

ALGEBRA LINIOWA Z ELEMENTAMI GEOMETRII ANALITYCZNEJ

WSHE, O/K-CE

1. CIAŁA

Definicja 1. Układ $\{\mathbb{K}; 0, 1; +, \cdot\}$ złożony ze zbioru $\mathbb{K}$, dwóch wyróżnionych elementów $0, 1 \in \mathbb{K}$ oraz dwóch działań $+: \mathbb{K} \times \mathbb{K} \rightarrow \mathbb{K}$, $\cdot: \mathbb{K} \times \mathbb{K} \rightarrow \mathbb{K}$ nazywamy *ciałem* jeżeli spełnione są następujące warunki:

- dla każdych dwóch elementów $a, b \in \mathbb{K}$ zachodzi $a + b = b + a$;
- dla każdego elementu $a \in \mathbb{K}$ zachodzi $a + 0 = 0 + a = a$;
- dla każdych trzech elementów $a, b, c \in \mathbb{K}$ zachodzi $(a + b) + c = a + (b + c)$;
- dla każdego elementu $a \in \mathbb{K}$ istnieje element $b \in \mathbb{K}$ taki, że $a + b = b + a = 0$; określony tak element oznaczmy $-a$;
- dla każdych dwóch elementów $a, b \in \mathbb{K}$ zachodzi $a \cdot b = b \cdot a$;
- dla każdego elementu $a \in \mathbb{K}$ zachodzi $a \cdot 1 = 1 \cdot a = a$;
- dla każdych trzech elementów $a, b, c \in \mathbb{K}$ zachodzi $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
- dla każdego niezerowego elementu $a \in \mathbb{K}$ istnieje element $b \in \mathbb{K}$ taki, że $a \cdot b = b \cdot a = 1$; określony tak element oznaczmy $\frac{1}{a}$;
- dla każdych trzech elementów $a, b, c \in \mathbb{K}$ zachodzi $(a + b) \cdot c = a \cdot c + b \cdot c$.

Przykład 2. Przykłady ciał:

- ciało liczb wymiernych $\mathbb{Q}$;
- ciało liczb rzeczywistych $\mathbb{R}$;

Uwaga 3. Następujące zbiory **nie** są ciałami:

- zbiór liczb naturalnych $\mathbb{N}$;
- zbiór liczb całkowitych $\mathbb{Z}$;

1.1. Ciała skończone (proste).

Stwierdzenie 4. Jeżeli p jest liczbą pierwszą, to układ $\{\mathbb{F}_p; 0, 1; \oplus, \odot\}$, gdzie:

- $\mathbb{F}_p = \{0, 1, \dots, p-1\}$;
- $a \oplus b := a + b \pmod{p}$, $a \odot b := a \cdot b \pmod{p}$

jest ciałem.

Ciało $\mathbb{F}_p$ nazywamy ciałem skończonym p -elementowym. W dalszych rozważaniach będziemy dodawanie/mnożenie w ciałach skończonych oznaczać $+$, $\cdot$.

Uwaga 5. W ciele $\mathbb{F}_p$ elementem przeciwnym do elementu a jest $p-a$ natomiast elementem odwrotnym jest a^{p-1} .

Przykład 6. Przykłady obliczeń w ciałach skończonych:

- w $\mathbb{F}_3$: $2 + 2 = 1$, $2 \cdot 2 = 1$;
- w $\mathbb{F}_5$: $2 + 2 = 4 = -1$, $2 \cdot 3 = 1$, $2 + 3 = 0$;
- w $\mathbb{F}_{127}$: $(87 + 36)^2/74 = 62$.

1.2. Algorytm potęgowania w ciałach skończonych. Załóżmy, iż mamy wykonać potęgowanie a^m w ciele $\mathbb{F}_p$. Sposób postępowania:

- (1) zapisujemy wykładnik w systemie dwójkowym;
- (2) podstawiamy $w := 1$, $k := 1$, $u := a$;
- (3) jeżeli k -ta cyfra dwójkowa jest jedynką, to mnożymy $w := w \cdot u$ (w ciele $\mathbb{F}_p$);
- (4) zwiększamy $k := k + 1$;
- (5) podnosimy u do kwadratu $u := u^2$ (w ciele $\mathbb{F}_p$);
- (6) jeśli pozostały nam cyfry dwójkowe, to wracamy do kroku 3
- (7) w zawiera wynik $w = a^m$ w $\mathbb{F}_p$.

Przykład 7. Chcemy obliczyć 3^{39} w ciele $\mathbb{F}_7$: wyznaczmy $39 = (100111)_2$, zatem

	w	u
	1	3
1	3	$9 \equiv 2 \pmod{7}$
1	6	4
1	$24 \equiv 3 \pmod{7}$	$16 \equiv 2 \pmod{7}$
0	3	4
0	3	2
1	6	4

W wyniku otrzymujemy $3^{39} = 6$ w $\mathbb{F}_7$.

1.3. Ciało liczb zespolonych.

Stwierdzenie 8. Układ $\{\mathbb{R} \times \mathbb{R}; (0, 0), (1, 0); \oplus, \odot\}$, gdzie:

- $(a, b) \oplus (x, y) := (a + x, b + y)$;
- $(a, b) \odot (x, y) := (ax - by, ay + bx)$

jest ciałem.

Określone powyżej ciało nazywamy *ciałem liczb zespolonych* i oznaczamy $\mathbb{C}$. Element $(0, 1)$ oznaczmy literą „ i ”. Możemy wtedy stosować uproszczony zapis $a + bi := (a, b)$. W dalszych rozważaniach będziemy dodawanie/mnożenie w ciele $\mathbb{C}$ oznaczać $+$, $\cdot$.

Uwaga 9. $i^2 = (0, 1) \cdot (0, 1) = (0 - 1, 0 + 0) = (-1, 0) = -1$.

Obserwacja 10.

- $(a + bi) + (x + yi) = (a + x) + (b + y)i$;
- $(a + bi)(x + yi) = ax + ayi + bxi + byi^2 = (ax - by) + (ay + bx)i$.
- Liczba odwrotna do $a + bi$:

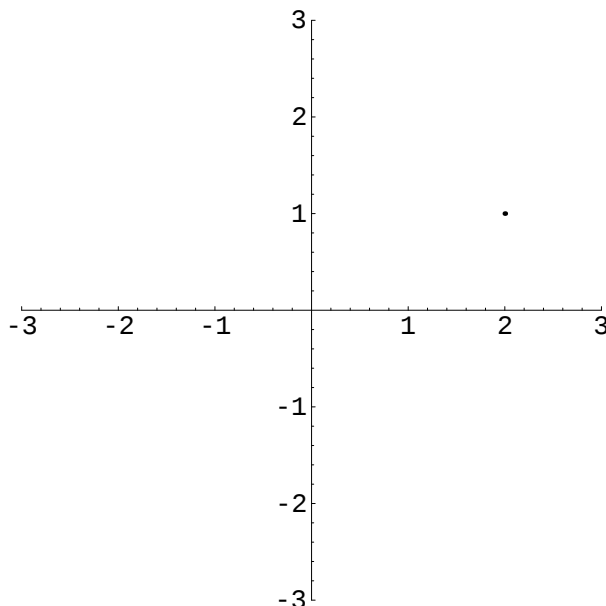
$$\frac{1}{a + bi} = \frac{a - bi}{(a + bi)(a - bi)} = \frac{a - bi}{a^2 + b^2} = \left(\frac{a}{a^2 + b^2}\right) + \left(\frac{-b}{a^2 + b^2}\right)i$$

Definicja 11. Jeśli $z := a + bi \in \mathbb{C}$, to liczbę $a - bi$ nazywamy *liczbą sprzężoną* z z i oznaczamy $\bar{z}$.

Uwaga 12. Własności:

- $\overline{\bar{z}} = z$;
- $\overline{z + w} = \bar{z} + \bar{w}$;
- $\overline{z \cdot w} = \bar{z} \cdot \bar{w}$;

1.4. Interpretacja geometryczna liczb zespolonych. Liczbę $a+bi$ interpretujemy jako punkt na płaszczyźnie $\mathbb{R}^2$ o współrzędnych (a, b) .



RYSUNEK 1. Liczba $2 + i$

Definicja 13. Dla liczby $z = a+bi$ wartość $\sqrt{a^2 + b^2}$ nazywamy modułem (jest to długość promienia wodzącego punktu (a, b)) i oznaczamy $|z|$.

Uwaga 14. Liczbę $z = a + bi$ można zapisać w postaci:

$$z = |z|(x + yi), \quad \text{gdzie} \quad x := \frac{a}{|z|}, \quad y := \frac{b}{|z|}.$$

Wówczas $x^2 + y^2 = 1$ zatem istnieje taka wartość $\varphi \in [0, 2\pi)$, że $\cos \varphi = x$ oraz $\sin \varphi = y$ (jest to kąt między osią OX a promieniem wodzącym punktu (a, b)). Wtedy

$$z = |z|(\cos \varphi + i \sin \varphi).$$

Powyższą postać nazywamy *postacią trygonometryczną* liczby zespolonej. Liczbę φ nazywamy *argumentem* liczby zespolonej.

Uwaga 15. *Własności:*

- $|z \cdot w| = |z| \cdot |w|$;
- $|z + w| \leq |z| + |w|$;
- $|z + w| \geq ||z| - |w||$;

- $|z| = \sqrt{z \cdot \bar{z}}$.

Uwaga 16. Jeżeli $z = |z|(\cos \varphi + i \sin \varphi)$ oraz $w = |w|(\cos \psi + i \sin \psi)$, to

$$\begin{aligned} z \cdot w &= |z||w|(\cos \varphi + i \sin \varphi)(\cos \psi + i \sin \psi) = \\ &= |z \cdot w|(\cos(\varphi + \psi) + i \sin(\varphi + \psi)). \end{aligned}$$

Twierdzenie 17 (Wzór Moivre'a). Jeżeli $z = |z|(\cos \varphi + i \sin \varphi)$, to

$$z^m = |z|^m(\cos m\varphi + i \sin m\varphi).$$

Twierdzenie 18. Jeżeli $z = |z|(\cos \varphi + i \sin \varphi)$, to

$$\sqrt[m]{z} = \left\{ \sqrt[m]{|z|} \left(\cos \frac{\varphi + 2k\pi}{m} + i \sin \frac{\varphi + 2k\pi}{m} \right) : k = 0, 1, \dots, m-1 \right\}.$$

Przykład 19.

$$\begin{aligned} \sqrt[3]{8i} &= \left\{ \sqrt[3]{8} \left(\cos \frac{\pi/2 + 2k\pi}{3} + i \sin \frac{\pi/2 + 2k\pi}{3} \right) : k = 0, 1, 2 \right\} = \\ &= \left\{ 2 \left(\cos \frac{\pi}{6} + i \sin \frac{\pi}{6} \right), 2 \left(\cos \frac{5}{6}\pi + i \sin \frac{5}{6}\pi \right), 2 \left(\cos \frac{3}{2}\pi + i \sin \frac{3}{2}\pi \right) \right\} = \\ &= \left\{ (\sqrt{3} + i), (-\sqrt{3} + i), -2i \right\} \end{aligned}$$

Twierdzenie 20. Dla dowolnej liczby a zachodzi:

$$e^{ia} = \cos(a) + i \sin(a).$$

Tutaj „ e ” oznacza podstawę logarytmu naturalnego.

Wniosek 21. Liczbę $z = |z|(\cos \varphi + i \sin \varphi)$ można zapisać w postaci

$$z = |z|e^{i\varphi}.$$

Postać tę nazywamy *postacią wykładniczą* liczby zespolonej.

Uwaga 22. Dla $z = |z|(\cos \varphi + i \sin \varphi) = |z|e^{i\varphi}$ mamy

$$z^m = \left(|z|e^{i\varphi} \right)^m = |z|^m e^{im\varphi} = |z|^m (\cos m\varphi + i \sin m\varphi).$$

2. METODA GAUSSA ROZWIĄZYWANIA UKŁADÓW RÓWNAŃ LINIOWYCH

Z układem równań liniowych nad ciałem $\mathbb{K}$

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases}$$

możemy związać macierz (uzupełnioną) tego układu:

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \cdots & & & & \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{pmatrix}$$

2.1. Algorytm eliminacji Gaussa. Stosując następujące operacje *elementarne* na macierzy/układzie

- przemnożenie wiersza przez niezerowy skalar
- dodanie do i -tego wiersza, wiersza j -tego przemnożonego ewentualnie przez skalar
- zmiana kolejności wierszy
- skreślenie wiersza zerowego

doprowadzamy macierz do następującej postaci zredukowanej:

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & c_{1r+1} & \cdots & c_{1n} & d_1 \\ 0 & 1 & 0 & \cdots & 0 & c_{2r+1} & \cdots & c_{2n} & d_2 \\ \cdots & & & & & & & & \\ 0 & 0 & 0 & \cdots & 1 & c_{rr+1} & \cdots & c_{rn} & d_r \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & d_{r+1} \end{pmatrix}$$

Wówczas jeśli $d_{r+1} \neq 0$, to układ nie ma rozwiązania. W przeciwnym wypadku wszystkie rozwiązania układu otrzymujemy:

$$\begin{cases} x_1 = d_1 - c_{1r+1}t_1 - \cdots - c_{1n}t_{n-r} \\ x_2 = d_2 - c_{2r+1}t_1 - \cdots - c_{2n}t_{n-r} \\ \cdots \\ x_r = d_r - c_{rr+1}t_1 - \cdots - c_{rn}t_{n-r}, \end{cases}$$

gdzie współczynniki $t_1, \dots, t_{n-r}$ są *dowolnymi* elementami ciała $\mathbb{K}$.

Przykład 23. Rozwiążemy nad ciałem $\mathbb{Q}$ liczb wymiernych układ równań:

$$\begin{cases} 2x_1 + 4x_2 + 2x_3 + 6x_4 = 6 \\ 3x_1 + 10x_2 + 10x_3 - 22x_4 = 8 \\ 2x_1 + 7x_2 + 7x_3 - 16x_4 = 5 \end{cases}$$

Budujemy macierz układu i dokonujemy przekształceń elementarnych:

$$\begin{aligned} & \begin{pmatrix} 2 & 4 & 2 & 6 & 6 \\ 3 & 10 & 10 & -22 & 8 \\ 2 & 7 & 7 & -16 & 5 \end{pmatrix} \cdot \frac{1}{2} \rightsquigarrow \begin{pmatrix} 1 & 2 & 1 & 3 & 3 \\ 3 & 10 & 10 & -22 & 8 \\ 2 & 7 & 7 & -16 & 5 \end{pmatrix} \begin{matrix} \\ -3 \cdot I \\ -2 \cdot I \end{matrix} \rightsquigarrow \\ & \rightsquigarrow \begin{pmatrix} 1 & 2 & 1 & 3 & 3 \\ 0 & 4 & 7 & -31 & -1 \\ 0 & 3 & 5 & -22 & -1 \end{pmatrix} \begin{matrix} \\ \\ -III \end{matrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & 1 & 3 & 3 \\ 0 & 1 & 2 & -9 & 0 \\ 0 & 3 & 5 & -22 & -1 \end{pmatrix} \begin{matrix} \\ \\ -2 \cdot II \\ -3 \cdot II \end{matrix} \rightsquigarrow \\ & \rightsquigarrow \begin{pmatrix} 1 & 0 & -3 & 21 & 3 \\ 0 & 1 & 2 & -9 & 0 \\ 0 & 0 & -1 & 5 & -1 \end{pmatrix} \begin{matrix} -3 \cdot III \\ 2 \cdot III \\ \cdot (-1) \end{matrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 6 & 6 \\ 0 & 1 & 0 & 1 & -2 \\ 0 & 0 & 1 & -5 & 1 \end{pmatrix} \end{aligned}$$

Ostatnia macierz jest zredukowana i reprezentuje układ:

$$\begin{cases} x_1 + 6x_4 = 6 \\ x_2 + x_4 = -2 \\ x_3 - 5x_4 = 1, \end{cases}$$

którego wszystkie rozwiązania są postaci:

$$\begin{cases} x_1 = 6 - 6t \\ x_2 = -2 - t \\ x_3 = 1 + 5t \\ x_4 = t, \end{cases}$$

gdzie t jest dowolną liczbą wymierną.

3. PRZESTRZENIE LINIOWE (WEKTOROWE)

Definicja 24. Układ $\{V, \mathbb{K}; +, \cdot; \Theta\}$ — gdzie V jest zbiorem, $\mathbb{K}$ ciałem, $+: V \times V \rightarrow V$ działaniem wewnętrznym, $\cdot: \mathbb{K} \times V \rightarrow V$ działaniem zewnętrznym oraz $\Theta \in V$ wyróżnionym elementem — nazywamy *przestrzenią liniową* V nad ciałem $\mathbb{K}$ jeśli spełnione są następujące warunki:

- dla każdych dwóch wektorów $v, w \in V$ zachodzi $v + w = w + v$;
- dla każdych trzech wektorów $u, v, w \in V$ zachodzi $(u + v) + w = u + (v + w)$;
- dla każdego wektora $v \in V$ zachodzi $v + \Theta = \Theta + v = v$;
- dla każdego wektora $v \in V$ istnieje $w \in V$ taki, że $v + w = \Theta$, wektor w oznaczamy $-v$;
- dla każdego skalaru $x \in \mathbb{K}$ oraz każdych dwóch wektorów $v, w \in V$ zachodzi $x(v + w) = x \cdot v + x \cdot w$;
- dla każdych dwóch skalarów $x, y \in K$ oraz każdego wektora $v \in V$ zachodzi $(x + y) \cdot v = x \cdot v + y \cdot v$;
- dla każdych dwóch skalarów $x, y \in K$ oraz każdego wektora $v \in V$ zachodzi $(x \cdot y) \cdot v = x \cdot (y \cdot v)$;
- dla każdego wektora $v \in V$ zachodzi $1 \cdot v = v$.

Przykład 25. Zbiór wektorów swobodnych na płaszczyźnie jest przestrzenią liniową.

Uwaga 26.

- $0 \cdot v = \Theta$, dla każdego wektora $v \in V$;
- $x \cdot \Theta = \Theta$, dla każdego skalaru $x \in \mathbb{K}$;
- $-1 \cdot v = -v$, dla każdego wektora $v \in V$.

Uwaga 27. Jeżeli $\mathbb{K}$ jest dowolnym ciałem, to $\mathbb{K}^n := \mathbb{K} \times \dots \times \mathbb{K}$ z działaniami $[x_1, \dots, x_n] + [y_1, \dots, y_n] := [x_1 + y_1, \dots, x_n + y_n]$ oraz $x \cdot [y_1, \dots, y_n] := [xy_1, \dots, xy_n]$ jest przestrzenią liniową.

Uwaga 28. Zbiór macierzy zadanego wymiaru o współczynnikach z ciała $\mathbb{K}$ jest przestrzenią liniową.

4. LINIOWA ZALEŻNOŚĆ WEKTORÓW

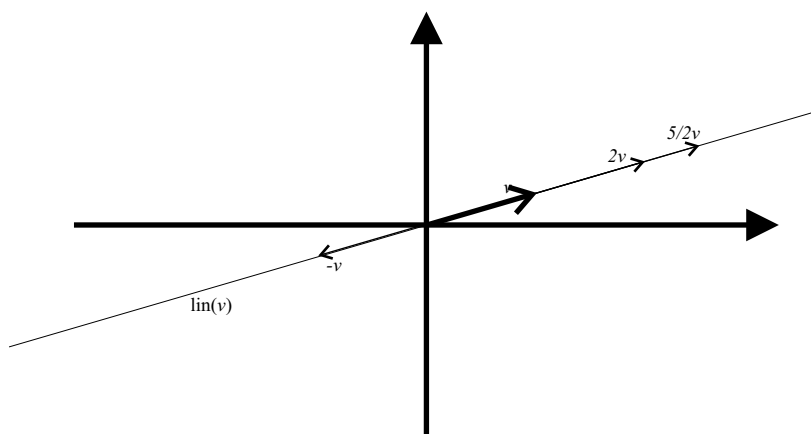
Definicja 29. Jeżeli V jest przestrzenią liniową nad ciałem $\mathbb{K}$ oraz $v_1, \dots, v_n \in V$, to *kombinacją liniową* wektorów $v_1, \dots, v_n$ nazywamy każdy wektor v postaci $v = x_1 v_1 + \dots + x_n v_n$, gdzie $x_1, \dots, x_n$ są dowolnymi skalarami z ciała $\mathbb{K}$. Zbiór wszystkich kombinacji liniowych wektorów $v_1, \dots, v_n$ oznaczamy $\text{lin}(v_1, \dots, v_n)$.

Uwaga 30. $\text{lin}(v) = \{x \cdot v : x \in \mathbb{K}\}$.

Przykład 31. Weźmy $V := \mathbb{K}^n$ i oznaczmy

$$\varepsilon_1 := [1, 0, \dots, 0], \varepsilon_2 := [0, 1, 0, \dots, 0], \dots, \varepsilon_n := [0, \dots, 0, 1].$$

Wtedy $\text{lin}(\varepsilon_1, \dots, \varepsilon_n) = V$, zaś $\text{lin}(\varepsilon_1, \varepsilon_2) = \{[x, y, 0, \dots, 0] : x, y \in \mathbb{K}\}$.



RYSUNEK 2. Interpretacja geometryczna $\text{lin}(v)$

Definicja 32. Skończony układ wektorów $v_1, \dots, v_n \in V$ nazywamy *liniowo zależnym* jeśli istnieją takie skalary $x_1, \dots, x_n \in \mathbb{K}$ **nie wszystkie równe zero**, że $x_1 v_1 + \dots + x_n v_n = \Theta$.

Przykład 33.

- układ $(\Theta, v_2, \dots, v_n)$ jest liniowo zależny. ($1 \cdot \Theta + 0v_2 + \dots + 0v_n = \Theta$);
- układ (v, v) jest liniowo zależny ($1 \cdot v + (-1) \cdot v = \Theta$).

Twierdzenie 34. Układ wektorów $v_1, \dots, v_n$ jest liniowo zależny wtedy i tylko wtedy, gdy pewien wektor tego układu jest kombinacją liniową pozostałych wektorów tego układu.

Definicja 35. Układ wektorów, który nie jest liniowo zależny nazywamy *liniowo niezależnym*.

Przykład 36. Wektory $\varepsilon_1, \dots, \varepsilon_n$ są liniowo niezależne.

Twierdzenie 37. *Jeżeli układ $(v_1, \dots, v_n)$ jest liniowo niezależny, to każdy podukład $(v_{i_1}, \dots, v_{i_k})$ tego układu też jest liniowo niezależny.*

4.1. Operacje elementarne na układzie wektorów.

Twierdzenie 38. *Jeżeli układ wektorów $w_1, \dots, w_n$ powstaje z układu $v_1, \dots, v_n$ za pomocą skończonej ilości operacji:*

- *mnożenia jednego z wektorów układu przez niezerowy skalar;*
- *dodania do i -tego wektora, wektora j -tego, pomnożonego ewentualnie przez skalar ($i \neq j$);*
- *zmiany porządku wektorów w układzie.*

Wówczas układ $w_1, \dots, w_n$ jest liniowo niezależny wtedy i tylko wtedy, gdy układ $v_1, \dots, v_n$ jest liniowo niezależny.

Przykład 39. Sprawdzić czy układ wektorów $v_1 := [2, 4, 2, 6, 6]$, $v_2 = [3, 10, 10, -22, 8]$, $v_3 = [2, 7, 7, -16, 5]$ jest liniowo niezależny. Poprzez operacje jak poprzednio doprowadzamy układ do postaci

$$w_1 = [1, 0, 0, 6, 6], w_2 = [0, 1, 0, 1, -2], w_3 = [0, 0, 1, -5, 1].$$

Dla tego układu łatwo wykazać liniową niezależność. Istotnie przypuśćmy, że

$$\Theta = x_1 w_1 + x_2 w_2 + x_3 w_3 = [x_1, x_2, x_3, 6x_1 + x_2 - 5x_3, 6x_1 - 2x_2 + x_3].$$

Czyli $x_1 = x_2 = x_3 = 0$, a zatem układ jest liniowo niezależny.