WYKŁADY ALGEBRY LINIOWEJ Z GEOMETRIĄ

Paweł G. Walczak

Wydział Matematyki, Uniwersytet Łódzki

Wstęp

Niniejszy tekst zawiera notatki autora do wykładu przedmiotu *Algebra liniowa z geometrią* dla studentów pierwszego roku kierunku "matematyka" w Uniwersytecie Łódzkim. Notatki mają charakter nieformalny, są dalekie od doskonałości, nie pokrywają w całości materiału prezentowanego w sali wykładowej. Mogą więc być pomocne w nauce pod warunkiem krytyczznego ich czytania, porównywania z notatkami własnymi i książkami polecanymi przez wykładowcę na początku roku akademickiego. Wszelkie uwagi krytyczne pochodzące od Słuchaczy są mile widziane i mogą posłużyć ulepszeniu poniższych notatek. Autor życzy wszystkim Słuchaczom wykładu przyjemności ze studiowania matematyki i powodzenia na egzaminach.

Rozdział 1. Struktury algebraiczne

1. Działania. Dla dowolnego zbioru A działaniem wewnętrznym w A nazywamy dowolną funkcję $\cdot : A \times A \to A$. Działanie takie nazywamy *łącznym*, gdy dla dowolnych elementów $a, b, c \in A$ zachodzi równość

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c. \tag{1}$$

Działanie to nazywamy *przemiennym*, gdy dla dowolnych $a, b \in A$ spełniony jest warunek

$$a \cdot b = b \cdot a. \tag{2}$$

Element e zbioru A nazywamy *lewostronnie* (odpowiednio, *prawostronnie*) *neutralnym*, jeżeli dla dowolnego $a \in A$ zachodzi równość

$$e \cdot a = a \quad \text{(odpowiednio, } a \cdot e = e\text{)}. \tag{3}$$

Element e nazywamy *neutralnym*, gdy jest jednocześnie lewostronnie i prawostronnie neutralnym.

Jeżeli działanie posiada element neutralny, $a, b \in A$ i spełniony jest warunek

$$a \cdot b = e \quad \text{(odpowiednio, } b \cdot a = e\text{)}, \tag{4}$$

to b nazywamy elementem *prawostronnie* (odpowiednio, *lewostronnie*) *odwrotnym* do a. Element jednocześnie prawo- i lewostronnie odwrotny nazywamy po prostu *odwrotnym* lub (zwłaszcza przy addytywnym $(+)$ oznaczeniu działania) *przeciwnym*.

Twierdzenie 1. *Dla dowolnego działania w A istnieje w A co najwyżej jeden element neutralny. Jeżeli działanie jest łączne i element neutralny istnieje, to każdy element $a \in A$ posiada co najwyżej jeden element odwrotny.*

Dowód. Przypuśćmy, że e_1 i e_2 są dwoma elementami neutralnymi. Z warunku (3) wynika od razu, że

$$e_1 = e_1 \cdot e_2 = e_2.$$

(Pierwsza równość wynika z lewostroonej neutralności e_1, druga - z prawostronnej neutralności e_2.) Podobnie, jeżeli b_1 i b_2 są odwrotne do a, to

$$b_1 = b_1 \cdot e = b_1 \cdot (a \cdot b_2) = (b_1 \cdot a) \cdot b_2 = e \cdot b_2 = b_2. \quad \square$$

Element odwrotny do a oznacza się zwykle przez a^{-1} w przypadku symboliki multiplikatywnej $(\cdot)$ lub przez $-a$ w przypadku symboliki addytywnej $(+)$. Powyższe twierdzenie uzasadnia poprawność takiego oznaczenia dla działania łącznego.

Przykłady. Dodawanie i mnożenie są przemiennymi i łącznymi działaniami wewnętrznymi w zbiorach liczb rzeczywistych $\mathbb{R}$, liczb wymiernych $\mathbb{Q}$, liczb całkowitych $\mathbb{Z}$ i liczb naturalnych $\mathbb{N}$. Ponadto działania te są wykonalne w zbiorach liczb postaci

$a + b\sqrt{p}$, gdzie a i b są dowolnymi liczbami całkowitymi, a p - ustaloną liczbą naturalną. Oczywiście, liczba 0 jest elementem neutralnym dodawania, a liczba 1 elementem neutralnym mnożenia. Liczba $-a$ jest elementem przeciwnym do a względem dodawania, a liczba $\frac{1}{a}$ $(a \neq 0)$ elementem odwrotnym do a względem mnożenia.

Dla dowolnej liczby naturalnej $q > 1$ można określić w zbiorze $\mathbb{Z}_q = \{0, 1, \ldots, q-1\}$ działania dodawania i mnożenia *modulo* q (oznaczone tak jak zwykłe dodawanie i mnożenie, ale istotnie od nich różne) w następujący sposób:

$$a + b = \quad \text{reszta z dzielenia sumy } a + b \text{ przez } q,$$

$$a \cdot b = \quad \text{reszta z dzielenia iloczynu } ab \text{ przez } q.$$

Działania te są przemienne i łączne, a 0 i 1 są ich elementami neutralnymi.

W zbiorze $\mathbb{R}^n = \mathbb{R} \times \ldots \mathbb{R}$ $(n = 2, 3, \ldots)$ n- elementowych ciągów liczb rzeczywistych można określić dodawanie + wzorem

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n).$$

Jest ono łączne i przemienne, a ciąg $\mathbf{0} = (0, \ldots 0)$ jest jego elementem neutralnym. Ciąg liczb przeciwnych $(-x_1, \ldots, -x_n)$ jest elementem przeciwnym do $(x_1, \ldots, x_n)$.

Dla $n = 2$ elementy zbioru $\mathbb{C} = \mathbb{R}^2$ nazywamy *liczbami zespolonymi.* W zbiorze $\mathbb{C}$ można określić mnożenie $\cdot$ wzorem

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2). \tag{5}$$

Tak określone działanie jest przemienne i łączne (sprawdzić !). Przy utożsamieniu liczb rzeczywistych x z parami postaci $(x, 0)$ liczba $1 = (1, 0)$ okazuje się być elementem neutralnym mnożenia podobnie jak $0 = (0, 0)$ jest elementem neutralnym dodawania liczb zespolonych. Liczba zespolona $i = (0, 1)$ nazywana jest *jednostką urojoną* i spełnia warunek $i^2 = i \cdot i = -1$. Przy takim oznaczeniu każdą liczbę zespoloną $z = (x, y)$ można zapisać w postaci sumy $z = x + yi$. W takiej sytuacji x jest *częścią rzeczywistą*, a y - *częścią urojoną* liczby zespolonej z. Liczbę rzeczywistą $|z| = \sqrt{x^2 + y^2}$ nazywa się *modułem* liczby z. Dla dowolnego $z = x + yi$ liczbę $\overline{z} = x - yi$ nazywamy *sprzężoną* do z. Oczywiście, $\overline{\overline{z}} = z$, $|\overline{z}| = |z|$ oraz $z \cdot \overline{z} = |z|^2$ dla dowolnego z. Wynika stąd, że jeśli $z \neq 0$, to liczba

$$\frac{\overline{z}}{|z|^2} = \left(\frac{x}{x^2 + y^2}, -\frac{y}{x^2 + y^2} \right)$$

jest elementem odwrotnym do z względem mnożenia.

Dla dowolnego zbioru A składanie przekształceń $\circ$ jest łącznym ale na ogół nieprzemiennym działaniem wewnętrznym w zbiorze wszystkich funkcji $f : A \to A$. Ponieważ złożenie funkcji różnowartościowych jest funkcją różnowartościową, a złożenie funkcji przekształcających A na A przekształca A na A, to działanie to jest wykonalne w zbiorze S_A wszystkich bijekcji zbioru A. Przekształcenie tożsamościowe id_A ($\mathrm{id}_A(x) = x$ dla każdego $x \in A$) jest elementem neutralnym tego działania. Funkcja odwrotna f^{-1} jest elementem odwrotnym do bijekcji f. Czytelnik bez trudu znajdzie przykłady przekształceń posiadających elementy lewo- lub prawostronnie odwrotne, a nie posiadających elementu odwrotnego.

W przypadku zbioru wyposażonego w dwa działania, powiedzmy + i ·, można badać związki między nimi. Na przykład, działanie · nazywamy *rozdzielnym* względem działania +, gdy dla dowolnych argumentów a, b i c spełniony jest warunek

$$(a+b)\cdot c = a\cdot c + b\cdot c. \tag{6}$$

Mnożenie liczb (rzeczywistych, całkowitych, zespolonych itp.) jest rozdzielne względem ich dodawania. Podobnie, mnożenie modulo q jest rozdzielne względem dodawania modulo q dla dowolnego q.

Dla dowolnych dwu zbiorów P i A przekształcenie iloczynu kartezjańskiego $P\times A$ w A nazywa się it działaniem zewnętrznym w A. Przykładem takiego działania może być przekształcenie $\cdot : \mathbb{R}\times\mathbb{R}^n \to \mathbb{R}^n$ dane wzorem

$$a\cdot(x_1,\ldots,x_n) = (ax_1,\ldots,ax_n).$$

2. Przegląd struktur algebraicznych. Przez *strukturę algebraiczną* rozumiemy układ złożony ze zbioru A i skończonego zbioru działań (wewnętrznych lub zewnętrznych) w A. Omówimy tu siedem podstawowych struktur algebraicznych.

Zbiór wyposażony w jedno działanie łączne nazywamy *półgrupą*.

Półgrupę nazywamy *grupą* jeżeli posiada element neutralny, a każdy jej element posiada element odwrotny. Jeżeli działanie w grupie jest przemienne, to grupę nazywamy *przemienną* lub *abelową*.

Trójkę $(A,+,\cdot)$ złożoną ze zbioru A i dwu działań wewnętrznych, dodawania i mnożenia, nazywamy *pierścieniem* jeżeli para $(A,+)$ stanowi grupę przemienną, a mnożenie jest działaniem łącznym i rozdzielnym względem dodawania. Pierścień A nazywamy *przemiennym*, gdy przemienne jest mnożenie w A.

Ciałem nazywamy pierścień przemienny z jednością (tj. z elementem neutralnym mnożenia), w którym każdy niezerowy (tj. różny od elementu neutralnego dodawania) element posiada element odwrotny względem mnożenia.

Modułem nad pierścieniem F nazywamy układ $(A,+,\cdot)$, w którym para $(A,+)$ jest grupą przemienną, a $\cdot : F\times A\to A$ jest działaniem zewnętrznym rozdzielnym względem dodawania w A ($x\cdot(a+b) = x\cdot a + x\cdot b$ dla dowolnych $a,b\in A$ i dowolnego $x\in F$) i względem dodawania w F ($(x+y)\cdot a = x\cdot a + y\cdot a$ dla dowolnych $x,y\in F$ i dowolnego$a\in A$) oraz spełniającym warunek

$$x\cdot(y\cdot a) = (xy)\cdot a$$

dla dowolnych $x,y\in F$ i $a\in A$.

Moduł nad ciałem F nazywamy *przestrzenią wektorową*, jeżeli dla każdego jego elementu a zachodzi równość

$$1\cdot a = a,$$

gdzie 1 jest jednością ciała F.

Wreszcie, algebrą nazywamy przestrzeń wektorową wyposażoną w jeszcze jedno wewnętrzne działanie · łączne, rozdzielne względem dodawania i spełniające warunek

$$a\cdot(xb) = (xa)\cdot b = x(a\cdot b)$$

dla dowolnych $x\in F$ i $a,b\in A$.

Przykłady. Liczby całkowite (z dodawaniem i mnożeniem) tworzą pierścień. Liczby wymierne, rzeczywiste i zespolone tworzą ciała. Liczby zespolone o module 1 oraz liczby wymierne lub rzeczywiste dodatnie z mnożeniem tworzą grupy. Zbiór $\mathbb{R}^n$ z dodawaniem i mnożeniem przez liczby rzeczywiste określonymi w paragrafie poprzednim tworzy przestrzeń wektorową nad ciałem $\mathbb{R}$. Podobnie określone działania przekształcają $\mathbb{Q}^n$ i $\mathbb{C}^n$ w przestrzenie wektorowe nad $\mathbb{Q}$ i $\mathbb{C}$, odpowiednio. Dla dowolnego $q > 1$ zbiór $\mathbb{Z}_q$ z działaniami wcześniej określonymi jest pierścieniem. Pierścień ten jest ciałem wtedy i tylko wtedy, gdy q jest liczbą pierwszą (udowodnić !).

3. Relacje równoważności i struktury ilorazowe. Załóżmy, że R jest relacją równoważności (tj., relacją zwrotną, symetryczną i przechodnią) w zbiorze A. Relacja taka jest *zgodna* z działaniem wewnętrznym $\cdot$ w A, gdy dla dowolych $a, a', b, b' \in A$ spełniony jest warunek

$$aRa' \ \wedge \ bRb' \Longrightarrow (a \cdot b)R(a' \cdot b'). \tag{1}$$

Podobnie, jeśli $\cdot : F \times A \to A$ jest działaniem zewnętrznym, to relacja R jest z nim zgodna, gdy dla dowolnych $a, a' \in A$ i $x \in F$ spełniony jest warunek

$$aRa' \Longrightarrow (x \cdot a)R(x \cdot a'). \tag{2}$$

Działania zgodne z relacją R wyznaczają działania tego samego typu w zbiorze A/R klas abstrakcji:

$$[a] \cdot [b] = [a \cdot b] \tag{3}$$

w przypadku działania zewnętrznego oraz

$$x \cdot [a] = [x \cdot a] \tag{4}$$

w przypadku działania zewnętrznego.

Jeżeli zbiór A jest wyposażony w strukturę algebraiczną, której wszystkie działania są zgodne z relacją R, to mówimy, że relacja ta jest zgodna ze strukturą algebraiczną. W takiej sytuacji struktura na A wyznacza podobną (tj. złożoną z takiej samej liczby działań takiego samego typu) strukturę algebraiczną na A/R. Strukturę taką nazywamy *ilorazową*.

Przykłady. Dla dowolnej liczby naturalnej $q > 1$, relacja R określona w zbiorze $\mathbb{Z}$ przy pomocy warunku

$$aRb \Longleftrightarrow \frac{1}{q}(a - b) \in \mathbb{Z} \tag{5}$$

jest relcją równoważności zgodną z dodawaniem i mnożeniem. Dodawanie i mnożenie wyznaczają więc odpowiednie działania z zbiorze $\mathbb{Z}/R$. Zbiór ten można w naturalny sposób przekształcić wzajemnie jednoznacznie na $\mathbb{Z}_q$:

$$[a] \mapsto \text{ reszta z dzielenia liczby } a \text{ przez } q. \tag{6}$$

Przekształcenie to wyznacza izomorfizm (w sensie wprowadzonym w następnym paragrafie) struktury ilorazowej w $\mathbb{Z}/R$ i wprowadzonej wcześniej struktury algebraicznej w $\mathbb{Z}_q$.

Relacja $\equiv$ określona w zbiorze $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ warunkiem

$$(a,b) \equiv (a',b') \Longleftrightarrow ab' - ba' = 0 \tag{7}$$

jest zgodna z mnożeniem $*$ określonym wzorem

$$(a,b) * (a'b') = (aa', bb'). \tag{8}$$

Jej klasy abstrakcji nazywamy *liczbami wymiernymi*, a z (8) wynika, że reguła mnożenia liczb wymiernych "licznik razy licznik" i "mianownik razy mianownik" jest poprawna. Czytelnik spróbuje znaleźć wzór określający dodawanie par liczb całkowitych prowadzące do zwykłego dodawania liczb wymiernych.

4. Homomorfizmy i izomorfizmy struktur algebraicznych.

Mając dwie struktury algebraiczne tego samego typu na zbiorach A i B oraz przekształcenie $h : A \to B$ możemy szukać związków pomiędzy wykonywaniem działań na elementach zbioru A, a wykonywaniem odpowiednich działań w B na ich obrazach danych poprzez h. Działania $\underset{A}{\cdot}$ w A i $\underset{B}{\cdot}$ w B nazywamy h- *zgodnymi*, gdy dla dowolnych elementów a i b zbioru A zachodzi równość

$$h(a) \underset{B}{\cdot} h(b) = h(a \underset{A}{\cdot} b). \tag{1}$$

Jeżeli wszystkie działania struktury na A są h-zgodne z odpowiednimi działaniami struktury na B i h przekształca elementy neutralne działań w A na elementy neutralne odpowiednich działań w B oraz - dla każdego $a \in A$ - elementy odwrotne do a względem działań w A na elementy odwrotne do $h(a)$ względem odpowiednich działań w B, to mówimy, że h jest *homomorfizmem* struktur algebraicznych. Jeżeli homomorfizm h jest bijekcją, to nazywamy go *izomorfizmem*. W tym przypadku przekształcenie odwrotne h^{-1} jest również homomorfizmem (udowodnić !).

Izomorfizmy struktur algebraicznych zachowują wszystkie własności algebraiczne (np., łączność czy przemienność) działań strukturalnych. Dlatego struktury izomorficzne (tj. takie, że istnieje izomorfizm jednej z nich na drugą) są z algebraicznego punktu widzenia nierozróżnialne i uznajemy je za identyczne.

Przykłady. Odwzorowanie tożsamościowe $x \mapsto x$ wyznacza homomorfizmy dwudziałaniowych struktur algebraicznych (z dodawaniem i mnożeniem) na zbiorach $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$. Podobnie, odwzorowanie $\mathbb{R} \ni x \mapsto (x,0) \in \mathbb{C}$ jest homomorfizmem odpowiednich struktur danych przez dodawanie i mnożenie liczb rzeczywistych i zespolonych. Dla dowolnej struktury algebraicznej na zbiorze A i zgodnej z nią relacji równoważności R naturalne rzutowanie $A \ni x \mapsto [x] \in A/R$ jest homomorfizmem struktury na A na strukturę ilorazową w A/R.

Rozdział 2. Grupy

1. Podstawowe pojęcia. Przypomnijmy, że grupą nazywamy parę $(G, \cdot)$, w której G jest zbiorem, a $\cdot$ działaniem łącznym w G, posiadającym element neutralny (*jedność grupy*) e i takim, że każdy element $g \in G$ posiada element odwrotny g^{-1}. Jeżeli działanie grupowe jest przemienne, to grupę nazywamy przemienną lub abelową.

Przykłady. Zbiory $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ z dodawaniem stanowią grupy przemienne. Zbiór $\mathbb{Z}_q$ z dodawaniem modulo q jest grupą przemienną. Podobnie, grupy przemienne tworzą zbiory $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$, $\mathbb{C} \setminus \{0\}$, $\mathbb{Q}_+$, $\mathbb{R}_+$ i $\{z \in \mathbb{C}; |z| = 1\}$ z mnożeniem. Bijekcje dowolnego, ustalonego zbioru X ze składaniem przekształceń tworzą grupę, na ogół nieprzemienną. W szczególności, grupę stanowią permutacje n-elementowe. Grupę tę nazywamy *grupą symetryczną* i oznaczamy symbolem S_n. Grupa S_n jest przemienna wtedy i tylko wtedy, gdy $n = 1$ lub $n = 2$. W tym pierwszym przypadku, grupa jest trywialna: składa się z samego elementu neutralnego e z działaniem określonym w jedyny możliwy sposób: $e \cdot e = e$.

Jeżeli G jest grupą skończoną, to liczbę jej elementów nazywamy jej *rzędem*. Np., rząd grupy S_n wynosi $n!$.

Jeśli A jest takim podzbiorem grupy G, że każdy element $g \in G$ można przedstawić w postaci

$$a_1^{k_1} \cdot \ldots \cdot a_l^{k_l} \tag{1}$$

dla pewnych $a_1, \ldots a_l \in A$ oraz $k_1, \ldots k_l \in \mathbb{Z}$, to mówimy, że zbiór A *generuje* grupę G. Na przykład, grupy $(\mathbb{Z}, +)$ i $(\mathbb{Z}_q, +)$ są generowane przez jeden element, liczbę 1. Grupy takie nazywamy *cyklicznymi*.

Jeżeli element a generuje grupę cykliczną G i wszystkie potęgi a^k, $k \in \mathbb{Z}$, są różne między sobą, to G jest grupą nieskończoną izomorficzną z $(\mathbb{Z}, +)$. Izomorfizm może być określony wzorem

$$G \ni a^k \mapsto k \in \mathbb{Z}. \tag{2}$$

Jeżeli dwie różne potęgi elementu a są równe, to pewna potęga a jest równa jednoći e. Jeżeli q jest najmniejszą liczbą naturalną taką, że $a^q = e$, to $G = \{e, a, a^2, \ldots, a^{q-1}\}$ jest grupą skończoną rzędu q izomorficzną z $(\mathbb{Z}_q, +)$. Tak więc, grupy addytywne $\mathbb{Z}$ i $\mathbb{Z}_q$, $q = 1, 2 \ldots$, są jedynymi, z dokładnością do izomorfizmu, grupami cyklicznymi. Ważnym przykładem skończonej grupy cyklicznej jest grupa pierwiastków stopnia q z jedności: $\{z \in \mathbb{C}; z^q = 1\}$ z mnożeniem.

Grupę nazywamy *skończenie generowaną*, jeżeli istnieje zbiór skończnony ją generujący. Prostym przykładem takiej grupy jest $(\mathbb{Z}^n, +)$. Generatorami są np. elementy $e_i = (\delta_i^1, \ldots, \delta_i^n)$, $i = 1, \ldots, n$. (Tu i w dalszym ciągu przyjmujemy, że $\delta_i^j = 0$, gdy $i \neq j$ oraz $\delta_i^j = 1$, gdy $i = j$. Tak określony symbol δ_i^j nazywamy *symbolem* (lub "*deltą*") *Kroneckera*. Ogólniej, dla dowolnego zbioru A istnieje pewna grupa abelowa G generowana przez A: $G = \{g : A \to \mathbb{Z}; g(x) = 0$ dla prawie wszystkich $x\}$ z działaniem określonym wzorem $(g_1 g_2)(x) = g_1(x) + g_2(x)$, $x \in A$, jest grupą przemienną z elementem neutralnym e, $e(x) = 0$ dla

N. H. Abel (1802 - 1829) - matamatyk norweski.

L. Kronecker (1823 - 1891) - urodzony w Legnicy matematyk niemiecki

każdego $x \in X$. Zbiór A można utożsamić z podzbiorem zbioru G złożonym z wszystkich funkcji $\hat{x}$, $x \in X$, danych wzorami: $\hat{x}(x) = 1$, $\hat{x}(y) = 0$, gdy $y \neq x$. Tak skonstruowaną grupę G nazywamy *abelową grupą wolną generowaną przez A*. Grupa ta jest skończenie generowana wtedy i tylko wtedy, gdy A jest zbiorem skończonym.

Podobnie, dla dowolnej rodziny $\{G_i; i \in I\}$ grup abelowych można skonstruować ich *sumę prostą* $G = \sum_i G_i = \{f : I \to \cup_i G_i; \forall i f(i) \in G_i \wedge f(i) = 0$ dla prawie wszystkich $i\}$ z działaniem $(f_1 f_2)(i) = f_1(i) + f_2(i)$, $i \in I$. Suma ta jest też grupą abelową.

Sumy (iloczyny) proste i grupy wolne mogą być rozważane w pełnej kategorii grup (niekoniecznie abelowych), ale jest to znacznie trudniejsze (por., S. Lang, Algebra, PWN).

2. Homomorfizmy grup. Zgodnie z ogólną definicją homomorfizmu struktur algebraicznych, homomorfizmem grupy $(G, \cdot)$ w grupę $(H, \cdot)$ jest przekształcenie $h : G \to H$ spełniające warunek

$$h(g \cdot g') = h(g) \cdot h(g') \quad (g, g' \in G) \tag{1}$$

oraz

$$h(g^{-1}) = h(g)^{-1} \quad (g \in G). \tag{2}$$

Przekształcenie takie przekształca jedność grupy G na jedność grupy H. Istotnie,

$$h(e) = h(e \cdot e^{-1}) = h(e) \cdot h(e^{-1}) = h(e) \cdot h(e)^{-1} = e',$$

gdy e jest jednością grupy G, a e' jednością H.

Warunki (1) i (2) można zastąpić równoważnym im warunkiem

$$h(g \cdot g'^{-1}) = h(g) \cdot h(g')^{-1} \quad (g, g' \in G). \tag{3}$$

Homomorfizm $h : G \to H$ nazywamy *monomorfizmem* (odp., *epimorfizmem*), gdy h jest różnowartościowe (odp., gdy $h(G) = H$). Homomorfizm grup jest więc izomorfizmem, gdy jest jednocześnie mono- i epimorfizmem. Izomorfizm grupy G na siebie nazywamy *automorfizmem*. Przypomnijmy, że grupy izomorficzne mają te same własności algebraiczne: obie są przemienne lub nie, obie są skończenie generowane lub nie itp.

Z definicji wynika od razu, że złożenie homomorfizmów grup jest homomorfizmem, złożenie monomorfizmów (epimorfizmów, izomorfizmów) jest monomorfizmem (epimorfizmem, izomorfizmem). Automorfizmem dowolnej grupy G jest odwzorowanie tożsamościowe id_G. Przekształcenie odwrotne do izomorfizmu jest też izomorfizmem. Wynika stąd, że wszystkie automorfizmy grupy G z działaniem składania przekształceń tworzą grupę $\mathrm{Aut}(G)$.

Przykład. Dla dowolnego elementu g grupy G rozważmy odwzorowanie

$$Ad(g) : G \to G, \quad Ad(g)(h) = ghg^{-1}. \tag{4}$$

Odwzorowanie to jest automorfizmem grupy G: $g(hh'^{-1})g^{-1} = (ghg^{-1}) \cdot (gh'g^{-1})^{-1}$, $h = Ad(g)(g^{-1}hg)$, jeżeli $ghg^{-1} = gh'g^{-1}$, to $h = g^{-1}(ghg^{-1})g = g^{-1}(gh'g^{-1})g = h'$. Z ostatniej implikacji wynika też, że $Ad(g)^{-1} = Ad(g^{-1})$. Podobnie, łatwo sprawdzić, że $Ad(gg') = Ad(g) \circ Ad(g')$. Przyporządkowanie

$$G \ni g \mapsto Ad(g) \in Aut(G)$$

jest więc homomorfizmem grup. Automorfizmy postaci $Ad(g)$ nazywa się *wewnętrznymi*. Tworzą one podgrupę (w sensie następnego paragrafu) grupy $Aut(G)$.

3. Podgrupy, grupy ilorazowe. Niepusty podzbiór H grupy $(G, \cdot)$ nazywamy *podgrupą*, gdy dla dowolnych elementów $g, g' \in H$ iloczyn $g \cdot g'^{-1}$ należy do H. Jeżeli H jest podgrupą i $g, g' \in H$, to $e = g \cdot g^{-1} \in H$, $g^{-1} = e \cdot g^{-1} \in H$ oraz $g \cdot g^{-1} = g \cdot (g^{-1})^{-1} \in H$. Wynika stąd, że zbiór H z działaniem grupowym w G ograniczonym do $H \times H$ jest grupą. Mówiąc "podgrupa" mamy na myśli zawsze grupę otrzymaną w ten sposób.

Zauważmy, że jeżeli H jest podgrupą grupy G, to odwzorowanie

$$id_H : H \to G, \quad H \ni x \mapsto x, \tag{1}$$

jest monomorfizmem grup.

Dla dowolnego podzbioru A grupy G i elemntu $g \in G$ wprowadźmy oznaczenia następujące:

$$gA = \{ga; a \in A\} \text{ i } Ag = \{ag; a \in A\}. \tag{2}$$

Jeżeli G jest grupą abelową, to oczywiście $gA = Ag$ dla wszystkich A i g. Warunek $gA = Ag$ jest też zawsze równoważny warunkowi $A = gAg^{-1}$. Jeżeli A jest podgrupą, to zbiory postaci (2) nazywamy odpowiednio *lewymi* i *prawymi warstwami* (elementu g względem podgrupy A).

Twierdzenie 1. *(Lagrange'a) Rząd każdej podgrupy grupy skończonej G jest dzielnikiem rzędu grupy G.* □

Dowód. Niech $H = \{a_1, \ldots, a_k\}$ będzie podgrupą grupy skończonej G. Zbiory (lewe warstwy) aH $(a \in G)$ są parami rozłączne, równoliczne i dają w sumie G. Jeżeli p jest liczbą warstw, to G zawiera dokładnie kp elementów. □

Podgrupę H grupy G nazywamy *niezmienniczą*, gdy warunek

$$gHg^{-1} = H \tag{3}$$

jest spełniony dla wszystkich $g \in G$. Widać od razu, że każda podgrupa grupy abelowej jest niezmiennicza.

Przykłady. Jeżeli $m \leq n$, to elementy grupy symetrycznej S_m można utożsamić z takimi permutacjami $\sigma \in S_n$, które zachowują elementy $m+1, \ldots, n$: $\sigma(k) = k$ dla $k = m+1, \ldots, n$. W ten sposób S_m staje się (izomorficzna z) podgrupą grupy S_n. Jest ona (sprawdzić !) podgrupą niezmienniczą.

Dla dowolnego homomorfizmu grup $h : G \to H$ zbiory

$$\ker(h) = \{g \in G; h(g) = e\} \text{ i } \operatorname{im}(h) = \{h(g); g \in G\} \tag{4}$$

są podgrupami, odpowiednio, grup G i H, co wynika bezpośrednio z przyjętych określeń. Podgrupę $\ker(h)$ nazywamy *jądrem* homomorfizmu, podgrupę $\operatorname{im}(h)$ - jego *obrazem*. Z implikacji

$$h(g) = e \Longrightarrow h(aga^{-1}) = h(a)h(g)h(a^{-1}) = h(a)h(a)^{-1} = e$$

J. L. Lagrange (1736 - 1812) - jeden z najwybitniejszych matematyków francuskich

wynika, że jądro dowolnego homomorfizmu jest podgrupą niezmienniczą. Obraz homomorfizmu niezmienniczy być nie musi. Z określenia jądra wynika łatwo, że homomorfizm jest monomorfizmem wtedy i tylko wtedy, gdy jego jądro jest *podgrupą trywialną*, złożoną z samej jedności.

Grupa izometrii płaszczyzny jest nie-niezmienniczą podgrupą grupy wszystkich bijekcji płaszczyzny.

Dla dowolnej podgrupy H grupy G zbiór $N_H = \{g \in G; gHg^{-1} = H$ jest podgrupą G. Jest to największa podgrupa o tej własności, że H jest jej podgrupą normalną. Nazywamy ją *normalizatorem* podgrupy H.

Dla dowolnej podgrupy H grupy G relacja

$$g \equiv h \iff gh^{-1} \in H \tag{5}$$

jest zwrotna, symetryczna i przechodnia, jest więc relacją równoważności w G. Jej klasami abstrakcji są zbiory postaci gH, $g \in G$.

Twierdzenie 2. *Relacja (5) jest zgodna z działaniem grupowym w G wtedy i tylko wtedy, gdy H jest podgrupą niezmienniczą.*

Dowód. Załóżmy najpierw, że H jest podgrupą niezmienniczą i weźmy cztery elementy $g, g', h, h' \in G$ takie, że $g \equiv g'$ i $h \equiv h'$. Wtedy $gg'^{-1} \in H$ oraz $hh'^{1} \in H$, a więc i

$$gh(g'h')^{-1} = ghh'^{-1}g'^{-1} = g(hh'^{-1})g^{-1}(gg'^{-1}) \in (gHg^{-1})H = H,$$

tj. $gh \equiv g'h'$, co oznacz, że relacja $\equiv$ jest zgodna z działaniem grupowym.

Odwrotnie, jeśli relacja (5) jest zgodna z działaniem, $g \in G$ i $h \in H$, to $h \equiv e$, $gh \equiv g$, a więc $ghg^{-1} \in H$, tj.

$$gHg^{-1} \subset H. \tag{6}$$

Z (6) wynika też, że $H = g^{-1}(gHg^{-1})g \subset g^{-1}Hg$ dla dowolnego $g \in G$. Zastępując g przez g^{-1} otrzymujemy relację

$$gHg^{-1} \subset H, \tag{7}$$

która w połączeniu z (6) daje równość (3) dowodzącą, że H jest podgrupą niezmienniczą. □

Powyższe twierdzenie dowodzi, że dla podgrupy niezmienniczej H zbiór $G/H = G/\equiv$ klas abstrakcji relacji (5) posiada naturalną strukturę grupy z działaniem danym wzorem

$$[g] \cdot [h] = [gh], \tag{8}$$

elementem neutralnym $[e] = H$ i elementem odwrotnym do $[g]$ równym $[g^{-1}]$. Otrzymaną w ten sposób grupę nazywamy *ilorazową*.

Twierdzenie 3. *Dla dowolnego epimorfizmu grup $f : G \to H$, grupa ilorazowa $G/\ker(f)$ jest izomorficzna z H.*

Dowód. Z definicji jądra wynika, że przekształcenie

$$G/\ker(f) \ni [g] \mapsto f(g) \in H \tag{9}$$

jest dobrze określone. Z określenia działania w grupie ilorazowej wynika, że jest ono homomorfizmem. Jest ono epimorfizmem, bo f było takim. Wreszcie, jeżeli $f(g) = f(h)$, to $gh^{-1} \in \ker(f)$, $g \equiv h$ i $[g] = [h]$, a zatem odwzorowanie (9) jest monomorfizmem. □

Wniosek. *Dla dowolnego homomorfizmu grup $f : G \to H$, grupy $im(f)$ i $G/\ker(f)$ są izomorficzne.* □

Przykład. Dla dowolnej grupy G zbiór G_0 wszystkich skończonych produktów elementów postaci

$$aba^{-1}b^{-1} \quad (a, b \in G) \tag{10}$$

jest podgrupą. Jest ona normalna: element

$$x(aba^{-1}b^{-1})x^{-1} = (xax^{-1})(xbx^{-1})(xax^{-1})^{-1}(xbx^{-1})^{-1} \tag{11}$$

jest elementem postaci (10). Podgrupę tę nazywa się *komutatorem* grupy G. Grupa ilorazowa G/G_0 jest przemienna:

$$[a] \cdot [b][a]^{-1}[b]^{-1} = [aba^{-1}b^{-1}] = [e], \tag{12}$$

ponieważ $aba^{-1}b^{-1} \in G_0$.

Rozdział 3. Pierścienie i ciała

1. Pierścienie, podpierścienie, ideały. Przypomnijmy, że pierścieniem nazywamy trójkę $(A, \cdot, +)$ złożoną ze zbioru A i dwu działań wewnętrznych $\cdot$ i $+$ spełniających następujące warunki:

(1) $\forall a, b, c \in A: \quad a + (b + c) = (a + b) + c$,
(2) $\forall a, b \in A: \quad a + b = b + a$,
(3) $\exists e \in A: \forall a \in A: \quad a + e = a$,
(4) $\forall a \in A: \exists b \in A: \quad a + b = e$,
(5) $\forall a, b, c \in A: \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c$,
(6) $\forall a, b, c \in A: \quad a \cdot (b + c) = a \cdot b + a \cdot c$.

Element a pierścienia A nazywamy *dzielnikiem zera*, gdy $a \neq 0$ i istnieje niezerowy element $b \in A$ taki, że

$$a \cdot b = 0. \tag{1}$$

Pierścień nazywamy *przemiennym*, gdy przemienne jest mnożenie $\cdot$. Jeżeli istnieje w A element neutralny mnożenia, to A nazywamy *pierścieniem z jedynką*. (Tradycyjnie, element neutralny dodawania $+$ oznaczamy symbolem 0, element neutralny mnożenia $\cdot$ - symbolem 1.) Przemienny pierścień z jedynką, a bez dzielników zera nazywamy *całkowitym*.

Przykłady. Pierścień $\mathbb{Z}$ jest całkowity. Pierścień wielomianów o współczynnikach w dowolnym pierścieniu całkowitym jest całkowity. Wynika stąd, że pierścień wielomianów n-zmiennych o współczynnikach w pierścieniu całkowitym jest całkowity dla dowolnego $n = 1, 2, \ldots$. Pierścień $\mathbb{Z}_q$ jest całkowity wtedy i tylko wtedy, gdy q jest liczbą pierwszą: Jeżeli $q = mn$, $m > 1$ i $n > 1$, to liczmy m i n są dzielnikami zera w $\mathbb{Z}_q$.

Dla dowolnego pierścienia A i zbioru X zbiór wszystkich funkcji $f: X \to A$ z działaniami określonymi wzorami

$$(f + g)(x) = f(x) + g(x), \quad (fg)(x) = f(x)g(x) \quad (x \in X), \tag{2}$$

jest pierścieniem. Pierścień funkcji jest przemienny wtedy i tylko wtedy, gdy przemienny jest pierścień A. Elementem neutralnym dodawania jest funkcja stała równa 0. Jeżeli A ma jedynkę 1, to funkcja stała równa 1 jest jedynką pierścienia funkcji. Podobnie, pierścień funkcji ma dzielniki zera wtedy i tylko wtedy, gdy istnieją dzielniki zera w A. Zatem, pierścień funkcji jest całkowity wtedy i tylko wtedy, gdy całkowity jest pierścień A.

Zbiór $B \subset A$ nazywamy *podpierścieniem* pierścienia A, gdy działania $+$ i $\cdot$ są wykonalne w B, $0 \in B$ oraz $-a \in B$ dla dowolnego $a \in B$. Podpierścień B z dizałaniami $+$ i $\cdot$ ograniczonymi do $B \times B$ jest pierścieniem. Zbiór I nazywamy *ideałem* (odpowiednio, *ideałem lewostronnym* lub *prawostronnym*, gdy jest podpierścieniem oraz iloczyny $a \cdot b$ i $b \cdot a$ (odpowiednio, $a \cdot b$ lub $b \cdot a$) należą do I dla

wszystkich $a \in A$ i $b \in I$. I jest więc ideałem wtedy i tylko wtedy, gdy jest jednocześnie ideałem lewo- i prawostronnym. Ideał I nazywamy *maksymalnym*, jeżeli każdy ideał I' zawierający I jest równy I lub A:

$$I \subset I' \Longrightarrow (I' = I \vee I' = A). \tag{3}$$

Przykłady. Zbiór $q\mathbb{Z}$ liczb podzielnych przez daną, ustaloną liczbę naturalną q jest ideałem pierścienia $\mathbb{Z}$. Ideał $q\mathbb{Z}$ jest maksymalny wtedy i tylko wtedy, gdy q jest liczbą pierwszą. Zbiór jednoelementowy $I = \{0\}$ jest ideałem dowolnego pierścienia. W pierścieniu funkcji $f : X \; toA$ zbiór $I_Y = \{f : X \to A; f|Y \equiv 0\}$ jest ideałem dla dowolnego zbioru $Y \subset X$. Ideał I_Y jest maksymalny wtedy i tylko wtedy, gdy Y jest zbiorem jednopunktowym. Dla dowolnej liczby naturalnej k, ideał pierścienia wielomianów nad pierścieniem A tworzą wszystkie wielomiany $(a_0, a_1, \dots)$, dla których $a_0 = a_1 = \cdots = a_k = 0$. Ideał ten jest maksymalny wtedy i tylko wtedy, gdy $k = 0$.

2. Ciała. Przypomnijmy, że ciałem nazywamy pierścień A z jednoćią $1 \neq 0$, w którym każdy niezerowy element a posiada element odwrotny a^{-1} względem mnożenia $\cdot$: $a \cdot a^{-1} = a^{-1} \cdot a = 1$. Z określenia wynika łatwo, że ciało nie posiada dzielników zera: Jeżeli $a \cdot b = 0$ i $b \neq 0$, to $0 = (a \cdot b) \cdot b^{-1} = a \cdot (b \cdot b^{-1}) = a \cdot 1 = a$.

Najmniejszą liczbę naturalną $m > 1$, dla jakiej istnieje element niezerowy $a \in A$ taki, że

$$ma = a + a + \cdots + a(m \text{ składników}) \quad = 0 \tag{1}$$

nazywamy *charakterystyką* ciała A. Jeżeli liczba taka nie istnieje, to A nazywamy *ciałem o charakterystyce 0* lub *ciałem bez charakterystyki*. Zauważmy, że jeli równość (1) zachodzi dla pewnego $a = 0$, to $mb = 0$ dla każdego $b \in A$. Rzeczywiście, z łączności mnożenia i rozdzielności mnożenia względem dodawania wynika, że

$$mb = (mb \cdot a) \cdot a^{-1} = (b \cdot (ma)) \cdot a^{-1} = 0 \cdot a^{-1} = 0. \tag{2}$$

Przykłady. Ciała $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ mają charakterystykę zero. Każde ciało o charakterystyce zero jest nieskończone. Jeżeli $q \in \mathbb{N}$ jest liczbą pierwszą, to ciało $\mathbb{Z}_q$ ma charakterystykę q.

Każdemu wielomianowi $(a_0, a_1, a_2, \dots)$ o współczynnikach w pierścieniu (w szczególności, ciele) A można przyporządkować *funkcję wielomianową*

$$A \ni x \mapsto a_0 + a_1 \cdot x + a_2 \cdot x^2 + \dots. \tag{3}$$

Na ogół przyporządkowanie to nie jest różnowartościowe. Np., funkcja wielomianowa $x \mapsto x + x^2$ nad ciałem $\mathbb{Z}_2$ jest tożsamościowo równa zeru. Jeżeli jednak A jest ciałem o charakterystyce zero, to przyporządkowanie (3) ustala wzajemnie jednoznaczną odpowiedniość między wielomianami ("ciągami współczynników"), a funkcjami wielomianowymi.

Odnotujmy, że jedynymi ideałami dowolnego ciała A są zbiory $\{0\}$ i A. Istotnie, jeżeli a jest niezerowym elementem ideału I i $b \in A$, to $ba \in I$ i $b = b^{-1}(ba) \in I$.

Podpierścień B ciała A jest *podciałem* (tj., jest ciałem z działaniami z A ograniczonymi do $B \times B$), gdy $1 \in B$ oraz $a^{-1} \in B$ dla każdego $a \in B$. W ten sposób zbiory $\mathbb{Q}$ i $\mathbb{R}$ są podciałami ciała $\mathbb{C}$, a również $\mathbb{Q}$ jest podciałem ciała $\mathbb{R}$.

3. Ciało ułamków.

Niech A będzie dowolnym pierścieniem całkowitym, $B = A \times (A \setminus \{0\})$. Zdefiniujmy w B relację $\equiv$ w następujący sposób:

$$(a,b) \equiv (a',b') \iff ab' - ba' = 0. \tag{1}$$

Relacja $\equiv$ jest oczywiście zwrotna i symetryczna. Jest też przechodnia: Jeżeli $(a,b) \equiv (a',b')$ i $(a',b') \equiv (a'',b'')$, to $ab' - ba' = 0$ i $a'b'' - b'a'' = 0$, a więc

$$(ab'' - ba'')b' = (ab' - ba')b'' + (a'b'' - b'a'')b = 0, \tag{2}$$

a ponieważ A nie ma dzielników zera i $b' \neq 0$, więc $ab'' - ba'' = 0$, tj, $(a,b) \equiv (a'',b'')$. Relacja $\equiv$ jest więc równoważnością i można brać pod uwagę zbiór $A/\equiv$ jej klas abstrakcji. Co więcej, relacja ta jest zgodna z określonymi następująco działaniami dodawania i mnożenia w B:

$$(a,b) + (c,d) = (ad + bc, bd), \quad (a,b) \cdot (c,d) = (ac, bd). \tag{3}$$

Rzeczywiście, jeżeli $(a',b') \equiv (a,b)$ i $(c',d') \equiv (c,d)$, to

$$(ad + bc)b'd' - bd(a'd' + b'c') = dd'(ab' - ba') + bb'(cd' - dc') = 0 \tag{4}$$

oraz

$$acb'd' - a'c'bd = cd'(ab' - ba') + a'b(cd' - dc') = 0. \tag{5}$$

Zgodnie z ogólnymi rozważaniami Rozdziału I, działania (3) indukują odpowiednie działania dodawania i mnożenia w zbiorze $A/\equiv$.

Twierdzenie. *Zbiór $A/\equiv$ z działaniami indukowanymi przez działania (3) w A jest ciałem.*

Tak otrzymane ciało nazywamy *ciałem ułamków* pierścienia A. Ciało liczb wymiernych jest ciałem ułamków pierścienia $\mathbb{Z}$.

Dowód. Większość wymaganych własności działań jest niemal oczywista. Jest też jasne, że klasy abstrakcji $[(0,1)]$ i $[(1,1)]$ są elementami neutralnymi dodawania i mnożenia. Wykażemy

(i) łączność dodawania,
(ii) rozdzielność mnożenia względem dodawania,
(iii) istnienie elementów odwrotnych.

Ad. (i). Niech $(a_i,b_i) \in B$ dla $i = 1,2,3$. Wtedy $[(a_1,b_1)] + [(a_2,b_2)] = [(a_1b_2 + a_2b_1, b_1b_2]$ oraz $[(a_2,b_2)] + [(a_3,b_3)] = [(a_2b_3 + a_3b_2, b_2b_3)]$, skąd

$$([(a_1,b_1)] + [(a_2,b_2)]) + [(a_3,b_3)] = [((a_1b_2 + a_2b_1)b_3 + b_1b_2a_3, b_1b_2b_3)] \tag{6}$$

oraz

$$[(a_1,b_1)] + ([(a_2,b_2)] + [(a_3,b_3)]) = [(a_1b_2b_3 + b_1(a_2b_3 + b_2a_3), b_1b_2b_3]. \tag{7}$$

Widać od razu, że prawe strony w (6) i (7) są równe.

Ad. (ii) Dla tych samych elementów (a_i, b_i) mamy

$$([(a_1, b_1) + (a_2, b_2)]) \cdot [(a_3, b_3)] = [((a_1b_2 + a_2b_1)a_3, b_1b_2b_3))], \tag{8}$$

oraz

$$\begin{aligned}([(a_1, b_1)] \cdot [(a_3, b_3)] + [(a_2, b_2)] \cdot [(a_3, b_3)] &= [(a_1a_3, b_1b_3)] + [(a_2a_3, b_2b_3)] \\ &= [(a_1a_3b_2b_3 + a_2a_3b_1b_3, b_1b_2b_3^2)].\end{aligned} \tag{9}$$

Teraz wyniki działa; w (8) i (9) są równe ponieważ

$$(a_1b_2 + a_2b_1)a_3b_1b_2b_3^2 - (a_1a_3b_2b_3 + a_2a_3b_1b_3)b_1b_2b_3 = 0.$$

Ad(iii) Jeżeli $z \neq 0$ w $A/\equiv$, to $z = [(a, b)]$ dla pewnych $a, b \in A$ różnych od zera ($a \neq 0$ i $b \neq 0$). Klasa $[(b, a)]$ jest dobrze określona (sprawdzić !) i

$$[(a, b)] \cdot [(b, a)] = [(ab, ab)] = [(1, 1)].$$

Zatem $z^{-1} = [(b, a)]$ jest elementem odwrotnym do z. $\square$

4. Pierwiastki wielomianów.

Załóżmy, że A jest pierścieniem całkowitym i nieskończonym. Wtedy wielomiany pozostają we wzajemnie jednoznacznej odpowiedniości z funkcjami wielomianowymi:

$$(a_0, a_1, \dots, a_n, 0, 0, \dots) \longleftrightarrow \sum_{i=1}^{n} a_i x^i, \tag{1}$$

będziemy je więc utożsamiać.

Element $c \in A$ nazywamy *pierwiastkiem* wielomianu

$$W(x) = \sum_{i=1}^{n} a_i x^i, \tag{2}$$

gdy $W(x) = 0$. Z równości

$$x^k - c^k = (x - c)(x^{k-1} + cx^{k-2} + \cdots + c^{k-1}) \tag{3}$$

wynika, że dla dowolnego $c \in A$ istnieje wielmomian W_1 stopnia o 1 niższego od stopnia W, dla którego

$$W(x) - W(c) = (x - c) \cdot W_1(x) \quad (x \in A). \tag{4}$$

Wynika stądże c jest pierwiatkiem wielomianu W wtedy i tylko wtedy, gdy

$$W(x) = (x - c) \cdot W_1(x) \quad (x \in A) \tag{5}$$

dla pewnego wielomianu W_1, tj. gdy W jest *podzielny* przez jednomian $x - c$. Jeżeli wielomian W jest podzielny przez $(x - c)^p$, a nie jest podzielny przez $(x - c)^{p+1}$, to liczbę $p \in \mathbb{N}$ nazywamy *krotnością* pierwiastka c. Z powyższych obserwacji wynika następujące twierdzenie:

Twierdzenie 1. *Wielomian stopnia n ma co najwyżej n pierwiastków (liczonych tyle razy ile wynosi ich krotność.* □

Przykłady. Istnieją wielomiany nie posiadające pierwiastków (np., x^2+1 nad ciałem $\mathbb{R}$). Jeżeli liczba wymierna przedstawiona jako ułamek nieskracalny p/q jest pierwiaskiem wielomianu o współczynnikach całkowitych, to q jest dzielnikiem współczynnika prz najwyższej potędze, podczas gdy p jest dzielnikiem wyrazu wolnego. (Daje to algorytm pozwalający znaleźć wszystkie pierwiastki wymierne takiego wielomianu.) Jeżeli liczba zespolona z jest pierwiastkiem wielomianu W o współczynnikach rzeczywistych, to $\bar{z}$ jest też pierwiastkiem W. Istnieją algorytmy (wzory Cardano i metoda Ferrariego) pozwalające znajdywać pierwiastki wielomianów stopnia 3 i 4. Udowodniono (w pierwszej połowie XIX wieku), że dla wielomianów wyższych stopni algorytmów takich nie ma.

Ciało A nazywamy *algebraicznie zupełnym*, gdy każdy wielomian W stopnia dodatniego o współczynnikach w A posiada pierwiastek. Jeżeli A jest ciałem zupełnym, to każdy wielomian W o współczynikach w A posiada dokładnie tyle (z uwzględnienim krotności) pierwiastków ie wynosi jego stopień.

Twierdzenie 2. *(zasadnicze twierdzenie algebry) Ciało $\mathbb{C}$ liczb zespolonych jest algebraicznie zupełne.*

Szkic dowodu. Dla dowolnego $r \geq 0$ obrazem okręgu $\{z; |z| = r\}$ danym przez wielomian W stopnia n jest pewna krzywa zamknięta c_r. Jeżeli W nie ma pierwiastków, to krzywa ta nie przechodzi przez 0, a więc można obliczyć przyrost argumentu wzdłuż c_r. Przyrost ten jest wielokrotnością kąta 2π. Z ciągłości funkcji W wynika, że przyrost ten jest stały w każdym takim przedziale $[r_1, r_2]$, dla którego W nie przyjuje wartości 0 w zbiorze $\{z; r_1 \leq |z| \leq r_2\}$. Jeśli W nie ma pierwiastków, to przyrost ten jest stale równy 0, bo jest równy 0 dla r = 0. Z drugiej strony, jeśli r jest dostatecznie duże i $W(z) = z^n \cdot f(z)$, to $|f(z) - 1| \leq \frac{1}{2}$ i $|arg f(z)| \leq \frac{\pi}{3}$, gdy $|z| = r$. Zatem przyrost argumentu dla W wzdłuż c_r jest taki sam jak dla wielomianu z^n, a więc wynosi $2n\pi$. Stąd $n = 0$, co należało udowodnić. □

Wynika stąd, że każdy wielomian nad ciałem $\mathbb{C}$ można rozłożyć na czynniki stopnia 1. Wcześniejsza obserwacja dotycząca pierwiastków zespolonych wielomianów rzeczywistych pokazuje, że każdy wielomian o współczynnikach rzeczywistych moña przedstawić jako iloczyn czynników liniowych i kwadratowych (wielomianów stopni 1 i 2).

5. Wielomiany wielu zmiennych..

Dla dowolnego pierścienia A oznaczmy przez $A[x]$ pierścień wielomianów (jednej zmiennej) o współczynnikach w A. Elementy pierścienia $A[x_1, x_2] := A[x_1][x_2]$ nazywamy *wielomianami dwu zmiennych.* S ca one wielomianami (jednej zmiennej) o współczynnikach w $A[x]$. Ogólnie, wielomiany o współczynnikach w pierścieniu $A[x_1, \ldots, x_n]$ wielomianów n zmiennych tworzą pierścień $A[x_1, \ldots, x_n x_{n+1}]$ wielomianów $n+1$ zmiennych. Wielomiany n zmiennych wyznaczają odpowiadające im funkcje wielomianowe postaci

$$W(x_1, \ldots, x_n) = \sum_{i_1=0}^{m_1} \cdots \sum_{i_n=0}^{m_n} a_{i_1,\ldots,i_n} x_1^{i_1} \cdot \ldots \cdot x_n^{i_n} \quad (x_1, \ldots, x_n \in A), \tag{1}$$

gdzie $a_{i_1,\ldots,i_n} \in A$ są współczynnikami wielomianu W. Jeżeli $a_{m_1,\ldots,m_n} \neq 0$, to liczbę $m = m_1 + \cdots + m_n$ nazywamy *stopniem* wielomianu (1).

Jednym z ważniejszych zadań algebry jest rozwiązywanie układów równań algebraicznych postaci

$$W_1(x_1, \dots x_n) = \dots = W_k(x_1, \dots, x_n) = 0, \tag{2}$$

gdzie W_j są wielomianami wielu zmiennych. Do układów tej postaci powrócimy później. Zauważmy tylko, że układy (2) są tym łatwiejsze do rozwiązania im niższe są stopnie wielomianów W_j. Obniżanie stopni wielomianów jest stosunkowo proste w przypadku, gdy są one *symetryczne*, tj. gdy ich współczynniki $a_{i_1,\dots,i_n}$ spełniają warunek

$$a_{i_{\tau(1)},\dots,i_{\tau(n)}} = a_{i_1,\dots,i_n} \tag{3}$$

dla dowolnej permutacji $\tau \in S_n$. Przykładami takich wielomianów są tzw. *elementarne wielomiany symetryczne* $\sigma_1, \dots, \sigma_n$ określone wzorami

$$\sigma_j(x_1, \dots, x_n) = \sum_{i_1 < \dots < i_j} x_{i_1} \cdot \dots \cdot x_{i_j}. \tag{4}$$

Np., dla $n = 2$ mamy

$$\sigma_1(x, y) = x + y, \quad \sigma_2(x, y) = xy,$$

zaś dla $n = 3$

$$\sigma_1 = x + y + z, \ \sigma_2 = xy + xz + yz, \ \sigma_3 = xyz.$$

Przy rozwiązywaniu algebraicznych układów symetrycznych istotną rolę odgrywa fakt następujący:

Twierdzenie. *Dla każdego wielomianu symetrycznego W (n zmiennych) istnieje dokładnie jeden wielomian P (n zmiennych) taki, że*

$$W(x_1, \dots, x_n) = P(\sigma_1(x_1, \dots, x_n), \dots, \sigma_n(x_1, \dots, x_n)) \tag{5}$$

dla wszystkich $x_1, \dots, x_n$. □

Dowód tego twierdzenia pomijamy.

Przykłady. Dla dwu i trzech zmiennych mamy np.

$$x^2 + y^2 = \sigma_1^2 - 2\sigma_2, \ x^2 + y^2 + z^2 = \sigma_1^2 - 2\sigma_2,$$

$$x^3 + y^3 = \sigma_1^3 - 3\sigma_1 \cdot \sigma_2.$$

Ogólniej, dla dowolnego n, $x_1, \dots, x_n$ i $t \in \mathbb{C}$ mamy

$$(1 + tx_1)(1 + tx_2) \cdot \dots \cdot (1 + tx_n) = \sum_{j=0}^{n} t^j \sigma_j(x_1, \dots, x_n). \tag{6}$$

W szczególności,

$$\begin{aligned}
&\sum_{m=0}^{n} \sigma_m(x_1^2,\ldots,x_n^2) = (1+x_1^2)\cdot\ldots\cdot(1+x_n^2)\\
&= [(1+ix_1)\cdot\ldots\cdot(1+ix_n)]\cdot[(1-ix_1)\cdot\ldots\cdot(1-ix_n)]\\
&= \left(\sum_{j=0}^{n} i^j\sigma_j(x_1,\ldots,x_n)\right)\cdot\left(\sum_{k=0}^{n}(-i)^k\sigma_k(x_1,\ldots,x_n)\right)\\
&= \sum_{l=0}^{2n}\sum_{j+k=l}(-1)^k\, i^{j+k}(\sigma_j\sigma_k)(x_1,\ldots,x_n)\\
&= \sum_{m=0}^{n}\sum_{j+k=2m}(-1)^{(k+m)}(\sigma_j\sigma_k)(x_1,\ldots,x_n).
\end{aligned}$$

Stąd

$$\sigma_m(x_1^2,\ldots,x_n^2) = (\sigma_m^2 + 2\sum_{k=1}^{m}(-1)^k\sigma_{m-k}\sigma_{m+k})(x_1,\ldots x_n).$$

Na przykład,

$$\begin{aligned}
&x_1^2+\cdots+x_n^2 = \sigma_1(x_1^2,\ldots,x_n^2) = \sigma_1^2 + (-1)^{(1+2)}\sigma_0\sigma_2\\
&= \sigma_1^2 - 2\sigma_2 = (x_1+\cdots+x_n)^2 - 2(x_1x_2+\cdots+x_{n-1}x_n).
\end{aligned}$$

Ogólnie, jeśli $\tau_k = \sum_{k=1}^{n} x_i^k$, to spełnione są tzw. *tożsamości Girarda-Newtona*:

$$\tau_k - \tau_{k-1}\sigma_1 + \cdots + (-1)^{k-1}\tau_1\sigma_{k-1} + (-1)^k k\sigma_k = 0, \quad k = 1,\ldots,n$$

pozwalające wyrazić funkcje τ_k w zależności od σ_j i odwrotnie (zob. np.: D G. Mead, *Newton identities*, American Mathematical Monthly, **99** (1992), 749 – 751):

$$\tau_k = \det\begin{bmatrix}
\sigma_1 & 1 & 0 & \ldots & 0 & 0\\
2\sigma_2 & \sigma_1 & 1 & \ldots & 0 & 0\\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots\\
(k-1)\sigma_{k-1} & \sigma_{k-2} & \sigma_{k-3} & \ldots & \sigma_1 & 1\\
k\sigma_k & \sigma_{k-1} & \sigma_{k-2} & \ldots & \sigma_2 & \sigma_1
\end{bmatrix}$$

oraz

$$\sigma_k = \frac{1}{k!}\cdot\det\begin{bmatrix}
\tau_1 & 1 & 0 & \ldots & 0 & 0\\
\tau_2 & \tau_1 & 2 & \ldots & 0 & 0\\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots\\
\tau_{k-1} & \tau_{k-2} & \tau_{k-3} & \ldots & \tau_1 & k-1\\
\tau_k & \tau_{k-1} & \tau_{k-2} & \ldots & \tau_2 & \tau_1
\end{bmatrix}$$

Rozdział 4. Przestrzenie wektorowe

1. Definicja i przykłady.

Przypomnijmy, że *przestrzenią wektorową* (lub *przestrzenią liniową*) nad ciałem F nazywamy układ $(V, +, \cdot)$, gdzie $+$ jest działaniem wewnętrznym w zbiorze V, zaś $\cdot : F \times V \to V$ - działaniem zewnętrznym, przy czym spełnione są następujące warunki:

(1) $\forall u, v, w \in V : u + (v + w) = (u + v) + w$,
(2) $\forall v, w \in V : v + w = w + v$,
(3) $\exists \theta \in V : \forall v \in V : \theta + v = v + \theta = v$,
(4) $\forall v \in V : \exists - v \in V : v + (-v) = (-v) + v = \theta$,
(5) $\forall a \in F : \forall v, w \in V : a \cdot (v + w) = a \cdot v + a \cdot w$,
(6) $\forall a, b \in F : \forall v \in V : (a + b) \cdot v = a \cdot v + b \cdot v$,
(7) $\forall a, b \in F : \forall v \in V : (ab) \cdot v = a \cdot (b \cdot v)$,
(8) $\forall v \in V : 1 \cdot v = v$.

Elementy przestrzeni wektorowej nazywamy *wektorami*, $-v$ nazywamy wektorem *przeciwnym* do v, wektor θ nazywamy *zerowym*. Powyższe własności działań wektorowych są zgodne z "obrazkową" intuicją, gdzie dwa wektory ("strzałki") uznaje się za identyczne, gdy są równoległe, zgodnie skierowane i mają tę samą długość. Np., przemienność (2) dodawania wektorów widać na rysunku równoległoboku z jedną przekątną.

Przykłady. $F^n = F \times \cdots \times F$ (n czynników) jest przestrzenią wektorową dla dowolnego $n = 1, 2, \ldots$. Zbiór wszystkich funkcji $f : X \to F$, gdzie X jest ustalonym zbiorem, stanowi przestrzeń wektorową. Zbiór wszystkich funkcji ciągłych $f : X \to \mathbb{R}$, gdzie X jest przestrzenią metryczną stanowi przestrzeń wektorową. Zbiór $\mathcal{M}(m, n)$ wszystkich *macierzy* postaci

$$A = [a_{ij}] = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{bmatrix} \tag{1}$$

o wyrazach $a_{ij} \in F$ (m i n są tu ustalonymi liczbami naturalnymi określającymi odpowiednio liczbę *wierszy* i *kolumn* macierzy) stanowi przestrzeń wektorową z dodawaniem i mnożeniem "wyraz po wyrazie":

$$[a_{ij}] + [b_{ij}] = [a_{ij} + b_{ij}], \quad c \cdot [a_{ij}] = [c \cdot a_{ij}]. \tag{2}$$

2. Baza i wymiar.

Wektory $v_1, \ldots, v_n$ przestrzeni wektorowej V nad F nazywamy *liniowo zależnymi*, gdy istnieją nieznikające jednocześnie ($\sum a_i^2 > 0$) współczynniki $x_1, \ldots, x_n \in F$, dla których liniowa kombinacja $x_1 v_1 + \cdots + x_n v_n$ jest wektorem zerowym. Wektory te są *liniowo niezależne*, gdy nie są liniowo zależne, tj. gdy

$$\sum x_i v_i = \theta \;\Rightarrow\; x_1 = \cdots = x_n = 0. \tag{1}$$

Z powyższej definicji wynika łatwo, że dopisanie wektora do wektorów liniowo zależnych pozostawia je liniowo zależnymi, podczas gdy usunięcie wektora spośród

wektorów liniowo niezależnych pozostawia je niezależnymi. Dowolny (być może nieskończony) podzbiór W przestrzeni V jest *liniowo niezależny*, gdy każdy skończony podzbiór zbioru W składa się z wektorów liniowo niezależnych.

Przykłady. Wektory $v = (a, b)$ i $w = (c, d)$ przestrzeni $\mathbb{R}^2$ są liniowo niezależne wtedy i tylko wtedy, gdy $ad - bc \neq 0$. Wektory $e_i = (\delta_i^1, \dots \delta_i^n)$ przestrzeni $\mathbb{R}^n$ są liniowo niezależne. Ogólnie, wektory $v_i = (a_{i1}, \dots, a_{in})$, $i = 1, \dots, m$, przestrzeni $\mathbb{R}^n$ są liniowo niezależne wtedy i tylko wtedy, gdy jedynym rozwiązaniem układu równań liniowych

$$a_{i1}x_1 + \dots a_{in}x_n = 0, \quad i = 1, \dots, m, \tag{2}$$

o niewiadomych $x_1, \dots, x_n$ jest układ $x_1 = \dots x_n = 0$. Dowolny zbiór wektorów zawierający wektor zerowy jest liniowo zależny. W przestrzeni wielomianów nad (na przykład) $\mathbb{R}$ wielomiany

$$x \mapsto x^n, \quad n = 0, 1, 2, \dots, \tag{3}$$

tworzą nieskończony zbiór liniowo niezależny. Podobnie, w przestrzeni wielomianów trygonometrycznych (nad $\mathbb{R}$) funkcje

$$x \mapsto \sin nx, \quad x \mapsto \cos nx, \quad n = 0, 1, 2, \dots, \tag{4}$$

są liniowo niezależne. W przestrzeni wszystkich funkcji $f : X \to \mathbb{R}$ niezależne są funkcje δ_a ($a \in A \subset X$) zwane *deltą Diraca* i określone wzorem

$$\delta_a(x) = \begin{cases} 1, \text{ gdy } & x = a, \\ 0, \text{ gdy } & a \neq x \in X. \end{cases}$$

Wektory liniowo niezależne $v_1, \dots v_n$ tworzą *bazę* przestrzeni wektorowej V, gdy każdy wektor $v \in V$ można przedstawić jako ich liniową kombinację:

$$\forall v \in V : \exists x_1, \dots x_n \in F : v = \sum x_i v_i. \tag{5}$$

Z liniowej niezależności wektorów bazy wynika, że przedstawienie wektora v w postaci ich liniowej kombinacji jest jednoznaczne. Ponadto, baza jest maksymaknym układem wektorów liniowo niezależnych: Jeżeli wektory $v_1, \dots v_n$ tworzą bazę i $v \in V$, to wektory $v, v_1, \dots v_n$ są liniowo zależne. (Istotnie, jeżeli przedstawimy v w postaci (5), to $(-1) \cdot v + x_1 v_1 + \dots + x_n v_n = \theta$ i $-1 \neq 0$.) Jest też odwrotnie: każdy maksymalny układ $v_1, \dots v_n$ liniowo niezależny jest bazą. (Rzeczywiście, jeżeli $v \in V$, to układ $v, v_1, \dots, v_n$ jest liniowo zależny, a więc $xv + \sum x_i v_i = \theta$ dla pewnych nieznikających jednocześnie współczynników $x, x_1, \dots, x_n$. Ponieważ wektory $v_1, \dots, v_n$ są liniowo niezależne, więc $x \neq 0$ i

$$v = -\frac{x_1}{x} v_1 + \dots - \frac{x_n}{x} v_n \tag{6}$$

jest liniową kombinacją wektorów $v_1, \dots, v_n$.)

Nie każda przestrzeń wektorowa posiada bazę. Jeżeli przestrzeń V posiada bazę $v_1, \dots v_n$, to liczb ce n (liczbę elementów bazy) nazywamy *wymiarem* przestrzeni V i oznaczamy symbolem $\dim V$ (dimension = wymiar (ang., franc.)). Tak więc, $\dim F^n = n$ i $\dim \mathcal{M}(m, n) = mn$ dla dowolnych m i n. Przestrzeń nie posiadającą bazy nazywamy *nieskończeniewymiarową*. Są takimi np. przestrzeń wszystkich funkcji rzeczywistych określonych na dowolnym zbiorze nieskończonym, przestrzeń wszystkich wielomianów lub wielomianów trygonometrycznych nad $\mathbb{R}$.

Powyższa definicja wymiaru wymaga sprawdzenia jej poprawności:

Twierdzenie. *Jeżeli* $v = \{v_1, \dots v_m\}$ *i* $w = \{w_1, \dots w_n\}$ *są bazami tej samej przestrzeni* V*, to* $m = n$*.*

Dowód. Przypuśćmy, że $m > n$. Wiemy, że v_1 jest liniową kombinacją wektorów bazy v: $v_1 = a_{11}w_1 + \cdots + a_{1n}w_n$. Ponieważ $v_1 \neq \theta$, więc np. $a_{1n} \neq 0$. Wtedy

$$w_n = \frac{1}{a_{1n}}v_1 - \frac{a_{11}}{a_{1n}}w_1 - \cdots - \frac{a_{1,n-1}}{a_{1n}}w_{n-1}, \tag{7}$$

a więc każdy wektor przestrzeni V jest liniową kobinacją wektorów $v_1, w_1, \dots, w_{n-1}$. W szczególności,

$$v_2 = b_{21}v_1 + a_{21}w_1 + \cdots + a_{2,n-1}w_{n-1}. \tag{8}$$

Poniewż wektory v_1, v_2 są liniowo niezależne, więc jeden ze współczynników a_{2j}, np. $a_{2,n-1}$, jest różny od zera. Wtedy każdy wektor przestrzeni V można przedstawić jako liniową kombinację wektorów $v_1, v_2, w_1, \dots, w_{n-2}$. Kontynuując to postępowanie (i korzystając z zasady indukcji) dochodzimy do wniosku , że każdy wektor przestrzeni V jest liniową kombinacją wektorów $v_1, \dots, v_n$. Przedstawiając w tej postaci wektor v_{m+1} dochodzimy do wniosku, że wektory $v_1, \dots, v_{m+1}$ są liniowo zależne. Sprzeczność. □

Przestrzeń wektorowa V skończonego wymiaru posiada wiele baz. Weźmy dwie, $v = (v_1, \dots, v_n)$ i $w = (w_1, \dots, w_n)$. Dla każdego $i \leq n$ wektor w_i jest liniową kombinacją wektorów bazy v,

$$w_i = a_{i1}v_1 + \cdots + a_{in}v_n, \tag{9}$$

przy czym współczynniki a_{ij} są wyznaczone jednoznacznie. Współczynniki te tworzą macierz kwadratową $A = [a_{ij}] \in \mathcal{M}(n, n)$ zwaną *macierzą przejścia* od bazy v do w. Jeżeli $u = (u_1, \dots u_n)$ jest trzecią bazą tej przestrzeni, $B = [b_{jk}]$ jest macierzą przejścia od w do u, a $C = [c_{ik}]$ macierzą przejścia od v do u, to macierz A, B i C są ze sobą związane warunkiem

$$c_{ik} = \sum_{j=1}^{n} a_{ij}b_{jk}, \quad i, k = 1, \dots, n. \tag{10}$$

W tej sytuacji mówimy, że macierz C jest iloczynem macierzy A i B:

$$C = A \cdot B. \tag{11}$$

Z określenia mnożenia macierzy wynika łatwo (sprawdzić !), że jest ono działaniem łącznym, a *macierz jednostkowa* $I = [\delta_{ij}]$ (macierz przejścia od bazy v do v) jest jego elementem neutralnym. Nie każda macierz $A \in \mathcal{M}(n, n)$ posiada element odwrotny. Macierze odwracalne tworzą grupę $\mathrm{GL}(n)$ zwanną *grupą liniową*.

3. Przekształcenia liniowe.

Przekształcenie $f : V \to W$ przestrzeni wektorowej V w przestrzeń wektorową W (nad tym samym ciałem F) nazywamy *liniowym*, gdy dla dowolnych $v, w \in V$ i $a, b \in F$ spełniony jest warunek

$$f(av + bw) = af(v) + bf(w). \tag{1}$$

Warunek ten równoważny jest koniunkcji dwu następujących:

$$f(v+w) = f(v) + f(w), \quad f(av) = af(v). \tag{2}$$

Każde przkształcenie liniowe spełnia też warunki

$$f(\theta) = \theta \ \text{ i } \ f(-v) = -f(v). \tag{3}$$

Podobnie jak dla grup, różnowartościowe przekształcenei liniowe nazywamy *monomorfizmem*, przekształcenie liniowe przestrzeni V na W nazywamy *epimorfizmem*, przekształcenie liniowe będące jednocześnie monomorfizmem i epimorfizmem nazywamy *izomorfizmem*. Przekształcenie takie jest odwracalne, przy czym przekształcenie odwrotne jest też liniowe. Przekształcenia liniowe przestrzeni liniowej w siebie nazywamy *endomorfizmami*.

Z określeń wynika łatwo, że złożenie przekształceń liniowych (odp., monomorfizmów, epimorfizmów, izomorfizmów czy endomorfizmów) jest przekształceniem liniowym (odp., mono-, epi-, izo- czy endo-morfizmem). Istotnie, jeżeli $f : U \to V$ i $g : V \to W$ są liniowe, $a, b \in F$ i $v, w \in U$, to

$$\begin{aligned}(g \circ f)(av + bw) &= g(f(av + bw)) = g(af(v) + bf(w)) \\ &= ag(f(v)) + bg(f(w)) = a(g \circ f)(v) + b(g \circ f)(w).\end{aligned} \tag{4}$$

Przykłady. Każde przekształcenie liniowe $f : F \to F$ jest postaci

$$f(x) = ax \quad (x \in F), \tag{5}$$

gdzie $a = f(1)$. Jeżeli $f : F^m \to F^n$ jest liniowe, $v = (v_1, \dots v_m)$ jest bazą przestrzeni V, $w = (w_1, \dots w_n)$ jest bazą przestrzeni W i $f(v_i) = a_{i1}w_1 + \cdots + a_{in}w_n$ dla $i \leq m$, to dla dowolnego $v = x_1v_1 + x_mv_m$ mamy

$$f(v) = \sum_{i=1}^{m} \sum_{j=1}^{n} x_i a_{ij} w_j. \tag{6}$$

Odwrotnie, każde przekształcenie określone wzorem (6) dla dowolnej macierzy $A = [a_{ij}]$ jest liniowe. Dla ustalonych baz v i w mamy więc wzajemnie jednoznaczną odpowiedniość $f \leftrightarrow A$ między przekształceniami liniowymi $V \to W$, a macierzami $A \in \mathcal{M}(m, n)$. Ponieważ przekształcenia liniowe można w naturalny sposób dodawać i mnożyć przez skalary, więc zbiór $\mathrm{L}(V, W)$ wszystkich przekształce ń liniowych $V \to W$ stanowi przestrzeń liniową. Jeżeli $\dim V = m$ i $\dim W = n$, to przestrzeń ta jest izomorficzna z $\mathcal{M}(m, n)$.

W szczególności, przekształcenie liniowe $\mathbb{R}^m \to \mathbb{R}^m$ odpowiadające macierzy λI jest podobieństwem o skali $|\lambda|$. Dla $\lambda = -1$ otrzymujemy symetrię o środku $(0, \dots, 0)$. Dla $m = 2$, $v = w = (e_1, e_2)$ przekształcenie o macierzy

$$\begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix} \tag{7}$$

jest obrotem o kąt α.

Złożeniu $g \circ f$ przekształceń liniowych $f : U \to V$ i $g : V \to W$ o macierzach $A = [a_{ij}] \in \mathcal{M}(m,n)$ i $B = [b_{jk}] \in M(n,p)]$ w bazach u, v i w przestrzeni U, V i W odpowiada macierz

$$C = A \cdot B = [c_{ik}] = \left[\sum_j a_{ij} b_{jk} \right] \tag{8}$$

nazywana - jak poprzednio - *iloczynem* macierzy A i B. Zauważmy, że iloczyn ten jest określony wtedy, gdy liczba kolumn macierzy A jest równa liczbie wierszy macierzy B. Mówimy krótko, że elementami macierzy $C = A \cdot B$ są iloczyny wierszy macierzy A przez kolumny macierzy B. Zauważmy wreszcie, że jeżeli $A \in \mathcal{M}(m,n)$, $B \in \mathcal{M}(n,p)$ i $C \in \mathcal{M}(p,r)$, to $AB \in \mathcal{M}(m,p)$, $BC \in \mathcal{M}(n,r)$ oraz

$$(AB)C = A(BC) \in \mathcal{M}(m,r). \tag{9}$$

4. Podprzestrzenie, przestrzenie ilorazowe.

Podzbiór W przestrzeni wektorowej V nazywamy *podprzestrzenią*, gdy dla dowolnych $v, w \in W$ i dowolnych skalarów a, b liniowa kombinacja $av + bw$ należy do W (równoważnie, gdy $v+w \in W$ i $av \in W$ o ile $v, w \in W$ i a jest skalarem). Zbiór W z działaniami dodawania wektorów i mnożenia wektorów przez skalary ograniczonymi do elementów z W jest przestrzenią wektorową.

Przykłady. Dla dowolnego niepustego podzbioru $A \subset V$ zbiór wszystkich liniowych kombinacji wektorów z A jest najmniejszą podprzestrzenią przestrzeni V zawierającą A. Nazywamy ją podprzestrzenią *generowaną* przez A i oznaczamy symbolem $\mathrm{Lin}(A)$. Jeżeli zbiór A jest sk'nczony, $A = \{v_1, \ldots, v_k\}$, a wektory v_j są liniowo niezależne, to $\dim \mathrm{Lin}(A) = k$.

Jeżeli W_1 i W_2 są podprzestrzeniami przestrzeni V, to podprzestrzeń $W = \mathrm{Lin}(W_1 \cup W_2)$ nazywamy *sumą* podprzestrzeni W_i i piszemy $W = W_1 + W_2$. Część wspólna podprzestrzeni W_1 i W_2 jest też podprzestrzenią. Jeżeli $W_1 \cap W_2 = \{0\}$, to przestrzeń W nazywamy *sumą prostą* podprzestrzeni W_i i piszemy $W = W_1 \oplus W_2$. Jeżeli $\dim W_i = k_i$, to $\dim (W_1 \oplus W_2) = k_1 + k_2$. Ogólniej, $\dim (W_1 + W_2) = k_1 + k_2 - k$, gdzie $k = \dim W_1 \cap W_2$.

Dla dowolnego przekształcenia liniowego $f : V \to W$ zbiory $\ker(f) = f^{-1}(\{0\}) \subset V$ i $\mathrm{im}(f) = f(V) \subset W$ są podprzestrzeniami zwanymi, odpowiednio, *jądrem* i *obrazem* przekształcenia f. Z przyjętych określeń wynika, że f jest epimorfizmem, gdy $\mathrm{im}(f) = W$, a monomorfizmem, gdy $\ker(f) = \{0\}$.

Jeeli W jest podprzestrzenią V, to relacja

$$v \equiv w \Leftrightarrow v - w \in W \tag{1}$$

jest równoważnością zgodną z działaniami w V. Zgodnie z ogólną teorią struktur algebraicznych wzory

$$[v] + [w] = [v + w], \quad a[v] = [av] \quad (v, w \in V,\ a \in F) \tag{2}$$

są dobrze określone i nadają zbiorowi $V/\equiv$ strukturę przestrzeni wektorowej nazywanej *przestrzenią ilorazową* i oznaczanej symbolem V/W.

Twierdzenie 1. *Jeżeli* $\dim V = n$ *i* $\dim W = m$*, to* $\dim V/W = n - m$*.*

Dowód. Wybierzmy bazę $v_1, \ldots, v_n$ przestrzeni V tak, by $v_1, \ldots v_m \in W$. Klasy $[v_{m+1}], \ldots, [v_n]$ tworzą bazę przestrzeni ilorazowej: Ponieważ $[v_i] = \theta$ dla $i \leq m$, więc każdy element przestrzeni V/W jest ich liniową kombinacją, a ponieważ równość

$$a_{m+1}[v_{m+1}] + \cdots + a_n[v_n] = [a_{m+1}v_{m+1} + \cdots + a_n v_n] = \theta \tag{3}$$

zachodzi wtedy, gdy $a_{m+1}v_{m+1} + a_n v_n \in W$, a więc gdy $a_{m+1} = \cdots = a_n = 0$, wię są one liniowo niezależne. □

Twierdzenie 2. *Dla dowolnego przekształcenia liniowego* $f : V \to W$ *przestrzenie* $\mathrm{im}(f)$ *i* $V/\ker(f)$ *są izomorficzne.*

Dowód. Podobnie jak w przypadku grup izomorfizmem jest przyporządkowanie

$$V/U \ni [v] \mapsto f(v) \tag{4}$$

($U = \ker(f)$) jest pożądanym izomorfizmem. □

Rozdział 5. Układy równań liniowych

1. Wyznacznik.

Niech $A = [a_{ij}, i, j \leq n]$ będzie macierzą kwadratową o elementach z ciała F. Przypomnijmy, że dla dowolnej permutacji $\sigma \in S_n$ $\mathrm{sgn}(\sigma)$ (znak permutacji) wynosi $(-1)^k$, gdzie k jest liczbą wszystkich inwersji w ciągu $(\sigma(1), \ldots, \sigma(k))$. *Wyznacznikiem* macierzy A nazywamy liczbę

$$\det A = |A| = \sum_{\sigma \in S_n} \mathrm{sgn}\sigma \cdot a_{1\sigma(1)} a_{2\sigma(2)} \cdot \ldots \cdot a_{n\sigma(n)}. \tag{1}$$

Na przykład, dla $n = 2$ mamy $\det A = a_{11}a_{22} - a_{12}a_{21}$.

Obliczanie wyznaczników wyższych stopni wymaga poznania ich własności.

Twierdzenie 1. *(i) Wyznacznik macierzy $A^\top$ transponowanej ($A^\top = [a_{ji}]$, gdy $A = [a_{ij}]$) jest równy* $\det A$. *(ii) Jeżeli macierz B powstaje z A przez zamianę kolumn lub wierszy, to* $\det B = -\det A$. *(iii) Jeżeli dwie kolumny (lub dwa wiersze) macierzy A są równe, to* $\det A = 0$. *(iv) Jeżeli jedna z kolumn lub jeden z wierszy macierzy A składa się z samych zer, to* $\det A = 0$. *(v) Jeżeli macierz B powstaje a A przez dodanie do jednej z kolumn (odp., wierszy) kombinacji liniowej innych kolumn (odp., wierszy) to* $\det B = \det A$.

Dowód. (i) Ponieważ $\mathrm{sgn}\sigma = \mathrm{sgn}\sigma^{-1}$, więc

$$\begin{aligned} \det A^\top &= \sum_{\sigma \in S_n} \mathrm{sgn}\sigma a_{\sigma(1)1} \ldots a_{\sigma(n)n} \\ &= \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma^{-1}) a_{1\sigma^{-1}(1)} \ldots a_{n\sigma^{-1}(n)} = \det A. \end{aligned} \tag{2}$$

(ii) Przeprowadzimy dowód w przypadku, gdy $B = [b_{ij}]$ powstaje z $A = [a_{ij}]$ przez zamianę dwu pierwszych kolumn, tj. gdy $b_{1j} = a_{2j}$, $b_{2j} = a_{1j}$ i $b_{ij} = a_{ij}$ dla $i > 2, i = 1, \ldots, n$. Oznaczmy przez τ transpozycję $(1, 2, \ldots, n) \mapsto (2, 1, \ldots n)$ i zauważmy, że przyporządkowanie $\sigma \mapsto \tau \circ \sigma$ jest bijekcją zbioru S_n na siebie oraz, że $\mathrm{sgn}(\tau \circ \sigma) = -\mathrm{sgn}\sigma$ dla wszystkich permutacji $\sigma \in S_n$. Zatem

$$\begin{aligned} \det B &= \sum_{\sigma \in S_n} \mathrm{sgn}\sigma a_{2\sigma(1)} a_{1\sigma(2)} a_{3\sigma(3)} \ldots a_{n\sigma(n)} \\ &= -\sum_{\sigma \in S_n} \mathrm{sgn}(\tau \circ \sigma) a_{1\tau(\sigma(1))} a_{2\tau(\sigma(2))} \ldots a_{n\tau(\sigma(n))} = -\det A. \end{aligned} \tag{3}$$

(iii) Teza wynika z (ii) i stąd, że przestawienie identycznych kolumn (wierszy) nie zmienia macierzy.

(iv) Jeżeli jedna z kolumn składa się z zer, to każdy ze składników sumy (1) zeruje się.

(v) Jeżeli np. $b_{1i} = a_{1i} + x a_{2i}$ dla $i = 1, \ldots, n$, to

$$\begin{aligned} \det B &= \sum_{\sigma \in S_n} \mathrm{sgn}\sigma \cdot (a_{1\sigma(1)} + x a_{2\sigma(1)}) a_{2\sigma(2)} \cdot \ldots \cdot a_{n\sigma(n)} \\ &= \sum_{\sigma \in S_n} \mathrm{sgn}\sigma \cdot a_{1\sigma(1)} a_{2\sigma(2)} \cdot \ldots \cdot a_{n\sigma(n)} \\ &\quad + x \sum_{\sigma \in S_n} \mathrm{sgn}\sigma \cdot a_{2\sigma(1)} a_{2\sigma(2)} \cdot \ldots \cdot a_{n\sigma(n)} = \det A, \end{aligned} \tag{4}$$

ponieważ druga z ostatnich sum równa jest wyznacznikowi macierz o dwu jednakowych kolumnach. □

Następne twierdzenie daje metodę sprowadzania obliczania wyznaczników stopnia n do obliczania wyznaczników stopnia $n-1$ metodą tzw. *rozwinięcia Laplace'a*.

Twierdzenie 2. *Dla dowolnego $i = 1, 2, \ldots n$ i dowolnej macierzy kwadratowej A stopnia n zachodzi równość*

$$\det A = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} A_{ij}, \tag{5}$$

gdzie A_{ij} jest wyznacznikiem macierzy powstałej a A poprzez skreślenie i-tej kolumny i j-ego wiersza.

Wyznaczniki A_{ij} (podobnie jak i wynaczniki macierzy otrzymanych z A poprzez skreślenie pewnej liczby kolumn i wierszy) nazywamy *minorami* macierzy A.

Dowód. Z twierdzenia 1 wynika, że wystarczy przeprowadzić dowód dla $i = n$. Dla każdego $j = 1, \ldots, n$ oznaczmy przez Σ_j zbiór wszystkich permutacji $\sigma \in S_n$, dla których $\sigma(n) = j$. Wtedy

$$\det A = \sum_{j=1}^{n} a_{nj} \cdot \sum_{\sigma \in \Sigma_j} \operatorname{sgn}\sigma \cdot a_{1\sigma(1)} \cdot \ldots \cdot a_{n-1,\sigma(n-1)} = \sum_{j=1}^{n} (-1)^{n+j} a_{nj} A_{nj}. \tag{6}$$

Ostatnią równość otrzymujemy z określenia wyznacznika A_{nj} poprzez porównanie znaku permutacji σ ze znakiem odpowiedniej permutacji $(n-1)$-elementowej. □

Uwaga. Z ostatnich dwu twierdzeń wynika, że również

$$\det A = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} A_{ij} \tag{7}$$

dla $j = 1, \ldots, n$.

Twierdzenie 3. *Dla dowolnych macierzy $A \in \mathcal{M}(m)$, $B \in \mathcal{M}(n)$ i $C \in \mathcal{M}(m, n)$ wyznacznik macierzy*

$$\begin{bmatrix} A & C \\ 0 & B \end{bmatrix} \tag{8}$$

wynosi $\det A \cdot \det B$.

(Zerem oznaczyliśmy tu macierz z $\mathcal{M}(n, m)$ o wszystkich wyrazach zerowych.)

Dowód. Przeprowadzimy indukcję ze względu na n.

Dla $n = 1$ odpowiednia równość wynika z twierdzenia 2 poprzez rozwinięcie wzdłuż ostatniego wiersza.

P.S. Laplace (1749–1827) - matematyk, fizyk i astronom francuski.

Przypuśćmy, że nasza równość jest spełniona dla macierzy B z $\mathcal{M}(n-1)$ i weźmy macierz $B \in \mathcal{M}(n)$ oraz dokonajmy rozwinięcia wyznacznika macierzy (8) względem ostatniego wiersza. Otrzymamy sumę postaci

$$\sum_{j=n+1}^{n+m} (-1)^{n+m+i} b_{n,j-m} D_j, \tag{9}$$

gdzie D_i jest wyznacznikiem macierzy postaci (8) otrzymanej przez skreślenie ostatniego wiersza i $(n+j)$-tej kolumny. Z założenia indukcyjnego wynika, że $D_j = \det A \cdot B_{n,j}$, gdzie $B_{n,j}$ jest odpowiednim minorem macierzy B. Zatem wyznacznik macierzy (8) wynosi

$$\sum_{i=1}^{m} (-1)^{n+i} b_{nj} B_{nj} \cdot \det A = \det B \cdot \det A.$$

Indukcja kończy dowód. □

Ostatnie twierdzenie z tej serii pokazuje, że funkcja $\det : \mathcal{M}(n) \to F$ jest homomorfizmem półgrup.

Twierdzenie 4. *Dla dowolnych macierzy $A, B \in \mathcal{M}(n)$ zachodzi równość*

$$\det(A \cdot B) = \det A \cdot \det B. \tag{10}$$

Dowód. Utwórzmy macierz

$$D = \begin{bmatrix} A & -I \\ 0 & B \end{bmatrix}. \tag{11}$$

Z poprzedniego twierdzenia wynika, że

$$\det D = \det A \cdot \det B. \tag{12}$$

Mnożąc kolumny o numerach $n+1, \ldots, 2n$ najpierw przez elementy pierwszej kolumny i dodając otrzymane iloczyny do pierwszej kolumny, potem przez elementy drugiej kolumny i dodając iloczyny do drugiej kolumny itd. stwierdzamy, że

$$\det D = \det \begin{bmatrix} 0 & -I \\ B \cdot A & B \end{bmatrix}.$$

Przestawiając kolumny (i-tą z $(n+i)$-tą dla $i = 1, \ldots, n$) otrzymujemy, że

$$\begin{aligned} \det D &= (-1)^n \det \begin{bmatrix} -I & 0 \\ B & B \cdot A \end{bmatrix} \\ &= (-1)^n \det(-I) \det(B \cdot A) = (-1)^{2n} \det(B \cdot A) = \det(B \cdot A). \end{aligned} \tag{13}$$

Porównując (12) z (13) dostajemy (10) (z A i B zamienionymi miejscami). □

Wniosek. *Macierz $A \in \mathcal{M}(n)$ jest odwracalna wtedy i tylko wtedy, gdy* $\det A \neq 0$.

Dowód. Jeżeli A jest macierzą odwracalną, to

$$\det A \cdot \det A^{-1} = \det(A \cdot A^{-1}) = \det I = 1, \tag{14}$$

skąd wynika że $\det A \neq 0$ (oraz, że $\det(A^{-1}) = (\det A)^{-1}$). Odwrotnie, jeżeli $detA \neq 0$, to macierz $B = [b_{ij}]$ o wyrazach

$$b_{ij} = (-1)^{i+j} \frac{1}{\det A} A_{ji}, \tag{15}$$

gdzie - jak poprzednio - A_{ij} jest minorem macierzy A otrzymanym przez skreślenie i-tego wiersza i j-tej kolumny, jest odwrotna do A. Rzeczywiście, ze wzoru (5) (rozwinięcie Laplace'a) wynika, że $\sum_j a_{ij}b_{ji} = 1$, a jeżeli $i \neq k$, to $\sum_j a_{ij}b_{jk} = (\det A)^{-1} \cdot \det C = 0$, gdzie C jest macierzą otrzymaną z A poprzez zastąpienie k-tego wiersza i-tym. Zatem istotnie $A \cdot B = I$. Podobnie, $B \cdot A = I$. □

2. Układy Cramera.

Rozważmy układ n równań liniowych z n niewiadomymi:

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \cdots \\ a_{n1}x_1 + \cdots + a_{nn}x_n = b_n. \end{cases} \tag{1}$$

Układ (1) nazywamy *układem Cramera*, gdy wyznacznik macierzy współczynników $A = [a_{ij}]$ jest różny od zera. Układ (1) można zapisać w postaci "wektorowej":

$$A \cdot X = B, \tag{2}$$

gdzie $X = (x_1, \ldots, x_n)$ i $B = (b_1, \ldots b_n) \in F^n$. Z "łączności" mnożenia macierzy wynika od razu, że układ Cramera (2) ma dokładnie jedno rozwiązanie

$$X = A^{-1} \cdot B. \tag{3}$$

Ze wzorów określających wyrazy macierzy odwrotnej i z rozwinięcia Laplace'a wynika od razu, że wzoór (3) można przedstawić w postaci

$$x_j = \frac{\det A_j}{\det A}, \quad (j = 1, \ldots, n), \tag{4}$$

gdzie A_i jest macierzą otrzymaną z A poprzez zastąpienie j-tej kolumny kolumną wyrazów wolnych $b_1, \ldots, b_n$. Wzory (4) noszą nazwę *wzorów Cramera*. Ze wzorów tych wynika, że jeèli układ Cramera jest jednorodny ($b_1 = \cdots = b_n = 0$), to jedynym jego rozwiązaniem jest $x_1 = \cdots = x_n = 0$. Innymi słowy, jeżeli $\det A \neq 0$, to kolumny (odp., wiersze) macierzy A są liniowo niezależne. Odwrotnie, jeżeli kolumny (wiersze) macierzy A są liniowo niezależne, to odwzorowanie liniowe odpowiadające macierzy A jest izomorfizmem, jest więc odwracalne, odwracalna jest też macierz A i $\det A \neq 0$. Powyższe rozumowanie dowodzi następującego twierdzenia:

Twierdzenie. *Macierz kwadratowa A ma niezerowy wyznacznik wtedy i tylko wtedy, gdy jej kolumny (wiersze) są wektorami liniowo niezależnymi.* □

3. Rząd macierzy prostokątnej.

Rzędem $rz(A)$ dowolnej macierzy prostokątnej $A = [a_{ij} \in \mathcal{M}(m,n)$ nazywamy maksymalny stopień jej niezerowego minora. Oczywiście, $rz(A) \leq \min\{m,n\}$. Z własności wyznacznika wynika od razu, że

$$rz(A^\top) = rz(A) \tag{1}$$

oraz, że rząd macierzy nie ulega zmianie, jeżeli do jednej z kolumn (jednego z wierszy) dodamy liniową kombinację pozostałych kolumn (wierszy). Operacja taka pozwala stosunkowo łatwo wyznaczać rzędy macierzy poprzez "wyzerowanie" maksymalnej liczby wierszy lub kolumn. Z ostatniego twierdzenia wynika też, że $rz(A)$ jest równy maksymalnej liczbie liniowo niezależnych kolumn (wierszy) macierzy A.

Przykład. Jeżeli

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

to $rz(A) = 2$, bo kolumny $(3,-6)$ i $(-1,7)$ są liniowo niezależne:

$$\det \begin{bmatrix} 3 & -1 \\ -6 & 7 \end{bmatrix} \neq 0.$$

Z powyższej definicji i twierdzenia o wyznaczniku iloczynu macierzy wynika, że

$$rz(AB) \leq rz(A) \cdot rz(B) \tag{2}$$

o ile tylko iloczyn macierzy A i B jest określony. Ponadto, jeżeli A (odp., B) jest macierzą kwadratową nieosobliwą ($\det A \neq 0$), to

$$rz(AB) = rz(B) \quad (\text{odp.}, rz(AB) = rz(A)). \tag{3}$$

4. Ogólne układy równań liniowych.

Rozważmy ogólny układ równań liniowych postaci

$$\begin{cases} a_{11}x_1 + \cdots + a_{1m}x_m = b_1 \\ \cdots \\ a_{n1}x_1 + \cdots + a_{nm}x_m = b_n. \end{cases} \tag{1}$$

Jest to układ n równań z m niewiadomymi o prostokątnej macierzy współczynników $A = [a_{ij}, i \leq n, j \leq m]$. Tak jak poprzednio, można go zapisać w postaci wektorowej

$$A \cdot X = B. \tag{2}$$

Oznaczmy przez A^d tzw. *macierz dołączoną* układu (1) (lub (2)), tj. macierz powstałą z A poprzez dopisanie kolumny wyrazów wolnych $B = (b_1, \ldots, b_n)$.

Twierdzenie. *(Kroneckera - Capellego) Układ (1) posiada rozwiązanie wtedy i tylko wtedy, gdy*

$$rz(A) = rz(A^d). \tag{3}$$

Dowód. Układ (1) posiada rozwiąnie wtedy i tylko wtedy, gdy wektor B jest liniową kombinacją kolumn $A_1, \ldots, A_m$ macierzy A, co ma miejsce wtedy i tylko wtedy, gdy maksymalna liczba liniowo niezależnych wektorów układu $A_1, \ldots A_n$ (równa rzędowi macierzy A) pokrywa się z maksymalną liczbą liniowo niezależnych wektorów układu $A_1, \ldots, A_n, B$ (równą rzędowi macierzy A^d). □

Jeżeli układ (1) jest jednorodny ($b_1 = \cdots = b_n = 0$), to dowolna kombinacja liniowa rozwiązań, jest rozwiązaniem układu (1), a więc rozwiązania tworzą podprzestrzeń wektorową przestrzeni F^m. Podprzestrzeń ta jest jądrem przekształcenia

$$f: \ F^m \ni X \mapsto A \cdot X \in F^n. \tag{4}$$

Kolumny macierzy A należa do obrazu im (f), a każdy element tego obrazu jest ich liniową kombinacją. Wynika stąd, że dim im (f) =rz (A). Z twierdzenia o związku jądra przekształcenia liniowego z jego obrazem wynika, że dim ker $(f) = m-$rz(A). Stąd

Twierdzenie 2. *Rozwiązania układu jednorodnego*

$$\begin{cases} a_{11}x_1 + \cdots + a_{1m}x_m = 0 \\ \ldots \\ a_{n1}x_1 + \cdots + a_{nm}x_m = 0, \end{cases} \tag{5}$$

tworzą przestrzeń wektorową wymiaru $m - rz(A)$. □

Wreszcie, jeżeli $(x_1, \ldots, x_m)$ jest jednym z rozwiązań układu (niejednorodnego) (1), to każde inne jego rozwiązanie można otrzymać dodając doń dowolne rozwiązanie układu jednorodnego (5). Używając terminologii z następnego rozdziału możemy powiedzieć, że *rozwiązania układu* (1) *tworzą przestrzeń afiniczną wymiaru* $m - rz(A)$.

Rozdział 6. Przestrzenie afiniczne

1. Pojęcia podstawowe.

Przestrzenią afiniczną nazywamy układ $(E, V, \overrightarrow{\cdot})$, gdzie E jest zbiorem *punktów*, V jest przestrzenią wektorową, a "strzałka" funkcją $E \times E \to V$ spełniającą następujące warunki:

(1) $\forall A, B, C \in E: \ \overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$,
(2) $\forall A, B \in E: \ \overrightarrow{AB} = \theta \ \Leftrightarrow \ A = B$,
(3) $\forall A \in E: \ \forall v \in V \ \exists B \in E \ \overrightarrow{AB} = v$.

Wymiar przestrzeni wektorowej V uważamy za wymiar przestrzeni afinicznej.

Z powyższych warunków wynika od razu, że

(1) $\forall A, B \in E: \ \overrightarrow{BA} = -\overrightarrow{AB}$,
(2) $\forall A, B, C \in E: \ (\overrightarrow{AB} = \overrightarrow{AC} \Rightarrow B = C$.

Dla dowolnych punktów $A, B \in E$ zbiór

$$\overline{AB} = \{X \in E; \exists t \in [0,1] : \overrightarrow{AX} = t\overrightarrow{AB}\} \tag{1}$$

nazywamy *odcinkiem* (o końcach A i B). Oczywiście, $\overline{AB} = \overline{BA}$. Jeżeli $A \in E$ i $v \in V$, to zbiór

$$l = \{X \in E; \exists t \in \mathbb{R} : \overrightarrow{AX} = tv\} \tag{2}$$

nazywamy prostą o *wektorze kierunkowym* v. Podobnie, zbiór postaci

$$\{X \in E; \exists t \in [0, +\infty) : \overrightarrow{AX} = tv\} \tag{3}$$

nazywamy *półprostą*. Równanie

$$\overrightarrow{AX} = tv \quad (t \in \mathbb{R}) \tag{4}$$

nazywa się *równaniem wektorowym prostej* (2).

Ogólniej, dla dowolnej podprzestrzeni $W \subset V$ i dowolnego punktu $A \in E$ zbiór

$$E' = \{X \in E; \overrightarrow{AX} \in W\} \tag{4}$$

nazywamy *podprzestrzenią afiniczną* przestrzeni E. Zbiór ten wraz z W i funkcją "strzałka" ograniczoną do $E' \times E'$ jest przestrzenią afiniczną. Dwie (różne) podprzestrzenie afiniczne odpowiadające tej samej podprzestrzeni W nazywamy *równoległymi*.

Zgodnie z powyższymi określeniami prosta jest jednowymiarową podprzestrzenią afiniczną. Łatwo widać, że część wspólna podprzestrzeni afinicznych jest taką podprzestrzenią. Np., część wspólna dwu różnych nierównoległych płaszczyzn (tj. podprzestrzeni dwuwymiarowych) w przestrzeni trójwymiarowej jest prostą.

Dwie podprzestrzenie afiniczne odpowiadające dwu podprzestrzeniom wektorowym, z któ rych jedna jest podprzestrzenią drugiej, nazywa się *równoległymi*. Dwie proste są równoległe, gdy mają ten sam wektor kierunkowy. Jeżeli dwie podprzestrzenie afiniczne są równoległe, to albo jedna zawiera się w drugiej, albo są rozłączne (udowodnić !).

2. Zbiory wypukłe.

Podzbiór X przestrzeni afninicznej E nazywamy wypukłym, gdy dla dowolnych punktów $A, B \in X$ odcinek $\overline{AB}$ zawiera się w X. Z definicji wynika od razu, że część wspólna dowolnej rodziny zbiorów wypukłych jest zbiorem wypukłym. W szczególności część wspólną X^c wszystkich zbiorów wypukłych zawierających dany zbiór X nazywa się *otoczką wypukła* zbioru X. X^c jest najmniejszą figurą wypukłą zawierającą X.

Punkty $A_0, A_1, \ldots, A_k$ przestrzeni afinicznej E nazywamy *afinicznie niezależnymi*, gdy wektory

$$\overrightarrow{A_0A_1}, \ldots, \overrightarrow{A_0A_k} \tag{1}$$

są liniowo niezależne. (Zwróćmy uwagę na to, że afiniczna niezależność punktów nie zależy od wyboru wspólnego początku wektorów (1).) Jeżeli punkty $A_0, \ldots, A_k$ są afinicznie niezależne to otoczkę wypukła $\triangle\{A_0, A_1, \ldots A_k\}$ zbioru $\{A_0, A_1, \ldots, A_k\}$ nazywamy *sympleksem k-wymiarowym o wierzchołkach* $A_0, A_1, \ldots A_k$.

Sympleks 0-wymiarowy jest zbiorem jednopunktowym, sympleks 1-wymiarowy - odcinkiem. Sympleks 2-wymiarowy nazywamy *trójkątem*, sympleks 3- wymiarowy - *czworościanem*. Sympleksy postaci $\triangle\{A_{i_0}, \ldots, A_{i_l}\}$ $(i_1 < \cdots < i_l,\ l \leq k)$ nazywamy *ścianami* sympleksu $\triangle\{A_0, A_1, \ldots A_k\}$. Ściany 0-wymiarowe pokrywają się więc z wierzchołkami sympleksu.

Twierdzenie. *$X \in \triangle\{A_0, A_1, \ldots A_k\}$ wtedy i tylko wtedy, gdy*

$$\overrightarrow{A_0X} = \sum_{i=1}^{k} t_i \overrightarrow{A_0A_i} \tag{2}$$

dla pewnych liczb $t_i \geq 0$ takich, że $\sum t_i \leq 1$.

Dowód. (Indukcja ze względu na k.) Dla $k = 0$ twierdzenie jest oczywiste, a dla $k = 1$ wynika bezpośrednio z definicji odcinka.

Przypuśćmy, że twierdzenie jest prawdziwe dla sympleksów $(k-1)$- wymiarowych i weźmy dowolne afinicznie niezależne punkty $A_0, A_1, \ldots, A_k$. Łatwo zauważyć, że $X \in \triangle\{A_0, A_1, \ldots A_k\}$ wtedy i tylko wtedy, gdy $X \in \overline{A_0Y}$ dla pewnego punktu Y sympleksu $\triangle A_1 \ldots A_k$. Z założenia indukcyjnego wynika, że

$$\overrightarrow{A_1Y} = \sum_{i=2}^{k} s_i \overrightarrow{A_1A_i} \tag{3}$$

dla pewnych liczb $s_1 \geq 0$, przy czym $\sum s_i \leq 1$. Z (3) i równości

$$\overrightarrow{A_0X} = t\overrightarrow{A_0Y} \quad (0 \leq t \leq 1) \tag{4}$$

wynika że

$$\begin{aligned}
\overrightarrow{A_0X} &= t\overrightarrow{A_0A_1} + t\overrightarrow{A_1Y} = t\overrightarrow{A_0A_1} + \sum_{i=2}^{k} ts_i\overrightarrow{A_1A_k} \\
&= t\overrightarrow{A_0A_1} + \sum_{i=2}^{k} ts_i(\overrightarrow{A_1A_0} + \overrightarrow{A_0A_k}) \\
&= t(1 - \sum_{i=2}^{k} s_i)\overrightarrow{A_0A_1} + \sum_{i=2}^{k} ts_i\overrightarrow{A_0A_i}. \qquad (5)
\end{aligned}$$

Widać od razu, że współczynniki ostatniej kombinacji liniowej są nieujemne, a ich suma nie przekracza 1. Odwrotnie, jeżeli współczynniki ostatniej kombinacji są nieujemne i ich suma nie przekracza 1, to to samo można powiedzieć o liczbach s_i. $\square$

Skończony zbiór $S = \{s_1, \ldots, s_m\}$ sympleksów nazywamy *kompleksem symplicjalnym*, gdy wszystkie ściany sympleksów z S należa do S, a część wspólna dwu sympleksów z S jest ich wspólną ścianą (lub zbiorem pustym). Np., kompleksem symplicjalnym jest zbiór wszystkich ścian danego sympleksu. Kompleks symplicjalny S nazywamy *triangulacją* zbioru X, gdy $\cup S = X$. Zbiór X nazywamy *wielościanem*, gdy posiada triangulację.

Uwaga. Jeżeli X jest wielościanem, a S jego triangulacją zawierającą b_i-sympleksów i-wymiarowych, to liczbę

$$\chi(X) = \sum (-1)^i b_i \tag{6}$$

nazywamy *charakterystyką Eulera* wielościanu X. Liczba ta nie zależy od wyboru triangulacji S i opisuje w pewien sposób "topologię" wielościanu X. (Przykłady !)

3. Przekształcenia afiniczne.

Niech $E = (P, V, \overrightarrow{\cdot})$ i $E' = (P', V' \overrightarrow{\cdot})$ będą przestrzeniami afinicznymi, $f : P \to P'$. Przekształcenie f nazywamy afinicznym, jeżeli dla pewnego punktu $A \in P$ istnieje przekształcenie liniowe $L : V \to V'$ takie, że dla dowolnego $X \in P$ spełniony jest warunek

$$\overrightarrow{A'X'} = L(\overrightarrow{AX}), \tag{1}$$

gdzie $A' = f(A)$ i $X' = f(X)$. (Można wykazać, że istnienie takiego L jest niezależne od wyboru punktu A.)

Z określenia i odpowiednich własności przekształceń liniowych wynika, że złożenie przekształceń afinicznych jest afiniczne i przekształcenie odwrotne do afinicznego (o ile istnieje) jest afiniczne. Wynika stąd, że różnowartościowe przekształcenia afiniczne przestrzeni E na siebie tworzą grupę. Grupę tę nazywamy *grupą afiniczną* przestrzeni E i oznaczamy symbolem $\mathrm{Aff}(E)$.

Przykłady. Dla dowolnej liczby $t \neq 0$ przekształcenie określone warunkiem

$$\overrightarrow{AX'} = t \cdot \overrightarrow{AX} \tag{2}$$

nazywamy *jednokładnością* o skali t i środku A. Jednokładność o skali -1 nazywamy *symetrią środkową*. Przekształcenie afiniczne odpowiadające przekształceniu liniowemu $L = id_E$ nazywamy *translacją* lub *przesunięciem (równoległym)* o wektor $v = \overrightarrow{AA'}$ (tu wektor v nie zależy od A).

Przekształcenia afiniczne zachowują "strukturę afiniczną" przestrzeni: przekształcają proste w proste, odcinki na odcinki, figury wypukłe na figury wypukłe, wielościany na wielościany.

Twierdzenie. *Jeżeli* $\dim E = n$*, to grupa* $Aff(E)$ *jest izomorficzna z iloczynem* $\mathbb{R}^n \times GL(n)$ *z działaniem określonym wzorem*

$$(x, A) \cdot (y, B) = (x + A \cdot y, A \cdot B). \tag{3}$$

Dowód. Łatwo sprawdzić, że działanie (3) jest łączne, para $(0, I)$ jest jego elementem neutralnym, a para $(-A^{-1} \cdot x, A^{-1})$ – elementem odwrotnym do (x, A).

Ustalmy punkt Q przestrzeni E i bazę $v_1, \ldots, v_n$ stowarzyszonej z E przestrzeni wektorowej V. Każdemu przekształceniu $f \in Aff(E)$ przyporządkujmy taką parę (x, A), że $x = (x_1, \ldots, x_n)$, $\overrightarrow{QQ'} = \sum x_i v_i$, zaś A jest macierzą przekształcenia liniowego L spełniającego warunek (1). Wystarczy pokazać, że przyporządkowanie to jest homomorfizmem grup.

Weźmy w tym celu drugie przekształcenie afiniczne g i odpowiadającą mu parę (y, B). B jest macierzą pewnego przekształcenia liniowego L', takiego, że

$$\overrightarrow{Q''X''} = L'(\overrightarrow{QX}) \tag{4}$$

dla dowolnego punktu X. (Tu $X'' = g(X)$.)

Połóżmy $X''' = f(g(X))$ dla dowolnego X. Wtedy

$$\overrightarrow{Q'''X'''} = L(\overrightarrow{Q''X''} = L(L'(\overrightarrow{QX})) \tag{5}$$

oraz

$$\overrightarrow{QQ'''} = \overrightarrow{QQ'} + \overrightarrow{Q'Q'''} = \overrightarrow{QQ'} + L(\overrightarrow{QQ''}). \tag{6}$$

Przedstawiając wektory w (6) w bazie $v_1, \ldots, v_n$ i pamiętając o tym, że przekształceniu $L \circ L'$ odpowiada macierz $A \cdot B$ wnioskujemy z (5) i (6), że złożeniu $f \circ g$ przyporządkowana została para $(x + A \cdot y, A \cdot B)$.

Ponadto, jeżeli K jest przekształceniem liniowym odpowiadającym przekształceniu f^{-1}, i $\tilde{X} = f^{-1}(X)$, to

$$L(K(\overrightarrow{QX})) = L(\overrightarrow{\tilde{Q}\tilde{X}}) = \overrightarrow{QX},$$

a więc $L \circ K = id$ i w ten sam sposób $K \circ L = id$, tj. $K = L^{-1}$. Wreszcie,

$$L(\overrightarrow{Q\tilde{Q}}) = \overrightarrow{Q'Q} = -\overrightarrow{QQ'},$$

skąd

$$\overrightarrow{Q\tilde{Q}} = -L^{-1}(\overrightarrow{QQ'}).$$

Ostatnie obserwacje dowodzą, że przekształceniu f^{-1} przyporządkowujemy parę $(-A^{-1} \cdot x, A^{-1})$. □

4. Geometria afiniczna.

Zgodnie ze słynnym *programem z Erlangen* F. Kleina (1872), geometria jest nauką o niezmiennikach grup przkształceń. W szczególności, *geometria afiniczna* jest nauką o niezmiennikach grupy przekształceń afinicznych. Do niezmienników takich należy m. in. współliniowość punktów, wypukłość, własność "leżenia między", czy stosunek podziału (mówimy, że punkt X dzieli parę punktów (A, B) w stosunku x, gdy punkty A, B, X są współliniowe i $\overrightarrow{XA} = x \cdot \overrightarrow{XB}$). Znaczna część geometrii elementarnej może być opisana w terminach geometrii afinicznej, geometria ta nie pozwala jednak mierzyć odległości punktów, kątów czy pól figur. Dlatego zachodzi potrzeba wprowadzenia dodatkowej struktury umożliwiającej takie "pomiary'. Jednym z mozliwych podejść do tego problemu jest wprowadzenie tzw. *iloczynu skalarnego* (Rozdział7).

Rozdział 7. Przestrzenie euklidesowe

1. Formy dwuliniowe.

Dla dowolnej przestrzeni wektorowej V nad ciałem F odwzorowanie $g : V \times V \to F$ spełniające warunki

$$g(au + bv, w) = ag(u, w) + bg(v, w),\ g(u, av + bw) = ag(u, v) + bg(u, w) \tag{1}$$

dla dowolnych wektorów $u, v, w \in V$ i dowolnych skalarów $a, b \in F$ nazywamy *formą dwuliniową* na V. Formę g nazywamy *symetryczną*, gdy

$$\forall v, w \in V :\ g(v, w) = g(w, v). \tag{2}$$

Formę symetryczną g nazywamy *niezdegenerowaną*, gdy równość $g(v, w) = 0$ dla wszystkich $w \in V$ implikuje warunek $v = \theta$. Dla formy niezdegenerowanej g na przestrzeni V skończonego wymiaru przyporządkowanie

$$V \ni v \mapsto g(v, \cdot) : V \to F \tag{3}$$

ustala izomorfizm przestrzeni V z przestrzenią V^* wszystkich odwzorowań liniowych $f : V \to F$. (Przestrzeń V^* nazywa się *dualną* lub *sprzężoną* do V.)

Jeżeli $v = \{v_1, \ldots, v_n\}$ jest bazą przestrzeni V, to każda forma dwuliniowa g na V daje się opisać przy pomocy macierzy kwadratowej $A = [a_{ij}]$ o wyrazach $a_{ij} = g(v_i, v_j)$. Forma g jest symetryczna, gdy symetryczna jest macierz A: $A = A^\top$. Forma g jest niezdegenerowana, gdy macierz A jest nieosobliwa: $\det A \neq 0$. Jeżeli $w = \{w_1, \ldots, w_n\}$ jest inną bazą przestrzeni V, C jest macierzą przejścia od bazy v do w: $w_k = \sum c_{ki} v_i$, zaś B jest macierzą formy g w bazie w:$b_{ij} = g(w_i, w_j)$, to macierze A, B i C są związane relacją

$$B = C \cdot A \cdot C^\top. \tag{4}$$

.

Formę symetryczną g na przestrzeni V nad ciałem $\mathbb{R}$ nazywamy *określoną dodatnio* (odp. *ujemnie, nieujemnie* lub *niedodatnio*), gdy dla dowolnego $0 \neq v \in V$ mamy $g(v, v) > 0$ (odp., < 0, ≥ 0 lub ≤ 0). Oczywiście, forma określona dodatnio jest określona nieujemnie, a g jest określona dodatnio wtedy i tylko wtedy, gdy forma $-g$ jest określona ujemnie. Ponadto, forma określona dodatnio lub ujemnie jest niezdegenerowana. Formę symetryczną, dodatnio określoną nazywamy *iloczynem skalarnym* na przestrzeni V.

Następujące twierdzenie daje kryterium dodatniej określoności w terminach macierzy.

Twierdzenie 1. *(Sylwestera) Forma symetryczna g o macierzy A jest określona dodatnio wtedy i tylko wtedy, gdy wszystkie minory główne M_k postaci $M_k = \det[a_{ij}, i, j \leq k]$ są dodatnie.*

Dowód. Przeprowadzimy indukcję ze względu na wymiar n przestrzeni V.

Dla $n = 1$ twierdzenie jest oczywiste: Forma g jest dodatnio określona wtedy i tylko wtedy gdy $g(v_1, v_1) > 0$.

Przypuśćmy, że twierdzenie jest prawdziwe dla przestrzeni wymiaru ¡ n i weźmy formę dwuliniową symetryczną g na przestrzeni V wymiaru n. Oznaczmy przez W

podprzestrzeń przestrzeni V generowaną przez wektory $v_1, \ldots, v_{n-1}$ bazy $v_1, \ldots, v_n$ przestrzeni V. Wybierzmy wektor $w \notin W$ taki, że $g(v_i, w) = 0$ dla $i = 1, \ldots, n-1$. (Istnienie takiego wektora wynika z teorii układów równań liniowych.) Łatwo zauważyć, że forma g jest dodatnio określona na V wyedy i tylko wtedy, gdy jest dodatnio określona na W i $g(w, w) > 0$. Z założenia indukcyjnego wynika, że forma g jest dodatnio określona na W wtedy i tylko wtedy, gdy $M_k > 0$ dla $k = 1, \ldots, n-1$. Pozostaje wykazać, że jeżeli minory $M_1, \ldots, M_{n-1}$ są dodatnie, to $g(w, w) > 0$ wtedy i tylko wtedy, gdy $\det A > 0$.

Jeżeli B jest macierzą formy g w bazie $v_1, \ldots, v_{n-1}, w$, to $\det B = g(w, w) \cdot M_{n-1}$, a z (4) wynika, że $\det B > 0 \Leftrightarrow \det A > 0$. Powiązanie powyższych obserwacji prowadzi do wniosku, że twierdzenie jest prawdziwe dla form na przestrzeniach n wymiarowych.

Indukcja kończy dowód. □

Wniosek. *Forma g o macierzy A jest określona ujemnie wtedy i tylko wtedy, gdy $(-1)^k M_k > 0$ dla $k = 1, \ldots, n$.* □

2. Długość wektora, kąt, prostopadłość.

Niech V będzie przestrzenią wektorową nad $\mathbb{R}$ z iloczynem skalarnym $g = \langle \cdot, \cdot \rangle$. Dla dowolnego $v \in V$ liczbę

$$\|v\| = \sqrt{\langle v, v \rangle} \tag{1}$$

nazywamy *długością* wektora v. Z dodatniej określoności iloczynu g wynika, że wyróżnik

$$4(\langle v, w \rangle^2 - \|v\|^2 \|w\|^2) \tag{2}$$

trójmianu kwadratowego

$$\langle v + xw, v + xw \rangle = \|v\|^2 + 2\langle v, w \rangle + x^2 \|w\|^2 \tag{3}$$

jest niedodatni, a więc spełniona jest tzw. *nierówność Schwarza*

$$|\langle v, w \rangle| \leq \|v\| \cdot \|w\|, \tag{4}$$

przy czym równość w (4) jest możliwa wtedy i tylko wtedy, gdy wyróżnik (2) jest równy zeru, co ma miejsce wtedy, gdy równanie $v + xw = \theta$ ma rozwiązanie, tj. gdy wektory v i w są liniowo zależne.

Z nierówności (4) wynika od razu tzw. *nierówność trójkąta*:

$$|v + w| \leq |v| + |w|. \tag{5}$$

Z nierówności (4) wynika też, że iloraz $\langle v, w \rangle / (|v| \cdot |w|)$ leży w przedziale $(-1, 1)$, co umożliwia zdefiniowanie go jako *cosinus kąta między wektorami* v i w:

$$\cos \measuredangle(v, w) = \frac{\langle v, w \rangle}{|v| \cdot |w|}. \tag{5}$$

Wektory v i w są liniowo zależne, gdy $\cos \measuredangle(v, w) = \pm 1$, tj. gdy $\measuredangle(v, w) = 0$ lub π. Jeżeli $\langle v, w \rangle = 0$, to $\measuredangle(v, w) = \frac{1}{2}\pi$ i wektory v, w nazywamy *prostopadłymi* lub *ortogonalnymi*. Piszemy wtedy, że $v \perp w$.

Jeżeli $v \neq \theta$, to zbiór $v^\perp$ wszystkich wektorów prostopadłych do v tworzy podprzestrzeń przestrzeni V, przy czym $\dim v^\perp = \dim V - 1$, gdy V jest przestrzenią skończeniewymiarową. Ogólniej, jeżeli W jest podprzestrzenią przestrzeni V, to zbiór

$$W^\perp = \{v \in V; \forall w \in W : v \perp w\} \tag{6}$$

nazywamy *ortogonalnym dopełnieniem* podprzestrzeni W. $W^\perp$ jest również podprzestrzenią przestrzeni V, przy czym

$$\dim W + \dim W^\perp = \dim V \tag{7}$$

w przypadku przestrzeni skończonego wymiaru.

Bazę $\{v_1, \dots v_n\}$ przestrzeni wektorowej V (z iloczynem skalarnym) nazywamy *ortonormalną*, gdy

$$\langle v_i, v_j \rangle = \delta_{ij} \tag{8}$$

dla wszystkich $i, j = 1, \dots, n$. Elementy bazy ortonormalnej są wektorami jednostkowymi wzajemnie do siebie prostopadłymi. Poniższe twierdznie dowodzi istnienia baz ortonormalnych. Zastosowana w dowodzie metoda konstrukcji zwana jest *ortogonalizacją Schmidta*.

Twierdzenie 1. *Dla dowolnej bazy $\{v_1, \dots, v_n\}$ przestrzeni V (z iloczynem skalarnym) istnieje taka baza ortonormalna $\{w_1, \dots w_n\}$, że w_j $(j = 1, \dots, n)$ jest liniową kombinacją wektorów $v_1, \dots, v_j$.*

Dowód. Niech $w_1 = v_1/|v_1|$. Przypuśćmy, że dla pewnego $j \geq 1$ skonstruowaliśmy wektory $w_1, \dots, w_j$ jednostkowe, wzajemnie prostopadłe i takie, że w_i jest liniową kombinacją wektorów $v_1, \dots, v_i$ dla $i = 1, \dots, j$. Niech

$$w'_{j+1} = v_{j+1} - \sum_{i=1}^{j} \langle v_{j+1}, w_i \rangle w_i.$$

Z liniowej niezależności wektorów bazy $\{v_i\}$ wynika, że $w'_{j+1} \neq \theta$, a ponadto widać łatwo, że $\langle w'_{j+1}, w_i \rangle = 0$ dla $i \leq j$. Przyjmijmy

$$w_{j+1} = w'_{j+1}/|w'_{j+1}|.$$

Konstruując w ten sposób wektory $w_1, \dots, w_n$ otrzymujemy poszukiwaną bazę ortonormalną. □

Przykłady. Dla iloczynu skalarnego w $\mathbb{R}^n$ danego wzorem $\langle x, y \rangle = \sum x_i y_i$, gdy $x = (x_1, \dots, x_n)$ i $y = (y_1, \dots, y_n)$, $\{e_1, \dots, e_n\}$, gdzie $e_i = (\delta_{1i}, \dots, \delta_{ni})$, jest bazą ortonormalną. W przypadku $n = 2$, wektory $v_1 = \cos\alpha e_1 + \sin\alpha e_2$ i $v_2 = -\sin\alpha e_1 + \cos\alpha e_2$ tworzą bazę ortonormalną przestrzeni $\mathbb{R}^2$. Ogólniej, jeżeli $v = \{v_1, \dots, v_n\}$ jest bazą ortonormalną i A jest macierzą przejścia od bazy $w = \{w_1, \dots, w_n\}$, to w jest bazą ortonormalną wtedy i tylko wtedy, gdy $A \in \mathrm{O}(n)$, tj. gdy $A \cdot A^\top = I$. (Widać od razu, że $\mathrm{O}(n)$ jest podgrupą grupy $\mathrm{GL}(n)$. Jej elementy nazywa się *macierzami ortogonalnymi*.)

3. Przestrzeń euklidesowa.

Przestrzenią euklidesową nazywamy przestrzeń afiniczną, której przetrzeń wektorowa jest wyposażona w iloczyn skalarny, jest to więc czwórka $E = (P, V, \overrightarrow{\cdot}, g)$, gdzie $(P, V, \overrightarrow{\cdot})$ jest przestrzenią afiniczną, zaś g jest iloczynem skalarnym w przestrzeni V. Dla dowolnych punktów A, B przestrzeni euklidesowej, długość $AB = |\overrightarrow{AB}\|$ wektora $\overrightarrow{AB}$ nazywamy *odległością* punktów A, B. Przestrzeń euklidesowa z tak określoną odległością punktów jest przestrzenią metryczną:

(1) $\forall A, B : AB \geq 0$ i $AB = 0 \Leftrightarrow A = B$,
(2) $\forall A, B : AB = BA$,
(3) $\forall A, B, C : AB + BC \geq AC$.

Pojęcia kąta między wektorami, prostopadłości wektorów itp. prowadzą w naturalny sposób do kąta między prostymi, prostopdadłości prostych i - ogólniej - podprzestrzeni.

Przekształcenia zachowujące odległość punktów (a więc i iloczyn skalarny wektorów) nazywamy *izometriami*. Są one przekształceniami afinicznymi, co widać łatwo z dyskusji nierówności Schwarza. Izometrie są oczywiście przekształceniami odwracalnymi i tworzą grupę przekształceń. W przypadku skończeniewymiarowym ($\dim V = n$) i przy wyborze bazy ortonormalnej odpowiadają one podgrupie $\mathbb{R}^n \times \mathrm{O}(n)$ grupy $\mathbb{R}^n \times \mathrm{GL}(n)$ przekształceń afinicznych. (W szczególności, izometriami są translacje.) Ponieważ każda skończeniewymiarowa przestrzeń z iloczynem skalarnym posiada bazę ortonormalną, to każda n-wymiarowa przestrzeń euklidesowa jest izometryczna z przestrzenią $\mathbb{R}^n$ z iloczynem skalarnym z ostatniego przykładu. W dalszym ciągu rozdziału ograniczymy się do tej standardowej przestrzeni.

4. Zbiory algebraiczne.

Zbiór $X \subset F^n$, gdzie F jest ciałem (w dalszym ciągu ograniczymy się do przypadku $F = \mathbb{R}$ choć przypadek $F = \mathbb{C}$ jest równie - a może nawet bardziej - interesujący), nazywamy *algebraicznym*, gdy istnieją wielomiany n zmiennych $P_1, \ldots, P_k$ takie, że

$$x \in X \quad \Leftrightarrow \quad P_1(x) = \cdots = P_k(x) = 0. \tag{1}$$

Zbiory algebraiczne są domknięte, a wszystkie wielomiany P znikające na danym zbiorze X tworzą ideał pierścienia wielomianów n zmiennych. Ogólny opis zbiorów algebraicznych jest zadaniem trudnym stanowiącym przedmiot tzw. *geometrii algebraicznej*. Tutaj ograniczymy się do klasyfikacji zbiorów algebraicznych opisywanych wielomianami stopnia 1 i (dla n = 2 i 3) 2.

A. Zbiory liniowe. Dla danego układu $L_1, \ldots, L_k$ $(k < n)$ funkcji postaci $L_i(x) = \langle a_i, x\rangle + b_i$, gdzie $a_i \in \mathbb{R}^n$ i $b_i \in \mathbb{R}$, zbiór $X = L^{-1}(0) \cap \cdots \cap L^{-1}(0)$ jest podprzestrzenią afiniczną przestrzeni $\mathbb{R}^n$. Wymiar tej podprzestrzeni wynosi na ogół $n - l$, gdzie l jest maksymalną liczbą liniowo niezależnych elementów zbioru $\{a_1, \ldots, a_k\}$. (Innymi słowy, l jest rzędem macierzy $A = [a_1, \ldots, a_k]$.) Wektory a_i są prostopadłe do podprzestrzeni X.

W szczególności, gdy $k = n - 1$ i wektory $a_1, \ldots, a_k$ są liniowo niezależne, to układ równań

$$L_1 = \cdots = L_k = 0 \tag{2}$$

opisuje prostą w $\mathbb{R}^n$. Układ ten tradycyjnie nazywa się *równaniem ogólnym* prostej. Dla $n = 2$ (tj., na płaszczyźnie) układ ten jest rzeczywiście pojedynczym równaniem

postaci

$$ax + by + c = 0, \tag{3}$$

gdzie $a^2 + b^2 > 0$. Wektor (a, b) jest prostopadły do prostej opisanej równaniem (3), a parametr c jest wyznaczony przez współrzędne dowlnego punktu tej prostej. Proste o równaniach (3) z tymi samymi (ogólniej, proporcjonalnymi) współczynnikami przy zmiennych x i y są równoległe, a proste o równaniach

$$a_i x + b_i y + c_i = 0, \quad i = 1, 2, \tag{4}$$

są prostopadłe, gdy $a_1 a_2 + b_1 b_2 = 0$.

Podobnie, dla $n = 3$ równanie

$$ax + by + cz + d = 0, \tag{5}$$

gdzie $a^2+b^2+c^2 > 0$, opisuje płaszczyznę w przestrzeni (trójwymiarowej) prostopadłą do wektora (a, b, c). Dwie takie płaszczyzny są równoległe, gdy współczynniki przy x, y i z są proporcjonalne, a są prostopadłe, gdy iloczyn skalarny wektorów złożonych z tych współcznynników jest równy zeru.

W literaturze klasycznej można znaleźć wiele specjalnych równań prostych i płaszczyzn (np. równanie odcinkowe) mających pewne szczególne znaczenie geometryczne.

B. Krzywe stożkowe.

Dla dowolnych dwu punktów F_1 i F_2 i liczby dodatniej $a > c = \frac{1}{2}F_1F_2$, zbiór wszystkich punktów P spełniających warunek $PF_1 + PF_2 = 2a$ nazywamy *elipsą* o *osi wielkiej* $2a$ i *ogniskach* F_1, F_2. Jeżeli punkty F_1 i F_2 mają współrzędne $(-c, 0)$ i $(c, 0)$, to nasza elipsa opisana jest równaniem

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1, \tag{6}$$

gdzie $b^2 = a^2 - c^2$. Ponadto, punkty elipsy mają tę własność, że stosunek ich odległości od ognisk do odległości od odpowiadających im prostych zwanych *kierownicami* (ich równania w omawianym powyżej przypadku mają postać $x = \pm\frac{a^2}{c}$) jest stały i wynosi $e = c/a$. Liczbę $e \in (0, 1)$ nazywamy *mimośrodem* elipsy. W szczególnym przypadku $F_1 = F_2 = F$ $(c = 0)$ elipsa jest *okręgiem* o środku F i promieniu a.

Podobnie, wszystkie punkty P spełniające warunek $|PF_1 - PF_2| = 2a$ $(a < c)$ tworzą *hiperbolę* o *osi rzeczywistej* $2a$ i *ogniskach* F_1, F_2. Jeżeli - jak poprzednio - ogniskami są punkty $(\pm c, 0)$, to hiperbola dana jest równaniem

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1, \tag{7}$$

gdzie $b^2 = c^2 - b^2$. (Liczbę b nazywa się czasem *półosią urojoną* hiperboli.) Podobnie jak w przypadku elipsy, stosunek odległości punktów hiperboli od kierownic $x = \pm\frac{a^2}{c}$ jest stały i równy mimośrodowi $e = c/a > 1$.

Na koniec, zbiór wszystkich punktów równooddalonych ($e = 1$) od punktu F i prostej k ($F \notin k$) nazywamy *parabolą* o *ognisku* F i *kierownicy* k. Jeżeli $F = (p/2, 0)$, zaś prosta k dana jest równaniem $x = -p/2$, to parabolę opisuje równanie

$$y^2 = 2px. \tag{8}$$

Liczbę p nazywa się *parametrem* paraboli.

Wszystkie te krzywe (elips ce, hiperbolę i parabolę) można przedstawić jako przekroje *powierzchni stożkowej* o równaniu

$$x^2 + y^2 - z^2 = 0$$

płaszczyznami nieprzecodzącymi przez wierzchołek stożka ($x = y = z = 0$) i nierównoległymi do osi stożka ($x = y = 0$). Na przekroju łatwo (!) pokazać geometryczną interpretację ognisk, kierownic i innych pojęć wspomnianych powyżej.

C. Powierzchnie drugiego stopnia. Powierzchnia stożkowa wspomniana powyżej jest opisana równaniem drugiego stopnia. Oto lista wszystkich "niezdegenerowanych" powierzchni w $\mathbb{R}^3$ opisywanych takimi równaniami:

(1) walec eliptyczny: $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$,
(2) walec hiperbliczny: $\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$,
(3) walec paraboliczny: $y^2 - 2px = 0$,
(4) powierzchnia stożkowa: $\frac{x^2}{a^2} + \frac{y^2}{b^2} - z^2 = 0$,
(5) elipsoida: $\frac{x^2}{a^2} + \frac{y^2}{b^2} + \frac{z^2}{c^2} = 1$,
(6) hiperboloida jednopowłokowa: $\frac{x^2}{a^2} + \frac{y^2}{b^2} - \frac{z^2}{c^2} = 1$, (uwaga: równanie to moña przedstawić w postaci

$$(\frac{x}{a} - \frac{z}{c})(\frac{x}{a} + \frac{z}{c}) = (1 - \frac{y}{b})(1 + \frac{y}{b})$$

wskazującej na to, że przez każdey punkt tej powierzchni przechodzą dwie proste całkowiczie w niej zawarte !)
(7) hiperboloida dwupowłokowa: $\frac{x^2}{a^2} - \frac{y^2}{b^2} - \frac{z^2}{c^2} = 1$,
(8) paraboloida eliptyczna: $\frac{x^2}{a^2} + \frac{y^2}{b^2} - 2pz = 0$,
(9) paraboloida hiperboliczna: $\frac{x^2}{a^2} - \frac{y^2}{b^2} - 2pz = 0$.

Ponadto, równania drugiego stopnia w $\mathbb{R}^3$ mogą przedstawiać "powierzchnie zdegenerowane", np. "podwójną płaszczyznę" ($x^2 = 0$), parę płaszczyzn przecinających się ($x^2 - y^2 = 0$) itd.

5. Objętość równoległościanu.

Równoległościanem rozpiętym na wektorach liniowo niezależnych $v_1, \dots v_k$ przestrzeni afinicznej E nazywamy zbiór

$$R = \{X; \overrightarrow{PX} = \sum_{i=1}^{k} t_i v_i, 0 \le t_i \le 1\}.$$

W szczególności, R jest odcinkiem, gdy $k = 1$, równoległobokiem, gdzy $k = 2$, itd.

Z analizy wiadomo, że objętości figur w n-wymiarowej przestrzeni euklidesowej oblicza się przybliżając te figury sumami mnogościowymi równoległościanów, a ich objętości sumami objętości tych równoległościanów. Zatem, kluczowym zagadnieniem dotyczącym objętości figur geometrycznych jest znalezienie wzoru wyrażającego objętość nazsego zbioru R.

Twierdzenie. *Kwadrat objętości $|R|$ równoległościanu R jest równy wyznacznikowi Grama wyznaczonego prze wektory $v_1, \ldots, v_k$, tzn.*

$$|R|^2 = \det[\langle v_i, v_j\rangle; i, j \leq k].$$

Uwaga. Zauważmy, że wyznacznik Grama $G(v_1, \ldots v_k) = \det[\langle v_i, v_j\rangle]$ jest zawsze nieujemny, a zeruje się wtedy i tylko wtedy, gdy wektory $v_1, \ldots, v_k$ są liniowo zależne. To pierwsze stwierdzenie wynika z poniższego dowodu, a to drugie stąd, że znikanie wzyznacznika jest równoważne liniowej zależności jego kolumn. Jeśli kolumny wyznacznika $G(v_1, \ldots, v_k)$ są liniowo zależne to np. $\langle v_k, v_i\rangle = \sum_{j<k} x_j \langle v_j, v_i\rangle$ dla wszystkich $i \leq k$ i pewnych $x_j \in \mathbb{R}$. Wtedy $v_k - \sum_j x_j v_j \perp \mathrm{Lin}(v_1, \ldots, v_k)$, a ponieważ oczywiście $v_k - \sum_j x_j v_j \in \mathrm{Lin}(v_1, \ldots, v_k)$, więc $v_k - \sum_j x_j v_j = 0$.

Dowód. Przeprowadzimy indukcję względem wymiaru k równoległościanu R.

1. Dla $k = 1$, $|R|^2 = |v|^2 = \langle v, v\rangle$, a więc dowodzona równość jest spełniona. Dla $k = 2$,

$$|R|^2 = |v_1|^2|v_2|^2 \sin^2 \sphericalangle(v_1, v_2) = |v_1|^2|v_2|^2(1 - \cos^2 \sphericalangle(v_1, v_2)) = |v_1|^2|v_2|^2 - \langle v_1, v_2\rangle^2$$

i znów dowodzona równość jest spełniona.

2. Przypuśćmy, że dowodzona równość jest spełniona dla równoległościanów rozpiętych na $j < k$ wektorach. Oznaczmy przez R' podstawę równoległościanu R, tj. równoległościan rozpięty na wektorach $v_1, \ldots v_{k-1}$. Wtedy

$$|R| = |R'| \cdot h,$$

gdzie h jest wysokością równoległościanu R, tj. długością składowej $v_k^\perp$ wektora v_k prostopadłej do hiperpłaszczyzny $\mathrm{Lin}\{v_1, \ldots, v_{k-1}\}$. Ponieważ

$$v_k^\perp = v_k - \sum_{j=1}^{k-1} x_j v_j,$$

gdzie $x_1, \ldots, x_{k-1}$ spełniają układ równań

$$\sum_{j=1}^{k-1} x_j \langle v_i, v_j\rangle = \langle v_k, v_i\rangle,$$

więc

$$h^2 = |v_k|^2 - 2\sum_j x_j \langle v_k, v_j\rangle + \sum_{i,j} x_i x_j \langle v_i, v_j\rangle = \langle v_k, v_k\rangle - \sum_j x_j \langle v_k, v_j\rangle.$$

Oznaczmy przez G wyznacznik Gramma wektorów $v_1, \ldots, v_k$, przez G_j jego minor otrzymany przez skreślenie k-tego wiersza i j-tej kolumny, przez G' wyznacznik Grama wektorów $v_1, \ldots, v_{k-1}$, a przez G'_j wyznacznik otrzymany z G' przez zastąpienie wyrazów j-tej kolumny iloczynami $\langle v_i, v_k\rangle$. Wtedy, na mocy wzorów Crammera,

$$G' \cdot x_j = G'_j,$$

a na mocy własności wyznaczników,

$$G'_j = (-1)^{k+j-1} G_j.$$

Ponadto, założenie indukcyjne implikuje równość

$$|R'|^2 = G'.$$

Zatem, korzystając z rozwinięcia Laplace'a dla wyznacznika G otrzymujemy

$$|R|^2 = G' \langle v_k, v_k \rangle - \sum_{j=1}^{k-1} (-1)^{k+j-1} \langle v_k, v_j \rangle \cdot G_j = G.$$

Indukcja kończy dowód. $\square$

Rozdział 8. Teoria spektralna

1. Wartości i wektory własne. Niech $f : V \to V$ będzie endomorfizmem przestrzeni wektorowej V. Niezerowy wektor $v \in V$ nazywamy *wektorem własnym* endomorfizmu f, gdy

$$f(v) = \lambda \cdot v$$

dla pewnego skalara λ. Skalar λ nazywamy wtedy *wartością własną* endomorfizmu f (odpowiadającą wektorowi v). Zbiór $\mathrm{Spec}(f)$ wszystkich wartości własnych endomorfizmu f nazywamy jego *spektrum*. Oczywiście, zbiór wszystkich wektorów własnych odpowidających tej samej wartości własnej λ tworzy (po dołączeniu doń wektora zerowego) podprzestrzeń $E\lambda$ przestrzeni V.

Na przykład, $\mathrm{Spec}(\mathrm{id}) = \{1\}$, obrót o kąt $\alpha \in (0, \pi)$ na płaszczyźnie ma puste spektrum, a wartościami własnymi endomorfizmu $f : \mathbb{R}^2 \to \mathbb{R}^2$ o macierzy

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

są liczby $\lambda_{1,2} = 0,5 \cdot (3 \pm \sqrt{5})$. Istotnie, z teorii układów równań liniowych wynika od razu następujące

Twierdzenie 1. *Liczba λ jest wartością własną endomorfizmu f o macierzy A wtedy i tylko wtedy, gdy*

$$\det(A - \lambda I) = 0. \quad \square \tag{1}$$

Łatwo zuważyć, że rozwiązania powyższego równania nie zależą od wyboru bazy w jakiej przedstawiliśmy f. Istotnie, jeżeli B jest macierzą endomorfizmu f w innej bazie, to $B = CAC^{-1}$ dla pewnej macierzy nieosobliwej C. Wtedy

$$\det(B - \lambda I) = \det[C(A - \lambda I)C^{-1}] = \det(A - \lambda I).$$

Dlatego, wartości własne endomorfizmu f jak i pewne funkcje z nich utworzone są *niezmiennikami* endomorfizmu. Są nimi np. elementarne funkcje symetryczne wartości własnych, w szczególności ich suma - *ślad* endomorfizmu. Ślad $\mathrm{tr}(f)$ endomorfizmu jest określony dobrze nawet wtedy, gdy wartości własne nie istnieją:

$$\mathrm{tr}(f) = a_{11} + \cdots + a_{nn},$$

gdy $A = [a_{ij}]$ jest macierzą f w dowolnej bazie $v_1, \ldots, v_n$. Podobnie, niezmiennikiem endomorfizmu jest jego *wyznacznik* $\det f = \det A$, który pokrywa się z iloczynem wwszystkich wartości własnych (o ile istnieją).

Równanie (1) jest równaniem algebraicznym stopnia $n = \dim V$, a więc posiada zawsze rozwiązania, jeśli V jest przestrzenią wektorową nad ciałem algebraicznie zupełnym. W szczególnoći ma to miejsce dla ciała liczb zespolonych:

Twierdzenie 2. *Każdy endomorfizm dowolnej zespolonej przestrzeni liniowej posiada przynajmniej jedną wartość własną (i wektor własny).* $\square$

Na przykład, wspomniany wcześniej obrót płaszczyzny $\mathbb{R}^2 \approx \mathbb{C}$ można traktować jako mnożenie przez zespoloną liczbę $e^{i\alpha}$, która jest oczywiście jego zespoloną

wartością własną. Ogólniej, każdy endomorfizm n- wymiarowej przestrzeni zespolonej V można traktować jako endomorfizm odpowiadającej jej $2n$-wymiarowej przestrzeni rzeczywistej. Odwrotnie, jeżeli V jest przestrzenią wektorową nad $\mathbb{R}$, to sumę prostą $V \oplus V$ można wyposażyć w naturaly sposób w strukturę zespolonej przestrzeni wektorowej przyjmując, że

$$(a + ib)(v, w) = (av - bw, aw + bv).$$

Tak otrzymana przestrzeń zespolona nazywana jest *kompleksyfikacją* przestrzeni rzeczywistej V i oznaczana sybolem $V_{\mathbb{C}}$. Piszemy $v + iw$ zamiast $(v, w) \in V_{\mathbb{C}}$.

Dowolny endomorfizm f przestrzeni V wyznacza w naturalny sposb swoją *kompleksyfikację* $f_{\mathbb{C}} : V_{\mathbb{C}} \to V_{\mathbb{C}}$:

$$f_{\mathbb{C}}(v + iw) = f(v) + if(w).$$

$f_{\mathbb{C}}$ jest przekształceniem $\mathbb{C}$-liniowym (sprawdzić !), jest więc endomorfizmem zespolonej przestrzeni wektorowej $V_{\mathbb{C}}$. Jego spektrum nazywamy *spektrum zespolonym* endomorfizmu rzeczywistego f. Każda zespolona przestrzeń wektorowa wymiaru n może być traktowana jako $2n$-wymiarowa przestrzeń rzeczywista, a każdy jej zespolony endomorfizm f jest też endomorfizmem rzeczywsitym i może być skompleksyfikowany. Wtedy $\mathrm{Spec}(f_{\mathbb{C}} = \mathrm{Spec}(f)$ $(\subset \mathbb{C})$, a więc definicja powyższa nie prowadzi do nieporozumień.

2. Endomorfizmy samosprzężone.

Jeżeli rzeczywista przestrzeń wektorowa V jest wyposażona w iloczyn skalarny g, to dla każdego endomorfizmu f tej przestrzeni warunek

$$g(f(v), w) = g(v, f^*(w))$$

wyznacza nowy jej endomorfizm f^*. Nazywamy go *endomorfizmem sprzężonym* do f, a f endomorfizmem *samosprzężonym*, gdy $f^* = f$. Jeżeli $A = [a_{ij}]$ jest macierzą endomorfizmu f w pewnej bazie ortonormalnej, to macierz transponowana $A^\top$ jest macierzą endomorfizmu f^*. Zatem, f jest samosprzążony wtedy i tylko wtedy, gdy jego macierz A w dowolnej bazie ortonormalnej jest symetryczna ($A^\top = A$). Łatwo sprawdzić, że warunek ten jest niezależny od wyboru bazy ortonormalnej: Jeśli B jest macierzą f w innej bazie ortonormalnej, to $B = CAC^{-1}$ dla pewnej macierzy ortogonalnej C; ponieważ $C^{-1} = C^\top$, więc $B^\top = (CAC^\top)^\top = CA^\top C^\top = CAC^{-1} = B$. Jeśli v jest wektorem własnym endomorfizmu samosprzężonego f, to przestrzeń $W = \mathrm{Lin}(v)^\perp$ jest f-niezmiennicza, tzn. $f(W) \subset W$ i poszukiwanie wektorów i wartości własnych można prowadzić indukcyjnie.

Podobnie, w przypadku zespolonym, jeżeli h jest tzw. *iloczynem hermitowskim* na przestrzeni V (nad $\mathbb{C}$), tzn. $h : V \times V \to \mathbb{C}$, h jest $\mathbb{C}$-liniowe ze względu na pierwszą zmienną, $h(v, w) = \overline{h(w, v)}$ i $h(v, v) > 0$ gdy $v \neq 0$, to endomorfizmem sprzężonym do $f : V \to V$ nazywamy taki endomorfiznm f^*, że

$$h(f(v), w) = h(v, f^*(w))$$

dla wszystkich v i w z V. Jeśli $f^* = f$, to f nazywamy endomorfizmem *samosprzężonym* lub *hermitowskim*. Większość pojęć geometrii euklidesowej (ortogonalność wektorów, baza ortogonalna i ortonormalna itd.) przenosi się automatycznie z przypadku euklidesowego. Podobnie, w przpadku hermitowskim zachodzi twierdzenie Schmidta o ortogonalizacji. W szczególności, ortogonalne uzupełnienie $W^\perp$ podprzestrzeni $W \subset V$ określa się przy pomocy warunku

$$v \in W^\perp \quad \Leftrightarrow \quad (\forall w \in W)\ h(v, w) = 0.$$

Oczywiście, $\dim W + \dim W^\perp = \dim V$.

Twierdzenie spektralne. (przypadek zespolony) *Jeżeli V jest skończenie wymiarową zespoloną przestrzenią wektorową z iloczynem hermitowskim h, zaś $f : V \to V$ jest endomorfizmem hermitowskim, to istnieje w V baza ortonormalna złożona z wektorów własnych f.*

Dowód. Na mocy wcześniejszego twierdzenia istnieje wektor własny v_1 endomorfizmu f. Niech $w_1 = h(v_1, v_1)^{-1/2} v_1$. Wtedy w_1 jest jednostkowym ($h(w_1, w_1) = 1$) wektorem własnym f. Przypuśćmy, że mamy wektory własne $w_1, \dots w_k$ ($k < n = \dim V$) takie, że $h(w_i, w_j) = \delta_{ij}$ dla wszystkich $i, j \leq k$. Niech $W = \mathrm{Lin}(w_1, \dots, w_k)$. Wtedy, W jest przestrzenią f-niezmienniczą (tzn. $f(W) \subset W$), a więc jej ortogonalne uzupełnienie $W^\perp$ jest też f niezmiennicze. $f|W^\perp$ jest więc endomorfizmem zespolonej przestrzeni wektorowej $W^\perp$ i $\dim W^\perp > 0$. Istnieje więc wektor własny $v_{k+1} \in W^\perp$. Niech $w_{k+1} = h(v_{k+1}, v_{k+1})^{-1/2} v_{k+1}$. Wektory własne $w_1, \dots, w_{k+1}$ tworzą układ ortonormalny (tj. $h(w_i, w_j) = \delta_{ij}$ dla wszystkich $i, j \leq k+1$. Indukcja kończy dowód. □

Poprzez kompleksyfikację przestrzeni i endomorfizmu rzeczywistego oraz zastosowanie stosownego iloczynu hermitowskiego można udowodnić (patrz (!) np. S. Lang, *Algebra*, PWN) następujące

Twierdzenie spektralne. (przypadek rzeczywisty) *Jeżeli V jest skończenie wymiarową rzeczywistą przestrzenią wektorową z iloczynem skalarnym g, zaś $f : V \to V$ jest endomorfizmem samosprzężonym, to istnieje w V baza ortonormalna złożona z wektorów własnych f.* □

Literatura:

G. Banaszak i W. Gajda, Elementy algebry liniowej.
A. BiaynickiBirula, Algebra liniowa z geometrią.
J. Gancarzewicz, Algebra liniowa z elementami geometrii
A. I. Kostrykin i J. I. Manin, Algebra liniowa i geometrią
Z. Opial, Algebra wyższa
S. Lang, Algebra