

Liniowa niezależność. Baza przestrzeni liniowej

Ostatnia aktualizacja: 3.11.2021 r.

Przypomnijmy, że na ostatnim wykładzie wprowadziliśmy pojęcie przestrzeni liniowej V nad ciałem K , której elementy nazywamy wektorami, wraz z operacjami dodawania wektorów i mnożenia wektorów przez skalar z ciała K . Na początku warto, w ramach wprowadzenia do nowego tematu, zwrócić uwagę na jedną konsekwencję aksjomatów, która będzie ciągle występowała w naszych rozumowaniach.

Uwaga 1. Niech V będzie przestrzenią liniową nad ciałem K . Niech $v \in V$ oraz $a \in K$. Wówczas

$$a \cdot v = 0 \implies a = 0 \text{ lub } v = 0.$$

Dowód wymaga uzasadnienia dwóch prostych obserwacji, które pozostawiam Czytelnikowi¹. Każda z nich wymaga osobnego rozumowania i napisania pewnego ciągu równości wynikających z aksjomatów.

- Niech $u, v \in V$. Wówczas istnieje dokładnie jeden $x \in V$ taki, że $u + x = v$.
- Zachodzą równości $a \cdot 0 = 0$ oraz $0 \cdot v = 0$.

Kluczową konstrukcją prowadzącą do wskazywania licznych przykładów przestrzeni liniowych jest pojęcie podprzestrzeni, czyli podzbioru przestrzeni liniowej zamkniętego na sumę wektorów i branie ich skalarnych wielokrotności, a zwłaszcza pojęcie podprzestrzeni rozpiętej przez układ wektorów. Przypomnijmy, że jeśli wektory β_1, \dots, β_m należą do przestrzeni V , to rozważać możemy zbiór kombinacji liniowych tych wektorów, czyli

$$\text{lin}(\beta_1, \dots, \beta_m).$$

W zbiorze tym są wszystkie wektory postaci $a_1\beta_1 + \dots + a_m\beta_m$, dla $a_1, \dots, a_m \in K$, a więc np.

$$\beta_1, \quad \beta_1 + \beta_3, \quad \beta_1 - 2\beta_2 + 3\beta_m, \quad \dots, \quad \beta_1 + \dots + \beta_m.$$

Celem tego i kolejnego wykładu będzie przede wszystkim badanie podprzestrzeni postaci $\text{lin}(\beta_1, \dots, \beta_m)$. W szczególności będziemy chcieli przedstawiać V jako przestrzeń rozpiętą na pewnym układzie wektorów. W dalszych rozumowaniach często będziemy korzystać z następującej naturalnej obserwacji, wynikającej wprost z aksjomatów przestrzeni liniowej.

Uwaga 2. Jeśli V jest przestrzenią liniową oraz $\beta_1, \dots, \beta_m \in V$, to

$$\text{lin}(\beta_1, \dots, \beta_m) \subseteq V.$$

Obserwacja ta jest naturalnym uogólnieniem spostrzeżenia dotyczącego zbioru rozwiązań jednorodnego układu równań liniowych o n niewiadomych o współczynnikach w ciele K . Znając pewne rozwiązania $\beta_1, \beta_2, \dots, \beta_r$ układu

$$U : \begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = 0 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = 0. \end{cases} \quad (*)$$

wiemy, że również elementy

$$a_1\beta_1 + a_2\beta_2 + \dots + a_r\beta_r$$

są rozwiązaniami tego układu, dla dowolnych układów skalarów $a_1, a_2, \dots, a_r \in K$. Przykładowo: wektory $(0, -1, 1, 0), (0, -1, 0, 1)$ są rozwiązaniami układu jednorodnego o współczynnikach w \mathbb{R} :

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = 0 \\ x_1 - x_2 - x_3 - x_4 = 0 \end{cases}$$

i dla każdego $s, t \in \mathbb{R}$ wektor postaci:

$$s(0, -1, 1, 0) + t(0, -1, 0, 1)$$

jest rozwiązaniem tego układu. Co więcej, w tym przypadku przestrzeń rozwiązań układu jednorodnego rozpięta jest przez dwa wektory i ma postać

$$\text{lin}((0, -1, 1, 0), (0, -1, 0, 1)).$$

W przyszłości pokażemy, że liczba wektorów potrzebnych do rozpięcia przestrzeni rozwiązań jednorodnego układu równań równa jest liczbie zmiennych niezależnych. Skąd jednak bierze się układ wektorów $(0, -1, 1, 0), (0, -1, 0, 1)$ i jakie są jego własności? O tym mówi następujące fundamentalne pojęcie.

¹W pokazywanych ostatnio przykładach przestrzeni liniowych (ciągi, macierze, funkcje) fakt ten wynika w zasadzie bezpośrednio z tego, że dla $a, b \in K$ mamy: $a \cdot b = 0 \implies a = 0$ lub $b = 0$.

Definicja 1. Układ wektorów β_1, \dots, β_m przestrzeni V nad ciałem K nazwiemy **liniowo zależnym**, jeśli istnieją elementy a_1, \dots, a_m ciała K , nie wszystkie równe 0, spełniające:

$$a_1\beta_1 + \dots + a_m\beta_m = 0.$$

Układ wektorów $\alpha_1, \dots, \alpha_m$ przestrzeni V nazwiemy **liniowo niezależnym**, jeśli nie jest liniowo zależny. Innymi słowy, dla takiego układu wektorów z równości $a_1\alpha_1 + \dots + a_m\alpha_m = 0$ wynika $a_1 = \dots = a_m = 0$. Pusty układ wektorów uważamy za liniowo niezależny.

Przykład 1. Układ złożony z jednego niezerowego wektora jest liniowo niezależny, na mocy Uwagi 1.

Przykład 2. Układ zawierający wektor zerowy jest liniowo zależny.

Przykład 3. Układ $(1, 0, 0), (2, 0, 0), (3, 0, 0), (4, 0, 0), (5, 0, 0)$ jest liniowo zależny w \mathbb{R}^3 , bo:

$$1(1, 0, 0) + 1(2, 0, 0) + 1(3, 0, 0) + 1(4, 0, 0) + (-2)(5, 0, 0) = (0, 0, 0),$$

oraz

$$\text{lin}((1, 0, 0), (2, 0, 0), (3, 0, 0), (4, 0, 0), (5, 0, 0)) = \text{lin}((1, 0, 0)).$$

Przykład 4. Wektory $(1, 0, 2), (\sqrt{2}, 1, 2\sqrt{2}), (0, 2\sqrt{2}, 0) \in \mathbb{R}^3$ są liniowo zależne, ponieważ

$$2(1, 0, 2) - \sqrt{2}(\sqrt{2}, 1, 2\sqrt{2}) + \frac{1}{2}(0, 2\sqrt{2}, 0) = (0, 0, 0).$$

Jeżeli jednak rozpatrzmy \mathbb{R}^3 jako przestrzeń liniową nad ciałem \mathbb{Q} (a chyba widać, że jest to całkowicie dopuszczalne), wówczas wektory te są liniowo niezależne! Istotnie, dla liczb wymiernych a, b, c warunek

$$\mathbf{a}(1, 0, 2) + \mathbf{b}(\sqrt{2}, 1, 2\sqrt{2}) + \mathbf{c}(0, 2\sqrt{2}, 0) = (0, 0, 0)$$

oznacza, że $(2a + \sqrt{2}b, b + 2\sqrt{2}c, 2a + 2\sqrt{2}b) = (0, 0, 0)$, a zatem $a = b = c = 0$.

Uogólnieniem sytuacji opisanej wyżej jest następujący fakt.

Przykład 5. W przestrzeni K^n rozważmy układ wektorów $\epsilon_1, \dots, \epsilon_n$, zdefiniowany w następujący sposób, dla $i = 1, \dots, n$:

$$\epsilon_i = (a_1, \dots, a_n), \quad \text{gdzie } a_j = \begin{cases} 1, & j = i, \\ 0, & j \neq i. \end{cases}$$

Na przykład dla $n = 3$ mamy $\epsilon_1 = (1, 0, 0), \epsilon_2 = (0, 1, 0), \epsilon_3 = (0, 0, 1)$. Pokażmy, że układ $\epsilon_1, \dots, \epsilon_n$ jest liniowo niezależny. Jeśli $a_1\epsilon_1 + \dots + a_n\epsilon_n = (0, \dots, 0)$, to zgodnie z działaniami w K^n mamy: $(a_1, a_2, \dots, a_n) = (0, \dots, 0)$. A zatem $a_1 = 0, a_2 = 0, \dots, a_n = 0$.

Przykład 6. Niech $0 \neq A = [a_{ij}] \in M_{m \times n}(K)$ będzie w postaci schodkowej oraz $\alpha_1, \dots, \alpha_r \in K^n$ – niezerowe wiersze macierzy A . Wówczas układ $\alpha_1, \dots, \alpha_r$ jest liniowo niezależny.

Dowód to indukcja po liczbie niezerowych wierszy r . Krok bazowy: układ złożony z jednego niezerowego wektora jest liniowo niezależny na mocy Uwagi 1. Przejdźmy do kroku indukcyjnego. Rozważmy macierz A w postaci schodkowej o r niezerowych wierszach $\alpha_1, \dots, \alpha_r$. Jeśli dla pewnych $\lambda_1, \dots, \lambda_r \in K$ mamy:

$$\lambda_1\alpha_1 + \lambda_2\alpha_2 + \dots + \lambda_r\alpha_r = (0, \dots, 0), \quad (\diamond)$$

to niech pierwszy niezerowy wyraz w wierszu α_1 stoi na k -tym miejscu.

$$\begin{bmatrix} 0 & \dots & 0 & a_{1k} & \dots & a_{1n} \\ 0 & \dots & 0 & 0 & \dots & a_{2n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & 0 & \dots & a_{rn} \end{bmatrix}$$

Suma k -tych współrzędnych wektorów $\lambda_1\alpha_1, \dots, \lambda_r\alpha_r$ równa jest k -tej współrzędnej wektora zerowego, czyli $\lambda_1a_{1k} + \lambda_2a_{2k} + \dots + \lambda_ra_{rk} = 0$. Jednak $a_{2k} = \dots = a_{rk} = 0$, bo A jest schodkowa. Co więcej, $a_{1k} \neq 0$. A zatem mamy $\lambda_1a_{1k} = 0$, czyli $\lambda_1 = 0$, zgodnie z Uwagą 1. A zatem w (\diamond) mamy: $\lambda_2\alpha_2 + \dots + \lambda_r\alpha_r = (0, \dots, 0)$. Skoro $\alpha_2, \dots, \alpha_r$ są kolejnymi wierszami macierzy schodkowej, to z założenia indukcyjnego wektory te tworzą układ liniowo niezależny, czyli mamy $\lambda_2 = \lambda_3 = \dots = \lambda_r = 0$. Pokazaliśmy, że $\lambda_1\alpha_1 + \dots + \lambda_r\alpha_r = (0, \dots, 0)$ implikuje $\lambda_1 = \dots = \lambda_r = 0$.

Widzimy zatem, że ostatni przykład pozwala rozwiązać następujące zagadnienie w przestrzeni K^n : dana jest podprzestrzeń $W = \text{lin}(\beta_1, \dots, \beta_m)$ w K^n . Znajdź układ liniowo niezależny $\alpha_1, \dots, \alpha_r$ taki, że $W = \text{lin}(\alpha_1, \dots, \alpha_r)$. Rozwiązanie jest takie: traktujemy wektory β_1, \dots, β_m jako wiersze macierzy $A \in M_{m \times n}(K)$ i doprowadzamy A do postaci schodkowej. Zgodnie z powyższą obserwacją niezerowe wiersze $\alpha_1, \dots, \alpha_r$ macierzy A' są liniowo niezależne. Co więcej, na poprzednim wykładzie pokazaliśmy, że wiersze macierzy A' rozpinają tę samą podprzestrzeń K^n , co wiersze macierzy A . A zatem problem jest rozwiązany, bo A' ma r niezerowych wierszy i $m - r$ wierszy zerowych, oraz:

$$\text{lin}(\alpha_1, \dots, \alpha_r) = \text{lin}(\alpha_1, \dots, \underbrace{\alpha_r \cdot \mathbf{0}, \dots, \mathbf{0}}_{m-r}) = \text{lin}(\beta_1, \dots, \beta_m).$$

W powyższym rozumowaniu układ liniowo niezależny $\alpha_1, \dots, \alpha_r$ rozpinający W nie musiał mieć wiele wspólnego z wyjściowym układem rozpinającym β_1, \dots, β_m . Pokażmy teraz, że również z układu β_1, \dots, β_m można wybrać podukład liniowo niezależny, rozpinający W . Potem staniemy przed fundamentalnym problemem pokazania, że ten podukład również ma r elementów.

Uwaga 3. Układ β_1, \dots, β_k jest liniowo zależny wtedy i tylko wtedy, gdy jeden z wektorów β_1, \dots, β_k jest kombinacją liniową pozostałych.

Intuicja jest następująca: liniowo zależny układ rozpinający nie jest „oszczędny” – można go „pomniejszyć” i wciąż rozpinąć (za pomocą „mniejszego” układu) tę samą podprzestrzeń. Z drugiej strony należy zauważyć delikatność założenia: nie twierdzimy, że każdy wektor w układzie liniowo zależnym musi być kombinacją pozostałych. Twierzimy tylko, że w układzie takim istnieje taki wektor.

Przykład 7. Układ $\{(1, 0, 0), (2, 0, 0), (1, 1, 1)\}$ jest liniowo zależny w \mathbb{R}^3 , bo

$$2(1, 0, 0) + (-1)(2, 0, 0) + \mathbf{0}(1, 1, 1) = (0, 0, 0)$$

ale

- $(1, 1, 1)$ **nie jest kombinacją liniową** $(1, 0, 0), (2, 0, 0)$,
- $(1, 0, 0) = \frac{1}{2}(2, 0, 0) + \mathbf{0}(1, 1, 1)$.
- $(2, 0, 0) = 2(1, 0, 0) + \mathbf{0}(1, 1, 1)$.

Dowód. Przypuśćmy, że układ wektorów β_1, \dots, β_k jest liniowo zależny. Istnieją zatem a_1, \dots, a_k , nie wszystkie równe 0, że $a_1\beta_1 + \dots + a_k\beta_k = \mathbf{0}$. Po ewentualnym przenumеровaniu wektorów możemy zakładać, że $a_1 \neq 0$ (tu nie ma żadnego oszustwa – proszę się nad tym chwilę zastanowić). Wtedy:

$$a_1\beta_1 = -a_2\beta_2 - \dots - a_k\beta_k, \text{ czyli } \beta_1 = -\frac{a_2}{a_1}\beta_2 - \frac{a_3}{a_1}\beta_3 - \dots - \frac{a_k}{a_1}\beta_k.$$

Zatem β_1 jest kombinacją liniową pozostałych wektorów układu.

Na odwrót: jeśli jeden z wektorów układu jest kombinacją liniową pozostałych, to po ewentualnym przenumеровaniu możemy zakładać, że $\beta_1 = b_2\beta_2 + \dots + b_k\beta_k$. Wtedy $\beta_1 - b_2\beta_2 - \dots - b_k\beta_k = \mathbf{0}$, przy czym współczynnik przy β_1 jest równy 1, a więc jest niezerowy. Stąd układ β_1, \dots, β_k jest liniowo zależny. \square

Powyższe stwierdzenie sugeruje następujący, oczywisty wniosek:

Wniosek 1. Niech $V = \text{lin}(\beta_1, \dots, \beta_n) \neq \mathbf{0}$. Wówczas z układu $\{\beta_1, \dots, \beta_n\}$ wybrać można liniowo niezależny podukład $\{\alpha_1, \dots, \alpha_k\}$ taki, że $V = \text{lin}(\alpha_1, \dots, \alpha_k) = \text{lin}(\beta_1, \dots, \beta_n)$.

Dowód. Załóżmy, że teza nie jest prawdziwa i weźmy najmniejsze n , dla którego istnieje układ wektorów $\mathcal{B} = \{\beta_1, \dots, \beta_n\}$, z którego nie można wybrać podukładu liniowo niezależnego, rozpinającego V . Oczywiście \mathcal{B} nie może być liniowo niezależny (wtedy szukanym podukładem byłby po prostu wyjściowy układ). A zatem istnieje β_i , które jest kombinacją liniową pozostałych wektorów z układu \mathcal{B} , nazwijmy układ tych pozostałych wektorów przez \mathcal{B}' . Zobaczymy, że mamy $\text{lin}(\mathcal{B}) = \text{lin}(\mathcal{B}')$. Rzeczywiście, zawieranie $\text{lin}(\mathcal{B}) \supseteq \text{lin}(\mathcal{B}')$ wynika stąd, że każda kombinacja liniowa wektorów z \mathcal{B}' jest też kombinacją liniową wektorów z \mathcal{B} . Z drugiej strony, biorąc kombinację $a_1\beta_1 + \dots + a_i\beta_i + \dots + a_n\beta_n$ widzimy, że skoro $\alpha_i \in \text{lin}(\mathcal{B}')$, to cała ta kombinacja należy do $\text{lin}(\mathcal{B}')$.

Nowy podukład \mathcal{B}' ma mniej niż n (ale więcej niż 0) elementów, a więc zgodnie z założeniem istnieje podukład liniowo niezależny \mathcal{A} układu \mathcal{B}' taki, że $\text{lin}(\mathcal{B}') = \text{lin}(\mathcal{A})$. A zatem \mathcal{A} jest również podukładem liniowo niezależnym w \mathcal{B} i mamy $\text{lin}(\mathcal{A}) = \text{lin}(\mathcal{B})$, sprzeczność. \square

W przestrzeni $V = \text{lin}(\beta_1, \dots, \beta_n)$ zawsze znajdziemy zatem pewien układ liniowo niezależny taki $\{\alpha_1, \dots, \alpha_k\}$ że $V = \text{lin}(\alpha_1, \dots, \alpha_k)$. Kluczowe twierdzenie, do którego zmierzamy brzmi:

Twierdzenie 1. Niech $V = \text{lin}(\beta_1, \dots, \beta_n)$. Jeśli dla pewnych układów liniowo niezależnych $\{\alpha_1, \dots, \alpha_r\}$, $\{\alpha'_1, \dots, \alpha'_s\}$ mamy

$$V = \text{lin}(\alpha_1, \dots, \alpha_r) = \text{lin}(\alpha'_1, \dots, \alpha'_s),$$

to $r = s$. Co więcej, żaden układ liniowo niezależny zawarty w V nie może mieć więcej niż r elementów.

Dowód tego rezultatu zajmie nam sporą część tego wykładu, ale ma on zasadnicze znaczenie dla całego kursu algebry liniowej. Zostawmy go jednak na później. W tym momencie skupimy się na istotnym pojęciu, które pojawiło się w jego sformułowaniu.

Definicja 2. Układ $\alpha_1, \dots, \alpha_k$ wektorów przestrzeni V nazywamy **bazą przestrzeni** V , jeśli spełnia on następujące dwa warunki:

- (a) układ $\alpha_1, \dots, \alpha_k$ jest liniowo niezależny,
- (b) układ $\alpha_1, \dots, \alpha_k$ rozpiną V , to znaczy $V = \text{lin}(\alpha_1, \dots, \alpha_k)$.

Zobaczymy kilka przestrzeni, w których możemy wskazać bazy.

Przykład 8. W przestrzeni K^n układ wektorów $\epsilon_1, \dots, \epsilon_n$, rozważanych w Przykładzie 3, jest bazą, zwaną **bazą standardową** przestrzeni K^n . Wiemy bowiem, że układ $\epsilon_1, \dots, \epsilon_n$ jest liniowo niezależny. Oczywiście mamy też $\text{lin}(\epsilon_1, \dots, \epsilon_n) = K^n$. Rzeczywiście², dowolny wektor (x_1, x_2, \dots, x_n) należy do $\text{lin}(\epsilon_1, \dots, \epsilon_n)$, bo $(x_1, \dots, x_n) = x_1(1, 0, \dots) + x_2(0, 1, 0, \dots) + \dots + x_n(0, 0, \dots, 1)$.

Przykład 9. Niech $V = \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1 + 2x_2 - x_3 = 0\}$, czyli $(x_1, x_2, x_3) \in V$ wtedy i tylko wtedy, gdy $x_1 = -2x_2 + x_3$. Wektory w V są zatem postaci:

$$(-2x_2 + x_3, x_2, x_3) = (2x_2, x_2, 0) + (x_3, 0, x_3) = x_2(-2, 1, 0) + x_3(1, 0, 1).$$

Stąd $V = \text{lin}((-2, 1, 0), (1, 0, 1))$. Wektory $(-2, 1, 0)$, $(1, 0, 1)$ są oczywiście liniowo niezależne (bo jeśli $a(-2, 1, 0) + b(1, 0, 1) = (0, 0, 0)$, to łatwo widzieć, że $a = b = 0$), a zatem układ ten jest bazą V .

Przykład 10. Niech $W = \text{lin}((1, 2, 1), (0, 1, 1), (1, 3, 2))$ będzie podprzestrzenią \mathbb{R}^3 . Jest to przestrzeń rozpięta przez 3 wektory, ale nie jest to „oszczędny” układ. Wektor $(1, 3, 2)$ jest kombinacją liniową $(1, 2, 1), (0, 1, 1)$. A zatem układ $\{(1, 2, 1), (0, 1, 1), (1, 3, 2)\}$ nie jest bazą W . Jest nią natomiast układ $\{(1, 2, 1), (0, 1, 1)\}$. Ale też układ $\{(1, 2, 1), (1, 3, 2)\}$ i wiele innych.

Twierdzenie 2. Niech $\alpha_1, \dots, \alpha_k$ będzie układem wektorów przestrzeni V . Wówczas następujące warunki są równoważne:

- (1) układ $\alpha_1, \dots, \alpha_k$ jest bazą przestrzeni V ,
- (2) każdy wektor $\alpha \in V$ można przedstawić w sposób jednoznaczny jako kombinację liniową układu $\alpha_1, \dots, \alpha_k$.

Definicja 3. Niech V będzie przestrzenią liniową nad ciałem K i niech $\alpha_1, \dots, \alpha_k$ będzie bazą V . **Współrzędnymi wektora** $\alpha \in V$ w bazie $\alpha_1, \dots, \alpha_k$ nazywamy układ elementów a_1, \dots, a_k ciała K spełniających

$$\alpha = a_1\alpha_1 + \dots + a_k\alpha_k.$$

Przykłady:

- Wektor $(1, 2, 1)$ ma współrzędne $1, 2, 1$ w bazie standardowej przestrzeni \mathbb{R}^3 ,
- Wektor $(1, 2, 1)$ ma współrzędne $-1, 1, 1$ w bazie $\{(1, 0, 0), (1, 1, 0), (1, 1, 1)\}$ przestrzeni \mathbb{R}^3 , bo $(1, 2, 1) = -1(1, 0, 0) + 1(1, 1, 0) + 1(1, 1, 1)$.
- Układ $(1, 0), (2, 0)$ nie jest bazą $V = \text{lin}((1, 0))$, bo mamy $(1, 0) = 1 \cdot (1, 0) = 1 \cdot (2, 0) + (-1) \cdot (1, 0)$.

²Proszę zauważyć, że korzystamy po cichu z Uwagi 2, nie komentując trywialnego zawierania $\text{lin}(\epsilon_1, \dots, \epsilon_n) \subseteq K^n$, a uzasadniając jedno tylko zawieranie, mianowicie $\text{lin}(\epsilon_1, \dots, \epsilon_n) \supseteq K^n$

Dowód. Zacznijmy od uzasadnienia implikacji (1) \Rightarrow (2). Niech $\alpha_1, \dots, \alpha_k$ będzie bazą przestrzeni V . Wówczas $V = \text{lin}(\alpha_1, \dots, \alpha_k)$, więc każdy $\alpha \in V$ jest kombinacją układu $\alpha_1, \dots, \alpha_k$. Pozostaje wykazać jednoznaczność. Gdyby:

$$\alpha = a_1\alpha_1 + \dots + a_k\alpha_k = a'_1\alpha_1 + \dots + a'_k\alpha'_k,$$

dla pewnych $a_1, \dots, a_k, a'_1, \dots, a'_k \in K$, to mielibyśmy:

$$(a_1 - a'_1)\alpha_1 + \dots + (a_k - a'_k)\alpha_k = 0.$$

Z liniowej niezależności wektorów $\alpha_1, \dots, \alpha_k$ wynikałoby zatem, że $a_1 - a'_1 = \dots = a_k - a'_k = 0$. A zatem rozkład każdego $\alpha \in V$ jest jednoznaczny.

Dowodzimy odwrotną implikację, (2) \Rightarrow (1). Przypuśćmy, że każdy wektor $\alpha \in V$ można jednoznacznie przedstawić jako kombinację układu $\alpha_1, \dots, \alpha_k$. Wykażemy, że $\alpha_1, \dots, \alpha_k$ jest bazą. Oczywiście skoro każdy wektor z V jest kombinacją liniową wektorów $\alpha_1, \dots, \alpha_k$, to układ ten rozpina V . A zatem warunek (b) z definicji bazy jest spełniony. Pozostaje pokazać, że układ $\alpha_1, \dots, \alpha_k$ jest liniowo niezależny. Przypuśćmy, że $a_1\alpha_1 + \dots + a_k\alpha_k = 0$, dla pewnych $a_1, \dots, a_k \in K$. Wówczas mamy:

$$a_1\alpha_1 + \dots + a_k\alpha_k = 0\alpha_1 + \dots + 0\alpha_k = 0,$$

a skoro także 0 ma jednoznaczny rozkład w V , to $a_1 = 0, a_2 = 0, \dots, a_k = 0$, co dowodzi liniowej niezależności $\alpha_1, \dots, \alpha_k$. \square

Na koniec chciałbym przedstawić kilka uwag i przykładów dotyczących liniowej niezależności przestrzeni, których nie można przedstawić jako $\text{lin}(\alpha_1, \dots, \alpha_n)$. Zacznijmy od ogólnej definicji liniowej niezależności.

Definicja 4. Układ $X = \{\alpha_i\}_{i \in T}$ wektorów przestrzeni V nazywamy **liniowo niezależnym**, jeśli każdy jego skończony podukład jest liniowo niezależny.

Przykłady (większość to całkiem ciekawe ćwiczenia):

- (a) układ $\{1, x, x^2, x^3, \dots\}$ jest liniowo niezależny w $K[x]$,
- (b) układ ciągów $a_1 = (1, 0, 0, \dots), a_2 = (0, 1, 0, \dots), a_3 = (0, 0, 1, \dots), \dots$ jest liniowo niezależny w K^∞ ,
- (c) układ ciągów $\{(1, t, t^2, t^3, \dots), t \in (0, 1)\}$ jest liniowo niezależny w \mathbb{R}^∞ ,
- (d) układ $\{\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}, \dots\} = \{\sqrt{p}, p \in P\}$, gdzie P - zbiór liczb pierwszych, jest liniowo niezależny w przestrzeni \mathbb{R} nad ciałem \mathbb{Q} ,
- (e) układ $\{\sin(x), \sin^2(x), \sin^3(x), \dots\} = \{\sin(x)^n, n \in \mathbb{N}_+\}$ jest liniowo niezależny w przestrzeni $F(\mathbb{R}, \mathbb{R})$.

Definicja 5. Układ $X = \{\alpha_i\}_{i \in T}$ wektorów przestrzeni V nazywamy **bazą**, jeśli jest on liniowo niezależny oraz $\text{lin}(X) = V$.

Na tym wykładzie nie będziemy zajmować się zbyt wiele przestrzeniami, których bazy mają nieskończenie wiele elementów, ale w uzupełnieniu i dodatkach pojawi się kilka ciekawych intuicji z nimi związanych. Warto odnotować, że z układów (a)-(e) tylko układ (a) jest bazą $K[x]$. Rzeczywiście, dowolny wielomian jest kombinacją liniową skończenie wielu elementów z układu $\{1, x, x^2, x^3, \dots\}$, a układ ten jest liniowo niezależny: jeśli $a_1 \cdot x^{i_1} + a_2 \cdot x^{i_2} + \dots + a_n x^{i_n}$ jest wielomianem zerowym, to oczywiście $a_1 = \dots = a_n$. Pozostałe układy są wprawdzie liniowo niezależne, ale nie stanowią bazy.

Przyjrzyjmy się nieco bliżej przykładowi (b). Ciągu

$$(1, 1, \dots) \in K^\infty,$$

którego wszystkie wyrazy są równe 1 nie można przedstawić jako kombinacji liniowej elementów postaci a_i . Zasadniczy problem powyższego przykładu polega nie na wskazywaniu dużych układów liniowo niezależnych w K^∞ , ale na tym, że te duże układy wskazane „wprost” są za małe by rozpinać całe K^∞ . Nawet jeśli dorzucimy do układu w (b) wektor złożony z samych jedynek, nie będziemy mieli bazy. Można znajdować kolejne wektory, które nie należą do przestrzeni rozpiętej przez ten poszerzony układ. Nawet gdybyśmy połączyli rodzinę w (b) z rodziną w (c) (dla $K = \mathbb{R}$), wciąż nie uzyskamy bazy.

O problemie znajdowania baz takich „dużych przestrzeni” powiemy nieco więcej następnym razem. Najpierw jednak pokażemy, że każde dwie bazy przestrzeni rozpiętej przez skończony układ wektorów są równoliczne i wprowadzimy pojęcie wymiaru takich przestrzeni. Kluczowym narzędziem pomocniczym (lematem) będzie twierdzenie o wymianie, udowodnione przez Steinitza w 1910 roku.

Uzupełnienie. Liniowo niezależne układy funkcji

W ostatniej części wykładu podaliśmy kilka przykładów liniowo niezależnych układów funkcji. W tym uzupełnieniu rozważymy kilka podstawowych przykładów. Badanie liniowej niezależności funkcji liniowych wielu zmiennych będzie dla nas za pewien czas dość istotne. Zacznijmy od prostej sytuacji.

Zadanie. Pokaż, że funkcje $\sin(x)$, $\cos(x)$ tworzą układ liniowo niezależny w $F(\mathbb{R}, \mathbb{R})$.

Korzystając z definicji liniowej niezależności należy pokazać, że jeśli dla pewnych a, b zachodzi równość:

$$a \sin(x) + b \cos(x) = 0(x),$$

to $a = b = 0$. Równość wyżej jest równością funkcji, a zatem zachodzić musi dla każdego $x \in \mathbb{R}$. Podstawiając rozmaite wartości x dostajemy ogrom warunków wiążących współczynniki a, b . Dla przykładu, biorąc $x_1 = 0$ oraz $x_2 = \pi/2$ otrzymujemy:

$$\begin{aligned} a \sin(0) + b \cos(0) &= a \cdot 0 + b \cdot 1 = 0, \\ a \sin\left(\frac{\pi}{2}\right) + b \cos\left(\frac{\pi}{2}\right) &= a \cdot 1 + b \cdot 0 = 0. \end{aligned}$$

Stąd $a = b = 0$.

Dodatek. Nieprzeliczalne układy lnz. Algebraiczna niezależność.

Poniższe zaskakujące zadanie trafiło kiedyś do zestawu domowego dla grupy JSIMowej. Za rozwiązanie i część dodatkowych uwag dziękuję dr. Ł. Kubatowi.

Zadanie. Ustawmy liczby wymierne \mathbb{Q} w ciąg $(q_n)_{n \in \mathbb{N}}$. Dla dowolnego $t \in \mathbb{R}$ niech

$$a(t) = \sum_{n \in N(t)} \frac{1}{n!}, \quad \text{gdzie } N(t) = \{n \in \mathbb{N} : q_n < t\}.$$

- (1) Sprawdź, że szereg definiujący $a(t)$ jest zbieżny (czyli definicja jest poprawna).
- (2) Wykaż, że dla dowolnych $s, t \in \mathbb{R}$ zachodzi $s \neq t \implies a(s) \neq a(t)$.
- (3) Udowodnij, że zbiór $A = \{a(t) : t \in \mathbb{R}\} \subseteq \mathbb{R}$ jest liniowo niezależny nad \mathbb{Q} .

Rozwiązanie. Zauważmy, że

$$a(t) = \sum_{n \in N(t)} \frac{1}{n!} < \sum_{n=0}^{\infty} \frac{1}{n!} = e,$$

co dowodzi (1). Gdy $s, t \in \mathbb{R}$ spełniają $s < t$, to $(s, t) \cap \mathbb{Q} \neq \emptyset$. Istnieje więc takie $n \in \mathbb{N}$, że $s < q_n < t$. Zatem $a(s) < a(s) + \frac{1}{n!} < a(t)$, co dowodzi (2). Aby udowodnić (3) założmy, dla dowodu nie wprost, że

$$q_1 a(t_1) + \dots + q_k a(t_k) = 0 \tag{*}$$

dla pewnych $t_1, \dots, t_k \in \mathbb{R}$ spełniających $t_1 > \dots > t_k$, gdzie liczby $q_1, \dots, q_k \in \mathbb{Q}$ nie są wszystkie równe zero. Wśród równości typu (*) możemy wybrać najkrótszą, czyli taką, w której k jest najmniejsze. Oczywiście musi być $k \geq 2$. Ponadto, dzięki minimalności k , koniecznie $q_1, \dots, q_k \neq 0$. Mnożąc (*) przez stosowną liczbę naturalną możemy założyć, że $q_1, \dots, q_k \in \mathbb{Z}$. Dla $t \in \mathbb{R}$ oraz $m \in \mathbb{N}$ niech

$$L_m(t) = \{n \in N(t) : n \leq m\} \quad \text{oraz} \quad R_m(t) = \{n \in N(t) : n > m\}.$$

Mnożąc (*) przez $m!$ otrzymujemy $L(m) = -R(m)$, gdzie

$$\begin{aligned} L(m) &= q_1 \left(\sum_{n \in L_m(t_1)} \frac{m!}{n!} \right) + \dots + q_k \left(\sum_{n \in L_m(t_k)} \frac{m!}{n!} \right), \\ R(m) &= q_1 \left(\sum_{n \in R_m(t_1)} \frac{m!}{n!} \right) + \dots + q_k \left(\sum_{n \in R_m(t_k)} \frac{m!}{n!} \right). \end{aligned}$$

Oczywiście $L(m) \in \mathbb{Z}$. Ponadto

$$\begin{aligned} |R(m)| &\leq |q_1| \left(\sum_{n \in R_m(t_1)} \frac{m!}{n!} \right) + \dots + |q_k| \left(\sum_{n \in R_m(t_k)} \frac{m!}{n!} \right) \\ &\leq |q_1| \left(\sum_{n > m} \frac{m!}{n!} \right) + \dots + |q_k| \left(\sum_{n > m} \frac{m!}{n!} \right) \\ &\leq \frac{|q_1| + \dots + |q_k|}{m+1} \left(\sum_{n > m} \frac{1}{(n-m)!} \right) \\ &\leq \frac{|q_1| + \dots + |q_k|}{m+1} e. \end{aligned}$$

Wynika stąd, że gdy m jest duże, to $|R(m)| < 1$. Skoro $R(m) = -L(m) \in \mathbb{Z}$, to musi zachodzić równość $L(m) = R(m) = 0$. Ponieważ zbiór $(t_2, t_1) \cap \mathbb{Q}$ jest nieskończony, to znajdziemy takie $m \in \mathbb{N}$ by jednocześnie $|R(m)| < 1$ (wtedy, jak wiemy, $L(m) = R(m) = 0$) oraz $t_2 < q_m < t_1$. W tej sytuacji mamy $m \in L_m(t_1) \setminus (L_m(t_2) \cup \dots \cup L_m(t_k))$. Zatem równość $L(m) = 0$ implikuje

$$-q_1 = q_1 \left(\sum_{\substack{n \in L_m(t_1) \\ n \neq m}} \frac{m!}{n!} \right) + q_2 \left(\sum_{n \in L_m(t_2)} \frac{m!}{n!} \right) + \dots + q_k \left(\sum_{n \in L_m(t_k)} \frac{m!}{n!} \right). \tag{**}$$

Obie strony równania (**) są liczbami całkowitymi. Ponadto prawa strona jest podzielna przez m . Zatem także q_1 jest podzielne przez m . W takim razie musi być $q_1 = 0$, gdyż m można wybrać tak, by $m > |q_1|$. Uzyskana sprzeczność ($q_1 = 0$) prowadzi do wniosku, że zbiór A jest liniowo niezależny nad \mathbb{Q} . \square

Uwaga. Dowodzi się, że choć zbiór A jest tej samej mocy co \mathbb{R} , to nie rozpiną on \mathbb{R} nad \mathbb{Q} . Można także wykazać (patrz J. von Neumann, *Ein System algebraisch unabhängiger Zahlen*, Math. Ann. **99** (1928), pp. 134–141), że liczby postaci

$$b(t) = \sum_{n=0}^{\infty} \frac{2^{2^{nt}}}{2^{2^{n^2}}} \quad \text{dla } t > 0$$

($[x]$ oznacza część całkowitą liczby $x \in \mathbb{R}$)

są nie tylko liniowo niezależne nad \mathbb{Q} , ale nawet **algebraicznie niezależne** nad \mathbb{Q} , tzn. dla dowolnego $n \geq 1$, dowolnych $0 < t_1 < \dots < t_n$ oraz dowolnego wielomianu zmiennych x_1, \dots, x_n , czyli dla pewnego $0 \neq f \in \mathbb{Q}[x_1, \dots, x_n]$ zachodzi $f(b(t_1), \dots, b(t_n)) \neq 0$.

Przykład ilustrujący algebraiczną zależność. Liczby $\sqrt{\pi}$ oraz $2\pi + 1$ są liniowo niezależne nad \mathbb{Q} , ale są algebraicznie zależne, ponieważ wielomian $2x^2 - y - 1 \in \mathbb{Q}[x, y]$ zeruje się dla $x = \sqrt{\pi}$ oraz $y = 2\pi + 1$.

Prof. J. Mycielski pokazał następujące twierdzenie (*Algebraic independence and measure*, Fund. Math **61** (1967), pp. 165–169) dla dowolnego doskonałego podzbioru \mathbb{R} (tzn. niepustego, domkniętego oraz bez punktów izolowanych), patrz: <http://matwbn.icm.edu.pl/ksiazki/fm/fm61/fm61117.pdf>.

Twierdzenie. Każdy doskonały podzbiór zbioru liczb rzeczywistych zawiera doskonały podzbiór, który jest algebraicznie niezależny nad \mathbb{Q} .

Pojęcie algebraicznej niezależności elementów \mathbb{R} nad \mathbb{Q} , a także elementów \mathbb{C} nad \mathbb{Q} , związane jest ściśle z pojęciem liczb algebraicznych i przestępnych, z którymi spotkaliście się Państwo (lub spotkacie) na Analizie Matematycznej. Pojęcie to jest bardzo subtelne i tajemnicze. Przestępnosć liczby π została udowodniona po raz pierwszy właśnie dzięki badaniu algebraicznej niezależności (dowód dla e dokonał elementarnymi metodami analitycznymi Hermite w 1873 roku). Zachodzi mianowicie następujący rezultat.

Twierdzenie (Lindemann-Weierstrass, 1885). Jeśli $\alpha_1, \dots, \alpha_n$ są liczbami algebraicznymi liniowo niezależnymi nad \mathbb{Q} , to liczby $e^{\alpha_1}, \dots, e^{\alpha_n}$ są algebraicznie niezależne nad \mathbb{Q} .

Aby zrozumieć jakie są związki tego wyniku z przestępnoscią odnotujmy inne, równoważne sformułowanie.

Twierdzenie (Baker, 1966). Jeśli $\alpha_1, \dots, \alpha_n$ są parami różnymi liczbami algebraicznymi, to liczby $e^{\alpha_1}, \dots, e^{\alpha_n}$ są liniowo niezależne nad ciałem liczb algebraicznych $\overline{\mathbb{Q}}$ (algebraiczne domknięcie \mathbb{Q} w \mathbb{C}).

Jak można stosować to twierdzenie? Jeśli α jest niezerową liczbą algebraiczną to zbiór $\{0, \alpha\}$ zawiera różne elementy algebraiczne, więc zbiór $\{e^0, e^\alpha\}$, czyli $\{1, e^\alpha\}$ jest liniowo niezależny nad ciałem liczb algebraicznych, w szczególności e^α nie jest algebraiczna. Gdy udowodnimy przestępnosć liczby e możemy z niej łatwo wywnioskować przestępnosć liczby π , korzystając ze słynnej tożsamości algebraicznej Eulera $e^{\pi i} + 1 = 0$. Dokładniej, gdyby π była liczbą algebraiczną to πi również, a wtedy przestępna musi być, na mocy poprzedniego argumentu liczba $e^{\pi i} = -1$, co jest niemożliwe. Zatem π jest przestępna. Prosty wariant tego argumentu pokazuje również, że dla niezerowej liczby algebraicznej α liczby $\sin(\alpha)$, $\cos(\alpha)$, $\operatorname{tg}(\alpha)$ i ich hiperboliczne odpowiedniki są liczbami przestępnymi.

Dowód Twierdzenia Lindemanna jest skomplikowany ale o zagadnieniach tego typu i szeregu innych rezultatów dotyczących liczb przestępnych: <http://www.math.leidenuniv.nl/~evertse/dio15-4.pdf>.

Pozostawiam Państwa z jeszcze jednym słynnym problemem otwartym w tej dziedzinie.



Trivia. Podział prostokąta na kwadraty, czyli intuicja miary.

Problem – Zadanie. Prostokąt R o bokach długości 1 oraz x , gdzie x jest liczbą niewymierną, nie może być złożony ze skończenie wielu kwadratów.

Założmy przeciwnie, że takie rozcięcie prostokąta o rozmiarach $1 \times x$ jest możliwe. Dzielimy go na kwadraty Q_1, \dots, Q_n , gdzie s_i jest długością boku każdego z kwadratów Q_i , dla $1 \leq i \leq n$. UWAGA: to wcale nie muszą (nie mogą wszystkie) być liczby wymierne! Potraktujemy te liczby jako... wektory!

Rozważać będziemy ciało \mathbb{R} jako przestrzeń liniową nad ciałem \mathbb{Q} . Mówiliśmy już kilkakrotnie, że to jest dość niezwykła, nieskończenie wymiarowa przestrzeń, kryjąca wiele niespodzianek. Niech $V \subseteq \mathbb{R}$ będzie podprzestrzenią rozpiętą przez liczby s_1, \dots, s_n . Czyli: V to zbiór kombinacji liniowych (o współczynnikach w \mathbb{Q}) tego układu liczb. Skoro (jak twierdzimy) możliwy jest podział prostokąta R na sumę kwadratów o bokach s_i , to mamy $1, x \in \text{lin}(s_1, s_2, \dots, s_n)$, bo $1, x$ są po prostu sumami pewnych s_i .

Teraz pojawia się sprytna (ale jakże często stosowana w matematyce) sztuczka. Określamy funkcję $f : V \rightarrow \mathbb{R}$ spełniającą warunki $f(1) = 1$, $f(x) = -1$ oraz taką, że dla każdych $x, y \in V$ mamy $f(x + y) = f(x) + f(y)$ oraz $f(qx) = qf(x)$, dla $q \in \mathbb{Q}$. Czy taka funkcja istnieje? Przecież to musiałyby być jedno z tych dziwnych rozwiązań równania Cauchy'ego postawionego na poprzednim wykładzie! Ach, ale tu mamy funkcję nie z \mathbb{R} do \mathbb{R} , tylko z V do \mathbb{R} . Dziwne, prawda? Funkcja taka jednak istnieje.

Owszem, skoro $1, x$ są liniowo niezależne nad \mathbb{Q} (a to łatwo sprawdzić), to układ ten możemy na mocy tw. Steinitza dopełnić do bazy $1, x, b_3, \dots, b_k$ przestrzeni V (niekoniecznie $k = n$, bo może niektóre s_i to kombinacje liniowe pozostałych?). Kładziemy dalej $f(1) = 1$, $f(x) = -1$ oraz $f(b_i) = 0$, dla $i = 3, 4, \dots$. Następnie mając funkcję f określoną na samej tylko bazie V bierzemy dowolny wektor $v \in V$ i rozpisujemy go (jednoznacznie!) w bazie $1, x, b_3, \dots, b_k$ w postaci $v = a_1 + a_2x + a_3b_3 + \dots + a_kb_k$, gdzie $a_i \in \mathbb{Q}$. Definiujemy teraz $f(v) := a_1f(1) + a_2f(x) + a_3f(b_3) + \dots + a_kf(b_k) = a_1 - a_2$. Zachęcam każdego do sprawdzenia, że teraz nasza funkcja spełnia warunki $f(x + y) = f(x) + f(y)$ oraz $qf(x) = f(qx)$. Tego typu funkcje wprowadzimy niedługo na wykładzie w większej ogólności. Na razie ograniczamy się do powyższych wyjaśnień. Zauważmy też, że absolutnie nie pojawił się **wzór na f** (w zwykłym sensie).

Rozważmy teraz, dla każdego prostokąta A o bokach a, b , gdzie $a, b \in V$, liczbę $v(A) = f(a)f(b)$. Jeśli prostokąt R rozmiarów $1 \times x$ byłby złożony z kwadratów Q_1, \dots, Q_n , to ze wzoru na sumę pól mamy:

$$v(R) = v(Q_1) + v(Q_2) + \dots + v(Q_n).$$

Jak to jest jednak możliwe, skoro $v(R) = f(1)f(x) = -1$, zaś $v(Q_i) = f(s_i)^2 \geq 0$, dla wszystkich i ? To jest sprzeczność. A zatem R nie może być rozcięty na kwadraty Q_1, \dots, Q_n . Problem rozwiązany.

Rozumowanie to może budzić wiele pytań. Wydaje się, że jest ono przesadnie skomplikowane i wymaga jakiejś strasznej maszynierii. Dlaczego to było konieczne? Oczywiście problemem jest fakt, że postulowany podział kwadratu jest stosunkowo dowolny, liczba składników jest duża, nie muszą to być kwadraty o bokach wymiernej długości – mimo wszystko mamy prawo być zaskoczeni. Użyliśmy poważnej technologii z wykładu, a nawet przemyciliśmy po cichu pojęcie przekształcenia liniowego. To powinno zastanowić.

Rzecz jasna istnieje drugie dno całego tego problemu. Tak naprawdę korzystaliśmy tu po cichu z własności addytywności pola na płaszczyźnie. Nie definiowaliśmy zbyt ściśle co oznacza rozbiecie na kwadraty itd. To oczywiście można doprecyzować. Ale jest pewien ogólniejszy problem. Nietrudno pokazać, że dowolny wielokąt na płaszczyźnie można pociąć na części, z których ułoży się prostokąt (a nawet kwadrat) – mówimy, że dowolny wielokąt jest **równoważny przez pocięcie** z prostokątem. Stąd sposób obliczenia pola dowolnego wielokąta jest wyznaczony jednoznacznie. Pytanie: **czy można dowolny wielokąt pociąć na skończoną liczbę mniejszych wielokątów, z których ułoży się prostopadłościan?**

To zaskakujące pytanie było jednym z tzw. 23 problemów Hilberta ogłoszonych w 1900 jako najpoważniejsze problemy matematyczne na nadchodzący XX wiek. Przynajmniej cztery są otwarte do dziś. Problem, który rozważamy rozwiązano jako jeden z pierwszych. Jeszcze w tym samym roku Max Dehn udowodnił, że istnieją pary wielokątów... które nie są równoważne przez pocięcie! Dowód ten jest zrozumiały dla wytrwałych i opisany bardzo przejrzyście w artykule prof. Marka Kordosa „Pole i objętość” na łamach czasopisma Delta (jest dostępny online – wystarczy wyszukać na stronie <http://www.deltami.edu.pl/>).