Formy hermitowskie i przekształcenia unitarne

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

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

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

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

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

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

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

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

Wyjaśnienie przynosi następująca definicja obejmująca wprowadzony wyżej „iloczyn".

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

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

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

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

$$\langle\,(z_1, z_2, \ldots, z_n), (z'_1, z'_2, \ldots, z'_n)\rangle = z_1\overline{z'_1} + z_2\overline{z'_2} + \ldots + z_n\overline{z'_n}.$$

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

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

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

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

Wynik ten motywuje wprowadzenie następującej definicji.

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

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

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

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

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

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

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

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

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

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

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

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

Dowód. Dla dowodu twierdzenia Pitagorasa zauważmy, że:

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

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

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

Wówczas z twierdzenia Pitagorasa:

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

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

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

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

□

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

czyli po uproszczeniu i mamy

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

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

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

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

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

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

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

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

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

A zatem ϕ obcięte do $\mathrm{lin}(x)^\perp$ jest endomorfizmem unitarnym przestrzeni wymiaru $n - 1$ (już wspominałem, że w przestrzeni unitarnej mamy $V = \mathrm{lin}(x) \oplus \mathrm{lin}(x)^\perp$), a zatem na mocy założenia indukcyjnego jest diagonalizowalny w pewnej bazie $\alpha_1, \ldots, \alpha_{n-1}$. Każdy z wektorów tej bazy jest prostopadły do x. A zatem układ $\alpha_1, \ldots, \alpha_{n-1}, x$ jest bazą ortogonalną V złożoną z wektorów własnych ϕ. □