy przestrzeni unitarnych

Ostatnie zmiany 12.06.2009 r.

W tym rozdziale, równoległe do rezultatów rozdziału 4 o endomorfizmach przestrzeni euklidesowych, rozpatrujemy endomorfizmy przestrzeni unitarnych spełniające warunki wyrażone w języku iloczynu skalarnego. Będą to endomorfizmy samosprężone, normalne i unitarne (tak nazywa się izometrie przestrzeni unitarnych).

7.1 Endomorfizmy sprzężone

Zakładamy, że V jest przestrzenią *unitarną*. A więc na V jest zadany *dodatnio* określony funkcyjonał hermitowski

$$(\cdot, \cdot) : V \times V \rightarrow \mathbb{C},$$

który nazywamy *iloczynem skalarnym*. Będziemy interpretować nieosobliwość przestrzeni unitarnej V poprzez izomorfizm grup addytywnych przestrzeni V i przestrzeni dualnej V^* ,

$$\Lambda_V : V \rightarrow V^*, \quad \Lambda_V(v) = \lambda_v$$

gdzie $\lambda_v : V \rightarrow \mathbb{C}$, $\lambda_v(x) = (x, v)$ dla $x \in V$ (zob. twierdzenie 5.4.1).

TWIERDZENIE 7.1.1. *Dla każdego endomorfizmu τ przestrzeni unitarnej V istnieje dokładnie jeden endomorfizm τ^* przestrzeni V spełniający warunek*

$$(\tau(v), u) = (v, \tau^*(u)) \quad \text{dla wszystkich } u, v \in V. \quad (7.1)$$

Dowód. Dla każdego $u \in V$ rozpatrzmy funkcyjonał liniowy μ na przestrzeni V określony następująco:

$$\mu(v) = (\tau(v), u) \quad \text{dla } v \in V.$$

Na podstawie twierdzenia 5.4.1 istnieje dokładnie jeden wektor $w \in V$ taki, że $\mu = \lambda_w$. Mamy zatem

$$(\tau(v), u) = \mu(v) = \lambda_w(v) = (v, w) \quad \text{dla wszystkich } v \in V.$$

W ten sposób każdemu wektorowi $u \in V$ przyporządkujemy jednoznacznie wektor $w \in V$, który oznaczamy $\tau^*(u)$, spełniający

$$(\tau(v), u) = (v, \tau^*(u)) \quad \text{dla wszystkich } u, v \in V.$$

Tutaj τ^* jest odwzorowaniem $\tau^* : V \rightarrow V$ spełniającym warunek (7.1) i pozostaje wykazać, że τ^* jest endomorfizmem przestrzeni V i że jest to jedyny endomorfizm przestrzeni V spełniający warunek (7.1).

Weźmy dowolne $v, x, y \in V$ oraz $a, b \in \mathbb{C}$. Wtedy

$$\begin{aligned} (v, \tau^*(ax + by)) &= (\tau(v), ax + by) = \bar{a}(\tau(v), x) + \bar{b}(\tau(v), y) \\ &= \bar{a}(v, \tau^*(x)) + \bar{b}(v, \tau^*(y)) = (v, a\tau^*(x) + b\tau^*(y)). \end{aligned}$$

Wobec nieosobliwości przestrzeni V wynika stąd, że $\tau^*(ax + by) = a\tau^*(x) + b\tau^*(y)$.

Pokażemy teraz, że endomorfizm τ^* spełniający (7.1) jest tylko jeden. Przypuśćmy, że istnieje jeszcze jeden endomorfizm ρ przestrzeni V taki, że

$$(v, \rho(u)) = (\tau(v), u) = (v, \tau^*(u)) \quad \forall v, u \in V.$$

Wtedy $(v, \rho(u) - \tau^*(u)) = 0$ dla każdego $v \in V$, skąd wobec nieosobliwości przestrzeni wynika, że $\rho(u) = \tau^*(u)$ dla każdego $u \in V$. A więc $\rho = \tau^*$. $\square$

DEFINICJA 7.1.1. (a) Endomorfizm τ^* przestrzeni unitarnej V , spełniający warunek (7.1),

$$(\tau(v), u) = (v, \tau^*(u)) \quad \text{dla wszystkich } u, v \in V$$

nazywamy *endomorfizmem sprzężonym* z endomorfizmem τ przestrzeni V .

(b) Endomorfizm τ nazywa się *samosprzężony* jeśli $\tau = \tau^*$, to znaczy, jeśli

$$(\tau(v), u) = (v, \tau(u)) \quad \text{dla wszystkich } u, v \in V.$$

Uwaga 7.1.1. Ponieważ iloczyn skalarny nie jest symetryczny, fakt, że w definicji endomorfizmu τ^* pojawia się on na miejscu drugiej zmiennej iloczynu skalarnego wydaje się mieć znaczenie. Okazuje się jednak, że tak nie jest, gdyż endomorfizm τ^* spełnia także warunek

$$(\tau^*(v), u) = (v, \tau(u)) \quad \text{dla wszystkich } v, u \in V. \quad (7.2)$$

Rzeczywiście, dla dowolnych $v, u \in V$ mamy

$$(\tau^*(v), u) = \overline{(u, \tau^*(v))} = \overline{(\tau(u), v)} = (v, \tau(u)).$$

Stąd wynika też natychmiast, że $(\tau^*)^* = \tau$. Mamy bowiem

$$(v, (\tau^*)^*(u)) = (\tau^*(v), u) = (v, \tau(u))$$

dla wszystkich $u, v \in V$ skąd wobec nieosobliwości iloczynu skalarnego otrzymujemy $(\tau^*)^* = \tau$. W dalszym ciągu piszemy τ^{**} zamiast $(\tau^*)^*$.

TWIERDZENIE 7.1.2. Niech V będzie przestrzenią unitarną. Odwzorowanie

$$\text{End}_{\mathbb{C}} V \rightarrow \text{End}_{\mathbb{C}} V, \quad \tau \mapsto \tau^*$$

ma następujące własności

$$(\sigma + \tau)^* = \sigma^* + \tau^*, \quad (\sigma\tau)^* = \tau^*\sigma^*, \quad (a\tau)^* = \bar{a}\tau^*,$$

dla każdego endomorfizmów σ, τ przestrzeni V i dla każdego skalaru $a \in \mathbb{C}$, a także

$$\mathbf{1}_V^* = \mathbf{1}_V, \quad \tau^{**} = \tau.$$

Dowód. Wykorzystujemy własność (7.1) definiującą endomorfizm sprzężony i nieosobliwość przestrzeni. A więc dla każdego $u, v \in V$ mamy

$$\begin{aligned}(v, (\sigma + \tau)^*(u)) &= ((\sigma + \tau)(v), u) = (\sigma(v), u) + (\tau(v), u) = (v, \sigma^*(u)) + (v, \tau^*(u)) \\ &= (v, (\sigma^* + \tau^*)(u)),\end{aligned}$$

skąd wynika, że $(\sigma + \tau)^*(u) = (\sigma^* + \tau^*)(u)$ dla każdego $u \in V$. Podobnie

$$(v, (\sigma\tau)^*(u)) = (\sigma\tau(v), u) = (\tau(v), \sigma^*(u)) = (v, \tau^*\sigma^*(u)),$$

oraz

$$(v, (a\tau)^*(u)) = ((a\tau)(v), u) = a(\tau(v), u) = a(v, \tau^*(u)) = (v, \bar{a}\tau^*(u))$$

dowodzą dwóch następnych własności. Pozostaje udowodnić, że $\mathbf{1}_V^* = \mathbf{1}_V$. Zauważmy, że dla dowolnych $u, v \in V$, mamy

$$(v, \mathbf{1}^*(u)) = (\mathbf{1}(v), u) = (v, u) = (v, \mathbf{1}(u)),$$

Wobec tego $\mathbf{1}^*(u) = \mathbf{1}(u)$ dla każdego $u \in V$. □

Wartości endomorfizmu sprzężonego

Pokażemy teraz wyraźny wzór na wartość $\tau^*(u)$ dla dowolnego wektora $u \in V$. Jeśli $v = x_1v_1 + \dots + x_nv_n$, gdzie $x_i \in \mathbb{C}$ oraz $v_1, \dots, v_n$ jest bazą ortonormalną przestrzeni V , to $(v, v_i) = x_i$. Wobec tego współrzędne wektora v w bazie ortonormalnej wyrażają się poprzez wartości iloczynu skalarnego i mamy ogólną formułę

$$v = (v, v_1)v_1 + \dots + (v, v_n)v_n \tag{7.3}$$

dla dowolnego $v \in V$ i dowolnej bazy ortonormalnej $\{v_1, \dots, v_n\}$ przestrzeni V .

W szczególności zatem dla wektora $v = \tau^*(u)$ mamy

$$\tau^*(u) = \sum_i (\tau^*(u), v_i)v_i = \sum_i (u, \tau(v_i))v_i,$$

gdzie wykorzystaliśmy (7.2). Jest to zapowiadana wyraźna formuła dla obliczenia wartości τ^* na dowolnym wektorze $u \in V$.

Uwaga 7.1.2. Jak pokazaliśmy powyżej, jeśli $v_1, \dots, v_n$ jest bazą ortonormalną przestrzeni unitarnej V , to dla każdego endomorfizmu τ przestrzeni mamy następujący wyraźny wzór dla działania endomorfizmu sprzężonego τ^* :

$$\tau^*(u) = \sum_{i=1}^n (u, \tau(v_i))v_i. \tag{7.4}$$

Dla badania własności endomorfizmu sprzężonego z τ , w szczególności dla dowodu twierdzenia 7.1.2, można byłoby posługiwać się tym wzorem. Jako przykład sprawdzimy tą metodą zachowanie się operacji sprzężenia endomorfizmu przy dodawaniu endomorfizmów. A więc dla $\sigma, \tau \in \text{End}_K V$ oraz dowolnego $u \in V$ mamy

$$\begin{aligned}(\sigma + \tau)^*(u) &= \sum_{i=1}^n (u, (\sigma + \tau)(v_i))v_i \\ &= \sum_{i=1}^n (u, \sigma(v_i))v_i + \sum_{i=1}^n (u, \tau(v_i))v_i \\ &= \sigma^*(u) + \tau^*(u) = (\sigma^* + \tau^*)(u).\end{aligned}$$

Pokazaliśmy więc, że $(\sigma + \tau)^* = \sigma^* + \tau^*$.

Macierz endomorfizmu sprzężonego.

Niech $\mathcal{B} = \{u_1, \dots, u_n\}$ będzie bazą ortonormalną przestrzeni unitarnej V i niech $\tau \in \text{End}_K V$. Niech

$$A = [a_{ij}] = m(\tau, \mathcal{B}) \quad \text{oraz} \quad B = [b_{ij}] = m(\tau^*, \mathcal{B}).$$

Wtedy $\tau(u_j) = \sum_i a_{ij} u_i$, $\tau^*(u_k) = \sum_i b_{ik} u_i$ oraz

$$a_{kj} = (\tau(u_j), u_k), \quad b_{jk} = (\tau^*(u_k), u_j)$$

i wobec tego

$$a_{kj} = (\tau(u_j), u_k) = (u_j, \tau^*(u_k)) = \overline{(\tau^*(u_k), u_j)} = \overline{b_{jk}}.$$

A więc $A = \bar{B}^T$. Macierz $\bar{B}^T$ nazywamy macierzą *sprzężoną* z macierzą B . Zauważmy, że $A = \bar{B}^T$ wtedy i tylko wtedy gdy $\bar{A}^T = B$. Zwykle macierz $\bar{A}^T$ oznacza się symbolem A^* . A więc macierz B endomorfizmu τ^* sprzężonego z endomorfizmem τ jest sprzężona z macierzą A endomorfizmu τ (obydwie macierze w tej samej bazie ortonormalnej przestrzeni unitarnej V):

$$m(\tau, \mathcal{B}) = A \quad \Rightarrow \quad m(\tau^*, \mathcal{B}) = A^* = \bar{A}^T. \quad (7.5)$$

Zgodnie z definicją 7.1.1 endomorfizm τ przestrzeni unitarnej V nazywa się *samosprzężonym*, jeśli

$$(\tau(v), u) = (v, \tau(u)) \quad \forall u, v \in V.$$

Jak zauważyliśmy w twierdzeniu 7.1.2, endomorfizm $\mathbf{1}_V$ jest samosprzężony. Ogólniej, jeśli $a \in \mathbb{R}$, to $a\mathbf{1}_V$ jest samosprzężony gdyż $(a\mathbf{1}_V)^* = \bar{a}\mathbf{1}_V = a\mathbf{1}_V$.

Łatwo też zauważyć, że dla dowolnego endomorfizmu σ przestrzeni unitarnej V endomorfizm $\tau = \sigma\sigma^*$ jest samosprzężony. Rzeczywiście,

$$\tau^* = (\sigma\sigma^*)^* = \sigma^{**}\sigma^* = \sigma\sigma^* = \tau.$$

Jeśli A jest macierzą endomorfizmu samosprzężonego τ w bazie ortonormalnej, to wobec $\tau = \tau^*$ mamy $A = A^*$. Macierz o tej własności nazywamy *hermitowską*. Następujące twierdzenie dowodzimy podobnie jak twierdzenie 4.2.2 w rozdziale 4.

TWIERDZENIE 7.1.3. Niech τ będzie endomorfizmem przestrzeni unitarnej V .

Następujące warunki są równoważne.

- (a) Endomorfizm τ jest samosprzężony.
- (b) Dla każdej bazy ortonormalnej $\mathcal{B}$ macierz endomorfizmu τ względem bazy $\mathcal{B}$ jest hermitowska.
- (c) Istnieje baza ortonormalna $\mathcal{B}$ taka, że macierz endomorfizmu τ względem bazy $\mathcal{B}$ jest hermitowska.

7.2 Endomorfizmy samosprzężone przestrzeni unitarnych

Następujący lemat, analogiczny do lematu 4.3.3, ma kluczowe znaczenie w dowodzie twierdzenia spektralnego w przypadku unitarnym.

LEMAT 7.2.1. Jeśli τ jest endomorfizmem samosprzężonym przestrzeni unitarnej V oraz U jest podprzestrzenią τ -niezmienniczą, to ortogonalne dopełnienie $U^\perp$ podprzestrzeni U jest także podprzestrzenią τ -niezmienniczą.

Dowód. Pokażemy, że jeśli $w \in U^\perp$, to także $\tau(w) \in U^\perp$. Jeśli $w \in U^\perp$, to dla każdego $u \in U$ mamy

$$(\tau(w), u) = (w, \tau(u)) = 0$$

gdyż $w \in U^\perp$ oraz $\tau(u) \in U$. Stąd wynika, że $\tau(w) \in U^\perp$. $\square$

LEMAT 7.2.2. *Każdy endomorfizm τ przestrzeni unitarnej ma podprzestrzeń niezmienniczą o wymiarze 1.*

Dowód. Wielomian minimalny p_τ endomorfizmu τ ma pierwiastek w ciele algebraicznie domkniętym $\mathbb{C}$ i wobec tego endomorfizm τ ma wektor własny, który rozpina jednowymiarową podprzestrzeń niezmienniczą. $\square$

LEMAT 7.2.3. *Każda wartość własna endomorfizmu samosprzężonego τ przestrzeni unitarnej V jest liczbą rzeczywistą.*

Dowód. Dla endomorfizmu samosprzężonego τ i dowolnego wektora $u \in V$ mamy

$$(\tau(u), u) = (u, \tau(u)) = \overline{(\tau(u), u)}.$$

Zatem $(\tau(u), u) \in \mathbb{R}$ dla każdego $u \in V$. W szczególności, jeśli u jest wektorem własnym należącym do wartości własnej a endomorfizmu τ , to $(\tau(u), u) = a(u, u) \in \mathbb{R}$. Ponieważ $(u, u) \in \mathbb{R}$, więc także $a \in \mathbb{R}$. $\square$

Twierdzenie spektralne

TWIERDZENIE 7.2.1 (Twierdzenie spektralne - przypadek unitarny). *Niech τ będzie endomorfizmem samosprzężonym przestrzeni unitarnej V . Wtedy istnieje baza ortonormalna przestrzeni V złożona z wektorów własnych endomorfizmu τ .*

Dowód. Indukcja ze względu na wymiar przestrzeni V . Niech $n = \dim V > 1$ i niech U będzie 1-wymiarową podprzestrzenią niezmienniczą endomorfizmu τ . Wtedy $U^\perp$ jest także τ -niezmiennicza na podstawie lematu 7.2.1 oraz

$$V = U \oplus U^\perp$$

na podstawie twierdzenia o rzucie prostopadłym. Na podstawie założenia indukcyjnego istnieje baza ortonormalna podprzestrzeni $U^\perp$ złożona z wektorów własnych endomorfizmu τ . Dołączając do niej wektor $u_1 \in U$ o długości 1 otrzymamy bazę ortonormalną przestrzeni V złożoną z wektorów własnych endomorfizmu τ . $\square$

Jeśli $v_1, \dots, v_n$ jest bazą ortonormalną przestrzeni unitarnej V złożoną z wektorów własnych endomorfizmu samosprzężonego τ oraz $a_1, \dots, a_n$ są odpowiednimi wartościami własnymi, to znaczy $\tau(v_i) = a_i v_i$, to na podstawie lematu 7.2.3 wszystkie a_i należą do ciała $\mathbb{R}$. Endomorfizm τ ma więc w bazie ortonormalnej $\mathcal{B} = \{v_1, \dots, v_n\}$ rzeczywistą macierz diagonalną:

$$m(\tau, \mathcal{B}) = \text{diag}(a_1, \dots, a_n) = \begin{bmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ & & \ddots & \\ 0 & 0 & \dots & a_n \end{bmatrix}.$$

Niech $\mathcal{B}$ i $\mathcal{B}'$ będą bazami ortonormalnymi przestrzeni unitarnej V i niech P będzie macierzą przejścia od bazy $\mathcal{B}$ do bazy $\mathcal{B}'$. Łatwo stwierdzić, że macierz P jest *unitarna*, to znaczy $P^{-1} = \bar{P}^T$. Jest to odpowiednik twierdzenia o bazach ortonormalnych przestrzeni euklidesowej: macierz przejścia P od bazy ortonormalnej przestrzeni euklidesowej do innej bazy ortonormalnej tej przestrzeni jest macierzą *ortogonalną*, to znaczy $P^{-1} = P^T$.

Twierdzenie 7.2.2. *Niech A będzie macierzą hermitowską o elementach z ciała $\mathbb{C}$. Wtedy istnieje macierz unitarna P o elementach z ciała $\mathbb{C}$ taka, że $P^{-1}AP$ jest macierzą diagonalną.*

Twierdzenie to mówi, że każda macierz hermitowska nad ciałem liczb zespolonych jest unitarnie podobna do macierzy diagonalnej.

7.3 Przemienne zbiory endomorfizmów samosprzężonych

LEMAT 7.3.1. *Niech $\mathcal{T}$ będzie przemennym zbiorem endomorfizmów przestrzeni unitarnej V , to znaczy $\tau\sigma = \sigma\tau$ dla każdych $\tau, \sigma \in \mathcal{T}$. Wtedy istnieje wspólny wektor własny dla wszystkich endomorfizmów zbioru $\mathcal{T}$ (to znaczy taki wektor $v \in V$, że $v \neq 0$ oraz dla każdego $\tau \in \mathcal{T}$ mamy $\tau(v) \in \mathbb{C}v$).*

Dowód. Postępujemy dokładnie tak jak w przypadku przestrzeni euklidesowej (zobacz lemat 4.4.1). Jeśli wszystkie endomorfizmy w zbiorze $\mathcal{T}$ są skalarne, to każdy niezerowy wektor przestrzeni V jest wspólnym wektorem własnym wszystkich endomorfizmów zbioru $\mathcal{T}$. W szczególności, jeśli $\dim V = 1$, to wszystkie endomorfizmy są skalarne i wobec tego lemat jest prawdziwy. Przeprowadzimy dowód indukcyjny ze względu na wymiar przestrzeni V . Niech $\dim V > 1$. Jeśli $\tau \in \mathcal{T}$ nie jest skalarne, to τ , jako endomorfizm przestrzeni wektorowej nad ciałem algebraicznie domkniętym ma wartość własną a i wektor własny $v \in V$ należący do a (w przypadku przestrzeni euklidesowej potrzebowaliśmy tutaj założenia, że endomorfizmy zbioru $\mathcal{T}$ są samosprzężone). Niech

$$U = \{u \in V : \tau(u) = au\}.$$

Jest to podprzestrzeń τ -niezmiennicza, a także, $U \neq 0$ oraz $U \neq V$ (bo τ nie jest skalarne). Ponadto, U jest σ -niezmiennicza dla każdego $\sigma \in \mathcal{T}$. Rzeczywiście, dla $u \in U$ mamy

$$\tau(\sigma(u)) = \sigma(\tau(u)) = \sigma(au) = a\sigma(u),$$

zatem $\sigma(u) \in U$. Zacieśnienia endomorfizmów $\sigma \in \mathcal{T}$ do podprzestrzeni U tworzą więc przemienne zbiory endomorfizmów przestrzeni unitarnej U i wobec $\dim U < \dim V$ na podstawie założenia indukcyjnego endomorfizmy zbioru $\mathcal{T}$ mają wspólny wektor własny w podprzestrzeni U . $\square$

Twierdzenie 7.3.1. *Jeśli $\mathcal{T}$ jest przemennym zbiorem endomorfizmów samosprzężonych przestrzeni unitarnej V , to V ma bazę ortonormalną $\{v_1, \dots, v_n\}$ taką, że każdy wektor v_i tej bazy jest wektorem własnym wszystkich endomorfizmów zbioru $\mathcal{T}$.*

Dowód jest taki sam jak w przypadku przestrzeni euklidesowej (zobacz twierdzenie 4.4.2).

7.4 Endomorfizmy normalne

Jeśli endomorfizm τ przestrzeni unitarnej V ma w pewnej bazie ortonormalnej przestrzeni V macierz diagonalną D , to endomorfizm sprzężony τ^* ma w tej samej bazie macierz D^* , która jest także macierzą diagonalną. Ponieważ macierze diagonalne są przemienne, więc $DD^* = D^*D$ i wobec tego także $\tau\tau^* = \tau^*\tau$. A więc każdy endomorfizm diagonalizowalny w bazie ortonormalnej przestrzeni unitarnej jest przemienne ze swoim endomorfizmem sprzężonym.

DEFINICJA 7.4.1. Endomorfizm τ przestrzeni unitarnej V nazywa się *normalny*, jeśli jest przemienny ze swoim endomorfizmem sprzężonym τ^* :

$$\tau\tau^* = \tau^*\tau.$$

Przykład 7.4.1. Każdy endomorfizm samosprzężony jest normalny. Ponadto, jeśli endomorfizm τ jest normalny, to endomorfizm sprzężony τ^* też jest normalny (jest przemienny z endomorfizmem $\tau^{**} = \tau$). Dwa dalsze przykłady: każdy endomorfizm skośny (spełniający $\tau^* = -\tau$) jest normalny i każdy endomorfizm unitarny (spełniający $\tau\tau^* = \tau^*\tau = \mathbf{1}$) jest normalny. Łatwo też zauważyć, że jeśli endomorfizm normalny τ jest odwracalny, to τ^{-1} jest normalny.

Uwaga 7.4.1. Sprawdzenie czy dany endomorfizm jest czy nie jest normalny jest bardzo proste. Jeśli endomorfizm τ jest zadany poprzez swoją macierz A w jakiejś bazie przestrzeni unitarnej, to znajdujemy bazę ortonormalną $\mathcal{B}$ tej przestrzeni i macierz B endomorfizmu τ w bazie $\mathcal{B}$ zgodnie z twierdzeniem 1.6.1. Endomorfizm τ^* ma w bazie $\mathcal{B}$ macierz B^* (zobacz 7.5) i wobec tego $\tau\tau^* = \tau^*\tau$ wtedy i tylko wtedy gdy $BB^* = B^*B$. Ten ostatni warunek sprawdza się bezpośrednim rachunkiem.

Uwaga 7.4.2. Istnieją endomorfizmy normalne, które nie są samosprzężone. Niech τ będzie endomorfizmem przestrzeni unitarnej V , który w pewnej bazie ortonormalnej $\mathcal{B}$ tej przestrzeni ma macierz diagonalną $m(\tau, \mathcal{B}) = \text{diag}(a_1, \dots, a_n) =: D$. Wtedy $m(\tau^*, \mathcal{B}) = D^* = \text{diag}(\overline{a_1}, \dots, \overline{a_n})$ i wobec tego $DD^* = D^*D$. Stąd wynika, że $\tau\tau^* = \tau^*\tau$ i wobec tego τ jest normalny. Tymczasem jeśli co najmniej jedna z liczb zespolonych $a_1, \dots, a_n$ nie jest liczbą rzeczywistą, to τ nie jest samosprzężony, gdyż endomorfizm samosprzężony ma rzeczywiste wartości własne (lemat 7.2.3).

LEMAT 7.4.1. (a) *Każdy endomorfizm τ przestrzeni unitarnej V ma jednoznaczne przedstawienie w postaci*

$$\tau = \sigma + i\rho$$

gdzie σ, ρ są endomorfizmami samosprzężonymi.

(b) $\tau^* = \sigma - i\rho$.

(c) *Endomorfizm τ jest normalny wtedy i tylko wtedy gdy $\sigma\rho = \rho\sigma$.*

Dowód. (a) Dla endomorfizmu τ obieramy

$$\sigma := \frac{1}{2}(\tau + \tau^*), \quad \rho := \frac{1}{2i}(\tau - \tau^*) = \frac{1}{2}i(\tau^* - \tau).$$

Wtedy $\sigma^* = \frac{1}{2}(\tau^* + \tau^{**}) = \sigma$ oraz $\rho^* = \frac{1}{2}i((\tau^*)^* - \tau^*) = -\frac{1}{2}i(\tau - \tau^*) = \rho$.

A więc σ i ρ są endomorfizmami samosprzężonymi. Zauważmy teraz, że

$$\sigma + i\rho = \frac{1}{2}(\tau + \tau^*) + i\frac{1}{2i}(\tau - \tau^*) = \tau,$$

co dowodzi (a), z wyjątkiem jednoznaczności przedstawienia. Część (b) jest natychmiastowa:

$$\tau^* = (\sigma + i\rho)^* = \sigma^* - i\rho^* = \sigma - i\rho$$

i wynika z niej także jednoznaczność przedstawienia z części (a). Wystarczy pokazać, że jeśli $\sigma + i\rho = 0$ dla samosprzężonych endomorfizmów σ, ρ , to $\sigma = \rho = 0$. Z równości $\sigma + i\rho = 0$ otrzymujemy na podstawie części (b) równość $\sigma - i\rho = 0$ i wobec tego (dodając i odejmując stronami) mamy $\sigma = 0$ i $\rho = 0$.

Dla dowodu (c) zauważmy, że

$$\begin{aligned} \tau\tau^* = \tau^*\tau &\iff (\sigma + i\rho)(\sigma - i\rho) = (\sigma - i\rho)(\sigma + i\rho) \iff -i\sigma\rho + i\rho\sigma = i\sigma\rho - i\rho\sigma \\ &\iff \sigma\rho = \rho\sigma. \end{aligned}$$

□

7.4.1 Charakteryzacja endomorfizmów normalnych

Następujące twierdzenie podaje definitywną charakteryzację endomorfizmów diagonalizowalnych w bazach ortonormalnych przestrzeni unitarnej.

TWIERDZENIE 7.4.1. *Niech τ będzie endomorfizmem przestrzeni unitarnej V . Następujące warunki są równoważne.*

- (a) *Endomorfizm τ jest normalny.*
- (b) *Istnieje baza ortonormalna przestrzeni V złożona z wektorów własnych endomorfizmu τ .*

Dowód. (a) $\Rightarrow$ (b) Niech τ będzie endomorfizmem normalnym i niech $\tau = \sigma + i\rho$ będzie przedstawieniem endomorfizmu τ z lematu 7.4.1. A więc endomorfizmy σ, ρ są samosprężone i przemienne. Na podstawie twierdzenia 7.3.1 istnieje baza ortonormalna $\{u_1, \dots, u_n\}$ przestrzeni V złożona z wektorów własnych endomorfizmów σ i ρ . Zatem istnieją $a_j, b_j \in \mathbb{R}$ takie, że

$$\sigma(u_j) = a_j u_j, \quad \rho(u_j) = b_j u_j, \quad j = 1, \dots, n.$$

Zatem wobec $\tau = \sigma + i\rho$ mamy

$$\tau(u_j) = \sigma(u_j) + i\rho(u_j) = (a_j + i b_j)u_j, \quad j = 1, \dots, n.$$

A więc $\{u_1, \dots, u_n\}$ jest bazą ortonormalną złożoną z wektorów własnych endomorfizmu normalnego τ .

(b) $\Rightarrow$ (a) zauważyliśmy już przed definicją endomorfizmu normalnego. □

Rozstrzygniemy jeszcze jedną wątpliwość związaną z diagonalizowalnością endomorfizmów przestrzeni unitarnej. Jak dotąd rozpatrywaliśmy jedynie endomorfizmy, które mają macierz diagonalną w pewnej bazie *ortonormalnej* przestrzeni unitarnej. Powstaje naturalne pytanie, czy endomorfizmy, które mają macierz diagonalną w pewnej bazie mają też macierz diagonalną w pewnej bazie ortonormalnej. Inaczej mówiąc, pytamy czy z tego, że istnieje baza przestrzeni unitarnej złożona z wektorów własnych endomorfizmu wynika, że istnieje baza *ortonormalna* tej przestrzeni złożona z wektorów własnych tego endomorfizmu. Odpowiedź jest negatywna (zobacz przykład 7.4.2). Najpierw zauważymy jeszcze dwie własności endomorfizmów normalnych.

LEMAT 7.4.2. *Niech τ będzie endomorfizmem normalnym przestrzeni unitarnej V i niech $u \in V$ będzie wektorem własnym endomorfizmu τ należącym do wartości własnej a . Wtedy u jest także wektorem własnym endomorfizmu sprzężonego τ^* i należy do wartości własnej $\bar{a}$.*

Dowód. Mamy udowodnić, że jeśli $\tau(u) = au$, to $\tau^*(u) = \bar{a}u$. W dowodzie wykorzystamy wyraźny wzór (7.4) dla wartości endomorfizmu τ^* :

$$\tau^*(u) = \sum_{i=1}^n (u, \tau(v_i))v_i,$$

gdzie $v_1, \dots, v_n$ tworzą bazę ortonormalną przestrzeni V . Zauważmy, że wobec normalności endomorfizmu τ istnieje baza ortonormalna $\mathcal{B} = \{v_1, \dots, v_n\}$ złożona z wektorów własnych endomorfizmu τ (na podstawie twierdzenia 7.4.1). Wektor u ma przedstawienie $u = \sum_i x_i v_i$, gdzie $x_i \in K$ i nie wszystkie x_i są równe zero. Wobec tego

$$\sum_i a x_i v_i = au = \tau(u) = \sum_i x_i \tau(v_i) = \sum_i x_i a_i v_i,$$

gdzie a_i jest wartością własną τ , do której należy wektor własny v_i . Stąd wynika, że jeśli $x_i \neq 0$, to $a_i = a$. Pokazaliśmy więc, że jeśli u jest wektorem własnym należącym do wartości własnej a , to u jest kombinacją liniową tych wektorów własnych v_i bazy ortonormalnej $\mathcal{B}$, które należą do wartości własnej a . Niech

$$U := \ker(\tau - a\mathbf{1}) = \{v \in V : \tau(v) = av\}.$$

Pokazaliśmy, że podprzestrzeń U jest rozpięta na tych wektorach bazy $\mathcal{B}$, które należą do wartości własnej a . Zmieniając ewentualnie porządek wektorów w bazie $\mathcal{B}$ możemy założyć, że wektory $v_1, \dots, v_\ell$ tworzą bazę podprzestrzeni U . Wtedy pozostałe wektory bazowe $v_{\ell+1}, \dots, v_n$ tworzą bazę ortogonalnego dopełnienia $U^\perp$ podprzestrzeni U . Zauważmy też, że

$$\tau(U^\perp) \subseteq U^\perp$$

gdyż podprzestrzeń $U^\perp$ jest rozpięta na wektorach własnych endomorfizmu τ . Wykorzystamy teraz wzór (7.4) dla obliczenia $\tau^*(u)$:

$$\begin{aligned} \tau^*(u) &= \sum_{i=1}^n (u, \tau(v_i))v_i = \sum_{i=1}^{\ell} (u, \tau(v_i))v_i + \sum_{i=\ell+1}^n (u, \tau(v_i))v_i \\ &= \sum_{i=1}^{\ell} (u, \tau(v_i))v_i = \sum_{i=1}^{\ell} (u, av_i)v_i \\ &= \bar{a} \sum_{i=1}^{\ell} (u, v_i)v_i = \bar{a} \sum_{i=1}^n (u, v_i)v_i \\ &= \bar{a}u. \end{aligned}$$

Tutaj $\sum_{i=\ell+1}^n (u, \tau(v_i))v_i = 0$, gdyż $u \in U$ oraz $\tau(v_i) \in U^\perp$. Ponadto $\sum_{i=1}^n (u, v_i)v_i = u$ na podstawie (7.3). $\square$

Uwaga 7.4.3. Lemat 7.4.2 można także udowodnić nie posługując się wyraźnym wzorem (7.4) dla wartości endomorfizmu τ^* . Najpierw zauważmy, że dla dowolnego endomorfizmu normalnego τ i dla każdego $v \in V$ mamy

$$\|\tau(v)\|^2 = (\tau(v), \tau(v)) = (v, \tau^*\tau(v)) = (v, \tau\tau^*(v)) = (\tau^*(v), \tau^*(v)) = \|\tau^*(v)\|^2.$$

Dalej zauważmy, że dla dowolnego skalaru $a \in \mathbb{C}$ endomorfizm $\tau - a\mathbf{1}$ jest normalny:

$$\begin{aligned} (\tau - a\mathbf{1})(\tau - a\mathbf{1})^* &= (\tau - a\mathbf{1})(\tau^* - \bar{a}\mathbf{1}) = \tau\tau^* - a\tau^* - \bar{a}\tau + a\bar{a}\mathbf{1} \\ &= \tau^*\tau - a\tau^* - \bar{a}\tau + a\bar{a}\mathbf{1} = (\tau^* - \bar{a}\mathbf{1})(\tau - a\mathbf{1}) \\ &= (\tau - a\mathbf{1})^*(\tau - a\mathbf{1}). \end{aligned}$$

Wobec tego dla dowolnego $a \in \mathbb{C}$ i dowolnego $v \in V$ mamy

$$\|(\tau - a\mathbf{1})(v)\|^2 = \|(\tau^* - \bar{a}\mathbf{1})(v)\|^2.$$

Jeśli teraz $\tau(u) = au$, to $\|(\tau - a\mathbf{1})(u)\| = 0$, skąd także $\|(\tau^* - \bar{a}\mathbf{1})(u)\| = 0$ i wobec tego $\tau^*(u) = \bar{a}u$.

LEMAT 7.4.3. Niech τ będzie endomorfizmem normalnym przestrzeni unitarnej V i niech a_1, a_2 będą różnymi wartościami własnymi endomorfizmu τ . Wtedy każde dwa wektory własne endomorfizmu τ należące do wartości własnych a_1, a_2 są prostopadłe.

Dowód. Niech $\tau(u_1) = a_1 u_1$ oraz $\tau(u_2) = a_2 u_2$. Wtedy

$$(\tau(u_1), u_2) = (a_1 u_1, u_2) = a_1 (u_1, u_2).$$

Z drugiej strony, wykorzystując normalność endomorfizmu τ i lemat 7.4.2, mamy

$$(\tau(u_1), u_2) = (u_1, \tau^*(u_2)) = (u_1, \bar{a}_2 u_2) = a_2 (u_1, u_2).$$

Zatem $a_1(u_1, u_2) = a_2(u_1, u_2)$ i ponieważ $a_1 \neq a_2$ otrzymujemy stąd $(u_1, u_2) = 0$. $\square$

Przykład 7.4.2. Wskażemy teraz przykład endomorfizmu diagonalizowalnego przestrzeni unitarnej, który *nie jest* diagonalizowalny w bazie ortonormalnej tej przestrzeni.

Niech $V = \mathbb{C}^2$ będzie standardową dwuwymiarową przestrzenią unitarną nad ciałem liczb zespolonych. Zatem dla wektorów $x = [x_1, x_2]$, $y = [y_1, y_2]$, gdzie $x_i, y_i \in \mathbb{C}$ mamy

$$(x, y) = x_1 \bar{y}_1 + x_2 \bar{y}_2.$$

Weźmy dwa wektory $v_1 = [1, 1]$, $v_2 = [0, i]$ i zauważmy, że są one liniowo niezależne. Stanowią zatem bazę przestrzeni V . Definiujemy teraz endomorfizm τ przestrzeni V kładąc

$$\tau(v_1) = v_1, \quad \tau(v_2) = i v_2.$$

A więc macierz $m(\tau, \mathcal{B})$ endomorfizmu τ w bazie $\mathcal{B} = \{v_1, v_2\}$ jest diagonalna:

$$m(\tau, \mathcal{B}) = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}.$$

Endomorfizm τ jest więc diagonalizowalny i wektory bazowe są wektorami własnymi należącymi do *różnych* wartości własnych $a_1 = 1$, $a_2 = i$. Ponieważ jednak $(v_1, v_2) = -i \neq 0$, wektory te nie są prostopadłe. Zatem na podstawie lematu 7.4.3 endomorfizm τ nie jest normalny, a więc na podstawie twierdzenia 7.4.1 nie istnieje baza ortonormalna przestrzeni V złożona z wektorów własnych endomorfizmu τ .

7.4.2 Przemienne zbiory endomorfizmów normalnych

Twierdzenie 7.4.1 daje satysfakcjonującą charakteryzację endomorfizmów przestrzeni unitarnej diagonalizowalnych w bazach ortonormalnych. Diagonalizowalne w bazach ortonormalnych są więc endomorfizmy normalne i tylko one. Rozpatrzmy teraz problem diagonalizowalności w najogólniejszej postaci, mianowicie znajdziemy warunek konieczny i wystarczający równoczesnej diagonalizowalności w bazie ortonormalnej *zbioru* endomorfizmów przestrzeni unitarnej. Inaczej mówiąc, znajdziemy warunek konieczny i wystarczający na to by dla zbioru $\mathcal{T}$ endomorfizmów przestrzeni unitarnej V istniała baza ortonormalna $\mathcal{B}$ przestrzeni V taka, że każdy wektor bazy $\mathcal{B}$ jest wektorem własnym każdego endomorfizmu zbioru $\mathcal{T}$. Jeden warunek konieczny wynika natychmiast z twierdzenia 7.4.1. Jeśli endomorfizmy zbioru $\mathcal{T}$ mają macierze diagonalne w pewnej bazie ortonormalnej przestrzeni V , to każdy endomorfizm tego zbioru musi być normalny. Drugim warunkiem koniecznym równoczesnej diagonalizowalności endomorfizmów zbioru $\mathcal{T}$ jest przemienność zbioru $\mathcal{T}$: każde dwa endomorfizmy $\sigma, \tau \in \mathcal{T}$ są przemienne. Rzeczywiście, równoczesna diagonalizowalność oznacza, że istnieje baza $\mathcal{B}$ przestrzeni V , w której macierze endomorfizmów σ i τ są diagonalne, a więc przemienne. Stąd wynika przemienność endomorfizmów σ i τ . W dalszym ciągu rozpatrywać będziemy więc zbiory $\mathcal{T}$ endomorfizmów przestrzeni unitarnej V , które są *normalne* i *przemienne*, to znaczy, każdy endomorfizm $\tau \in \mathcal{T}$ jest normalny oraz $\sigma\tau = \tau\sigma$ dla każdych $\sigma, \tau \in \mathcal{T}$.

Rozpoczynamy od następującej charakteryzacji normalności endomorfizmu.

Twierdzenie 7.4.2. Niech τ będzie endomorfizmem przestrzeni unitarnej V . Endomorfizm τ jest normalny wtedy i tylko wtedy gdy istnieje wielomian $f \in \mathbb{C}[X]$ taki, że

$$\tau^* = f(\tau).$$

Dowód. Jeśli $\tau^* = f(\tau)$, to $\tau f(\tau) = f(\tau)\tau$ na podstawie twierdzenia 1.4.1, zatem τ jest normalny.

Założmy teraz, że τ jest endomorfizmem normalnym. Na podstawie twierdzenia 7.4.1 istnieje baza ortonormalna $\{u_1, \dots, u_n\}$ przestrzeni V złożona z wektorów własnych endomorfizmu τ . Niech $\tau(u_j) = a_j u_j$ dla $j = 1, \dots, n$ i pewnych $a_j \in \mathbb{C}$. Wtedy na podstawie lematu 7.4.2 mamy $\tau^*(u_j) = \bar{a}_j u_j$. Obieramy teraz wielomian $f \in \mathbb{C}[X]$ taki, że $f(a_j) = \bar{a}_j$, dla $j = 1, \dots, n$. Wtedy

$$f(\tau)(u_j) = f(a_j)u_j = \bar{a}_j u_j = \tau^*(u_j),$$

dla wszystkich wektorów bazy $\{u_1, \dots, u_n\}$. Pierwsza równość wynika tutaj z lematu 1.5.1. Stąd wynika, że $f(\tau) = \tau^*$. $\square$

Uwaga 7.4.4. Objaśnimy istnienie wielomianu f , który w zadanych punktach a_j przyjmuje zadane wartości $\bar{a}_j$. Jest to konsekwencja tak zwanej *formuły interpolacyjnej* Lagrange'a. Jeśli F jest dowolnym ciałem (niekoniecznie algebraicznie domkniętym) oraz c_j, b_j , $j = 1, \dots, m$ są dowolnymi elementami ciała F , takimi, że $c_i \neq c_j$ dla $i \neq j$, to istnieje wielomian $f \in F[X]$ taki, że

$$f(c_j) = b_j, \quad j = 1, \dots, m.$$

Rzeczywiście, niech $g_i \in F[X]$ będzie iloczynem wszystkich czynników liniowych $X - c_j$ z wyjątkiem czynnika $X - c_i$. Wtedy wielomian

$$f(X) = b_1 \frac{g_1(X)}{g_1(c_1)} + b_2 \frac{g_2(X)}{g_2(c_2)} + \dots + b_m \frac{g_m(X)}{g_m(c_m)}$$

przyjmuje w punkcie c_j wartość b_j . Zauważmy, że ta konstrukcja pozwala wskazać wielomian f stopnia $\leq m - 1$, który w zadanych m punktach przyjmuje zadane wartości.

Wniosek 7.4.1. Jeśli τ jest endomorfizmem normalnym przestrzeni unitarnej V , to endomorfizm sprzężony τ^* jest przemienny z każdym endomorfizmem σ , z którym przemienny jest endomorfizm τ :

$$\sigma\tau = \tau\sigma \quad \Rightarrow \quad \sigma\tau^* = \tau^*\sigma.$$

Dowód. Na podstawie twierdzenia 7.4.2 mamy $\tau^* = f(\tau)$ dla pewnego $f \in K[X]$. Zauważmy, że $\sigma\tau = \tau\sigma$ pociąga $\sigma f(\tau) = f(\tau)\sigma$. Zatem $\sigma\tau^* = \sigma f(\tau) = f(\tau)\sigma = \tau^*\sigma$. $\square$

Wniosek 7.4.2. Jeśli $\mathcal{T} = \{\tau_i : i \in I\}$ jest zbiorem przemiennym endomorfizmów normalnych przestrzeni unitarnej V , to zbiór

$$\mathcal{S} := \mathcal{T} \cup \mathcal{T}^* = \{\tau_i : i \in I\} \cup \{\tau_i^* : i \in I\}$$

jest także zbiorem przemiennym endomorfizmów normalnych przestrzeni V .

Dowód. Każde dwa endomorfizmy zbioru $\mathcal{T}$ są przemiennie na podstawie założenia i wobec tego także każde dwa endomorfizmy zbioru $\mathcal{T}^*$ są przemiennie:

$$\tau_i^* \tau_j^* = (\tau_j \tau_i)^* = (\tau_i \tau_j)^* = \tau_j^* \tau_i^*.$$

Ponadto każdy endomorfizm zbioru $\mathcal{T}$ jest przemienny z każdym endomorfizmem zbioru $\mathcal{T}^*$. Rzeczywiście,

$$\tau_i \tau_j^* = \tau_j^* \tau_i$$

wynika z wniosku 7.4.1 dla $\sigma = \tau_i$ oraz $\tau = \tau_j$. $\square$

Zbiór $\mathcal{S}$ ma następującą własność: jeśli $\tau \in \mathcal{S}$, to $\tau^* \in \mathcal{S}$. Taki zbiór endomorfizmów przestrzeni unitarnej nazywa się zbiorem *samosprzężonym*. Zauważyliśmy więc, że każdy przemienny i normalny zbiór $\mathcal{T}$ endomorfizmów przestrzeni unitarnej V zawiera się w pewnym przemiennym, normalnym i samosprzężonym zbiorze $\mathcal{S}$ endomorfizmów przestrzeni V .

LEMAT 7.4.4. *Niech $\mathcal{S}$ będzie samosprzężonym zbiorem endomorfizmów przestrzeni unitarnej V . Niech W będzie $\mathcal{S}$ –niezmienniczą podprzestrzenią przestrzeni V (to znaczy, W jest podprzestrzenią niezmienniczą każdego endomorfizmu zbioru $\mathcal{S}$). Wtedy $W^\perp$ jest także $\mathcal{S}$ –niezmienniczą podprzestrzenią przestrzeni V .*

Dowód. Niech $x \in W^\perp$ oraz $\tau \in \mathcal{S}$. Należy udowodnić, że $(\tau(x), W) = 0$, albo równoważnie, że $(x, \tau^*(W)) = 0$. Ponieważ $\mathcal{S}$ jest zbiorem samosprzężonym, więc wraz z endomorfizmem τ zawiera endomorfizm τ^* i wobec tego W jest podprzestrzenią niezmienniczą endomorfizmu τ^* . Zatem $\tau^*(W) \subseteq W$ oraz dla każdego $w \in W$ mamy $\tau^*(w) \in W$ i wobec tego $(x, \tau^*(w)) = 0$. $\square$

Możemy teraz sformułować główne twierdzenie o równoczesnej ortonormalnej diagonalizowalności zbiorów endomorfizmów przestrzeni unitarnych.

TWIERDZENIE 7.4.3. *Niech $\mathcal{T} = \{\tau_i : i \in I\}$ będzie zbiorem endomorfizmów przestrzeni unitarnej V . Następujące warunki są równoważne.*

- (a) *Zbiór $\mathcal{T}$ jest normalny i przemienny.*
- (b) *Przestrzeń V ma bazę ortonormalną, której każdy wektor jest wektorem własnym każdego endomorfizmu zbioru $\mathcal{T}$.*

Dowód. (a) $\Rightarrow$ (b) Przeprowadzimy dowód indukcyjny ze względu na wymiar $n := \dim V$. Jeśli $n = 1$, to twierdzenie jest oczywiście prawdziwe, załóżmy więc, że $n > 1$. Niech $\mathcal{S} := \mathcal{T} \cup \mathcal{T}^*$, gdzie $\mathcal{T}^* = \{\tau_i^* : i \in I\}$. Wtedy $\mathcal{S}$ jest zbiorem przemiennym i samosprzężonym. Na podstawie lematu 7.3.1 istnieje niezerowy wektor $u \in V$ taki, że u jest wektorem własnym każdego endomorfizmu zbioru $\mathcal{S}$. Można oczywiście założyć, że $\|u\| = 1$. Niech $W := \mathbb{C}u$. Jest to jednowymiarowa podprzestrzeń niezmiennicza każdego endomorfizmu zbioru $\mathcal{S}$. Na podstawie lematu 7.4.4 podprzestrzeń $W^\perp$ jest także $\mathcal{S}$ –niezmiennicza. Ponieważ ma ona wymiar mniejszy niż przestrzeń V , na podstawie założenia indukcyjnego ma bazę ortonormalną złożoną z wektorów własnych $v_2, \dots, v_n$ wszystkich endomorfizmów zbioru $\mathcal{T}$. Po dołączeniu wektora u otrzymujemy bazę ortonormalną przestrzeni V .

(b) $\Rightarrow$ (a) zauważyliśmy już wcześniej analizując warunki konieczne równoczesnej diagonalizowalności zbioru endomorfizmów przestrzeni unitarnej. $\square$

Przykład 7.4.3. Jako pierwszy przykład zastosowania twierdzenia 7.4.3 pokażemy, że jeśli σ i τ są endomorfizmami normalnymi i $\sigma\tau = \tau\sigma$, to dla każdych $a, b \in \mathbb{C}$ endomorfizm $a\sigma + b\tau$ jest normalny. Rzeczywiście, zbiór $\{\sigma, \tau\}$ jest normalny i przemienny i wobec tego na podstawie twierdzenia 7.4.3 istnieje baza ortonormalna $\{v_1, \dots, v_n\}$ przestrzeni V taka, że $\sigma(v_i) = c_i v_i$, $\tau(v_i) = d_i v_i$ dla pewnych $c_i, d_i \in \mathbb{C}$. Wobec tego

$$(a\sigma + b\tau)(v_i) = (ac_i + bd_i)v_i, \quad i = 1, \dots, n,$$

skąd na podstawie twierdzenia 7.4.1 endomorfizm $a\sigma + b\tau$ jest normalny.

Stąd też wynika, że jeśli endomorfizm τ jest normalny, to $f(\tau)$ jest normalny dla każdego wielomianu $f \in \mathbb{C}[X]$. Jest to oczywiste gdy $f = X^k$, gdyż $\tau\tau^* = \tau^*\tau$ pociąga $\tau^k(\tau^k)^* = \tau^k(\tau^*)^k = (\tau^*)^k\tau^k = (\tau^k)^*\tau^k$. Natomiast dla dowolnego wielomianu $f = \sum_{k=0}^n c_k X^k$ normalność $f(\tau)$ wynika z normalności $c_k\tau^k$ oraz przemienności składników $f(\tau)$.

Uwaga 7.4.5. Implikację (a) $\Rightarrow$ (b) w twierdzeniu 7.4.3 można także udowodnić przez wykorzystanie twierdzenia 7.3.1 o istnieniu bazy ortonormalnej złożonej z wektorów własnych przemiennej rodziny endomorfizmów samosprężonych przestrzeni unitarnej. Każdy endomorfizm $\tau \in \mathcal{T}$ przedstawiamy w postaci $\tau = \sigma + i\rho$, gdzie σ, ρ są samosprężone. Na podstawie lematu 7.4.1 endomorfizmy σ, ρ są przemienne, natomiast z wniosku 7.4.1 wynika, że $\sigma = \frac{1}{2}(\tau + \tau^*)$ oraz $\rho = \frac{1}{2}i(\tau^* - \tau)$ są przemienne z każdym endomorfizmem zbioru $\mathcal{T}$. Nawet więcej, jeśli przez $\mathcal{S}$ oznaczymy zbiór wszystkich endomorfizmów samosprężonych σ, ρ występujących w przedstawieniach $\tau = \sigma + i\rho$ endomorfizmów zbioru $\mathcal{T}$, to zbiór $\mathcal{S}$ jest przemienny. Pozostaje tylko sprawdzić, że dla $\tau = \sigma + i\rho \in \mathcal{T}$ oraz $\tau' = \sigma' + i\rho' \in \mathcal{T}$ mamy $\sigma\sigma' = \sigma'\sigma$ oraz $\sigma\rho' = \rho'\sigma$. Otóż wiemy już, że σ jest przemienny z τ' , zatem

$$\sigma\sigma' + i\sigma\rho' = \sigma'\sigma + i\rho'\sigma,$$

skąd biorąc endomorfizmy sprzężone otrzymujemy

$$\sigma'\sigma - i\rho'\sigma = \sigma\sigma' - i\sigma\rho'.$$

Dodając i odejmując stronami otrzymamy $\sigma\sigma' = \sigma'\sigma$ oraz $\sigma\rho' = \rho'\sigma$. Zbiór $\mathcal{S}$ jest więc przemiennym zbiorem endomorfizmów samosprężonych. Zatem na podstawie twierdzenia 7.3.1 istnieje baza ortonormalna złożona z wektorów własnych wszystkich endomorfizmów zbioru $\mathcal{S}$. Każdy wektor tej bazy jest też wektorem własnym każdego endomorfizmu $\tau \in \mathcal{T}$.

7.5 Endomorfizmy unitarne

W rozdziale czwartym mówiliśmy już o izometriach przestrzeni dwuliniowych. W przestrzeni unitarnej endomorfizmy spełniające warunek zachowywania funkcjonału hermitowskiego nazywają się endomorfizmami unitarnymi.

DEFINICJA 7.5.1. Endomorfizm τ przestrzeni unitarnej V nazywamy *unitarnym*, jeśli spełnia następujący warunek:

$$(\tau(u), \tau(v)) = (u, v) \quad \forall u, v \in V.$$

Zauważmy, że endomorfizm unitarny zachowuje *długości* wektorów, gdyż dla dowolnego $v \in V$ mamy

$$\|\tau(v)\|^2 = (\tau(v), \tau(v)) = (v, v) = \|v\|^2.$$

Ponieważ dla $0 \neq v \in V$ mamy $\|v\| > 0$, wynika stąd, że endomorfizm unitarny τ przeprowadza wektory niezerowe na niezerowe, jest zatem endomorfizmem nieosobliwym. Endomorfizmy unitarne przestrzeni unitarnych mają więc podstawowe własności izometrii przestrzeni dwuliniowych i wobec tego endomorfizmy unitarne przestrzeni unitarnej V nazywamy także *izometriami* przestrzeni unitarnej V .

LEMAT 7.5.1. Endomorfizm τ przestrzeni unitarnej V jest izometrią wtedy i tylko wtedy, gdy

$$(\tau(u), \tau(u)) = (u, u) \quad \forall u \in V.$$

Dowód. Konieczność tego warunku jest oczywista. Jeśli zaś ten warunek jest spełniony, to dla dowolnych $u, v \in V$ mamy

$$(\tau(u+v), \tau(u+v)) = (u+v, u+v).$$

Stąd

$$(\tau(u), \tau(v)) + (\tau(v), \tau(u)) = (u, v) + (v, u).$$

Podstawiając tu iv w miejsce v i dzieląc przez i otrzymamy

$$-(\tau(u), \tau(v)) + (\tau(v), \tau(u)) = -(u, v) + (v, u).$$

Odejmując stronami dwie ostatnie równości otrzymujemy $(\tau(u), \tau(v)) = (u, v)$ dla wszystkich $u, v \in V$. $\square$

Zanotujmy następującą charakteryzację endomorfizmów unitarnych w języku endomorfizmów sprzężonych.

TWIERDZENIE 7.5.1. *Endomorfizm τ przestrzeni unitarnej V jest izometrią wtedy i tylko wtedy, gdy*

$$\tau^* \tau = 1_V.$$

Dowód. Jeśli τ jest izometrią, to dla każdych $u, v \in V$ mamy

$$(u, v) = (\tau(u), \tau(v)) = (u, \tau^* \tau(v)).$$

Stąd wynika, że $\tau^* \tau = 1_V$. Na odwrót, jeśli $\tau^* \tau = 1_V$, to

$$(u, v) = (u, \tau^* \tau(v)) = (\tau(u), \tau(v))$$

dla każdych $u, v \in V$ i wobec tego τ jest izometrią przestrzeni V . $\square$

WNIOSEK 7.5.1. *Endomorfizm τ przestrzeni unitarnej V jest izometrią V wtedy i tylko wtedy, gdy jest odwracalny oraz*

$$\tau^{-1} = \tau^*.$$

WNIOSEK 7.5.2. *Izometria τ przestrzeni unitarnej V jest endomorfizmem normalnym przestrzeni V .*

WNIOSEK 7.5.3. *Dla każdej izometrii τ przestrzeni unitarnej V istnieje baza ortonormalna przestrzeni V złożona z wektorów własnych izometrii τ .*

WNIOSEK 7.5.4. *Endomorfizm normalny τ przestrzeni unitarnej V jest izometrią V wtedy i tylko wtedy, gdy każda wartość własna endomorfizmu τ ma wartość bezwzględną 1.*

Dowód. Jeśli τ jest normalny, to jest diagonalizowalny, zatem istnieje baza ortonormalna $v_1, \dots, v_n$ przestrzeni V złożona z wektorów własnych endomorfizmu τ . Niech $\tau(v_j) = a_j v_j$, gdzie $a_j \in \mathbb{C}$. Jeśli τ jest izometrią, to

$$(v_j, v_j) = (\tau(v_j), \tau(v_j)) = (a_j v_j, a_j v_j) = a_j \overline{a_j} (v_j, v_j),$$

skąd wynika, że $a_j \overline{a_j} = 1$. A więc $|a_j| = 1$. Z drugiej strony, jeśli wszystkie $|a_j| = 1$, to dla dowolnego wektora $v = c_1 v_1 + \dots + c_n v_n$ mamy

$$\begin{aligned} \|\tau(v)\|^2 &= \|c_1 a_1 v_1 + \dots + c_n a_n v_n\|^2 \\ &= c_1 a_1 \cdot \overline{c_1 a_1} + \dots + c_n a_n \cdot \overline{c_n a_n} \\ &= c_1 \overline{c_1} \cdot a_1 \overline{a_1} + \dots + c_n \overline{c_n} \cdot a_n \overline{a_n} \\ &= c_1 \overline{c_1} + \dots + c_n \overline{c_n} = \|v\|^2. \end{aligned}$$

Zatem τ jest izometrią. $\square$

7.6 Symetrie i grupa unitarna

Wszystkie pojęcia i fakty o izometriach, symetriach i grupie ortogonalnej przestrzeni euklidesowej omawiane w rozdziałach 4.5 – 4.8 mają swoje odpowiedniki w przestrzeniach unitarnych. Przedstawimy je tutaj w nieco skróconej wersji. Przede wszystkim łatwo sprawdza się, że iloczyn $\sigma\tau$ dwóch izometrii jest izometrią i wobec wniosku 7.5.1 izometrie przestrzeni unitarnej (endomorfizmy unitarne) tworzą grupę, którą nazywamy *grupą unitarną* przestrzeni V i oznaczamy $\mathcal{U}(V)$.

Macierzowa reprezentacja grupy unitarnej

Następujące twierdzenie otrzymuje się przez naturalną modyfikację twierdzenia 4.7.1.

Twierdzenie 7.6.1. *Niech V będzie n -wymiarową przestrzenią unitarną i niech $A = [(v_i, v_j)]$ będzie macierzą przestrzeni V w bazie $\mathcal{B} = \{v_1, \dots, v_n\}$ przestrzeni V .*

(a) *Automorfizm σ przestrzeni wektorowej V jest izometrią przestrzeni unitarnej V wtedy i tylko wtedy gdy macierz $S = \mathbf{m}(\sigma, \mathcal{B})$ automorfizmu σ w bazie $\mathcal{B}$ spełnia*

$$S^t \overline{A} S = A.$$

(b) *Grupa unitarna $\mathcal{U}(V)$ przestrzeni V jest izomorficzna z podgrupą*

$$\{S \in \mathbf{GL}(n, \mathbb{C}) : S^t \overline{A} S = A\}$$

grupy macierzy $\mathbf{GL}(n, \mathbb{C})$.

Symetrie

Jeśli u jest niezerowym wektorem przestrzeni unitarnej V , to na podstawie twierdzenia 5.5.1 mamy rozkład

$$V = \text{lin}\{u\} \oplus \text{lin}\{u\}^\perp$$

i wobec tego dla każdej liczby zespolonej a możemy określić endomorfizm $\sigma_{u,a}$ przestrzeni V , który działa następująco:

$$\sigma_{u,a}(u) = au, \quad \sigma_{u,a}(w) = w \quad \text{dla każdego } w \in \text{lin}\{u\}^\perp.$$

Mamy więc

$$\sigma_{u,a} : V \rightarrow V, \quad \sigma_{u,a}(cu + w) = acu + w \quad \text{dla } c \in \mathbb{C}, w \in \text{lin}\{u\}^\perp.$$

Ponieważ dla liczby zespolonej a takiej, że $a\bar{a} = 1$ mamy

$$\begin{aligned} (\sigma_{u,a}(cu + w), \sigma_{u,a}(cu + w)) &= (acu + w, acu + w) = (acu, acu) + (w, w) \\ &= a\bar{a}(cu, cu) + (w, w) = (cu + w, cu + w) \end{aligned}$$

więc na podstawie lematu 7.5.1 stwierdzamy, że jeśli $|a| = 1$, to endomorfizm $\sigma_{u,a}$ jest izometrią przestrzeni unitarnej V . Izometrię $\sigma_{u,a}$ nazywamy symetrią przestrzeni unitarnej V wzdłuż wektora u .

Zauważmy, że $\sigma_{u,1} = \mathbf{1}_V$ oraz symetria $\sigma_{u,-1}$ jest określona tak samo jak symetria przestrzeni euklidesowej wzdłuż wektora u .

Grupa unitarna

Twierdzenie 7.6.2. Grupa unitarna $\mathcal{U}(V)$ przestrzeni unitarnej V jest generowana przez symetrie. Dokładniej, jeśli $n = \dim V > 1$, to każda izometria przestrzeni unitarnej V jest iloczynem co najwyżej n symetrii.

Dowód. Niech τ będzie izometrią przestrzeni unitarnej V . Na podstawie wniosku 7.5.4 istnieje baza ortonormalna $\mathcal{B} = \{u_1, \dots, u_n\}$ złożona z wektorów własnych, przy czym jeśli $\tau(u_j) = a_j u_j$, to $|a_j| = 1$. Rozpatrzmy symetrie σ_{u_j, a_j} , $j = 1, \dots, n$. Łatwo zauważyć, że

$$\tau = \sigma_{u_1, a_1} \cdots \sigma_{u_n, a_n}.$$

Rzeczywiście, dla każdego wektora bazowego u_j mamy

$$\sigma_{u_1, a_1} \cdots \sigma_{u_n, a_n}(u_j) = \sigma_{u_1, a_1} \cdots \sigma_{u_j, a_j}(u_j) = \sigma_{u_1, a_1} \cdots \sigma_{u_{j-1}, a_{j-1}}(a_j u_j) = a_j u_j = \tau(u_j).$$

i stąd wynika równość $\tau = \sigma_{u_1, a_1} \cdots \sigma_{u_n, a_n}$. $\square$

Uwaga 7.6.1. W przypadku grupy izometrii przestrzeni euklidesowej twierdzenie 4.8.2 o generowaniu tej grupy przez symetrie otrzymaliśmy poprzez zastosowanie twierdzenia Witta mówiącego, że dla każdej pary różnych wektorów u i w przestrzeni euklidesowej V takich, że $\|u\| = \|w\|$ istnieje symetria przestrzeni V przeprowadzająca u na w . Symetrię tę konstruuje się bardzo prosto. Wobec $\|u\| = \|w\|$ mamy $(u, u) = (w, w)$ i stąd wykorzystując symetrię iloczynu skalarnego otrzymujemy $(u - w, u + w) = 0$. Zatem

$$\sigma_{u-w}(u) = \sigma_{u-w}\left(\frac{1}{2}(u - w) + \frac{1}{2}(u + w)\right) = -\frac{1}{2}(u - w) + \frac{1}{2}(u + w) = w. \quad (7.6)$$

To podejście jest całkowicie niedostępne w przypadku przestrzeni unitarnych. Mianowicie w przestrzeni unitarnej V nie jest na ogół prawdą, że jeśli $\|u\| = \|w\|$, to $(u - w, u + w) = 0$. Najprostszy kontrprzykład otrzymuje się następująco. Weźmy dowolny niezerowy wektor $u \in V$ oraz $w = iu \in V$. Wtedy $\|iu\| = |i|\|u\| = \|u\|$, tymczasem

$$(u - iu, u + iu) = ((1 - i)u, (1 + i)u) = (1 - i)^2 \|u\| \neq 0.$$

W książce [9] S. Romana, *Advanced linear algebra*, Springer 2005, sformułowane jest błędne twierdzenie (Theorem 10.11 na str. 214) mówiące, że jeśli $(u, u) = (w, w) \neq 0$, to symetria $\sigma_{u-w, -1}$ przeprowadza u na w . Autor argumentuje, że $(u, u) = (w, w)$ pociąga $(u - w, u + w) = 0$ (co jak wiemy jest fałszywe) i stosuje (7.6). Na tym błędnym twierdzeniu oparte jest źle sformułowane twierdzenie (Theorem 10.12) o generowaniu grupy unitarnej przez symetrie. Sformułowanie i argumentacja użyte przez autora są poprawne w przypadku przestrzeni euklidesowej, ale są fałszywe w przypadku przestrzeni unitarnej. Jak widzimy z twierdzenia 7.6.2 grupę unitarną $\mathcal{U}(V)$ generują wszystkie symetrie $\sigma_{u, a}$ gdzie $|a| = 1$, a nie zbiór takich symetrii z $a = -1$.

7.7 Rozkład biegunowy

Definicja 7.7.1. Endomorfizm samosprzężony σ przestrzeni unitarnej V nazywa się *dodatni*, jeśli spełnia następujący warunek:

$$(\sigma(u), u) \geq 0 \quad \forall u \in U.$$

Na przykład, dla każdego $\rho \in \text{End } V$ endomorfizm $\sigma = \rho\rho^*$ jest samosprzężony i dodatni.

Twierdzenie 7.7.1. (a) *Każdy niezerowy endomorfizm ρ przestrzeni unitarnej V można przedstawić w postaci*

$$\rho = \tau\sigma,$$

gdzie σ jest samosprzężonym endomorfizmem dodatnim i τ jest izometrią przestrzeni V .

(b) *Każdy niezerowy endomorfizm ρ przestrzeni unitarnej V można przedstawić w postaci*

$$\rho = \sigma_1\tau_1,$$

gdzie σ_1 jest samosprzężonym endomorfizmem dodatnim i τ_1 jest izometrią przestrzeni V .

Dowód. (a) Najpierw przypuśćmy, że wymagane przedstawienie endomorfizmu ρ istnieje i poszukajmy wskazówki jak określone muszą być endomorfizmy τ i σ występujące w tym przedstawieniu. Jeśli $\rho = \tau\sigma$, to $\rho^* = \sigma^*\tau^* = \sigma\tau^{-1}$, zatem

$$\rho^*\rho = \sigma\tau^{-1} \cdot \tau\sigma = \sigma^2.$$

A więc σ należy obrać tak, by $\rho^*\rho = \sigma^2$. Ponadto, dla każdego $v \in V$ musimy mieć $\rho(v) = \tau(\sigma(v))$, co pokazuje jak należy określić τ na im σ

Przystępujemy więc do dowodu, że dla endomorfizmu niezerowego ρ istnieje samosprzężony endomorfizm dodatni σ taki, że $\rho^*\rho = \sigma^2$. Najpierw zauważamy, że endomorfizm $\rho^*\rho$ jest samosprzężony, a także dodatni gdyż

$$(\rho^*\rho(u), u) = (\rho(u), \rho(u)) \geq 0 \quad \text{dla każdego } u \in V.$$

Jeśli a jest wartością własną endomorfizmu $\rho^*\rho$, to $a \in \mathbb{R}$ (na podstawie lematu 7.2.3) i jest liczbą nieujemną. Rzeczywiście, jeśli u jest wektorem własnym należącym do wartości własnej a , to $\rho^*\rho(u) = au$ oraz

$$a(u, u) = (au, u) = (\rho^*\rho(u), u) \geq 0$$

skąd wynika, że $a \geq 0$. Niech $u_1, \dots, u_n$ będzie bazą ortonormalną przestrzeni V złożoną z wektorów własnych endomorfizmu $\rho^*\rho(u)$ i niech $\rho^*\rho(u_i) = a_i u_i$ dla $i = 1, \dots, n$. Wtedy a_i są nieujemnymi liczbami rzeczywistymi i możemy zdefiniować endomorfizm σ przestrzeni V wymagając by na bazie $u_1, \dots, u_n$ działał on następująco:

$$\sigma(u_i) = \sqrt{a_i} u_i, \quad i = 1, \dots, n.$$

Wtedy

$$\sigma^2(u_i) = a_i u_i = \rho^*\rho(u_i) \quad \text{dla } i = 1, \dots, n,$$

skąd wynika, że $\sigma^2 = \rho^*\rho$. Należy teraz pokazać, że σ jest samosprzężonym endomorfizmem dodatnim. Samosprzężoność σ wynika stąd, że jest to endomorfizm diagonalizowalny w bazie ortonormalnej i ma rzeczywiste wartości własne (zob. twierdzenie 7.1.3), natomiast dodatniość σ wynika stąd, że σ ma nieujemne wartości własne.

Przystępujemy teraz do konstrukcji endomorfizmu τ . Najpierw zauważmy, że dla każdego $v \in V$ mamy

$$\|\sigma(v)\|^2 = (\sigma(v), \sigma(v)) = (\sigma^2(v), v) = (\rho^*\rho(v), v) = (\rho(v), \rho(v)) = \|\rho(v)\|^2. \quad (7.7)$$

Teraz określimy τ na im σ kładąc

$$\tau(\sigma(v)) = \rho(v) \quad \text{dla } v \in V.$$

Przedstawienie wektora podprzestrzeni im σ w postaci $\sigma(v)$ nie jest na ogół jednoznaczne (chyba, że σ jest bijekcją) i wobec tego musimy sprawdzić dobrą określoność τ na im σ .

Jeśli $\sigma(x) = \sigma(y)$ dla $x, y \in V$, to $\sigma(x - y) = 0$ i wobec tego na podstawie (7.7) mamy $\rho(x - y) = 0$, czyli $\rho(x) = \rho(y)$. Zatem τ jest dobrze określonym odwzorowaniem na $\text{im } \sigma$ i oczywiście $\tau : \text{im } \sigma \rightarrow V$ jest homomorfizmem przestrzeni wektorowych. Można nawet powiedzieć, że τ jest izometrycznym zanurzeniem $\text{im } \sigma$ w przestrzeń V gdyż

$$\|\tau(\sigma(v))\| = \|\rho(v)\| = \|\sigma(v)\|$$

na podstawie (7.7). Rozszerzymy teraz homomorfizm $\tau : \text{im } \sigma \rightarrow V$ do endomorfizmu $\tau : V \rightarrow V$ w następujący sposób. Obieramy bazę ortonormalną $v_1, \dots, v_k$ podprzestrzeni $\text{im } \sigma$. Wtedy $\tau(v_1), \dots, \tau(v_k)$ są parami ortogonalnymi wektorami przestrzeni V . Rozszerzamy $v_1, \dots, v_k$ do bazy ortonormalnej $v_1, \dots, v_k, v_{k+1}, \dots, v_n$ przestrzeni V i rozszerzamy układ $\tau(v_1), \dots, \tau(v_k)$ do bazy ortonormalnej $\tau(v_1), \dots, \tau(v_k), u_{k+1}, \dots, u_n$ przestrzeni V . Rozszerzamy teraz definicję τ do endomorfizmu $\tau : V \rightarrow V$ takiego, że

$$\tau(v_{k+i}) = u_{k+i}, \quad i = 1, \dots, n - k.$$

Endomorfizm τ przeprowadza więc bazę ortonormalną $v_1, \dots, v_k, v_{k+1}, \dots, v_n$ przestrzeni V na bazę ortonormalną $\tau(v_1), \dots, \tau(v_k), u_{k+1}, \dots, u_n$ tej przestrzeni, jest zatem izometrią. Ponadto, $\tau(\sigma(v)) = \rho(v)$ dla każdego $v \in V$, a więc $\tau\sigma = \rho$, gdzie σ jest samosprzężonym endomorfizmem dodatnim zaś τ jest izometrią przestrzeni V .

(b) Na podstawie części (a), dla endomorfizmu ρ^* mamy przedstawienie

$$\rho^* = \tau\sigma,$$

gdzie σ jest samosprzężonym endomorfizmem dodatnim i τ jest izometrią przestrzeni V . Zatem

$$\rho = (\rho^*)^* = \sigma^* \tau^* = \sigma \tau^{-1} = \sigma_1 \tau_1$$

gdzie $\sigma_1 = \sigma$ jest samosprzężonym endomorfizmem dodatnim oraz $\tau_1 = \tau^{-1}$ jest izometrią przestrzeni V . □

Twierdzenie 7.7.1 bywa nazywane twierdzeniem o rozkładzie biegunowym. Jest to kolejna analogia własności endomorfizmów przestrzeni unitarnej i liczb zespolonych. Naśladuje ono przedstawienie niezerowej liczby zespolonej r w postaci $r = ts = st$, gdzie s jest dodatnią liczbą rzeczywistą ($s = |r|$) oraz t jest liczbą zespoloną o module 1.

Rozdział 8

Ciała rzeczywście domknięte

Ostatnie zmiany 6.06.2009 r.

W tym rozdziale przedstawiamy podstawowe pojęcia teorii ciał uporządkowanych. W szczególności dyskutujemy ciała rzeczywście domknięte, które stanowią właściwe dla potrzeb algebry liniowej uogólnienie ciała $\mathbb{R}$ liczb rzeczywistych.

8.1 Ciała formalnie rzeczywiste

Ciało K nazywa się *formalnie rzeczywiste* (lub krótko, *rzeczywiste*) jeśli $-1 \in K$ nie daje się przedstawić jako suma kwadratów elementów ciała K .

Wprowadzamy następujące oznaczenie dla zbioru wszystkich skończonych sum kwadratów niezerowych elementów ciała K :

$$\sum \dot{K}^2 := \{a_1^2 + \dots + a_n^2 \in K : a_1, \dots, a_n \in \dot{K}, n \geq 1\}.$$

Tutaj $\dot{K} = K \setminus \{0\}$ oznacza zbiór różnych od zera elementów ciała K . Zauważmy, że

$$-1 \in \sum \dot{K}^2 \Leftrightarrow 0 \in \sum \dot{K}^2,$$

zatem ciało K jest rzeczywiste wtedy i tylko wtedy gdy $0 \notin \sum \dot{K}^2$.

Oto kilka elementarnych ale ważnych obserwacji o ciałach rzeczywistych.

Uwaga 8.1.1. (a) Ciało formalnie rzeczywiste ma charakterystykę zero.

Mianowicie, jeśli $\text{char } K = p \neq 0$, to $0 = p \cdot 1 = p \cdot 1^2 \in \sum \dot{K}^2$.

(b) Jeśli K jest ciałem formalnie rzeczywistym, to każde podciało F ciała K jest także formalnie rzeczywiste.

Wynika to stąd, że $\sum \dot{F}^2 \subseteq \sum \dot{K}^2$.

(c) Jeśli K jest ciałem formalnie rzeczywistym, to $\sum \dot{K}^2$ jest podgrupą mnożeniową grupy $\dot{K}$.

Rzeczywiście, zbiór $\sum \dot{K}^2$ jest zamknięty ze względu na mnożenie i jeśli $a = \sum a_i^2 \in \sum \dot{K}^2$, to

$$a^{-1} = a \cdot (a^{-1})^2 \in \sum \dot{K}^2,$$

gdyż $\dot{K}^2 \subseteq \sum \dot{K}^2$.

(d) Jeśli K jest ciałem formalnie rzeczywistym i ciało F jest izomorficzne z K , to F jest ciałem formalnie rzeczywistym.

Jeśli bowiem $i : K \rightarrow F$ jest izomorfizmem ciał, to $i(\sum \dot{K}^2) = \sum \dot{F}^2$.

(e) Jeśli K jest ciałem formalnie rzeczywistym oraz $a \in \sum \dot{K}^2$, to $K(\sqrt{a})$ jest ciałem formalnie rzeczywistym.

Niech $a \in \dot{K} \setminus \dot{K}^2$ oraz $E := K(\sqrt{a})$. Jeśli $0 \in \sum \dot{E}^2$, to istnieją $x_i, y_i \in K$, nie wszystkie równe zero, takie, że

$$0 = \sum_i (x_i + y_i \sqrt{a})^2 = \sum_i x_i^2 + a \sum_i y_i^2 + 2 \sum_i x_i y_i \sqrt{a}.$$

Stąd wynika, że $\sum x_i^2 + a \sum y_i^2 = 0$. Wystarczy teraz zauważyć, że $a \in \sum \dot{K}^2$ pociąga $0 \in \sum \dot{K}^2$, wbrew założeniu.

Uwaga 8.1.2. Definicję ciała formalnie rzeczywistego można także sformułować w języku form kwadratowych. Formę kwadratową

$$\varphi(X_1, \dots, X_n) = \sum_{i,j=1}^n a_{ij} X_i X_j$$

o współczynnikach a_{ij} w ciele K nazywamy *nieizotropową* nad ciałem K jeśli równanie

$$\varphi(X_1, \dots, X_n) = 0$$

nie ma niezerowego rozwiązania w ciele K . W przeciwnym razie formę nazywamy *izotropową*. A więc, na przykład, forma $X_1^2 + X_2^2 + X_3^2$ jest nieizotropowa nad ciałem $\mathbb{R}$ liczb rzeczywistych ale jest izotropowa nad ciałem $\mathbb{C}$ liczb zespolonych.

Ciało K jest formalnie rzeczywiste gdy dla każdej liczby naturalnej n forma kwadratowa

$$X_1^2 + X_2^2 + \dots + X_n^2$$

jest nieizotropowa nad ciałem K .

Jednym z głównych tematów teorii ciał formalnie rzeczywistych jest problem zachowania rzeczywistości przy rozszerzeniach ciała. Rozpoczynamy od przypadku rozszerzeń kwadratowych ciał.

STWIERDZENIE 8.1.1. *Niech K będzie ciałem formalnie rzeczywistym. Jeśli $K(\sqrt{a})$ nie jest ciałem formalnie rzeczywistym, to $-a \in \sum \dot{K}^2$.*

Dowód. Jeśli $\sum_i (x_i + y_i \sqrt{a})^2 = 0$ dla pewnych $x_i, y_i \in K$, to $\sum x_i^2 + a \sum y_i^2 = 0$. Zauważmy, że nie wszystkie y_i są równe zero, gdyż przeczyłoby to formalnej rzeczywistości ciała K . Zatem w formalnie rzeczywistym ciele K mamy $\sum y_i^2 \neq 0$ i wobec tego

$$-a = \frac{\sum x_i^2}{\sum y_i^2} \in \sum \dot{K}^2$$

na podstawie uwagi 8.1.1(e). □

TWIERDZENIE 8.1.1. *Niech K będzie ciałem formalnie rzeczywistym i niech $a \in \dot{K} \setminus \dot{K}^2$. Ciało $K(\sqrt{a})$ jest formalnie rzeczywiste wtedy i tylko wtedy gdy $-a \notin \sum \dot{K}^2$.*

Dowód. ¹ It will be more convenient to prove the equivalent statement that the field $K(\sqrt{a})$ is nonreal if and only if $-a \in \sum \dot{K}^2$. By Stwierdzenie 8.1.1, it remains to prove the ‘only if’ part of the statement. So assume $-a \in \sum \dot{K}^2$, and write explicitly $-a = a_1^2 + \dots + a_n^2$, where $a_i \in \dot{K}$. Then $(\sqrt{a})^2 + a_1^2 + \dots + a_n^2 = 0$ showing that the field $K(\sqrt{a})$ is nonreal. □

¹Fragmenty tekstu w języku angielskim pochodzą z mojej książki *Bilinear Algebra*, Gordon and Breach Science Publishers, Amsterdam 1997.

Przykład 8.1.1. We apply the above criterion to the quadratic number field $\mathbb{Q}(\sqrt{a})$, where $a \in \mathbb{Q} \setminus \mathbb{Q}^2$. Observe that a rational number $r \neq 0$ is a sum of squares of rational numbers if and only if $r > 0$. For if $r > 0$ and $r = m/n$, where m and n are positive integers, then $r = mn \cdot (1/n)^2$ is the sum of squares of rational numbers, and, on the other hand, the negative rational numbers clearly are not sums of squares. Thus, by Twierdzenie 8.1.1, the quadratic field $\mathbb{Q}(\sqrt{a})$ is formally real if and only if $a > 0$. While this latter condition is much simpler than the one in Twierdzenie 8.1.1, it uses the fact that $\mathbb{Q}$ is an *ordered* field. Twierdzenie 8.1.1 invokes only the arithmetic structure of the field K and does not presuppose any order structure on K .

In general, we view *number* fields as the subfields of the field $\mathbb{C}$ of complex numbers. Keeping this in mind we can say that the quadratic number field $\mathbb{Q}(\sqrt{a})$ is formally real if and only if it is contained in the field $\mathbb{R}$ of real numbers.

W przypadku rozszerzeń ciał formalnie rzeczywistych stopnia nieparzystego sytuacja jest znacznie prostsza.

Twierdzenie 8.1.2. *Niech E będzie rozszerzeniem stopnia nieparzystego ciała K . Jeśli K jest ciałem formalnie rzeczywistym, to E także jest ciałem formalnie rzeczywistym.*

Na podstawie uwagi 8.1.2 wystarczyłoby udowodnić następujący fakt.

Jeśli ciało E jest rozszerzeniem stopnia nieparzystego ciała K i forma kwadratowa $\varphi = X_1^2 + X_2^2 + \cdots + X_n^2$ jest nieizotropowa nad ciałem K , to forma φ jest także nieizotropowa nad ciałem E .

Okazuje się, że bez większego wysiłku można udowodnić jeszcze ogólniejsze twierdzenie pochodzące od T. A. Springera.

Twierdzenie 8.1.3. (Twierdzenie Springera).

Niech E będzie rozszerzeniem stopnia nieparzystego ciała K o charakterystyce $\neq 2$ i niech $\varphi = a_1X_1^2 + \cdots + a_kX_k^2$ będzie formą kwadratową o współczynnikach z ciała K . Jeśli forma φ jest nieizotropowa nad K , to φ jest nieizotropowa nad E .

Dowód. We induct on the degree $n = [E : K]$. If $n = 1$, there is nothing to prove. So assume $n > 1$ is an odd integer. The field E has a primitive element θ such that $E = K(\theta)$. Thus every element of E has a unique representation as the value $g(\theta)$ of a polynomial $g \in K[t]$ of degree $< n$. We will write f for the minimal polynomial of θ . Thus $f \in K[t]$ is monic irreducible and $f(\theta) = 0$.

Suppose φ is isotropic over E . So there are nonzero polynomials $g_1, \dots, g_k$ in $K[t]$ of degrees $< n$ such that

$$a_1g_1(\theta)^2 + \cdots + a_kg_k(\theta)^2 = 0. \quad (8.1)$$

If the polynomials $g_1, \dots, g_k$ have the greatest common divisor $d \in K[t]$, then $g_i = d \cdot G_i$, $i = 1, \dots, k$, where the polynomials G_i are relatively prime and $d(\theta) \neq 0$, since $\deg d < n$. Then from (8.1) it follows that the polynomials G_i satisfy $a_1G_1(\theta)^2 + \cdots + a_kG_k(\theta)^2 = 0$. Thus we can assume from the beginning that in (8.1) the polynomials $g_1, \dots, g_k$ are relatively prime.

Consider the polynomial $g := a_1g_1^2 + \cdots + a_kg_k^2 \in K[t]$. We have $g(\theta) = 0$, hence g is divisible by the minimal polynomial f of the primitive element θ , that is, $g = f \cdot h$, where $h \in K[t]$. We claim that

(a) $g \neq 0$, and

(b) $\deg h$ is odd and $\deg h < n$.

To prove (a) we show that the highest coefficient of g is a nonzero element of K . So let $m := \max \{ \deg g_i : 1 \leq i \leq k \}$. Then the highest coefficient of g is the value of the form φ at the k -tuple $(c_1, \dots, c_k)$, where c_i is the highest coefficients of the polynomial

g_i if its degree is equal to m , and zero otherwise. Since φ is anisotropic over K , we have $\varphi(c_1, \dots, c_k) \neq 0$, and so g is a nonzero polynomial.

(b) follows from the computation of the degree of g :

$$\deg h + n = \deg h + \deg f = \deg g = 2m < 2n,$$

and from the fact that n is odd.

Now (b) implies that h has an irreducible (over K) factor h_1 of odd degree and $\deg h_1 \leq \deg h < n$. Let θ_1 be a zero of h_1 in an extension field F of K . Then also $h(\theta_1) = 0$ and

$$a_1 g_1(\theta_1)^2 + \dots + a_k g_k(\theta_1)^2 = g(\theta_1) = f(\theta_1)h(\theta_1) = 0.$$

The field $E_1 = K(\theta_1) \subseteq F$ has degree $[E_1 : K] = \deg h_1 < n$, and by induction hypothesis the form φ is anisotropic over E_1 . Hence $g_i(\theta_1) = 0$ for $i = 1, \dots, k$. It follows that the minimal polynomial h_1 of θ_1 divides all the polynomials $g_1, \dots, g_k$, contrary to the fact that they are relatively prime polynomials. Hence (8.1) leads to a contradiction and so φ cannot be isotropic over E . $\square$

Przykład 8.1.2. All cubic extensions of the rational number field $\mathbb{Q}$ are formally real fields (as well as all odd degree extensions of $\mathbb{Q}$). While for quadratic extensions we have observed that $\mathbb{Q}(\sqrt{a})$ is formally real if and only if it is contained in the field $\mathbb{R}$ of real numbers, for cubic number fields the latter is no longer a necessary condition for the reality of the field.

Podstawowe znaczenie w teorii ciał formalnie rzeczywistych mają ciała *rzeczywiście domknięte* (*ang.* real closed fields).

DEFINICJA 8.1.1. Ciało F nazywa się *rzeczywiście domknięte* jeśli ma następujące dwie własności:

- (a) F jest formalnie rzeczywiste.
- (b) Każde formalnie rzeczywiste algebraiczne rozszerzenie K ciała F jest równe F .

In other words, a real field F is real closed if it has no proper algebraic extensions that are formally real fields. A real closed field is closed with respect to reality of the field: no proper algebraic extension of the field can be a real field. We recognize the prototype of a real closed field: it is the real field $\mathbb{R}$. It has just one proper algebraic extension, the field $\mathbb{C}$ of complex numbers, and the extension is a nonreal field. However basic this example is, it is far from being isolated.

TWIERDZENIE 8.1.4. Dla każdego formalnie rzeczywistego ciała K istnieje rozszerzenie algebraiczne F ciała K , które jest ciałem *rzeczywiście domkniętym*.

Dowód. We consider the family $\mathcal{F}$ of all formally real algebraic extensions of the field K contained in a fixed algebraic closure $\bar{K}$ of K . The family $\mathcal{F}$ is nonempty, since $K \in \mathcal{F}$. We view $\mathcal{F}$ as a partially ordered set with the field inclusion as the partial ordering relation. A maximal element F in $\mathcal{F}$, if it exists, is a formally real algebraic extension of K with no proper formally real algebraic extensions (by the maximality of F). Hence F , if it exists, is a real closed field containing K . The proof is thus reduced to showing that the family $\mathcal{F}$ has a maximal element, and for this we will use the Kuratowski-Zorn Lemma.

Let $\mathcal{C} := \{E_a : a \in A\}$ be a chain in $\mathcal{F}$ (that is, $E_a \in \mathcal{F}$ for all $a \in A$, and $E_a \subseteq E_b$ or $E_b \subseteq E_a$ for all $a, b \in A$). We must show that every such $\mathcal{C}$ is bounded in $\mathcal{F}$, that is, there is an $E \in \mathcal{F}$ such that $E_a \subseteq E$ for all $a \in A$. A natural candidate for E is the union of all fields in $\mathcal{C}$:

$$E := \bigcup \{E_a : a \in A\}.$$

It certainly contains all the E_a , $a \in A$, and it remains to show that $E \in \mathcal{F}$. First of all, we show that E is a field. So let $x, y \in E$. Then there are $a, b \in A$ such that $x \in E_a$ and $y \in E_b$, and since $\mathcal{C}$ is a chain, we have either $E_a \subseteq E_b$ or $E_b \subseteq E_a$. In the first case $x, y \in E_b$, in the second, $x, y \in E_a$. Thus either $x - y \in E_b$ or $x - y \in E_a$, and it follows that always $x - y \in E$. Similarly, $x/y \in E$, if $y \neq 0$, showing that E is a subfield of $\bar{K}$.

Now we prove that E is a formally real field. Suppose not, and let

$-1 = x_1^2 + \cdots + x_n^2$, with the x_i 's in E . Then each x_i lies in a field $E_{a(i)}$ of the chain $\mathcal{C}$. Since $\mathcal{C}$ is a chain, one of the fields $E_{a(i)}$, call it E_a , contains all the others, and then E_a contains all the x_i 's. It follows that E_a is a nonreal field, a contradiction.

Thus we have proved that the field E is an upper bound for the chain $\mathcal{C}$ and $E \in \mathcal{F}$. By the Kuratowski-Zorn Lemma, the family $\mathcal{F}$ contains a maximal element F , and this is a real closed field containing K . $\square$

WNIOSEK 8.1.1. *Jeśli F jest ciałem rzeczywiście domkniętym, to:*

(a) $\sum \dot{F}^2 = \dot{F}^2$.

(b) $|\dot{F}/\dot{F}^2| = 2$.

(c) *Każdy wielomian $f \in F[t]$ stopnia nieparzystego ma pierwiastek w ciele F .*

Dowód. (a) Suppose $a \in \sum \dot{F}^2 \setminus \dot{F}^2$. Then $F(\sqrt{a})$ is a quadratic extension of F and, by Uwaga 8.1.1(e), it is a formally real field, contrary to the hypothesis that F is real closed.

(b) Clearly, $\dot{F} \neq \dot{F}^2$. Suppose that $|\dot{F}/\dot{F}^2| \geq 4$. Then there is an $a \in \dot{F}$ such that $1, -1, a, -a$ lie in four distinct square classes of F . Thus $a \notin \dot{F}^2$ and $-a \notin \dot{F}^2 = \sum \dot{F}^2$, the latter by (a). Hence, by Theorem 8.1.1, $F(\sqrt{a})$ is a formally real quadratic extension of F , a contradiction.

(c) A polynomial $f \in F[t]$ of odd degree must have a factor h of odd degree which is irreducible over F . If θ is a zero of h in an extension field of F , then $F(\theta)$ is a formally real extension of F (by Theorem 8.1.2). Thus $F(\theta) = F$ and $\theta \in F$, as required. $\square$

Uwaga 8.1.3. Ciało K nazywa się ciałem *pitagorejskim* jeśli $\sum \dot{K}^2 = \dot{K}^2$. A więc, na podstawie wniosku 8.1.1, każde ciało rzeczywiście domknięte jest ciałem pitagorejskim.

Uwaga 8.1.4. Można udowodnić następujący kluczowy fakt:

Jeśli F jest ciałem rzeczywiście domkniętym, to jego kwadratowe rozszerzenie $F(\sqrt{-1})$ jest ciałem algebraicznie domkniętym.

Dowód można znaleźć w książce S. Lang, *Algebra*, PWN Warszawa 1973, na str. 224–225, 302.

8.2 Ciała uporządkowane

Ciało K nazywa się ciałem uporządkowanym przez relację binarną $>$ określoną na ciele K , jeśli dla wszystkich $a, b, c \in K$,

$$a > b \quad \text{ i } \quad b > c \Rightarrow a > c,$$

$$a > b \quad \text{ albo } \quad a = b \quad \text{ albo } \quad b > a,$$

$$a > b \Rightarrow a + c > b + c,$$

$$a > b \quad \text{ i } \quad c > 0 \Rightarrow ac > bc.$$

Nie możemy wykluczyć, że ciało K ma więcej niż jedną relację porządkującą i wobec tego piszemy $(K, >)$ dla zaznaczenia, że K jest uporządkowane przez relację $>$.

Jeśli $(K, >)$ jest ciałem uporządkowanym, to specjalną rolę grają elementy *dodatnie* w porządku $>$, a więc elementy zbioru

$$P := \{x \in K : x > 0\}.$$

Zauważmy, że dla $a, b \in K$,

$$a > b \Leftrightarrow a + (-b) > b + (-b) \Leftrightarrow a - b > 0 \Leftrightarrow a - b \in P.$$

Oznacza to, że zbiór P elementów dodatnich w porządku $>$ ciała K charakteryzuje kompletnie relację porządkującą $>$ na ciele K . W związku z tym piszemy także (K, P) zamiast $(K, >)$ i zbiór P nazywamy *porządkiem* ciała K .

A więc porządek P ciała K jest podzbiorem ciała K . Nasuwa się oczywiste pytanie jak rozpoznać podzbiory P ciała K , które są faktycznie porządkami ciała K ? Okazuje się, że istnieje w pełni satysfakcjonująca odpowiedź na to pytanie.

TWIERDZENIE 8.2.1. *Niech P będzie podzbiorem ciała K . Na to by istniała relacja porządkująca $>$ na ciele K ze zbiorem elementów dodatnich P potrzeba i wystarcza by zbiór P miał następujące własności:*

- (1) $P + P \subseteq P$,
- (2) $P \cdot P \subseteq P$,
- (3) $P \cup -P = \dot{K}$,

gdzie $-P := \{x \in K : -x \in P\}$.

Dowód. Let P be the set of positive elements of an ordered field $(K, >)$. If $a, b \in P$, then $a + b > 0$ and $ab > 0$ by compatibility of $>$ with addition and multiplication in K . Thus $a + b \in P$ and $ab \in P$. This proves properties (1) and (2) of P .

To prove (3), take any $a \in \dot{K}$. By the trichotomy property of the relation $>$ we have either $a > 0$ or $0 > a$, that is, either $a \in P$ or $-a \in P$, as desired.

Now let us assume that the subset $P \subseteq K$ has properties (1), (2) and (3). We define the binary relation $>$ on K be setting

$$a > b \quad :\Leftrightarrow \quad a - b \in P.$$

We now show that the relation $>$ has the four properties defining an ordering relation on K . So let $a, b, c \in K$ and assume first that $a > b$ and $b > c$. Then $a - b \in P$ and $b - c \in P$, and since P is closed under addition by (1), we have $a - c = (a - b) + (b - c) \in P$. Thus $a > c$ and the relation $>$ is transitive.

If $a \neq b$, then $a - b \in \dot{K} = P \cup -P$. Hence either $a - b \in P$ and $a > b$, or $a - b \in -P$ and $b > a$. To prove trichotomy for $>$ we have to verify that we cannot have simultaneously $a > b$ and $b > a$. This will follow from the fact that P and $-P$ are disjoint sets: $P \cap -P = \emptyset$. Contrary to this, let us suppose that there is an $x \in P$ with $-x \in P$. Then $0 = x + (-x) \in P$, according to (1), and this contradicts (3).

It remains to prove compatibility of $>$ with addition and multiplication in K . Suppose $a > b$. Then $(a + c) - (b + c) = a - b \in P$ and if $c > 0$ then $ac - bc = (a - b)c \in P$, showing that $a + c > b + c$ and $ac > bc$, as required. $\square$

Uwaga 8.2.1. Wobec twierdzenia 8.2.1 podzbiór P ciała K jest porządkiem ciała K , jeśli spełnia warunki (1), (2), (3) twierdzenia 8.2.1. A oto lista dalszych elementarnych obserwacji o porządkach ciał.

(4) Jeśli P jest porządkiem ciała K , to $\dot{K}^2 \subseteq P$ oraz $\sum \dot{K}^2 \subseteq P$.

For if $a \in \dot{K}$, then either $a \in P$ or $-a \in P$. If $a \in P$, then by (2), $a^2 \in P$, and if $-a \in P$, then again by (2), $a^2 = (-a)(-a) \in P$. Hence $\dot{K}^2 \subseteq P$ and from this and (1) it follows that $\sum \dot{K}^2 \subseteq P$.

(5) Jeśli K jest ciałem uporządkowanym, to K jest ciałem formalnie rzeczywistym oraz $\text{char } K = 0$.

If P is an ordering of K , then $\sum \dot{K}^2 \subseteq P \subseteq \dot{K}$, by (3) and (4). Hence $0 \notin \sum \dot{K}^2$. And $\text{char } K = 0$, by Remark 8.1.1(a).

(6) Jeśli P jest porządkiem ciała K , to P jest podgrupą mnożeń grupy $\dot{K}$ ciała K o indeksie dwa: $[\dot{K} : P] = 2$.

P is a subset of $\dot{K}$ (by (3)), is closed under multiplication (by (2)) and contains the squares (by (4)). Hence for each $a \in P$, we have $a^{-1} = a \cdot (1/a)^2 \in P$. Thus P is a subgroup of $\dot{K}$. We have shown in the proof of Theorem 8.2.1 that $P \cap -P = \emptyset$, so that (3) is the decomposition of the group $\dot{K}$ into cosets modulo the subgroup P . Thus $[\dot{K} : P] = 2$.

(7) Jeśli P i P' są dwoma porządkami ciała K oraz $P \subseteq P'$, to $P = P'$. Inaczej mówiąc, różne porządki są nieporównywalne.

Suppose $P \subseteq P'$ and $P \neq P'$. Choose an $x \in P' \setminus P$. Then, by (3), $-x \in P$ and so $x, -x \in P'$, whence $0 = x + (-x) \in P'$, a contradiction.

(8) Jeśli μ jest automorfizmem ciała K i P jest porządkiem ciała K , to $\mu(P)$ jest także porządkiem ciała K .

Verifying (1), (2) and (3) for $\mu(P)$ is easy and is left to the reader. It is worthwhile to observe that (8) can be used to produce examples of fields with more than one ordering.

(9) Jeśli ciało E jest rozszerzeniem ciała K i Q jest porządkiem ciała E , to $P := Q \cap K$ jest porządkiem ciała K .

Porządek $P = Q \cap K$ ciała K nazywa się porządkiem *indukowanym* przez porządek Q ciała E .

Easy verification that P satisfies (1), (2) and (3) is left to the reader.

(10) Ciało $\mathbb{C}$ liczb zespolonych nie jest ciałem uporządkowanym.

Ciało $\mathbb{R}$ liczb rzeczywistych ma dokładnie jeden porządek $P = \dot{\mathbb{R}}^2$.

Ciało rzeczywście domknięte F ma dokładnie jeden porządek $P = \dot{F}^2$.

Ciało $\mathbb{Q}$ liczb wymiernych ma dokładnie jeden porządek $P = \sum \dot{\mathbb{Q}}^2$ indukowany przez jedyny porządek ciała $\mathbb{R}$.

$\mathbb{C}$ nie jest ciałem formalnie rzeczywistym, zatem nie jest ciałem uporządkowanym na podstawie (5).

Jeśli P jest porządkiem ciała $\mathbb{R}$, to $\dot{\mathbb{R}}^2 \subseteq P$ na podstawie (4). Tymczasem $\dot{\mathbb{R}}^2$ jest porządkiem ciała $\mathbb{R}$, gdyż zbiór ten oczywiście spełnia warunki (1), (2), (3). Zatem $\dot{\mathbb{R}}^2 = P$ na podstawie (7). Ta argumentacja stosuje się do dowolnego ciała rzeczywście domkniętego F .

Jeśli P jest porządkiem ciała $\mathbb{Q}$, to $S := \sum \dot{\mathbb{Q}}^2 \subseteq P$. Na podstawie (7) wystarczy sprawdzić, że S jest porządkiem ciała $\mathbb{Q}$. Zbiór S jest oczywiście zamknięty ze względu na dodawanie i mnożenie. Aby sprawdzić (3) obieramy różną od zera liczbę wymierną $r = m/n$, gdzie m i n są liczbami całkowitymi i $n > 0$. Wtedy $r \in S$ gdy $m > 0$ (zobacz przykład 8.1.1) oraz $r \in -S$ gdy $m < 0$. Stąd wynika, że $S \cup -S = \dot{\mathbb{Q}}$. Zatem S jest porządkiem ciała $\mathbb{Q}$.

Udowodnimy teraz tak zwane pierwsze twierdzenie Artina-Schreiera, które wyjaśnia ostatecznie związek pomiędzy ciałami formalnie rzeczywistymi i ciałami uporządkowanymi.

TWIERDZENIE 8.2.2. *Ciało K jest ciałem uporządkowanym wtedy i tylko wtedy gdy jest ciałem formalnie rzeczywistym.*

Dowód. We have already observed that an ordered field is formally real. Now we prove the converse. So let us assume that K is a formally real field. Then, by Theorem 8.1.4, there exists a real closed field F containing K . But a real closed field is uniquely ordered (by Uwaga 8.2.1.(10)), hence F induces an ordering on its subfield K (by Uwaga 8.2.1.(9)). Thus K is an ordered field. $\square$

In view of this result we will use interchangeably the phrases ‘formally real’ and ‘ordered’, unless we want to work with a specified ordering of the real field K . The first Artin-Schreier theorem can be restated as follows.

WNIOSEK 8.2.1. *Ciało K ma przynajmniej jeden porządek wtedy i tylko wtedy gdy*

$$-1 \notin \sum \dot{K}^2.$$

Drugie podstawowe twierdzenie Artina-Schreiera podaje arytmetyczną charakteryzację elementów totalnie dodatnich ciała formalnie rzeczywistego K .

DEFINICJA 8.2.1. Niech K będzie dowolnym ciałem. Element $a \in K$ nazywa się *totalnie dodatni*, jeśli jest dodatni w każdym porządku ciała K .

This definition is somewhat tricky since we speak about orderings of an *arbitrary* field K . Traditionally, it is meant that in a nonreal field K (having no orderings) *every* field element is totally positive, that is, it is meant that the condition put on all orderings is automatically satisfied when there are no orderings at all. This trick allows simultaneous formulation of results for real and nonreal fields as exemplified in the second Artin-Schreier theorem below.

Returning to totally positive elements, it is an interesting problem to find all totally positive elements of a field. This becomes trivial when the field has a unique ordering (or has no orderings), but it looks hopelessly in the general case. It seems that first we have to find *all* orderings of the field, and only then, taking their intersection, we can get a hold on totally positive elements. However, it turns out that there is a simpler and more elegant solution to this problem. Notice that by Remark 8.2.1(4), $\sum \dot{K}^2 \subseteq P$ for *every* ordering P of the real field K . Hence nonzero sums of squares in K are examples of totally positive elements of K . The second Artin-Schreier theorem asserts that there are no more totally positive elements in K .

TWIERDZENIE 8.2.3. *Niech K będzie ciałem o charakterystyce $\neq 2$. Element $a \in K$ jest totalnie dodatni wtedy i tylko wtedy gdy $a \in \sum \dot{K}^2$.*

Dowód. First we dispose of the case of a nonreal field K . We have agreed that all elements of a nonreal field are totally positive. On the other hand, every element of a nonreal field can be written as a sum of squares of nonzero elements of the field.

Thus in the rest of proof we assume that K is a formally real field. It is sufficient to show that every totally positive element of K belongs to $\sum \dot{K}^2$. Contrary to this, suppose that $a \in K$ is totally positive and is not a sum of squares in K . Then the field $K(\sqrt{-a})$ is formally real (by Theorem 8.1.1), hence, by the first Artin-Schreier Theorem 8.2.2, it has an ordering P' , say. Observe that, by Remark 8.2.1.(4), $-a = (\sqrt{-a})^2 \in P'$.

On the other hand, let $P := K \cap P'$ be the ordering of K induced by P' . Then $a \in P$, since a is totally positive, and $-a \in P$, since $-a \in P'$. But P is closed under addition, hence $0 = a + (-a) \in P$, a contradiction. This proves that $a \in \sum \dot{K}^2$, as required. $\square$

Uwaga 8.2.2. We have excluded fields of characteristic two, since when $\text{char } K = 2$, then $\sum \dot{K}^2 = K^2$, and the squares need not comprise all of K .

We will often use the set of *all* orderings of a field K and so we introduce the symbol $X(K)$ for that set. Thus $P \in X(K)$ means that P is an ordering of the field K , and $X(K) \neq \emptyset$ if and only if K is a formally real field. The set of all totally positive elements of K can be written as $\bigcap \{ P : P \in X(K) \}$, and the second Artin-Schreier theorem asserts that, if $\text{char } K \neq 2$, then

$$\bigcap \{ P : P \in X(K) \} = \sum \dot{K}^2.$$

The following definition introduces an arithmetic invariant of a field with an immediate interpretation in theory of formally real fields.

DEFINICJA 8.2.2. Let K be an arbitrary field. The *Pythagoras number* of the field K is the smallest positive integer $p = p(K)$, with the property that every sum of nonzero squares in K can be written as the sum of p squares in K . If such a number p does not exist, we say that K has infinite Pythagoras number and write $p(K) = \infty$.

The determination of $p(K)$ is, in general, a challenging problem. We discuss first the easiest cases.

Przykład 8.2.1. When $\text{char } K = 2$, then every sum of squares in K is a square in K , hence $p(K) = 1$, a case of no further interest.

So assume K is a nonreal field and $\text{char } K \neq 2$. Clearly, $s(K) \leq p(K)$, and on the other hand, for each $a \in K$, we have the identity

$$a = (a+1)^2/4 + (-1)(a-1)^2/4,$$

showing that a can be written as the sum of $s(K)+1$ squares in K . Thus for every nonreal field K ,

$$s(K) \leq p(K) \leq s(K) + 1.$$

In particular, when K has odd characteristic p , then K contains the prime field $\mathbb{F}_p$ and so we have the inequality $s(K) \leq s(\mathbb{F}_p) \leq 2$ for the level of K . Thus for every field K of odd characteristic,

$$1 \leq s(K) \leq p(K) \leq s(K) + 1 \leq 3.$$

Another obvious observation is that for K a formally real field, $p(K) = 1$ is equivalent to saying that K is a Pythagorean field (see Remark 8.1.3). Every real closed field has Pythagoras number 1.

Less trivial is determination of $p(\mathbb{Q})$. A classic result in number theory asserts that every positive integer is the sum of four squares of integers (Lagrange's theorem). An easy consequence is that $p(\mathbb{Q}) = 4$. A more general result of C.L. Siegel establishes that $p(K) = 2, 3$ or 4 for every algebraic number field K .

Uwaga 8.2.3. The problem of determining the Pythagoras number of the rational function field $K_n := \mathbb{R}(X_1, \dots, X_n)$ in n indeterminates over the reals turns out to be extremely difficult and remains open for $n > 2$. For $n = 1$, the only case tractable by elementary methods, one shows that $p(K_1) = 2$. The following estimates hold for $n \geq 1$:

$$n + 1 \leq p(K_n) \leq 2^n.$$

The lower estimate was proved by J.W.S. Cassels in 1964, the upper by A. Pfister in 1967. For $n = 2$ these estimates give $p(K_2) = 3$ or 4 , but deciding which one of the two is the true value of $p(K_2)$ turned out to be a very difficult task. In 1971 J.W.S. Cassels, W.J. Ellison and A. Pfister proved eventually that $p(K_2) = 4$. Their proof uses sophisticated methods of theory of elliptic curves over function fields and does not generalize to $n > 2$. To show that $p(K_2) = 4$ it suffices to point out a rational function $f \in K_2$ which is totally positive (and so a sum of squares in K_2) but cannot be represented as the sum of three squares in K_2 . Cassels, Ellison and Pfister's choice is

$$f = 1 + X^2Y^4 + X^4Y^2 - 3X^2Y^2.$$

The fact that f is the sum of squares in $\mathbb{R}(X, Y)$ follows from the identity

$$(1 + X^2) \cdot f = (1 - X^2Y^2)^2 + X^2(1 - Y^2)^2 + X^2Y^2(1 - X^2)^2.$$

It is amazing that the machinery of elliptic curves is needed to show that the polynomial f is not representable as the sum of 3 squares in the function field $\mathbb{R}(X, Y)$, seemingly an elementary problem. Another surprising property of the polynomial f is that, even though it is a sum of squares of rational functions, it cannot be expressed as the sum of squares of (any number of) polynomials in $\mathbb{R}[X, Y]$!

There is a conjecture that $p(K_n) = 2^n$ for all n , but no progress has been achieved for $n \geq 3$.

The Pythagoras number can be defined for any commutative ring R (just replace in Definition 8.2.2 the field K with R). Thus, for instance, $p(\mathbb{Z}) = 4$ by Lagrange's theorem. Here the ring $\mathbb{Z}$ and its field of quotients $\mathbb{Q}$ have equal Pythagoras numbers. This is not always so. M. D. Choi, Z. D. Dai, T. Y. Lam and B. Reznick proved in 1982 that the polynomial ring $\mathbb{R}[X_1, \dots, X_n]$ in $n \geq 2$ indeterminates over the reals has *infinite* Pythagoras number, while for its field of quotients K_n we have the Pfister's bound $p(K_n) \leq 2^n$.

8.3 Rzeczywiste domknięcie ciała uporządkowanego

Now we return to real closed fields. We have seen that, given a formally real field K , there exists a real closed extension field F of K inducing on K an ordering (see proof of Theorem 8.2.2). We are going to analyze this connection more closely and to establish that, in fact, all orderings of a real field K are induced by real closed fields.

We fix an ordering P of the field K and consider the extension field E of K obtained by adjoining to K the square roots of all elements of P :

$$E = K(\sqrt{P}) := K(\{\sqrt{p} : p \in P\}).$$

The field E will play a role in the construction of a real closed field inducing on K the ordering P . Recall that the elements of E are of the form

$$\frac{f(s_1, \dots, s_m)}{g(s_1, \dots, s_m)},$$

where f and g are polynomials in $m \geq 1$ indeterminates with coefficients in K and $s_1, \dots, s_m \in \{\sqrt{p} : p \in P\}$ are square roots of elements of P with $g(s_1, \dots, s_m) \neq 0$.

It follows that each element $a \in E$ belongs to a *finite* extension of K of the form $K(\sqrt{p_1}, \dots, \sqrt{p_k})$, where $p_1, \dots, p_k \in P$.

STWIERDZENIE 8.3.1. *Niech (K, P) będzie ciałem uporządkowanym. Wtedy rozszerzenie $E = K(\sqrt{P})$ ciała K jest ciałem formalnie rzeczywistym.*

Dowód. We claim that E has the following property: for all $b_1, \dots, b_n \in P$ and all $a_1, \dots, a_n \in \dot{E}$,

$$b_1 a_1^2 + \dots + b_n a_n^2 \neq 0.$$

Clearly, for $b_1 = \dots = b_n = 1$, this property implies that E is a formally real field.

Suppose that E does not have the required property. Then there are $b_1, \dots, b_n \in P$ and $a_1, \dots, a_n \in \dot{E}$ such that

$$b_1 a_1^2 + \dots + b_n a_n^2 = 0. \quad (8.2)$$

Each a_i in (8.2) is contained in a finite extension $K(\sqrt{p_1}, \dots, \sqrt{p_k})$ with the $p_i \in P$. Hence there are also $p_1, \dots, p_m \in P$ such that simultaneously

$$a_1, \dots, a_n \in K(\sqrt{p_1}, \dots, \sqrt{p_m}). \quad (8.3)$$

The number m of square roots of elements of P needed here is not uniquely determined, but each set of the a_i 's certainly determines the smallest number m of square roots needed in (8.3). Now we select the sets $b_1, \dots, b_n \in P$ and $a_1, \dots, a_n \in \dot{E}$ with the property that they satisfy (8.2) and the corresponding number m in (8.3) is smallest possible. We are going to reach a contradiction by constructing another relation of the type (8.2) requiring only $m - 1$ square roots in (8.3).

Certainly $m \geq 1$, since when $m = 0$, we have $K(\sqrt{p_1}, \dots, \sqrt{p_m}) = K$ and by (8.3) all the $a_i \in \dot{K}$, hence $b_1 a_1^2 + \dots + b_n a_n^2 \in P$, contrary to (8.2).

The field $K(\sqrt{p_1}, \dots, \sqrt{p_m})$ can be viewed as a quadratic extension

$$K(\sqrt{p_1}, \dots, \sqrt{p_m}) = K^*(\sqrt{p_m})$$

of the field $K^* := K(\sqrt{p_1}, \dots, \sqrt{p_{m-1}})$. Here $K^*(\sqrt{p_m})$ is a quadratic extension of K^* , since otherwise we would have $K^*(\sqrt{p_m}) = K^*$, contrary to the choice of the number m . Thus we can write

$$a_i = x_i + y_i \sqrt{p_m}, \quad x_i, y_i \in K^*, \quad i = 1, \dots, n.$$

Now (8.2) can be written in the following form

$$0 = \sum b_i a_i^2 = \sum (b_i x_i^2 + b_i p_m y_i^2) + 2\sqrt{p_m} \sum b_i x_i y_i,$$

and it follows that

$$\sum (b_i x_i^2 + b_i p_m y_i^2) = 0.$$

Here we have obtained a relation of the type (8.2), where all the b_i and $b_i p_m$ are in P and $x_i, y_i \in K^* = K(\sqrt{p_1}, \dots, \sqrt{p_{m-1}})$. This, however, contradicts our choice of the number m . Thus relations (8.2) are impossible in E and so E is a formally real field. $\square$

Now we come to the theorem on inducing orderings of a real field by the real closed fields.

TWIERDZENIE 8.3.1. *Niech K będzie ciałem formalnie rzeczywistym i niech P będzie porządkiem ciała K . Wtedy istnieje ciało F o następujących własnościach:*

- (a) *F jest rzeczywiście domkniętym algebraicznym rozszerzeniem ciała K ,*
- (b) *F indukuje porządek P na K , to znaczy, $P = K \cap \dot{F}^2$.*

Dowód. Let $E := K(\sqrt{P})$. By Proposition 8.3.1, E is a formally real field, hence, by Theorem 8.1.4, there exists a real closed algebraic extension F of the field E . Thus we have the tower of algebraic extensions $K \subseteq E \subseteq F$, and so F is an algebraic extension of K . This proves (a).

Now let $P' = K \cap \dot{F}^2$ be the ordering of K induced by the unique ordering $\dot{F}^2$ of F . We show that $P = P'$ and for this it suffices to show that $P \subseteq P'$ (by Remark 8.2.1(7)). So let $p \in P$. Then $p = (\sqrt{p})^2 \in \dot{E}^2$, hence also $p \in \dot{F}^2$. Thus $p \in K \cap \dot{F}^2 = P'$, showing that $P \subseteq P'$. This proves (b). $\square$

DEFINICJA 8.3.1. Rzeczywiście domknięte algebraiczne rozszerzenie F ciała K indukujące porządek P na ciele K nazywa się *rzeczywistym domknięciem* ciała uporządkowanego (K, P) .

Thus we have proved that every ordered field has a real closure. As to the uniqueness, E. Artin and O. Schreier proved that any two real closures F_1 and F_2 of an ordered field (K, P) are isomorphic over K . In fact, there is a unique isomorphism between F_1 and F_2 which is identity on K . For a proof, see S. Lang's *Algebra*, p. 277. Thus we can speak of *the* real closure of an ordered field.

Przykład 8.3.1. We show here that the field $K = \mathbb{Q}(t)$ of rational functions in one indeterminate t over the field of rational numbers $\mathbb{Q}$ has infinitely many (in fact, uncountably many) orderings, hence also infinitely many pairwise nonisomorphic real closures.

The idea is to associate with every transcendental real number α an ordering of the field K . If $\alpha \in \mathbb{R}$ is a transcendental number and $g \in \mathbb{Q}[t]$ is a nonzero polynomial, then the value $g(\alpha)$ is a nonzero real number. Hence, given a rational function $h = f/g \in \mathbb{Q}(t)$, where $f, g \in \mathbb{Q}[t]$ and $g \neq 0$, we can consider the value $h(\alpha) = f(\alpha)/g(\alpha)$ of the rational function h at the point α . We now set

$$P_\alpha := \{ h \in K : h(\alpha) > 0 \},$$

where $>$ is the order relation in the real field $\mathbb{R}$. It is easy to verify that

$$P_\alpha + P_\alpha \subseteq P_\alpha, \quad P_\alpha \cdot P_\alpha \subseteq P_\alpha, \quad P_\alpha \cup -P_\alpha = \dot{K}.$$

Thus P_α is an ordering of K . Now we show that, if α and β are real transcendental numbers and $\alpha \neq \beta$, then $P_\alpha \neq P_\beta$.

Let, say, $\alpha < \beta$ (an inequality in $\mathbb{R}$). Then there exists a rational number a such that $\alpha < a < \beta$. Consider the polynomial $h = t - a \in K$. We have $h(\alpha) = \alpha - a < 0$, hence $h \notin P_\alpha$. On the other hand, we have $h(\beta) = \beta - a > 0$, hence $h \in P_\beta$. This shows that $P_\alpha \neq P_\beta$.

We have established that the assignment $\alpha \mapsto P_\alpha$ is an injective map from the set $\mathcal{T}$ of all real transcendental numbers into the set $X(K)$ of all orderings of K . Since $\mathcal{T}$ is known to be uncountable, it follows that so is $X(K)$.

Let K_α and K_β be the real closures of K inducing the orderings P_α and P_β on K . If there exists a field isomorphism $i : K_\alpha \rightarrow K_\beta$ over K (i.e., leaving fixed every element of K), then

$$P_\alpha = i(P_\alpha) = K \cap i(\dot{K}_\alpha^2) = K \cap \dot{K}_\beta^2 = P_\beta.$$

Hence for distinct transcendental numbers α and β the real closures K_α and K_β are nonisomorphic over K . Thus the field $K = \mathbb{Q}(t)$ has infinitely many real closures pairwise nonisomorphic over K .

Rozdział 9

Ogólne przestrzenie euklidesowe i unitarne

Ostatnie zmiany 30.05.2009 r.

Główne twierdzenia tego cyklu wykładów dotyczą endomorfizmów przestrzeni euklidesowych i unitarnych. Oczywiście w twierdzeniach tych wykorzystujemy pewne kluczowe własności ciała liczb rzeczywistych $\mathbb{R}$ i ciała liczb zespolonych $\mathbb{C}$. Najprostszym przykładem są twierdzenia o istnieniu wartości własnych endomorfizmów samosprężonych, które są konsekwencją algebraicznej domkniętości $\mathbb{C}$ oraz rzeczywistej domkniętości $\mathbb{R}$. Okazuje się, że w całym wykładzie korzystaliśmy wyłącznie z takich własności ciała $\mathbb{R}$, które mają wszystkie ciała rzeczywwiście domknięte. Ponadto, własności ciała $\mathbb{C}$, które są podstawą twierdzeń o endomorfizmach przestrzeni unitarnych, redukują się do dwóch faktów: (a) $\mathbb{C} = \mathbb{R}(i)$, to znaczy, $\mathbb{C}$ jest kwadratowym rozszerzeniem $\mathbb{R}$ o $\sqrt{-1}$, oraz (b) $\mathbb{C}$ jest ciałem algebraicznie domkniętym. Jeśli F jest dowolnym ciałem rzeczywwiście domkniętym, to na podstawie uwagi 8.1.4, ciało $F(\sqrt{-1})$ jest ciałem algebraicznie domkniętym. Tak więc ciało $F(\sqrt{-1})$ jest dokładnie w takiej samej relacji do ciała rzeczywwiście domkniętego F jak ciało $\mathbb{C}$ do ciała $\mathbb{R}$.

Te obserwacje pozwalają stwierdzić, że wszystkie pojęcia zdefiniowane dla przestrzeni euklidesowych i wszystkie twierdzenia o endomorfizmach przestrzeni euklidesowych pozostają w mocy, jeśli zastąpić w nich ciało liczb rzeczywistych $\mathbb{R}$ dowolnym ciałem rzeczywwiście domkniętym F . Podobnie, wszystkie pojęcia zdefiniowane dla przestrzeni unitarnych i wszystkie twierdzenia o endomorfizmach przestrzeni unitarnych pozostają w mocy, jeśli zastąpić w nich ciało liczb zespolonych $\mathbb{C}$ kwadratowym rozszerzeniem $F(\sqrt{-1})$ dowolnego ciała rzeczywwiście domkniętego.

Jako przykład takiego podejścia sformułujemy niektóre definicje i ważniejsze twierdzenia w ich optymalnej ogólności.

DEFINICJA. Przestrzenią *euklidesową* nazywamy skończenie wymiarową przestrzeń dwuliniową V nad ciałem rzeczywwiście domkniętym F z dodatnio określonym symetrycznym funkcyjonałem dwuliniowym

$$(\ , \) : V \times V \rightarrow F$$

zwanym iloczynem skalarnym na przestrzeni V .

Tutaj dodatnią określoność iloczynu skalarnego rozumiemy następująco: dla każdego niezerowego wektora $v \in V$ wartość iloczynu skalarnego (v, v) jest *dodatnim* elementem ciała F (a więc (v, v) jest kwadratem pewnego niezerowego elementu ciała F). Tak jak w rozdziale 3 definiujemy normę wektora, dowodzimy nierówności Cauchy'ego-Schwarza oraz istnienia baz ortonormalnych. Wszystkie rezultaty rozdziału 4 pozostają prawdziwe dla przestrzeni euklidesowych nad dowolnym ciałem rzeczywwiście domkniętym. Szczególnie

jasno widać to w dowodach kluczowych lematów o istnieniu wektorów własnych endomorfizmów samosprzężonych, gdzie wykorzystaliśmy wszystkie własności ciała $\mathbb{R}$ charakterystyczne dla ciał rzeczywiście domkniętych (w szczególności rozkładalność wielomianów na iloczyn czynników liniowych i kwadratowych z ujemnymi wyróżnikami). Finalnym twierdzeniem w naszej dyskusji endomorfizmów samosprzężonych było twierdzenie 4.4.2, którego ogólna wersja brzmi następująco.

Twierdzenie. *Jeśli $\mathcal{T}$ jest przemiennym zbiorem endomorfizmów samosprzężonych przestrzeni euklidesowej V nad dowolnym ciałem rzeczywiście domkniętym F , to V ma bazę ortonormalną $\{v_1, \dots, v_n\}$ taką, że każdy wektor v_i jest wektorem własnym wszystkich endomorfizmów zbioru $\mathcal{T}$.*

Rozdział 5 o funkcjonalach półtoraliniowych, przestrzeniach hermitowskich, twierdzeniu o rzucie prostopadłym i istnieniu baz ortogonalnych można bez żadnych zmian przenieść na przestrzenie wektorowe nad dowolnym ciałem $F(\sqrt{-1})$, gdzie F jest ciałem rzeczywiście domkniętym. Podobnie jest w rozdziale 6, gdzie wprowadzamy przestrzenie unitarne wymagając dodatniej określoności funkcjonału hermitowskiego. Wreszcie w rozdziale 7 również nie korzystamy z żadnych własności ciał $\mathbb{R}$ i $\mathbb{C}$, które nie przysługiwałyby ciałom F i $F(\sqrt{-1})$, gdzie F jest rzeczywiście domknięte. Tak więc także nasze główne twierdzenie 7.4.3 o równoczesnej ortonormalnej diagonalizowalności zbiorów endomorfizmów przestrzeni unitarnych jest prawdziwe w ogólnych przestrzeniach unitarnych i brzmi następująco.

Twierdzenie. *Niech $\mathcal{T} = \{\tau_i : i \in I\}$ będzie zbiorem endomorfizmów przestrzeni unitarnej V nad ciałem $F(\sqrt{-1})$, gdzie F jest ciałem rzeczywiście domkniętym. Następujące warunki są równoważne.*

- (a) *Zbiór $\mathcal{T}$ jest normalny i przemienny.*
- (b) *Przestrzeń V ma bazę ortonormalną, której każdy wektor jest wektorem własnym każdego endomorfizmu zbioru $\mathcal{T}$.*

Bibliografia

- [1] S. Axler, *Linear algebra done right*. 2nd edition. Springer 1997.
- [2] Jonathan S. Golan, *Foundations of Linear Algebra*. Kluwer Academic Publishers 1995.
- [3] P. R. Halmos, *Finite-dimensional vector spaces*, 2nd edition, Van Nostrand, New York 1958.
- [4] I. N. Herstein, *Topics in algebra*, 2nd edition, John Wiley & Sons, New York 1975. Chapters 4 and 6.
- [5] I. Kaplansky, *Linear algebra and geometry. A second course*. Boston 1969.
- [6] A. I. Kostrikin, *Wstęp do algebry. Algebra liniowa*. PWN Warszawa 2004.
- [7] Peter D. Lax, *Linear algebra*. John Wiley & Sons, Inc. 1996.
- [8] Derek J. S. Robinson, *A course in linear algebra with applications*. 2nd ed. World Scientific 2006.
- [9] Steven Roman, *Advanced linear algebra*. 2nd ed. Springer 2005.