Podprzestrzenie niezmiennicze

Na ostatnim wykładzie omówiliśmy klasę endomorfizmów diagonalizowalnych, a więc takich, które mają bazę złożoną z wektorów własnych, i których macierz w tej bazie jest diagonalna. Nie każdy endomorfizm ϕ przestrzeni V nad ciałem K jest diagonalizowalny. Co możemy zatem powiedzieć o jego geometrii?

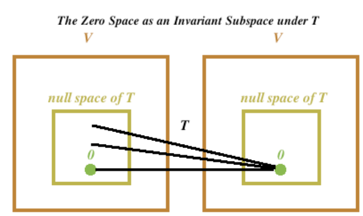
Każda podprzestrzeń własna endomorfizmu ϕ przestrzeni liniowej V ma tę własność, że nie zmienia się (jako cała przestrzeń) przy działaniu ϕ, to znaczy: $\phi(V_{(a)}) = V_{(a)}$. Uogólnieniem tej własności jest pojęcie podprzestrzeni niezmienniczej, któremu poświęcony jest ten wykład.

Definicja 14. *Niech ϕ będzie endomorfizmem przestrzeni liniowej V nad ciałem K. Podprzestrzeń $W \subseteq V$ nazwiemy* NIEZMIENNICZĄ WZGLĘDEM *ϕ (lub ϕ-niezmienniczą) wtedy i tylko wtedy, gdy $\phi(W) \subseteq W$.*

Przykłady.

- Niech $\phi \in \mathrm{End}(V)$. Wówczas V oraz podprzestrzeń zerowa są zawsze niezmiennicze względem ϕ.

  Podprzestrzenie te nazywamy trywialnymi podprzestrzeniami niezmienniczymi.



Schemat – $\ker T \in \mathrm{End}(V)$ jest zawsze podprzestrzenią T-niezmienniczą. Źródło: `http://mathonline.wikidot.com/`.

- Niech $\phi \in \mathrm{End}(V)$. Wówczas $\ker(\phi)$ oraz $\mathrm{im}(\phi)$ są niezmiennicze względem ϕ. Np. jeśli $\phi(v) = w$, to $\phi(w) \in \mathrm{im}(\phi)$.
- Niech $\phi \in \mathrm{End}(V)$ oraz niech $0 \neq \alpha \in V$ będzie wektorem własnym ϕ. Wówczas $\mathrm{lin}(\alpha)$ jest podprzestrzenią ϕ-niezmienniczą.
- Niech a będzie wartością własną $\phi \in \mathrm{End}(V)$. Wówczas $V_{(a)}$ jest podprzestrzenią ϕ-niezmienniczą.
- Niech $\phi \in \mathrm{End}(\mathbb{R}^4)$ będzie zadany w bazie standardowej macierzą

$$M(\phi)_{st}^{st} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

  Łatwo widzieć, że $\mathrm{lin}((1,0,0,0),(0,1,0,0))$ oraz $\mathrm{lin}((0,0,1,0),(0,0,0,1))$ są (oczywiście nie jedynymi) podprzestrzeniami niezmienniczymi endomorfizmu ϕ. Nie są to też podprzestrzenie własne.

Definicja 15. *Niech $\phi : V \to W$ będzie przekształceniem liniowym oraz niech $U \subseteq V$ będzie podprzestrzenią ϕ-niezmienniczą. Przez $\phi|_U$ rozumieć będziemy endomorfizm przestrzeni U zadany wzorem: $\phi|_U(u) = \phi(u)$, dla każdego $u \in U$.*

Oznaczenie to sugeruje, że mowa jest o obcięciu przekształcenia f do podprzestrzeni U, ale obcięcie jest formalnie definiowane jako przekształcenie z U do V. Nam natomiast zależy na tym, żeby macierz endomorfizmu $\phi|_U$ była kwadratowa, co oczywiście ma sens w przypadku podprzestrzeni niezmienniczych. Taka konwencja jest przyjmowana w wielu źródłach, mimo pewnego braku precyzji (którą oczywiście da się, przy większej liczbie narzędzi, uzyskać).

Tak jak endomorfizm ma wektor własny wtedy i tylko wtedy, gdy jego wielomian charakterystyczny ma pierwiastek, tak istnienie nietrywialnych (różnych od zera i całości) podprzestrzeni niezmienniczych zależne jest od rozkładalności wielomianu ϕ w ciele K na czynniki oraz od możliwości przedstawienia macierzy przekształcenia ϕ w bazie w odpowiedniej postaci blokowej.

Fakt 27. *Niech $\phi \in \operatorname{End}(V)$ oraz niech U będzie podprzestrzenią V różną od 0 i V. Następujące warunki są równoważne:*

(1) $U \subseteq V$ jest podprzestrzenią ϕ-niezmienniczą,

(2) istnieje baza $\mathcal{A}$ przestrzeni V oraz taka macierz $A \in M_{\dim U}(K)$, że

$$M(\phi)_{\mathcal{A}}^{\mathcal{A}} = \begin{bmatrix} A & B \\ 0 & C \end{bmatrix},$$

gdzie A jest macierzą $\phi|_U$ w pewnej bazie przestrzeni U.

Gdy spełniony jest jeden z warunków wyżej, wówczas istnieje $g \in K[\lambda]$, że:

$$w_\phi(\lambda) = w_{\phi|_U}(\lambda) \cdot g(\lambda).$$

W dodatku omówimy fundamentalny problem odwrotny: kiedy rozkład wielomianu charakterystycznego implikuje rozkład związany z podprzestrzeniami niezmienniczymi. Czytelnik może jednak zadać sobie pytanie jak zrozumieć przypadek, gdy $B = 0$? Co wiemy o $g \in K[\lambda]$?

Dowód. Załóżmy (1). Niech $\mathcal{A}' = (\alpha_1, \dots, \alpha_k)$ będzie bazą U oraz niech $(\alpha_{k+1}, \dots, \alpha_n)$ będzie dopełnieniem bazy $\mathcal{A}'$ do bazy $\mathcal{A}$ przestrzeni V. Obrazy wektorów $\alpha_1, \dots, \alpha_k$ po zastosowaniu ϕ należą do U, a więc do $\operatorname{lin}(\alpha_1, \dots, \alpha_k)$. A zatem pierwsze k kolumn macierzy $M(\phi)_{\mathcal{A}}^{\mathcal{A}}$ może mieć niezerowe wyrazy jedynie w pierwszych k wierszach. W szczególności istnieją takie macierze $A \in M_k(K)$, $B \in M_{k\times(n-k)}(K)$ oraz $C \in M_{(n-k)\times k}(K)$, że:

$$M(\phi)_{\mathcal{A}}^{\mathcal{A}} = \begin{bmatrix} A & B \\ 0 & C \end{bmatrix}.$$

Uzyskaliśmy zatem (2). Odwrotna implikacja (2) $\Rightarrow$ (1) jest teraz jasna. Co więcej,

$$w_\phi(\lambda) = \det \begin{bmatrix} A - \lambda I_k & B \\ 0 & C - \lambda I_{n-k} \end{bmatrix}.$$

A zatem $w_\phi(\lambda) = \det(A - \lambda I_k)\det(C - \lambda I_{n-k})$. Jednak $\det(A - \lambda I_k)$ to wielomian charakterystyczny endomorfizmu $\phi|_U$. Dowód jest zakończony. □

Przyjrzyjmy się teraz dokładniej szczególnej sytuacji gdy wielomian charakterystyczny rozkłada sie na czynniki liniowe. Wiąże się ona oczywiście ściśle z ciałem, nad którym prowadzone są rozważania.

Fakt 28. *Niech V będzie przestrzenią skończenie wymiarową nad ciałem K oraz niech $\phi \in \mathrm{End}(V)$. Następujące warunki są równoważne:*

(1) $w_\phi(\lambda)$ rozkłada się na czynniki liniowe,

(2) istnieje baza $\mathcal{A}$, w której macierz $M(\phi)_{\mathcal{A}}^{\mathcal{A}}$ jest górnotrójkątna.

Dowód. Dowodzimy (1) $\Rightarrow$ (2) przez indukcję ze względu na $\dim(V)$. Dla $\dim(V) = 1$ teza jest oczywista. Jak wygląda zatem krok indukcyjny? Z faktu, że $w_\phi(\lambda)$ rozkłada się na czynniki liniowe wynika, że ϕ ma wartość własną c, dla pewnego wektora własnego $\alpha \neq 0$. Dopełnijmy wektor α do bazy $\mathcal{A}$ przestrzeni V wektorami $(\beta_1, \ldots, \beta_{n-1})$. Wówczas w bazie $\mathcal{A}$ macierz $M(\phi)_{\mathcal{A}}^{\mathcal{A}}$ ma postać:

$$M(\phi)_{\mathcal{A}}^{\mathcal{A}} = \begin{bmatrix} c & A \\ 0 & B \end{bmatrix},$$

gdzie $A \in M_{1\times(n-1)}(K)$ oraz $B \in M_{n-1}(K)$.

Niech $B = M(\psi)_{st}^{st}$, dla pewnego endomorfizmu ψ przestrzeni $n-1$ wymiarowej $V' = \mathrm{lin}(\beta_1, \ldots, \beta_{n-1})$. Zauważmy, że

$$w_\phi(\lambda) = (c - \lambda) \cdot w_\psi(\lambda),$$

czyli $w_\psi(\lambda)$ rozkłada się na czynniki liniowe.

Z założenia indukcyjnego istnieje baza $\mathcal{B}$ przestrzeni V', że ψ ma w niej macierz górnojtrójkątną B'. W języku macierzy oznacza to, że istnieje macierz odwracalna S rozmiaru $n-1$ taka, że $B' = S^{-1}BS$. Rozważmy macierz S' rozmiarów $n \times n$ postaci

$$\begin{bmatrix} 1 & 0 \\ 0 & S \end{bmatrix},$$

gdzie w pierwszym wierszu i w pierwszej kolumnie poza przekątną stoją zera. Jest jasne, że:

$$S'^{-1} \cdot M(\phi)_{\mathcal{A}}^{\mathcal{A}} \cdot S' = \begin{bmatrix} 1 & 0 \\ 0 & S^{-1} \end{bmatrix} \cdot \begin{bmatrix} c & A \\ 0 & B \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & S \end{bmatrix} = \begin{bmatrix} c & A \\ 0 & B' \end{bmatrix}.$$

Stąd macierz $M(\phi)_{\mathcal{A}}^{\mathcal{A}}$ jest podobna do macierzy górnotrójkątnej, co jest równoważne z istnieniem bazy, w której ϕ ma macierz górnotrójkątną.

Implikacja (2) $\Rightarrow$ (1). Zauważmy, że jeśli $A = [a_{ij}]$ jest górnotrójkątna, to jej wielomian charakterystyczny jest (jako wyznacznik macierzy górnotrójkątnej $A - \lambda I$) postaci $(a_{11} - \lambda)(a_{22} - \lambda) \ldots (a_{nn} - \lambda)$. □

Zauważmy, że to twierdzenie dotyczy także pewnej klasy endomorfizmów niediagonalizowalnych, ponieważ wielomian charakterystyczny endomorfizmu zadanego macierzą

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

rozkłada się na czynniki liniowe, bo jest postaci $(1-\lambda)^2$. Endomorfizmy takie nazywamy TRIANGULARYZOWALNYMI.

Co ma ten dowód wspólnego z podprzestrzeniami niezmienniczymi? Jeśli $M(\phi)_{\mathcal{A}}^{\mathcal{A}}$ jest górnotrójkątna, to każda podprzestrzeń rozpięta przez pierwsze k wektorów układu $\mathcal{A}$ jest niezmiennicza względem $\mathcal{A}$.

Geometrycznie możemy wyobrażać sobie, że V wraz ze wskazanymi podprzestrzeniami rozpiętymi przez pierwsze k wektorów bazy przypomina przekrój drzewa, w którym koncentrycznie układają się słoje reprezentujące kolejne podprzestrzenie (coraz większych wymiarów). Endomorfizm ϕ działa na V w taki sposób, że jeśli znajdowaliśmy się w „obszarze ograniczonym danym słojem" (czyli w danej podprzestrzeni), to ϕ nas z niego nie wyprowadzi.

Zajmiemy się teraz wykorzystaniem następującej prostej obserwacji. Jeśli v należy do podprzestrzeni ϕ-niezmienniczej U przestrzeni V, to do U należą również wektory:

$$\phi(v), \quad \phi(\phi(v)), \quad \phi(\phi(\phi(v)), \quad \ldots.$$

Definicja 16. *Niech* $\phi \in \mathrm{End}(V)$. PODPRZESTRZENIĄ ϕ-CYKLICZNĄ *przestrzeni V rozpiętą przez wektor α nazywamy:*

Lub: przestrzenią cykliczną wzgl. endomorfizmu ϕ rozpiętą przez wektor α.

$$V_\alpha = \mathrm{lin}(\alpha, \phi(\alpha), \phi^2(\alpha), \phi^3(\alpha), \ldots), \textit{ gdzie } \phi^n = \underbrace{\phi \circ \phi \circ \ldots \circ \phi}_{n}.$$

Przykłady:

- Niech $\phi = \mathrm{id}_V$. Wówczas dla każdego $\alpha \in V$ mamy:

  $$\alpha = \phi(\alpha) = \phi^2(\alpha) = \ldots,$$

  czyli $V_\alpha = \mathrm{lin}(v)$.

- Niech ϕ będzie jednokładnością o skali λ na V. Wówczas dla każdego $\alpha \in V$ mamy:

  $$\phi(\alpha) = \lambda \cdot \alpha, \quad \phi^2(\alpha) = \lambda^2 \cdot \alpha, \quad \phi^3(\alpha) = \lambda^3 \cdot \alpha, \quad \ldots,$$

  czyli $V_\alpha = \mathrm{lin}(\alpha)$.

- Niech ϕ będzie symetrią $\mathbb{R}^2$ względem $(1,0)$ wzdłuż $(0,1)$. Wówczas:

  $$(1,0) = \phi(1,0) = \phi^2(1,0) = \ldots,$$

  $$\phi((1,1)) = (1,-1), \quad \phi((1,-1)) = (1,1), \ldots,$$

  czyli $V_{(1,0)} = \mathrm{lin}(1,0)$, $V_{(0,1)} = \mathrm{lin}(0,1)$ ale $V_{(1,1)} = \mathbb{R}^2$.

- Niech $\phi \in \mathrm{End}(K^n)$ dany będzie wzorem:

  Proszę zapamiętać ten endomorfizm. Jest dość ważny, a to jego macierz:

  $$M(\phi)_{st}^{st} = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ 0 & 0 & 0 & \ldots & 0 & 0 \end{bmatrix} \in M_n(K).$$

  $$\phi((x_1, x_2, \ldots, x_n)) = (x_2, x_3, \ldots, x_n, 0).$$

  Wówczas

  $$\begin{aligned} \phi(1,1\ldots,1,1,1) &= (1,1,\ldots,1,1,0), \\ \phi^2(1,1\ldots,1,1,1) &= \phi(1,1\ldots,1,1,0) = (1,1,\ldots,1,0,0), \\ \phi^3(1,1\ldots,1,1,1) &= \phi^2(1,1\ldots,1,1,0) = \phi(1,1\ldots,1,0,0) = (1,1,\ldots,0,0,0), \\ &\vdots \\ \phi^{n-1}(1,1\ldots,1,1,1) &= \phi^{n-2}(1,1\ldots,1,0) = \ldots = \phi(1,1\ldots,0,0) = (1,0,\ldots,0,0), \\ \phi^n(1,1\ldots,1,1,1) &= (0,0,0,\ldots,0,0). \end{aligned}$$

  Zatem $V_{(1,1,1,\ldots,1,1)} = K^n$.

Z podprzestrzeniami cyklicznymi związane są następujące określenia.

Definicja 17. *Niech $w \in K[\lambda]$ będzie postaci $a_0 + a_1\lambda + \ldots + a_n\lambda^n$. Niech $\phi \in \mathrm{End}(V)$, gdzie V jest nad ciałem K oraz niech $A \in M_s(K)$. Definiujemy:*

- $w(\phi) = a_0 \cdot \mathrm{id}_V + a_1 \cdot \phi + \ldots + a_n \cdot \phi^n \in \mathrm{End}(V)$,
- $w(A) = a_0 I + a_1 A + \ldots + a_n A^n \in M_s(K)$.

Obserwacja. Jeśli dla $w, v, z \in K[\lambda]$ mamy $w = v + z$, to $w(\phi) = v(\phi) + z(\phi)$, a jeśli $w = v \cdot z$, to $w(\phi) = v(\phi) \cdot z(\phi) = z(\phi) \cdot v(\phi)$.

Definicja 18. *Niech $\phi \in \mathrm{End}(V)$, gdzie V jest nad ciałem K. Podprzestrzeń*

$$E(\phi) = \{w(\phi) \mid w \in K[\lambda]\} \subseteq \mathrm{End}(V)$$

nazywamy ALGEBRĄ ENDOMORFIZMU ϕ.

Możemy teraz napisać, że dla endomorfizmu ϕ podprzestrzeń cykliczna rozpięta przez wektor v złożona jest ze wszystkich wektorów postaci:

$$V_v = \{f(v), f \in E(\phi)\}.$$

Sformułuję teraz kilka zadań, które są nietrudnymi, ale bardzo pouczającymi ćwiczeniami. Są one niezbędne do dowodu twierdzenia Cayleya-Hamiltona, które zaraz sformułuję (ale na wykładzie nie będzie ono dowodzone). Samo stosowanie twierdzenia wlicza się do materiału. Oto te ćwiczenia.

Ćwiczenie. Własności podprzestrzeni ϕ-cyklicznej V_α, dla $\phi \in \mathrm{End}(V)$.

- V_α jest **najmniejszą względem inkluzji** podprzestrzenią ϕ-niezmienniczą zawierającą wektor α.
- Jeśli $0 \neq \alpha$, to bazą V_α jest układ
$$\mathcal{B} = (\alpha, \phi(\alpha), \phi^2(\alpha), \phi^3(\alpha), \ldots, \phi^{k-1}(\alpha)) \quad \text{gdzie } k = \dim V_\alpha.$$
- Niech $k = \dim V_\alpha$ oraz niech $c_0, \ldots, c_{k-1} \in K$ spełniają
$$c_0\alpha + c_1\phi(\alpha) + \ldots + c_{k-1}\phi^{k-1}(\alpha) + \phi^k(\alpha) = 0.$$
Wówczas
$$M(\phi|_{V_\alpha})_{\mathcal{B}}^{\mathcal{B}} = \begin{bmatrix} 0 & 0 & \ldots & 0 & -c_0 \\ 1 & 0 & \ldots & 0 & -c_1 \\ 0 & 1 & \ldots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -c_{k-1} \end{bmatrix}. \qquad (*)$$
Co więcej:
$$w_{\phi|_{V_\alpha}}(\lambda) = (-1)^k \cdot (c_0 + c_1\lambda + \ldots + c_{k-1}\lambda^{k-1} + \lambda^k).$$

Jesteśmy gotowi sformułować twierdzenie Cayleya-Hamiltona.

Fakt 29. *Jeśli $A \in M_n(K)$ oraz $w = w_A(\lambda)$ jest wielomianem charakterystycznym macierzy A, to $w(A) = 0$.*

Twierdzenie noszące nazwisko wielkich matematyków XIX wieku. Pokazali oni w połowie tamtego stulecia jedynie pewne szczególne przypadki. Co znamienne, Cayley nie widział powodu ani sensu szukania dowodu dla macierzy dowolnego rozmiaru. Zostało ono udowodnione przez Frobeniusa w 1878 roku, który uświadomił sobie dopiero w 1896 roku, że ktoś już o tym problemie myślał przed nim. Zgodnie z ówczesnym zwyczajem przyznał pierwszeństwo swoim słynnym poprzednikom.

Zanim przedstawię dowód zobaczmy jak użyteczne i zaskakujące twierdzenie mamy przed sobą. Mówi ono, że dla każdej macierzy rozmiaru n macierz A^n jest kombinacją liniową swoich niższych potęg.

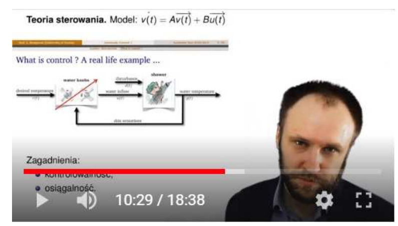
Dla przykładu: jeśli A to macierz 3×3 o wielomianie charakterystycznym $-\lambda^3 + 1$, to na mocy twierdzenia Cayleya-Hamiltona mamy

$$-A^3 + I = 0.$$

Stąd $A^3 = I$. A zatem chcąc wyliczyć na przykład A^{1000} mamy po prostu

$$A^{1000} = (A^3)^{333}A = A.$$

Istnieją też bardziej wyrafinowane zastosowania tej metody.



Więcej przykładów i agitacji: `https://youtu.be/wSGW9E06Wg8`.

Twierdzenie to pozwala także w ciekawy sposób odwracać niektóre macierze. Jeśli wiemy, dla przykładu, że macierz odwracalna A ma wielomian charakterystyczny $\lambda^5 + \lambda - 1$, to oczywiście

$$A^5 + A - I = 0.$$

Mnożąc tę równość z dowolnej strony przez A^{-1} dostajemy warunek: $A^4 + I - A^{-1} = 0$. A zatem

$$A^{-1} = A^4 + I.$$

W niektórych przypadkach twierdzenie Cayleya-Hamiltona znacznie ułatwia odwracanie macierzy.

Zanim przedstawimy dowód odnotujmy jeszcze jeden ważny komentarz dotyczący kolejnych wykładów. Naszym celem będzie omówienie twierdzenia Jordana, które znacznie uogólnia Fakt 28, ale którego dowodu nie poznamy (choć jest w skrypcie). Twierdzenie to mówi, że endomorfizm przestrzeni V, którego wielomian charakterystyczny rozkłada się na czynniki liniowe wyznacza taką bazę V, w której macierz ϕ jest blokowo diagonalna, czyli ma postać:

$$A = \begin{bmatrix} J_1 & 0 & \dots & 0 \\ 0 & J_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & J_k \end{bmatrix},$$

Poszczególne bloki diagonalne J_i mają bardzo elegancką postać — są to tzw. klatki Jordana.

Dowód. Niech $\phi \in \mathrm{End}(V)$ oraz $A = M(\phi)_{st}^{st}$, przy czym $\dim(V) = n$. Aby pokazać, że $w_A(A) = 0$ wystarczy pokazać, że

$$w_\phi(\phi)(v) = 0,$$

dla dowolnego $v \in V$. Weźmy więc dowolny niezerowy wektor $\alpha \in V$. Rozważamy podprzestrzeń cykliczną V_α wymiaru k. A zatem

$$0 = a_0\alpha + a_1\phi(\alpha) + \ldots + a_{k-1}\phi^{k-1}(\alpha) + \phi^k(\alpha),$$

bo baza V_α złożona jest z $\alpha, \ldots, \phi^{k-1}(\alpha)$ (patrz ćwiczenie wyżej). Niech $q(\lambda) = a_0 + a_1\lambda + \ldots + a_{k-1}\lambda^{k-1} + \lambda^k \in K[\lambda]$. Rozszerzamy bazę V_α do bazy $\mathcal{A}$ całego V. Wówczas, zgodnie z twierdzeniem o macierzy przekształcenia mającego podprzestrzeń ϕ-niezmienniczą mamy

$$M(\phi)_{\mathcal{A}}^{\mathcal{A}} = \begin{bmatrix} X & Y \\ 0 & Z \end{bmatrix},$$

gdzie $X \in M_k(K)$. Możemy dokładnie opisać blok X tej macierzy, bo wiemy co robi ϕ z pierwszymi k wektorami $\alpha, \phi(\alpha), \phi^2(\alpha), \ldots, \phi^{k-1}(\alpha)$ bazy $\mathcal{A}$:

$$X = \begin{bmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_{k-1} \end{bmatrix}.$$

Rzeczywiście

$$\begin{aligned} \phi(\alpha) &= \phi(\alpha), \\ \phi(\phi(\alpha)) &= \phi^2(\alpha), \\ &\ldots \\ \phi(\phi^{k-1}(\alpha)) &= \phi^k(\alpha) = -(a_0\alpha + a_1\phi(\alpha) + \ldots + a_{k-1}\phi^{k-1}(\alpha)). \end{aligned}$$

Cóż nam to wszystko dało? Otóż wiemy, że wielomian charakterystyczny $\phi|_{V_\alpha}$ jest dzielnikiem wielomianu charakterystycznego ϕ, bo V_α jest niezmiennicza. Ale macierz $\phi|_{V_\alpha}$ w bazie $\alpha, \ldots, \phi^{k-1}(\alpha)$ ma dokładnie postać X. A więc wielomian charakterystyczny X jest dzielnikiem wielomianu charakterystycznego endomorfizmu ϕ. Wielomian charakterystyczny tej macierzy to $q(\lambda)$, czyli (jak wiemy z innego z ćwiczeń) $(-1)^k(a_0 + a_1\lambda + \ldots + a_{k-1}\lambda^{k-1} + \lambda^k)$. A zatem wiemy, że $w_\phi(\lambda) = q(\lambda) \cdot h(\lambda) = h(\lambda) \cdot q(\lambda)$, dla pewnego $h \in K[\lambda]$. Ale przecież

$$q(\phi)(\alpha) = (-1)^k(a_0\alpha + a_1\phi(\alpha) + \ldots + a_{k-1}\phi^{k-1}(\alpha) + \phi^k(\alpha)) = 0.$$

W szczególności mamy $w_\phi(\phi)(\alpha) = h(\phi) \cdot q(\phi)(\alpha) = h(\phi) \cdot 0 = 0$. Zatem $w_\phi(\phi)$ to przekształcenie zerowe. $\square$

Uzupełnienie. Endomorfizmy nilpotentne

Na wykładzie pokazaliśmy twierdzenie dotyczące tzw. endomorfizmów triangularyzowalnych, czyli takich, których macierz w pewnej bazie jest macierzą górnotrójkątną. Jeśli $\phi \in \mathrm{End}(V)$ jest triangularyzowalny i $M(\phi)_{\mathcal{A}}^{\mathcal{A}}$ jest górnotrójkątna dla bazy $\mathcal{A} = (\alpha_1, \ldots, \alpha_n)$ przestrzeni V, to mamy zależności:

$$\begin{aligned}
\phi(\alpha_1) &\in \mathrm{lin}(\alpha_1)\\
\phi(\alpha_2) &\in \mathrm{lin}(\alpha_1, \alpha_2)\\
\phi(\alpha_3) &\in \mathrm{lin}(\alpha_1, \alpha_2, \alpha_3)\\
&\vdots\\
\phi(\alpha_{n-1}) &\in \mathrm{lin}(\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_{n-1}).
\end{aligned}$$

a zatem mamy **wstępujący łańcuch** $n+1$ **podprzestrzeni** ϕ-niezmienniczych:

$$\{0\} \subset \mathrm{lin}(\alpha_1) \subset \mathrm{lin}(\alpha_1, \alpha_2) \subset \mathrm{lin}(\alpha_1, \alpha_2, \alpha_3) \subset \ldots \subset \mathrm{lin}(\alpha_1, \ldots, \alpha_{n-1}) \subset V.$$

Szczególnie czytelną ilustrację tej sytuacji otrzymujemy wtedy, gdy α_i są wektorami własnymi. Wówczas ϕ jest endomorfizmem diagonalizowalnym. Niezwykle istotnym przypadkiem są także te endomorfizmy triangularyzowalne, których wielomian charakterystyczny ma postać $(a-\lambda)^k$, dla pewnego a. Rozważymy szczególny przypadek, gdy $a = 0$.

Definicja 19. *Endomorfizm ϕ skończenie wymiarowej przestrzeni liniowej V nazywamy* NILPOTENTNYM, *jeśli istnieje liczba całkowita $k > 0$ taka, ze*

$$\phi^k = 0. \qquad (\heartsuit)$$

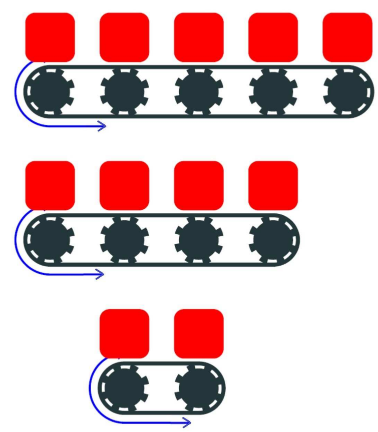
Najmniejsze k spełniające $(\heartsuit)$ nazywamy STOPNIEM NILPOTENTNOŚCI ϕ. *Macierz $A \in M_n(K)$ nazywamy* NILPOTENTNĄ STOPNIA k, *jeśli $A^k = 0$ oraz $A^{k-1} \neq 0$.*

Kluczowy przykład. Jeśli $\dim V = n$ oraz $\phi \in \mathrm{End}(V)$ jest nilpotentny stopnia n to istnieje niezerowy wektor $\alpha \in V$ taki, że $V = V_\alpha$ jest podprzestrzenią cykliczną oraz V ma bazę

$$\mathcal{A} = \{\phi^{n-1}(\alpha), \phi^{n-2}(\alpha), \ldots, \phi(\alpha), \alpha\},$$

w której $M(\phi)_{\mathcal{A}}^{\mathcal{A}}$ jest macierzą postaci:

$$\begin{bmatrix} 0 & 1 & 0 & \ldots & 0 & 0\\ 0 & 0 & 1 & \ldots & 0 & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & 0 & \ldots & 0 & 1\\ 0 & 0 & 0 & \ldots & 0 & 0 \end{bmatrix} \in M_n(K). \qquad (*)$$



Ilustracja „działania" endomorfizmów nilpotentnych odpowiednio stopni 5, 4, 2. Ale też można myśleć, że wszystkie taśmociągi działają jednocześnie i wtedy opisujemy endomorfizm przestrzeni K^{11} za pomocą macierzy wpisanej na kolejnej stronie. Źródło: `http://qirui.li/` – polecam slajdy z bardzo pomysłowymi poglądowymi ilustracjami tematów z algebry liniowej.

Endomorfizm nilpotentny może być bardziej skomplikowany, np. dany za pomocą macierzy:

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

Przypomnijmy uwagę, którą przywoływać będziemy wielokrotnie na kolejnych wykładach. Jeśli A jest macierzą blokowo-diagonalną o blokach kwadratowych $J_1, \ldots, J_k$, to macierz A^m jest macierzą blokowo-diagonalną o blokach $J_1^m, J_2^m, \ldots, J_k^m$. Stąd stopień nilpotentności macierzy (po lewej) N równy jest 5.

Z naszego punktu widzenia macierze czy endomorfizmy nilpotentne można traktować jako endomorfizmy *zupełnie innej natury geometrycznej* niż diagonalizowalne. Proszę sprawdzić, że endomorfizm diagonalizowalny, który jest jednocześnie nilpotentny musi być zerowy. Jednym z kluczowych wyników teorii endomorfizmów jest twierdzenie o addytywnym rozkładzie Jordana-Chevalleya, które mówi, co następuje.

Endomorfizm nilpotentny zabija (czyni zerem), po dostatecznej liczbie aplikacji, dowolny niezerowy wektor przestrzeni, na której działa.

Fakt 30 (Twierdzenie Jordana-Chevalleya)**.** *Niech V będzie skończenie wymiarową przestrzenią liniową nad K oraz niech $\phi \in \mathrm{End}(V)$ będzie triangularyzowalny. Wówczas istnieje jednoznaczny rozkład*

$$\phi = \phi_S + \phi_N, \qquad (*)$$

- *gdzie ϕ_S jest diagonalizowalny,*
- *ϕ_N jest nilpotentny,*
- *oraz $\phi_S \circ \phi_N = \phi_N \circ \phi_S$.*

Co więcej ϕ_S, ϕ_N należą do algebry endomorfizmu ϕ (są wielomianami od ϕ).

Niech $D_n(K)$ oraz $N_n(K)$ oznaczają odpowiednio zbiory macierzy diagonalizowalnych nad K oraz nilpotentnych nad K. Żaden z tych zbiorów nie jest podprzestrzenią $M_n(K)$, np:

$$\begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \notin D_2(K)$$

oraz

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \notin N_2(K).$$

Zagadka: czym są podprzestrzenie $\mathrm{lin}(D_n(K))$ i $\mathrm{lin}(N_n(K))$. Czy to $M_n(K)$?

W twierdzeniu istotna jest przemienność ϕ_S, ϕ_N, inaczej da się znaleźć wiele rozkładów na endomorfizm diagonalizowalny i nilpotentny, np.:

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix},$$

a przecież ϕ zadane macierzą A jest diagonalizowalne.

Opis endomorfizmów nilpotentnych uzyskamy jako szczególny przypadek twierdzenia Jordana, któremu poświęcimy dwa kolejne wykłady. Nie jest on, jak widzimy, banalny.

Warto natomiast wspomnieć, że podstawowa metoda dowodu tego ogólnego rezultatu oparta jest o analizę struktury endomorfizmów nilpotentnych.

Dodatek. Rozkłady ϕ-niezmiennicze

Niezwykle istotnym spojrzeniem na teorię endomorfizmów jest spojrzenie nie tylko z perspektywy macierzy przekształcenia, ale wynikających z niej rozkładów przestrzeni, na której działa endomorfizm. Przypomnijmy kluczową definicję, wspominaną w uzupełnieniach do wykładów w pierwszym semestrze.

Definicja 20. *Niech $V_1, V_2, \ldots, V_k$ będą podprzestrzeniami przestrzeni V. Powiemy, że V jest* SUMĄ PROSTĄ PODPRZESTRZENI *$V_1, V_2, \ldots, V_k$, co oznaczamy jako $V = V_1 \oplus V_2 \oplus \ldots \oplus V_k$, jeśli zachodzi jeden z dwóch równoważnych warunków:*

(1) każdy wektor $v \in V$ rozkłada się w sposób jednoznaczny na sumę postaci $v_1 + v_2 + \ldots + v_k$, gdzie $v_i \in V_i$.

(2) $V = V_1 + V_2 + \ldots + V_k$ oraz jeśli W_i oznacza sumę podprzestrzeni $V_1, \ldots, V_k$ z wyłączeniem składnika V_i, to $V_i \cap W_i = \{0\}$, dla $i = 1, \ldots, k$.

Z Wniosku 27 z wykładu 3 wynika następujący fundamentalny fakt.

Zauważmy, że geometria przekształcenia mającego macierz jak obok przypomina geometrię endomorfizmu diagonalizowalnego, przy czym rolę „osi jednokładności" przejmują składniki proste, a zamiast rozkładać wektor w bazie z wektorów własnych rozkładamy go w bazie będącej sumą mnogościową wybranych k baz przestrzeni składowych.

Fakt 31. *Niech $V = V_1 \oplus \ldots \oplus V_k$ oraz niech $\phi \in \mathrm{End}(V)$ będzie taki, że $V_1, \ldots, V_k$ są podprzestrzeniami ϕ-niezmienniczymi w V. Wówczas ϕ ma w pewnej bazie $\mathcal{A}$ macierz blokowo-diagonalną postaci*

$$M(\phi)_{\mathcal{A}}^{\mathcal{A}} = \begin{bmatrix} A_1 & 0 & 0 & \ldots & 0 \\ 0 & A_2 & 0 & \ldots & 0 \\ 0 & 0 & A_3 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & A_k \end{bmatrix},$$

gdzie $A_i \in M_{\dim(V_i)}(K)$.

Niestety uzyskiwanie rozkładów przestrzeni liniowych na sumy proste podprzestrzeni niezmienniczych bywa bardzo trudne. Zauważmy, że kryterium diagonalizowalności macierzy dotyczy dokładnie sytuacji, gdy V jest sumą prostą podprzestrzeni własnych. Skąd jednak wiadomo, że taki warunek zachodzi? Niestety nie jest prawdą nad każdym ciałem, że jeśli $W \subseteq V$ jest podprzestrzenią niezmienniczą względem $\phi \in \mathrm{End}(V)$, to istnieje podprzestrzeń ϕ-niezmiennicza W' taka, ze $W \oplus W' = V$. Wybór odpowiednich podprzestrzeni (i ciała!), dla których takie dopełnienia da się uzyskać jest treścią głębokich twierdzeń.

Jest to w istocie jeden z centralnych problemów algebry, leżący u podstaw tzw. teorii reprezentacji.

Twierdzenie, któremu poświęcimy ten dodatek opowiada o pięknym i zaskakującym związku pomiędzy rozkładami na sumy proste, rozkładalnością wielomianu charakterystycznego oraz geometrią.

Definicja 21. *Niech $\phi \in \mathrm{End}(V)$. Niech V będzie sumą prostą postaci*

$$V = V_1 \oplus \ldots \oplus V_r \qquad (*).$$

*Powiemy, że **rozkład** $(*)$ **jest ϕ-niezmienniczy**, jeśli każda z podprzestrzeni V_i jest ϕ-niezmiennicza.*

Przykłady:

- jeśli $\phi \in \mathrm{End}(V)$ jest rzutem, to rozkład $V = \ker(\phi) \oplus \mathrm{im}(\phi)$ jest ϕ-niezmienniczy,
- jeśli $\phi \in \mathrm{End}(V)$ jest diagonalizowalny, to rozkład V na sumę prostą podprzestrzeni własnych jest ϕ-niezmienniczy.

Kluczowa idea. Jeśli znajdziemy rozkład ϕ-niezmienniczy postaci $V = V_1 \oplus \ldots \oplus V_r$, to badanie działania ϕ na V sprowadza się do badania *niezależnych działań* ϕ na każdym z V_i. Podsumujmy.

Fakt 32. *Niech V będzie wymiaru n nad ciałem K. Niech $\phi \in \mathrm{End}(V)$. Załóżmy, że mamy rozkład ϕ-niezmienniczy $V = V_1 \oplus \ldots \oplus V_r$. Istnieje baza $\mathcal{A}$ przestrzeni V, że:*

*(1) macierz $M(\phi)_{\mathcal{A}}^{\mathcal{A}}$ ma postać **blokowo-diagonalną***

$$\begin{bmatrix} A_1 & 0 & \ldots & 0 \\ 0 & A_2 & \ldots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \ldots & A_r \end{bmatrix}, \quad \text{gdzie } A_i \in M_{\dim V_i}(K), \qquad (*)$$

(2) $w_\phi(\lambda) = w_{A_1}(\lambda) \cdot \ldots \cdot w_{A_r}(\lambda)$.

Prawdziwy *cud* polega na tym, że odpowiednia rozkładalność wielomianu charakterystycznego gwarantuje rozkłady ϕ-niezmiennicze. Przyjrzymy się tej sprawie, przywołując wiedzę z materiałów uzupełniających z pierwszego semestru.

Definicja 22. *Niech K bedzie ciałem.*

- *wielomian $f \in K[x]$ nazywamy* ROZKŁADALNYM, *jeśli istnieją wielomiany $p, q \in K[x]$ stopnia mniejszego niż f takie, że*

  $$f(x) = p(x)q(x).$$

  Niezerowy wielomian, który nie jest rozkładalny nazywamy wielomianem NIEROZKŁADALNYM.

- NAJWIĘKSZYM WSPÓLNYM DZIELNIKIEM *wielomianów $p_1, \ldots, p_n$ należących do $K[x]$ nazywamy wielomian najwyższego możliwego stopnia dzielący wszystkie te wielomiany. Jeśli 1 jest największym wspólnym dzielnikiem $p_1, \ldots, p_n$, wówczas mówimy, że wielomiany te są* WZGLĘDNIE PIERWSZE.

Fakt 33 (Twierdzenie o rozkładzie prymarnym)**.** *Niech $p \in K[\lambda]$ będzie wielomianem o rozkładzie*

$$p = p_1 \dots p_k,$$

gdzie $p_1, \dots, p_k$ są czynnikami względnie pierwszymi. Niech $\phi \in \mathrm{End}(V)$. Wówczas ma miejsce rozkład

$$\ker p(\phi) = \ker p_1(\phi) \oplus \dots \oplus \ker p_k(\phi)$$

na sumę prostą ϕ-niezmienniczych podprzestrzeni w V.

Dwie kluczowe intuicje dotyczące powyższego fundamentalnego wyniku.

- Jeśli V jest skończenie wymiarową przestrzenią nad ciałem K, to dla każdego $\phi \in \mathrm{End}(V)$ mamy $w_\phi(\phi) = 0$ (twierdzenie Cayleya-Hamiltona), czyli $\ker p(\phi) = V$ dla $p = w_\phi(\lambda)$.
- Nawet jeśli $\dim V = \infty$, ale mimo to $\phi \in \mathrm{End}(V)$ spełnia równanie wielomianowe, np. rzut $\phi \in \mathrm{End}(V)$ spełnia $(\phi^2 - \phi)(\alpha) = 0$, dla $\alpha \in V$, to twierdzenie działa.

Zobaczmy przykłady takich rozkładów.

- Rozważmy $\phi \in \mathrm{End}(\mathbb{R}^4)$ dany macierzą:

$$M(\phi)_{st}^{st} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

  Oczywiście $w_\phi(\lambda) = (1-\lambda)^4$, ale ϕ nie jest diagonalizowalny, bo $\dim V_{(1)} = \dim \ker(\phi - \mathrm{id}) = 2$. Z drugiej strony biorąc wektory bazowe $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4$ mamy:

$$\begin{aligned} &\phi(\epsilon_1) = \epsilon_1 && \Rightarrow (\phi - \mathrm{id})(\epsilon_1) = 0, \\ &\phi(\epsilon_2) = \epsilon_1 + \epsilon_2 \Rightarrow (\phi - \mathrm{id})(\epsilon_2) = \epsilon_1 && \Rightarrow (\phi - \mathrm{id})^2(\epsilon_2) = 0, \\ &\phi(\epsilon_3) = \epsilon_2 + \epsilon_3 \Rightarrow (\phi - \mathrm{id})(\epsilon_3) = \epsilon_2 && \Rightarrow (\phi - \mathrm{id})^3(\epsilon_3) = 0. \\ &\phi(\epsilon_4) = \epsilon_4 && \Rightarrow (\phi - \mathrm{id})(\epsilon_4) = 0. \end{aligned}$$

  Zatem $\mathbb{R}^4 = \ker(\phi - \mathrm{id})^3$. Co ciekawe, $\ker(\phi - \mathrm{id})^3$ rozkłada się.

Ale o tym powie nam już twierdzenie Jordana. W rozkładzie wielomianu $w_\phi(\lambda)$ mamy jeden czynnik, z dokładnością do wzgl. pierwszości, czyli $p_1 = (1-\lambda)^4$.

- Rozważmy $\phi \in \mathrm{End}(\mathbb{R}^4)$ dany macierzą:

$$M(\phi)_{st}^{st} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \end{bmatrix}.$$

  Łatwo widzieć, że $w_\phi(\lambda) = \lambda^4 + 1$. A zatem $w_\phi(\lambda)$ nie ma pierwiastków w $\mathbb{R}$. Mamy jednak

$$\mathbb{R}^4 = \ker(\phi^4 + \mathrm{id}) = \ker(\phi^2 - 2\phi + 2\,\mathrm{id}) \oplus \ker(\phi^2 + 2\phi + 2\,\mathrm{id}),$$

  zatem mimo, że ϕ nie jest triangularyzowalny, istnieje baza $\mathcal{A}$ przestrzeni $\mathbb{R}^4$, w której ϕ ma macierz blokowo-diagonalną:

$$\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}, \qquad \text{dla pewnych } A, B \in M_2(\mathbb{R}).$$

Inaczej mówiąc $w_\phi(\lambda) = p_1 p_2$, gdzie $p_1 = \lambda^2 - 2\lambda + 2$, $p_2 = \lambda^2 + 2\lambda + 2$.

Trivia. Twierdzenie Cayleya-Hamiltona na konkursach

Warto wspomnieć, że studenci mogą brać udział w wielu konkursach na poziomie pierwszych lat studiów matematycznych. Do najstarszych i najsłynniejszych należy amerykański Putnam, największy zasięg i globalny prestiż ma IMC (International Mathematics Competition for University Students), a nie brakuje także konkursów lokalnych. W niektórych krajach np. Rumunii zadania z analizy matematycznej oraz algebry liniowej i abstrakcyjnej występują na najwyższych poziomach krajowej olimpiady. Zachęcam do pracy z ciekawymi problemami z tych konkursów. Potrafi to dać wiele satysfakcji — bywa i frustrujące.

Zacząć można od forum AOPS: https://artofproblemsolving.com/community/c15_undergraduate_contests, ale przydatne w tym kontekście będą również książki autorstwa Titu Andreescu lub Fuzhena Zhanga.

Na zawodach bardzo często korzystać należy z następującej, prostej wersji twierdzenia Cayleya-Hamiltona dotyczącej macierzy $X \in M_2(K)$, która mówi, że zachodzi równość

$$X^2 - \operatorname{tr}(X)X + \det(X)I = 0.$$

Dowód to po prostu bezpośredni rachunek. Jeśli

$$X = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

to macierz $X^2 - \operatorname{tr}(X)X + \det(X)I$ równa jest:

$$\begin{bmatrix} a^2+bc & ab+bd \\ ac+cd & bc+d^2 \end{bmatrix} - \begin{bmatrix} (a+d)a & (a+d)b \\ (a+d)c & (a+d)d \end{bmatrix} + \begin{bmatrix} ad-bc & 0 \\ 0 & ad-bc \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Oto trzy przykładowe zadania, gdzie wykorzystywany jest powyższy fakt. Są to niestandardowe problemy konkursowe, zwłaszcza zadanie drugie, ale warto docenić jak sprytnie korzysta się ze znanych nam faktów (nie tylko z tego semestru).

Zadanie 1. Niech $A, B \in M_2(K)$, gdzie $\det A = \det B = 1$. Pokaż, że

$$\operatorname{tr}(AB) - \operatorname{tr}(A)\operatorname{tr}(B) + \operatorname{tr}(AB^{-1}) = 0.$$

ROZWIĄZANIE. Z twierdzenia wyżej mamy

$$B^2 - (\operatorname{tr} B)B + I_2 = 0,$$

co po przemnożeniu przez AB^{-1} z lewej daje

$$AB - \operatorname{tr}(B)A + AB^{-1} = 0. \qquad (\dagger)$$

Teraz trzeba zauważyć, że dla dowolnych macierzy kwadratowych $X, Y \in M_n(K)$ oraz $\lambda \in K$ mamy $\operatorname{tr}(X+Y) = \operatorname{tr}(X) + \operatorname{tr}(Y)$ i $\operatorname{tr}(\lambda X) = \lambda \operatorname{tr}(X)$. Zatem obkładając równość $(\dagger)$ funkcją tr otrzymujemy tezę. ■

Zadanie 2. Pokaż, że istnieje tylko jedna macierz $X \in M_2(\mathbb{Z}_5)$ taka, że:

$$X^5 = \begin{bmatrix} 4 & 2 \\ 4 & 1 \end{bmatrix}.$$

Rozwiązanie. Zauważmy, że ślad i wyznacznik macierzy po prawej, nazwijmy ją A, to odpowiednio: 0 oraz 1. Szukamy macierzy rozmiaru 2×2, która w piątej potędze ma taki ślad i wyznacznik. To oznacza, na mocy twierdzenia Cayleya-Hamiltona, że

$$(X^5)^2 + I = 0.$$

Zatem $A^2 + I = 0$. Czyli $A^5 = A$. Zatem A jest rozwiązaniem postawionego równania. Zauważmy dalej, że $\det X^5 = 1$, a równanie $x^5 = 1$ ma w $\mathbb{Z}^5$ jedynie rozwiązanie $x = 1$. Zatem równanie Cayleya-Hamiltona dla macierzy X ma postać:

$$X^2 - \text{tr}(X)X + I = 0.$$

Podnosimy całość do potęgi piątej:

$$X^{10} = (\text{tr}(X) - I)^5,$$

co nad ciałem $\mathbb{Z}_5$ jest równe po prostu $\text{tr}(X)^5 X - I$ (bo I jest przemienna z X oraz zachodzi cudowna tożsamość $(x+y)^5 = x^5 + y^5$). Co więcej, w ciele $\mathbb{Z}^5$ mamy $x^5 = x$, więc tak naprawdę $X^{10} = \text{tr}(X)X - I$. Ale przecież $X^{10} = A^2 = -I$, czyli $\text{tr}(X)X = 0$, co oznacza $\text{tr}(X) = 0$. A zatem $X^2 = -I$, czyli $X^5 = X = A$. ∎

Inne podejście: skoro A spełnia wyjściowe równanie to można pokazać, że dowolne inne rozwiązanie X musi mieć te same wartości własne, co macierz A (macierz X ma te same wartości własne, co X^5, bo jesteśmy nad $\mathbb{Z}_5$). Ale A ma dwie różne wartości własne: $2, 3$. A zatem X musi być również diagonalizowalna. Dla macierzy diagonalizowalnej X nad $\mathbb{Z}_5$ mamy zaś $X^5 = X$, co daje $X = A$.

Zadanie 3. Niech $A, B \in M_2(\mathbb{R})$ spełniają warunek

$$AB = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}.$$

Wyznacz $((BA)^{-1} + BA)^{2019}$.

Rozwiązanie. Korzystając z faktu, że dla dowolnych macierzy kwadratowych X, Y mamy

$$\text{tr}(XY) = \text{tr}(YX), \quad \det(XY) = \det(YX)$$

widzimy, że

$$\text{tr}(BA) = \text{tr}(AB) = 3, \quad \det(BA) = \det(AB) = 1.$$

Zatem na mocy twierdzenia Cayleya-Hamiltona:

$$(BA)^2 - 3(BA) + I = 0.$$

Mnożąc uzyskaną równość przez $(BA)^{-1}$ dostajemy:

$$BA + (BA)^{-1} = 3I.$$

∎