Spis treści

1

Arytmetyka liczb całkowitych

Zbiór liczb *całkowitych* oznaczamy przez $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$. Zbiór liczb *naturalnych* oznaczamy przez $\mathbb{N} = \{1, 2, 3, ...\}$.

1.1 Podzielność

Definicja 1 *Niech $a, b \in \mathbb{Z}$. Mówimy, że b* dzieli *a (co zapisujemy jako $b \mid a$) jeżeli istnieje liczba całkowita $n \in \mathbb{Z}$ taka, że $a = bn$. Liczbę b nazywamy* dzielnikiem *liczby a. Liczbę a nazywamy* wielokrotnością *liczby b.*

Twierdzenie 2 *Niech a, b, c, n będą liczbami całkowitymi. Wówczas:*

1. *$1 \mid a$ i $a \mid a$.*
2. *Jeżeli $a \mid b$ i $b \mid c$, to $a \mid c$.*
3. *Jeżeli $n \mid a$ i $n \mid b$, to $n \mid ax + by$, dla dowolnych $x, y \in \mathbb{Z}$.*

Twierdzenie 3 (O dzieleniu z resztą) *Niech $a \in \mathbb{Z}$ i $b \in \mathbb{N}$. Wówczas istnieje dokładnie jedna para liczb całkowitych q, r taka, że*

$$a = bq + r \ \text{ i } 0 \leq r < b.$$

Liczbę q nazywamy ilorazem*, a liczbę r nazywamy* resztą *(z dzielenia a przez b).*

Dowód. Przyjmując $q = \left\lfloor \frac{a}{b} \right\rfloor$ i $r = a - b\left\lfloor \frac{a}{b} \right\rfloor$ dostajemy parę spełniającą tezę twierdzenia. Ponadto, warunki twierdzenia określają tę parę jednoznacznie. W istocie, przypuśćmy, że mamy również $a = bq' + r'$ i $0 \le r' < b$. Wówczas $b(q - q') = r' - r$. Stąd $q - q' = 0$. ■

Największy wspólny dzielnik liczb całkowitych a i b oznaczamy przez (a, b).

Definicja 4 *Jeżeli $(a, b) = 1$, to mówimy, że liczby a i b są* względnie pierwsze*.*

Twierdzenie 5 (Euklides) *Niech $a, b \in \mathbb{N}$. Jeżeli $(a, b) = 1$ to istnieją liczby całkowite x, y takie, że*

$$ax + by = 1.$$

Dowód. Niech $a \le b$. Jeżeli $a = b = 1$, to można przyjąć $x = 1$ i $y = 0$. Przypuśćmy, że twierdzenie jest prawdziwe dla wszystkich par liczb względnie pierwszych, których suma jest mniejsza niż $a + b$. Niech

$$b = aq + r$$

gdzie $r < a$ jest resztą z dzielenia b przez a. Z własności podzielności wynika, że $1 = (a, b) = (a, r)$. Ponieważ

$$a + b \ge a + a > a + r$$

więc, na mocy założenia indukcyjnego, istnieją liczby całkowite x', y' takie, że

$$ax' + ry' = 1.$$

Podstawiając do tego równania $r = b - aq$ dostajemy

$$\begin{aligned} ax' + (b - aq)y' &= 1 \\ a(x' - qy') + by' &= 1. \end{aligned}$$

Zatem, $x = x' - qy'$ i $y = y'$ są liczbami całkowitymi spełniającymi równanie $ax + by = 1$. ■

Wniosek 6 *Jeżeli $(a, b) = 1$ i $a \mid bc$, to $a \mid c$.*

Dowód. Niech x, y będą liczbami całkowitymi, które spełniają równanie $ax + by = 1$. Wówczas

$$acx + bcy = c.$$

Ponieważ $a \mid bc$, więc $a \mid acx + bcy = c$. ■

1.2 Liczby pierwsze

Definicja 7 *Liczbę naturalną p nazywamy* liczbą pierwszą *jeżeli $p > 1$ i jedynymi jej dzielnikami są* 1 *i p. Liczbę naturalną $n > 1$, która nie jest liczbą pierwszą nazywamy liczbą* złożoną.

Jeżeli $n > 1$ jest liczbą złożoną, to istnieje rozkład $n = ab$ na iloczyn liczb naturalnych spełniających warunek $1 < a, b < n$. Jeżeli p jest liczbą pierwszą i $p = ab$, to musi być $a = 1$ i $b = p$ (lub $a = p$ i $b = 1$).

Liczby pierwsze możemy zdefiniować również w następujący geometryczny sposób. Dla każdego $k \in \mathbb{N}$ zdefiniujmy zbiór punktów $A_k = \{(k, kn) : n = 1, 2, ...\}$ i rozważmy sumę $A = A_1 \cup A_2 \cup ....$ Liech L_n będzie prostą o równaniu $x = n$. Wówczas p jest liczbą pierwszą wtedy i tylko wtedy, gdy $|L_p \cap A| = 2$.

Twierdzenie 8 *Jeżeli p jest liczbą pierwszą i $p \mid ab$, to $p \mid a$ lub $p \mid b$.*

Dowód. Jeżeli p nie dzieli a, to mamy $(p, a) = 1$. Stąd, na mocy Wniosku ?, $p \mid b$. Podobnie, jeżeli p nie dzieli b, to musi dzielić a. ■

Twierdzenie 9 *Niech $n > 1$ będzie liczbą naturalną. Najmniejszy dzielnik liczby n większy od* 1 *jest liczbą pierwszą. Ponadto, jeżeli n jest liczbą złożoną, to dzielnik ten nie przekracza $\sqrt{n}$.*

Dowód. Niech $p > 1$ będzie najmniejszym dzielnikiem liczby n. Przypuśćmy, że p jest liczbą złożoną i $p = ab$, $1 < a, b < p$. Wówczas $a \mid n$ i $a < p$, co przeczy minimalności p. Zatem p musi być liczbą pierwszą.

Jeżeli n jest liczbą złożoną, to $n = ab$, przy czym $1 < a \leq b < n$. Zauważmy, że $a \leq \sqrt{n}$ (ponieważ $n = ab \geq aa \geq a^2$). Niech q będzie najmniejszym dzielnikiem pierwszym liczby a. Ponieważ q jest dzielnikiem n, więc $p \leq q$. Z drugiej strony $q \leq a \leq \sqrt{n}$, a więc $p \leq \sqrt{n}$. ■

Twierdzenie 10 (Euklides) *Liczb pierwszych jest nieskończenie wiele.*

Dowód. Niech p_k oznacza k-tą z kolei liczbę pierwszą i niech $a = p_1 p_2 ... p_k$ będzie iloczynem wszystkich liczb pierwszych od p_1 do p_k. Rozważmy liczbę

$$n = a + 1 = p_1 p_2 ... p_k + 1.$$

Niech p będzie najmniejszym dzielnikiem pierwszym liczby n. Pokażemy, że $p > p_k$. W istocie, przypuśćmy, że $p = p_i$ dla pewnego $i = 1, ..., k$. Ponieważ, $p \mid n$ i $p \mid a$, więc

$$p \mid n - a = 1.$$

To jest sprzeczność. Zatem p nie może być żadną z liczb pierwszych $p_1, ..., p_k$. Wobec tego zbiór liczb pierwszych nie może być skończony. ■

Twierdzenie 11 *Istnieją dowolnie duże odstępy między kolejnymi liczbami pierwszymi.*

Dowód. Niech $n \geq 2$ będzie dowolną liczbą naturalną. Rozważmy ciąg $n - 1$ kolejnych liczb naturalnych

$$n! + 2, n! + 3, ..., n! + n.$$

Żadna z tych liczb nie jest liczbą pierwszą. ■

Twierdzenie 12 (Postulat Bertranda) *Dla każdego n, między n a $2n$ znajduje się liczba pierwsza.*

Rozważmy naturalne ustawienie liczb $1, 2, ..., n^2$ w kwadrat K_n. Na przykład, dla $n = 5$ mamy

$$K_5 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 \\ 16 & 17 & 18 & 19 & 20 \\ 21 & 22 & 23 & 24 & 25 \end{bmatrix}.$$

Conjecture 13 (Sierpiński) *W każdym wierszu kwadratu K_n znajduje się liczb pierwsza.*

Definicja 14 *Mówimy, że funkcje $f(n)$ i $g(n)$ są równe asymptotycznie (co zapisujemy jako $f(n) \sim g(n)$) jeżeli*

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1.$$

Niech $\pi(n)$ oznacza liczbę liczb pierwszych nie większych od n. Poniższe twierdzenie orzeka, że prawdopodobieństwo tego, że losowo wybrana liczba spośród $1, ..., n$ jest pierwsza dąży do $1/\ln n$ przy $n \to \infty$.

Twierdzenie 15 (Twierdzenie o Liczbach Pierwszych) $\pi(n) \sim \frac{n}{\ln n}$.

Twierdzenie 16 (Dirichlet) *Jeżeli $(a, b) = 1$, to ciąg arytmetyczny $an + b$, $n = 0, 1, 2, ...$ zawiera nieskończenie wiele liczb pierwszych.*

Twierdzenie 17 (Green & Tao, 2004) *Istnieją dowolnie długie ciągi arytmetyczne składające się z samych liczb pierwszych.*

1.3 Podstawowe Twierdzenie Arytmetyki

Każda liczba całkowita $n > 1$ rozkłada się na iloczyn liczb pierwszych. Oczywiście czynniki w iloczynie mogą się powtarzać; możemy je wówczas pogrupować, zapisać w postaci potęg i uporządkować według wielkości podstaw. W ten sposób otrzymamy *rozkład kanoniczny* liczby n:

$$n = p_1^{k_1} p_2^{k_2} ... p_s^{k_s},$$

gdzie $p_1 < p_2 < ... < p_s$ są różnymi liczbami pierwszymi, a $k_i \geq 1$ dla $i = 1, 2, ..., s$.

Twierdzenie 18 (Podstawowe Twierdzenie Arytmetyki) *Rozkład kanoniczny liczby całkowitej $n > 1$ jest jednoznaczny.*

Dowód. Załóżmy, że istnieją liczby złożone, które mają różne rozkłady kanoniczne. Niech N będzie najmniejszą z takich liczb. Mamy więc

$$N = p_1 p_2 ... p_k = q_1 q_2 ... q_m,$$

gdzie p_i, q_j są liczbami pierwszymi. Zauważmy, że p_1 nie może być równe żadnej z liczb q_j, ponieważ wtedy liczba N/p_1 byłaby liczbą mniejszą od N posiadającą dwa różne rozkłady kanoniczne. Niech $a_j = q_j q_{j+1} ... q_m$. Ponieważ $p_1 \mid q_1 a_2$, więc $p \mid q_1$ lub $p \mid a_2$. W pierwszym przypadku mamy $p_1 = q_1$, co już wykluczyliśmy, zatem musi być $p_1 \mid a_2$. Ale wówczas mamy $p_1 \mid q_2 a_3$ i stąd $p_1 \mid q_2$ lub $p_1 \mid a_3$. Podobnie, pierwszy przypadek oznacza, że $p_1 = q_2$ co przeczy minimalności N, a więc mamy $p_1 \mid a_3$. Kontynuując w ten sposób dostajemy w końcu $p \mid a_m = q_m$, czyli $p_1 = q_m$, co tak samo przeczy minimalności N. To kończy dowód. ■

1.4 Arytmetyka modulo m

Niech $m > 0$ będzie ustaloną liczbą całkowitą. Rozważmy zbiór wszystkich reszt z dzielenia przez m

$$\mathbb{Z}_m = \{0, 1, ..., m-1\}.$$

W zbiorze reszt $\mathbb{Z}_m$ określamy działania dodawania i mnożenia *modulo* m przyjmując za wynik resztę z dzielenia przez m zwykłej sumy $a+b$ i zwykłego iloczynu ab liczb $a, b \in \mathbb{Z}_m$. Działania modulo m oznaczamy zwykłymi symbolami działań arytmetycznych z ewentualnym dopiskiem $(\mathrm{mod}\, m)$. Na przykład

$$3 + 4 = 2 \ (\mathrm{mod}\, 5),\ \ 2 \times 4 = 3 \ (\mathrm{mod}\, 5).$$

Dopisek $(\mathrm{mod}\, m)$ zwykle opuszczamy jeżeli liczba m jest ustalona i jasna z kontekstu.

Wyniki dodawania i mnożenia $(\mathrm{mod}\, m)$ dogodnie jest przedstawiać w formie tabliczki (na wzór tabliczki mnożenia). Na przykład, dla $m = 6$ mamy

+	**0**	**1**	**2**	**3**	**4**	**5**
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

×	**0**	**1**	**2**	**3**	**4**	**5**
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Definicja 19 *Niech $a \in \mathbb{Z}_m$. Jeżeli równanie $ax = 1$ ma rozwiązanie w $\mathbb{Z}_m$, to a nazywamy* elementem odwracalnym *w $\mathbb{Z}_m$. Zbiór wszystkich elementów odwracalnych w $\mathbb{Z}_m$ oznaczamy symbolem $\mathbb{Z}_m^*$.*

Na przykład, $\mathbb{Z}_6^* = \{1, 5\}$.

Twierdzenie 20 *Element $a \in \mathbb{Z}_m$ jest odwracalny wtedy i tylko wtedy, gdy liczby a i m są względnie pierwsze.*

Dowód. Przypuśćmy, że a jest elementem odwracalnym w $\mathbb{Z}_m$. Niech $x \in \mathbb{Z}_m$ będzie rozwiązaniem równania $ax = 1$. To oznacza, że liczba całkowita ax zostawia resztę 1 przy dzieleniu przez m:

$$ax = mq + 1.$$

Niech $d = (a, m)$. Ponieważ $d \mid a$ i $d \mid m$ więc $d \mid ax$ i $d \mid mq$ i w konsekwencji $d \mid ax - mq = 1$. Stąd $d = 1$.

Na odwrót, przypuśćmy, że $(a, m) = 1$. Niech $x < y$ będą dowolnymi elementami z $\mathbb{Z}_m$. Przypuśćmy, że $ax = ay$ w $\mathbb{Z}_m$. Wówczas $a(y - x) = 0$, co oznacza, że $m \mid a(y - x)$. Na mocy Wniosku ? otrzymujemy $m \mid y - x$. Ale $0 < y - x < m$ co daje sprzeczność. Zatem, jeżeli $x \neq y$, to $ax \neq ay$ w $\mathbb{Z}_m$. Wobec tego, wśród elementów

$$a \cdot 0, a \cdot 1, ..., a \cdot (m - 1)$$

żadne dwa nie są identyczne, a ponieważ jest ich tyle samo ile wszystkich reszt $(\bmod\, m)$, więc któryś z nich musi być równy 1. Stąd, $ax = 1$ dla pewnego $x \in \mathbb{Z}_m$, co oznacza, że a jest elementem odwracalnym. ■

1.5 Funkcja Eulera

Niech n będzie liczbą naturalną. Symbolem $\varphi(n)$ oznaczamy liczbę nieskracalnych ułamków właściwych o mianowniku n. Na przykład, $\varphi(18) = 6$:

$$\frac{1}{18}, \frac{5}{18}, \frac{7}{18}, \frac{11}{18}, \frac{13}{18}, \frac{17}{18}.$$

Funkcja $n \mapsto \varphi(n)$ nosi nazwę *funkcji Eulera.*

Twierdzenie 21 *Niech $n = p_1^{k_1} p_2^{k_2} ... p_r^{k_r}$, będzie rozkładem kanonicznym liczby n. Wówczas*

$$\varphi(n) = (p^{k_1} - p^{k_1 - 1})(p^{k_2} - p^{k_2 - 1})...(p^{k_r} - p^{k_r - 1}).$$

Dowód. Rozważmy zbiór U_n wszystkich ułamków właściwych o mianowniku n. Spośród nich dokładnie $\frac{n}{p_1}$ ułamków skraca się przez p_1. Odrzucając każdy taki ułamek pozostanie $n - \frac{n}{p_1} = n\left(1 - \frac{1}{p_1}\right)$ ułamków. Wśród tych $n\left(1 - \frac{1}{p_1}\right)$ ułamków znajduje się dokładnie $\frac{1}{p_2} n\left(1 - \frac{1}{p_1}\right)$ takich, których licznik dzieli się przez p_2. Zatem, po ich odrzuceniu pozostanie

$$n\left(1 - \frac{1}{p_1}\right) - \frac{1}{p_2} n\left(1 - \frac{1}{p_1}\right) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)$$

ułamków. Postępując dalej w ten sam sposób aż do ostatniego czynnika p_r, usuniemy ze zbioru U_n wszystkie ułamki skracalne, a liczba tych, które pozostaną wyniesie dokładnie

$$n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_r}\right).$$

Podstawiając za n rozkład kanoniczny otrzymujemy wzór stanowiący tezę twierdzenia. ■

Wniosek 22 *Jeżeli $(a, b) = 1$, to $\varphi(ab) = \varphi(a)\varphi(b)$.*

Twierdzenie 23 (Euler) *Jeżeli a jest elementem odwracalnym w $\mathbb{Z}_m$, to $a^{\varphi(m)} = 1 (\mathrm{mod}\, m)$.*

Dowód. Niech $a \in \mathbb{Z}_m^*$ i niech $r_1, ..., r_k \in \mathbb{Z}_m^*$ będzie dowolnym ustawieniem wszystkich elmentów odwracalnych w ciąg. Na mocy Twierdzenia ? mamy $k = \varphi(m)$. Rozważmy ciąg $ar_1, ar_2, ..., ar_k$. Żadne dwa z jego wyrazów nie są równe ponieważ $ar_i = ar_j$ implikuje $r_i = r_j$. Ponadto każdy z wyrazów ar_i jest odwracalny (odwrotnością elementu ar_i jest iloczyn $a^{-1} r_i^{-1}$). Stąd ciąg $ar_1, ..., ar_k$ jest permutacją wyrazów ciągu $r_1, ..., r_k$. Zatem

$$(ar_1)(ar_2)...(ar_k) = r_1 r_2 ... r_k.$$

Stąd

$$a^k r_1 r_2 ... r_k = r_1 r_2 ... r_k.$$

Wobec tego, że każdy element r_i jest odwracalny, ostatnia równość implikuje $a^k = 1$. ■

2

Liczby zespolone

2.1 Liczby rzeczywiste

Zbiór *liczb rzeczywistych* będziemy oznaczać przez $\mathbb{R}$. Zbiór *liczb wymiernych* oznaczamy literą $\mathbb{Q}$. Przpomnijmy, że każdą liczbę wymierną możemy przedstawić w postaci ułamka $\frac{a}{b}$, gdzie a i b są liczbami całkowitymi, przy czym $b \neq 0$. Będziemy w dalszym ciągu wykorzystywać naturalną geometryczną interpretację liczb rzeczywistych jako punktów na prostej (osi liczbowej).

Twierdzenie 24 *Każdy odcinek o dodatniej długości na osi liczbowej zawiera liczbę wymierną.*

Dowód. Niech x i y będą dowolnymi różnymi punktami na prostej i niech d oznacza odległość między x i y. Wybierzmy liczbę naturalną n tak, aby $\frac{1}{n} < 2d$. Wówczas odkładając odcinek o długości $\frac{1}{n}$ odpowiednią liczbę razy, powiedzmy m, dostaniemy liczbę $\frac{m}{n}$ znajdującą się między x a y. ■

Twierdzenie 25 *Zbiór liczb wymiernych można ustawić w ciąg.*

Dowód. Najpierw ustawimy w ciąg liczby wymierne dodatnie. Można to zrobić na przykład według wzrostu sumy licznika i mianownika:

$$\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{3}{1}, \frac{1}{4}, \frac{2}{3}, \frac{3}{2}, \frac{4}{1}, \dots .$$

W ten sposób, każdy ułamek nieskracalny dodatni (czyli każda liczba wymierna dodatnia) ma swoje miejsce w tym ciągu. Ułamki ujemne ustawiamy tak samo i przeplatamy z dodatnimi umieszczając dodatkowo na początku liczbę 0:

$$0, \frac{1}{1}, -\frac{1}{1}, \frac{1}{2}, -\frac{1}{2}, \frac{2}{1}, -\frac{2}{1}, \frac{1}{3}, -\frac{1}{3}, \frac{3}{1}, -\frac{3}{1}, \frac{1}{4}, -\frac{1}{4}, \dots .$$

■

Twierdzenie 26 *Zbioru liczb rzeczywistych nie da się ustawić w ciąg.*

Dowód. Przypuśćmy, że ciąg P_1, P_2,... zawiera wszystkie liczby rzeczywiste. Niech I będzie dowolnym odcinkiem o dodatniej długości. Wybierzmy odcinek I_1 zawarty w I tak aby punkt P_1 nie należał do I_1. Następnie wybierzmy odcinek $I_2 \subset I_1$, tak aby $P_2 \notin I_2$. Postępując tak dalej otrzymamy ciąg odcinków $I_1 \supset I_2 \supset \dots$ takich, że $P_i \notin I_i$, dla $i = 1, 2, \dots$. Niech P będzie punktem należącym do każdego z odcinków I_i. Wówczas $P \neq P_i$ dla każdego $i = 1, 2, \dots$. Zatem, ciąg $P_1, P_2, \dots$ nie może zawierać wszystkich liczb rzeczywistych. ■

Twierdzenie 27 *Długość przekątnej kwadratu o boku* 1 *nie jest liczbą wymierną.*

Dowód. Niech x oznacza długość przekątnej kwadratu o boku 1. Przypuśćmy, że $x = \frac{a}{b}$, dla pewnych liczb naturalnych a i b. Z Twierdzenia Pitagorasa dostajemy

$$1^2 + 1^2 = x^2.$$

Stąd

$$a^2 = 2b^2.$$

Ale to równanie jest sprzeczne z Podstawowym Twierdzeniem Arytmetyki. W istocie, kwadrat każdej liczby naturalnej zawiera w rozkładzie *parzystą* liczbę dwójek. Zatem liczba dwójek w rozkładzie a^2 jest parzysta, natomiast liczba dwójek w rozkładzie $2b^2$ jest nieparzysta. ■

Definicja 28 *Liczbę rzeczywistą α nazywamy* liczbą algebraiczną *jeżeli istnieje wielomian $f(x)$ o współczynnikach wymiernych taki, że $f(\alpha) = 0$.* Stopniem *liczby algebraicznej α nazywamy najmniejszą liczbę całkowitą $n = \deg(\alpha)$ taką, że istnieje wielomian $f(x)$ o współczynnikach wymiernych stopnia n, którego α jest pierwiastkiem.*

Na przykład, każda liczba wymierna q jest liczbą algebraiczną stopnia 1, ponieważ jest pierwiastkiem wielomianu $f(x) = x - q$. Na odwrót, każda liczba algebraiczna stopnia 1 musi byc liczbą wymierną. Liczba $\sqrt{2}$ jest liczbą algebraiczną stopnia 2, ponieważ jest niewymierna i pierwiastkiem wielomianu kwadratowego $f(x) = x^2 - 2$.

Twierdzenie 29 *Zbiór liczb algebraicznych można ustawić w ciąg.*

Dowód. Zbiór wszystkich skończonych ciągów liczb naturalnych można ustawić w ciąg, np. według wielkości sumy wyrazów ciągu:

$$1, 11, 2, 111, 12, 21, 3, 1111, 112, 121, 13, 211, 22, 31, 4, ...$$

Stąd, można ustawić w ciąg wszystkie wielomiany o współczynnikach wymiernych, a ponieważ wielomian stopnia n ma co najwyżej n pierwiastków, więc także ich wszystkie pierwiastki. ■

Z tego twierdzenia wynika w szczególności, że istnieją liczby, które nie są algebraiczne. Nazywamy je liczbami *przestępnymi*. Chociaż wiemy, że musi istnieć nieskończenie wiele liczb przestępnych, to jednak w przypadku konkretnej liczby stwierdzenie czy jest ona przestępna czy nie jest na ogół trudne. Że liczba π jest przestępna udowodnił dopiero Lindemann w roku 1882, a jego dowód rozstrzygnął ostatecznie kwestię słynnej *kwadratury koła*. Problem ten polegał na skonstruowaniu kwadratu o polu równym polu danego koła jednostkowego. Długość boku tego kwadratu powinna wynosić zatem $\sqrt{\pi}$. Jak się okazało znacznie później zadanie to jest niewykonalne.

Przypuśćmy, że mamy dany odcinek o długości 1 i chcemy skonstruować (cyrklem i linijką) odcinek o zadanej długości x. Czy dla każdej liczby rzeczywistej dodatniej x taka konstrukcja istnieje? *Liczby konstruowalne* to długości odcinków, które mogą być skonstruowane geometrycznie.

Twierdzenie 30 *Liczba rzeczywista $x > 0$ jest konstruowalna wtedy i tylko wtedy, gdy jest liczbą algebraiczną, której stopień jest potęgą dwójki.*

Ponieważ liczba $\sqrt{\pi}$ nie jest nawet algebraiczna więc nie jest również konstruowalna.

Podzielmy odcinek $[0, 1]$ na dwa równe odcinki, lewy L i prawy P. Następnie podzielmy każdą z połówek L i P znowu na połowy i oznaczmy je symbolicznie jako LL, LP, PL i PP. I tak dalej. Otrzymujemy w ten sposób *słowa* zbudowane z dwóch liter L i P, a każdemu słowu długości n odpowiada pewien odcinek długości $\frac{1}{2^n}$.

Niech $x \in [0,1]$ będzie liczbą rzeczywistą i niech S_1, S_2, ... będzie ciągiem słów takich, że każdy z odpowiednich przedziałów zawiera liczbę x. Zamieniając L na 0 i P na 1 w słowie S_n dostaniemy *rozwinięcie dwójkowe* liczby x z dokładnością do n miejsc po przecinku.

Podobnie ma się rzecz z *rozwinięciami dziesiętnymi*, z tym, że teraz dzielimy odcinki na 10 identycznych części. Właśnie dlatego potrzebujemy aż dziesięciu cyfr do zapisywania takich rozwinięć. Oto kilka przykładów rozwinięć dziesiętnych ważnych stałych matematycznych:

$\frac{-1+\sqrt{5}}{2} = .\,618\,033\,988\,749\,894\,848\,204\,586\,834\,365\,638\,117\,720\,309\,179\,805\,8$

$\sqrt{2} = 1.\,414\,213\,562\,373\,095\,048\,801\,688\,724\,209\,698\,078\,569\,671\,875\,376\,9$

$\pi = 3.\,141\,592\,653\,589\,793\,238\,462\,643\,383\,279\,502\,884\,197\,169\,399\,375\,1$

$e = 2.\,718\,281\,828\,459\,045\,235\,360\,287\,471\,352\,662\,497\,757\,247\,093\,7$

$\ln 2 = .\,693\,147\,180\,559\,945\,309\,417\,232\,121\,458\,176\,568\,075\,500\,134\,360\,26.$

2.2 Liczby "urojone"

Rozważmy równanie $x^2 + 1 = 0$. Oznaczmy "liczbę" spełniajacą to równanie symbolem i (od ang. *imaginary* = *urojony*). Oczywiście i nie jest liczbą rzeczywistą. Wszystko co na razie możemy powiedzieć o tej "urojonej liczbie" to własność

$$i^2 = -1.$$

Zbiór *liczb zespolonych* powstaje jako efekt końcowy włączenia liczby i do systemu arytmetycznego liczb rzeczywistych.

Definicja 31 *Liczbą zespoloną nazywamy dowolne wyrażenie postaci $a+bi$, gdzie a, b są liczbami rzeczywistymi.*

Zbiór liczb zespolonych będziemy oznaczać przez $\mathbb{C}$.

2.3 Arytmetyka liczb zespolonych

W zbiorze $\mathbb{C}$ określamy działania dodawania i mnożenia jak następuje. Niech $z_1 = a + bi$, $z_2 = c + di$, gdzie $a, b, c, d \in \mathbb{R}$ będą liczbami zespolonymi. Sumę i iloczyn liczb zespolonych z_1, z_2 definiujemy wzorami

$$\begin{aligned} z_1 + z_2 &= (a + c) + (b + d)i \\ z_1 z_2 &= (ac - bd) + (ad + bc)i. \end{aligned}$$

Twierdzenie 32 *Mnożenie liczb zespolonych jest działaniem przemiennym, łącznym i rozdzielnym względem dodawania. Ponadto, dla każdej liczby zespolenej $z \neq 0$ istnieje liczba zespolona t taka, że $zt = 1$.*

Dowód. Dowód twierdzenia zostawiamy do samodzielnego przeprowadzenia. ■

2.4 Geometria liczb zespolonych

Liczbę zespoloną $z = x + yi$ określa para liczb rzeczywistych (x, y). Naturalną geometryczną interpretacją liczb zespolonych jest więc zbiór punktów płaszczyzny; liczbie $z = x + yi$ odpowiada punkt o współrzędnych (x, y).

Niech $P = (x, y)$ będzie punktem odpowiadającym liczbie z i niech $r = \sqrt{x^2 + y^2}$ będzie odległością punktu P od środka układu współrzędnych O. Niech α oznacza kąt (skierowany przeciwnie do ruchu wskazówek zegarka) między odcinkiem PO a dodatnią częścią osi X. Wówczas, z definicji funkcji trygonometrycznych dostajemy

$$z = r(\cos\alpha + i \sin\alpha).$$

Ten zapis nazywamy *postacią trygonometryczną* liczby z.

Twierdzenie 33 *Niech $z = r(\cos\alpha + i\sin\alpha)$, $t = s(\cos\beta + i\sin\beta)$ będą liczbami zespolonymi w postaci trygonometrycznej. Wówczas*

$$zt = rs(\cos(\alpha + \beta) + i \sin(\alpha + \beta)).$$

Dowód. Korzystając z wzorów trygonometrycznych na sinus i cosinus sumy dwóch kątów dostajemy:

$$\begin{aligned} zt &= r(\cos\alpha + i\sin\alpha)\cdot s(\cos\beta + i\sin\beta) \\ &= rs\left((\cos\alpha\cos\beta - \sin\alpha\sin\beta) + i(\sin\alpha\cos\beta + \cos\alpha\sin\beta)\right) \\ &= rs(\cos(\alpha+\beta) + i\sin(\alpha+\beta)). \end{aligned}$$

To kończy dowód. ■

Wniosek 34 *Niech $z = r(\cos\alpha + i\sin\alpha)$. Wówczas $z^n = r^n(\cos n\alpha + i\sin n\alpha)$.*

2.5 Pierwiastki z jedynki i wielokąty foremne

Definicja 35 *Niech t będzie liczbą zespoloną i niech n będzie liczbą naturalną. Pierwiastkiem stopnia n z liczby t nazywamy dowolne rozwiązanie równania $z^n = t$ w zbiorze liczb zespolonych.*

Twierdzenie 36 *Niech $t = s(\cos\beta + i\sin\beta)$, $n \in \mathbb{N}$. Wówczas wszystkie rozwiązania równania $z^n = t$ dane są wzorami:*

$$z_k = \sqrt[n]{s}\left(\cos\frac{\beta+2k\pi}{n} + i\sin\frac{\beta+2k\pi}{n}\right),\ k = 0,1,...,n-1.$$

Dowód. Na mocy Wniosku ? dostajemy

$$\begin{aligned} z_k^n &= \left(\sqrt[n]{s}\right)^n\left(\cos n\cdot\frac{\beta+2k\pi}{n} + i\sin n\cdot\frac{\beta+2k\pi}{n}\right) \\ &= s\left(\cos(\beta+2k\pi) + i\sin(\beta+2k\pi)\right) \\ &= s\left(\cos\beta + i\sin\beta\right). \end{aligned}$$

Ponadto $z_i \neq z_j$ dla $i \neq j$, $(i,j = 0,1,...,n-1)$. Zatem są to wszystkie rozwiązania równania $z^n = t$, ponieważ wielomian stopnia n nie może mieć więcej niż n pierwiastków. ■

Wniosek 37 *Wszyskie pierwiastki stopnia n z liczby $t = 1$ dane są wzorami*

$$\varepsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n},\ k = 0,1,...,n-1.$$

Punkty płaszczyzny odpowiadające liczbom ε_k tworzą n-kąt foremny wpisany w okrąg jednostkowy, którego jednym z wierzchołków jest punkt $(1,0)$. Ponadto,

$$\varepsilon_k \varepsilon_l = \varepsilon_{k+l (\mathrm{mod}\, n)}$$

dla dowolnych $k, l = 0, 1, ..., n-1$.

Liczbę zespoloną $z = x + yi$ nazywamy *liczbą konstruowalną* jeżeli liczby rzeczywiste x i y są konstruowalne. Liczby całkowite postaci

$$F_k = 2^{2^k} + 1, k \geq 0,$$

nazywamy *liczbami Fermata.* Pierwszych pięć liczb Fermata to $3, 5, 17, 257, 65537$. Wszystkie są liczbami pierwszymi. Nie wiadomo, czy istnieje choćby jeszcze jedna liczba pierwsza Fermata.

Twierdzenie 38 (Gauss) *Wielokąt foremny jest konstruowalny wtedy i tylko wtedy, gdy liczba jego wierzchołków ma postać $n = 2^r p_1 p_2 ... p_s$,gdzie $r, s \geq 0$, a $p_1, p_2, ..., p_s$ są różnymi liczbami pierwszymi Fermata.*

Dowód. Niech

$$G_N = \cos \frac{2\pi}{N} + i \sin \frac{2\pi}{N}.$$

Można pokazać, że G_N jest liczbą algebraiczną stopnia $\varphi(N)$. Wystarczy więc zobaczyć, że $\varphi(N)$ jest potęgą dwójki wtedy i tylko wtedy, gdy N ma postać opisaną w tezie twierdzenia. Niech $N = 2^r q_1^{r_1} ... q_s^{r_s}$ będzie rozkładem liczby N na czynniki pierwsze, w którym $r \geq 0, r_i \geq 1$, a liczby q_i są nieparzyste i parami różne. Wówczas

$$\varphi(N) = \varphi(2^r) \prod_{i=1}^{s} q_i^{r_i - 1}(q_i - 1).$$

Stąd $r_i = 1$ i q_i muszą być potęgami dwójki. To kończy dowód. ■

Z tego tiwerdzenia wynika w szczególności, że nie istnieje konstrukcja geometryczna 9-kąta foremnego, natomiast można skonstruować 17-kąt foremny.

2.6 Zasadnicze Twierdzenie Algebry

3

Geometria analityczna

4

Układy równań liniowych i macierze

4.1 Układ równań liniowych

Równanie liniowe można zapisać w ogólnej postaci następująco

$$a_1x_1 + a_2x_2 + ... + a_nx_n = b. \tag{4.1}$$

Liczby $a_1, ..., a_n$ nazywamy *współczynnikami* równania, a liczbę b - *wyrazem wolnym*. Te liczby są w danym równaniu stałe. Natomiast $x_1, ..., x_n$ to *zmienne* lub *niewiadome*.

Rozwiązaniem równania liniowego (1.1) nazywamy dowolny ciąg liczb $s_1, ..., s_n$ spełniających to równanie, to znaczy takich, że jeżeli podstawimy $x_1 = s_1, ..., x_n = s_n$ do równania (1.1) to otrzymamy prawdziwą równość. Na przykład, liczby $2, 3, -4$ stanowią jedno z możliwych rozwiązań równania

$$6x_1 - 3x_2 + 4x_3 = -13,$$

ponieważ kładąc $x_1 = 2$, $x_2 = 3$ i $x_3 = -4$ dostajemy

$$6(2) - 3(3) + 4(-4) = 12 - 9 - 16 = -13.$$

Bardziej ogólnie, zbiór składający się z m równań liniowych, z których każde ma n niewiadomych nazywamy *układem równań liniowych.* Taki układ zapisujemy następująco

$$
\begin{aligned}
a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n &= b_1 \\
a_{21}x_1 + a_{22}x_2 + ... + a_{2n}x_n &= b_2 \\
..... \\
a_{m1}x_1 + a_{m2}x_2 + ... + a_{mn}x_n &= b_m
\end{aligned}
\tag{4.2}
$$

Rozwiązaniem układu równań liniowych (1.2) jest ciąg liczb $s_1, ..., s_n$ spełniających *każde* równanie tego układu. Aby znaleźć wszystkie rozwiązania danego układu równań liniowych można zastosować *metodę eliminacji.* Polega ona, zgrubsza, na eliminowaniu kolejnych niewiadomych z kolejnych równań, aż do otrzymania równania z jedną niewiadomą. Do tego celu służą operacje mnożenia równania przez niezerową stałą i dodawania równań stronami.

Przykład 39 *Rozważmy następujący układ równań.*

$$
\begin{aligned}
x - 3y &= -3 \\
2x + y &= 8.
\end{aligned}
$$

Aby wyeliminować x z drugiego równania dodajemy do niego pierwsze równanie pomnożone przez (-2). Otrzymujemy wówczas równanie

$$7y = 14,$$

skąd dostajemy natychmiast $y = 2$. Następnie podstawiamy $y = 2$ do pierwszego równania i otrzymujemy $x = 3$. Podstawiając obie liczby do równań układu widzimy, że oba równania są spełnione.

Przykład 40 *(brak rozwiązań)*

$$
\begin{aligned}
x - 3y &= -7 \\
2x - 6y &= 7.
\end{aligned}
$$

Przykład 41 $(x = 1, y = -2, z = 3)$

$$x + 2y + 3z = 6$$
$$2x - 3y + 2z = 14$$
$$3x + y - z = -2.$$

Przykład 42 *(nieskończenie wiele rozwiązań, $x = r + 4, y = r - 4, z = r$)*

$$x + 2y - 3z = -4$$
$$2x + y - 3z = 4.$$

Przykład 43 $(x = 2, y = 4)$

$$x + 2y = 10$$
$$2x - 2y = -4$$
$$3x + 5y = 26.$$

Przykład 44 *(brak rozwiązań)*

$$x + 2y = 10$$
$$2x - 2y = -4$$
$$3x + 5y = 20.$$

Metoda eliminacji polega więc na wielokrotnym powtarzaniu następujących trzech operacji.

1. **Zamiana miejscami dwóch równań.**
2. **Mnożenie równania stronami przez niezerową stałą.**
3. **Dodawanie pomnożonego równania do innego równania stronami.**

4.2 Macierze

Na początek przedstawimy szereg podstawowych definicji wraz z ilustrującymi je przykładami.

Definicja 45 Macierzą *A wymiaru $m \times n$ nazywamy prostokątną tablicę zawierającą mn liczb* *ułożonych w m poziomych* wierszach *i n pionowych* kolumnach:

$$A=\begin{bmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ ... & ... & ... & ... \\ a_{m1} & a_{m2} & ... & a_{mn} \end{bmatrix}.$$

W przypadku $m=n$ mówimy, że A jest macierzą kwadratową *wymiaru n, a elementy $a_{11},a_{22},...,a_{nn}$ stanowią jej* główną przekątną. *Macierz A zapisujemy również skrótowo jako*

$$A=[a_{ij}]\,,$$

gdzie $1\le i\le m$ oraz $1\le j\le n$.

Przykład 46 *Rozważmy macierze*

$$\begin{aligned} A &= \begin{bmatrix} 1 & 2 & 3 \\ -1 & 0 & 1 \end{bmatrix},\ B=\begin{bmatrix} 1 & 4 \\ 2 & -3 \end{bmatrix},\ C=\begin{bmatrix} 1 \\ -1 \\ 2 \end{bmatrix}, \\ D &= \begin{bmatrix} 1 & 1 & 0 \\ 2 & 0 & 1 \\ 3 & -1 & 2 \end{bmatrix},\ E=[3]\,,\ F=\begin{bmatrix} -1 & 0 & 2 \end{bmatrix}. \end{aligned}$$

Na przykład A jest macierzą wymiaru 2×3, w której $a_{12}=2$, $a_{21}=-1$. B, D i E są macierzmi kwadratowymi wymiarów 2, 3 i 1, odpowiednio. Ponadto, $b_{22}=-3$, $d_{32}=-1$ i $e_{11}=3$, a liczby 1, 0, 2 leżą na głównej przekątnej macierzy D. Warto podkreślić, że macierze takie jak C i F mogą być również traktowane jako wektory.

Definicja 47 *Macierz kwadratową $A=[a_{ij}]$, w której każdy element leżący poza główną przekątną jest zerem, to znaczy, $a_{ij}=0$, gdy $i\neq j$, nazywamy macierzą* diagonalną.

Przykład 48 *Macierze*

$$G = \begin{bmatrix} 4 & 0 \\ 0 & -2 \end{bmatrix}, \; H = \begin{bmatrix} -3 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

są diagonalne.

Definicja 49 *Macierz diagonalną $A = [a_{ij}]$, której wszystkie elementy na głównej przekątnej są równe, nazywamy macierzą* skalarną. *W notacji matematycznej $a_{ij} = c$, dla $i = j$, oraz $a_{ij} = 0$, jeżeli $i \neq j$.*

Przykład 50 *Następujące macierze są skalarne*

$$I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \; J = \begin{bmatrix} -2 & 0 \\ 0 & -2 \end{bmatrix}.$$

Definicja 51 *Dwie macierze $A = [a_{ij}]$ i $B = [b_{ij}]$ wymiaru $m \times n$ są* równe *jeżeli $a_{ij} = b_{ij}$, dla wszystkich $1 \leq i \leq m$, $1 \leq j \leq n$. Macierze różnych wymiarów nigdy nie są porównywane.*

Definicja 52 (Dodawanie macierzy) *Jeżeli $A = [a_{ij}]$ i $B = [b_{ij}]$ są macierzami wymiaru $m \times n$, to ich sumą jest macierz $C = [c_{ij}]$, także wymiaru $m \times n$, określona warunkiem*

$$c_{ij} = a_{ij} + b_{ij}, \; (1 \leq i \leq m, 1 \leq j \leq n).$$

Innymi słowy, C powstaje przez dodanie odpowiadających sobie elementów macierzy A i B. Oczywiście sumę macierzy A i B zapisujemy jako $A + B$.

Przykład 53 *Jeżeli*

$$A = \begin{bmatrix} 1 & -2 & 4 \\ 2 & -1 & 3 \end{bmatrix} \; i \; B = \begin{bmatrix} 0 & 2 & -4 \\ 1 & 3 & 1 \end{bmatrix},$$

to

$$A + B = \begin{bmatrix} 1+0 & -2+2 & 4+(-4) \\ 2+1 & -1+3 & 3+1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 3 & 2 & 4 \end{bmatrix}.$$

Definicja 54 (Mnożenie macierzy przez liczbę) *Jeżeli* $A = [a_{ij}]$ *jest macierzą wymiaru* $m \times n$*, a* r *jest liczbą rzeczywistą, to iloczynem macierzy* A *przez liczbę* r *jest macierz* $B = [b_{ij}]$ *wymiaru* $m \times n$ *spełniająca warunek*

$$b_{ij} = ra_{ij}, \ (1 \le i \le m, 1 \le j \le n).$$

Iloczyn macierzy A *przez liczbę* r *oznaczamy jako* rA.

Przykład 55 *Jeżeli* $r = -3$ *i*

$$A = \begin{bmatrix} 4 & -2 & 3 \\ 2 & -5 & 0 \\ 3 & 6 & -2 \end{bmatrix},$$

to

$$\begin{aligned} rA &= (-3)\begin{bmatrix} 4 & -2 & 3 \\ 2 & -5 & 0 \\ 3 & 6 & -2 \end{bmatrix} = \begin{bmatrix} (-3)4 & (-3)(-2) & (-3)(3) \\ (-3)2 & (-3)(-5) & (-3)(0) \\ (-3)(3) & (-3)(6) & (-3)(-2) \end{bmatrix} \\ &= \begin{bmatrix} -12 & 6 & -9 \\ -6 & 15 & 0 \\ -9 & -18 & 6 \end{bmatrix}. \end{aligned}$$

Różnicę macierzy A i B definiujemy jako $A - B = A + (-1)B$.

Definicja 56 (Transpozycja macierzy) *Jeżeli* $A = [a_{ij}]$ *jest macierzą* $m \times n$*, to macierz* $A^T = \left[a_{ij}^T\right]$ *wymiaru* $n \times m$ *określoną warunkiem*

$$a_{ij}^T = a_{ji}, \ (1 \le i \le m, 1 \le j \le n),$$

nazywamy transpozycją *macierzy* A*. Innymi słowy, Macierz* A^T *powstaje z macierzy* A *poprzez zamianę wierszy na kolumny.*

Przykład 57 *Niech*

$$A = \begin{bmatrix} 4 & -2 & 3 \\ 0 & 5 & -2 \end{bmatrix}, \ B = \begin{bmatrix} 6 & 2 & -4 \\ 3 & -1 & 2 \\ 0 & 4 & 3 \end{bmatrix}, \ C = \begin{bmatrix} 5 & 4 \\ -3 & 2 \\ 2 & -3 \end{bmatrix},$$

$$D = \begin{bmatrix} 3 & -5 & 1 \end{bmatrix}, \ E = \begin{bmatrix} 2 \\ -1 \\ 3 \end{bmatrix}.$$

Wówczas

$$A^T = \begin{bmatrix} 4 & 0 \\ -2 & 5 \\ 3 & -2 \end{bmatrix}, \ B^T = \begin{bmatrix} 6 & 3 & 0 \\ 2 & -1 & 4 \\ -4 & 2 & 3 \end{bmatrix}, \ C^T = \begin{bmatrix} 5 & -3 & 2 \\ 4 & 2 & -3 \end{bmatrix},$$

$$D^T = \begin{bmatrix} 3 \\ -5 \\ 1 \end{bmatrix}, \ E^T = \begin{bmatrix} 2 & -1 & 3 \end{bmatrix}.$$

4.3 Iloczyn skalarny i mnożenie macierzy

W tej części wprowadzimy operację *mnożenia macierzy.* Inaczej niż w przypadku dodawnia macierzy, operacja ta posiada posiada cechy znacznie odróżniające ją od zwykłego mnożenia liczb.

Definicja 58 Iloczynem skalarnym *dwóch wektorów*

$$a = \begin{bmatrix} a_1 & a_2 & \ldots & a_n \end{bmatrix} \ i \ b = \begin{bmatrix} b_1 \\ b_2 \\ \ldots \\ b_n \end{bmatrix}$$

nazywamy liczbę $a \circ b$ określoną wzorem

$$a \circ b = a_1 b_1 + a_2 b_2 + ... + a_n b_n = \sum_{i=1}^{n} a_i b_i.$$

Iloczyn skalarny jest ważną operacją, która będzie wykorzystywana także w następnych częściach wykładu.

Przykład 59 *Iloczyn skalarny wektorów*

$$u = \begin{bmatrix} 1 & -2 & 3 & 4 \end{bmatrix} \ i \ v = \begin{bmatrix} 2 \\ 3 \\ -2 \\ 1 \end{bmatrix}$$

wynosi

$$u \circ v = (1)(2) + (-2)(3) + (3)(-2) + (4)(1) = -6.$$

Definicja 60 (Mnożenie macierzy) *Jeżeli $A = [a_{ij}]$ jest macierzą wymiaru $m \times p$, a $B = [b_{ij}]$ jest macierzą wymiaru $p \times n$, to* iloczyn macierzy *A i B, oznaczany przez AB, jest macierzą $C = [c_{ij}]$ wymiaru $m \times n$, określoną wzorem*

$$c_{ij} = a_{i1} b_{1j} + a_{i2} b_{2j} + ... + a_{ip} b_{pj} = \sum_{k=1}^{p} a_{ik} b_{kj}, \tag{4.3}$$

dla wszystkich $1 \leq i \leq m, 1 \leq j \leq n$.

Równanie (1.3) mówi, że element na pozycji (i, j) w iloczynie macierzy A i B jest iloczynem skalarnym i-tego wiersza macierzy A i j-tej kolumny macierzy B. Oznaczmy przez $w_i(A)$ i $k_j(B)$ ów wiersz i ową kolumnę. Wówczas wzór (1.3) może być zapisany jako

$$c_{ij} = w_i(A) \circ k_j(B).$$

Zauważmy ponadto, że iloczyn macierzy A i B jest określony jedynie wtedy, gdy liczba elementów w wierszu macierzy A jest taka sama jak liczba elementów w kolumnie macierzy B, lub inaczej, gdy liczba kolumn macierzy A zgadza się z liczbą wierszy w macierzy B.

Można zadać sobie naturalne pytanie, dlaczego mnożenie macierzy zostało zdefiniowane w tak skomplikowany sposób, podczas gdy równość macierzy czy dodawanie są tak naturalne? Otóż, jedynie dogłębne zrozumienie związku pomiędzy macierzami a *przekształceniami liniowymi*, oraz operacją składania funkcji, pokazuje, że ta definicja jest również całkowicie naturalna.

Przykład 61 *Niech*

$$A = \begin{bmatrix} 1 & 2 & -1 \\ 3 & 1 & 4 \end{bmatrix} \text{ i } B = \begin{bmatrix} -2 & 5 \\ 4 & -3 \\ 2 & 1 \end{bmatrix}.$$

Wówczas

$$\begin{aligned} AB &= \begin{bmatrix} (1)(-2)+(2)(4)+(-1)(2) & (1)(5)+(2)(-3)+(-1)(1) \\ (3)(-2)+(1)(4)+(4)(2) & (3)(5)+(1)(-3)+(4)(1) \end{bmatrix} \\ &= \begin{bmatrix} 4 & -2 \\ 6 & 16 \end{bmatrix}. \end{aligned}$$

Przykład 62 *Niech*

$$A = \begin{bmatrix} 1 & -2 & 3 \\ 4 & 2 & 1 \\ 0 & 1 & -2 \end{bmatrix} \text{ i } B = \begin{bmatrix} 1 & 4 \\ 3 & -1 \\ -2 & 2 \end{bmatrix}.$$

Obliczmy jedynie element znajdujący się na pozycji $(3,2)$ *w macierzy* AB*. Zgodnie z definicją mnożenia macierzy, przy oznaczeniu* $AB = C$*, mamy*

$$\begin{aligned} c_{32} &= w_3(A) \circ k_2(B) \\ &= \begin{bmatrix} 0 & 1 & -2 \end{bmatrix} \circ \begin{bmatrix} 4 \\ -1 \\ 2 \end{bmatrix} = -5. \end{aligned}$$

Jak już wspomnieliśmy wcześniej, mnożenie macierzy różni się pod wieloma względami od mnożenia liczb. Na przykład, nie jest ono przemienne, to znaczy AB nie musi być równe BA. Jest kilka powodów, dla których tak się dzieje.

1. BA może nie być wogóle określone; tak jest wtedy, gdy $n \neq m$.

2. Jeżeli BA jest określone, co oznacza, że $m = n$, to macierz BA ma wymiar $p \times p$, zaś AB jest macierzą wymiaru $m \times m$, stąd, jeżeli $m \neq p$, to AB i BA są różnych wymiarów i nie mogą być równe.

3. Nawet jeśli AB i BA są tego samego wymiaru, to nie muszą być równe.

4. Należy podkreślić, że jeżeli AB i BA są tego samego wymiaru, to może się zdarzyć, że $AB = BA$.

Zilustrujemy te cztery możliwe sytuacje na przykładach.

Przykład 63 *Jeżeli A jest macierzą 2×3, a B jest macierzą 3×4, to AB ma wymiar 2×4, zaś BA nie istnieje.*

Przykład 64 *Jeżeli A jest macierzą 2×3, a B jest macierzą 3×2, to AB ma wymiar 2×2, zaś BA ma wymiar 3×3.*

Przykład 65 *Niech*

$$A = \begin{bmatrix} 1 & 2 \\ -1 & 3 \end{bmatrix}, \ B = \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}.$$

Wtedy

$$AB = \begin{bmatrix} 2 & 3 \\ -2 & 2 \end{bmatrix}, \ \textit{natomiast } BA = \begin{bmatrix} 1 & 7 \\ -1 & 3 \end{bmatrix}.$$

Przykład 66 *Jeżeli A i B są macierzami diagonalnymi tego samego wymiaru, to z pewnością zachodzi równość $AB = BA$.*

Czasami potrzebne jest jedynie obliczenie jednej kolumny macierzy AB bez wyznaczania całego iloczynu. Łatwo widać, że j-ta kolumna macierzy AB jest iloczynem macierzy A i j-tej kolumny macierzy B, co można zapisać wzorem

$$k_j(AB) = A(k_j(B)). \tag{4.4}$$

Przykład 67 *Jeżeli*

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \\ -1 & 5 \end{bmatrix} \; i \; B = \begin{bmatrix} -2 & 3 & 4 \\ 3 & 2 & 1 \end{bmatrix},$$

to druga kolumna iloczynu AB jest równa

$$A(k_2(B)) = \begin{bmatrix} 1 & 2 \\ 3 & 4 \\ -1 & 5 \end{bmatrix} \begin{bmatrix} 3 \\ 2 \end{bmatrix} = \begin{bmatrix} 7 \\ 17 \\ 7 \end{bmatrix}.$$

Pokażemy teraz pewien zapis wykorzystujący mnożenie macierzy, który będzie szczególnie przydatny przy układach równań liniowych. Niech

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix} \text{ i } C = \begin{bmatrix} c_1 \\ c_2 \\ \dots \\ c_n \end{bmatrix}.$$

Wówczas możemy napisać

$$\begin{aligned}
AC &= \begin{bmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ ... & ... & ... & ... \\ a_{m1} & a_{m2} & ... & a_{mn} \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ ... \\ c_n \end{bmatrix} = \begin{bmatrix} w_1(A) \circ C \\ w_2(A) \circ C \\ ... \\ w_m(A) \circ C \end{bmatrix} \\
&= \begin{bmatrix} a_{11}c_1 + a_{12}c_2 + ... + a_{1n}c_n \\ a_{21}c_1 + a_{22}c_2 + ... + a_{2n}c_n \\ ... \\ a_{m1}c_1 + a_{m2}c_2 + ... + a_{mn}c_n \end{bmatrix} \\
&= c_1 \begin{bmatrix} a_{11} \\ a_{21} \\ ... \\ a_{m1} \end{bmatrix} + c_2 \begin{bmatrix} a_{12} \\ a_{22} \\ ... \\ a_{m2} \end{bmatrix} + ... + c_n \begin{bmatrix} a_{1n} \\ a_{2n} \\ ... \\ a_{mn} \end{bmatrix} \\
&= c_1k_1(A) + c_2k_2(A) + ... + c_nk_n(A).
\end{aligned}$$

To ostatnie wyrażenie nazywamy *kombinacją liniową* kolumn macierzy A. Widzimy zatem, że iloczyn macierzy A wymiaru $m \times n$ i macierzy C wymiaru $n \times 1$ może być przedstawiony w postaci kombinacji liniowej kolumn macierzy A, której *współczynniki* są elementami macierzy C:

$$AC = c_1k_1(A) + c_2k_2(A) + ... + c_nk_n(A). \tag{4.5}$$

Przykład 68 *Niech*

$$A = \begin{bmatrix} 2 & -1 & -3 \\ 4 & 2 & -2 \end{bmatrix} \ i\ C = \begin{bmatrix} 2 \\ -3 \\ 4 \end{bmatrix}.$$

Wówczas

$$\begin{aligned} AC &= \begin{bmatrix} 2 & -1 & -3 \\ 4 & 2 & -2 \end{bmatrix} \begin{bmatrix} 2 \\ -3 \\ 4 \end{bmatrix} = \begin{bmatrix} -5 \\ -6 \end{bmatrix} \\ &= 2\begin{bmatrix} 2 \\ 4 \end{bmatrix} - 3\begin{bmatrix} -1 \\ 2 \end{bmatrix} + 4\begin{bmatrix} -3 \\ -2 \end{bmatrix}. \end{aligned}$$

Wobec wzorów (1.4) i (1.5) możemy więc napisać

$$k_j(AB) = A(k_j(B)) = b_{1j}k_1(A) + b_{2j}k_2(A) + ... + b_{pj}k_p(A).$$

Przykład 69 *Dla macierzy z Przykładu 20 mamy*

$$AB = \begin{bmatrix} 1 & 2 \\ 3 & 4 \\ -1 & 5 \end{bmatrix} \begin{bmatrix} -2 & 3 & 4 \\ 3 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 4 & 7 & 6 \\ 6 & 17 & 16 \\ 17 & 7 & 1 \end{bmatrix}.$$

Kolumny macierzy AB mogą być rozpisane następująco.

$$\begin{aligned} k_1(AB) &= \begin{bmatrix} 4 \\ 6 \\ 17 \end{bmatrix} = A(k_1(B)) = -2\begin{bmatrix} 1 \\ 3 \\ -1 \end{bmatrix} + 3\begin{bmatrix} 2 \\ 4 \\ 5 \end{bmatrix} \\ k_2(AB) &= \begin{bmatrix} 7 \\ 17 \\ 7 \end{bmatrix} = A(k_2(B)) = 3\begin{bmatrix} 1 \\ 3 \\ -1 \end{bmatrix} + 2\begin{bmatrix} 2 \\ 4 \\ 5 \end{bmatrix} \\ k_3(AB) &= \begin{bmatrix} 6 \\ 16 \\ 1 \end{bmatrix} = A(k_3(B)) = 4\begin{bmatrix} 1 \\ 3 \\ -1 \end{bmatrix} + 1\begin{bmatrix} 2 \\ 4 \\ 5 \end{bmatrix}. \end{aligned}$$

Rozważmy teraz ogólną postać układu równań liniowych

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

Następnie zdefiniujmy macierze

$$A = \begin{bmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ ... & ... & ... & ... \\ a_{m1} & a_{m2} & ... & a_{mn} \end{bmatrix},\ X = \begin{bmatrix} x_1 \\ x_2 \\ ... \\ x_n \end{bmatrix},\ B = \begin{bmatrix} b_1 \\ b_2 \\ ... \\ b_m \end{bmatrix}.$$

Wówczas

$$AX = \begin{bmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ ... & ... & ... & ... \\ a_{m1} & a_{m2} & ... & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ ... \\ x_n \end{bmatrix} = \begin{bmatrix} a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n \\ a_{12}x_1 + a_{22}x_2 + ... + a_{2n}x_n \\ ..... \\ a_{m1}x_1 + a_{m2}x_2 + ... + a_{mn}x_n \end{bmatrix}.$$

Elementy iloczynu AX to nic innego jak lewe strony równań rozważanego układu, zatem cały układ równań można zapisać w postaci jednego równania macierzowego

$$AX = B.$$

Macierz A nazywamy *macierzą współczynników układu*, a macierz

$$\left[\begin{array}{cccc|c} a_{11} & a_{12} & ... & a_{1n} & b_1 \\ a_{21} & a_{22} & ... & a_{2n} & b_2 \\ ... & ... & ... & ... & ... \\ a_{m1} & a_{m2} & ... & a_{mn} & b_n \end{array}\right],$$

nazywamy *macierzą rozszerzoną*. Macierz rozszerzona może być również zapisana w skrócie jako $[A|\,b]$. Na odwrót, każda macierz zawierająca więcej niż jedną kolumnę może być traktowana jako macierz rozszerzona pewnego układu równań. Obie macierze odgrywają kluczową rolę w metodach rozwiązywania układów równań.

Przykład 70 *Rozważmy układ równań*

$$\begin{aligned} 2x + 3y - 4z &= 7 \\ -2x \qquad\quad + z &= 5 \\ 3x + 2y + 2z &= 3. \end{aligned}$$

Podstawiając

$$A = \begin{bmatrix} 2 & 3 & -4 \\ -2 & 0 & 1 \\ 3 & 2 & 2 \end{bmatrix}, \; X = \begin{bmatrix} x \\ y \\ z \end{bmatrix}, \; B = \begin{bmatrix} 5 \\ 7 \\ 3 \end{bmatrix},$$

możemy zapisać układ równań w postaci macierzowej

$$AX = B.$$

Macierzą współczynników układu jest A, zaś macierz rozszerzona ma postać

$$\left[\begin{array}{rrr|r} 2 & 3 & -4 & 5 \\ -2 & 0 & 1 & 7 \\ 3 & 2 & 2 & 3 \end{array}\right].$$

Przykład 71 *Macierz*

$$\left[\begin{array}{rrr|r} 2 & -1 & 3 & 4 \\ 3 & 0 & 2 & 5 \end{array}\right]$$

jest macierzą rozszerzoną układu

$$\begin{aligned} 2x - y + 3z &= 4 \\ 3x \qquad + 2z &= 5. \end{aligned}$$

Z naszej poprzedniej dyskusji wynika, że układ równań może być także zapisany w postaci kombinacji liniowej kolumn macierzy A:

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

Odwrotnie, każde równanie tego typu przedstawia jakiś układ równań.

4.4 Algebraiczne własności działań na macierzach

W tej części przedstawimy szereg podstawowych własności zdefiniowanych wcześniej działań na macierzach. Własności te będą prezentowane w postaci twierdzeń, których dowody, w większości przypadków, zostaną pominięte, lub pozostawione do samodzielnego przeprowadzenia.

Twierdzenie 72 (Własności dodawania macierzy) *Niech A, B, C i D będą macierzami wymiaru $m \times n$. Wówczas zachodzą następujące własności.*

(a) $A + B = B + A$.

(b) $A + (B + C) = (A + B) + C$.

(c) Istnieje dokładnie jedna macierz O wymiaru $m \times n$ taka, że

$$A + O = A,$$

dla każdej macierzy A. Macierz O nazywamy macierzą zerową.

(d) Dla każdej macierzy A istnieje dokładnie jedna macierz D, tego samego wymiaru, spełniająca równanie

$$A + D = O.$$

Macierz D oznaczamy przez $-A$ i nazywamy macierzą przeciwną *do A.*

Twierdzenie 73 (Własności mnożenia macierzy) *Przy założeniu, że macierze A, B i C są odpowiednich wymiarów mamy:*

(a) $A(BC) = (AB)C$,

(b) $A(B+C) = AB + AC$,

(c) $(A+B)C = AC + BC$.

Przykład 74 *Niech*

$$A = \begin{bmatrix} 5 & 2 & 3 \\ 2 & -3 & 4 \end{bmatrix}, \; B = \begin{bmatrix} 2 & -1 & 1 & 0 \\ 0 & 2 & 2 & 2 \\ 3 & 0 & -1 & 3 \end{bmatrix} \; i \; C = \begin{bmatrix} 1 & 0 & 2 \\ 2 & -3 & 0 \\ 0 & 0 & 3 \\ 2 & 1 & 0 \end{bmatrix}.$$

Wówczas

$$A(BC) = \begin{bmatrix} 5 & 2 & 3 \\ 2 & -3 & 4 \end{bmatrix} \begin{bmatrix} 0 & 3 & 7 \\ 8 & -4 & 6 \\ 9 & 3 & 3 \end{bmatrix} = \begin{bmatrix} 43 & 16 & 56 \\ 12 & 30 & 8 \end{bmatrix}$$

i

$$(AB)C = \begin{bmatrix} 19 & -1 & 6 & 13 \\ 16 & -8 & -8 & 6 \end{bmatrix} \begin{bmatrix} 1 & 0 & 2 \\ 2 & -3 & 0 \\ 0 & 0 & 3 \\ 2 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 43 & 16 & 56 \\ 12 & 30 & 8 \end{bmatrix}.$$

Przykład 75 *Niech*

$$A = \begin{bmatrix} 2 & 2 & 3 \\ 3 & -1 & 2 \end{bmatrix}, \; B = \begin{bmatrix} 1 & 0 \\ 2 & 2 \\ 3 & -1 \end{bmatrix} \; i \; C = \begin{bmatrix} -1 & 2 \\ 1 & 0 \\ 2 & -2 \end{bmatrix}.$$

Wtedy

$$A(B+C) = \begin{bmatrix} 2 & 2 & 3 \\ 3 & -1 & 2 \end{bmatrix} \begin{bmatrix} 0 & 2 \\ 3 & 2 \\ 5 & -3 \end{bmatrix} = \begin{bmatrix} 21 & -1 \\ 7 & -2 \end{bmatrix}$$

i

$$AB + AC = \begin{bmatrix} 15 & 1 \\ 7 & -4 \end{bmatrix} + \begin{bmatrix} 6 & -2 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 21 & -1 \\ 7 & -2 \end{bmatrix}.$$

Szczególną rolę odgrywa macierz skalarna wymiaru $n \times n$, której główna przekątna składa się z samych jedynek:

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

Nazywamy ją *macierzą jednostkową*. Jeżeli A jest macierzą wymiaru $m \times n$, to, jak łatwo sprawdzić,

$$I_m A = A I_n = A.$$

Jeżeli A jest macierzą kwadratową wymiaru n, a p jest liczbą naturalną, to w znany sposób możemy określić potęgę

$$A^p = \underbrace{A \cdot A \cdot ... \cdot A}_{\text{p czynników}}.$$

Podobnie, definiujemy również

$$A^0 = I_n.$$

Łatwo sprawdzić, że zachodzą znane wzory

$$A^p A^q = A^{p+q},$$

oraz

$$(A^p)^q = A^{pq}.$$

Należy jednak zwrócić uwagę na to, że w ogólności

$$(AB)^p \neq A^p B^p,$$

chyba, że $AB = BA$.

Odnotujemy teraz dwie kolejne osobliwości dotyczące mnożenia macierzy. Jeżeli a i b są liczbami rzeczywistymi, to równość $ab = 0$ może mieć miejsce tylko wtedy, gdy jedna z liczb a lub b jest zerem. Inaczej jest w przypadku macierzy.

Przykład 76 *Jeśli*

$$A = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} \ i\ B = \begin{bmatrix} 4 & -6 \\ -2 & 3 \end{bmatrix},$$

to

$$AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},$$

pomimo, że ani A ani B nie jest macierzą zerową.

Jeżeli a, b i c są liczbami rzeczywistymi, dla których zachodzi równość $ab = ac$ i $a \neq 0$, to w konsekwencji $a = b$. Ta własność, zwana *prawem skracania*, nie zachodzi w przypadku macierzy, jak pokazuje następny przykład.

Przykład 77 *Jeśli*

$$A = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix},\ B = \begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix} \ i\ C = \begin{bmatrix} -2 & 7 \\ 5 & -1 \end{bmatrix},$$

to

$$AB = AC = \begin{bmatrix} 8 & 5 \\ 16 & 10 \end{bmatrix},$$

ale $B \neq C$.

Twierdzenie 78 (Własności iloczynu macierzy przez liczbę) *Jeżeli r i s są liczbami rzeczywistymi, a A i B są macierzami, to*

(a) $r(sA) = (rs)A$,

(b) $(r+s)A = rA + sA$,

(c) $r(A+B) = rA + rB$,

(d) $A(rB) = r(AB) = (rA)B$.

Twierdzenie 79 (Własności transpozycji macierzy) *Jeżeli r jest liczbą rzeczywistą, a A i B są macierzami, to*

(a) $\left(A^T\right)^T = A$,

(b) $(A+B)^T = A^T + B^T$,

(c) $(AB)^T = B^T A^T$,

(d) $(rA)^T = rA^T$.

Przykład 80 *Niech*

$$A = \begin{bmatrix} 1 & 3 & 2 \\ 2 & -1 & 3 \end{bmatrix} \text{ i } B = \begin{bmatrix} 0 & 1 \\ 2 & 2 \\ 3 & -1 \end{bmatrix}.$$

Wówczas

$$(AB)^T = \begin{bmatrix} 12 & 7 \\ 5 & -3 \end{bmatrix}$$

i

$$B^T A^T = \begin{bmatrix} 0 & 2 & 3 \\ 1 & 2 & -1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & -1 \\ 2 & 3 \end{bmatrix} = \begin{bmatrix} 12 & 7 \\ 5 & -3 \end{bmatrix}.$$

Definicja 81 *Macierz* $A = [a_{ij}]$ *nazywamy* symetryczną *jeżeli*

$$A^T = A.$$

Inaczej mówiąc, A *jest symetryczna jeśli jest kwadratowa i* $a_{ij} = a_{ji}$, *dla wszystkich* $i, j = 1, 2, ..., n$. *W takiej macierzy elementy położone symetrycznie względem głównej przekątnej są równe.*

Przykład 82 *Macierze*

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{bmatrix} \text{ i } I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

są symetryczne.

4.5 Metody rozwiązywania układów równań liniowych

W tej części usystematyzujemy znaną już metodę rozwiązywania układu równań, polegającą na sukcesywnej eliminacji niewiadomych. Punktem wyjścia jest macierz rozszerzona danego układu, która następnie poddawana jest transformacjom przekształcającym ją do pewnej szczególnej postaci. Otrzymana w ten sposób nowa macierz reprezentuje układ równań o *dokładnie tych samych* rozwiązaniach co wyjściowy, ale ma o wiele dogodniejszą postać. Na przykład, jeżeli macierz rozszerzona pewnego układu ma postać

$$\left[\begin{array}{rrrr|r} 1 & 0 & 0 & 2 & 4 \\ 0 & 1 & 0 & -1 & -5 \\ 0 & 0 & 1 & 3 & 6 \end{array}\right],$$

to jego rozwiązania mogą być znalezione bardzo łatwo. Zadanie polega więc na takim manipulowaniu macierzą rozszerzoną układu, aby przybrała ona podobną postać, bez naruszenia zbioru rozwiązań.

Definicja 83 (Postać kanoniczna macierzy) *Mówimy, że macierz ma* postać kanoniczną *jeśli spełnia następujące warunki:*

(a) Wszystkie wiersze składające się z samych zer, o ile wogóle występują znajdują się na samym dole.

(b) Pierwsza od lewej niezerowa liczba (o ile wiersz nie składa się z samych zer) jest równa 1. Nazywamy ją wiodącą jedynką *tego wiersza.*

(c) Wiodąca jedynka niższego wiersza znajduje się na prawo od wiodącej jedynki wyższego wiersza.

(d) Jeżeli kolumna zawiera wiodącą jedynkę pewnego wiersza, to wszystkie pozostałe jej elementy są zerami.

Przykład 84 *Macierze*

$$A = \begin{bmatrix} 1 & 0 & 0 & 4 \\ 0 & 1 & 0 & 5 \\ 0 & 0 & 1 & 2 \end{bmatrix}, \; B = \begin{bmatrix} 1 & 2 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix},$$

$$C = \begin{bmatrix} 1 & 0 & 0 & 3 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

znajdują się w postaci kanonicznej.

Przykład 85 *Macierze*

$$A = \begin{bmatrix} 1 & 2 & 0 & 4 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -3 \end{bmatrix}, \; B = \begin{bmatrix} 1 & 0 & 3 & 4 \\ 0 & 2 & -2 & 5 \\ 0 & 0 & 1 & 2 \end{bmatrix},$$

$$C = \begin{bmatrix} 1 & 0 & 3 & 4 \\ 0 & 1 & -2 & 5 \\ 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \; D = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & -2 & 5 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

nie są w postaci kanonicznej, ponieważ nie spełniają warunku (a), (b), (c), i (d), odpowiednio.

Zajmiemy się teraz procedurą doprowadzającą macierz do postaci kanonicznej. Opiera się ona na *wierszowych operacjach elementarnych*, które odpowiadają w oczywisty sposób znanym operacjom na równaniach.

Definicja 86 *Trzy następujące rodzaje operacji na wierszach macierzy A nazywamy operacjami elementarnymi:*

(a) Zamiana miejscami dwóch wierszy macierzy A.

(b) Pomnożenie wszystkich elementów wiersza przez liczbę $c \neq 0$.

(c) Dodanie do wiersza innego wiersza pomnożonego przez pewną liczbę.

Przykład 87 *Niech*

$$A = \begin{bmatrix} 0 & 0 & 1 & 2 \\ 2 & 3 & 0 & -2 \\ 3 & 3 & 6 & -9 \end{bmatrix}.$$

Wówczas zamiana wierszy pierwszego i trzeciego, co zapisujemy jako $w_1(A) \leftrightarrows w_3(A)$*, daje macierz*

$$B = \begin{bmatrix} 3 & 3 & 6 & -9 \\ 2 & 3 & 0 & -2 \\ 0 & 0 & 1 & 2 \end{bmatrix}.$$

Po pomnożeniu trzeciego wiersza macierzy B przez $\frac{1}{3}$*, w skrócie* $\frac{1}{3}w_3(B)$*, dostajemy*

$$C = \begin{bmatrix} 0 & 0 & 1 & 2 \\ 2 & 3 & 0 & -2 \\ 1 & 1 & 2 & -3 \end{bmatrix}.$$

Wreszcie, dodając do trzeciego wiersza macierzy C drugi wiersz pomnożony przez (-2)*, w notacji* $(-2)w_2(C) + w_3(C)$*, otrzymujemy*

$$D = \begin{bmatrix} 0 & 0 & 1 & 2 \\ 2 & 3 & 0 & -2 \\ -1 & -3 & 6 & -5 \end{bmatrix}.$$

Definicja 88 *Macierze A i B wymiaru* $m \times n$ *nazywamy* równoważnymi *(wierszowo), jeżeli jedną znich możemy otrzymać z drugiej w wyniku skończonego ciągu wierszowych operacji elementarnych.*

Przykład 89 *Macierz*

$$A = \begin{bmatrix} 1 & 2 & 4 & 3 \\ 2 & 1 & 3 & 2 \\ 1 & -1 & 2 & 3 \end{bmatrix}$$

jest wierszowo równoważna macierzy

$$D = \begin{bmatrix} 2 & 4 & 8 & 6 \\ 1 & -1 & 2 & 3 \\ 4 & -1 & 7 & 8 \end{bmatrix}.$$

W istocie, wykonując operację $2w_3(A) + w_2(A)$ *dostaniemy*

$$B = \begin{bmatrix} 1 & 2 & 4 & 3 \\ 4 & -1 & 7 & 8 \\ 1 & -1 & 2 & 3 \end{bmatrix},$$

a następnie zamieniając $w_2(B)$ *i* $w_3(B)$*, otrzymujemy*

$$C = \begin{bmatrix} 1 & 2 & 4 & 3 \\ 1 & -1 & 2 & 3 \\ 4 & -1 & 7 & 8 \end{bmatrix}.$$

Wreszcie, po wykonaniu operacji $2w_1(C)$ *otrzymamy macierz* D*.*

Twierdzenie 90 *Każda macierz jest równoważna dokładnie jednej macierzy w postaci kanonicznej.*

Zilustrujemy dowód tego ważnego twierdzenia na przykładzie, pokazując kolejne kroki doprowadzające pewną macierz A do postaci kanonicznej. Dowód jednoznaczności tej postaci pominiemy.

Przykład 91 *Niech*

$$A = \begin{bmatrix} 0 & 2 & 3 & -4 & 1 \\ 0 & 0 & 2 & 3 & 4 \\ 2 & 2 & -5 & 2 & 4 \\ 2 & 0 & -6 & 9 & 7 \end{bmatrix}.$$

Krok 1. *Znajdujemy pierwszą od lewej kolumnę zawierającą element niezerowy* (kolumnę wiodącą) *i zaznaczamy w niej pierwszy od góry taki element. Nazywamy go* elementem wiodącym.

$$A = \begin{bmatrix} 0 & 2 & 3 & -4 & 1 \\ 0 & 0 & 2 & 3 & 4 \\ \mathbf{2} & 2 & -5 & 2 & 4 \\ 2 & 0 & -6 & 9 & 7 \end{bmatrix}.$$

Krok 2. *Jeśli trzeba, zamieniamy wiersze tak aby zaznaczony element znalazł się w lewym górnym rogu.*

$$A_1 = \begin{bmatrix} \mathbf{2} & 2 & -5 & 2 & 4 \\ 0 & 0 & 2 & 3 & 4 \\ 0 & 2 & 3 & -4 & 1 \\ 2 & 0 & -6 & 9 & 7 \end{bmatrix}, \ (w_1 \rightleftarrows w_3)\,.$$

Krok 3. *Mnożymy pierwszy wiersz A_1 przez odwrotność elementu wiodącego, aby otrzymać wiodącą jedynkę.*

$$A_2 = \begin{bmatrix} \mathbf{1} & 1 & -\frac{5}{2} & 1 & 2 \\ 0 & 0 & 2 & 3 & 4 \\ 0 & 2 & 3 & -4 & 1 \\ 2 & 0 & -6 & 9 & 7 \end{bmatrix}, \ \left(\frac{1}{2}w_1\right).$$

Krok 4. *Teraz dodajemy pierwszy wiersz pomnożony przez odpowiednie stałe do pozostałych wierszy, po to by wszystkie elementy wiodącej kolumny, oprócz wiodącej jedynki, stały się zerami.*

$$A_3 = \begin{bmatrix} \mathbf{1} & 1 & -\frac{5}{2} & 1 & 2 \\ 0 & 0 & 2 & 3 & 4 \\ 0 & 2 & 3 & -4 & 1 \\ 0 & -2 & -1 & 7 & 3 \end{bmatrix}, \ (-2w_1 + w_4)\,.$$

Krok 5. *Następnie powtarzamy wszystko od początku na macierzy, która powstaje przez pominięcie pierwszego wiersza macierzy A_3.*

$$B = \begin{bmatrix} 0 & 0 & 2 & 3 & 4 \\ 0 & \mathbf{2} & 3 & -4 & 1 \\ 0 & -2 & -1 & 7 & 3 \end{bmatrix},$$

$$B_1 = \begin{bmatrix} 0 & \mathbf{2} & 3 & -4 & 1 \\ 0 & 0 & 2 & 3 & 4 \\ 0 & -2 & -1 & 7 & 3 \end{bmatrix}, \quad (w_1 \rightleftarrows w_2)$$

$$B_2 = \begin{bmatrix} 0 & \mathbf{1} & \frac{3}{2} & -2 & \frac{1}{2} \\ 0 & 0 & 2 & 3 & 4 \\ 0 & -2 & -1 & 7 & 3 \end{bmatrix}, \quad \left(\frac{1}{2} w_2\right)$$

$$B_3 = \begin{bmatrix} 0 & \mathbf{1} & \frac{3}{2} & -2 & \frac{1}{2} \\ 0 & 0 & 2 & 3 & 4 \\ 0 & 0 & 2 & 3 & 4 \end{bmatrix}, \quad (2w_1 + w_3)\,.$$

Krok 6. *Podobnie powtarzamy kroki 1-4 na macierzy ograniczonej do następnych wierszy.*

$$C = \begin{bmatrix} 0 & 0 & \mathbf{2} & 3 & 4 \\ 0 & 0 & 2 & 3 & 4 \end{bmatrix},$$

$$C_1 = C_2 = \begin{bmatrix} 0 & 0 & \mathbf{1} & \frac{3}{2} & 2 \\ 0 & 0 & 2 & 3 & 4 \end{bmatrix}, \quad \left(\frac{1}{2} w_1\right)$$

$$C_3 = \begin{bmatrix} 0 & 0 & \mathbf{1} & \frac{3}{2} & 2 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, (-2w_1 + w_2)\,.$$

Krok 7 (ostatni). *Kiedy już wszystkie wiodące jedynki się ujawniły, możemy, po dopisaniu pominiętych wcześniej wierszy, przystąpić do zerowania elementów znajdujących nad nimi. W tym celu wygodnie jest wykonywać odpowiednie operacje w odwrotnym kierunku, z dołu do góry.*

$$D = \begin{bmatrix} \mathbf{1} & 1 & -\frac{5}{2} & 1 & 2 \\ 0 & \mathbf{1} & \frac{3}{2} & -2 & \frac{1}{2} \\ 0 & 0 & \mathbf{1} & \frac{3}{2} & 2 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$D_1 = \begin{bmatrix} \mathbf{1} & 1 & -\frac{5}{2} & 1 & 2 \\ 0 & \mathbf{1} & 0 & -\frac{17}{4} & -\frac{5}{2} \\ 0 & 0 & \mathbf{1} & \frac{3}{2} & 2 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad \left(-\frac{3}{2}w_3 + w_2\right)$$

$$D_2 = \begin{bmatrix} \mathbf{1} & 1 & 0 & \frac{19}{4} & 7 \\ 0 & \mathbf{1} & 0 & -\frac{17}{4} & -\frac{5}{2} \\ 0 & 0 & \mathbf{1} & \frac{3}{2} & 2 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad \left(\frac{5}{2}w_3 + w_1\right)$$

$$D_3 = \begin{bmatrix} \mathbf{1} & 0 & 0 & 9 & \frac{19}{2} \\ 0 & \mathbf{1} & 0 & -\frac{17}{4} & -\frac{5}{2} \\ 0 & 0 & \mathbf{1} & \frac{3}{2} & 2 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad (-1w_2 + w_1)\,.$$

Ta ostatnia macierz ma nareszcie upragnioną postać kanoniczną.

Twierdzenie 92 *Niech $AX = B$ i $CX = D$ będą dwoma układami m równań z n niewiadomymi. Jeżeli macierze rozszerzone $[A|\,B]$ i $[C|\,D]$ są równoważne, to układy te mają takie same zbiory rozwiązań.*

Wniosek 93 *Jeżeli A i C są równoważne, to układy równań $AX = 0$ i $CX = 0$ mają ten sam zbiór rozwiązań.*

Metoda rozwiązywania układu równań, przedstawiona w Przykładzie 35, znana jest również pod nazwą *redukcji Gaussa-Jordana.* Składa się ona z trzech głównych kroków:

Krok 1. *Utworzenie macierzy rozszerzonej układu $[A|\,B]$.*

Krok 2. *Doprowadzenie macierzy rozszerzonej do postaci kanonicznej, poprzez operacje elementarne na wierszach.*

Krok 3. *Uzyskanie rozwiązania układu poprzez wyznaczenie niewiadomych odpowiadających wiodącym jedynkom.*

Przedstawimy teraz szereg przykładów stosowania tej metody, prowadzących do różnych możliwych sytuacji.

Przykład 94 (Dokładnie jedno rozwiązanie) *Rozwiążemy następujący układ równań*

$$\begin{aligned} x+2y+3z &= 9 \\ 2x-y+z &= 8 \\ 3x \quad -z &= 3 \end{aligned}$$

metodą Gaussa-Jordana.

Krok 1. Tworzymy macierz rozszerzoną:

$$\left[\begin{array}{rrr|r} 1 & 2 & 3 & 9 \\ 2 & -1 & 1 & 8 \\ 3 & 0 & -1 & 3 \end{array}\right].$$

Krok 2. Przekształcamy macierz rozszerzoną do postaci kanonicznej

$$\left[\begin{array}{rrr|r} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 3 \end{array}\right],$$

za pomocą (raczej sporej liczby) operacji elementarnych.

Krok 3. Odczytujemy rozwiązanie:

$$\begin{aligned} x &= 2 \\ y &= -1 \\ z &= 3. \end{aligned}$$

Przykład 95 (Nieskończenie wiele rozwiązań) *Dany jest układ równań*

$$\begin{aligned} x+y+2z-5w &= 3 \\ 2x+5y-z-9w &= -3 \\ 2x+y-z+3w &= -11 \\ x-3y+2z+7w &= -5. \end{aligned}$$

Krok 1. Tworzymy macierz rozszerzoną

$$\left[\begin{array}{rrrr|r} 1 & 1 & 2 & -5 & 3 \\ 2 & 5 & -1 & -9 & -3 \\ 2 & 1 & -1 & 3 & -11 \\ 1 & -3 & 2 & 7 & -5 \end{array}\right].$$

Krok 2. Redukcja Gaussa-Jordana

$$\left[\begin{array}{rrrr|r} 1 & 0 & 0 & 2 & -5 \\ 0 & 1 & 0 & -3 & 2 \\ 0 & 0 & 1 & -2 & 3 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right].$$

Krok 3. Wyznaczamy niewiadome odpowiadające wiodącym jedynkom

$$\begin{aligned} x &= -5 - 2w \\ y &= 2 + 3w \\ z &= 3 + 2w \end{aligned}$$

i zapisujemy rozwiązanie

$$\begin{aligned} x &= -5 - 2r \\ y &= 2 + 3r \\ z &= 3 + 2r \\ w &= r, \end{aligned}$$

gdzie r *oznacza dowolną liczbę rzeczywistą.*

Przykład 96 (Nieskończenie wiele rozwiązań) *Dany jest (raczej nieprzyjemny) układ równań*

$$\begin{aligned}
x_1 + 2x_2 \quad - 3x_4 + x_5 \quad &= 2\\
x_1 + 2x_2 + x_3 - 3x_4 + x_5 + 2x_6 &= 3\\
x_1 + 2x_2 \quad - 3x_4 + 2x_5 + x_6 &= 4\\
3x_1 + 6x_2 + x_3 - 9x_4 + 4x_5 + 3x_6 &= 9.
\end{aligned}$$

Krok 1. Macierz rozszerzona ma postać

$$\left[\begin{array}{cccccc|c}
1 & 2 & 0 & -3 & 1 & 0 & 2\\
1 & 2 & 1 & -3 & 1 & 2 & 3\\
1 & 2 & 0 & -3 & 2 & 1 & 4\\
3 & 6 & 1 & -9 & 4 & 3 & 9
\end{array}\right].$$

Krok 2. Po redukcji Gaussa-Jordana otrzymujemy

$$\left[\begin{array}{cccccc|c}
1 & 2 & 0 & -3 & 0 & -1 & 0\\
0 & 0 & 1 & 0 & 0 & 2 & 1\\
0 & 0 & 0 & 0 & 1 & 1 & 2\\
0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}\right].$$

Krok 3. Wyznaczamy niewiadome odpowiadające wiodącym jedynkom

$$\begin{aligned}
x_1 &= -2x_2 + 3x_4 + x_6\\
x_3 &= 1 - 2x_6\\
x_5 &= 2 - x_6,
\end{aligned}$$

i zapisujemy pełne rozwiązanie

$$\begin{aligned}
x_1 &= -2r + 3s + t \\
x_2 &= r \\
x_3 &= 1 - 2t \\
x_4 &= s \\
x_5 &= 2 - t \\
x_6 &= t,
\end{aligned}$$

gdzie r, s *i* t *oznaczają dowolne liczby rzeczywiste.*

Przykład 97 (Brak rozwiązań) *Niech dany będzie układ równań*

$$\begin{aligned}
x + 2y + 3z + 4w &= 5 \\
x + 3y + 5z + 7w &= 11 \\
x \quad\quad - z - 2w &= -6.
\end{aligned}$$

Po zredukowaniu macierzy rozszerzonej do postaci kanonicznej otrzymujemy macierz

$$\left[\begin{array}{cccc|c} 1 & 0 & -1 & -2 & 0 \\ 0 & 1 & 2 & 3 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array}\right].$$

Ostatnie równanie odpowiadającego jej układu

$$0x + 0y + 0z + 0w = 1$$

nie ma żadnych rozwiązań. W konsekwencji, cały układ równań, także nie posiada rozwiązań.

Definicja 98 *Układ równań postaci*

$$a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n = 0$$
$$a_{12}x_1 + a_{22}x_2 + ... + a_{2n}x_n = 0$$
$$.....$$
$$a_{m1}x_1 + a_{m2}x_2 + ... + a_{mn}x_n = 0$$

nazywamy układem jednorodnym*. Rozwiązanie*

$$x_1 = x_2 = ... = x_n = 0$$

nazywamy rozwiązaniem trywialnym*, natomiast rozwiązanie, w którym choćby jedna z liczb x_i jest różna od zera, nazywamy rozwiązaniem* nietrywialnym*.*

Oczywiście, każdy jednorodny układ równań posiada co najmniej jedno rozwiązanie, mianowicie rozwiązanie trywialne. Może się zdarzyć, że jest ono jedynym rozwiązaniem takiego układy, ale moży być również tak, że rozwiązań będzie nieskończenie wiele.

Przykład 99 *Rozważmy jednorodny układ równań*

$$\begin{aligned} x + 2y + 3z &= 0 \\ -x + 3y + 2z &= 0 \\ 2x + y - 2z &= 0. \end{aligned}$$

Postać kanoniczna macierzy tego układu jest równa I_3, zatem jedynym rozwiązaniem jest rozwiązanie trywialne

$$x = y = z = 0.$$

Przykład 100 *Rozważmy układ równań*

$$\begin{aligned} x + y + z + w &= 0 \\ x \quad + w &= 0 \\ x + 2y + z \quad &= 0. \end{aligned}$$

Macierz

$$\left[\begin{array}{cccr|c} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{array}\right]$$

przedstawia postać kanoniczną macierzy rozszerzonej tego układu. Otrzymujemy więc nieskończenie wiele rozwiązań postaci

$$\begin{aligned} x &= -r \\ y &= r \\ z &= -r \\ w &= r, \end{aligned}$$

gdzie r jest dowolną liczbą rzeczywistą.

Twierdzenie 101 *Jeżeli liczba równań jednorodnego układu jest mniejsza od jego liczby niewiadomych, to układ ten posiada rozwiązanie nietrywialne.*

4.6 Macierze odwracalne

W tej części skupimy uwagę na macierzach kwadratowych i określimy pojęcie macierzy odwrotnej, stanowiące uogólnienie odwrotności liczby niezerowej.

Definicja 102 *Macierz A wymiaru $n\times n$ nazywamy* odwracalną *(lub* nieosobliwą*), jeśli istnieje taka macierz B wymiaru $n \times n$, że*

$$AB = BA = I_n.$$

Macierz B nazywamy wówczas odwrotnością macierzy A. Jeżeli taka macierz B nie istnieje, to A nazywamy nieodwracalną *(lub* osobliwą*).*

Przykład 103 *Niech*

$$A = \begin{bmatrix} 2 & 3 \\ 2 & 2 \end{bmatrix}, B = \begin{bmatrix} -1 & \frac{3}{2} \\ 1 & -1 \end{bmatrix}.$$

Wówczas

$$AB = BA = I_2,$$

co oznacza, że A jest macierzą odwracalną i B jest odwrotnością A.

Twierdzenie 104 *Jeżeli macierz A jest odwracalna, to jej odwrotność jest jednoznaczna.*

Dowód. Niech B i C będą odwrotnościami macierzy A. Wówczas

$$BA = AC = I_n.$$

Stąd

$$B = BI_n = B(AC) = (BA)C = I_nC = C,$$

co kończy dowód. ■

Od tej pory będziemy oznaczać odwrotność macierzy A przez A^{-1}.

Przykład 105 *Niech*

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}.$$

Aby znaleźć A^{-1} oznaczmy

$$A^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Równanie $AA^{-1} = I_2$ prowadzi do układu równań z rozwiązaniem

$$a = -2, b = 1, c = \frac{3}{2} \text{ i } d = -\frac{1}{2}.$$

Stąd

$$A^{-1} = \begin{bmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{bmatrix}.$$

Przykład 106 *Niech*

$$A = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}.$$

Podobny układ równań tym razem nie ma rozwiązania. Wnioskujemy więc, że macierz A jest osobliwa.

Twierdzenie 107 (Własności odwrotności)

(a) Jeżeli A jest macierzą nieosobliwą, to A^{-1} też jest macierzą nieosobliwą i

$$(A^{-1})^{-1} = A.$$

(b) Jeżeli macierze A i B są nieosobliwe, to macierz AB też jest nieosobliwa i

$$(AB)^{-1} = B^{-1}A^{-1}.$$

(c) Jeżeli A jest nieosobliwa, to

$$(A^T)^{-1} = (A^{-1})^T.$$

Dowód. Punkt (a) wynika wprost z definicji odwrotności. W punktach (b) i (c) wystarczy sprawdzić, że macierze $B^{-1}A^{-1}$ i $(A^{-1})^T$ spełnieją definicję macierzy odwrotnej, odpowiednio. ■

Wniosek 108 *Jeżeli macierze $A_1, A_2, ..., A_r$ wymiaru $n \times n$ są nieosobliwe, to ich iloczyn też jest macierzą nieosobliwą i*

$$(A_1A_2...A_r)^{-1} = A_r^{-1}A_{r-1}^{-1}...A_1^{-1}.$$

Twierdzenie 109 *Przypuśćmy, że A i B są macierzami wymiaru $n \times n$. Wówczas, jeśli $AB = I_n$, to również $BA = I_n$.*

Opiszemy teraz praktyczną metodę wyznaczania macierzy odwrotnej A^{-1}. Jeżeli A jest daną macierzą wymiaru $n \times n$, to poszukujemy macierzy B takiej, że

$$AB = I_n.$$

Oznaczmy kolumny macierzy B przez $X_1, X_2, ..., X_n$, gdzie

$$X_j = \begin{bmatrix} b_{1j} \\ b_{2j} \\ ... \\ b_{nj} \end{bmatrix}, (1 \leq j \leq n).$$

Natomiast kolumny macierzy jednostkowej I_n oznaczmy przez $E_1, ...E_n$. Na mocy wzoru $k_j(AB) = Ak_j(B)$ wnioskujemy, że problem znalezienia macierzy B jest równoznaczny ze znalezieniem macierzy X_j spełniających równania

$$AX_j = E_j, \ \ (1 \leq j \leq n).$$

Zatem, wyznaczenie B jest równoważne rozwiązaniu n układów równań liniowych, z których każdy ma n równań i n niewiadomych. Każdy z tych układów może być rozwiązany z osobna metodą Gaussa - Jordana, ale, ponieważ macierz współczynników każdego układu jest ta sama, więc możemy przeprowadzić redukcję na wspólnej macierzy rozszerzonej, postaci

$$[A| \ E_1E_2...E_n] = [A| \ I_n] \, .$$

Po przeprowadzeniu redukcji tej macierzy do postaci kanonicznej $[C| \ D]$ możliwe są dwie sytuacje.

(1) $C = I_n$. Wtedy oczywiście mamy $B = D$.

(2) $C \neq I_n$. Wtedy macierz C musi zawierać wiersz zerowy i któryś z rozpatrywanych układów równań nie ma rozwiązania. Zatem, macierz odwrotna do A w tym wypadku nie istnieje.

Procedurę wyznaczania macierzy odwrotnejdo A możemy zatem streścić w trzech krokach.

Krok 1. Tworzymy macierz rozszerzoną $[A| \ I_n]$ wymiaru $n \times 2n$ przez dopisanie do A macierzy jednostkowej I_n.

Krok 2. Sprowadzamy macierz $[A| \ I_n]$ do postaci kanonicznej metodą Gaussa - Jordana.

Krok 3. Niech $[C| \ D]$ będzie otrzymaną postacią kanoniczną. Możliwe są dwie sytuacje.

(a) Jeżeli $C = I_n$, to $A^{-1} = D$.

(b) Jeżeli $C \neq I_n$, to A^{-1} nie istnieje.

Przykład 110 *Znajdziemy (o ile istnieje) odwrotność macierzy*

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 3 \\ 5 & 5 & 1 \end{bmatrix}.$$

Krok 1. *Tworzymy macierz* $[A|\ I_3]$

$$[A|\ I_3] = \left[\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 2 & 3 & 0 & 1 & 0 \\ 5 & 5 & 1 & 0 & 0 & 1 \end{array}\right].$$

Krok 2. *Redukujemy tę macierz do postaci kanonicznej*

$$[C|\ D] = \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & \frac{13}{8} & -\frac{1}{2} & -\frac{1}{8} \\ 0 & 1 & 0 & -\frac{15}{8} & \frac{1}{2} & \frac{3}{8} \\ 0 & 0 & 1 & \frac{5}{4} & 0 & -\frac{1}{4} \end{array}\right].$$

Krok 3. *Odczytujemy rozwiązanie*

$$A^{-1} = \begin{bmatrix} \frac{13}{8} & -\frac{1}{2} & -\frac{1}{8} \\ -\frac{15}{8} & \frac{1}{2} & \frac{3}{8} \\ \frac{5}{4} & 0 & -\frac{1}{4} \end{bmatrix}.$$

Przykład 111 *Znaleźć (o ile istnieje) odwrotność macierzy*

$$A = \begin{bmatrix} 1 & 2 & -3 \\ 1 & -2 & 1 \\ 5 & -2 & -3 \end{bmatrix}.$$

Krok 1. Formujemy macierz rozszerzoną

$$[A|\ I_3] = \left[\begin{array}{ccc|ccc} 1 & 2 & -3 & 1 & 0 & 0 \\ 1 & -2 & 1 & 0 & 1 & 0 \\ 5 & -2 & -3 & 0 & 0 & 1 \end{array}\right].$$

Krok 2. Przeprowadzamy redukcję Gaussa - Jordana, w wyniku której otrzymujemy macierz

$$\left[\begin{array}{ccc|ccc} 1 & 2 & -3 & 1 & 0 & 0 \\ 0 & -4 & 4 & -1 & 1 & 0 \\ 0 & 0 & 0 & -2 & -3 & 1 \end{array}\right].$$

Krok 3. W tym momencie jest jasne, że nie jest możliwe aby $C = I_n$. Wnioskujemy zatem, że A^{-1} nie istnieje.

Twierdzenie 112 *Macierz wymiaru $n \times n$ jest nieosobliwa wtedy i tylko wtedy, gdy jest równoważna macierzy jednostkowej.*

Przypuśćmy, że A jest macierzą nieosobliwą i rozważmy układ równań

$$AX = B.$$

Ponieważ istnieje macierz odwrotna do A, więc możemy rozwiązać ten układ równań mnożąc obie strony przez A^{-1}:

$$\begin{aligned} A^{-1}(AX) &= A^{-1}B \\ (A^{-1}A)X &= A^{-1}B \\ I_nX &= A^{-1}B \\ X &= A^{-1}B. \end{aligned}$$

Zatem, w przypadku gdy macierz współczynników układu jest nieosobliwa, układ ma dokładnie jedno rozwiązanie $X = A^{-1}B$.

Twierdzenie 113 *Jeżeli A jest macierzą wymiaru $n \times n$, to jednorodny układ równań*

$$AX = 0$$

ma rozwiązanie nietrywialne wtedy i tylko wtedy, gdy macierz A jest osobliwa.

Twierdzenie 114 *Macierz wymiaru $n \times n$ jest nieosobliwa wtedy i tylko wtedy, gdy układ równań*

$$AX = B$$

ma dokładnie jedno rozwiązanie, dla dowolnej macierzy B wymiaru $n \times 1$.

Podsumujmy nasze spostrzeżenia w postaci listy zdań równoważnych własności nieosobliwości.

Następujące zdania są równoważne.

1. Macierz A jest nieosobliwa.

2. Układ $AX = 0$ ma tylko trywialne rozwiązanie.

3. Macierz A jest równoważna macierzy I_n.

4. Układ $AX = B$ ma dokładnie jedno rozwiązanie, przy dowolnej macierzy B, wymiaru $n \times 1$.

4.7 Wyznacznik macierzy

Definicja 115 *Niech $S = \{1, 2, ..., n\}$ będzie zbiorem liczb naturalnych od 1 do n. Dowolne ustawienie elementów zbioru S w jakimkolwiek porządku $j_1 j_2 ... j_n$ nazywamy* permutacją *zbioru S.*

Dla przykładu, 4231 jest permutacją zbioru $S = \{1, 2, 3, 4\}$. Łatwo zauważyć, że istnieje dokładnie $n!$ różnych permutacji zbioru S. Parę elementów j_r i j_s nazywamy *inwersją* w permutacji $j_1 j_2 ... j_n$ jeżeli $r < s$, ale $j_r > j_s$. Na przykład, 4 i 2 stanowią inwersję w permutacji 4231. Permutacje dzielimy na *parzyste* i *nieparzyste* w zależności od parzystości liczby inwersji w nich występujących. Na przykład, permutacja 4231 jest nieparzysta ponieważ zawiera 5 inwersji $42, 43, 41, 21, 31$.

Definicja 116 *Niech* $A = [a_{ij}]$ *będzie macierzą wymiaru* $n \times n$*.* Wyznacznikiem *macierzy* A *nazywamy liczbę określoną wzorem*

$$\det A = |A| = \sum (\pm) a_{1j_1} a_{2j_2} ... a_{nj_n},$$

gdzie sumowanie przebiega po wszystkich permutacjach $j_1 j_2 ... j_n$ *zbioru* $S = \{1, 2, ..., n\}$*. Znak* $+$ *lub* $-$ *jest zgodny z parzystością permutacji* $j_1 j_2 ... j_n$*.*

Przykład 117 *Niech* $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$*. Wówczas* $\det A = a_{11}a_{22} - a_{12}a_{21}$*.*

Przykład 118 *Niech* $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$*. Wówczas*

$$\begin{aligned} \det A &= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} \\ &\quad -a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}. \end{aligned}$$

Przykład 119 *Obliczymy wyznacznik macierzy* $A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \\ 3 & 1 & 2 \end{bmatrix}$*.*

$$\begin{aligned} \det A &= 1 \cdot 1 \cdot 2 + 2 \cdot 3 \cdot 3 + 3 \cdot 2 \cdot 1 \\ &\quad -3 \cdot 1 \cdot 3 - 2 \cdot 2 \cdot 2 - 1 \cdot 3 \cdot 1 \\ &= 2 + 18 + 6 - 9 - 8 - 3 \\ &= 6. \end{aligned}$$

Uderzający jest fakt szybkiego wzrostu liczby operacji arytmetycznych potrzebnych do obliczenia wyznacznika stopnia n. W istocie, już dla $n = 10$ dostajemy $10! = 3628\,800$ permutacji, a dla $n = 100$ mamy ich już $100! = 93\,326\,215\,443\,944\,152\,681\,699\,238\,856\,266\,700\,490\,715\,968\,264\,381\,621\,468\,592\,963\,895\,217\,599\,993\,229\,915\,608\,941\,463\,976\,156\,518\,286\,253\,697\,920\,827\,223\,758\,251\,185\,210\,916\,864\,000\,000\,000\,000\,000\,000\,000\,000$. Będziemy zatem potrzebować innych, bardziej efektywnych metod obliczania wyznaczników. W tym celu przyjrzymy się najpierw własnościom wyznacznika.

Twierdzenie 120 *Wyznaczniki macierzy A i jej transpozycji są równe, to znaczy,*

$$\det A = \det A^T.$$

Twierdzenie 121 *Jeżeli macierz B powstała z macierzy A w wyniku zamiany miejscami dwóch wierszy (lub dwóch kolumn), to* $\det B = -\det A$.

Przykład 122 *Niech* $A = \begin{bmatrix} 2 & -1 \\ 3 & 2 \end{bmatrix}$ *i* $B = \begin{bmatrix} 3 & 2 \\ 2 & -1 \end{bmatrix}$. *Wtedy* $\det A = 7$ *i* $\det B = -7$.

Wniosek 123 *Jeżeli dwa wiersze (lub dwie kolumny) macierzy A są identyczne, to* $\det A = 0$.

Twierdzenie 124 *Jeżeli macierz A zawiera wiersz (lub kolumnę) składający się z samych zer, to* $\det A = 0$.

Twierdzenie 125 *Jeżeli macierz B powstała z macierzy A w wyniku pomnożenia wiersza (lub kolumny) przez pewną liczbę c, to* $\det B = c \det A$.

Przykład 126 *Stosując powyższe twierdzenia możemy upraszczać rachunki wyciągając wspólne czynniki z wierszy i kolumn przed wyznacznik. Na przykład,*

$$\begin{vmatrix} 1 & 2 & 3 \\ 1 & 5 & 3 \\ 2 & 8 & 6 \end{vmatrix} = 2 \begin{vmatrix} 1 & 2 & 3 \\ 1 & 5 & 3 \\ 1 & 4 & 3 \end{vmatrix} = 2 \cdot 3 \begin{vmatrix} 1 & 2 & 1 \\ 1 & 5 & 1 \\ 1 & 4 & 1 \end{vmatrix} = 2 \cdot 3 \cdot 0 = 0.$$

Twierdzenie 127 *Jeżeli macierz B została otrzymana z macierzy A w wyniku dodania do pewnego wiersza kombinacji liniowej pozostałych wierszy, to* $\det B = \det A$.

Przykład 128 *Mamy*

$$\begin{vmatrix} 1 & 2 & 3 \\ 2 & -1 & 3 \\ 1 & 0 & 1 \end{vmatrix} = \begin{vmatrix} 5 & 0 & 9 \\ 2 & -1 & 3 \\ 1 & 0 & 1 \end{vmatrix} = 4,$$

poprzez operację $2w_2 + w_1$.

Twierdzenie 129 *Jeżeli A jest macierzą trójkątną ($a_{ij} = 0$ gdy $i > j$), to*

$$\det A = a_{11}a_{22}...a_{nn}.$$

Ostatnie twierdzenie sugeruje pewną metodę obliczania wyznacznika poprzez sprowadzenie macierzy do postaci trójkątnej. Zilustrujemy to w następnym przykładzie.

Przykład 130 *Mamy*

$$\left|\begin{array}{rrr} 4 & 3 & 2 \\ 3 & -2 & 5 \\ 2 & 4 & 6 \end{array}\right|_{\frac{1}{2}w_3} = 2\left|\begin{array}{rrr} 4 & 3 & 2 \\ 3 & -2 & 5 \\ 1 & 2 & 3 \end{array}\right|_{w_1 \leftrightarrow w_3} = -2\left|\begin{array}{rrr} 1 & 2 & 3 \\ 3 & -2 & 5 \\ 4 & 3 & 2 \end{array}\right|_{-3w_1+w_2, -4w_1+w_3}$$

$$\begin{aligned} &= -2\left|\begin{array}{rrr} 1 & 2 & 3 \\ 0 & -8 & -4 \\ 0 & -5 & -10 \end{array}\right|_{-\frac{1}{4}w_2 \leftrightarrow -\frac{1}{5}w_3} = -(-2)(-4)(-5)\left|\begin{array}{rrr} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{array}\right|_{-2w_2+w_3} \\ &= -(-2)(-4)(-5)\left|\begin{array}{rrr} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & -3 \end{array}\right| = 2 \cdot 4 \cdot 5 \cdot (-3) = -120. \end{aligned}$$

Twierdzenie 131 *Wyznacznik iloczynu dwóch macierzy jest równy iloczynowi ich wyznaczników, to znaczy*

$$\det(AB) = (\det A)(\det B).$$

Przykład 132 *Niech* $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ *i* $B = \begin{bmatrix} 2 & -1 \\ 1 & 2 \end{bmatrix}$. *Wtedy* $\det A = -2$, $\det B = 5$ *i*

$$\begin{aligned} \det(AB) &= \det \begin{bmatrix} 4 & 3 \\ 10 & 5 \end{bmatrix} = 20 - 30 = -10 \\ &= (-2)(5) = (\det A)(\det B). \end{aligned}$$

Wniosek 133 *Jeżeli A jest macierzą nieosobliwą, to* $\det A \neq 0$ *i*

$$\det A^{-1} = \frac{1}{\det A}.$$

Przykład 134 *Niech* $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$. *Wówczas* $\det A = -2$ *i*

$$A^{-1} = \begin{bmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{bmatrix}.$$

Ponadto, $\det A^{-1} = -\frac{1}{2} = \frac{1}{\det A}$.

4.8 Rozwinięcie Laplace'a

W tej części poznamy inną metodę obliczania wyznacznika wykorzystującą tzw. *rozwinięcie Laplace'a*. Będziemy potrzebować następujących definicji.

Definicja 135 *Niech $A = [a_{ij}]$ będzie macierzą $n \times n$. Niech M_{ij} oznacza podmacierz wymiaru $(n-1) \times (n-1)$ otrzymaną z A poprzez usunięcie i-tego wiersza i j-tej kolumny. Wyznacznik* $\det M_{ij}$ *nazywamy* minorem *elementu a_{ij}. Wyrażenie*

$$A_{ij} = (-1)^{i+j} \det M_{ij}$$

nazywamy dopełnieniem (algebraicznym) *elementu a_{ij}.*

Przykład 136 *Niech*

$$A = \begin{bmatrix} 3 & -1 & 2 \\ 4 & 5 & 6 \\ 7 & 1 & 2 \end{bmatrix}.$$

Wówczas $\det M_{12} = \det \begin{bmatrix} 4 & 6 \\ 7 & 2 \end{bmatrix} = -34$, $\det M_{23} = \det \begin{bmatrix} 3 & -1 \\ 7 & 2 \end{bmatrix} = 10$. *Ponadto,* $A_{12} = (-1)^{1+2} \det M_{12} = (-1)(-34) = 34$, *oraz* $A_{23} = (-1)^{2+3} \det M_{23} = (-1)(10) = -10$.

Wyrażenie $(-1)^{i+j}$ określa znak $\pm$ w zależności od parzystości sumy $i+j$. Znaki te mogą układają się naprzemiennie zarówno według wierszy jak i kolumn:

$$\begin{bmatrix} + & - \\ - & + \end{bmatrix}, \begin{bmatrix} + & - & + \\ - & + & - \\ + & - & + \end{bmatrix}, \begin{bmatrix} + & - & + & - \\ - & + & - & + \\ + & - & + & - \\ - & + & - & + \end{bmatrix}.$$

Następujące twierdzenie przedstawia nowy, rekurencyjny sposób obliczania wyznaczników.

Twierdzenie 137 (Rozwinięcie Laplace'a) *Niech $A = [a_{ij}]$ będzie macierzą wymiaru $n \times n$. Wówczas dla każdego $1 \leq i \leq n$,*

$$\det A = a_{i1}A_{i1} + a_{i2}A_{i2} + ... + a_{in}A_{in}$$

oraz dla każdego $1 \leq j \leq n$,

$$\det A = a_{1j}A_{1j} + a_{2j}A_{2j} + ... + a_{nj}A_{nj}.$$

Pierwszy z tych wzorów nosi nazwę rozwinięcia wyznacznika $\det A$ *według i-tego wiersza, drugi zaś nazywany jest rozwinięciem według j-tej kolumny.*

Przykład 138 *W celu obliczenia wyznacznika macierzy*

$$A = \begin{bmatrix} 1 & 2 & -3 & 4 \\ -4 & 2 & 1 & 3 \\ 3 & 0 & 0 & -3 \\ 2 & 0 & -2 & 3 \end{bmatrix}$$

zauważmy wpierw, że najlepiej będzie rozwijać go według trzeciego wiersza lub drugiej kolumny

(z uwagi na zera). Przy wyborze pierwszej możliwości otrzymujemy

$$\begin{aligned}\det A &= 3\begin{vmatrix} 2 & -3 & 4 \\ 2 & 1 & 3 \\ 0 & -2 & 3 \end{vmatrix} + 3\begin{vmatrix} 1 & 2 & -3 \\ -4 & 2 & 1 \\ 2 & 0 & -2 \end{vmatrix} = 3 \times 20 + 3 \times (-4) \\ &= 48\end{aligned}$$

Przykład 139 *Ten sam wyznacznik możemy również obliczyć nieco inaczej, wykorzystując poprzednie własności.*

$$\begin{aligned}\det A &= \left.\begin{vmatrix} 1 & 2 & -3 & 4 \\ -4 & 2 & 1 & 3 \\ 3 & 0 & 0 & -3 \\ 2 & 0 & -2 & 3 \end{vmatrix}\right|_{k_1+k_4} = \begin{vmatrix} 1 & 2 & -3 & 5 \\ -4 & 2 & 1 & -1 \\ 3 & 0 & 0 & 0 \\ 2 & 0 & -2 & 5 \end{vmatrix} = 3\left.\begin{vmatrix} 2 & -3 & 5 \\ 2 & 1 & -1 \\ 0 & -2 & 5 \end{vmatrix}\right|_{-w_1+w_2} \\ &= 3\begin{vmatrix} 2 & -3 & 5 \\ 0 & 4 & -6 \\ 0 & -2 & 5 \end{vmatrix} = 3 \times 2\begin{vmatrix} 4 & -6 \\ -2 & 5 \end{vmatrix} = 3 \times 2 \times (20 - 12) \\ &= 48.\end{aligned}$$

4.9 Odwrotność macierzy

Przyjrzymy się teraz wyrażeniu

$$a_{i1}A_{k1} + a_{i2}A_{k2} + ... + a_{in}A_{kn},$$

w przypadku gdy $i \neq k$. To doprowadzi nas do nowego wzoru na odwrotność macierzy nieosobliwej.

Twierdzenie 140 *Jeżeli* $A = [a_{ij}]$ *jest macierzą wymiaru* $n \times n$, *to dla wszystkich* $i, j \neq k$

zachodzą wzory

$$\begin{aligned} a_{i1}A_{k1} + a_{i2}A_{k2} + ... + a_{in}A_{kn} &= 0, \\ a_{1j}A_{1k} + a_{2j}A_{2k} + ... + a_{nj}A_{nk} &= 0. \end{aligned}$$

Definicja 141 *Macierz D_A określoną wzorem*

$$D_A = [A_{ij}]^T$$

nazywamy macierzą dopełnień *stowarzyszoną z macierzą A.*

Przykład 142 *Niech*

$$A = \begin{bmatrix} 3 & -2 & 1 \\ 5 & 6 & 2 \\ 1 & 0 & -3 \end{bmatrix}.$$

Obliczymy macierz dopełnień D_A. W tym celu najpierw znajdujemy wszystkie dopełnienia algebraiczne elementów macierzy A, a następnie ustawiamy je odpowiednio w macierz. Ponieważ

$$\begin{aligned} A_{11} &= -18, \ \ A_{12} = 17, \ \ A_{13} = -6, \\ A_{21} &= -6, \ \ A_{22} = -10, \ \ A_{23} = -2, \\ A_{31} &= -10, \ \ A_{32} = -1, \ \ A_{33} = 28, \end{aligned}$$

więc

$$D_A = \begin{bmatrix} -18 & -6 & -10 \\ 17 & -10 & -1 \\ -6 & -2 & 28 \end{bmatrix}.$$

Twierdzenie 143 *Jeżeli $A = [a_{ij}]$ jest macierzą $n \times n$, to*

$$AD_A = D_A A = (\det A) I_n.$$

Przykład 144 *Rozważmy macierze A i D_A z poprzedniego przykładu. Mamy*

$$
\begin{aligned}
AD_A &= \begin{bmatrix} 3 & -2 & 1 \\ 5 & 6 & 2 \\ 1 & 0 & -3 \end{bmatrix} \begin{bmatrix} -18 & -6 & -10 \\ 17 & -10 & -1 \\ -6 & -2 & 28 \end{bmatrix} = \begin{bmatrix} -94 & 0 & 0 \\ 0 & -94 & 0 \\ 0 & 0 & -94 \end{bmatrix} \\
&= (-94) \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.
\end{aligned}
$$

Wniosek 145 *Jeżeli $A = [a_{ij}]$ jest macierzą $n \times n$ i $\det A \neq 0$, to*

$$A^{-1} = \frac{1}{\det A} D_A.$$

Wniosek 146 *Macierz A jest nieosobliwa wtedy i tylko wtedy, gdy $\det A \neq 0$.*

Wniosek 147 *Jeżeli $A = [a_{ij}]$ jest macierzą $n \times n$, to jednorodny układ równań $AX = 0$ ma rozwiązanie nietrywialne wtedy itylko wtedy, gdy $\det A = 0$.*

4.10 Reguła Cramera

Wykorzystamy rezultaty poprzedniej sekcji do wyprowadzenia jeszcze jednej metody rozwiązywania układów równań liniowych o n równaniach i n niewiadomych.

Twierdzenie 148 (Reguła Cramera) *Niech $AX = B$ będzie układem n równań z n niewiadomymi. Jeżeli $\det A \neq 0$, to układ ten ma dokładnie jedno rozwiązanie wyrażające się wzorami*

$$x_i = \frac{\det A_i}{\det A}, \quad i = 1, 2, ..., n,$$

gdzie A_i oznacza macierz otrzymaną w wyniku zastąpienia i-tej kolumny macierzy A przez kolumnę wyrazów wolnych B.

Przykład 149 *Rozważmy następujący układ równań.*

$$\begin{aligned} -2x_1+3x_2-x_3 &= 1\\ x_1+2x_2-x_3 &= 4\\ -2x_1-x_2+x_3 &= -3. \end{aligned}$$

Mamy

$$A=\begin{bmatrix} -2 & 3 & -1\\ 1 & 2 & -1\\ -2 & -1 & 1 \end{bmatrix},\ B=\begin{bmatrix} 1\\ 4\\ -3 \end{bmatrix}$$

oraz

$$A_1=\begin{bmatrix} 1 & 3 & -1\\ 4 & 2 & -1\\ -3 & -1 & 1 \end{bmatrix},\ A_2=\begin{bmatrix} -2 & 1 & -1\\ 1 & 4 & -1\\ -2 & -3 & 1 \end{bmatrix},\ A_3=\begin{bmatrix} -2 & 3 & 1\\ 1 & 2 & 4\\ -2 & -1 & -3 \end{bmatrix}.$$

Stąd $\det A=-2$, $\det A_1=-4$, $\det A_2=-6$, $\det A_3=-8$ *i*

$$\begin{aligned} x_1 &= \frac{\det A_1}{\det A}=\frac{-4}{-2}=2\\ x_2 &= \frac{\det A_2}{\det A}=\frac{-6}{-2}=3\\ x_3 &= \frac{\det A_3}{\det A}=\frac{-8}{-2}=4. \end{aligned}$$

5

Przestrzenie wektorowe

W tym rozdziale zapoznamy się z najważniejszym pojęciem Algebry Liniowej - *przestrzenią wektorową*. Ograniczymy się przy tym do *przestrzeni rzeczywistych*, w których zbiorem *skalarów* jest $\mathbb{R}$. Podstawowym modelem przestrzeni wektorowej jest zbiór wektorów płaszczyzny lub przestrzeni 3-wymiarowej z dobrze znanymi operacjami dodawania wektorów i mnożenia wektora przez skalar. Własności tych przestrzeni stanowią punkt wyjścia ogólnej definicji przestrzeni wektorowej.

5.1 Definicja przestrzeni wektorowej

Definicja 150 *Niech V będzie pewnym zbiorem z określonymi działaniami "dodawania" $u \oplus v$ i "mnożenia" $r \odot u$, dla dowolnych elementów $u, v \in V$ i $r \in \mathbb{R}$. Zbiór V nazywamy* przestrzenią wektorową *nad $\mathbb{R}$ jeżeli dla dowolnych elementów $u, v, w \in V$ i dowolnych liczb rzeczywistych $r, s \in \mathbb{R}$ spełnione są następujące warunki.*

1) $u \oplus v \in V$.

2) $u \oplus (v \oplus w) = (u \oplus v) \oplus w$.

3) $u \oplus v = v \oplus u$.

4) Istnieje element neutralny $0 \in V$ taki, że

$$u \oplus 0 = u.$$

5) Dla każdego $u \in V$ istnieje element przeciwny $-u \in V$ spełniający równość

$$u \oplus (-u) = 0.$$

a) $r \odot u \in V$.

b) $r \odot (u \oplus v) = (r \odot u) \oplus (r \odot v)$.

c) $(r + s) \odot u = (r \odot u) \oplus (s \odot u)$.

d) $r \odot (s \odot u) = (rs) \odot u$.

e) $1 \odot u = u$.

Elementy zbioru V nazywamy oczywiście wektorami *natomiast liczby rzeczywiste określane są tutaj mianem* skalarów.

Przedstawimy teraz kilka typów przestrzeni wektorowych.

Przykład 151 *Podstawowym typem przestrzeni wektorowych są przestrzenie, w których $V = \mathbb{R}^n$, a operacje dodawania i mnożenia określone są następująco. Niech $u, v \in \mathbb{R}^n$ i $r \in \mathbb{R}$. Wówczas, jeżeli $u = [u_1, u_2, ...u_n]$ i $v = [v_1, v_2, ..., v_n]$, to*

$$\begin{aligned} u \oplus v &= [u_1 + v_1, u_2 + v_2, ..., u_n + v_n], \\ r \odot u &= [ru_1, ru_2, ..., ru_n]. \end{aligned}$$

Przykład 152 *Symbolem $M_{m\times n}(\mathbb{R})$ oznaczamy przestrzeń wektorową macierzy wymiaru $m \times n$ o elementach rzeczywistych. Wektorami są więc tu macierze ustalonego wymiaru $m \times n$, skalarami liczby rzeczywiste, a operacjami zwykłe dodawanie macierzy i mnożenie macierzy przez liczbę.*

Przykład 153 *Kolejnego przykładu przestrzeni wektorowej dostarczają wielomiany. Przestrzeń wielomianów o współczynnikach rzeczywistych stopnia co najwyżej n oznaczamy symbolem $P_n(\mathbb{R})$.*

Przykład 154 *Istnieją również całkiem "egzotyczne" przestrzenie wektorowe o dość przewrotnie określonych operacjach. Jeżeli przyjmiemy $V = \{x \in \mathbb{R} : x > 0\}$ oraz*

$$u \oplus v = uv, \;\; r \odot u = u^r,$$

to również otrzymamy przestrzeń wektorową.

Twierdzenie 155 *Jeżeli V jest przestrzenią wektorową, to dla każdego $u \in V$ i $r \in \mathbb{R}$ mamy*

a) $0u = 0$,

b) $r0 = 0$,

c) jeżeli $ru = 0$, *to* $r = 0$ *lub* $u = 0$,

d) $(-1)u = -u$.

Własności podane w twierdzeniu są prostymi konsekwencjami definicji przestrzeni wektorowej.

5.2 Podprzestrzenie

Definicja 156 *Niech V będzie przestrzenią wektorową. Podzbiór $W \subseteq V$ nazywamy* podprzestrzenią V *jeżeli W również jest przestrzenią wektorową z tymi samymi operacjami co V.*

Twierdzenie 157 *Podzbiór W przestrzeni wektorowej V jest jej podprzestrzenią wtedy i tylko wtedy, gdy spełnione są następujące warunki.*

1) Jeżeli $u, v \in W$, to $u \oplus v \in W$.

2) Jeżeli $u \in W$ i $r \in \mathbb{R}$, to $r \odot u \in W$.

Przykład 158 *Niech A będzie macierzą wymiaru $m \times n$. Wówczas zbiór*

$$W = \{x \in \mathbb{R}^n : Ax = 0\}$$

jest podprzestrzenią w $\mathbb{R}^n$.

Przykład 159 *Niech $V = M_n(\mathbb{R})$ i niech $W = \{A \in V : A = A^T\}$. Ponieważ suma dwóch macierzy symetrycznych jest macierzą symetryczną i iloczyn macierzy symetrycznej przez liczbę także jest macierzą symetryczną , więc W jest podprzestrzenią V.*

Definicja 160 *Niech $v_1, ..., v_n$ będą wektorami przestrzeni V i niech $c_1, ..., c_n$ będą liczbami rzeczywistymi. Wówczas wektor*

$$v = c_1 v_1 + ... + c_n v_n$$

nazywamy kombinacją liniową *wektorów* $v_1, ..., v_n$ *o współczynnikach* $c_1, ..., c_n$.

Przykład 161 *Na przykład wektor* $(1,2)$ *jest kombinacją liniową wektorów* $(1,1)$ *i* $(1,0)$, *ponieważ*

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

Definicja 162 *Zbiór wszystkich kombinacji liniowych wektorów* $v_1, ...v_n$ *nazywamy* powłoką liniową *generowaną przez zbiór* $S = \{v_1, ..., v_n\}$ *i oznaczamy symbolem* $Lin(S)$.

Twierdzenie 163 *Niech* $S = \{v_1, ...v_k\}$ *będzie skończonym zbiorem wektorów pewnej przestrzeni* V. *Wówczas powłoka liniowa* $Lin(S)$ *jest podprzestrzenią w* V.

Dowód. Oznaczmy $W = Lin(S)$ i rozważmy sumę $u + v$ dwóch wektorów z W. Jeżeli $u, v \in W$, to

$$\begin{aligned} u &= b_1v_1 + ... + b_nv_n, \\ v &= c_1v_1 + ... + c_nv_n. \end{aligned}$$

Wówczas

$$\begin{aligned} u + v &= (b_1v_1 + ... + b_nv_n) + (c_1v_1 + ... + c_nv_n) \\ &= (b_1 + c_1)v_1 + ... + (b_n + c_n)v_n, \end{aligned}$$

co oznacza, że $u + v \in W$. Podobnie można się upewnić, że $ru \in W$, co kończy dowód.

5.3 Liniowa niezależność

Definicja 164 *Mówimy, że wektory* $v_1, v_2, ..., v_n \in V$ rozpinają *(lub* generują*) przestrzeń* V *jeżeli*

$$Lin(v_1, v_2, ..., v_n) = V.$$

Przykład 165 *Na przykład wektory* $v_1 = (1,1)$ *i* $v_2 = (1,0)$ *rozpinają płaszczyznę. Aby to* *zobaczyć rozważmy dowolny wektor $v = (a, b)$. Jeżeli pokażemy, że równanie*

$$x_1(1,1) + x_2(1,0) = (a,b)$$

zawsze ma rozwiązanie, to tym samym pokażemy, że $v \in Lin(v_1, v_2)$. Ponieważ macierz tego układu

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

jest nieosobliwa, więc, bez względu na a i b, zawsze istnieje (dokładnie jedno) rozwiązanie.

Definicja 166 *Wektory $v_1, v_2, ..., v_n \in V$ nazywamy* liniowo niezależnymi *jeżeli równanie*

$$x_1v_1 + x_2v_2 + ... + x_nv_n = 0$$

ma dokładnie jedno *rozwiązanie w liczbach $x_1, ..., x_n$. W przeciwnym razie mówimy, że wektory są* liniowo zależne.

Przykład 167 *Wektory z poprzedniego przykładu są liniowo niezależne ponieważ, wobec odwracalności macierzy A, układ $AX = 0$, a tym samym równanie*

$$x_1(1,1) + x_2(1,0) = (0,0),$$

ma dokładnie jedno rozwiązanie.

Przykład 168 *Wektory $(1,1)$ i $(2,2)$ są liniowo zależne. W istocie, równanie*

$$x_1(1,1) + x_2(2,2) = (0,0)$$

prowadzi do układu jednorodnego o macierzy

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

której wyznacznik jest równy 0. Rozwiązań jest więc nieskończenie wiele.

Przykład 169 *Wektory* $(1,1)$, $(1,0)$ *i* $(0,-1)$ *również są liniowo zależne. Równanie*

$$x_1(1,1)+x_2(1,0)+x_3(0,-1)=(0,0)$$

prowadzi do układu jednorodnego o macierzy

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

Rozwiązań jest więc nieskończenie wiele, z uwagi nawymiar tej macierzy. W istocie, z tego samego powodu każdy zbiór składający się więcej niż n *wektorów przestrzeni* $\mathbb{R}^n$ *będzie liniowo zależny.*

Twierdzenie 170 *Wektory niezerowe* $v_1, v_2, ..., v_n \in V$ *są liniowo zależne wtedy i tylko wtedy, gdy istnieje wśród nich wektor* v_j*, będący liniową kombinacją poprzedzających go wektorów* $v_1, v_2, ..., v_{j-1}$.

Dowód. Przypuśćmy najpierw, że istnieje wektor v_j taki, że

$$v_j = c_1 v_1 + ... + c_{j-1} v_{j-1}.$$

Wówczas, równanie

$$x_1 v_1 + ... + x_j v_j + ... + x_n v_n = 0$$

posiada rozwiązanie niezerowe

$$\begin{aligned} x_i &= c_i, \text{ dla } 1 \le i \le j-1, \\ x_j &= -1, \\ x_i &= 0, \text{ dla } j+1 \le i \le n, \end{aligned}$$

a więc wektory $v_1, v_2, ..., v_n$ są liniowo zależne.

Na odwrót, przypuśćmy, że wektory $v_1, v_2, ..., v_n$ są liniowo zależne i niech j będzie największą liczbą spośród $1, 2, ..., n$ taką, że $x_j \neq 0$. Wówczas, $x_i = 0$, dla $i > j$ i możemy napisać

$$\begin{aligned} x_1v_1 + ... + x_jv_j &= 0 \\ x_jv_j &= -x_1v_1 - ... - x_{j-1}v_{j-1} \\ v_j &= \left(-\frac{x_1}{x_j}\right)v_1 + ... + \left(-\frac{x_{j-1}}{x_j}\right)v_{j-1}, \end{aligned}$$

co kończy dowód.

5.4 Baza i wymiar przestrzeni wektorowej

Definicja 171 *Mówimy, że wektory $v_1, v_2, ..., v_n \in V$ tworzą* bazę *przestrzeni V jeśli są liniowo niezależne oraz $Lin(v_1, v_2, ..., v_n) = V$.*

Twierdzenie 172 *Niech $S = \{v_1, v_2, ..., v_n\}$ będzie zbiorem niezerowych wektorów przestrzeni V i niech $W = Lin(S)$. Wówczas pewien podzbiór zbioru S jest bazą przestrzeni W.*

Dowód. Jeżeli wektory zbioru S są liniowo niezależne to S jest bazą W. Przypuśćmy więc, że S jest liniowo zależny i niech v_j będzie wektorem z poprzedniego twierdzenia

$$v_j = c_1v_1 + ... + c_{j-1}v_{j-1}.$$

Łatwo zauważyć, że usunięcie wektora v_j ze zbioru S nie zmieni powłoki liniowej generowanej przez S. W istocie, zastępując v_j w dowolnej kombinacji liniowej zbioru S przez $c_1v_1 + ... + c_{j-1}v_{j-1}$ otrzymamy kombinację wektorów zbioru $S - \{v_j\}$. Zatem

$$Lin(S) = Lin(S - \{v_j\}).$$

Jeżeli zbiór $T = S - \{v_j\}$ jest liniowo niezależny, to T jest bazą W. W przeciwnym razie powtarzamy to samo postępowanie w stosunku do zbioru T, usuwając z niego kolejny zbędny wektor. Ponieważ liczba wektorów jest skończona, więc prędzej czy później otrzymamy zbiór niezależny generujący przestrzeń W, co było do udowodnienia.

Przykład 173 *Niech* $S = \{(1,1),\ (1,0), (0,-1)\}$*. Z poprzednich przykładów wiemy, że* S *jest liniowo zależny oraz* $Lin(S) = \mathbb{R}^2$*. Jednak mamy*

$$(0,-1) = -(1,1) + (1,0).$$

Zatem $Lin(S) = Lin(T)$*, gdzie* $T = \{(1,1),\ (1,0)\}$*. Ponieważ* T *jest niezależny, więc* T *jest bazą* $Lin(S)$*.*

Twierdzenie 174 *Niech* $S = \{v_1, v_2, ..., v_n\}$ *będzie bazą przestrzeni* V *i niech* $T = \{w_1, w_2, ..., w_m\}$ *będzie zbiorem wektorów liniowo niezależnych z* V*. Wówczas* $m \leq n$*.*

Dowód. Ponieważ S jest bazą przestrzeni V, więc $T \subseteq Lin(S)$ i w szczególności

$$w_1 = c_1 v_1 + ... + c_n v_n.$$

Zbiór T jest niezależny, a zatem $w_1 \neq 0$ i stąd $c_i \neq 0$ dla pewnego $1 \leq i \leq n$. Dla wygody przyjmijmy, że $i = 1$ po ewentualnym przenumerowaniu wektorów zbioru S. Wobec tego wektor v_1 może być przedstawiony w postaci kombinacji liniowej wektorów zbioru $S_1 = \{w_1, v_2, ..., v_n\}$ i w konsekwencji

$$Lin(S) = Lin(S_1).$$

Innymi słowy, wymiana wektora v_1 na w_1 nie zmieniła powłoki rozpiętej przez S. Ponadto zauważmy, że zbiór S_1 pozostaje liniowo niezależny. Rzeczywiście, przypuśćmy, że jakiś wektor v_j jest kombinacją wektorów $w_1, v_2, ..., v_{j-1}$

$$v_j = b_1 w_1 + b_2 v_2 + ... + b_{j-1} v_{j-1}.$$

Zauważmy, że musi być $b_1 \neq 0$, gdyż w przeciwnym razie zbiór $\{v_2, ..., v_n\}$, a co za tym idzie także S, byłby zależny. Stąd otrzymujemy

$$\begin{aligned} v_j &= b_1(c_1 v_1 + ... + c_n v_n) + b_2 v_2 + ... + b_{j-1} v_{j-1} \\ 0 &= (b_1 c_1) v_1 + d_2 v_2 + ... + d_n v_n, \end{aligned}$$

przy czym $b_1 c_1 \neq 0$, co jest sprzeczne z niezależnością zbioru S. Zatem zbiór S_1 jest bazą przestrzeni V.

Powtarzając to samo postępowanie do zbioru S_1 i wektora w_2 dostaniemy nową bazę

$$S_2 = \{w_1, w_2, v_3, ..., v_n\},$$

itd. Gdyby $m > n$, to otrzymalibyśmy w końcu zbiór $S_n = \{w_1, ..., w_n\}$ generujący całą przestrzeń i wektory $w_{n+1}, w_{n+2}, ..., w_m$ nie należące do S_n. Stąd, na przykład

$$w_{n+1} \in Lin(S_n)$$

co przeczy niezależności zbioru W. Dowód twierdzenia jest więc zakończony.

Wniosek 175 *Dwie dowolne bazy przestrzeni wektorowej V mają tę samą liczbę elementów.*

Przykład 176 *Najprostszą bazę przestrzeni $\mathbb{R}^2$ stanowią wektory $e_1 = (1, 0)$ i $e_2 = (0, 1)$. Wobec powyższego wniosku, każda inna baza musie mieć również dokładnie dwa wektory. Podobnie, każda baza przestrzeni $\mathbb{R}^n$ składa się z dokładnie n wektorów.*

Definicja 177 Wymiarem *niezerowej przestrzeni wektorowej V nazywamy liczbę wektorów dowolnej bazy V. Wymiar przestrzeni V oznaczamy symbolem* $\dim V$.

Przykład 178 *Łatwo zauważyć, że $\dim \mathbb{R}^n = n$, $\dim M_{m\times n} = mn$ oraz $\dim P_n = n+1$.*

Podamy jeszcze bez dowodów dwa użyteczne twierdzenia dotyczące baz przestrzeni wektorowych.

Twierdzenie 179 *Jeżeli S jest zbiorem liniowo niezależnych wektorów przestrzeni V, to istnieje baza przestrzeni V zawierająca zbiór S.*

Twierdzenie 180 *Niech V będzie przestrzenią wektorową wymiaru n i niech $S = \{v_1, v_2, ..., v_n\}$ będzie podzbiorem V. Wówczas*

1) Jeżeli S jest linowo niezależny, to S jest bazą V.

2) Jeżeli S generuje V, to S jest bazą V.

6

Przekształcenia liniowe