Michał Domka

Algebra Liniowa i Geometria Analityczna

materiały dydaktyczne

---

1. Podstawowe struktury algebraiczne

Definicja: Iloczynem kartezjańskim zbiorów A i B nazywamy zbiór $A \times B = \{(a, b), a \in A, b \in B\}$.
PRZYKŁAD: Dla $A = \{\square, \triangle\}$ oraz $B = \{\heartsuit, \diamondsuit, \clubsuit, \spadesuit\}$ zachodzi:
$A \times B = \{(\square, \heartsuit), (\square, \diamondsuit), (\square, \clubsuit), (\square, \spadesuit), (\triangle, \heartsuit), (\triangle, \diamondsuit), (\triangle, \clubsuit), (\triangle, \spadesuit)\}$.
Definicja: Działaniem (wewnętrznym) na zbiorze X nazywamy funkcję $X \times X \to X$.
Innymi słowy, działaniem wewnętrznym na zbiorze X nazywamy funkcję, która każdej parze elementów tego zbioru przyporządkowuje pewien element tego samego zbioru.
PRZYKŁAD:

- dodawanie liczb naturalnych: $\mathbb{N} \times \mathbb{N} \ni (a, b) \mapsto a + b \in \mathbb{N}$,
- dzielenie liczb rzeczywistych różnych od 0: $\mathbb{R}^* \times \mathbb{R}^* \ni (a, b) \mapsto a/b \in \mathbb{R}^*$,
- działanie na zbiorze $A = \{\square, \triangle\}$ określone jako: $(\square, \square) \mapsto \square$, $(\square, \triangle) \mapsto \triangle$, $(\triangle, \square) \mapsto \triangle$, $(\triangle, \triangle) \mapsto \square$.

Dla działania oznaczonego jako $\bullet$, wynik tego działania dla argumentów (a, b) będziemy oznaczać jako $a \bullet b$.
Definicja: Niech $\bullet$ będzie działaniem na zbiorze X.
Działanie $\bullet$ jest łączne, jeżeli $\forall x, y, z \in X : x \bullet (y \bullet z) = (x \bullet y) \bullet z$.
Działanie $\bullet$ jest przemienne, jeżeli $\forall x, y \in X : x \bullet y = y \bullet x$.
$e \in X$ jest elementem neutralnym działania $\bullet$, jeżeli $\forall x \in X : x \bullet e = e \bullet x = x$.
$y \in X$ jest elementem symetrycznym (przeciwnym, odwrotnym) do elementu x działania $\bullet$, jeżeli $x \bullet y = y \bullet x = e$, gdzie e jest elementem neutralnym.
PRZYKŁAD:

- Działanie dodawania liczb rzeczywistych jest łączne, przemienne, posiada element neutralny, którym jest 0, i każdy element zbioru posiada element symetryczny, którym jest liczba przeciwna.
- Działanie odejmowania liczb rzeczywistych nie jest łączne, nie jest przemienne, nie posiada elementu neutralnego i w związku z tym nie możemy mówić o elementach symetrycznych.
- Działanie mnożenia wielomianów rzeczywistych jest łączne, przemienne, posiada element neutralny, którym jest wielomian stały równy 1, ale elementy symetryczne istnieją tylko dla wielomanów stałych różnych od 0.
- Wprowadzone powyżej działanie na zbiorze A jest łączne, przemienne, posiada element neutralny $\square$ i każdy element zbioru A jest swoim własnym elementem symetrycznym.

Jeżeli działanie $\bullet$ jest łączne, możemy stosować notację $a \bullet b \bullet c$ zamiast $(a \bullet b) \bullet c$.
Definicja: Niech $\bullet$ będzie działaniem na zbiorze G. Zbiór G z działaniem $\bullet$ nazywamy grupą, jeżeli działanie $\bullet$ jest łączne, posiada element neutralny i każdy element zbioru G posiada element przeciwny. Grupę, której działanie jest przemienne, nazywamy grupą przemienną lub abelową.
PRZYKŁAD:

- Zbiór liczb rzeczywistych z działaniem dodawania jest grupą przemienną.
- Zbiór liczb rzeczywistych różnych od zera z działaniem mnożenia jest grupą przemienną.
- ZbiórA z wprowadzonym wyżej działaniem jest grupą przemienną.

Przykłady grup nieprzemiennych poznamy w kolejnych rozdziałach. Jako ciekawostkę podać można informację, że każda skończona grupa mająca co najwyżej 4 elementy jest przemienna.
Definicja: Niech $\circ, \diamond$ będą działaniami na zbiorze X. Działanie $\diamond$ jest rozdzielne względem $\circ$, jeżeli $\forall x, y, z \in X$: $(x \circ y) \diamond z = (x \diamond z) \circ (y \diamond z)$ oraz $x \diamond (y \circ z) = (x \diamond y) \circ (x \diamond z)$.
PRZYKŁAD: Działanie mnożenia jest rozdzielne względem dodawania na zbiorze liczb rzeczywistych oraz zbiorze funkcji rzeczywistych.
Definicja: Niech $+, \cdot$ będą działaniami na zbiorze F. Działanie $+$ będziemy nazywać dodawaniem, a $\cdot$ mnożeniem. Zbiór F nazywamy ciałem (ang. *field*), jeżeli: $(F, +)$ jest grupą abelową, $(F \setminus \{e_+\}, \cdot)$ jest grupą abelową (gdzie e_+ jest elementem neutralnym dla dodawania) oraz mnożenie jest rozdzielne względem dodawania.
PRZYKŁAD:

- Zbiór liczb rzeczywistych ze standardowymi działaniami dodawania i mnożenia jest ciałem.
- Zbiór liczb wymiernych ze standardowymi działaniami dodawania i mnożenia jest ciałem.
- Zbiór liczb całkowitych ze standardowymi działaniami dodawania i mnożenia nie jest ciałem.
- Zbiór wielomianów rzeczywistych ze standardowymi działaniami dodawania i mnożenia nie jest ciałem.
- Zbiór A z wprowadzonym wyżej działaniem jako dodawaniem oraz działaniem $\square \cdot \square = \square \cdot \triangle = \triangle \cdot \square = \square, \triangle \cdot \triangle = \triangle$ jako mnożeniem jest ciałem. Jest to najprostszy przykład ciała skończonego.

Ciało jest zatem strukturą algebraiczną, która ma podobne własności algebraiczne jak zbiór liczb rzeczywistych. Istnieje również rodzina struktur o właściwościach słabszych niż ciała:
Definicja: Niech $+, \cdot$ będą działaniami na zbiorze R. Zbiór R nazywamy pierścieniem (ang. *ring*), jeżeli: $(R, +)$ jest grupą abelową, mnożenie jest łączne oraz mnożenie jest rozdzielne względem dodawania. Pierścieniem z jedynką nazywamy pierścień, który posiada element neutralny względem mnożenia. Pierścieniem z dzieleniem nazywamy pierścień z jedynką, w którym każdy element inny niż element neutralny dla dodawania posiada element odwrotny względem mnożenia. Pierścieniem przemiennym nazywamy pierścień, w którym mnożenie jest przemienne.
PRZYKŁAD:

- Zbiór liczb całkowitych jest pierścieniem przemiennym z jedynką.
- Zbiór liczb całkowitych parzystych jest pierścieniem przemiennym bez jedynki.
- Zbiór wielomianów rzeczywistych jest pierścieniem przemiennym z jedynką.

Poprzez analogię do liczb rzeczywistych, element symetryczny do a względem dodawania będziemy nazywać elementem przeciwnym do a i oznaczać $-a$. Element symetryczny do a względem mnożenia będziemy nazywać elementem odwrotnym do a i oznaczać a^{-1}. Na ogół będziemy pomijać symbol mnożenia i pisać ab zamiast $a \cdot b$. O ile nie będzie rodziło to niejasności, elementy neutralne dla dodawania i mnożenia w pierścieniach nazywać będziemy odpowiednio zerem i jedynką oraz oznaczać jako 0 i 1. Zatem we wprowadzonym wcześniej ciele A zachodzi: $0 = \square$, $1 = \triangle$ oraz w konsekwencji $1 + 1 = 0$:-)
Zauważmy, że dzięki istnieniu elementów przeciwnych w każdym pierścieniu określone jest również działanie odejmowania: $a - b = a + (-b)$. W pierścieniu przemiennym z jedynką określone jest również działanie dzielenia przez elementy posiadające odwrotność względem mnożenia: $a/b = a \cdot b^{-1}$ (czyli w ciele przez każdy element różny od 0).
Uwaga: W literaturze spotyka się niespójności w kwestii nazewnictwa pierścieni. Niektórzy autorzy pierścieniem nazywają strukturę, którą my zdefiniowaliśmy jako pierścień z jedynką albo tę, którą my nazwaliśmy pierścieniem przemiennym.

2. Liczby zespolone

Rozważmy zbiór $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$. Wprowadźmy na nim działania dodawania i mnożenia:

$$(a, b) + (c, d) = (a + c, b + d) \tag{1}$$
$$(a, b) \cdot (c, d) = (ac - bd, ad + bc) \tag{2}$$

Zbiór $\mathbb{R}^2$ z tak zdefiniowanymi działaniami jest ciałem: elementem neutralnym dla dodawania jest $(0, 0)$, elementem przeciwnym dla dodawania dla (a, b) jest $(-a, -b)$, elementem neutralnym dla mnożenia jest $(1, 0)$, elementem odwrotnym względem mnożenia dla $(a, b) \neq (0, 0)$ jest $(a/(a^2 + b^2), -b/(a^2 + b^2))$:

$$(a, b) \cdot \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right) = \left(a\frac{a}{a^2 + b^2} - b\frac{-b}{a^2 + b^2}, a\frac{-b}{a^2 + b^2} + b\frac{a}{a^2 + b^2}\right) = (1, 0) \tag{3}$$

Sprawdzenie łączności, przemienności oraz rozdzielności pozostawiamy jako ćwiczenie. Określone w ten sposób ciało nazywamy ciałem liczb zespolonych (ang. *complex numbers*) i oznaczamy jako $\mathbb{C}$. Zauważmy teraz, że:

- elementem neutralnym dla dodawania w ciele liczb rzeczywistych jest 0, a w ciele liczb zespolonych $(0, 0)$,
- elementem neutralnym dla mnożenia w ciele liczb rzeczywistych jest 1, a w ciele liczb zespolonych $(1, 0)$,
- każdą liczbę zespoloną możemy traktować jako wektor na płaszczyźnie, który z kolei możemy pomnożyć przez liczbę rzeczywistą; okazuje się, że pomnożenie wektora przez liczbę rzeczywistą c daje ten sam wynik, co pomnożenie tego wektora jako liczby zespolonej przez liczbę zespoloną $(c, 0)$: $c(a, b) = (ca, cb) = (a, b)(c, 0)$

Analizując powyższe własności możemy zauważyć, że liczby zespolone postaci $(a, 0)$ zachowują się podobnie jak liczby rzeczywiste. Możemy zatem utożsamiać liczbę zespoloną $(a, 0)$ z liczbą rzeczywistą a. Utożsamienie to nie prowadzi do sprzeczności: jeżeli liczbę rzeczywistą a utożsamimy z $(a, 0)$, a liczbę b z $(b, 0)$, to dodając je jako liczby zespolone otrzymamy liczbę $(a + b, 0)$, którą możemy utożsamiać z $a + b$, czyli sumą tych liczb dodanych jako liczby rzeczywiste. Nie ma zatem znaczenia, czy liczby rzeczywiste będziemy dodawać jako liczby rzeczywiste, czy jako liczby zespolone o drugim elemencie równym zero - wynik będzie taki sam, o ile również utożsamimy go z liczbą rzeczywistą. Analogiczne własności zachodzą dla mnożenia: $ab = a \cdot b \rightsquigarrow (a, 0) \cdot (b, 0) = (ab, 0) \rightsquigarrow ab$, znajdowania liczby przeciwnej względem dodawania: $-a \rightsquigarrow -(a, 0) = (-a, 0) \rightsquigarrow -a$ oraz znajdowania odwrotności względem mnożenia: $a^{-1} \rightsquigarrow (a, 0)^{-1} = (a^{-1}, 0) \rightsquigarrow a^{-1}$.
Zbiór liczb zespolonych możemy zatem traktować jako rozszerzenie zbioru liczb rzeczywistych. Innymi słowy, zbiór liczb zespolonych ma tę własność, że jego podzbiór $\{(a, 0), a \in \mathbb{R}\}$ przy dodawaniu i mnożeniu zachowuje się dokładnie tak, jak zbiór liczb rzeczywistych.
Wprowadźmy teraz oznaczenie $i = (0, 1)$. Zachodzi:

$$i^2 = (0, 1) \cdot (0, 1) = (-1, 0) = -1 \tag{4}$$

Wprowadzoną w ten sposób liczbę i nazywamy jednostką urojoną. Dowolną liczbę (a, b) możemy zapisać jako $(a, 0) + (0, b) = (a, 0) \cdot (1, 0) + (b, 0) \cdot (0, 1) = a + bi$. Ostatnie wyrażenie to tzw. postać kanoniczna liczby zespolonej. Postać kanoniczna ułatwia wykonywanie operacji arytmetycznych:

$$(a + bi) + (c + di) = (a + b) + (c + d)i \tag{5}$$
$$(a + bi)(c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i \tag{6}$$

Dla liczby zespolonej $z = a + bi$, liczbę a nazywamy częścią rzeczywistą i oznaczamy $\mathrm{Re}(z)$, natomiast liczbę b nazywamy częścią urojoną $\mathrm{Im}(z)$. Zwróćmy uwagę, że część urojona jest liczbą rzeczywistą, tj. $\mathrm{Im}(z) = b \neq bi$.
Dowolną liczbę zespoloną z możemy zapisać jako:

$$z = a + bi = \sqrt{a^2 + b^2}\left(\frac{a}{\sqrt{a^2 + b^2}} + i\frac{b}{\sqrt{a^2 + b^2}}\right) \tag{7}$$

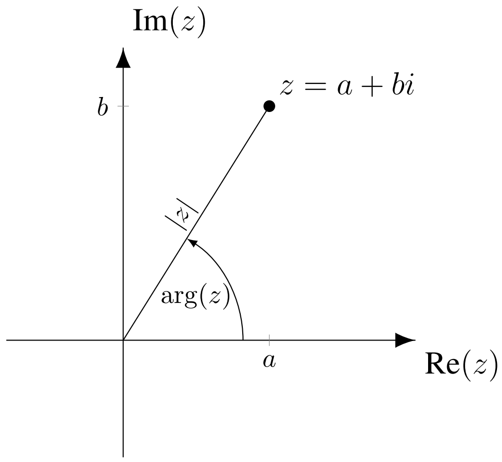
Zauważmy, że liczby $\frac{a}{\sqrt{a^2+b^2}}$ i $\frac{b}{\sqrt{a^2+b^2}}$ mają taką własność, że suma ich kwadratów równa się 1. Istnieje zatem $\varphi \in \mathbb{R}$, takie że $\cos\varphi = \frac{a}{\sqrt{a^2+b^2}}$ oraz $\sin\varphi = \frac{b}{\sqrt{a^2+b^2}}$. Ponadto, tak wyznaczone φ jest jedyne z dokładnością do 2π. Wprowadzając dodatkowo oznaczenie $r = \sqrt{a^2+b^2}$ otrzymujemy:

$$z = r(\cos\varphi + i\sin\varphi) \tag{8}$$

Jest to tzw. postać trygonometryczna liczby zespolonej. Przy takim zapisie, liczbę r nazywamy modułem liczby zespolonej i oznaczamy $|z|$, natomiast φ nazywamy argumentem liczby zespolonej i oznaczamy $\arg(z)$.
PRZYKŁAD:

$$z = 2 + 2\sqrt{3}i = 4\Big(\frac{1}{2} + i\frac{\sqrt{3}}{2}\Big) = 4\Big(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}\Big) \tag{9}$$
$$|z| = 4,\ \ \arg(z) = \frac{\pi}{3}$$

Liczbę zespoloną $z = a + bi$ możemy utożsamiać z punktem na płaszczyźnie o współrzędnych (a, b). W takiej sytuacji moduł i argument mają interpretację geometryczną: $|z|$ jest odległością tego punktu od $(0, 0)$, natomiast $\arg(z)$ jest kątem między dodatnią półosią osi OX, a wektorem łączącym $(0, 0)$ z (a, b).



Weźmy teraz dwie liczby zespolone $z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1)$ oraz $z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2)$. Zachodzi:

$$\begin{aligned} z_1z_2 = r_1(\cos\varphi_1 + i\sin\varphi_1)\cdot r_2(\cos\varphi_2 + i\sin\varphi_2) = r_1r_2(&\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2 + \\ &i(\cos\varphi_1\sin\varphi_2 + \sin\varphi_1\cos\varphi_2)) \end{aligned} \tag{10}$$

Z tożsamości trygonometrycznych wiadomo, że $\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2 = \cos(\varphi_1 + \varphi_2)$ oraz $(\cos\varphi_1\sin\varphi_2 + \sin\varphi_1\cos\varphi_2) = \sin(\varphi_1 + \varphi_2)$, zatem:

$$z_1z_2 = r_1r_2(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)) \tag{11}$$

Czyli:

$$|z_1z_2| = |z_1|\cdot|z_2| \tag{12}$$
$$\arg(z_1z_2) = \arg(z_1) + \arg(z_2) \tag{13}$$

Zauważmy teraz, że $|1| = 1$, $\arg(1) = 0$. Zatem dla $z \neq 0$:

$$\begin{aligned} &zz^{-1} = 1 \implies |zz^{-1}| = 1 \wedge \arg(zz^{-1}) = 0 \implies |z|\cdot|z^{-1}| = 1 \wedge \arg(z) + \arg(z^{-1}) = 0 \implies \\ &|z^{-1}| = |z|^{-1} \wedge \arg(z^{-1}) = -\arg(z) \end{aligned} \tag{14}$$

PRZYKŁAD: Dla $z = 2 + 2\sqrt{3}i$ mamy:

$$z^{-1} = \frac{1}{4}\Big(\cos\frac{-\pi}{3} + i\sin\frac{-\pi}{3}\Big) = \frac{1}{8} - i\frac{\sqrt{3}}{8} \tag{15}$$

Z (12), (13) oraz (14) wynika zatem, że dla $n \in \mathbb{N}$:

$$z^n = |z|^n(\cos n\varphi + i\sin n\varphi) \tag{16}$$
$$z^{-n} = (z^n)^{-1} = |z|^{-n}(\cos(-n\varphi) + i\sin(-n\varphi)) \tag{17}$$

Własność (16) zachodzi zatem również dla $n \in \mathbb{Z}$. Zależność ta nosi nazwę wzoru de Moivre'a i pozwala nam w łatwy sposób podnosić liczby zespolone do wysokich potęg o całkowitym wykładniku.
PRZYKŁAD: Dla $z = 2 + 2\sqrt{3}i$ mamy:

$$z^8 = 4^8\Big(\cos\frac{8\pi}{3} + i\sin\frac{8\pi}{3}\Big) = 4^8\Big(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\Big) \tag{18}$$

Uwaga: Wzoru (16) nie możemy stosować do podnoszenia liczb zespolonych do wykładników niebędacych liczbami całkowitymi. Operacja podnoszenia do niecałkowitej potęgi zdefiniowana jest wyłącznie dla liczb rzeczywistych dodatnich. W ogólnym przypadku liczby zespolonej (podobnie jak np. macierzy) nie da się podnieść do niecałkowitej potęgi, zatem nie da się np. obliczyć pierwiastka z liczby zespolonej. Podnoszenie do potęgi naturalnej jest natomiast dobrze określone w każdym pierścieniu jako: $a^n = a \cdot \ldots \cdot a$. Podnoszenie do potęgi całkowitej ujemnej jest dobrze zdefiniowane w każdym pierścieniu z dzieleniem (zatem także i w ciele) jako $a^{-n} = (a^n)^{-1}$.

Sprzężeniem liczby zespolonej $z = a+bi$ nazywamy liczbę $\bar{z} = a-bi$ (oznaczaną czasami jako z^*). Zauważmy, że $|\bar{z}| = |z|$ oraz $\arg(\bar{z}) = -\arg(z)$. Ponadto, $z^{-1} = \frac{\bar{z}}{|z|^2}$.
Istnieje jeszcze jedna szeroko stosowana postać liczby zespolonej: postać wykładnicza. Wykorzystując rozwinięcie funkcji sinus, cosinus oraz funkcji wykładniczej w szereg Taylora można pokazać, że:

$$r(\cos\varphi + i\sin\varphi) = re^{i\varphi} \tag{19}$$

Zastosowanie tej postaci jeszcze bardziej upraszcza mnożenie, dzielenie i potęgowanie liczb zespolonych, bowiem:

$$re^{i\varphi} \cdot se^{i\psi} = rse^{i(\varphi+\psi)} \tag{20}$$
$$(re^{i\varphi})^{-1} = r^{-1}e^{-i\varphi} \tag{21}$$
$$(re^{i\varphi})^n = r^n e^{in\varphi} \tag{22}$$

Ze wzoru (19) wynika ponadto, że:

$$e^{i\pi} + 1 = 0 \tag{23}$$

Jedna z najważniejszych własności liczb zespolonych wynika z poniższego twierdzenia:
Twierdzenie (zasadnicze twierdzenie algebry): Każdy wielomian stopnia $n > 0$ o zespolonych współczynnikach można przedstawić jako iloczyn n wielomianów pierwszego stopnia:

$$p(z) = a(z-z_1)(z-z_2)\ldots(z-z_n) \tag{24}$$

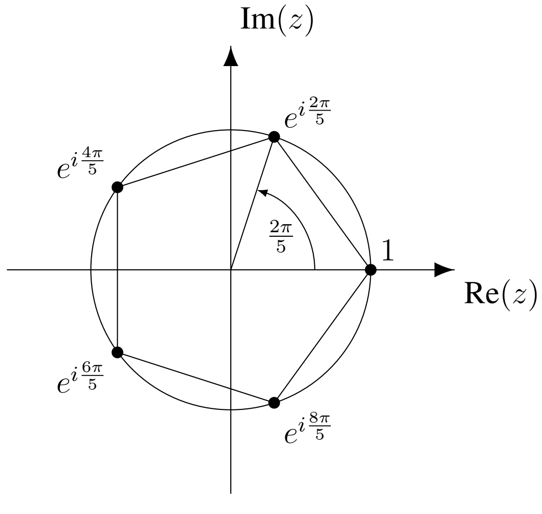
Bezpośrednią konsekwencją twierdzenia jest fakt, że każdy wielomian zespolony stopnia n posiada dokładnie n pierwiastków (licząc z krotnościami).
PRZYKŁAD:

$$\begin{aligned} p(z) &= z^3 - z^2 + 3z + 5 = (z+1)(z^2-2z+5) = (z+1)(z^2-2z+1+4) = (z+1)((z-1)^2-(2i)^2) = \\ &= (z+1)(z-1-2i)(z-1+2i) \end{aligned} \tag{25}$$

Zatem pierwiastkami powyższego wielomianu p są $z_1 = -1$, $z_2 = 1+2i$ oraz $z_3 = 1-2i$. Zauważmy, że $z_2 = z_3^*$. Ta własność zachodzi dla każdego wielomianu o rzeczywistych współczynnikach: jeżeli z jest jego pierwiastkiem, to z^* również i ich krotności są równe.
PRZYKŁAD: Rozważmy równanie wielomianowe na liczbach zespolonych $z^n = 1$. Podstawiając $z = re^{i\varphi}$ otrzymamy:

$$r^n e^{in\varphi} = 1 = 1e^{i\cdot 0} \implies r = 1 \wedge n\varphi = 0 + 2k\pi \implies \varphi = \frac{2k\pi}{n}, k = 0, \ldots, n-1$$

Np. dla $n = 5$ otrzymujemy rozwiązania: 1, $e^{i\frac{2\pi}{5}}$, $e^{i\frac{4\pi}{5}}$, $e^{i\frac{6\pi}{5}}$, $e^{i\frac{8\pi}{5}}$. Zauważmy, że na płaszczyźnie zespolonej rozwiązania te tworzą n-kąt foremny wpisany w okrąg jednostkowy.



3. Macierze

Macierzą nazywamy prostokątną tablicę z liczbami.
PRZYKŁAD:
$\left[\begin{array}{ccc} 4 & -3 & 1 \\ 3 & 0 & -2 \end{array}\right]$

Elementy macierzy nazywamy wyrazami. Mówimy, że macierz jest $m \times n$, jeżeli ma m wierszy i n kolumn. Zbiór macierzy $m \times n$, których wyrazy są elementami zbioru A, oznaczamy jako $A^{m\times n}$. Macierz nazywamy kwadratową, jeżeli ma tyle samo kolumn, co wierszy. Przekątną macierzy kwadratowej tworzą wyrazy biegnące od lewego górnego do prawego dolnego rogu. Macierz kwadratową nazywamy trójkątną górną (dolną), jeżeli wszystkie jej wyrazy leżące pod (nad) przekątną, są równe 0. Macierz kwadratową nazywamy diagonalną, jeżeli wszystkie jej wyrazy leżące poza przekątną są równe 0. Macierzą jednostkową I nazywamy macierz diagonalną, której wszystkie wyrazy na przekątnej równe są 1.
PRZYKŁAD:
macierz trójkątna górna: $\left[\begin{array}{ccc} -1 & 1 & 2 \\ 0 & 5 & -2 \\ 0 & 0 & 1 \end{array}\right]$, macierz trójkątna dolna: $\left[\begin{array}{ccc} 1 & 0 & 0 \\ 3 & 2 & 0 \\ 0 & 1 & 1 \end{array}\right]$, macierz diagonalna: $\left[\begin{array}{ccc} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 5 \end{array}\right]$,
macierz jednostkowa: $\left[\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right]$

Wektorem kolumnowym nazywamy macierz o jednej kolumnie. Wektorem wierszowym nazywamy macierz o jednym wierszu. Mówiąc po prostu wektor, mamy na myśli wektor kolumnowy.
Transpozycją macierzy A nazywamy macierz A^T, która jest jej odbiciem symetrycznym względem przekątnej.
PRZYKŁAD:
$A = \left[\begin{array}{ccc} 4 & -3 & 1 \\ 3 & 0 & -2 \end{array}\right]$, $A^T = \left[\begin{array}{cc} 4 & 3 \\ -3 & 0 \\ 1 & -2 \end{array}\right]$

Dla macierzy zdefiniowane są trzy podstawowe działania: dodawanie, mnożenie macierzy przez liczbę oraz mnożenie macierzy przez siebie. Aby można było dodać dwie macierze, muszą być one takich samych wymiarów. Suma dwóch macierzy to macierz o takich samych wymiarach, której poszczególne wyrazy stanowią sumę odpowiadających wyrazów macierzy, które dodajemy.
PRZYKŁAD:

$$\left[\begin{array}{cc} 1 & 2 \\ 3 & 4 \end{array}\right] + \left[\begin{array}{cc} 5 & 6 \\ 7 & 8 \end{array}\right] = \left[\begin{array}{cc} 6 & 8 \\ 10 & 12 \end{array}\right]$$

Tak zdefiniowane działanie jest łączne, przemienne, posiada element neutralny oraz każda macierz posiada element symetryczny, zatem zbiór macierzy rzeczywistych $m \times n$ z działaniem dodawania tworzy grupę abelową.
Iloczyn macierzy i liczby to macierz, której każdy wyraz jest iloczynem odpowiedniego wyrazu wyjściowej macierzy oraz tej liczby.
PRZYKŁAD:

$$5 \cdot \left[\begin{array}{cc} 1 & 2 \\ 3 & 4 \end{array}\right] = \left[\begin{array}{cc} 5 & 10 \\ 15 & 20 \end{array}\right]$$

Dla każdych dwóch macierzy A i B o takich samych wymiarach oraz liczb α i β, zachodzi:

$$\alpha(A + B) = \alpha A + \alpha B$$
$$(\alpha + \beta)A = \alpha A + \beta A$$
$$(\alpha\beta)A = \alpha(\beta A)$$

Nieco bardziej skomplikowaną operacją jest mnożenie macierzy przez siebie. Mnożenie macierzy można wykonać wyłącznie wtedy, gdy liczba kolumn macierzy z lewej strony mnożenia jest równa liczbie wierszy macierzy z prawej strony mnożenia. W wyniku otrzymujemy macierz, której liczba wierszy równa jest liczbie wierszy macierzy z lewej strony, a liczba kolumn - liczbie kolumn macierzy z prawej strony. Np. iloczynem macierzy $k \times m$ i $m \times n$ jest macierz $k \times n$. W i-tym wierszu i j-tej kolumnie macierzy, którą otrzymamy znajduje się suma iloczynów wyrazów z i-tego wiersza macierzy po lewej stronie przez odpowiadające im wyrazy z j-tej kolumny macierzy po prawej stronie.
PRZYKŁAD:

$$\left[\begin{array}{ccc} 2 & 3 & 2 \\ 1 & 2 & 4 \end{array}\right] \cdot \left[\begin{array}{ccc} 1 & 2 & 4 \\ 5 & 4 & 3 \\ 2 & 4 & 3 \end{array}\right] = \left[\begin{array}{ccc} 2\cdot1+3\cdot5+2\cdot2 & 2\cdot2+3\cdot4+2\cdot4 & 2\cdot4+3\cdot3+2\cdot3 \\ 1\cdot1+2\cdot5+4\cdot2 & 1\cdot2+2\cdot4+4\cdot4 & 1\cdot4+2\cdot3+4\cdot3 \end{array}\right] =$$
$$= \left[\begin{array}{ccc} 21 & 24 & 23 \\ 19 & 25 & 22 \end{array}\right]$$

Dla każdych macierzy A, B, C o odpowiednich wymiarach oraz liczby α zachodzi:

$$A(BC) = (AB)C$$
$$(A+B)C = AC + BC$$
$$A(B+C) = AB + AC$$
$$\alpha(AB) = (\alpha A)B = A(\alpha B)$$
$AI = IA = A$, gdzie I jest macierzą jednostkową
$$(AB)^T = B^T A^T$$

W ogólnym przypadku mnożenie macierzy nie jest przemienne:

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

Zbiory macierzy rzeczywistych $\mathbb{R}^{n\times n}$ oraz zespolonych $\mathbb{C}^{n\times n}$ o wymiarach $n \times n$ tworzą zatem pierścienie nieprzemienne z jedynką. Jedną z konsekwencji nieprzemienności mnożenia jest, że z faktu $B = C$, nie wynika $AB = CA$ (wynika natomiast, że $AB = AC$ oraz $BA = CA$). Wykonując działania na macierzach musimy zatem pilnować, który czynnik stoi po której stronie. Ponadto, w pierścieniu macierzy istnieją tzw. dzielniki zera (tj. iloczyn dwóch niezerowych macierzy może być równy 0).
Definicja: Wyznacznikiem macierzy nazywamy funkcję $\det$, która macierzy kwadratowej przyporządkowuje liczbę i ma następujące właściwości:
$i)$ $\det(I) = 1$
$ii)$ wyznacznikiem macierzy mającej dwie identyczne kolumny jest 0
$iii)$ wyznacznik jest liniową funkcją kolumn
Istnieje dokładnie jedna funkcja, spełniająca powyższą definicję, ale do pokazania tego potrzebujemy jeszcze jednej własności:
Lemat: Dla funkcji spełniającej definicję wyznacznika spełniony jest następujący warunek: zamiana miejscami dwóch kolumn zmienia wyznacznik na przeciwny.
Dowód: Rozważmy macierz $[A_1, \ldots, A_i, \ldots, A_j, \ldots, A_n]$, gdzie A_k są kolejnymi kolumnami. Zamieniając miejscami i-tą oraz j-tą kolumnę otrzymujemy macierz $[A_1, \ldots, A_j, \ldots, A_i, \ldots, A_n]$. Z $ii)$ wynika, że

$$\det\big([A_1, \ldots, A_i + A_j, \ldots, A_i + A_j, \ldots, A_n]\big) = 0 \tag{26}$$

Z $iii)$ wynika natomiast, że

$$\begin{aligned}\det\big([A_1, \ldots, A_i + A_j, \ldots, A_i + A_j, \ldots, A_n]\big) &= \det\big([A_1, \ldots, A_i, \ldots, A_i + A_j, \ldots, A_n]\big) + \\ &+ \det\big([A_1, \ldots, A_j, \ldots, A_i + A_j, \ldots, A_n]\big) = \det\big([A_1, \ldots, A_i, \ldots, A_i, \ldots, A_n]\big) + \\ &+ \det\big([A_1, \ldots, A_i, \ldots, A_j, \ldots, A_n]\big) + \det\big([A_1, \ldots, A_j, \ldots, A_i, \ldots, A_n]\big) + \\ &+ \det\big([A_1, \ldots, A_j, \ldots, A_j, \ldots, A_n]\big)\end{aligned} \tag{27}$$

Po ponownym zastosowaniu $ii)$ w celu usunięcia wyznaczników macierzy o dwóch identycznych kolumnach, na mocy (26) otrzymujemy

$$\det\big([A_1, \ldots, A_i, \ldots, A_j, \ldots, A_n]\big) = -\det\big([A_1, \ldots, A_j, \ldots, A_i, \ldots, A_n]\big) \tag{28}$$

co kończy dowód. □
Pokażemy teraz, że wyznacznik jest jednoznacznie wyznaczony na podstawie definicji. Pokażemy to na przykładzie macierzy 2×2, jednak łatwo wyobrazić sobie uogólnienie dowodu na macierze o dowolnym wymiarze. Rozważmy wyznacznik ogólnej postaci macierzy 2×2. Zachodzi:

$$\begin{aligned}\det\begin{bmatrix} a & b \\ c & d \end{bmatrix} &= \det\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} + \det\begin{bmatrix} 0 & b \\ c & d \end{bmatrix} = \det\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} + \det\begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} + \det\begin{bmatrix} 0 & b \\ c & 0 \end{bmatrix} + \\ &+ \det\begin{bmatrix} 0 & 0 \\ c & d \end{bmatrix} = ab \cdot \det\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} + ad \cdot \det\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + bc \cdot \det\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + \\ &+ cd \cdot \det\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} = ad - bc\end{aligned} \tag{29}$$

Pierwsze trzy przejścia wynikają z $iii)$, natomiast ostatnie z $i)$, $ii)$ oraz z lematu. Powtarzając powyższe rozumowanie dla macierzy $n \times n$ można zauważyć, że dla macierzy $A \in \mathbb{C}^{n\times n}$, której wyrazy to a_{ij} (i - numer wiersza, j - numer kolumny) otrzymujemy:

$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \ldots a_{n\sigma(n)} \tag{30}$$

gdzie S_n oznacza zbiór permutacji zbioru n-elementowego, natomiast sgn(σ) to tzw. znak permutacji, tj. $(-1)^k$, gdzie k jest liczbą zamian dwóch elementów, które musimy wykonać, aby sprowadzić permutację do identyczności.
PRZYKŁAD: $S_3 = \{(1,2,3),(1,3,2),(2,3,1),(2,1,3),(3,1,2),(3,2,1)\}$. Permutacja $\sigma_1 = (1,2,3)$ jest identycznością, zatem aby sprowadzić ją do identyczności musimy wykonać 0 zamian elementów, czyli sgn$(\sigma_1) = (-1)^0 = 1$. Permutację $\sigma_2 = (1,3,2)$ możemy sprowadzić do identyczności wykonując jedną zamianę (zamieniając miejscami drugi i trzeci element), zatem sgn$(\sigma_2) = (-1)^1 = -1$. Dla macierzy $A = [a_{ij}]\,, i, j \in \{1,2,3\}$ otrzymujemy:

$$\det(A) = a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} + a_{12}a_{23}a_{31} - a_{12}a_{21}a_{33} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} \tag{31}$$

PRZYKŁAD:

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

$$\det(A) = 2\cdot 3\cdot 0 - 2\cdot 1\cdot(-2) + (-1)\cdot 1\cdot 2 - (-1)\cdot 0\cdot 0 + 3\cdot 0\cdot(-2) - 3\cdot 3\cdot 2 = -16 \tag{32}$$

Dla dowolnych macierzy $A, B \in \mathbb{C}^{n\times n}$ oraz $\alpha \in \mathbb{C}$ zachodzi:

$$\det(A) = \det(A^T)$$
$$\det(\alpha A) = \alpha^n \det(A)$$
$$\det(AB) = \det(A)\cdot\det(B)$$

Zauważmy, że wyznacznik macierzy trójkątnej równy jest iloczynowi wyrazów z przekątnej (dla każdej permutacji σ z wyjątkiem identyczności, dla pewnego i wyraz $a_{i\sigma(i)}$ leży pod lub nad przekątną, zatem zawierający go składnik jest równy 0 i ostatecznie wzór (30) zredukuje się do jednego składnika odpowiadającego identyczności). Ponadto dodanie do dowolnej kolumny macierzy A innej kolumny tej samej macierzy pomnożonej przez liczbę, nie zmienia jej wyznacznika:

$$\begin{aligned}\det\big([A_1,\ldots,A_i,\ldots,A_j,\ldots,A_n]\big) = \det\big([A_1,\ldots,A_i,\ldots,A_j,\ldots,A_n]\big) + \\ + \alpha\det\big([A_1,\ldots,A_i,\ldots,A_i,\ldots,A_n]\big) = \det\big([A_1,\ldots,A_i,\ldots,A_j+\alpha A_i,\ldots,A_n]\big)\end{aligned} \tag{33}$$

Skoro transpozycja nie zmienia wyznacznika, to powyższa własność (podobnie jak ii) oraz iii) z definicji wyznacznika) zachodzi również dla wierszy.
Zauważmy, że liczba operacji, które musimy wykonać, aby obliczyć wyznacznik ze wzoru (30) jest większa niż $n!$. W praktycznych sytuacjach wyznacznik liczy się zatem innymi metodami: metodą rozwinięć Laplace'a lub metodą eliminacji Gaussa.
Metoda rozwinięć Laplace'a: Minorem M_{ij} macierzy A nazywamy wyznacznik macierzy otrzymanej z macierzy A poprzez usunięcie jej i-tego wiersza oraz j-tej kolumny.
PRZYKŁAD:
Dla $A = \begin{bmatrix} 2 & -1 & 3 \\ 0 & 3 & 1 \\ 2 & -2 & 0 \end{bmatrix}$: $M_{12} = \det\begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix} = -2$, $M_{33} = \det\begin{bmatrix} 2 & -1 \\ 0 & 3 \end{bmatrix} = 6$
Twierdzenie: Niech $A \in \mathbb{C}^{n\times n}$ oraz $k \in \{1,\ldots,n\}$. Wtedy $\det(A) = \sum_{i=1}^n (-1)^{i+k} a_{ik} M_{ik} = \sum_{j=1}^n (-1)^{k+j} a_{kj} M_{kj}$, gdzie M_{ij} są minorami macierzy A.
PRZYKŁAD:
Rozważmy znów macierz $A = \begin{bmatrix} 2 & -1 & 3 \\ 0 & 3 & 1 \\ 2 & -2 & 0 \end{bmatrix}$. Możemy wybrać dowolny wiersz lub kolumnę, względem której będziemy rozwijać macierz. Wybierzmy pierwszą kolumnę. Wtedy wyznacznik liczymy z pierwszego wzoru dla $k = 1$:

$$\det(A) = (-1)^{1+1}\cdot 2\cdot\begin{vmatrix} 3 & 1 \\ -2 & 0 \end{vmatrix} + (-1)^{2+1}\cdot 0\cdot\begin{vmatrix} -1 & 3 \\ -2 & 0 \end{vmatrix} + (-1)^{3+1}\cdot 2\cdot\begin{vmatrix} -1 & 3 \\ 3 & 1 \end{vmatrix} = 4 - 20 = -16 \tag{34}$$

Wybierając drugi wiersz, z drugiego wzoru dla $k = 2$ otrzymamy:

$$\det(A) = (-1)^{2+1}\cdot 0\cdot\begin{vmatrix} -1 & 3 \\ -2 & 0 \end{vmatrix} + (-1)^{2+2}\cdot 3\cdot\begin{vmatrix} 2 & 3 \\ 2 & 0 \end{vmatrix} + (-1)^{2+3}\cdot 1\cdot\begin{vmatrix} 2 & -1 \\ 2 & -2 \end{vmatrix} = -18 + 2 = -16 \tag{35}$$

Metoda eliminacji Gaussa: Skoro dodanie do dowolnego wiersza macierzy innego wiersza pomnożonego przez stałą (lub wykonanie analogicznej operacji na kolumnach) nie zmienia wyznacznika, to możemy przeprowadzać te operacje aż do sprowadzenia macierzy do postaci trójkątnej, dla której policzenie wyznacznika jest trywialne.
PRZYKŁAD:
Rozważmy $A = \begin{bmatrix} 2 & -1 & 3 \\ 0 & 3 & 1 \\ 2 & -2 & 0 \end{bmatrix}$. Odejmijmy od trzeciego wiersza pierwszy: $\begin{bmatrix} 2 & -1 & 3 \\ 0 & 3 & 1 \\ 0 & -1 & -3 \end{bmatrix}$, a następnie dodajmy do trzeciego wiersza drugi pomnożony przez $\frac{1}{3}$: $\begin{bmatrix} 2 & -1 & 3 \\ 0 & 3 & 1 \\ 0 & 0 & -2\frac{2}{3} \end{bmatrix}$. Wyznacznik ostatniej macierzy to $2\cdot 3\cdot(-2\frac{2}{3}) = -16$.

Definicja: Macierz kwadratową nazywamy odwracalną (ang. *invertible*) lub nieosobliwą (ang. *nonsingular*), jeżeli istnieje macierz A^{-1}, taka że $AA^{-1} = A^{-1}A = I$, gdzie I jest macierzą nieosobliwą. Wtedy A^{-1} nazywamy macierzą odwrotną do A.
Jeżeli macierz jest nieosobliwa, to istnieje dokładnie jedna macierz będąca jej odwrotnością. Dla dowolnych nieosobliwych macierzy $A, B \in \mathbb{C}^{n\times n}$ zachodzi:

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

Twierdzenie: Macierz jest nieosobliwa wtedy i tylko wtedy, gdy jej wyznacznik jest różny od 0.
Do dowodu powyższego twierdzenia potrzebna nam będzie macierz dołączona do macierzy A, tj. $A^D = \left[(-1)^{i+j}M_{ij}\right]^T$, gdzie M_{ij} są minorami macierzy A. Zachodzi: $AA^D = A^DA = \det(A)\cdot I$.
Dowód twierdzenia: /$\Longrightarrow$/ Załóżmy, że macierz A jest nieosobliwa; chcemy pokazać, że jej wyznacznik jest różny od 0. Skoro A jest nieosobliwa, to posiada odwrotność A^{-1}, taką że $AA^{-1} = I$. Wtedy:

$$1 = \det(I) = \det(AA^{-1}) = \det(A)\cdot\det(A^{-1}) \tag{36}$$

Zatem $\det(A) \neq 0$.
/$\Longleftarrow$/ Załóżmy, że wyznacznik macierzy A jest różny od zera; chcemy pokazać, że macierz A posiada odwrotność. Przyjmując $A' = \frac{1}{\det(A)}A^D$, otrzymamy $AA' = A'A = I$, zatem A' jest odwrotnością A. □

PRZYKŁAD:

Rozważmy macierz

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

$\det(A) = -16$, zatem macierz odwrotna do A istnieje. Zgodnie z konstrukcją macierzy odwrotnej przedstawioną w dowodzie twierdzenia:

$$A^{-1} = \frac{1}{\det(A)}\begin{bmatrix} M_{11} & -M_{21} & M_{31} \\ -M_{12} & M_{22} & -M_{32} \\ M_{13} & -M_{23} & M_{33} \end{bmatrix} = \frac{1}{-16}\begin{bmatrix} 2 & -6 & -10 \\ 2 & -6 & -2 \\ -6 & 2 & 6 \end{bmatrix} \tag{37}$$

Powyższa metoda liczenia macierzy odwrotnej, podobnie jak metoda Laplace'a liczenia wyznacznika, ma dużą złożoność obliczeniową. Istnieje jednak szybsza metoda, analogiczna do metody eliminacji Gaussa dla wyznaczników.
Metoda eliminacji Gaussa odwracania macierzy: Zapiszmy obok siebie macierz, którą chcemy odwrócić oraz macierz jednostkową. Wykonujemy równocześnie na obu macierzach te same operacje: dodawania do danego wiersza innego wiersza pomnożonego przez stałą, mnożenia wiersza przez stałą oraz zamiany dwóch wierszy (możemy również wykonywać analogiczne operacje na kolumnach, nie możemy jednak mieszać operacji na wierszach i kolumnach). W momencie, gdy wyjściowa macierz zostanie sprowadzona do macierzy jednostkowej, druga macierz będzie szukaną odwrotnością.

PRZYKŁAD:

Szukamy odwrotności macierzy

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

Zapiszmy tę macierz oraz macierz jednostkową:

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

Pomnóżmy drugi wiersz przez $\frac{1}{3}$, a od trzeciego odejmijmy pierwszy:

$$\begin{bmatrix} 2 & -1 & 3 \\ 0 & 1 & \frac{1}{3} \\ 0 & -1 & -3 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{3} & 0 \\ -1 & 0 & 1 \end{bmatrix}$$

Dodajmy do trzeciego drugi, a następnie pomnóżmy go przez $\frac{-3}{8}$:

$$\begin{bmatrix} 2 & -1 & 3 \\ 0 & 1 & \frac{1}{3} \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{3} & 0 \\ \frac{3}{8} & -\frac{1}{8} & -\frac{3}{8} \end{bmatrix}$$

Odejmijmy od drugiego trzeci pomnożony przez $\frac{1}{3}$, a następnie dodajmy do pierwszego drugi:

$$\begin{bmatrix} 2 & 0 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} \frac{7}{8} & \frac{3}{8} & \frac{3}{8} \\ -\frac{1}{8} & \frac{3}{8} & \frac{1}{8} \\ \frac{3}{8} & -\frac{1}{8} & -\frac{3}{8} \end{bmatrix}$$

Odejmijmy od pierwszego trzeci pomnożony przez 3, a następnie pomnóżmy go przez $\frac{1}{2}$.

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} -\frac{1}{8} & \frac{3}{8} & \frac{5}{8} \\ -\frac{1}{8} & \frac{3}{8} & \frac{1}{8} \\ \frac{3}{8} & -\frac{1}{8} & -\frac{3}{8} \end{bmatrix}$$

Macierz po prawej stronie to szukana odwrotność.
Dowód poprawności metody: Wykonanie każdej operacji jest równoważne z pomnożeniem macierzy przez pewną macierz z lewej (w przypadku operacji na wierszach) lub prawej (w przypadku operacji na kolumnach) strony. Na przykład, pomnożenie drugiego wiersza przez α jest równoważne pomnożeniu macierzy z lewej strony przez macierz

$$\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & \alpha & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

natomiast dodanie do pierwszego wiersza drugiego pomnożonego przez β:

$$\begin{bmatrix} 1 & \beta & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

Zaczynamy od macierzy A oraz I. Po wykonaniu pierwszej operacji na wierszach, zadanej przez macierz P_1, otrzymujemy P_1A oraz P_1. Po drugiej operacji otrzymujemy P_2P_1A oraz P_2P_1. Ostatecznie, po k operacjach otrzymujemy $P_k \dots P_1A$ oraz $P_k \dots P_1$. Jeżeli pierwsza z tych macierzy jest macierzą jednostkową, to $P_k \dots P_1 = A^{-1}$, czyli druga macierz jest szukaną odwrotnością macierzy A. Jeżeli wykonujemy operacje na kolumnach, to sytuacja jest analogiczna, ale otrzymujemy $AQ_1 \dots Q_k$ oraz $Q_1 \dots Q_k$. Zauważmy, że szukając odwrotności tą metodą, nie możemy mieszać ze sobą operacji na wierszach i kolumnach. W takim przypadku otrzymalibyśmy macierze postaci $PAQ = I$ i PQ, zatem druga z nich nie musi być odwrotnością A. □

Na koniec tego rozdziału zauważmy jeszcze, że pomimo, iż na wstępie zdefiniowaliśmy macierz jako tablicę z liczbami, to nic nie stoi na przeszkodzie, aby rozważać macierze, których wyrazami są elementy dowolnego zbioru. Aby na tak zdefiniowanych macierzach móc wprowadzić działania dodawania i mnożenia, wymagamy, aby działania te były zdefiniowane na wyrazach macierzy. Tak będzie np. w przypadku, gdy wyrazy macierzy będą elementami pewnego pierścienia. Aby działania na takich macierzach miały własności zbliżone do działań na macierzach rzeczywistych lub zespolonych, załóżmy, że pierścień ten jest pierścieniem przemiennym z jedynką (np. rozważamy macierze, których wyrazami są funkcje rzeczywiste). Dla takich macierzy zachodzą bez zmian prawie wszystkie przedstawione w tym rozdziale własności; jedynym wyjątkiem jest twierdzenie o odwracalności, które w takim przypadku przyjmuje postać: macierz jest odwracalna wtedy i tylko wtedy, gdy jej wyznacznik jest odwracalny.

PRZYKŁAD:

Rozważmy macierz kwadratową, której wyrazy są liczbami całkowitymi. Chcemy stwierdzić, kiedy macierz ta posiada odwrotność, której wyrazy również są liczbami całkowitymi. Zauważmy, że liczby całkowite tworzą pierścień przemienny z jedynką, zatem możemy ograniczyć się do macierzy nad tym pierścieniem i wyjściowy problem sprowadzić do problemu istnienia odwrotności (nad tym pierścieniem). Zgodnie z przytoczoną wyżej własnością, macierz nad pierścieniem jest odwracalna, jeżeli jej wyznacznik jest odwracalny (w tym pierścieniu). W pierścieniu liczb całkowitych odwracalne są tylko liczby 1 i -1, zatem wyjściowa macierz jest posiada odwrotność o całkowitych wyrazach wtedy i tylko wtedy, gdy jej wyznacznik jest równy ± 1.

4. Przestrzenie wektorowe

Definicja: Działaniem zewnętrznym na zbiorze X nad zbiorem Y nazywamy funkcję $Y \times X \to X$.

PRZYKŁAD:

- mnożenie wektorów przez liczby,
- podnoszenie macierzy kwadratowych do potęg naturalnych dodatnich: $\mathbb{N}_* \times \mathbb{R}^{n \times n} \ni (k, A) \mapsto A^k \in \mathbb{R}^{n \times n}$.

Definicja: Przestrzenią wektorową (liniową) nad ciałem F nazywamy zbiór U z działaniem wewnętrznym $+$ oraz działaniem zewnętrznym $\cdot$ nad F, takimi że $(U, +)$ jest grupą abelową oraz $\forall u, v \in U, \alpha, \beta \in F$ zachodzi:

$$(\alpha + \beta) \cdot u = \alpha \cdot u + \beta \cdot u$$
$$\alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v$$
$$(\alpha\beta) \cdot u = \alpha \cdot (\beta \cdot u)$$
$$1 \cdot u = u$$

Elementy przestrzeni nazywamy wektorami, natomiast elementy ciała, nad którym ta przestrzeń jest zdefiniowana - skalarami.

Uwaga: Rozważając przestrzenie wektorowe mamy do czynienia z dwoma działaniami dodawania: dodawaniem skalarów oraz dodawaniem wektorów. Oba działania oznaczamy tym samym symbolem $+$, jednak zawsze z kontekstu jesteśmy w stanie stwierdzić, które dodawanie występuje w którym miejscu, np. w pierwszym równaniu powyższej definicji, $+$ w wyrażeniu $\alpha+\beta$ oznacza dodawanie skalarów, natomiast w wyrażeniu $\alpha\cdot u+\beta\cdot u$ - dodawanie wektorów. Analogicznie dla mnożenia: zdefiniowane są działania mnożenia skalarów przez siebie oraz mnożenia skalarów przez wektory. Podobnie jak dla mnożenia elementów ciała, znak $\cdot$ na ogół bedziemy pomijać. Przestrzeń wektorowa jest grupą, zatem posiada element neutralny (dla dodawania); będziemy nazywać go i oznaczać zerem. W kontekście przestrzeni wektorowej pojawiają się zatem dwa zera: zero skalarne (element neutralny dla dodawania w ciele) oraz wektorowe (element neutralny dla dodawania w przestrzeni).

PRZYKŁAD:

- dla ciała F, zbiór $F^n=\{(a_1,\ldots,a_n),a_i\in F\}$, z działaniami: $(a_1,\ldots,a_n)+(b_1,\ldots,b_n)=(a_1+b_1,\ldots,a_n+b_n)$ oraz $c\cdot(a_1,\ldots,a_n)=(ca_1,\ldots,ca_n)$, jest przestrzenią wektorową nad F,
- zbiór funkcji rzeczywistych ze standardowymi działaniami dodawania i mnożenia przez liczby rzeczywiste jest przestrzenią wektorową nad $\mathbb{R}$,
- zbiór wielomianów rzeczywistych stopnia co najwyżej drugiego ze standardowymi działaniami dodawania i mnożenia przez liczby rzeczywiste jest przestrzenią wektorową nad $\mathbb{R}$,
- zbiór liczb zespolonych z działaniami dodawania i mnożenia przez liczby rzeczywiste jest przestrzenią wektorową nad $\mathbb{R}$,
- zbiór liczb zespolonych z działaniami dodawania i mnożenia przez liczby zespolone jest przestrzenią wektorową nad $\mathbb{C}$,
- zbiór macierzy zespolonych z działaniami dodawania oraz mnożenia przez liczby rzeczywiste jest przestrzenią wektorową nad $\mathbb{R}$,
- zbiór macierzy zespolonych z działaniami dodawania oraz mnożenia przez liczby zespolone jest przestrzenią wektorową nad $\mathbb{C}$.

Elementy przestrzeni F^n będziemy zapisywać również jako wektory kolumnowe, tj. $\begin{bmatrix} a_1 & a_2 & \ldots & a_n \end{bmatrix}^T$.

Definicja: Liniową kombinacją wektorów $u_1,\ldots,u_k\in U$ nazywamy wyrażenie postaci $\sum_{i=1}^k\alpha_iu_i$, gdzie α_i są skalarami. Skalary te nazywamy współczynnikami liniowej kombinacji.

Definicja: Wektory $u_1,\ldots,u_k$ są liniowo niezależne, gdy z faktu $\sum_{i=1}^k\alpha_iu_i=0$ wynika, że $\forall i:\alpha_i=0$.

Innymi słowy, wektory są liniowo niezależne, gdy jedyną ich liniową kombinacją równą zero jest kombinacja o zerowych współczynnikach.

PRZYKŁAD: Rozważmy wektory $u_1=(1,0,0)$, $u_2=(0,1,0)$ oraz $u_3=(0,0,1)$. Przyrównajmy ich liniową kombinację do zera: $\sum_{i=1}^3\alpha_iu_i=0$. Podstawiając za u_i odpowiednie wektory otrzymamy: $(\alpha_1,\alpha_2,\alpha_3)=(0,0,0)$, zatem $\alpha_1=\alpha_2=\alpha_3=0$, czyli wektory są liniowo niezależne.

PRZYKŁAD: Rozważmy wektory $u_1=(1,0,1)$, $u_2=(0,1,0)$ oraz $u_3=(2,0,2)$. Przyrównajmy ich liniową kombinację do zera: $\sum_{i=1}^3\alpha_iu_i=0$. Podstawiając za u_i odpowiednie wektory otrzymamy: $(\alpha_1+2\alpha_3,\alpha_2,\alpha_1+2\alpha_3)=(0,0,0)$, co jest spełnione np. dla $\alpha_1=-2,\alpha_2=0,\alpha_3=1$. Istnieje zatem liniowa kombinacja równa zero, której nie wszystkie współczynniki są równe 0, czyli wektory są liniowo zależne.

Lemat: Wektory są liniowo zależne wtedy i tylko wtedy, gdy któryś z nich można przedstawić jako liniową kombinację pozostałych.

Dowód: /$\Longrightarrow$/ Wybierzmy liniowo zależne wektory $u_1,\ldots,u_k$. Pokażemy, że któryś z nich można przedstawić jako liniową kombinację pozostałych. Skoro wektory są liniowo zależne, to istnieją skalary α_i, nie wszystkie równe 0, takie że $\sum_{i=1}^k\alpha_iu_i=0$. Niech j będzie indeksem, dla którego $\alpha_j\neq0$. Wtedy $\alpha_ju_j=\sum_{i=1,i\neq j}^k-\alpha_iu_i$. Skalary α_i należą do ciała, zatem skoro $\alpha_j\neq0$, to α_j posiada odwrotność α_j^{-1} i w konsekwencji $u_j=\sum_{i=1,i\neq j}^k-\alpha_i\alpha_j^{-1}u_i$, co jest szukanym przedstawieniem u_j jako liniowej kombinacji pozostałych wektorów.

/$\Longleftarrow$/ Wybierzmy wektory $u_1,\ldots,u_k$, takie że któryś z nich da się przedstawić jako liniową kombinację pozostałych. Pokażemy, że wektory są liniowo zależne. Załóżmy, że u_j da się przedstawić jako kombinację pozostałych. Wtedy $u_j=\sum_{i=1,i\neq j}^k\alpha_iu_i$. Oznaczając $\alpha_j=-1$, otrzymujemy $\sum_{i=1}^k\alpha_iu_i=0$. $\alpha_j\neq0$, zatem otrzymaliśmy liniową kombinację, której nie wszystkie współczynniki są równe 0, czyli wektory są liniowo zależne. $\square$

Definicja: Wektory $u_1,\ldots,u_k\in U$ generują przestrzeń U, jeżeli każdy wektor z przestrzeni U możemy przedstawić jako liniową kombinację tych wektorów.

PRZYKŁAD: Rozważmy wektory $u_1=(1,0,0)$, $u_2=(0,1,0)$ oraz $u_3=(0,0,1)$ z przestrzeni F^3. Wybierzmy dowolny wektor z $v\in F^3$ i zapiszmy go jako (a,b,c). Zachodzi $v=au_1+bu_2+cu_3$, zatem v da się przedstawić jako liniową kombinację wektorów u_i. Wektor v wybraliśmy dowolnie, zatem każdy wektor da się przedstawić jako liniową kombinację wektorów u_i, czyli wektory te generują przestrzeń F^3.

PRZYKŁAD: Rozważmy wektory $u_1=(1,0,1)$, $u_2=(0,1,0)$ oraz $u_3=(1,1,1)$ z przestrzeni F^3. Ich liniowa kombinacja ma postać: $(\alpha_1+\alpha_3,\alpha_2+\alpha_3,\alpha_1+\alpha_3)$, zatem nie możemy otrzymać w ten sposób np. wektora $(1,0,0)$, czyli wektory te nie generują przestrzeni F^3.

Definicja: Bazą przestrzeni U nazywamy układ wektorów tej przestrzeni, które są liniowo niezależne oraz generują tę przestrzeń.

PRZYKŁAD: Układ wektorów $(1,0,0),(0,1,0),(0,0,1)$ stanowi bazę przestrzeni F^3; bazę takiej postaci nazywamy bazą kanoniczną. Inną bazę tej przestrzeni stanowi układ $(1,0,0),(1,1,0),(1,1,1)$. Układ wektorów $(1,0,0),(0,1,0)$ nie jest bazą tej przestrzeni (wektory są liniowo niezależne, ale nie generują przestrzeni); podobnie układ $(1,0,0),(0,1,0),(0,0,1),(1,1,1)$ (wektory generują przestrzeń, ale są liniowo zależne).

PRZYKŁAD: Rozważmy przestrzeń Π_3 wielomianów stopnia co najwyżej trzeciego. Bazą (kanoniczną) tej przestrzeni jest układ wielomianów: $x^3,x^2,x,1$.

Lemat: Jeżeli w przestrzeni istnieje układ złożony z n wektorów generujących, to każdy układ $(n+1)$ wektorów tej przestrzeni jest liniowo zależny.
Dowód: Niech wektory $u_1, \ldots, u_n$ stanowią układ generujący przestrzeni oraz dane są wektory $v_1, \ldots, v_{n+1}$. Chcemy pokazać, że wektory v_i są liniowo zależne. Rozważmy zatem liniową kombinację wektorów v_i równą 0:

$$\sum_{i=1}^{n+1} \alpha_i v_i = 0 \tag{38}$$

Pokażemy, że istnieją skalary α_i, nie wszystkie równe 0, dla których powyższa równość jest spełniona. Wektory u_j generują przestrzeń, zatem każdy z wektorów v_i można przedstawić jako ich liniową kombinację. Niech zatem:

$$v_i = \sum_{j=1}^{n} \beta_{ij} u_j \tag{39}$$

Wstawiając powyższe do równania (38) otrzymujemy:

$$\sum_{i=1}^{n+1} \alpha_i \sum_{j=1}^{n} \beta_{ij} u_j = 0 \tag{40}$$

W powyższej sumie możemy zmienić kolejność sumowania:

$$\sum_{j=1}^{n} \Big(\sum_{i=1}^{n+1} \beta_{ij} \alpha_i \Big) u_j = 0 \tag{41}$$

Warunkiem wystarczającym, aby ta zależność była spełniona jest, by dla każdego j zachodziło:

$$\sum_{i=1}^{n+1} \beta_{ij} \alpha_i = 0 \tag{42}$$

co stanowi układ n równań liniowych z $(n+1)$ niewiadomymi α_i. Jeżeli wszystkie współczynniki β_{1j} są równe 0, to $\alpha_1 = 1$, $\alpha_i = 0$ dla $i = 2, \ldots, n+1$ jest szukanym niezerowym zestawem skalarów. Jeżeli natomiast dla pewnego j zachodzi: $\beta_{1j} \neq 0$, to z j-tego równania układu zmienną α_1 możemy uzależnić od pozostałych niewiadomych, a następnie wstawić do pozostałych równań redukując w ten sposób liczbę równań i niewiadomych o jeden. Kontynuując tę procedurę dochodzimy albo do sytuacji opisanej powyżej albo do jednego równania z dwoma niewiadomymi postaci: $\gamma_n \alpha_n + \gamma_{n+1} \alpha_{n+1} = 0$, które ma więcej niż jedno rozwiązanie, w szczególności zatem ma rozwiązanie niezerowe. Ostatecznie zatem istnieją skalary α_i, nie wszystkie równe 0, takie że spełnione jest równanie (38), zatem wektory v_i są liniowo zależne. □

Twierdzenie: Jeżeli przestrzeń posiada bazę złożoną z $n \in \mathbb{N}$ wektorów, to wszystkie bazy tej przestrzeni mają n wektorów.
Dowód: Załóżmy, że przestrzeń posiada bazę $\mathcal{B}_1$ złożoną z n wektorów oraz bazę $\mathcal{B}_2$ złożoną z $m \neq n$ wektorów. Bez straty ogólności możemy założyć, że $m > n$. Wybierzmy dowolnych $n+1$ wektorów z bazy $\mathcal{B}_2$. Te wektory są liniowo niezależne, ponieważ należą do bazy. Stanowi to jednak sprzeczność z lematem, ponieważ w przestrzeni tej istnieje układ n wektorów generujących, którym jest baza $\mathcal{B}_1$. □

Definicja: Wymiarem przestrzeni wektorowej nazywamy liczbę elementów jej bazy.
Na mocy powyższego twierdzenia wymiar przestrzeni jest dobrze określony, ponieważ każda baza tej samej przestrzeni ma tyle samo elementów.
PRZYKŁAD:

- dla ciała F, przestrzeń F^n posiada bazę kanoniczną $(1, 0, \ldots, 0), (0, 1, \ldots, 0), \ldots, (0, 0, \ldots, 1)$, zatem jej wymiar nad ciałem F jest równy n,
- $\dim \Pi_n = n + 1$ (przestrzeń wielomianów stopnia co najwyżej n-tego),
- bazę przestrzeni $\mathbb{C}$ nad ciałem $\mathbb{R}$ stanowi para wektorów 1 oraz i, zatem wymiar $\mathbb{C}$ nad $\mathbb{R}$ jest równy 2,
- bazę przestrzeni $\mathbb{C}$ nad ciałem $\mathbb{C}$ stanowi jeden wektorów 1, zatem wymiar $\mathbb{C}$ nad $\mathbb{C}$ jest równy 1.

Własności baz:
$i)$ Każda przestrzeń posiada bazę.
$ii)$ W przestrzeni n-wymiarowej każdy układ n wektorów liniowo niezależnych stanowi bazę.
$iii)$ W przestrzeni n-wymiarowej każdy układ n wektorów generujących stanowi bazę.
$iv)$ W przestrzeni n-wymiarowej każdy układ wektorów liniowo niezależnych można uzupełnić do bazy.
$v)$ W przestrzeni n-wymiarowej każdy układ wektorów generujących można zawęzić do bazy.
Dowód własności $i)$ pomijamy, ponieważ wymaga on zastosowania lematu Kuratowskiego-Zorna, co wykracza poza zakres tego przedmiotu, natomiast dowody własności $ii) - v)$ pozostawiamy jako ćwiczenie.
PRZYKŁAD: Żeby stwierdzić, czy wektory $(1, 0, -1), (2, -1, 3), (0, 0, -2)$ stanowią bazę przestrzeni $\mathbb{R}^3$, wystarczy zbadać ich liniową niezależność lub rozstrzygnąć, czy generują przestrzeń; na mocy $ii)$ lub $iii)$ nie trzeba sprawdzać obu tych własności.
Lemat: Niech U będzie pewną przestrzenią, a $b_1, \ldots, b_n$ - jej bazą. Wtedy dla każdego $u \in U$ istnieje dokładnie jeden zestaw skalarów $\alpha_1, \ldots, \alpha_n$, taki że $u = \sum_{i=1}^{n} \alpha_i b_i$. Skalary te nazywamy współrzędnymi wektora u w bazie b_i.

Dowód lematu pozostawiamy jako ćwiczenie. W przyszłości wykorzystywać będziemy wektor współrzędnych danego wektora w danej bazie, tj. wektor $(\alpha_1, \ldots, \alpha_n)$.
Definicja: Niech $\bullet$ będzie działaniem wewnętrznym na zbiorze X, a Y - podzbiorem X. Działaniem indukowanym na Y nazywamy działanie $Y \times Y \ni (y_1, y_2) \mapsto y_1 \bullet y_2 \in Y$.
Działanie indukowane przyjmuje zatem dokładnie te same wartości, co wyjściowe działanie, ale określone jest na podzbiorze zbioru, na którym określone było wyjściowe działanie. Zauważmy, że aby działanie indukowane było dobrze określone, musi zachodzić $\forall y_1, y_2 \in Y : y_1 \bullet y_2 \in Y$. W takim przypadku mówimy, że ten zbiór jest zamknięty ze względu na to działanie.
PRZYKŁAD: Rozważmy zbiór liczb rzeczywistych. Możemy indukować działanie dodawania na jego podzbiory $\{0\}, \mathbb{N}, \mathbb{Q}$ otrzymując poprawnie określone działania wewnętrzne na tych zbiorach. Nie możemy natomiast indukować dodawania na zbiorze $\{0, 1\}$, ponieważ suma dwóch elementów tego zbioru nie musi należeć do tego zbioru (zbiór ten nie jest zamknięty ze względu na dodawanie).
W związku z tym, że działanie oryginalne i indukowane przyjmują te same wartości dla danych argumentów, nie musimy ich rozróżniać, będziemy zatem oznaczać je tym samym symbolem.
Definicja: Niech $\bullet$ będzie działaniem zewnętrznym na zbiorze X nad zbiorem Z, a Y - podzbiorem X. Działaniem indukowanym na Y nazywamy działanie $Z \times Y \ni (z, y) \mapsto z \bullet y \in Y$.
Dla działania zewnętrznego zachodzi analogiczna własność: aby działanie indukowane było dobrze określone, musi zachodzić $\forall z \in Z, y \in Y : z \bullet y \in Y$.
Definicja: Niech U będzie przestrzenią wektorową nad ciałem F. Podprzestrzenią przestrzeni U nazywamy jej podzbiór V, który wraz z działaniami indukowanymi sam jest przestrzenią wektorową.
Uwaga: Wprowadzenie działania indukowanego na V jest zabiegiem czysto formalnym, jednak musimy go wykonać, aby ze zbioru V móc uczynić przestrzeń wektorową. Nie możemy bowiem wyposażyć V bezpośrednio w oryginalne działania na U, ponieważ nie są one działaniami na V, czego wymaga definicja przestrzeni.
PRZYKŁAD:
Rozważmy przestrzeń $\mathbb{R}^2$ oraz jej podzbiór $V = \{(x_1, x_2) \in \mathbb{R}^2 : x_2 = 3x_1\}$. Pokażmy najpierw, że działania indukowane na V są dobrze określone. Weźmy $(x_1, x_2), (y_1, y_2) \in V$; chcemy pokazać, że $(x_1, x_2) + (y_1, y_2) \in V$. Zachodzi: $x_2 = 3x_1$ oraz $y_2 = 3y_1$, zatem $x_2 + y_2 = 3(x_1 + y_1)$, czyli $(x_1 + y_1, x_2 + y_2) \in V$. Weźmy teraz $(x_1, x_2) \in V$ oraz $\alpha \in \mathbb{R}$; chcemy pokazać, że $\alpha \cdot (x_1, x_2) \in V$. Znów $x_2 = 3x_1$, zatem $\alpha x_2 = 3\alpha x_1$, czyli $(\alpha x_1, \alpha x_2) \in V$. Sprawdźmy teraz, czy V z działaniami indukowanymi spełnia definicję przestrzeni. Zauważmy, że łączność i przemienność indukowanego dodawania wynikają wprost z łączności i przemienności dodawania na wyjściowej przestrzeni; podobnie wszystkie własności mnożenia przez skalar. Pozostaje nam zatem sprawdzić, czy istnieje element neutralny oraz elementy symetryczne dla dodawania. Obie te własności są spełnione, bowiem $(0, 0) \in V$ oraz dla $(x_1, x_2) = (x_1, 3x_1) \in V$ zachodzi $(-x_1, -x_2) = (-x_1, -3x_1) \in V$, gdzie $(x_1, x_2) + (-x_1, -x_2) = (0, 0)$.
Twierdzenie: Niech U będzie przestrzenią wektorową nad ciałem F. $V \subset U$ jest jej podprzestrzenią wtedy i tylko wtedy, gdy zbiór V jest niepusty oraz jest zamknięty ze względu na dodawanie oraz mnożenie przez skalar.
Dowód: /$\Longrightarrow$/ Skoro V jest podprzestrzenią, to działania indukowane są dobrze określone, zatem V jest zamknięty ze względu oba działania. Ponadto, V z indukowanym dodawaniem jest grupą abelową, zatem posiada element neutralny, czyli jest niepusty.
/$\Longleftarrow$/ Podobnie jak w powyższym przykładzie, łączność i przemienność indukowanego dodawania oraz własności indukowanego mnożenia wynikają ze spełnienia tych własności przez działania na U. Wybierzmy teraz pewien element $v \in V$ (jesteśmy w stanie wybrać taki element, ponieważ V jest niepusty). Z zamkniętości ze względu na mnożenie wynika, że $0 \cdot v = 0 \in V$, czyli V posiada element neutralny dla dodawania. Ponadto, również z zamkniętości dla mnożenia, $(-1) \cdot v = -v \in V$, czyli V posiada element przeciwny do v. $\square$
Uwaga: W powyższym dowodzie wykorzystaliśmy dwie własności: $0 \cdot v = 0$ oraz $(-1) \cdot v = -v$. Ich dowód pozostawiamy jako ćwiczenie.

5. Odwzorowania liniowe I

Niech X i Y będą przestrzeniami wektorowymi nad ciałem K.
Definicja: Odwzorowaniem liniowym (homomorfizmem przestrzeni liniowych) nazywamy funkcję $F : X \to Y$, taką że: $\forall x_1, x_2 \in X, \alpha \in K$ zachodzi:

$$F(x_1 + x_2) = F(x_1) + F(x_2)$$
$$F(\alpha x_1) = \alpha F(x_1)$$

Lemat: Niech K będzie ciałem, a F - odwzorowaniem liniowym $K^m \to K^n$. Istnieje dokładnie jedna macierz $A \in K^{n \times m}$, taka że $\forall x \in K^m : F(x) = Ax$.
Dowód: Niech $x = (x_1, \ldots, x_m)$. Oznaczmy przez e_i wektory bazy kanonicznej na K^m. Wtedy $x = \sum_{i=1}^m x_i e_i$, zatem $F(x) = F(\sum_{i=1}^m x_i e_i) = \sum_{i=1}^m x_i F(e_i)$. Dla macierzy $A = \begin{bmatrix} F(e_1) & \ldots & F(e_m) \end{bmatrix}$ otrzymujemy więc $F(x) = Ax$, czyli A jest szukaną macierzą. Załóżmy teraz, że macierze A oraz A' spełniają warunek z tezy lematu. Oznaczmy ich kolumny przez odpowiednio A_i oraz A'_i. Wtedy $A_i = Ae_i = F(e_i) = A'e_i = A'_i$, czyli kolumny obu macierzy są takie same, czyli $A = A'$. $\square$

PRZYKŁAD: Dla $F : \mathbb{R}^2 \ni (x_1, x_2) \mapsto (x_1, 2x_1 + x_2, x_1 - 3x_2) \in \mathbb{R}^3$, zachodzi: $F(x) = Ax$, gdzie:
$$A = \begin{bmatrix} 1 & 0 \\ 2 & 1 \\ 1 & -3 \end{bmatrix}$$

Rozważmy teraz przestrzenie X oraz Y nad ciałem K oraz odwzorowanie liniowe $F : X \to Y$. Niech wektory $b_1, \dots, b_m$ stanowią bazę X, natomiast $c_1, \dots, c_n$ - bazę Y. Każdy wektor $x \in X$ można jednoznacznie przedstawić jako liniową kombinację wektorów b_i, zatem każdemu wektorowi x można jednoznacznie przyporządkować wektor współczynników tej kombinacji: $\pi : X \ni x \mapsto (\alpha_1, \dots, \alpha_m) \in K^m$, gdzie: $x = \sum_{i=1}^m \alpha_i b_i$. Analogicznie: $\rho : Y \ni y \mapsto (\beta_1, \dots, \beta_n) \in K^n$ gdzie: $y = \sum_{i=1}^n \beta_i c_i$. Możemy zatem wprowadzić odwzorowanie $F' : K^m \to K^n$, które wektorom współrzędnych wektorów $x \in X$ przyporządkowuje wektory współrzędnych ich obrazów $F(x)$.

$$\begin{tikzcd} X \arrow[r, "F"] \arrow[d, "\pi"'] & Y \arrow[d, "\rho"] \\ K^m \arrow[r, "F'"] & K^n \end{tikzcd}$$

Zauważmy, że F' jest odwzorowaniem liniowym $K^m \to K^n$, na mocy lematu ma zatem postać mnożenia przez macierz. Tę macierz będziemy nazywać macierzą odwzorowania F w bazach $b_1, \dots, b_m$ oraz $c_1, \dots, c_n$.
PRZYKŁAD: Rozważmy odwzorowanie:

$$F : \mathbb{R}^{2\times2} \ni \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto (a+2b)x^2 + (b-c)x + (a+d) \in \Pi_2$$

Wprowadźmy na obu przestrzeniach bazy kanoniczne. Wtedy macierzy $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ odpowiada wektor współrzędnych $\begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix}$, natomiast wielomianowi $F(M)$ - wektor współrzędnych $\begin{bmatrix} a+2b \\ b-c \\ a+d \end{bmatrix}$. Macierz odwzorowania F w tych bazach to macierz, przez którą musimy pomnożyć wektor $\begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix}$ aby uzyskać wektor $\begin{bmatrix} a+2b \\ b-c \\ a+d \end{bmatrix}$. Tą macierzą jest $\begin{bmatrix} 1 & 2 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$. Zauważmy, że macierz odwzorowania zależy od wyboru baz: dla bazy na Π_2: x^2+1, $2x^2+x$, 1 oraz kanonicznej na $\mathbb{R}^{2\times2}$, otrzymamy: $F(M) = (a+2c)(x^2+1) + (b-c)(2x^2+x) + (-2c+d)\cdot 1$, czyli $F(M)$ odpowiada wektor współrzędnych $\begin{bmatrix} a+2c \\ b-c \\ -2c+d \end{bmatrix}$, zatem macierz odwzorowania w tych bazach to $\begin{bmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & -2 & 1 \end{bmatrix}$.
Definicja: Jądrem (ang. *kernel*) odwzorowania liniowego $F : X \to Y$ nazywamy zbiór $\ker F = \{x \in X : F(x) = 0\}$.
Obrazem (ang. *image*) odwzorowania liniowego $F : X \to Y$ nazywamy zbiór $\operatorname{Im} F = \{y \in Y : \exists x \in X : F(x) = y\}$.
PRZYKŁAD: Rozważmy odwzorowanie $F : \Pi^2 \ni p \mapsto \big(p(1), p(-2)\big) \in \mathbb{R}^2$. Oznaczmy $p(s) = as^2 + bs + c$. Jądro odwzorowania to zbiór $\ker F = \{p \in \Pi_2 : F(p) = 0\}$. Warunek $F(p) = 0$ prowadzi do układu równań: $p(1) = 0 \wedge p(-2) = 0$ lub równoważnie: $a+b+c = 0 \wedge 4a-2b+c = 0$, co prowadzi do $a = b$, $c = -2a$, zatem $\ker F = \{a(s^2+s-2), a \in \mathbb{R}\}$. Obrazem odwzorowania jest zbiór $\operatorname{Im} F = \{(y_1, y_2) \in \mathbb{R}^2 : \exists p \in \Pi_2 : \big(p(1), p(-2)\big) = (y_1, y_2)\}$. Warunek z definicji obrazu przyjmuje postać: $a+b+c = y_1 \wedge 4a-2b+c = y_2$, zatem do obrazu należą wszystkie pary (y_1, y_2), dla których ten układ posiada rozwiązanie (a, b, c). Okazuje się, że układ dla wszystkich par (y_1, y_2) posiada rozwiązanie równe np. $(a, b, c) = (y_1/3 + y_2/6, 2y_1/3 - y_2/6, 0)$, zatem obrazem jest cała przestrzeń $\mathbb{R}^2$.
PRZYKŁAD: Rozważmy odwzorowanie $F : \mathbb{C} \ni z \mapsto (1+2i)\operatorname{Re}(z) \in \mathbb{C}$, przy czym $\mathbb{C}$ traktujemy jako przestrzeń nad $\mathbb{R}$. Wtedy $\ker F = \{ai, a \in \mathbb{R}\}$, $\operatorname{Im} F = \{(1+2i)a, a \in \mathbb{R}\}$.
Lemat: Jądro i obraz są podprzestrzeniami liniowymi przestrzeni odpowiednio X oraz Y.
Dowód lematu pozostawiamy jako ćwiczenie.
Twierdzenie: Niech X i Y będą przestrzeniami wektorowymi, $\dim X < \infty$, a $F : X \to Y$ - odwzorowaniem liniowym. Wtedy: $\dim X = \dim \ker F + \dim \operatorname{Im} F$.
Dowód: Oznaczmy: $k = \dim \ker F$, $m = \dim X - \dim \ker F$. Wystarczy udowodnić, że wymiar obrazu równy jest m. Wybierzmy dowolną bazę jądra i oznaczmy jej wektory jako $b_1, \dots, b_k$. Wektory te są liniowo niezależne i należą do X, zatem można je uzupełnić do bazy X. Oznaczmy wektory tego uzupełnienia jako $c_1, \dots, c_m$ (wtedy wektory $b_1, \dots, b_k, c_1, \dots, c_m$ tworzą bazę X). Pokażemy, że $F(c_1), \dots, F(c_m)$ tworzą bazę obrazu. Wszystkie te wektory należą do obrazu, ponieważ są to wartości, które odwzorowanie przyjmuje dla wektorów c_i. Na potrzeby pokazania liniowej niezależności załóżmy, że istnieją skalary α_i, takie że:

$$\sum_{i=1}^m \alpha_i F(c_i) = 0 \tag{43}$$

Z liniowości F możemy przenieść skalary α_i oraz sumę pod odwzorowanie i otrzymać:

$$F\Big(\sum_{i=1}^m \alpha_i c_i\Big) = 0 \tag{44}$$

Zatem $\sum_{i=1}^{m} \alpha_i c_i \in \ker F$. Ale jądro jest generowane przez wektory b_i, zatem istnieją skalary $\beta_1, \ldots, \beta_k$, takie że:

$$\sum_{i=1}^{m} \alpha_i c_i = \sum_{i=1}^{k} \beta_i b_i \tag{45}$$

czyli:

$$\sum_{i=1}^{m} \alpha_i c_i + \sum_{i=1}^{k} -\beta_i b_i = 0 \tag{46}$$

Wektory b_i i c_i stanowią bazę X, zatem są liniowo niezależne, więc wszystkie skalary α_i oraz $-\beta_i$ występujące w powyższym równaniu są równe 0, czyli $F(c_1), \ldots, F(c_m)$ są liniowo niezależne. Pokażemy teraz, że dodatkowo wektory te generują obraz. Weźmy zatem $y \in \operatorname{Im} F$. Skoro y należy do obrazu, to istnieje $x \in X : y = F(x)$. Taki wektor x możemy przedstawić jako liniową kombinację wektorów b_i oraz c_i, czyli istnieją skalary γ_i, δ_i, takie że:

$$x = \sum_{i=1}^{m} \gamma_i c_i + \sum_{i=1}^{k} \delta_i b_i \tag{47}$$

Zatem:

$$y = F(x) = F\Big(\sum_{i=1}^{m} \gamma_i c_i + \sum_{i=1}^{k} \delta_i b_i\Big) = F\Big(\sum_{i=1}^{m} \gamma_i c_i\Big) + F\Big(\sum_{i=1}^{k} \delta_i b_i\Big) \tag{48}$$

Wektor $\sum_{i=1}^{k} \delta_i b_i$ należy do jądra, zatem $F\big(\sum_{i=1}^{k} \delta_i b_i\big) = 0$ i w konsekwencji:

$$y = F\Big(\sum_{i=1}^{m} \gamma_i c_i\Big) = \sum_{i=1}^{m} \gamma_i F(c_i) \tag{49}$$

Dowolny wektor y należący do obrazu przedstawiliśmy jako liniową kombinację wektorów $F(c_1), \ldots, F(c_m)$, zatem wektory te generują obraz. Ostatecznie, wektory te stanowią bazę obrazu, zatem wymiar obrazu równy jest m. □

6. Własności funkcji

Niech X, Y będą zbiorami, a f - funkcją $X \to Y$.
Definicja: f nazywamy iniekcją (funkcją różnowartościową), gdy $\forall x_1, x_2 \in X : f(x_1) = f(x_2) \implies x_1 = x_2$.
f nazywamy surjekcją, gdy $\forall y \in Y\ \exists x \in X : y = f(x)$.
f nazywamy bijekcją, gdy f jest iniekcją oraz surjekcją.
PRZYKŁAD: $X = \{1, 2, 3\}$, $Y = \{A, B, C\}$. Funkcja $f : X \to Y$, $f(1) = A, f(2) = B, f(3) = C$ jest iniekcją oraz surjekcją, zatem jest również bijekcją.
PRZYKŁAD: $X = \{1, 2, 3\}, Y = \{A, B, C, D\}$. Funkcja $f : X \to Y$, $f(1) = A, f(2) = B, f(3) = C$ jest iniekcją, ale nie jest surjekcją.
PRZYKŁAD: $X = \{1, 2, 3\}, Y = \{A, B\}$. Funkcja $f : X \to Y$, $f(1) = A, f(2) = B, f(3) = B$ jest surjekcją, ale nie jest iniekcją.
Niech $\#X$ oznacza liczbę elementów zbioru X. Zauważmy, że:

- jeżeli f jest iniekcją, to $\#X \leq \#Y$,
- jeżeli f jest surjekcją, to $\#X \geq \#Y$,
- jeżeli f jest bijekcją, to $\#X = \#Y$,
- jeżeli $\#X = \#Y < \infty$, to f jest iniekcją $\iff$ f jest surjekcją.

Definicja: Identycznością na X nazywamy funkcję $\mathrm{id}_X : X \ni x \mapsto x \in X$.
Niech teraz X, Y, Z będą zbiorami, f - funkcją $X \to Y$, a g - funkcją $Y \to Z$.
Definicja: Złożeniem funkcji f i g nazywamy funkcję $g \circ f : X \ni x \mapsto g(f(x)) \in Z$.
Definicja: Funkcją odwrotną do funkcji $f : X \to Y$ nazywamy funkcję $h : Y \to X$, taką że $h \circ f = \mathrm{id}_X$ oraz $f \circ h = \mathrm{id}_Y$. Funkcję odwrotną do f będziemy oznaczać jako f^{-1}.
PRZYKŁAD: Niech $X = \{1, 2, 3\}$, $Y = \{A, B, C\}$, $f : X \to Y$, $f(1) = A, f(2) = B, f(3) = C$. Wtedy $f^{-1}(A) = 1, f^{-1}(B) = 2, f^{-1}(C) = 3$.
PRZYKŁAD: Funkcją odwrotną do funkcji $[0, \infty) \ni x \mapsto x^2 \in [0, \infty)$ jest funkcja $[0, \infty) \ni x \mapsto \sqrt{x} \in [0, \infty)$.
PRZYKŁAD: Funkcją odwrotną do funkcji $\mathbb{R} \ni x \mapsto e^x \in [0, \infty)$ jest funkcja $[0, \infty) \ni x \mapsto \ln x \in \mathbb{R}$.
Twierdzenie: Funkcja posiada funkcję odwrotną wtedy i tylko wtedy, gdy jest bijekcją.
Lemat: Niech X będzie dowolnym niepustym zbiorem. Zbiór wszystkich bijekcji $X \to X$ wraz z działaniem składania funkcji tworzy grupę.
Dowód lematu pozostawiamy jako ćwiczenie.