

GEOMETRIA Z ALGEBRĄ LINIOWĄ II

(dalsze notatki do wykładu i kolejne długie opowiadania)

ARKADIUSZ MĘCEL



Dale Gardner odzyskuje satelitę Westar 6 (1984). Być może także dzięki twierdzeniu Eulera o osi obrotu bryły sztywnej (1776).

Materiał realizowany według skryptu *Wykłady z Algebry Liniowej II* doc. dr. Tadeusza Koźniewskiego
<https://mimuw.edu.pl/~amecel/alglin.html>
ostatnia aktualizacja: 24 kwietnia 2024

Spis treści

1	Endomorfizmy, macierze podobne	5
1.1	Zadania do samodzielnej pracy	12
1.2	Uzupełnienie. Macierze endomorfizmu w różnych bazach	13
1.3	Dodatek. Dyskretny układ dynamiczny	16
1.4	Trivia. Lights Out	18
2	Wartości własne endomorfizmu, wielomian charakterystyczny	19
2.1	Zadania do samodzielnej pracy	25
2.2	Uzupełnienie. Potęgi macierzy i rekurencje liniowe	26
2.3	Dodatek. Grafy i ich macierze sąsiedztwa	28
2.4	Trivia. PCA, czyli w jakich kierunkach patrzeć na dane?	31
3	Diagonalizowalność	32
3.1	Zadania do samodzielnej pracy	38
3.2	Uzupełnienie. Probabilistyka na sześciennym kostce	39
4	Sformułowanie twierdzenia Jordana	42
4.1	Zadania do samodzielnej pracy	48
4.2	Endomorfizmy triangularyzowalne	49
4.3	Dodatek. Podobieństwo nad ciałami nieskończonymi	51
4.4	Trivia. Problem Collatza	52
5	Wyznaczanie bazy Jordana	54
5.1	Zadania do samodzielnej pracy	60
5.2	Uzupełnienie. Trudniejsze zadania o postaci i bazie Jordana	61
5.3	Dodatek. Endomorfizmy nilpotentne i ich geometria Podprzestrzenie pierwiastkowe	64
6	Podprzestrzenie niezmiennicze	67
	Twierdzenie Cayleya-Hamiltona	67
6.1	Zadania do samodzielnej pracy	72
6.2	Uzupełnienie. Rozkłady ϕ -niezmiennicze	73
6.3	Dodatek. Rodziny endomorfizmów przemiennych Wspólna diagonalizowalność i triangularyzowalność	76
6.4	Trivia. Twierdzenie Cayleya-Hamiltona na konkursach	80
7	Przestrzenie afiniczne w przestrzeniach liniowych	82
7.1	Zadania do samodzielnej pracy	90
7.2	Uzupełnienie. Geometria afiniczna, czyli jaka?	91
7.3	Dodatek. Kombinacje i zbiory wypukłe	96
7.4	Trivia. SET, czyli przestrzeń afiniczna nad \mathbb{Z}_3	99
8	Afiniczna niezależność, bazy punktowe i układy bazowe	101
8.1	Afiniczna niezależność, baza punktowa, układ bazowy	105
8.2	Uzupełnienie. Wymiar przecięcia przestrzeni afinicznych	106
8.3	Dodatek. Współliniowość, współrzędne barycentryczne oraz intuicje i twierdzenia geometrii elementarnej	109
8.4	Trivia. Twierdzenie Helly’ego	114

9	Przekształcenia afiniczne	118
9.1	Zadania do samodzielnej pracy	127
9.2	Wielościanny, stożki i dualność	128
10	Formy dwuliniowe i iloczyn skalarny	136
10.1	Zadania do samodzielnej pracy	141
10.2	Uzupełnienie. Dlaczego cosinus?	142
10.3	Dodatek. Iloczyn skalarny i funkcjonały	143
10.4	Trivia. Zastosowania nierówności Cauchy-ego Schwarz	144
11	Prostopadłość	145
11.1	Zadania do samodzielnej pracy	150
11.2	Trivia. Czy względna pierwszość to prostopadłość?	151
12	Rzut prostopadły i ortogonalizacja	153
12.1	Zadania do samodzielnej pracy	157
12.2	Uzupełnienie. Metoda najmniejszych kwadratów	158
13	Macierze form dwuliniowych. Kryterium Sylwestera	160
13.1	Zadania do samodzielnej pracy	166
13.2	Uzupełnienie. Kryterium Sylwestera ze skryptu	167
13.3	Trivia. Inne kątomierze, czyli o aksonometrii	170
14	Przestrzenie euklidesowe afiniczne	172
14.1	Zadania do samodzielnej pracy	178
14.2	Uzupełnienie. Dlaczego ogólny wzór na odległość działa?	179
15	Macierz Grama. Miara n-wymiarowa	180
15.1	Zadania do samodzielnej pracy	187
15.2	Dodatek. Miara Jordana i zasada Cavalieriego	188
15.3	Trivia. Zastosowania macierzy Grama w zadaniach	194
16	Orientacja i iloczyn wektorowy	198
16.1	Zadania do samodzielnej pracy	202
16.2	Uzupełnienie. Orientowalność i transformacje ciągłe	203
16.3	Trivia. Nieprzystające odpowiedniki	205
17	Izometrie liniowe i afiniczne. Macierze ortogonalne	206
17.1	Uzupełnienie. Rozpoznawanie i zliczanie izometrii	215
17.2	Dodatek. Macierze ortogonalne i rozkłady	218
18	Składanie izometrii	221
18.1	Uzupełnienie. Grupy izometrii i obrotów	228
18.2	Dodatek. Punkty stałe i klasyfikowanie izometrii	230
18.3	Trivia. Twierdzenia o przedłużaniu	232
19	Przekształcenia samosprężone	
	Twierdzenie spektralne (rzeczywiste)	233
19.1	Uzupełnienie. Największa i najmniejsza wartość własna	239
19.2	Trivia. Twierdzenie spektralne w teorii grafów	240
20	Formy hermitowskie	
	Przekształcenia unitarne	241
20.1	Uzupełnienie. Twierdzenie spektralne (wersja zespolona)	247
20.2	Dodatek. Operatory zespolone przypominają liczby	250
20.3	Trivia. Zasadnicze twierdzenie algebry — zrób to sam!	252
21	Przestrzenie dwuliniowe i ich bazy prostopadłe	253
21.1	Uzupełnienie. Formy i macierze antysymetryczne	260
21.2	Dodatek. Podprzestrzenie całkowicie zdegenerowane	261

22 Kongruentność macierzy rzeczywistych i zespolonych	264
22.1 Uzupełnienie. Twierdzenie Jacobiego	269
22.2 Dodatek. Izometrie przestrzeni dwuliniowych. Kongruencja macierzy diagonalnych	270
22.3 Trivia. Sygnatura, a geometria elementarna	273
23 Formy kwadratowe	279
23.1 Uzupełnienie. Minima i maksima	286
23.2 Dodatek. Twierdzenie Hasse-Minkowskiego	288
23.3 Notka historyczna. Sumy kwadratów	289
24 Wielomiany i funkcje wielomianowe	292
Zbiory algebraiczne	292
24.1 Uzupełnienie. Wielomiany jednorodne Przestrzenie i przekształcenia rzutowe	298
24.2 Dodatek. Wstęp do algebry wieloliniowej. O iloczynie tensorowym, n-formach i n-wektorach	303
24.3 To nie trivia. Wielomiany symetryczne	313
25 Hiperpowierzchnie stopnia 2	315
25.1 Uzupełnienie. Powierzchnie prostokreślne	329
25.2 Dodatek. Klasyfikacja izometryczna i rzutowa Kilka słów o stożkowych	331
25.3 Trivia. Pringles	336

Rozdział 1

Endomorfizmy, macierze podobne

W pierwszym semestrze poznaliśmy podstawowe własności przestrzeni liniowych oraz przekształceń liniowych między tymi przestrzeniami. Wątek geometryczny naszego wykładu sprowadzał się w zasadniczej mierze do budowania intuicji związanych z pojęciem wymiaru przestrzeni liniowej i poznawaniem jego własności (choćby poprzez opis wymiaru sumy i przecięcia podprzestrzeni). Drugi semestr rozpoczniemy¹ od pytania o geometryczną interpretację przekształceń liniowych. Brzmi ono w sposób następujący.

Jakie własności geometryczne przekształcenia liniowego możemy odczytać z macierzy $M(\phi)_{\mathcal{B}}$ przekształcenia liniowego $\phi : V \rightarrow W$ pomiędzy przestrzeniami skończonego wymiaru, poza informacją dotyczącą wymiarów obrazu i jądra tego przekształcenia?

Niezwykle precyzyjne informacje otrzymać możemy w przypadku, gdy² $V = W$ oraz $\mathcal{A} = \mathcal{B}$.

Definicja 1.1: Endomorfizm i macierz endomorfizmu w bazie

Niech V będzie przestrzenią liniową nad ciałem K .

- Przekształcenie liniowe $\phi : V \rightarrow V$ nazywamy ENDOMORFIZMEM PRZESTRZENI V . Zbiór endomorfizmów przestrzeni V oznaczamy $\text{End}(V)$. Innymi słowy $\text{End}(V) = L(V, V)$.
- MACIERZĄ ENDOMORFIZMU ϕ W BAZIE \mathcal{A} nazywamy macierz $M(\phi)_{\mathcal{A}}$.

A zatem: zamiast rozważania ogólnych przekształceń liniowych $\phi : V \rightarrow W$ i odpowiadających im macierzy prostokątnych rozważać będziemy przekształcenia $\phi : V \rightarrow V$ opisane macierzami kwadratowymi. Kluczowe jest tu to, że w $\text{End}(V)$ wprowadzić można działanie składania przekształceń, które czyni je tak zwaną ALGEBRĄ. Co z tego wynika? Załóżmy, że $A = M(\phi)_{\mathcal{A}}$ oraz $\phi \in \text{End}(V)$. Wówczas $M(\phi \circ \phi)_{\mathcal{A}} = A^2$.

Centralne pytanie na najbliższe wykłady brzmi: jak „najprościej” wyglądać mogą macierze endomorfizmów przestrzeni skończonego wymiaru w zależności od wyboru bazy? W tle pojawi się też geometria.

Rozważmy następujący przykład „motywacyjny”. Endomorfizm przestrzeni liniowej \mathbb{R}^2 zadany wzorem

$$\phi((x_1, x_2)) = (2x_1 + x_2, x_1 + 2x_2)$$

spełnia $\phi((1, -1)) = (1, -1)$ oraz $\phi((1, 1)) = (3, 3)$, a więc ϕ ma w bazie $\mathcal{A} = ((1, -1), (1, 1))$ macierz

$$M(\phi)_{\mathcal{A}} = \begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix},$$

Dlaczego nas to interesuje? Okazuje się bowiem, że w bazie \mathcal{A} „widzimy” geometrię przekształcenia ϕ . Jest ono swego rodzaju *rozciąganiem* w kierunkach (osiach) $(1, -1)$ oraz $(1, 1)$ w skali odpowiednio **1**, **3**. Mówiąc bardziej precyzyjnie, dla dowolnych $a, b \in \mathbb{R}$ mamy:

$$\phi(a(1, -1) + b(1, 1)) = 1 \cdot a(1, -1) + 3 \cdot b(1, 1).$$

¹Ostatnia aktualizacja: 06.05.2023 r.

²Omówienie jak wygląda sytuacja, gdy $V = W$, ale $\mathcal{A} \neq \mathcal{B}$ dokonane zostanie w uzupełnieniu do tego wykładu.

Przejdźmy do opisu macierzy ustalonego endomorfizmu. Zaczniemy od prostej obserwacji³.

Obserwacja 1.1

Niech \mathcal{A}, \mathcal{B} będą bazami przestrzeni liniowej V wymiaru n nad ciałem K oraz niech $\phi \in \text{End}(V)$. Niech $A = M(\phi)_{\mathcal{A}}^{\mathcal{A}}$ oraz $B = M(\phi)_{\mathcal{B}}^{\mathcal{B}}$. Wówczas

$$B = C^{-1}AC,$$

gdzie $C = M(\text{id})_{\mathcal{B}}^{\mathcal{A}}$, tzn. $C \in M_n(K)$ jest macierzą zmiany współrzędnych od \mathcal{B} do \mathcal{A} .

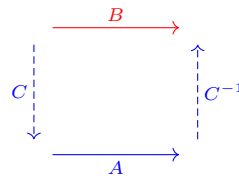
Dowód. Zgodnie z formułą opisującą macierz złożenia przekształceń liniowych mamy:

$$B = M(\phi)_{\mathcal{B}}^{\mathcal{B}} = M(\text{id} \circ \phi \circ \text{id})_{\mathcal{B}}^{\mathcal{B}} = M(\text{id})_{\mathcal{A}}^{\mathcal{B}} \cdot M(\phi)_{\mathcal{A}}^{\mathcal{A}} \cdot M(\text{id})_{\mathcal{B}}^{\mathcal{A}} = C^{-1}AC.$$

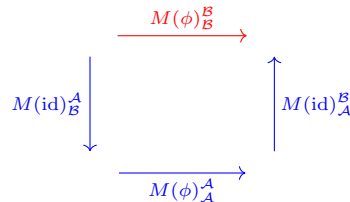
□

Zatrzymamy się na moment, żeby spojrzeć na dowód powyższego rezultatu z nieco innej perspektywy. W poprzednim semestrze wspominaliśmy o interpretacji diagramowej złożenia przekształceń liniowych. Warto jest prześledzić sformułowanie i dowód powyższej obserwacji w ten właśnie sposób. Pozwoli to nam unikać pomyłek (gdzie C^{-1} , a gdzie C ?) i w sposób naturalny interpretować pewne rozumowania.

Macierz A reprezentuje endomorfizm $\phi \in \text{End}(V)$, który czytamy we współrzędnych V w bazie \mathcal{A} , zaś macierz B reprezentuje ten sam endomorfizm, ale na V patrzymy inaczej — w bazie \mathcal{B} . Zapiszmy za pomocą diagramu równość macierzy $B = C^{-1}AC$. Pytamy czy istnieje taka macierz odwracalna C , że:

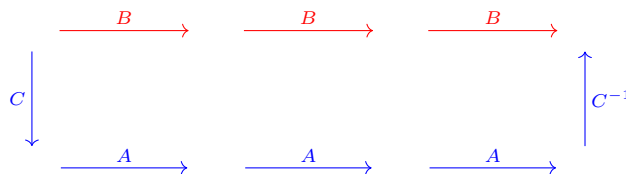


Zwróćmy uwagę na kolejność składania strzałek reprezentujących poszczególne macierze iloczynu $C^{-1}AC$. Macierz $C = M(\text{id})_{\mathcal{B}}^{\mathcal{A}}$ znajdujemy patrząc na równość $M(\phi)_{\mathcal{B}}^{\mathcal{B}} = M(\text{id})_{\mathcal{A}}^{\mathcal{B}} \cdot M(\phi)_{\mathcal{A}}^{\mathcal{A}} \cdot M(\text{id})_{\mathcal{B}}^{\mathcal{A}}$.



Możemy też zupełnie uprościć zapis i wskazać tylko to, co w dowodzie wyżej istotne, czyli $\phi = \text{id} \circ \phi \circ \text{id}$.

Poniższy diagram natomiast wyraża równość $B^3 = (C^{-1}AC)^3 = (C^{-1}AC)(C^{-1}AC)(C^{-1}AC) = C^{-1}A^3C$.



³Przypomnienie: I_n (lub I , o ile nie prowadzi to do nieporozumień) oznaczamy macierz identyczościową w $M_n(K)$. Macierz $A \in M_n(K)$ nazywamy odwracalną, jeśli istnieje $B \in M_n(K)$ taka, że $AB = BA = I$.

Powyższa obserwacja wyraźnie wskazuje na różnicę pomiędzy macierzami endomorfizmów w różnych bazach i macierzami w ustalonej bazie. Motywuje też wprowadzenie fundamentalnego dla nas pojęcia.

Definicja 1.2: Macierze podobne

Macierze $A, B \in M_n(K)$ nazywamy **PODOBNYMI** (NAD CIAŁEM K), jeśli istnieje macierz odwracalna $C \in M_n(K)$ taka, że:

$$B = C^{-1}AC.$$

Przykłady.

- Rozważmy macierze kwadratowe $A, B \in M_2(\mathbb{Q})$ oraz macierz odwracalną $P \in M_2(\mathbb{Q})$ postaci:

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

Macierze A, B są podobne, a dokładniej $B = P^{-1}AP$, ponieważ:

$$P^{-1} = \begin{bmatrix} 0 & -1 \\ 1 & 2 \end{bmatrix} \quad \text{oraz} \quad P^{-1}AP = \begin{bmatrix} 0 & -1 \\ 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} -1 & 2 \\ 3 & 1 \end{bmatrix} \cdot \begin{bmatrix} 2 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -5 & -3 \\ 6 & 5 \end{bmatrix}.$$

- Macierze

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \text{oraz} \quad B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

są podobne⁴ nad dowolnym ciałem K , bowiem $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^{-1} \cdot \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

Obserwacja 1.2

Niech $A, B \in M_n(K)$. Następujące warunki są równoważne:

- macierze A, B są podobne,
- istnieje $\phi \in \text{End}(K^n)$ oraz bazy \mathcal{A}, \mathcal{B} przestrzeni K^n takie, że

$$A = M(\phi)_{\mathcal{A}}^{\mathcal{A}}, \quad \text{oraz} \quad B = M(\phi)_{\mathcal{B}}^{\mathcal{B}}.$$

Dowód. Implikacja (b) \Rightarrow (a) wynika z poprzedniej obserwacji. Dowodzimy zatem (a) \Rightarrow (b). Przypuśćmy, że $B = C^{-1}AC$, dla pewnej macierzy odwracalnej C . Niech endomorfizm ϕ przestrzeni K^n będzie zadany warunkiem $M(\phi)_{st}^{st} = A$. Niech \mathcal{B} będzie bazą przestrzeni K^n złożoną z kolumn macierzy C . Wówczas $C = M(\text{id})_{\mathcal{B}}^{st}$, więc $C^{-1} = M(\text{id})_{st}^{\mathcal{B}}$. Stąd:

$$B = C^{-1}AC = M(\text{id})_{st}^{\mathcal{B}} \cdot M(\phi)_{st}^{st} \cdot M(\text{id})_{\mathcal{B}}^{st} = M(\phi)_{\mathcal{B}}^{\mathcal{B}}.$$

Otrzymaliśmy $A = M(\phi)_{st}^{st}$ oraz $B = M(\phi)_{\mathcal{B}}^{\mathcal{B}}$. □

⁴W tym przypadku C jest macierzą operacji elementarnej zamiany wierszy/kolumn i mamy dodatkowo równość

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

Dla dowolnej macierzy permutacyjnej $P \in S_n$, powstałej (jak pamiętamy) z macierzy identycznościowej $I \in M_n(K)$ przez permutację kolumn mamy

$$P^{-1} = P^T.$$

Z faktu tego wynikają dwa ważne wnioski. Pierwszy jest taki, że jeśli dane są dwie bazy przestrzeni n -wymiarowej V :

$$\mathcal{A} = (\alpha_1, \alpha_2, \dots, \alpha_n), \quad \mathcal{B} = (\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)}),$$

przy czym \mathcal{B} jest bazą powstałą przez zamianę kolejności wektorów w bazie \mathcal{A} za pomocą permutacji σ reprezentowanej przez macierz P , to dla $\phi \in \text{End}(V)$ mamy:

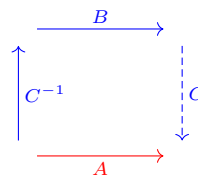
$$A = M(\phi)_{\mathcal{A}}^{\mathcal{A}} \iff P^{-1}AP = M(\phi)_{\mathcal{B}}^{\mathcal{B}}.$$

Obserwacja ta ma zastosowanie choćby w tzw. algebraicznej teorii grafów, ponieważ mówi, że macierze sąsiedztwa (patrz dodatek do kolejnego wykładu) dwóch izomorficznych grafów są podobne. Inną ważną perspektywą jest sama własność macierzy permutacyjnych, których odwrotność równa jest ich transpozycji. Macierze takie (o współczynnikach rzeczywistych) nazywamy ortogonalnymi. Mają one zasadnicze znaczenie w opisie tzw. izometrii. Za kilka wykładów poznamy je bliżej.

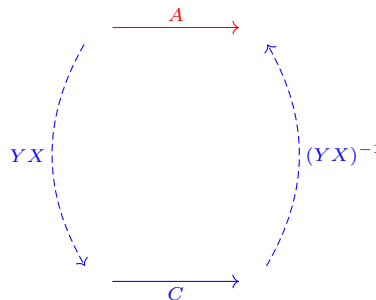
Relacja podobieństwa w zbiorze $M_n(K)$ jest relacją równoważności. Czasem podobieństwo macierzy nad ciałem K oznacza się symbolem $A \sim_K B$, lub nawet $A \sim B$. Nie piszemy natomiast „macierze podobne nad ciałem K ”, bowiem jak się okazuje — i nie jest to łatwe — jeśli macierze o wyrazach w ciele K są podobne nad ciałem $L \supseteq K$, to muszą być też podobne nad K . Temat ten omówimy dokładniej w jednym z dodatków.

- Zwrotność relacji podobieństwa. Dla każdej $A \in M_n(K)$ mamy $A = I_n \cdot A \cdot I_n = (I_n)^{-1} \cdot A \cdot I_n$, a zatem A jest macierzą podobną do samej siebie.

- Symetryczność relacji podobieństwa. Jeśli dla macierzy $A, B \in M_n(K)$ macierz A jest podobna do macierzy B , to istnieje macierz odwracalna C , że $B = C^{-1}AC$. W rezultacie otrzymujemy $A = CBC^{-1} = (C^{-1})^{-1}BC^{-1}$, czyli także macierz B jest podobna do A .



- Przechodność relacji podobieństwa. Załóżmy, że dla $A, B, C \in M_n(K)$ istnieją macierze odwracalne $X, Y \in M_n(K)$, takie że $A = X^{-1}BX$ oraz $B = Y^{-1}CY$, to $A = X^{-1}Y^{-1}CYX = (YX)^{-1}C(YX)$.



Kluczowe przykłady dla zrozumienia „geometrii” klas podobieństwa.

- Dla dowolnej macierzy odwracalnej $C \in M_n(K)$ mamy: $C^{-1} \cdot I \cdot C = C^{-1}C = I$.
- Niech $V = W \oplus U$ i niech $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$ będzie taką bazą przestrzeni V , że $(\alpha_1, \dots, \alpha_k)$ (dla pewnego $1 \leq k < n$) jest bazą przestrzeni W oraz $(\alpha_{k+1}, \dots, \alpha_n)$ jest bazą przestrzeni U . Niech $\phi : V \rightarrow V$ będzie rzutem V na W oraz niech ψ będzie symetrią V względem W wzdłuż U . Wówczas macierz $R_k = M(\phi)_{\mathcal{A}}^{\mathcal{A}}$ ma w pierwszych k kolumnach pierwsze k wektorów bazy standardowej K^n , zaś dalej kolumny zerowe. Podobnie macierz $S_k = M(\psi)_{\mathcal{A}}^{\mathcal{A}}$ jest postaci:

$$R_k = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{bmatrix} \quad S_k = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 & -1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 0 & \dots & -1 \end{bmatrix}.$$

Widzimy więc, że „geometrię jednokładności” można rozpoznać po klasie podobieństwa jej macierzy. Podobnie „rozpoznajemy” rzut lub symetrię, ale tu morał jest inny — macierz R_k jest podobna do macierzy KAŻDEGO rzutu przestrzeni n -wymiarowej (nad K) na podprzestrzeń wymiaru k . Jak się okaże, również inne klasy podobieństwa niosą za sobą różne „geometrie” endomorfizmów.

Problem rozstrzygnięcia kiedy dane dwie macierze kwadratowe są podobne jest skomplikowany. Zaczniemy od wskazania kilku niezmienników podobieństwa.

Definicja 1.3: Ślad macierzy kwadratowej

ŚLADEM MACIERZY $A = [a_{ij}] \in M_n(K)$ nazywamy sumę wyrazów stojących na przekątnej macierzy A , to znaczy element

$$\operatorname{tr}(A) = \sum_{i=1}^n a_{ii} \in K.$$

Ślad jest niezwykle istotnym obiektem i niezmiennikiem wielu ważnych konstrukcji, pomimo swojej pozornej prostoty. Oczywiście kluczowe jest stwierdzenie, że jest to element ciała. Gdy $A = I_n \in M_n(K)$ jest macierzą identyczności, to w zależności od K może mieć ona zupełnie inny ślad (wystarczy rozważyć $K = \mathbb{Z}_p$). Oto kluczowa własność⁵ w kontekście podobieństwa macierzy. Jej dowód to łatwe ćwiczenie.

Obserwacja 1.3: Ćwiczenie

Dla dowolnych macierzy $A, B \in M_n(K)$ zachodzi równość $\operatorname{tr}(AB) = \operatorname{tr}(BA)$.

Mówiąc o niezmiennikach podobieństwa, mamy na myśli przede wszystkim niezmienniki liczbowe: rząd, wyznacznik i ślad. Przypomnijmy, że dla dowolnej macierzy A przez rząd $r(A)$ tej macierzy oznaczamy wymiar przestrzeni kolumnowej A (czy też wymiar obrazu przekształcenia zadanego przez tą macierz). Przez $\det A$ oznaczamy wyznacznik macierzy kwadratowej A .

Obserwacja 1.4

Jeśli macierze $A, B \in M_n(K)$ są podobne, to:

$$r(A) = r(B), \quad \det(A) = \det(B), \quad \operatorname{tr}(A) = \operatorname{tr}(B).$$

Dowód. Jeśli A i B są macierzami podobnymi, to na mocy Obserwacji 1.2 istnieje $\phi \in \operatorname{End}(K^n)$ oraz bazy \mathcal{A}, \mathcal{B} przestrzeni K^n takie, że $A = M(\phi)_{\mathcal{A}}^{\mathcal{A}}, B = M(\phi)_{\mathcal{B}}^{\mathcal{B}}$. A zatem $r(A) = r(B)$ (co pokazywaliśmy już w poprzednim semestrze). Dalej, skoro macierze A, B są podobne, to istnieje macierz odwracalna C , że $B = C^{-1}AC$. Zatem z wzoru Cauchy'ego:

$$\det(B) = \det(C^{-1}AC) = \det(C^{-1}) \det(A) \det(C) = \frac{\det(A) \det C}{\det(C)} = \det(A).$$

Wreszcie, korzystając z Obserwacji 1.3 dla $C^{-1}A$ oraz C — $\operatorname{tr}(B) = \operatorname{tr}(C^{-1}AC) = \operatorname{tr}(CC^{-1}A) = \operatorname{tr}(A)$. \square

Definicja 1.4: Wyznacznik i ślad endomorfizmu

Niech $\dim V < \infty$ oraz niech $\phi \in \operatorname{End}(V)$.

- WYZNACZNIKIEM ENDOMORFIZMU ϕ , oznaczanym przez $\det \phi$, nazywamy taki element $\det(A) \in K$, gdzie $A = M(\phi)_{\mathcal{A}}^{\mathcal{A}}$, dla pewnej bazy \mathcal{A} przestrzeni V .
- ŚLADEM ENDOMORFIZMU, oznaczanym przez $\operatorname{tr} \phi$, nazywamy taki element $\operatorname{tr}(A) \in K$, gdzie $A = M(\phi)_{\mathcal{A}}^{\mathcal{A}}$, dla pewnej bazy \mathcal{A} przestrzeni V .

⁵Zwracam uwagę, że iloczyn śladów nie musi być śladem iloczynu. Jeśli weźmiemy na przykład $A = B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, to $\operatorname{tr}(A) = \operatorname{tr}(B) = \operatorname{tr}(A) \operatorname{tr}(B) = 0$, ale $\operatorname{tr}(AB) = \operatorname{tr}(I_2) = \dots$ zależy od ciała K . Jeśli byłoby nad ciałem liczb rzeczywistych to $\operatorname{tr}(I_2) = 2$, ale nad \mathbb{Z}_2 ślad I_2 równy jest 0.

Czytelnik zechce zauważyć, że poniższe dwie macierze mają takie same rzędy, wyznaczniki i ślady nad dowolnym ciałem:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Macierze te oczywiście nie są podobne, ponieważ do macierzy I_2 podobna jest tylko ona sama.

Kolejnym ważnym niezmiennikiem endomorfizmu są jego tzw. wartości własne oraz wielomian charakterystyczny. Powiemy o nich na kolejnym wykładzie. Dziś przedstawimy następującą motywację, przypominając definicję z poprzedniego semestru.

Definicja 1.5: Macierze diagonalne

Niech $A = [a_{ij}] \in M_n(K)$. Zbiór wyrazów $\{a_{11}, a_{22}, \dots, a_{nn}\}$ nazywamy PRZEKĄTNĄ macierzy A . Powiemy, że A jest DIAGONALNA, jeśli wszystkie jej wyrazy poza przekątną są zerowe.

Oto przykłady macierzy diagonalnych rozmiaru 3 o wyrazach rzeczywistych:

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

Gdybyśmy zapytali czy którekolwiek dwie z tych macierzy są podobne, wówczas bez żadnych niezmienników powiedzielibyśmy, że nie, ponieważ intuicyjnie rozumiemy geometrię endomorfizmów \mathbb{R}^3 zadawanych przez nie w bazie standardowej — i są to endomorfizmy działające w różny sposób. Istotnie:

- endomorfizm zadany macierzą A jest symetrią względem podprzestrzeni wymiaru 2,
- endomorfizm zadany macierzą B opisuje homotetię (jednokładność) o skali 2,
- endomorfizm zadany macierzą C ma obraz dwuwymiarowy — jest rzutem,
- endomorfizm ϕ zadany macierzą D jest izomorfizmem, ale nie jest ani symetrią, ani jednokładnością. Intuicyjnie widzimy, że „rozciąga” on odpowiednie wektory bazy standardowej w skali: **1**, **2**, **3**. Dokładniej oznacza to, że jeśli $\epsilon_1, \epsilon_2, \epsilon_3$ są wektorami bazy standardowej oraz $a, b, c \in \mathbb{R}$, to

$$\phi(a_1\epsilon_1 + a_2\epsilon_2 + a_3\epsilon_3) = \mathbf{1} \cdot a_1\epsilon_1 + \mathbf{2} \cdot a_2\epsilon_2 + \mathbf{3} \cdot a_3\epsilon_3.$$

Zachęcam Czytelnika do zastanowienia się kiedy dwie macierze diagonalne są podobne (nad ustalonym ciałem). Jak się okaże jest tak tylko wtedy, gdy przekątne tych macierzy różnią się jedynie kolejnością wyrazów. Fakt ten pokażemy w większej ogólności, ale ma on niewątpliwie wymowę geometryczną.

Wróćmy do motywującego nas przykładu z początku wykładu. Pokazaliśmy przykład endomorfizmu przestrzeni \mathbb{R}^2 , który w bazie $\mathcal{A} = ((1, -1), (1, 1))$ ma macierz diagonalną

$$M(\phi)_{\mathcal{A}} = \begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix},$$

choć sam wzór $\phi((x_1, x_2)) = (2x_1 + x_2, x_1 + 2x_2)$ tego przekształcenia niekoniecznie na to wskazuje. Mamy jednak „nowy wzór” napisany we współrzędnych w bazie \mathcal{A} :

$$\phi(a(1, -1) + b(1, 1)) = \mathbf{1} \cdot a(1, -1) + \mathbf{3} \cdot b(1, 1).$$

Określone tu całkowicie intuicyjnie „kierunki rozciągania” tego endomorfizmu nazwiemy na kolejnym wykładzie wektorami własnymi endomorfizmu. Wkrótce też odpowiemy na dwa fundamentalne pytania.

- Jak opisać endomorfizmy, których macierze w pewnej bazie są diagonalne?
- Jak opisać endomorfizmy, które tak jak obrót w \mathbb{R}^2 nie mają w żadnej bazie macierzy diagonalnej?

1.1 Zadania do samodzielnej pracy

Zadania ilustrujące umiejętności niezbędne do zaliczenia przedmiotu oznaczone są symbolem ♠.

Przy tych zadaniach dodany jest opis umiejętności, które sprawdzają.

1. (♠ Wyznaczanie macierzy endomorfizmu w zadanej bazie)

Dla endomorfizmu $\phi : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ danego wzorem $\phi((x_1, x_2)) = (3x_1 + 4x_2, 5x_1 - 2x_2)$ oraz baz $\mathcal{A}_1 = \{(4, 1), (3, 1)\}$, $\mathcal{A}_2 = \{(2, 3), (5, 8)\}$, $\mathcal{A}_3 = \{(4, 2), (1, 1)\}$ znajdź macierze

$$A_1 = M(\phi)_{\mathcal{A}_1}^{\mathcal{A}_1}, \quad A_2 = M(\phi)_{\mathcal{A}_2}^{\mathcal{A}_2}, \quad A_3 = M(\phi)_{\mathcal{A}_3}^{\mathcal{A}_3}$$

oraz macierze odwracalne D, E, F spełniające $A_1 = D^{-1}A_2D$, $A_2 = E^{-1}A_3E$, $A_3 = F^{-1}A_1F$.

2. (♠ Wyznaczanie macierzy sumy i złożenia) Endomorfizm $\phi_1 \in \text{End}(\mathbb{R}^2)$ ma w bazie standardowej macierz A_1 , zaś endomorfizm $\phi_2 \in \text{End}(\mathbb{R}^2)$ ma w bazie $\mathcal{A} = ((1, -3), (0, 4))$ macierz A_2 , gdzie

$$A_1 = \begin{bmatrix} 2 & 1 \\ 3 & -4 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 0 & 1 \\ -3 & 5 \end{bmatrix}.$$

Znajdź macierze endomorfizmów $\phi_1 + \phi_2$, $\phi_2 \circ \phi_1$ oraz $\phi_2^3 = \phi_2 \circ \phi_2 \circ \phi_2$ w bazie \mathcal{A} .

3. Rozstrzygnij, czy dane macierze są podobne:

(a) $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ oraz $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$,

(b) $\begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}$ oraz $\begin{bmatrix} 3 & -1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 2 \end{bmatrix}$,

(c) $\begin{bmatrix} 1 & 2-i & 1+i \\ 4+i & 1+i & 0 \\ 1+i & 1 & 1 \end{bmatrix}$ oraz $\begin{bmatrix} 1 & 1+i & 2-i \\ 3-i & 1+i & 0 \\ 1 & 27 & 1-i \end{bmatrix}$,

(d) $\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$ oraz $\begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 1 \end{bmatrix}$,

(e) $\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ oraz $\begin{bmatrix} -2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$.

4. Wykaż, że funkcja $\text{tr} : M_n(K) \rightarrow K$ przypisująca macierzy A jej ślad jest przekształceniem liniowym. Wykaż, że $\text{tr}(AB) = \text{tr}(BA)$, dla dowolnych $A, B \in M_n(K)$.
5. Macierze $A, B \in M_n(\mathbb{R})$ są podobne. Czy macierze $A + I$ oraz $B - I$ mogą być podobne?
6. Macierze A oraz $3A$ są podobne. Wyznacz $\text{tr} A$ oraz $\det A$.
7. Niech $A \in M_n(K)$. Wykaż, że jeśli jedyną podobną do A jest A , to $A = aI$, dla pewnego $a \in K$.
8. Wykaż, że macierze $A = \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix}$ oraz $B = \begin{bmatrix} a & 1 \\ 0 & d \end{bmatrix}$ są podobne wtedy i tylko wtedy, gdy $a \neq d$.
9. Wykaż, że jeśli $A \in M_n(K)$ i $\det A \neq 0$, to dla każdej macierzy $B \in M_n(K)$ macierze AB oraz BA są podobne. Podaj przykład macierzy $A, B \in M_n(K)$, takich że macierze AB i BA nie są podobne.
10. Niech V będzie przestrzenią liniową nad ciałem K oraz niech $\phi \in \text{End}(V)$. Wykaż, że jeśli weźmiemy dwa różne elementy $a, b \in K$, wówczas:

$$\ker((\phi - a \text{id}_V) \circ (\phi - b \text{id}_V)) = \ker(\phi - a \text{id}_V) \oplus \ker(\phi - b \text{id}_V).$$

1.2 Uzupełnienie. Macierze endomorfizmu w różnych bazach

Przyglądając się izomorfizmom przestrzeni liniowych łatwo stwierdzimy, że macierze ich przekształceń w dowolnych (być może różnych) bazach są dowolnymi macierzami odwracalnymi. W szczególności dla dowolnego izomorfizmu istnieją bazy, w których ma on macierz identycznościową.

Obserwacja 1.5

Niech $\phi : K^n \rightarrow K^n$ będzie izomorfizmem. Istnieją takie bazy \mathcal{A}, \mathcal{B} przestrzeni K^n , że:

$$M(\phi)_{\mathcal{A}}^{\mathcal{B}} = I_n.$$

Dowód. Niech $(\alpha_1, \dots, \alpha_n)$ będzie bazą K^n . Wówczas $(\phi(\alpha_1), \dots, \phi(\alpha_n))$ jest również bazą K^n , bo ϕ to izomorfizm. A zatem biorąc pierwszą z tych baz jako \mathcal{A} , a drugą jako \mathcal{B} dostajemy, że $M(\phi)_{\mathcal{A}}^{\mathcal{B}} = I_n$. \square

Geometrycznie obserwacja ta może być interpretowana tak, że izomorfizm przestrzeni liniowych jest jedynie swego rodzaju przejściem z jednego układu współrzędnych do drugiego.

Obserwacja 1.6

Każda macierz odwracalna w $M_n(K)$ jest macierzą izomorfizmu $\phi : K^n \rightarrow K^n$ w pewnych bazach.

Dowód. Niech $G \in M_n(K)$ będzie macierzą odwracalną. Niech \mathcal{A}, \mathcal{B} będą takimi bazami przestrzeni K^n , że $M(\phi)_{\mathcal{A}}^{\mathcal{B}} = I_n$. Wystarczy pokazać, że istnieje baza \mathcal{C} przestrzeni K^n , że $G = M(\text{id})_{\mathcal{C}}^{\mathcal{A}}$, bo wówczas

$$M(\phi)_{\mathcal{C}}^{\mathcal{B}} = M(\phi)_{\mathcal{A}}^{\mathcal{B}} \cdot M(\text{id})_{\mathcal{C}}^{\mathcal{A}} = I_n G = G.$$

Otóż szukaną bazę \mathcal{C} można odczytać z kolumn macierzy AG , gdzie $A = M(\text{id})_{\mathcal{C}}^{\mathcal{A}}$. Wówczas mamy

$$G = A^{-1}(AG) = M(\text{id})_{st}^{\mathcal{A}} \cdot M(\text{id})_{\mathcal{C}}^{st} = M(\text{id})_{\mathcal{C}}^{\mathcal{A}}.$$

\square

A zatem dowolna macierz odwracalna rozmiaru n nad ciałem K jest macierzą dowolnego izomorfizmu przestrzeni wymiaru n nad ciałem K .

Definicja 1.6: Macierze równoważne

Macierze $A, B \in M_{m \times n}(K)$ nazywamy RÓWNOWAŻNYMI, jeśli istnieją takie macierze odwracalne $C \in M_m(K)$ oraz $D \in M_n(K)$ takie, że $B = CAD$.

Obserwacja 1.7

Dla macierzy $A, B \in M_{m \times n}(K)$ następujące warunki są równoważne:

- (i) macierze A oraz B są równoważne,
- (ii) istnieje przekształcenie liniowe $\phi : K^n \rightarrow K^m$ oraz bazy $\mathcal{A}, \mathcal{A}'$ przestrzeni K^n i bazy $\mathcal{B}, \mathcal{B}'$ przestrzeni K^m , że $A = M(\phi)_{\mathcal{A}}^{\mathcal{B}}$ oraz $B = M(\phi)_{\mathcal{A}'}^{\mathcal{B}'}$,
- (iii) B może być otrzymana z A ciągiem operacji elementarnych na wierszach i kolumnach,
- (iv) $r(A) = r(B)$.

Dowód. Dowodzimy (i) \Rightarrow (ii). Niech $M(\phi)_{st}^{st} = A$ oraz niech $B = CAD$. Przez \mathcal{C}, \mathcal{D} określamy bazy złożone odpowiednio z kolumn macierzy odwracalnych C^{-1} i D . Wówczas $C = M(\text{id})_{st}^{\mathcal{C}}$ oraz $D = M(\text{id})_{\mathcal{D}}^{st}$. Stąd $B = CAD = M(\phi)_{\mathcal{D}}^{\mathcal{C}}$.

Implikacja (ii) \Rightarrow (iii) wynika z tego, że macierz jest odwracalna wtedy i tylko wtedy, gdy jest iloczynem macierzy operacji elementarnych (I semestr). W szczególności skoro $B = M(\text{id})_{\mathcal{B}'}^{\mathcal{B}'} \cdot A \cdot M(\text{id})_{\mathcal{A}'}^{\mathcal{A}'}$, gdzie $M(\text{id})_{\mathcal{B}'}^{\mathcal{B}'}$ oraz $M(\text{id})_{\mathcal{A}'}^{\mathcal{A}'}$ są odwracalne, to mamy (iii).

Implikacja (iii) \Rightarrow (iv) jest jasna, ponieważ wykonanie operacji elementarnej nie zmienia rzędu.

Natomiast jeśli zachodzi (iv) to znaczy, że za pomocą operacji elementarnych na wierszach i kolumnach każdą z macierzy A i B można sprowadzić za pomocą operacji elementarnych do macierzy $X = [x_{ij}]$, gdzie $r = r(A) = r(B)$ oraz

$$x_{ij} = \begin{cases} 1, & \text{dla } i = j = 1, \dots, r, \\ 0, & \text{dla pozostałych } i, j, \end{cases}$$

czyli do macierzy rozmiaru $m \times n$ o postaci blokowej

$$X = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}.$$

Rzeczywiście, wiemy że macierze tego samego rzędu można sprowadzić za pomocą operacji elementarnych na wierszach do postaci A', B' , które są w zredukowanej postaci schodkowej i mają $r = r(A) = r(B)$ niezerowych wierszy. Innymi słowy istnieją macierze odwracalne $E, G \in M_m(K)$, że $A' = EA$ oraz $B' = GB$, gdzie E, G — iloczyny odpowiednich macierzy operacji elementarnych na wierszach. Teraz zaczynamy wykonywać operacje kolumnowe. Po pierwsze porządkujemy kolumny tak, by wyrazy wiodące stojące w pierwszych r wierszach stały w pierwszych r kolumnach. Innymi słowy za pomocą operacji kolumnowych sprowadzamy macierze A' oraz B' do postaci A'' oraz B'' postaci blokowej:

$$A'' = \begin{bmatrix} I_r & * \\ 0 & 0 \end{bmatrix}, \quad B'' = \begin{bmatrix} I_r & ** \\ 0 & 0 \end{bmatrix}.$$

Widzimy zatem, że za pomocą pierwszych r kolumn można za pomocą operacji kolumnowych doprowadzić te macierze do postaci X . Innymi słowy istnieją macierze odwracalne E, F, G, H , że

$$X = EAF \quad \text{oraz} \quad X = GBH.$$

Zatem $EAF = GBH$, czyli

$$A = E^{-1}GBHF^{-1}.$$

Macierze $E^{-1}G$ oraz HF^{-1} są odwracalne, więc uzyskujemy (i). □

W świetle przytoczonego twierdzenia powyższa definicja mówi, że macierze są równoważne wtedy i tylko wtedy, gdy są macierzami tego samego przekształcenia liniowego. Równoważność macierzy nie jest na pozór pojęciem mówiącym za wiele o geometrii przekształcenia, choć jest ono przydatne z punktu widzenia samej teorii macierzy. W jednym z kolejnych dodatków powiemy jednak o macierzach wielomianowych i problemie charakteryzacji podobieństwa macierzy nad dowolnym ciałem. Wówczas pojęcie równoważności owych macierzy wielomianowych (odpowiednio rozumiane) okaże się zaskakująco pożyteczne.

Wniosek 1.1

Dla każdego przekształcenia liniowego $\phi : K^n \rightarrow K^m$ rzędu r istnieją bazy \mathcal{A}, \mathcal{B} przestrzeni K^n, K^m takie, że $M(\phi)_{\mathcal{A}}^{\mathcal{B}} = A$, przy czym $A \in M_{m \times n}(K)$ oraz $A = [a_{ij}]$, gdzie

$$a_{ij} = \begin{cases} 1, & \text{dla } i = j = 1, \dots, r, \\ 0, & \text{dla pozostałych } i, j, \end{cases}$$

czyli do macierzy rozmiaru $m \times n$ o postaci blokowej $\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$.

Nietrudno widzieć, że równoważność jest relacją równoważności w zbiorze $M_{m \times n}(K)$. Wniosek wyżej mówi, że jest $\min(m, n) + 1$ klas równoważności macierzy rozmiaru $m \times n$ (nad dowolnym ciałem), bowiem każdą macierz rozmiaru $m \times n$ można sprowadzić, za pomocą operacji elementarnych na wierszach i kolumnach do jednej z $\min(m, n) + 1$ macierzy zero-jedynkowych o postaci blokowej jak wyżej.

Oczywiście rozważano bardziej skomplikowane problemy. Załóżmy, że mamy macierz rozmiaru $m \times (r + s)$ o postaci blokowej z blokami $A \in M_{m \times r}(K)$ oraz $B \in M_{m \times s}$ postaci

$$[A \ B]. \quad (\dagger)$$

Założmy też, że możemy wykonywać wszystkie operacje wierszowe (na całej macierzy blokowej), ale operacje kolumnowe mogą być wykonywane „w obrębie” bloku kolumn: od 1 do r lub „w obrębie” bloku kolumn od $r + 1$ do $r + s$ (to znaczy: nie można na przykład dodać do kolumny r kolumny $r + s$, albo ich zamienić, ale można zamienić kolumny $r + 1, r + 2$ należące do bloku B).

Oto przykład. Rozważmy macierz M o blokach 3×2 oraz 3×1 postaci:

$$M = \left[\begin{array}{cc|c} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{array} \right].$$

Wówczas wykonać możemy serię operacji wierszowych i kolumnowych, które „nie mieszają” tych bloków, dostając:

$$\begin{aligned} \left[\begin{array}{cc|c} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{array} \right] &\xrightarrow{w_2 - 4w_1} \left[\begin{array}{cc|c} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 7 & 8 & 9 \end{array} \right] \xrightarrow{w_3 - 7w_1} \left[\begin{array}{cc|c} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & -6 & -12 \end{array} \right] \xrightarrow{(-3)w_2} \\ &\left[\begin{array}{cc|c} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & -6 & -12 \end{array} \right] \xrightarrow{w_3 + 6w_2} \left[\begin{array}{cc|c} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{array} \right] \xrightarrow{w_1 - 2w_2} \left[\begin{array}{cc|c} 1 & 0 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{array} \right]. \end{aligned}$$

Uzyskaliśmy postać wierszową zredukowaną. Teraz czas na operacje kolumnowe, respektujące bloki.

$$\left[\begin{array}{cc|c} 1 & 0 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{array} \right] \xrightarrow{(-1)k_3} \left[\begin{array}{cc|c} 1 & 0 & 1 \\ 0 & 1 & -2 \\ 0 & 0 & 0 \end{array} \right] \xrightarrow{w_2 + 2w_1} \left[\begin{array}{cc|c} 1 & 0 & 1 \\ 2 & 1 & 0 \\ 0 & 0 & 0 \end{array} \right] \xrightarrow{k_1 - 2k_2} \left[\begin{array}{cc|c} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{array} \right].$$

Zachęcam do wykazania, że problem macierzy o postaci (\dagger) można rozwiązać sprowadzając każdą z nich do nieoczywistej postaci blokowej

$$\left[\begin{array}{ccc|cc} I_a & 0 & 0 & 0 & I_a & 0 \\ 0 & I_b & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I_c & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right].$$

Czy za pomocą takich operacji elementarnych można uzyskać jedynie SKOŃCZENIE WIELE MACIERZY (zerojedynkowych)? Jaką mają postać? Mnożeniu przez jakie macierze odpowiada ten problem?

A jeśli mielibyśmy analogiczny problem dotyczący macierzy o trzech blokach

$$[A \ B \ C]?$$

A gdybyśmy mieli dowolną macierz blokową i dopuszczalne by było tylko „działanie w obrębie bloków wierszy” i „działanie w obrębie bloków kolumn” (oczywiście na całą macierz, nie tylko na bloki)?

Powyższe pytania prowadzą do tzw. problemów macierzowych i były rozważane od początku XX wieku. W drugiej jego połowie były jednym z nurtów rozwoju ważnej gałęzi algebry: teorii reprezentacji algebr skończenie wymiarowych. Więcej (wraz z przykładami) można przeczytać w rozdziale pierwszym tekstu: https://www.matem.unam.mx/~christof/cursos/12_SAB/1111_RepThBook.pdf.

1.3 Dodatek. Dyskretny układ dynamiczny

Teoria endomorfizmów, a w szczególności problem znajdowania macierzy diagonalnej podobnej do danej ma liczne zastosowania między innymi w tak zwanych dyskretnych układach dynamicznych.

Rozważmy następujący przykład⁶ Weźmy „ekosystem” złożony z:

- m_n (milionów) much,
- z_n (tysiący) żab.

Po roku liczba much/żab zmienia się zgodnie z (nierealnym) modelem liniowym:

$$\begin{cases} m_{n+1} &= -0,36z_n + 1,22m_n, \\ z_{n+1} &= 0,38z_n + 0,24m_n. \end{cases} \quad (\spadesuit)$$

Jak rozumieć taki model? Muchy się rozmnażają, ale też są zjadane. Żaby gdy nie mają co jeść, wymierają. Mimo wszystko co roku również się rozmnażają, ale w zupełnie innym tempie. Oto nasze pytanie, **Jaka jest dynamika tego układu w zależności od wyboru z_0, m_0 ?**

Widzimy, że naśladując rozumowania dotyczące rekurencji mamy:

$$\begin{bmatrix} z_{n+1} \\ m_{n+1} \end{bmatrix} = \begin{bmatrix} 0,38 & 0,24 \\ -0,36 & 1,22 \end{bmatrix}^n \cdot \begin{bmatrix} z_0 \\ m_0 \end{bmatrix}. \quad (\diamond)$$

Niech $\phi : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ dany będzie macierzą

$$M(\phi)_{st} = \begin{bmatrix} 0,38 & 0,24 \\ -0,36 & 1,22 \end{bmatrix}.$$

Czytelnik zechce zauważyć, że $\phi((1, 3)) = 1,1 \cdot (1, 3)$ oraz $\phi((2, 1)) = 0,5 \cdot (2, 1)$. Mamy zatem, dla $a, b \in \mathbb{R}$:

$$\phi(a(1, 3) + b(2, 1)) = 1,1 \cdot a(1, 3) + 0,5 \cdot b(2, 1) \iff M(\phi)_{\mathcal{A}}^{\mathcal{A}} = \begin{bmatrix} 1,1 & 0 \\ 0 & 0,5 \end{bmatrix}.$$

Dlaczego postać diagonalna rozważanego endomorfizmu jest tak wygodna? Przepisujemy równanie (\diamond) w bazie \mathcal{A} , przyjmując:

$$\begin{bmatrix} z_0 \\ m_0 \end{bmatrix} = c_0 \cdot \begin{bmatrix} 1 \\ 3 \end{bmatrix} + d_0 \cdot \begin{bmatrix} 2 \\ 1 \end{bmatrix}, \quad \begin{bmatrix} z_{n+1} \\ m_{n+1} \end{bmatrix} = c_{n+1} \cdot \begin{bmatrix} 1 \\ 3 \end{bmatrix} + d_{n+1} \cdot \begin{bmatrix} 2 \\ 1 \end{bmatrix},$$

skąd dostajemy:

$$\begin{bmatrix} c_{n+1} \\ d_{n+1} \end{bmatrix} = \begin{bmatrix} 1,1 & 0 \\ 0 & 0,5 \end{bmatrix}^n \cdot \begin{bmatrix} c_0 \\ d_0 \end{bmatrix} = \begin{bmatrix} (1,1)^n c_0 \\ (0,5)^n d_0 \end{bmatrix}.$$

Zatem:

$$\begin{cases} z_{n+1} &= 1 \cdot (1,1)^n c_0 + 2 \cdot (0,5)^n d_0 \\ m_{n+1} &= 3 \cdot (1,1)^n c_0 + 1 \cdot (0,5)^n d_0 \end{cases}. \quad (\heartsuit)$$

⁶Źródło. K. Behrend, *Dynamical Systems and Matrix Algebra*, <http://www.math.ubc.ca/~behrend/math223/DynSys.pdf>. Zamiast czytać można też obejrzeć:

Przykład: muchy i żaby

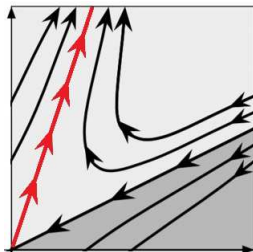


Po co nam potęgi macierzy? Film z czasów pandemii: <https://youtu.be/NkmoGML5uxs>

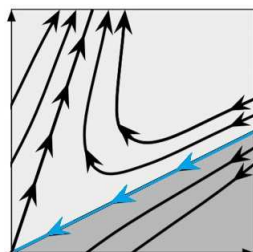
Zwróćmy uwagę, że uzyskany opis jest znacznie wygodniejszy od wyjściowego. Opisywanie „wektora much i żab” w standardowej bazie \mathbb{R}^2 układem (♠) zamiast w bazie z wektorów własnych, za pomocą układu (♡), nie pozwala poprawnie ocenić dynamiki układu, czyli tego jakie są skutki wyboru określonych wartości początkowych z_0, m_0 .

Interpretacja graficzna uzyskanego wyniku w zależności od wyboru c_0, d_0 .

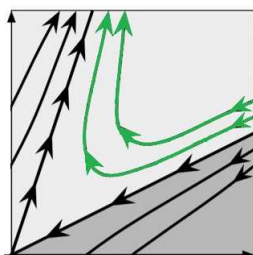
- Jeśli $c_0 = 1, d_0 = 0$, czyli $(z_0, m_0) = (1, 3)$ oraz $(z_{n+1}, m_{n+1}) = ((1, 1)^n, 3 \cdot (1, 1)^n)$, to populacje **rosną** w tym samym tempie: stosunek much do żab jest stały!



- Jeśli $c_0 = 0, d_0 = 1$, czyli $(z_0, m_0) = (2, 1)$ oraz $(z_{n+1}, m_{n+1}) = (2 \cdot (0, 5)^n, (0, 5)^n)$, to populacje **maleją** w tym samym tempie: stosunek much do żab jest stały!



- Jeśli $c_0 > 0, d_0 > 0$, to populacje być może pewien czas maleją, potem przyrastają. Stosunek żab do much zmierza „asymptotycznie” do 1 : 3 (w istocie: 1 : 3000). A jakie układy c_0, d_0 prowadzą do zagłady gatunków? Jest ona, jak się okazuje, możliwa.



Zagadnienia tu opisane są oczywiście jedynie drobną zabawką, ale opowiadają o jednym z ważnych zastosowań teorii endomorfizmów – rozwiązywaniu układów liniowych równań różniczkowych i różnicowych.

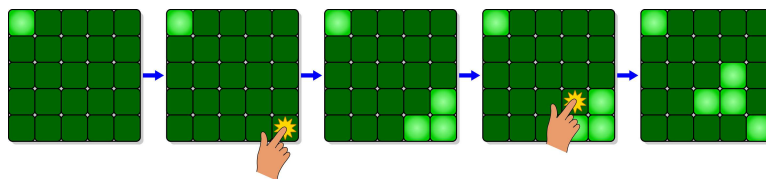
Na koniec warto jednak pomyśleć chwilę nad pewną komplikacją. Wyobraźmy sobie, że ktoś chce STEROWAĆ populacją much i żab mimo znajomości jej dynamiki. Jak to robi? Każdego roku wprowadza do ekosystemu pewną liczbę osobników, ale – uwaga – zachowując ich wyjściowe proporcje! Oto jak „wygląda” ekosystem po dwóch latach.

$$\begin{bmatrix} z'_2 \\ m'_2 \end{bmatrix} = \begin{bmatrix} 0,38 & 0,24 \\ -0,36 & 1,22 \end{bmatrix}^2 \begin{bmatrix} z_0 \\ m_0 \end{bmatrix} + a_1 \begin{bmatrix} 0,38 & 0,24 \\ -0,36 & 1,22 \end{bmatrix} \begin{bmatrix} z_0 \\ m_0 \end{bmatrix} + a_2 \begin{bmatrix} z_0 \\ m_0 \end{bmatrix}.$$

Jak teraz opisać liczbę osobników każdego roku w zależności od a_1, a_2 ? Czy można uzyskać dowolny rezultat? Jak zależy to od macierzy układu? Mowa tu o tzw. teorii sterowania. Zainteresowanych odsyłam do tekstu: <http://cse.lab.imtlucca.it/~bemporad/teaching/ac/pdf/01-Introduction.pdf>.

1.4 Trivia. Lights Out

W 1995 roku Tiger Electronics wydało grę *Lights Out*. Gra składa się z tablicy rozmiaru 5 na 5 złożonej z 25 przycisków, z których każdy jest w jednym z dwóch stanów: włączony (wtedy przycisk jest podświetlony) lub wyłączony. Po rozpoczęciu gry włącza się losowa konfiguracja przycisków. Naciśnięcie dowolnego przycisku spowoduje przełączenie tego przycisku, a także jego sąsiadów (ale nie po przekątnej).



Ilustracja gry w Lights Out. Źródło: domena publiczna.

Zadaniem jest wyłączenie wszystkich świateł, najlepiej za pomocą jak najmniejszej liczby ruchów.

W 1998 roku Marlow Anderson oraz Todd Fell użyli metod algebry liniowej⁷ do pokazania, że nie wszystkie konfiguracje prowadzą do rozwiązania oraz, że dla każdej rozwiązywalnej konfiguracji istnieją dokładnie 4 strategie (nie mające zbędnych ruchów). Idea jest prosta: każdą z tablic reprezentować można jednoznacznie jako element przestrzeni $M_5(\mathbb{Z}_2)$. W ten sposób wciśnięcie klawisza w i -tym wierszu i j -tej kolumnie odpowiada dodawaniu pewnej macierzy $T_{ij} \in M_5(\mathbb{Z}_2)$, na przykład (dla ilustracji wyżej):

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

Dla dowolnych macierzy $A, B \in M_5(\mathbb{Z}_2)$ mamy $A + B = B + A$ oraz $A + A = 0$, więc widzimy, że:

- kolejność wciskania przycisków nie ma znaczenia dla strategii,
- żadnego przycisku nie trzeba wciskać więcej niż raz.

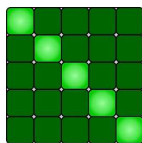
Załóżmy, że wyjściową konfigurację świateł opisuje macierz B . Problem wyłączenia świateł w B równoważny jest zatem pytaniu: czy B należy do $\text{lin}(T_{ij}, 1 \leq i, j \leq 5)$? A zatem jest to w istocie problem rozwiązania układu równań — w tym przypadku o 25 niewiadomych (o współczynnikach w \mathbb{Z}_2). Nietrudno sprawdzić, że macierz $A \in M_{25 \times 25}(\mathbb{Z}_2)$ tego układu ma 25 bloków rozmiaru 5×5 postaci:

$$A = \begin{bmatrix} C & I_5 & 0 & 0 & 0 \\ I_5 & C & I_5 & 0 & 0 \\ 0 & I_5 & C & I_5 & 0 \\ 0 & 0 & I_5 & C & I_5 \\ 0 & 0 & 0 & I_5 & C \end{bmatrix}, \quad \text{gdzie} \quad C = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Widzimy zatem, że sprawdzając, czy można „zgasić światła” w macierzy B rozwiązujemy układ równań $Ax = b$, gdzie b jest wektorem o 25 współrzędnych złożonym z kolejnych wyrazów macierzy B . Dla przykładu, gdy B jest macierzą po prawej na ilustracji wyżej, to wektor b ma postać:

$$b = (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1).$$

Czym jest $x \in \mathbb{Z}_2^{25}$? To wektor wskazujący które przyciski mamy wcisnąć, aby ze zgaszonej macierzy dostać macierz B . Odnotujmy dwie ciekawe sytuacje, związane z teorią endomorfizmów: pierwsza, gdy rozwiązanie układu $Ax = 0$ zwraca strategie, które nie zmieniają oświetlenia na tablicy oraz druga, gdy rozwiązanie układu $Ax = x$ zwraca te strategie, w których wciśnięcie odpowiednich przycisków sprawia, że jedynie wciśnięte przyciski są zapalone. Przykładem tej sytuacji jest wciśnięcie przycisków na przekątnej, startując od pustej tablicy. Jest jeszcze 31 innych przykładów (bo $r(A - I) = 20$). Jakie to przykłady?



⁷Wyjaśnienie tego szkicu i ładny opis problemu można znaleźć w rozdziale 24. pięknej książki „Permutation puzzles”, dostępnej pod adresem <http://www.sfu.ca/~jtmulhol/math302/notes/permutation-puzzles-book.pdf> (strona autora). Jeśli zechcecie tam Państwo zajrzeć, dowiedzie się czemu ten temat umieściłem w kontekście wektorów i wartości własnych.

Rozdział 2

Wartości własne endomorfizmu, wielomian charakterystyczny

Na poprzednim wykładzie wprowadziliśmy pojęcie endomorfizmu oraz jego macierzy w bazie. Pokazaliśmy, że dowolne dwie macierze endomorfizmu są podobne oraz ustaliliśmy podstawowe niezmienniki podobieństwa: rząd, ślad oraz wyznacznik. Dziś¹ zajmiemy się pojęciami wektora i wartości własnej endomorfizmu oraz odniesiemy je do problemu rozstrzygnięcia, czy endomorfizm może mieć w pewnej bazie macierz diagonalną. Wprowadzimy też niezmiennik podobieństwa — wielomian charakterystyczny.

Definicja 2.1: Wektor własny, podprzestrzeń własna

Niech V będzie przestrzenią liniową nad ciałem K oraz niech $\phi \in \text{End}(V)$.

- Wektor $\alpha \in V$ nazywamy WEKTOREM WŁASNYM endomorfizmu ϕ jeśli:
 - $\alpha \neq 0$,
 - istnieje $a \in K$ takie, że $\phi(\alpha) = a \cdot \alpha$.
- Element $a \in K$ spełniający powyższe warunki nazywamy WARTOŚCIĄ WŁASNĄ endomorfizmu ϕ , zaś o wektorze α mówimy, że jest WEKTOREM WŁASNYM ϕ o WARTOŚCI WŁASNEJ a .
- Jeśli a jest wartością własną endomorfizmu $\phi \in \text{End}(V)$, to zbiór

$$V_{(a)} = \{\alpha \in V \mid \phi(\alpha) = a \cdot \alpha\}$$

nazywamy PODPRZESTRZENIĄ^a WŁASNĄ ENDOMORFIZMU ϕ odpowiadającą wart. własnej a .

^aPodprzestrzeń ta składa się z wektorów własnych endomorfizmu ϕ o wartości własnej a oraz z wektora zerowego.

Oto przykłady.

- Jeśli $\phi : K^n \rightarrow K^n$ jest jednokładnością o skali a , to każdy niezerowy wektor K^n jest wektorem własnym o wartości własnej a . Zatem $V_{(a)} = K^n$.
- Endomorfizm $\phi \in \text{End}(\mathbb{R}^2)$ o macierzy postaci:

$$M(\phi)_{st}^{st} = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$$

ma dwie wartości własne: 1, 2 oraz $V_{(1)} = \text{lin}((1, 0))$, $V_{(2)} = \text{lin}((0, 1))$, co można sprawdzić wypisując wzór na ϕ lub sprawdzając, że wektory $(1, 0)$ oraz $(0, 1)$ są wektorami własnymi macierzy $M(\phi)_{st}^{st}$:

$$\begin{aligned} \phi((1, 0)) &= \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = 1 \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \\ \phi((0, 1)) &= \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} = 2 \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \end{aligned}$$

¹Ostatnia aktualizacja: 06.05.2023 r.

- Endomorfizm $\phi \in \text{End}(\mathbb{R}^3)$ zadany wzorem

$$\phi((x_1, x_2, x_3)) = (x_1 + 2x_2 + 4x_3, 3x_1 + 2x_2 + 2x_3, x_1 + 6x_2)$$

ma wektor własny $(1, 1, 1)$ o wartości własnej 7, tzn. $\phi((1, 1, 1)) = (7, 7, 7) = 7 \cdot (1, 1, 1)$.

- Choć na tym wykładzie interesować nas będą jedynie endomorfizmy przestrzeni skończenie wymiarowych, warto wspomnieć przykłady nieskończenie wymiarowe: weźmy $T \in \text{End}(K^\infty)$ postaci:

$$T((a_1, a_2, a_3, \dots)) = (a_2, a_3, a_4, \dots).$$

Nietrudno sprawdzić, że dowolny element ciała K jest wartością własną tego endomorfizmu. Czy potraficie Państwo wskazać odpowiednie wektory własne?

- Branie pochodnej to endomorfizm przestrzeni $K[x]$. Łatwo widzieć, że jego jedyną wartością własną jest 0. A gdy zamiast $K[x]$ weźmiemy podprzestrzeń funkcji różniczkowalnych w $F(\mathbb{R}, \mathbb{R})$?
- Endomorfizm $\phi : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ postaci

$$\phi((x_1, x_2)) = (-x_2, x_1)$$

nie ma rzeczywistych wartości własnych. Z geometrycznego punktu widzenia jest to obrót o $\pi/2$.

Określamy również pojęcie wektora własnego i wartości własnej macierzy kwadratowej.

Definicja 2.2: Wartość własna macierzy

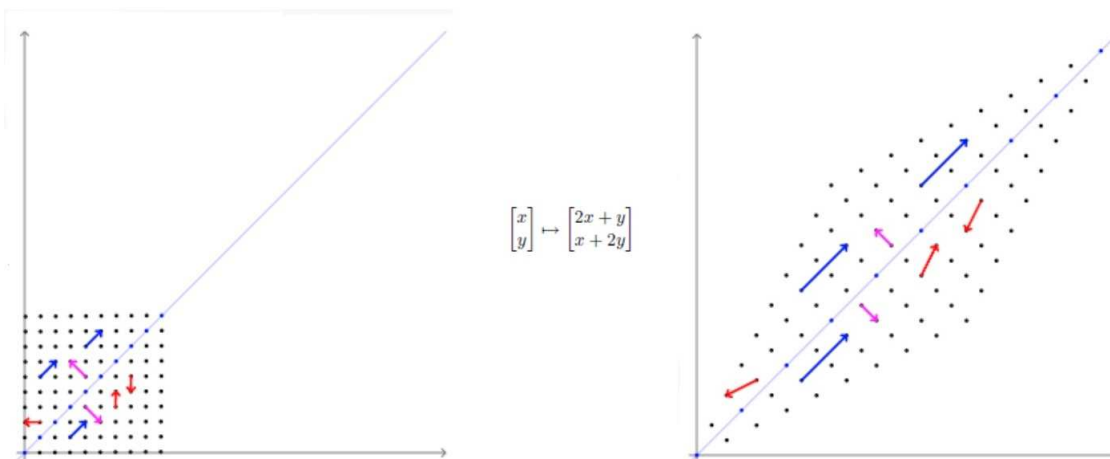
Niech $A \in M_n(K)$. Mówimy, że $a \in K$ jest WARTOŚCIĄ WŁASNĄ MACIERZY A , jeśli a jest wartością własną endomorfizmu $\phi \in \text{End}(K^n)$ zadanego wzorem $M(\phi)_{st}^{st} = A$. Niezerowy wektor $v \in K^n$ nazwiemy WEKTOREM WŁASNYM MACIERZY A o wartości własnej a , jeśli $A \cdot v = a \cdot v$.

Z geometrycznego punktu widzenia powyższe definicje są bardzo czytelne. Wektor własny endomorfizmu to taki niezerowy wektor, który w wyniku działania endomorfizmu zostaje jedynie przeskalowany.

Przykład. Na \mathbb{R}^2 działamy przekształceniem liniowym ϕ przeprowadzającym wektor $\begin{bmatrix} x \\ y \end{bmatrix}$ na wektor

$$\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2x + y \\ x + 2y \end{bmatrix}.$$

Wektorami własnymi tego przekształcenia są (na przykład, bo każda ich skalarna wielokrotność też) $(1, -1)$ oraz $(1, 1)$, zaś odpowiadające im wartości własne to 1, 3. Innych wartości własnych ϕ nie ma.



Źródło: Wikipedia²

²Uwaga — obiekty na rysunkach ilustrują tzw. wektory zaczepione w (tzw.) punktach. Formalną definicję poznamy za kilka wykładów, ale raczej nikt nie powinien mieć problemu z interpretacją.

Od tej pory zakładamy aż do odwołania, że rozważane przestrzenie liniowe są skończonego wymiaru. Pozostałą część wykładu poświęcimy problemowi znajdowania wartości własnych endomorfizmu. W tym celu kluczowe jest przypomnienie fundamentalnego rezultatu poznanego przez nas w pierwszym semestrze.

Twierdzenie 2.1

Niech $A \in M_n(K)$. Następujące warunki są równoważne:

- (a) układ równań postaci $Ax = 0$ ma NIEZEROWE rozwiązanie $v \in K^n$,
- (b) $\det(A) = 0$.

Zacznijmy od przykładu. Niech $\phi : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ będzie endomorfizmem przestrzeni \mathbb{R}^3 zadany macierzą:

$$M(\phi)_{st}^{st} = \begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 1 \end{bmatrix}.$$

Znalezienie wektorów i wartości własnych endomorfizmu ϕ sprowadza się do rozwiązania układu:

$$\begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \lambda \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} \lambda x_1 \\ \lambda x_2 \\ \lambda x_3 \end{bmatrix}.$$

Przekształcając równoważnie mamy zatem:

$$\begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \lambda \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \iff \left(\begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 1 \end{bmatrix} - \lambda \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right) \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

Należy więc rozstrzygnąć dla jakich wartości $\lambda \in \mathbb{R}$ jednorodny układ o macierzy $M(\phi)_{st}^{st} - \lambda I_3$ postaci:

$$\begin{bmatrix} 1 - \lambda & 2 & 2 \\ 2 & 1 - \lambda & 2 \\ 2 & 2 & 1 - \lambda \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

MA NIEZEROWE ROZWIĄZANIE, gdyż wektor własny ma być niezerowy. Korzystamy z Twierdzenia 2.1. Macierz $M(\phi)_{st}^{st} - \lambda I$ musi być rzędu < 3 , więc szukamy λ takich, że $\det(M(\phi)_{st}^{st} - \lambda I) = 0$. Mamy:

$$\begin{vmatrix} 1 - \lambda & 2 & 2 \\ 2 & 1 - \lambda & 2 \\ 2 & 2 & 1 - \lambda \end{vmatrix} = -(\lambda - 5)(\lambda + 1)^2.$$

Stąd wartościami własnymi ϕ są -1 oraz 5 , a po rozwiązaniu układów o macierzach $M(\phi)_{st}^{st} + I$ oraz $M(\phi)_{st}^{st} - 5I$ dostajemy podprzestrzenie własne:

$$V_{(-1)} = \text{lin}((-1, 1, 0), (-1, 0, 1)), \quad V_{(5)} = \text{lin}((1, 1, 1)).$$

Zauważmy, że układ $\mathcal{A} = ((-1, 1, 0), (-1, 0, 1), (1, 1, 1))$ jest bazą \mathbb{R}^3 złożoną z wektorów własnych ϕ .

Definicja 2.3: Wielomian charakterystyczny macierzy/endomorfizmu

Dla macierzy $A \in M_n(K)$ WIELOMIANEM CHARAKTERYSTYCZNYM A nazywamy:

$$w_A(\lambda) = \det(A - \lambda I) \in K[\lambda].$$

Niech $\phi \in \text{End}(V)$, gdzie V jest przestrzenią skończonego wymiaru nad ciałem K . Niech \mathcal{A} będzie dowolną bazą przestrzeni V . WIELOMIANEM CHARAKTERYSTYCZNYM endomorfizmu ϕ nazywamy

$$w_\phi(\lambda) = \det(M(\phi)_{\mathcal{A}}^{\mathcal{A}} - \lambda I) \in K[\lambda].$$

Obserwacja 2.1

Wielomian charakterystyczny endomorfizmu $\phi \in \text{End}(V)$ nie zależy od wyboru bazy, to znaczy: dla dowolnych baz \mathcal{A}, \mathcal{B} przestrzeni skończenie wymiarowej V mamy

$$\det(M(\phi)_{\mathcal{A}} - \lambda I) = \det(M(\phi)_{\mathcal{B}} - \lambda I).$$

Jeśli $A, B \in M_n(K)$ są podobne oraz $A = M(\phi)_{st}^{st}, B = M(\psi)_{st}^{st}$, to $w_\phi(\lambda) = w_\psi(\lambda)$.

Dowód. Niech C będzie macierzą odwracalną taką, że $C^{-1}AC = B$. Wówczas także

$$C^{-1}(A - \lambda I)C = C^{-1}AC - C^{-1}\lambda I \cdot C = B - \lambda I.$$

Teza wynika zatem ze wzoru Cauchy'ego:

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

□

Przykłady.

- Dla $\phi \in \text{End}(\mathbb{R}^3)$ danego wzorem $\phi((x_1, x_2, x_3)) = (x_1 + 2x_2 + 2x_3, 2x_1 + x_2 + 2x_3, 2x_1 + 2x_2 + x_3)$ mamy

$$w_\phi(\lambda) = -(\lambda - 5)(\lambda + 1)^2 = -\lambda^3 + 3\lambda^2 + 9\lambda + 5.$$

- Dla $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ mamy $A - \lambda I = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} - \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} = \begin{bmatrix} 1 - \lambda & 2 \\ 3 & 4 - \lambda \end{bmatrix}$, a zatem

$$w_A(\lambda) = \begin{vmatrix} 1 - \lambda & 2 \\ 3 & 4 - \lambda \end{vmatrix} = \lambda^2 - 5\lambda + 4 - 6 = \lambda^2 - 5\lambda - 2.$$

- Niech $A \in M_n(K)$ będzie macierzą górnotrójkątną, dolnotrójkątną lub diagonalną, która na przekątnej ma kolejno wyrazy a_{11}, \dots, a_{nn} . Wówczas

$$w_A(\lambda) = (a_{11} - \lambda) \cdot (a_{22} - \lambda) \cdot \dots \cdot (a_{nn} - \lambda).$$

Zwróćmy uwagę, że w dowodzie pojawił się następujący ważny fakt, z którego wielokrotnie jeszcze skorzystamy, godny również podsumowania w formie diagramowej.

Wniosek 2.1

Niech $A, B \in M_n(K)$. Wówczas dla dowolnego $\lambda \in K$ równoważne są warunki:

- macierze A, B są podobne,
- macierze $A - \lambda I$ oraz $B - \lambda I$ są podobne.

Co więcej, jeśli zachodzi dowolny z powyższych warunków, to istnieje taka macierz odwracalna $C \in M_n(K)$, że $B = C^{-1}AC$ oraz $B - \lambda I = C^{-1}(A - \lambda I)C$.



Uwaga:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

mają równe wielomiany charakterystyczne $(1 - \lambda)^2$, ale nie są podobne (nad dowolnym ciałem).

Obserwacja 2.2

Niech $A = (a_{ij}) \in M_n(K)$. Zachodzi równość:

$$w_A(\lambda) = \det(A - \lambda I) = (-1)^n \lambda^n + (-1)^{n-1} \operatorname{tr}(A) \lambda^{n-1} + \dots + \det A.$$

Dowód. Dla $n = 1$ teza jest oczywista. Dla $n = 2$ mamy:

$$\begin{vmatrix} a_{11} - \lambda & a_{12} \\ a_{21} & a_{22} - \lambda \end{vmatrix} = (a_{11} - \lambda)(a_{22} - \lambda) - a_{12}a_{21} = \lambda^2 - (a_{11} + a_{22})\lambda + a_{11}a_{22} - a_{12}a_{21} = \lambda^2 - \operatorname{tr} A \cdot \lambda + \det A.$$

Przeprowadzimy dwa rozumowania indukcyjne³ ze względu na n . Oto ich tezy.

- (i) Dla dowolnych macierzy $X = [x_{ij}], Y = [y_{ij}] \in M_n(K)$ funkcja $f(\lambda) = \det(X + \lambda Y)$ jest funkcją wielomianową stopnia nie większego niż n .
- (ii) Niech $A = [a_{ij}] \in M_n(K)$, dla $n \geq 1$. Wówczas

$$\det(A - \lambda I) = (a_{11} - \lambda)(a_{22} - \lambda) \dots (a_{nn} - \lambda) + v(\lambda),$$

gdzie v jest wielomianem stopnia co najwyżej $n - 2$.

Pierwszy fakt mówi, że wyznacznik macierzy rozmiaru n , której każdy wyraz jest wielomianem zmiennej λ stopnia nie większego niż 1 (o współczynnikach w K) jest wielomianem stopnia równego co najwyżej n . Dla $n = 1$ teza jest oczywista. Natomiast krok indukcyjny dla macierzy postaci $Z = X + \lambda Y$ otrzymujemy poprzez rozwinięcie Laplace'a względem pierwszego wiersza. W ten sposób otrzymujemy sumę postaci:

$$\det Z = (x_{11} + \lambda y_{11}) \cdot \det Z_{11} - (x_{12} + \lambda y_{12}) \cdot \det Z_{12} + \dots + (-1)^n \cdot (x_{1n} + \lambda y_{1n}) \cdot \det Z_{1n}.$$

Oczywiście każda z macierzy Z_{1i} powstałych z Z przez usunięcie pierwszego wiersza i kolumny i -tej jest również postaci $X' + \lambda Y'$, dla pewnych $X', Y' \in M_{n-1}(K)$. A zatem z założenia indukcyjnego każdy z wyznaczników $\det Z_{1i}$ jest wielomianem zmiennej λ stopnia nie większego niż $n - 1$. Stąd $\deg \det Z \leq n$.

Dowodzimy (ii). Policzmy wyznacznik macierzy $B = A - \lambda I$ za pomocą rozwinięcia Laplace'a względem pierwszego wiersza tej macierzy, złożonego z wyrazów: $a_{11} - \lambda, a_{12}, a_{13}, \dots, a_{1n}$. Niech B_{ij} będą macierzami powstałymi z B przez wykreślenie i -tego wiersza i j -tej kolumny. Szukany wyznacznik jest zatem sumą:

$$(a_{11} - \lambda) \cdot \det B_{11} - a_{12} \cdot \det B_{12} + \dots + (-1)^{n+1} \cdot a_{1n} \cdot \det B_{1n}.$$

Z założenia indukcyjnego $\det B_{11}$ jest wielomianem stopnia $n - 1$ postaci $(a_{22} - \lambda) \dots (a_{nn} - \lambda) + v'(\lambda)$, gdzie $\deg(v') \leq n - 3$. Pozostaje pokazać, że dla $j > 1$ wyznacznik B_{1j} jest wielomianem zmiennej λ stopnia nie większego niż $n - 2$.

Rzeczywiście, dla $j > 1$ macierz B_{1j} ma $j - 1$ -wszy wiersz i 1-wszą kolumnę niezawierające wyrazów zależnych od λ . Zamienimy wiersze o indeksach 1 oraz $j - 1$. Zmienia to jedynie znak wyznacznika i daje macierz C_{1j} , której pierwszy wiersz i pierwsza kolumna nie zawierają wyrazów zależnych od λ . Licząc wyznacznik C_{1j} względem pierwszego wiersza dostajemy zatem sumę skalarów przemnożonych przez wyznaczniki macierzy rozmiaru nie większego niż $n - 2$, które są takie, jak macierze opisane w (i). A zatem $\det C_{1j}$, i także $\det B_{1j}$, są wielomianami stopnia nie większego niż $n - 2$, co kończy dowód (ii).

W szczególności pokazaliśmy, że $w_A(\lambda)$ jest wielomianem stopnia równego n . Co więcej, na mocy (ii) widzimy, że aby znaleźć współczynniki wielomianu $w_A(\lambda)$ stojące przy λ^n oraz λ^{n-1} wystarczy znaleźć analogiczne współczynniki wielomianu $(a_{11} - \lambda)(a_{22} - \lambda) \dots (a_{nn} - \lambda)$. Łatwo widzieć, że współczynniki te są równe odpowiednio

$$(-1)^n \quad \text{oraz} \quad (-1)^{n-1}(a_{11} + a_{22} + \dots + a_{nn}) = (-1)^{n-1} \operatorname{tr}(A).$$

Pozostaje zauważyć, że dla $\lambda = 0$ wartość funkcji $\det(A - \lambda I)$ równa jest $\det(A)$. □

³Można dwa rozumowania zastąpić jednym, korzystając ze wzoru permutacyjnego na wyznacznik. Wiemy, że $\det(A - \lambda I)$ jest sumą $n!$ elementów:

$$\operatorname{sgn}(\sigma) \cdot x_{\sigma(1)1} x_{\sigma(2)2} \cdot x_{\sigma(n)n},$$

indeksowanych permutacjami $\sigma \in S_n$. Każdy z nich jest iloczynem wyrazów macierzy A oraz tyłu elementów postaci $(a_{kk} - \lambda)$, ile jest punktów stałych permutacji σ , czyli takich k , że $\sigma(k) = k$. Zauważmy, że każda permutacja zbioru n elementowego ma albo n punktów stałych, czyli jest identycznością, albo ma $\leq n - 2$ punkty stałe. Dostajemy więc (ii).

Naszym kolejnym celem jest pokazanie, że wartościami własnymi endomorfizmu przestrzeni skończonej wymiarowej są dokładnie pierwiastki jego wielomianu charakterystycznego.

Obserwacja 2.3

Niech ϕ będzie endomorfizmem skończonej wymiarowej przestrzeni liniowej V nad ciałem K . Następujące warunki są równoważne dla $a \in K$:

- (i) a jest wartością własną ϕ ,
- (ii) a jest pierwiastkiem wielomianu charakterystycznego $w_A(\lambda)$.

Niech \mathcal{A} będzie bazą przestrzeni V . Załóżmy, że niezerowy wektor $\alpha \in V$ ma w bazie \mathcal{A} współrzędne x_1, \dots, x_n . Wówczas α jest wektorem własnym ϕ o wartości własnej a wtedy i tylko wtedy, gdy

$$(A - aI) \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Dowód. Następujące warunki są równoważne dla wektora $v \in V$ oraz $\lambda \in K$:

$$\phi(v) = a \cdot v \iff \phi(v) - av = 0 \iff (\phi - a \text{id})(v) = 0 \iff v \in \ker(\phi - a \text{id}).$$

A zatem a jest wartością własną endomorfizmu ϕ wtedy i tylko wtedy, gdy $\ker(\phi - a \text{id}) \neq 0$, bowiem wektor własny musi być niezerowy. Równoważnie: $\det(\phi - a \text{id}) = 0$. Niech $A = M(\phi)_{\mathcal{A}}^{\mathcal{A}}$. Wówczas dla każdego $a \in K$ mamy:

$$M(\phi - a \cdot \text{id})_{\mathcal{A}}^{\mathcal{A}} = A - aI.$$

Zatem $\ker(\phi - \lambda \text{id}) \neq 0$ wtedy i tylko wtedy, gdy jednorodny układ równań liniowych o macierzy $A - aI$ ma niezerowe rozwiązanie. Na mocy Twierdzenia 1.1 widzimy więc, że warunek (i) jest równoważny z (ii). \square

Wniosek 2.2

Dla każdego $a \in K$ mamy $V_{(a)} = \ker(\phi - a \cdot \text{id}_V)$, czyli $V_{(a)}$ składa się z wektorów, których współrzędne w bazie \mathcal{A} są wektorami stanowiącymi przestrzeń rozwiązań układu równań liniowych o macierzy $A - aI$.

Z Wniosku 2.2 dostajemy klasyfikację macierzy diagonalnych, z dokładnością do podobieństwa.

Wniosek 2.3

Niech $A \in M_n(K)$ będzie macierzą górnotrójkątną lub dolnotrójkątną, która na przekątnej ma kolejno wyrazy a_{11}, \dots, a_{nn} . Wówczas wyrazy te są wszystkimi (uwzględniając krotności) pierwiastkami wielomianu charakterystycznego macierzy A . Co więcej, macierze diagonalne $D_1, D_2 \in M_n(K)$ są podobne wtedy i tylko wtedy, gdy mają identyczne wielomiany charakterystyczne, czyli gdy różnią się co najwyżej kolejnością wyrazów na przekątnej.

Z Obserwacji 2.2 i wzorów Viete'a dostajemy następujący bardzo istotny wniosek.

Wniosek 2.4

Jeśli wielomian charakterystyczny $w_A(\lambda)$ macierzy $A \in M_n(K)$ ma n pierwiastków w ciele K , to:

- suma wartości własnych macierzy A (uwzględniając krotności) równa jest $\text{tr } A$,
- iloczyn wartości własnych macierzy A (uwzględniając krotności) równy jest $\det A$.

Na kolejnym wykładzie przyjrzymy się endomorfizmom, które mają bazy złożone z wektorów własnych. W takiej bazie macierz endomorfizmu jest diagonalna, dlatego endomorfizmy te nazywać będziemy diagonalizowalnymi. Liczne zastosowania tego typu endomorfizmów (dyskretne układy dynamiczne, rekurencje, grafy, procesy Markowa, statystyka) prezentujemy w materiałach dodatkowych do kolejnych wykładów.

2.1 Zadania do samodzielnej pracy

Zadania ilustrujące umiejętności niezbędne do zaliczenia przedmiotu oznaczone są symbolem ♠.

Przy tych zadaniach dodany jest opis umiejętności, które sprawdzają.

1. (♠ Znajdowanie wartości własnych i baz odpowiadających im przestrzeni własnych)
Znaleźć wartości własne i bazy odpowiadających im przestrzeni własnych endomorfizmu ϕ , gdzie

- (a) $\phi : \mathbb{R}^2 \rightarrow \mathbb{R}^2$, gdzie $\phi((x_1, x_2)) = (2x_1 - x_2, -x_1 + 2x_2)$,
- (b) $\phi : \mathbb{R}^2 \rightarrow \mathbb{R}^2$, gdzie $\phi((x_1, x_2)) = (5x_1 + x_2, -x_1 + 3x_2)$,
- (c) $\phi : \mathbb{R}^3 \rightarrow \mathbb{R}^3$, gdzie $\phi((x_1, x_2, x_3)) = (x_1 - x_2, x_1 + 3x_2 + x_3, 2x_3)$,
- (d) $\phi : \mathbb{R}^3 \rightarrow \mathbb{R}^3$, gdzie $\phi((x_1, x_2, x_3)) = (4x_1 + x_2, 3x_1 + 2x_2, 7x_1 - x_2 + 5x_3)$,
- (e) $\phi : \mathbb{R}^4 \rightarrow \mathbb{R}^4$, gdzie $\phi((x_1, x_2, x_3, x_4)) = (-6x_1 - x_2 + 2x_3, 3x_1 + 2x_2 + x_4, -14x_1 - 2x_2 + 5x_3, -x_4)$.

2. (♠ Stwierdzenie czy dana macierz diagonalna jest macierzą danego endomorfizmu)
Dla każdego $t \in \mathbb{R}$ endomorfizm $\phi_t : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ przestrzeni liniowej \mathbb{R}^3 dany jest następującym wzorem $\phi_t((x_1, x_2, x_3)) = (2x_1 + x_2, x_1 + 2x_2, x_1 + x_2 + tx_3)$. Niech

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

- (a) Znajdź wszystkie $t \in \mathbb{R}$, dla których istnieją bazy \mathcal{A}, \mathcal{B} przestrzeni \mathbb{R}^3 , takie że $M(\phi_t)_{\mathcal{A}}^{\mathcal{B}} = A$. Dla ϕ_2 podać przykład takich baz (jeśli istnieją).
 - (b) Znajdź wszystkie $t \in \mathbb{R}$, dla których istnieje baza \mathcal{A} przestrzeni \mathbb{R}^3 , taka że $M(\phi_t)_{\mathcal{A}}^{\mathcal{A}} = A$. Dla każdego takiego $t \in \mathbb{R}$ podać przykład takiej bazy.
3. Niech $A \in M_n(\mathbb{R})$ będzie macierzą o niepustym zbiorze rzeczywistych wartości własnych. Czy macierz $A + I$ może mieć ten sam zbiór rzeczywistych wartości własnych co A ?
4. Wykaż, że jeśli $\phi \in \text{End}(V)$ jest izomorfizmem, to przestrzeń liniowa V ma identyczne podprzestrzenie własne względem ϕ oraz ϕ^{-1} .
5. Niech $n > 1$ oraz niech $\Phi \in \text{End}(M_n(\mathbb{R}))$ będzie dany wzorem $\Phi(M) = M^T$, dla każdej macierzy $M \in M_n(\mathbb{R})$. Znaleźć wartości własne tego endomorfizmu.
6. Na przestrzeni $\mathbb{R}[x]_{\leq n}$ wielomianów stopnia $\leq n$ określono endomorfizm postaci $f \mapsto f(ax + b)$. Wykaż, że wartościami własnymi tego endomorfizmu są liczby $1, a, \dots, a^n$.
7. Niech $A \in M_n(\mathbb{R})$ i załóżmy, że A^m jest macierzą zerową, dla pewnego $m \geq 1$. Czy 5 może być wartością własną A ?
8. Niech $\phi : V \rightarrow V$ będzie endomorfizmem n -wymiarowej przestrzeni liniowej V nad ciałem K . Załóżmy, że $\dim \ker(\phi) = k$. Czy istnieje wielomian $g(\lambda) \in K[\lambda]$, taki że $w_\phi(\lambda) = \lambda^k \cdot g(\lambda)$?
9. Udowodnij, że jeśli wszystkie niezerowe wektory przestrzeni liniowej V są wektorami własnymi endomorfizmu ϕ , to endomorfizm ten jest homotetią.
10. Endomorfizmy ϕ, ψ skończenie wymiarowej przestrzeni liniowej $V \neq 0$ nad ciałem liczb zespolonych spełniają warunek $\phi^2 = \text{id}_V = \psi^2$.
- (a) Pokaż, że jeśli dla pewnego wektora $0 \neq v \in V$ oraz pewnych $a, b \in \mathbb{C}$ spełniona jest równość:

$$v = a \cdot \phi(v) + b \cdot \psi(v),$$

to b jest wartością własną endomorfizmu $\psi - (a \cdot \psi \circ \phi)$ przestrzeni V .

- (b) Pokaż, że istnieje taka niezerowa liczba $a \in \mathbb{C}$, że endomorfizm $\psi - (a \cdot \psi \circ \phi)$ przestrzeni V ma niezerową wartość własną.

2.2 Uzupełnienie. Potęgi macierzy i rekurencje liniowe

Ci z Państwa, który zetknęli się z rekurencjami⁴, mogli słyszeć o wielomianie/równaniu charakterystycznym rekurencji liniowej, pozwalającym na wyznaczanie wzoru ogólnego na ciąg będący jej rozwiązaniem. Okazuje się, że za równaniem tym stoi algebra liniowa i jego rozwiązania są wartościami własnymi.

Definicja 2.4: Liniowy ciąg rekurencyjny rzędu k

Niech K będzie ciałem. Przez LINIOWY CIĄG REKURENCYJNY rozumiem ciąg $(X_n) \in K^\infty$ rzędu k określony warunkami:

- $X_0, \dots, X_{k-1} \in K$ – dane,
- dla $n \geq k$ mamy liczby $c_0, c_1, \dots, c_{k-1} \in K$, dla których:

$$X_n - c_{k-1}X_{n-1} - \dots - c_0X_{n-k} = 0, \quad \text{dla } n \geq k.$$

Zauważmy, że dowolne rozwiązanie (X_n) rekurencji rzędu k uzyskać można poprzez określenie pierwszych k wyrazów X_0, \dots, X_{k-1} . Na ich podstawie pozostałe wyrazy wyznaczamy ze wzoru wyżej. Najsłynniejszą zapewne rekurencją jest równanie rzędu drugiego postaci $x_{n+2} = x_{n+1} + x_n$ dla $a_1 = 1, a_2 = 1$ rozwiązaniem tej rekurencji jest ciąg Fibonacciego. Pochodzi on z rozważania następującego problemu.

Ile par królików będziemy mieli na końcu roku, jeśli zaczniemy w styczniu z jedną parą królików, ta w każdym miesiącu, poczynając od marca, wyda na świat kolejną parę królików i z każdej pary urodzą się kolejne pary po dwóch miesiącach od narodzin?

Nietrudno widzieć, że zbiór rozwiązań danej rekurencji liniowej jest podprzestrzenią K^∞ . Jak się okazuje, w niektórych sytuacjach rozwiązania rekurencji są bardzo eleganckie. Dzieje się tak wtedy, gdy wskazać można odpowiednią liczbę liniowo niezależnych ciągów geometrycznych, które ją spełniają.

Obserwacja 2.4

Niech $0 \neq \alpha \in K$. Ciąg geometryczny (a_k) dany wzorem $a_k = \alpha^n$ spełnia rekurencję (2.4) wtedy i tylko wtedy, gdy α jest rozwiązaniem równania:

$$\lambda^k - c_{k-1}\lambda^{k-1} - c_{k-2}\lambda^{k-2} - \dots - c_1\lambda - c_0 = 0.$$

Dowód. Jeśli $\alpha^{n+k} = c_{k-1}\alpha^{n+k-1} + c_{k-2}\alpha^{n+k-2} + \dots + c_0\alpha^n$. W zatem oczywiście po wyłączeniu $\alpha^n \neq 0$ widzimy, że α spełnia równanie wyżej. Dowód w drugą stronę jest analogiczny. \square

Dla przykładu, równaniem charakterystycznym rekurencji $X_{n+2} = X_{n+1} + X_n$ jest $\lambda^2 - \lambda - 1 = 0$. I rzeczywiście, rozwiązaniami tej rekurencji są między innymi ciągi geometryczne α_1^n oraz α_2^n , gdzie $\alpha = \frac{1+\sqrt{5}}{2}, \beta = \frac{1-\sqrt{5}}{2}$. Wiedząc, że przestrzeń rozwiązań tego układu jest dwuwymiarowa wiemy, że także ciąg Fibonacciego jest kombinacją liniową powyższych wektorów. Jaka? Łatwo to sprawdzić.

Okazuje się, że równanie charakterystyczne przywołane wyżej to wielomian charakterystyczny pewnej macierzy. A jego pierwiastki to wartości własne. Rzeczywiście, mamy:

$$\begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ -c_0 & -c_1 & -c_2 & \dots & -c_{k-1} \end{bmatrix} \cdot \begin{bmatrix} X_0 \\ X_1 \\ X_2 \\ \vdots \\ X_{k-1} \end{bmatrix} = \begin{bmatrix} X_1 \\ X_2 \\ X_3 \\ \vdots \\ X_k \end{bmatrix} \implies \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ -c_0 & -c_1 & -c_2 & \dots & -c_{k-1} \end{bmatrix}^n \cdot \begin{bmatrix} X_0 \\ X_1 \\ X_2 \\ \vdots \\ X_{k-1} \end{bmatrix} = \begin{bmatrix} X_n \\ X_{n+1} \\ X_{n+2} \\ \vdots \\ X_{n+k-1} \end{bmatrix}.$$

Stąd rozwiązanie rekurencji wymaga podnoszenia macierzy do potęgi. Dochodzimy do wartości własnych.

⁴Wszystkim, którzy chcieliby się dowiedzieć więcej o ciągach rekurencyjnych polecam bardzo ciekawe materiały dydaktyczne prof. W. Guzickiego: <https://www.mimuw.edu.pl/~guzicki/materiały/Rekurencja.pdf>.

Nasze dalsze rozważania oparte są na następującym rachunku. Niech

$$A = C^{-1}DC,$$

gdzie D jest macierzą diagonalną oraz C – macierzą odwracalną. Wówczas:

$$A^n = (C^{-1}DC)^n = C^{-1}DCC^{-1}DCC^{-1}\dots CC^{-1}DC = C^{-1}D^nC,$$

przy tym D^n to macierz diagonalna mająca na przekątnej n -te potęgi odpowiednich elementów z D .

Dlaczego tak interesuje nas podobieństwo do macierzy diagonalnej? Znajomość potęgi macierzy znajdującej się po lewej stronie równości jest kluczowa do ewentualnego określenia wzoru na n -ty wyraz ciągu rekurencyjnego. Łatwiej liczy się jednak potęgi macierzy diagonalnej, niż dowolnej. Jak się okazuje, podnoszenie do potęgi jest całkiem przyjemne, jeśli macierz jest podobna do diagonalnej. Problem w tym, że wypisana po lewej macierz $k \times k$ nie musi być zawsze podobna do macierzy diagonalnej (na przykład dla $X_n = 4X_{n-1} - 4X_{n-2}$), a to znacznie utrudnia wyznaczenie ogólnej formuły dla dowolnej liniowej rekurencji. Może się jednak zdarzyć klasyczna sytuacja, gdy takie podobieństwo można stwierdzić. Dzieje się to na przykład, jak pokażemy wkrótce, gdy wielomian charakterystyczny macierzy endomorfizmu ma n parami różnych pierwiastków. Tak się dzieje w przypadku ciągu Fibonacciego F_n zadanego warunkami:

$$F_0 = 0, \quad F_1 = 1, \quad F_{n+1} - F_n - F_{n-1} = 0, \quad \text{dla } n \geq 2.$$

Weźmy $\phi \in \text{End}(\mathbb{R}^2)$ dany wzorem $\phi(x, y) = (y, x + y)$. Wówczas:

$$\phi(F_{n-1}, F_n) = (F_n, F_{n+1}).$$

Zatem (przy oznaczeniu $\phi^n = \underbrace{\phi \circ \phi \circ \dots \circ \phi}_n$) mamy:

$$(F_n, F_{n+1}) = \phi^n(F_0, F_1) = \phi^n(0, 1).$$

Wartościami własnymi ϕ są

- $\lambda_+ = \frac{1+\sqrt{5}}{2}$ o wektorze własnym $\alpha_+ = \left(1, \frac{1+\sqrt{5}}{2}\right)$,
- $\lambda_- = \frac{1-\sqrt{5}}{2}$ o wektorze własnym $\alpha_- = \left(1, \frac{1-\sqrt{5}}{2}\right)$.

Przy tym $(0, 1) = \frac{1}{\sqrt{5}}(\alpha_+ - \alpha_-)$. Stąd:

$$(F_n, F_{n+1}) = \phi^n(0, 1) = \phi^n\left(\frac{1}{\sqrt{5}}(\alpha_+ - \alpha_-)\right) = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n \alpha_+ - \left(\frac{1-\sqrt{5}}{2}\right)^n \alpha_-\right).$$

Rachunek powyższy przełożyć można na język macierzy:

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}^n \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} F_n \\ F_{n+1} \end{bmatrix} \quad (*).$$

A zatem jeśli uda nam się wyznaczyć dowolną potęgę macierzy

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

to będziemy mieli kontrolę nad wyrazem ogólnym ciągu Fibonacciego. Mamy $w_A(\lambda) = \lambda^2 - \lambda - 1$, stąd wartości własne macierzy A to

$$\lambda_1 = \frac{1+\sqrt{5}}{2}, \quad \lambda_2 = \frac{1-\sqrt{5}}{2}.$$

Macierz A jest natomiast podobna do macierzy diagonalnej:

$$A = S^{-1} \cdot \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} \cdot S.$$

Wyznaczywszy S^{-1} (ta macierz ma w kolumnach wektory własne A) oraz S uzyskujemy z (*) słynny wzór Bineta:

$$F_n = \frac{\lambda_1^n - \lambda_2^n}{\sqrt{5}}.$$

Wciąż nie wyjaśniliśmy skąd się wzięła macierz wypisana na poprzedniej stronie i dlaczego przypisane rekurencji równanie charakterystyczne jest wielomianem charakterystycznym tej macierzy. O tym przekonamy się na wykładzie szóstym. Sam rachunek wielomianu charakterystycznego nie jest zresztą trudny.

2.3 Dodatek. Grafy i ich macierze sąsiedztwa

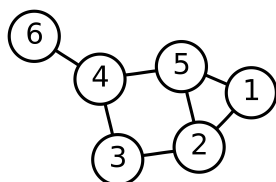
Algebra liniowa niewątpliwie pozwoli nam zrozumieć wiele obiektów geometrycznych i fenomenów w analizie. Chciałbym raz na jakiś czas zasygnalizować inny piękny kierunek jej zastosowań – kombinatorykę (czy mądrzej: matematykę dyskretną). Jednym z podstawowych narzędzi kombinatorycznych są grafy, a do badania ich własności przydają się, jak się okazuje, rozmaite związane z nimi macierze. Badanie własności tych macierzy, między innymi ich wektorów i wartości własnych, może służyć dowodzeniu pięknych twierdzeń. Interpretacja grafowa rozmaitych sytuacji kombinatorycznych jest taka: n osób i ich układ znajomości reprezentuje graficznie graf (nie)zorientowany o n wierzchołkach. Znajomość reprezentowana jest przez krawędź pomiędzy wierzchołkami. Nie ma krawędzi z wierzchołkiem do niego samego i nie ma krawędzi wielokrotnych pomiędzy dwoma wierzchołkami. Taki graf nazywamy czasem w kombinatoryce GRAFEM PROSTYM. Najpierw pokażemy jak związać z takim grafem pewną (jedną z wielu) macierz.

Definicja 2.5: Macierz sąsiedztwa grafu

Dla (niezorientowanego) grafu prostego G o wierzchołkach postaci $1, 2, \dots, n$ definiujemy MACIERZ SĄSIEDZTWA $A(G) = [a_{ij}] \in M_n(\mathbb{C})$ warunkami:

- $a_{ij} = 1$, jeśli wierzchołki i oraz j są połączone w G ,
- $a_{ij} = 0$, jeśli $i = j$ lub wierzchołki i, j nie są połączone w G .

Rozważmy następujący przykład grafu:



Macierz sąsiedztwa powyższego grafu to:

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

Macierz $A(G)$ (ang. *adjacency matrix*) jest dla grafów niezorientowanych macierzą symetryczną, to znaczy $A(G) = A(G)^T$. Jak się okazuje, rozmaite własności grafu G odczytać można z typowo algebraicznych własności $A(G)$. Osobom mającym doświadczenie w metodach teorii grafów polecam wykład *Metody algebraiczne w teorii grafów* zamieszczony na portalu wazniak.mimuw.edu.pl.

ŚCIEŻKA DŁUGOŚCI n w grafie niezorientowanym G to ciąg n krawędzi postaci $a_0 - a_1 - \dots - a_n$, gdzie $a - b$ reprezentuje połączenie wierzchołków a oraz b . Wierzchołki mogą występować w ścieżce wiele razy. Jest jasne, że jeśli w grafie jest cykl zamknięty, to żadna z potęg macierzy sąsiedztwa nie jest zerowa. Kluczowym powodem badania macierzy sąsiedztwa jest następująca, prosta obserwacja, której dowód (ładna motywacja dla mnożenia macierzy) pozostawiam Czytelnikowi.

Obserwacja 2.5

Niech G będzie skończonym niezorientowanym grafem prostym. Wyraz znajdujący się w i -tym wierszu i j -tej kolumnie macierzy $A(G)^n$ opisuje liczbę ścieżek długości n od wierzchołka i do wierzchołka j w grafie G .

Dla zilustrowania pewnych ciekawych własności macierzy sąsiedztwa zostawiam poniżej kilka zadań do samodzielnego rozwiązania⁵. Niektóre wymagają całkiem sporej pomysłowości.

⁵Więcej zadań będziemy mogli zrobić w połowie semestru, gdy wykażemy tzw. rzeczywiste twierdzenie spektralne

ZADANIE 1. Wektor stopni wierzchołków (niezorientowanego) grafu prostego G równy jest iloczynowi macierzy $A(G)$ przez wektor v postaci....?

ZADANIE 2. Jeśli G_1, G_2 są parą izomorficznych⁶ grafów skończonych o macierzach sąsiedztwa $A(G_1), A(G_2)$, to istnieje macierz permutacyjna P taka, że:

$$A(G_2) = P^{-1}A(G_1)P.$$

W szczególności macierze $A(G_1), A(G_2)$ mają ten sam zbiór wartości własnych (z krotnościami).

ZADANIE 3. Jeśli graf G jest prosty, ale nie jest spójny, wówczas można tak ponumerować jego wierzchołki, aby $A(G)$ było macierzą blokowo-diagonalną o liczbie bloków diagonalnych równej liczbie składowych spójności G .

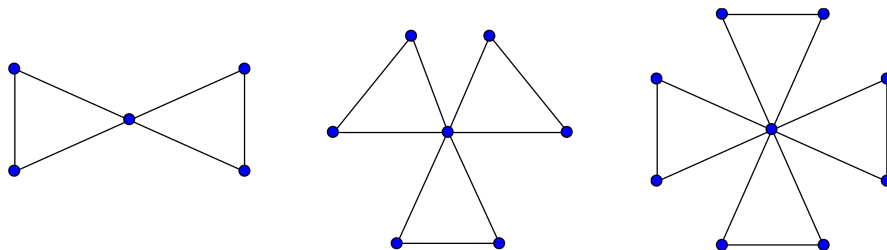
ZADANIE 4. Załóżmy, że graf G jest dwudzielny. Wówczas jeśli λ jest wartością własną $A(G)$, to $-\lambda$ również jest wartością własną $A(G)$. Czy zachodzi fakt odwrotny?

ZADANIE 5. Pokaż, że jeśli λ jest wartością własną macierzy $A(G)$ grafu G , to $|\lambda| \leq \Delta(G)$, gdzie $\Delta(G)$ to maksymalny stopień wierzchołka w grafie G .

To oczywiście jedynie bardzo proste własności $A(G)$ związane z wartościami własnymi. Jest ich znacznie więcej, a w zasadzie są całe podręczniki związane z badaniem metod algebraicznych w teorii grafów. Jednym z niezwykle pięknych wyników w tej tematyce jest następujące twierdzenie.

Twierdzenie 2.2: O przyjaźni (Erdős, Rényi, Sós), 1966

Założmy, że w gronie $n > 1$ osób każde dwie osoby mają dokładnie jednego wspólnego znajomego (A jest znajomym $B \iff B$ jest znajomym A). Wówczas istnieje w tym gronie osoba, która jest znajomym wszystkich pozostałych.



Przykłady tzw. grafów przyjaźni, czyli takich, które realizują tezę twierdzenia o przyjaźni. Źródło wikipedia.org.

To dość zaskakujące twierdzenie jest jednym z wielu pięknych zastosowań tzw. spektralnej teorii grafów. Istnieje też trudny czysto kombinatoryczny dowód tego rezultatu. Poniżej przedstawiam dowód algebraiczny. W tym momencie może on nie być do końca zrozumiały, ale proszę wrócić w to miejsce za jakiś dwa wykłady i być wszystko stanie się bardziej jasne. Już teraz jednak można z pożytkiem śledzić piękny pomysł dowodu. Niech G będzie grafem prostym opisującym układ przyjaźni n osób z twierdzenia.

Oto plan dowodu w czterech krokach⁷.

1. Pokażemy, że w opisanej sytuacji dwie osoby nieznanne mają taką samą liczbę znajomych.
2. Pokażemy, że gdyby teza nie zachodziła, to wszyscy musieliby mieć taką samą liczbę znajomych.
3. Niech K będzie grafem k -regularnym (z każdego wierzchołka wychodzi k krawędzi) o n wierzchołkach, opisującym kontrprzykład do twierdzenia. Pokażemy, że $n = k^2 - k + 1$.
4. Wyznamy wartości własne $A(G)^2$. Co to powie o wartościach własnych $A(G)$ oraz o n i k ?

⁶To znaczy: G_1, G_2 mają po n wierzchołków, dla pewnego n , i istnieje permutacja $\sigma \in S_n$ taka, że (i, j) jest krawędzią G_1 wtedy i tylko wtedy, gdy $(\sigma(i), \sigma(j))$ jest krawędzią w G_2

⁷Na podstawie notatek dr R. Quinlan ze spektralnej teorii grafów: *Spectral Graph Theory MA500-1: Lecture Notes*, <https://maths.nuigalway.ie/~rquinlan/teaching/spectralgraphtheory.pdf>.

Dowód. Załóżmy, że sytuacja opisana w twierdzeniu reprezentowana jest przez pewien skończony niezorientowany graf prosty G (dla każdego dwóch wierzchołków G istnieje trzeci, z którym te dwa są połączone), ale wbrew tezie nie istnieje jeden wierzchołek G , który byłby połączony ze wszystkimi. Kroki 1. i 2. polegają na pokazaniu, że w opisanej sytuacji G musi być REGULARNY, to znaczy: z każdego wierzchołka wychodzi tyle samo krawędzi, powiedzmy k . Innymi słowy: jeśli nie zachodzi sytuacja opisana w zadaniu to wszyscy muszą mieć tyle samo przyjaciół.

Weźmy dwa niepołączone wierzchołki u, v grafu G reprezentujące dwóch nieznanymych. Niech $k = \deg u$ będzie stopniem u (liczbą połączeń z innymi wierzchołkami) i niech x_1, \dots, x_k będą sąsiadami u , gdzie x_1 jest owym unikatowym znajomym u oraz v . Dla każdego i od 1 do k , niech y_i będzie owym dokładnie jednym znajomym v oraz x_i . Wtedy wszystkie y_i są parami różne, bo gdyby któreś dwa z nich się pokrywały, to ów wierzchołek gdzie by się pokrywały miałby więcej niż jednego wspólnego znajomego z u . Zatem v ma stopień co najmniej k i $\deg u \leq \deg v$. Ten sam argument działa jednak, gdy zamienimy role u oraz v , więc dostajemy również $\deg u \leq \deg v$, a w rezultacie $\deg u = \deg v$. Punkt 1. w naszym planie jest zrealizowany. W opisanej sytuacji dwie osoby nieznanome mają taką samą liczbę znajomych.

Niech teraz w będzie dowolnym wierzchołkiem G , innym niż x_1 . Skoro u oraz v mają tylko jednego wspólnego znajomego (właśnie x_1), to w nie jest połączony z jednym z nich. Skoro $\deg u = \deg v = k$, to także $\deg w = k$, na mocy punktu 1. A zatem wszystkie wierzchołki G mają stopień k , być może poza x_1 . Jeśli, wbrew tezie, istnieje wierzchołek G , który nie ma połączenia z x_1 , to ten wierzchołek ma stopień k (to pokazaliśmy), a więc i x_1 ma stopień k . A zatem jeśli graf spełnia założenia twierdzenia, ale nie jego tezę, musi być regularny, co daje nam krok 2.

Założmy teraz, że K jest grafem k -regularnym spełniającym warunki twierdzenia i policzmy ile K ma wierzchołków. Zliczamy ścieżki długości 2 grafu K startujące z ustalonego wierzchołka x . Ich liczba to k^2 , bo każdy ma k znajomych, a każdy z nich dokładnie k kolejnych. Między każdym wierzchołkiem $y \neq x$ istnieje dokładnie jedna ścieżka długości 2 zaczynająca się w x (ta obserwacja jest kluczowa do pokazania kroku kombinatorycznego). A zatem licząc ile jest wszystkich wierzchołków grafu za pomocą ścieżek długości 2 każdy wierzchołek G policzyliśmy raz — oprócz x , który policzyliśmy k razy. Odejmujemy nadmiarowe $k - 1$ razy i widzimy, że

$$n = k^2 - k + 1$$

gdzie n to liczba wierzchołków grafu K . Krok 3. jest zakończony i możemy przejść do wielkiego finału.

Założmy, że G jest grafem opisującym sytuację w twierdzeniu i nie spełnia on tezy. Zgodnie z krokiem 2., że G jest regularny stopnia k . Przejdźmy do macierzy sąsiedztwa $A = A(G)$. Co o niej wiemy? Nie za wiele. Ale wiemy coś o A^2 . Skoro każde dwa wierzchołki grafu G mają dokładnie jednego wspólnego sąsiada, to macierz A^2 ma k na przekątnej (idziemy do jednego z k sąsiadów i wracamy) oraz 1 wszędzie indziej, bo 1 jest liczbą ścieżek długości 2 pomiędzy różnymi wierzchołkami w G .

Policzenie wielomianu charakterystycznego macierzy A^2 wyżej jest ładnym i pouczającym ćwiczeniem. Zapisujemy $A^2 = (k-1)I + J$, gdzie I jest macierzą identycznościową, zaś J jest macierzą, której wszystkie wyrazy to 1. Wartości własne A^2 to pierwiastki wielomianu

$$\det((k-1)I + J - \lambda I) = \det((k-1-\lambda)I + J).$$

A zatem liczba λ_0 jest wartością własną A^2 wtedy i tylko wtedy, gdy $\lambda_0 + k - 1$ jest wartością własną J . Czytelnik zechce sprawdzić, że wartościami własnymi macierzy J złożonej z samych jedynek są n (wektor własny z samych jedynek) oraz 0, będące pierwiastkiem $n - 1$ -krotnym. A zatem wartościami własnymi macierzy A^2 są $k - 1$, która występuje $n - 1$ razy oraz $n + k - 1 = k^2$ (wzór wyżej na liczbę wierzchołków), która jest pierwiastkiem pojedynczym. Po co to wszystko?

„CruX” polega na tym, że wartości własne A to pierwiastki kwadratowe⁸ wartości własnych A^2 . A zatem wartości własne A mogą wynosić jedynie k lub $\pm\sqrt{k-1}$. I kluczowa myśl: wartości własne macierzy A dodają się (z krotnościami) do zera, zgodnie z Wnioskiem 2.1, a na przekątnej A są zera, czyli mamy $\text{tr}(A) = 0$. Zatem jeśli $\sqrt{k-1}$ ma (jako wartość własna A) krotność r , zaś $-\sqrt{k-1}$ ma krotność s , to

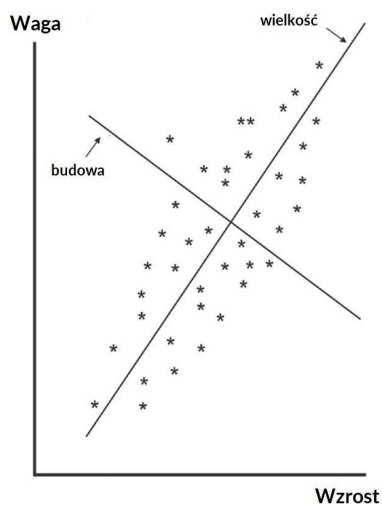
$$k + (r - s)\sqrt{k-1} = 0.$$

Analiza teorio-liczbowa tego warunku mówi, że $k - 1$ dzieli k^2 , czyli k musi być równe 1 lub 2. W tych przypadkach G jednak ma wspólnego „przyjaciela” innych wierzchołków. Dostaliśmy sprzeczność. \square

⁸Jeśli $Av = \lambda v$, to $A^2v = A(Av) = A \cdot \lambda v = \lambda^2 v$.

2.4 Trivia. PCA, czyli w jakich kierunkach patrzeć na dane?

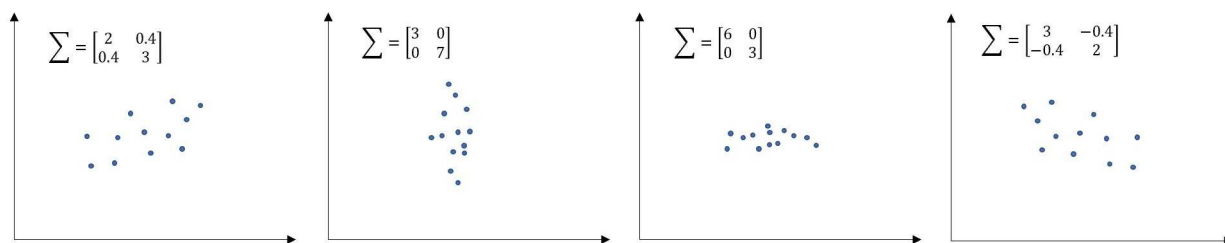
Analizując zbiory danych zainteresowani jesteście szukaniem w nich prawidłowości. Statystyka zna wiele metod uzyskiwania tego typu wyników. Jedną z nich jest PCA (Principal Components Analysis, czyli tzw. analiza składowych głównych), o której wypowiemy kilka intuicji, związanych z wektorami własnymi. Oto prosty przykład. Załóżmy, że zmierzaliśmy wzrost i wagę pewnej grupy osób. Chcielibyśmy zaprezentować wyniki naszych pomiarów na płaszczyźnie, umieszczając gwiazdkę w miejscu każdego z wyników. Współrzędna pozioma opisuje wzrost, a pionowa — wagę. Oto przykładowa prezentacja wyników.



Parametry wzrostu i wagi są oczywiście silnie skorelowane, czego używa się wprowadzając wielkość zwaną BMI. Oczywiście korelacja nie jest doskonała, ponieważ budowa ciała zależy od szeregu czynników. Przyglądając się jednak danym o bardzo silnej korelacji zmiennych widzimy, że istnieje kierunek, „wokół którego” oscylują silnie skorelowane dane. Kierunek ten nazwać można *osią główną*. Dlaczego to jest ciekawe? Najbardziej skorelowane dane „układają się” wzdłuż pewnej prostej i kierunek tej osi przyjmując za kierunek odniesienia i nadać mu nazwę rozmiaru (standardowego). Skąd wzięliśmy położenie tej prostej? Od każdego punktu reprezentującego pomiar prowadzimy odcinek prostopadły do tej prostej. Dalej liczymy średnią z kwadratów tych odległości. Okaże się, że dla wybranej prostej osiągamy zarówno „maksymalną” wariancję (rozrzut rzutów na prostej) i „minimalny” błąd, spośród wszystkich prostych⁹.

Możemy też rozważać drugi kierunek (nie tylko w naszym przypadku) prostopadły do osi głównej, pokazujący kierunek „największych rozbieżności” pomiędzy wagą, a wzrostem. Czy taki kierunek można jakoś interpretować? Nazwijmy go „budową ciała” i zamiast reprezentować wyniki jako pary liczb (wzrost, waga) reprezentujemy je jako pary (rozmiar, budowa). Kluczowa jest prostopadłość — ponieważ w języku statystyki oznacza ona nieskorelowanie zmiennych (a jeśli są to zmienne losowe — to ich niezależność).

Opowieść powyższa może ma jakiś sens, ale czy ma jakiś związek z wektorami i wartościami własnymi? W istocie wyznaczone kierunki są wektorami własnymi rzeczywistej symetrycznej macierzy¹⁰ kowariancji. Taka macierz ma rozmiar $d \times d$, gdzie d jest liczbą badanych parametrów. W naszym przypadku ma rozmiar 2×2 . Nie wchodząc w szczegóły¹¹ zobaczymy kilka zestawów danych i ich macierzy kowariancji:



⁹Może poniższy GIF dobrze pokaże o co chodzi: <https://i.stack.imgur.com/Q7HIP.gif>. Patrz też: <https://stats.stackexchange.com/questions/2691/making-sense-of-principal-component-analysis-eigenvectors-eigenvalues>.

¹⁰Takie macierze mają prostopadłe wektory własne, co będzie jednym z ważniejszych twierdzeń tego wykładu.

¹¹Odsyłam do wykładów ze Statystyki II (paragraf 3.2.2, str. 18): <https://mst.mimuw.edu.pl/wyklady/st2/wyklad.pdf>. Niech to Państwa nie przerazi. Więcej intuicji: <https://www.neuraldesigner.com/blog/principal-components-analysis>. Można to tłumaczyć nawet bez matematyki: https://kb.osu.edu/bitstream/handle/1811/69494/ASK_1998_83_102.pdf.

Rozdział 3

Diagonalizowalność

Na ostatnim wykładzie postawiony został problem rozpoznawania natury geometrycznej endomorfizmu. Pojęcie macierzy endomorfizmu w ustalonej bazie uzasadnia wprowadzenie relacji (równoważności) podobieństwa w $M_n(K)$. Klasy równoważności tej relacji służą m.in. do rozróżniania rozmaitych, różnych geometrycznie przekształceń. Wprowadzone na ostatnim wykładzie pojęcia wektora i wartości własnej są kluczowe dla zrozumienia jakie właściwie geometryczne własności przekształceń nas interesują. Dziś¹ poznamy jedną z najważniejszych własności tego typu: diagonalizowalność.

Obserwacja 3.1

Niech $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$ będzie bazą przestrzeni liniowej V i niech $\phi \in \text{End}(V)$. Następujące warunki są równoważne

- (i) macierz $M(\phi)_{\mathcal{A}}^{\mathcal{A}}$ jest diagonalna
- (ii) wektory $\alpha_1, \dots, \alpha_n$ są wektorami własnymi endomorfizmu ϕ .

Dowód. Załóżmy (i). Niech a_1, a_2, \dots, a_n będą kolejnymi wyrazami na diagonalu macierzy $M(\phi)_{\mathcal{A}}^{\mathcal{A}}$, tzn.

$$M(\phi)_{\mathcal{A}}^{\mathcal{A}} = \begin{bmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_n \end{bmatrix}.$$

Z definicji macierzy przekształcenia liniowego mamy:

$$\phi(\alpha_1) = a_1 \cdot \alpha_1, \quad \phi(\alpha_2) = a_2 \cdot \alpha_2, \quad \dots \quad \phi(\alpha_n) = a_n \cdot \alpha_n.$$

W szczególności baza \mathcal{A} jest bazą złożoną z wektorów własnych endomorfizmu ϕ , czyli dostajemy (ii). Druga implikacja jest równie oczywista. Jeśli baza \mathcal{A} złożona jest z wektorów własnych, to współrzędne wektora $\phi(\alpha_j)$ w bazie \mathcal{A} są zerowe, poza być może j -tą współrzędną (przy α_j). \square

Definicja 3.1: Endomorfizm diagonalizowalny

Niech $\phi \in \text{End}(V)$. Mówimy, że endomorfizm ϕ jest **DIAGONALIZOWALNY**, jeśli istnieje baza przestrzeni liniowej V złożona z wektorów własnych endomorfizmu ϕ .

Dobrze nam już znane (choć niejedyne) przykłady endomorfizmów diagonalizowalnych to identyczność, jednokładność, rzut oraz symetria. Podstawowym przykładem endomorfizmu niediagonalizowalnego jest obrót (o kąt różny od wielokrotności π) w przestrzeni rzeczywistej. Inny omawiany już wielokrotnie antyprzykład to endomorfizm zadany macierzą

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

¹Ostatnia aktualizacja: 06.05.2023 r.

Obserwacja 3.2

Niech $\dim(V) < \infty$. Endomorfizm $\phi \in \text{End}(V)$ jest diagonalizowalny wtedy i tylko wtedy, gdy ma w pewnej bazie macierz diagonalną.

Przeformułujmy pojęcia diagonalizowalności z języka endomorfizmów do języka relacji podobieństwa.

Definicja 3.2: Macierz diagonalizowalna nad ciałem K

Macierz $A \in M_n(K)$ nazywamy DIAGONALIZOWALNĄ NAD CIAŁEM K , jeśli istnieje taka macierz odwracalna $C \in M_n(K)$, że macierz $C^{-1}AC$ jest diagonalna. Innymi słowy, macierz A jest podobna do macierzy diagonalnej należącej do $M_n(K)$.

Powyższe definicje są oczywiście równoważne. Macierz A jest diagonalizowalna (nad ciałem K) wtedy i tylko wtedy, gdy $\phi \in \text{End}(V)$ zadany przez $A = M(\phi)_{st}^{st}$ jest diagonalizowalny.

Zwróćmy uwagę na to, że macierz o wyrazach w ciele K może nie być diagonalizowalna nad K , natomiast może być diagonalizowalna nad pewnym ciałem zawierającym K . Klasycznym przykładem jest wielokrotnie już wspomniany obrót w \mathbb{R}^2 o kąt 90° . W bazie standardowej endomorfizm ten ma macierz

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

Macierz ta nie jest diagonalizowalna nad \mathbb{R} , ale jeśli potraktujemy ją jako macierz o wyrazach zespolonych (z których wszystkie są akurat rzeczywiste), to możemy wskazać podobną do niej macierz diagonalną:

$$\begin{bmatrix} -i & i \\ 1 & 1 \end{bmatrix}^{-1} \cdot \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} -i & i \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} \frac{i}{2} & \frac{1}{2} \\ -\frac{i}{2} & \frac{1}{2} \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} -i & i \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & -\frac{i}{2} \\ \frac{1}{2} & \frac{i}{2} \end{bmatrix} \cdot \begin{bmatrix} -i & i \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}.$$

Skoro mówimy o bazach złożonych z wektorów własnych, spróbujmy najpierw zrozumieć zależność pomiędzy wektorami własnymi endomorfizmu odpowiadającymi parami różnym wartościom własnym.

Obserwacja 3.3

Niech V będzie przestrzenią liniową nad ciałem K , niech $\phi \in \text{End}(V)$, oraz niech:

- $a_1, a_2, \dots, a_k \in K$ – parami różne wartości własne ϕ ,
- $\beta_1 \in V_{(a_1)}, \beta_2 \in V_{(a_2)}, \dots, \beta_k \in V_{(a_k)}$ (czyli $\phi(\beta_i) = a_i \cdot \beta_i$, dla $1 \leq i \leq k$).

Wówczas jeśli $\beta_1 + \dots + \beta_k = 0$, to $\beta_1 = \beta_2 = \dots = \beta_k = 0$.

Dowód. Stosujemy indukcję po k . Dla $k = 1$ teza jest oczywista. Przechodzimy do kroku indukcyjnego, zakładając, że teza jest spełniona dla $k - 1$. Niech β_1, \dots, β_k spełniają założenia i niech $\beta_1 + \dots + \beta_k = 0$. Stosując ϕ do obydwu stron tej równości dostajemy:

$$0 = \phi(\beta_1 + \dots + \beta_k) = \phi(\beta_1) + \dots + \phi(\beta_k) = a_1\beta_1 + \dots + a_k\beta_k.$$

Możemy także przemnożyć wyjściowe założenie przez a_1 i dostać

$$a_1\beta_1 + \dots + a_1\beta_k = 0$$

A ta i poprzednia równość dają łącznie $a_1\beta_1 + a_1\beta_2 + \dots + a_1\beta_k = a_1\beta_1 + a_2\beta_2 + \dots + a_k\beta_k$, czyli:

$$(a_2 - a_1)\beta_2 + \dots + (a_k - a_1)\beta_k = 0.$$

Składnik $(a_i - a_1)\beta_i$ należy do $V_{(a_i)}$, dla $i = 2, \dots, k$, więc z założenia indukcyjnego wynika, że

$$(a_2 - a_1)\beta_2 = (a_3 - a_1)\beta_3 = \dots = (a_k - a_1)\beta_k = 0.$$

Skoro a_1, \dots, a_k są parami różne², to mamy $\beta_2, \dots, \beta_k = 0$. A zatem równość $\beta_1 + \dots + \beta_k = 0$ redukuje się do $\beta_1 = 0$, co kończy krok indukcyjny i cały dowód. \square

Rezultat ten prowadzi do fundamentalnego wniosku.

²Korzystamy tu z pierwszego faktu o przestrzeniach liniowych: jeśli $a \cdot \alpha = 0$, to $a = 0$ lub $\alpha = 0$, dla $a \in K$ oraz $v \in V$.

Obserwacja 3.4

Niech V będzie przestrzenią liniową nad ciałem K , niech $\phi \in \text{End}(V)$ oraz niech:

- a_1, a_2, \dots, a_k – parami różne wartości własne ϕ ,
- $\alpha_1, \dots, \alpha_k$ – wektory własne odpowiadające (odpowiednio) wartościom własnym a_1, \dots, a_k .

Wówczas układ $\alpha_1, \dots, \alpha_k$ jest liniowo niezależny.

Dowód. Przypuśćmy, że $b_1\alpha_1 + \dots + b_k\alpha_k = 0$, dla pewnych skalarów $b_1, \dots, b_k \in K$. Wówczas $b_i\alpha_i \in V_{(a_i)}$, dla $i = 1, 2, \dots, k$. Na mocy poprzedniej Obserwacji mamy zatem, że $b_i\alpha_i = 0$, dla $i = 1, 2, \dots, k$. Stąd także $b_1 = b_2 = \dots = b_k = 0$, bowiem $\alpha_i \neq 0$, dla $i = 1, \dots, k$. \square

W dowodzie wykorzystaliśmy założenie, że α_i są wektorami własnymi, więc muszą być niezerowe. Oto kluczowy wniosek.

Wniosek 3.1

Jeśli endomorfizm n wymiarowej przestrzeni liniowej ma n różnych wartości własnych, to jest on diagonalizowalny.

Oczywiście warunek posiadania n różnych wartości własnych nie jest konieczny do diagonalizowalności, bowiem macierz diagonalna może mieć te same wyrazy w różnych miejscach na przekątnej — jak choćby sama macierz identycznościowa. W sytuacji gdy wielomian charakterystyczny ma pierwiastki wielokrotne, diagonalizowalność zależy od wymiarów przestrzeni własnych odpowiadających parami różnym wartościom własnym. Temu zagadnieniu poświęcimy resztę wykładu.

Obserwacja 3.5

Niech $w_\phi(\lambda)$ będzie wielomianem charakterystycznym endomorfizmu ϕ przestrzeni V nad ciałem K oraz niech k będzie krotnością pierwiastka a wielomianu charakterystycznego tego endomorfizmu, czyli takim elementem K , że

$$w_\phi(\lambda) = (\lambda - a)^k \cdot g(\lambda),$$

przy czym a nie jest pierwiastkiem wielomianu g . Wówczas $k \geq \dim V_{(a)}$.

Dowód. Niech $\alpha_1, \dots, \alpha_r$ będzie bazą przestrzeni $V_{(a)}$. Uzupełnijmy ją wektorami $\beta_{r+1}, \dots, \beta_n$ do bazy \mathcal{A} przestrzeni V . Wówczas macierz ϕ w bazie \mathcal{A} ma postać blokową:

$$A = M(\phi)_{\mathcal{A}}^{\mathcal{A}} = \begin{bmatrix} aI_r & B \\ 0 & C \end{bmatrix},$$

dla pewnych $B \in M_{r \times (n-r)}(K)$, $C \in M_{n-r}(K)$. W szczególności

$$A - \lambda I = \begin{bmatrix} (a - \lambda)I_r & B \\ 0 & C - \lambda I_{n-r} \end{bmatrix}.$$

Zatem (patrz³ Obserwacja 13.10 w notatkach z GAL I):

$$w_\phi = \det(A - \lambda I) = (a - \lambda)^r \cdot \det(C - \lambda I).$$

Skoro $\det(C - \lambda I)$ jest wielomianem zmiennej λ , to z definicji krotności⁴ mamy $k \geq r = \dim V_{(a)}$. \square

³Chodzi o wyznacznik macierzy blokowo-górnotrójkątnej. Dla $X \in M_m(K)$, $Y \in M_{m \times n}(K)$ oraz $Z \in M_n(K)$ mamy:

$$\begin{vmatrix} X & Y \\ 0 & Z \end{vmatrix} = \begin{vmatrix} I_m & 0 \\ 0 & Z \end{vmatrix} \cdot \begin{vmatrix} I_m & Y \\ 0 & I_n \end{vmatrix} \cdot \begin{vmatrix} X & 0 \\ 0 & I_n \end{vmatrix} = |Z| \cdot 1 \cdot |X| = |X| \cdot |Z|.$$

⁴Uważny Czytelnik może dokładniej zastanowić się nad tym krokiem. Jeśli zachodzi równość dwóch wielomianów z $K[\lambda]$, z których każdy jest podzielny przez ten sam czynnik liniowy, to równe są też ilorazy tych wielomianów przez ów wspólny czynnik. Kluczowe jest tu założenie, że współczynniki są w ciele (ogólniej: w pierścieniu będącym dziedziną całkowitości).

Definicja 3.3: Krotność algebraiczna i krotność geometryczna wartości własnej

Niech a będzie wartością własną endomorfizmu ϕ . Liczbę k występującą w poprzednim lemacie nazywamy KROTNOŚCIĄ ALGEBRAICZNĄ wartości własnej a endomorfizmu ϕ . Liczbę $\dim V_{(a)}$ nazywamy KROTNOŚCIĄ GEOMETRYCZNĄ wartości własnej a .

Kluczowy przykład rozróżniający te pojęcia: dla endomorfizmów danych macierzami:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

mamy równość wielomianów charakterystycznych $(\lambda - 1)^2$. A zatem krotność algebraiczna wartości własnej 1 wynosi dla obydwu endomorfizmów 2. Różnicę wnosi krotność geometryczna. Dla endomorfizmu identycznościowego równa jest ona 2, a dla endomorfizmu danego macierzą po prawej — wynosi ona 1.

Obserwacja 3.6

Niech a_1, \dots, a_k będą wartościami własnymi endomorfizmu ϕ przestrzeni V . Wówczas:

$$\dim V_{(a_1)} + \dim V_{(a_2)} + \dots + \dim V_{(a_k)} \leq \dim V.$$

Dowód. Wiemy, że $\dim V = \deg w_\phi(\lambda)$, zaś liczba pierwiastków (z krotnościami) wielomianu o współczynnikach z ciała nie przekracza jego stopnia. Teza wynika zatem z Obserwacji 3.4. \square

Możemy teraz sformułować kluczowe twierdzenie tego wykładu⁵.

Twierdzenie 3.1: Charakteryzacja endomorfizmów diagonalizowalnych

Niech V będzie skończenie wymiarową przestrzenią liniową nad ciałem K i niech $\phi \in \text{End}(V)$. Niech $a_1, \dots, a_k \in K$ będą wszystkimi, parami różnymi, wartościami własnymi endomorfizmu ϕ . Wówczas endomorfizm ϕ jest diagonalizowalny wtedy i tylko wtedy, gdy:

$$\dim V_{(a_1)} + \dim V_{(a_2)} + \dots + \dim V_{(a_k)} = \dim V.$$

Zanim pokażemy dowód tego rezultatu, zobaczmy przykład zadania ze starego kolokwium.

Zadanie. Znajdź wszystkie takie $s, t \in \mathbb{Z}_5$, że macierz

$$A = \begin{bmatrix} 1 & 0 & 0 \\ s & 2 & 0 \\ 1 & t & 1 \end{bmatrix} \in M_{3 \times 3}(\mathbb{Z}_5)$$

jest diagonalizowalna nad ciałem pięcioelementowym \mathbb{Z}_5 .

ROZWIĄZANIE. Niech $\phi : \mathbb{Z}_5^3 \rightarrow \mathbb{Z}_5^3$ będzie endomorfizmem takim, że $M(\phi)_{st}^st = A$. Teza jest równoważna wskazaniu takich $s, t \in \mathbb{Z}_5$, dla których endomorfizm ϕ jest diagonalizowalny, czyli istnieje baza \mathbb{Z}_5^3 złożona z wektorów własnych ϕ . Wielomian charakterystyczny ϕ równy jest wielomianowi charakterystycznemu macierzy dolnotrójkątnej A , czyli $w_\phi(\lambda) = w_A(\lambda) = (1 - \lambda)^2(2 - \lambda) \in \mathbb{Z}_5[\lambda]$. A zatem ϕ ma wartości własne 1, 2. Mają one odpowiednio krotności algebraiczne 2 oraz 1. A zatem podprzestrzeń własna $V_{(2)}$ jest wymiaru 1. Aby ϕ było diagonalizowalne potrzeba zatem i wystarcza, by $V_{(1)}$ była wymiaru 2. Mamy:

$$A - I = \begin{bmatrix} 0 & 0 & 0 \\ s & 1 & 0 \\ 1 & t & 0 \end{bmatrix}$$

Układ równań dany powyższą macierzą ma przestrzeń rozwiązań $V_{(1)}$ wymiaru 2 wtedy i tylko wtedy, gdy $r(A - I) = 1$. Jest tak wtedy i tylko wtedy, gdy $st = 1$. A zatem szukane pary $(s, t) \in \mathbb{Z}_5^2$, dla których macierz A jest diagonalizowalna to $(1, 1), (2, 3), (3, 2), (4, 4)$. \blacksquare

⁵Czytelnikowi pamiętającemu czym jest rozkład przestrzeni V na sumę prostą dowolnej liczby podprzestrzeni polecam (niezbyt trudną, po prześledzeniu poniższych argumentów) próbę samodzielnego pokazania, że do dwóch równoważnych warunków z tezy twierdzenia poniżej można dołączyć trzeci: $V_{(a_1)} \oplus V_{(a_2)} \oplus \dots \oplus V_{(a_k)} = V$. Więcej — w jednym z dodatków.

Przejdźmy do dowodu Twierdzenia 3.1 charakteryzującego endomorfizmy diagonalizowalne.

Dowód. Zacniemy od pokazania, że każdy układ wektorów przestrzeni V , który jest złożony z k liniowo niezależnych układów wektorów z podprzestrzeni własnych $V_{(a_i)}$ (dla $i = 1, \dots, k$) jest liniowo niezależny.

Rozważmy więc k układów $\alpha_{i1}, \dots, \alpha_{im_i}$ liniowo niezależnych w $V_{(a_i)}$ — każdy złożony z m_i wektorów. Przypuśćmy, że:

$$\begin{aligned} &a_{11}\alpha_{11} + \dots + a_{1m_1}\alpha_{1m_1} + \\ &+ a_{21}\alpha_{21} + \dots + a_{2m_2}\alpha_{2m_2} + \\ &\qquad\qquad\qquad + \dots + \\ &+ a_{k1}\alpha_{k1} + \dots + a_{km_k}\alpha_{km_k} = 0, \end{aligned}$$

dla pewnych $a_{11}, \dots, a_{km_k} \in K$. Oznaczmy każdą z sum częściowych należących do odpowiedniego $V_{(a_i)}$:

$$\beta_i = a_{i1}\alpha_{i1} + \dots + a_{im_i}\alpha_{im_i} \in V_{(a_i)} \quad \text{dla } i = 1, \dots, k.$$

Skoro $\beta_1 + \dots + \beta_k = 0$, to na mocy Obserwacji 3.3 mamy $\beta_i = 0$, dla wszystkich i . Stąd dostajemy

$$a_{i1}\alpha_{i1} + \dots + a_{im_i}\alpha_{im_i} = 0.$$

Wobec liniowej niezależności każdego z układów $\alpha_{i1}, \dots, \alpha_{im_i}$ mamy $a_{i1}, \dots, a_{im_i} = 0$, dla wszystkich i . A zatem cały rozważany układ złożony z k podukładów pochodzących z V_{a_i} jest liniowo niezależny.

Z obserwacji tej wynika natychmiast, że jeśli zachodzi warunek

$$\dim V_{(a_1)} + \dim V_{(a_2)} + \dots + \dim V_{(a_k)} = \dim V,$$

to układ

$$\alpha_{11}, \dots, \alpha_{1m_1}, \alpha_{21}, \dots, \alpha_{2m_2}, \dots, \alpha_{k1}, \dots, \alpha_{km_k}$$

jest bazą przestrzeni V złożoną z wektorów własnych endomorfizmu ϕ . W szczególności endomorfizm ten jest diagonalizowalny.

Pozostaje więc wykazać, że jeśli przestrzeń V posiada bazę złożoną z wektorów własnych (czyli gdy ϕ jest endomorfizmem diagonalizowalnym), to zachodzi $\dim V_{(a_1)} + \dim V_{(a_2)} + \dots + \dim V_{(a_k)} = \dim V$.

Niech \mathcal{A} będzie bazą przestrzeni V złożonej z wektorów własnych endomorfizmu ϕ , mającego wartości własne a_1, \dots, a_k . Dla każdego $i = 1, \dots, k$ niech $\beta_{i1}, \dots, \beta_{in_i}$ będą wszystkimi tymi spośród wektorów bazy \mathcal{A} , które należą do $V_{(a_i)}$. Wówczas

$$n_1 + \dots + n_k = \dim V.$$

Ponadto wówczas dla każdego i układ $\beta_{i1}, \dots, \beta_{in_i}$ jest liniowo niezależny, więc $n_i \leq \dim V_{(a_i)}$. Zatem

$$\dim V = n_1 + \dots + n_k \leq \dim V_{(a_1)} + \dots + \dim V_{(a_k)} \leq \dim V,$$

na mocy Wniosku 3.1. Zatem z diagonalizowalności ϕ mamy $\dim V_{(a_1)} + \dots + \dim V_{(a_k)} = \dim V$. \square

Diagonalizowalność jest niezwykle elegancką własnością. Podstawową jej motywacją jest problem badania w jaki sposób zachowują się kolejne iteracje endomorfizmu. Przypomnijmy ważną kwestię.

Obserwacja 3.7

Niech V będzie przestrzenią wymiaru n nad ciałem K . Dla dowolnego $\phi \in \text{End}(V)$ oraz dla dowolnej bazy \mathcal{A} endomorfizmu ϕ macierz n -krotnego złożenia endomorfizmu ϕ w bazie \mathcal{A} , czyli endomorfizmu

$$\phi^n = \underbrace{\phi \circ \phi \circ \dots \circ \phi}_n$$

jest równa $(M(\phi)_{\mathcal{A}})^n$.

Zobaczmy dwa przykłady ważnych zastosowań diagonalizowalności w kontekście następującego faktu.

Obserwacja 3.8

Niech $A = C^{-1}DC$, gdzie D jest macierzą diagonalną oraz C – macierzą odwracalną. Wówczas:

$$A^n = (C^{-1}DC)^n = C^{-1}DCC^{-1}DCC^{-1} \dots CC^{-1}DC = C^{-1}D^nC.$$

Macierz D^n jest diagonalna i ma na przekątnej n -te potęgi odpowiednich elementów z przekątnej D .

Zobaczmy przykład zastosowania tej obserwacji.

Zadanie. Wyznacz macierz A^{2020} , gdzie

$$A = \begin{bmatrix} 7 & 3 \\ 3 & -1 \end{bmatrix} \in M_2(\mathbb{R}).$$

ROZWIĄZANIE. Wielomian charakterystyczny macierzy A równy jest

$$\begin{vmatrix} 7 - \lambda & 3 \\ 3 & -1 - \lambda \end{vmatrix} = (7 - \lambda)(-1 - \lambda) - 9 = \lambda^2 - 6\lambda - 16 = (\lambda + 2)(\lambda - 8).$$

A zatem macierz A jest podobna do macierzy diagonalnej:

$$A = P^{-1} \cdot \begin{bmatrix} -2 & 0 \\ 0 & 8 \end{bmatrix} \cdot P,$$

przy czym macierz P^{-1} zawiera w kolumnach wektory własne o wartościach własnych $-2, 8$ — na przykład $(1, -3)$ oraz $(3, 1)$. Istotnie, jeśli $\phi \in \text{End}(\mathbb{R}^2)$ zadany jest warunkiem $A = M(\phi)_{st}^{st}$ oraz jeśli przyjmiemy $\mathcal{A} = ((1, -3), (3, 1))$, wówczas $D = M(\phi)_{\mathcal{A}}^{\mathcal{A}}$ oraz $P = M(\text{id})_{st}^{\mathcal{A}}$. Zatem:

$$P^{-1} = \begin{bmatrix} 1 & 3 \\ -3 & 1 \end{bmatrix}.$$

W rezultacie dostajemy:

$$A^{2020} = \left(P^{-1} \cdot \begin{bmatrix} -2 & 0 \\ 0 & 8 \end{bmatrix} \cdot P \right)^{2020} = P^{-1} \cdot \begin{bmatrix} 2^{2020} & 0 \\ 0 & 8^{2020} \end{bmatrix} \cdot P.$$

■

Inny przykład — tym razem pytanie krótkiej odpowiedzi. Warto dobrze przemyśleć poniższą odpowiedź.

Zadanie. Macierz rzeczywista A rozmiarów 2×2 ma wartości własne 1 i 2. Wyznaczyć

$$\det(A^3 - 3A^2 + A + 5I).$$

ROZWIĄZANIE. Traktujemy A jako macierz endomorfizmu ϕ przestrzeni dwuwymiarowej w bazie standardowej. Wówczas wartość $\det(\phi^3 - 3\phi^2 + \phi + 5\text{id})$ nie zależy od wyboru macierzy przekształcenia ϕ . W szczególności, skoro endomorfizm ϕ przestrzeni dwuwymiarowej ma dwie różne wartości własne, to jest on diagonalizowalny (mamy $2 = V_{(1)} + V_{(2)}$) i ma w pewnej bazie macierz $J = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$. A zatem

$$\det(A^3 - 3A^2 + A + 5I) = \det(J^3 - 3J^2 + J + 5I) = \begin{vmatrix} 1^3 - 3 \cdot 1^2 + 1 + 5 & 0 \\ 0 & 2^3 - 3 \cdot 2^2 + 2 + 5 \end{vmatrix} = 12.$$

■

Sklassyfikowaliśmy endomorfizmy diagonalizowalne w języku wymiarów podprzestrzeni własnych. Niestety baza z wektorów własnych nie zawsze istnieje nawet jeśli wielomian charakterystyczny rozkłada się na czynniki liniowe. Co możemy zatem powiedzieć o geometrycznych własnościach takiego endomorfizmu? Jak się okaże, kluczowe będzie rozważenie dodatkowej klasy endomorfizmów — tak zwanych endomorfizmów nilpotentnych. Mają one tę własność, że złożone ze sobą pewną liczbę razy stają się przekształceniem zerowym. Pozwolą one na zrozumienie centralnego wyniku tej części kursu — twierdzenia Jordana.

3.1 Zadania do samodzielnej pracy

Zadania ilustrujące umiejętności niezbędne do zaliczenia przedmiotu oznaczone są symbolem ♠.

Przy tych zadaniach dodany jest opis umiejętności, które sprawdzają.

1. (♠ Stwierdzanie czy macierz jest diagonalizowalna)

Dla każdej z poniższych macierzy A_1, A_2, A_3, A_4 rozstrzygnij czy jest ona diagonalizowalna nad \mathbb{R} oraz czy jest diagonalizowalna nad \mathbb{C} :

$$A_1 = \begin{bmatrix} 1 & 2 & 0 \\ 2 & -2 & 0 \\ 0 & 0 & -3 \end{bmatrix}, \quad A_2 = \begin{bmatrix} -3 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 2 & -2 \end{bmatrix}, \quad A_3 = \begin{bmatrix} 0 & 2 & 0 \\ -2 & 0 & 0 \\ 0 & 0 & 2 \end{bmatrix}, \quad A_4 = \begin{bmatrix} 0 & 1 & 0 \\ -4 & 4 & 0 \\ -2 & 1 & 2 \end{bmatrix}.$$

Znajdź wszystkie takie $s, t \in \mathbb{Z}_5$, że macierz

$$A = \begin{bmatrix} 1 & 0 & 0 \\ s & 2 & 0 \\ 1 & t & 1 \end{bmatrix} \in M_{3 \times 3}(\mathbb{Z}_5)$$

jest diagonalizowalna nad ciałem pięcioelementowym \mathbb{Z}_5 .

2. (♠ Wyznaczanie potęg macierzy diagonalizowalnych)

- Wyznacz macierz $\begin{bmatrix} 7 & 3 \\ 3 & -1 \end{bmatrix}^{2020}$.
- Endomorfizm $\phi : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ jest dany wzorem $\phi((x_1, x_2, x_3)) = (3x_1, x_1 + 2x_2 + x_3, x_1 + x_2 + 2x_3)$. Niech $A = M(\phi)_{st}^{st}$. Oblicz A^m dla $m \in \mathbb{N}$.
- Niech $s \in \mathbb{R}$ oraz niech macierz $A_s \in M_4(\mathbb{R})$ będzie postaci:

$$A_s = \begin{bmatrix} -2 & -2 & 0 & 0 \\ s & s & 0 & 0 \\ 0 & 0 & -4 & 4 \\ 0 & 0 & -s & s \end{bmatrix}.$$

Dla jakich wartości $s \in \mathbb{R}$ macierz A_s jest diagonalizowalna nad \mathbb{R} ? Wyznacz $(A_3)^{100}$.

3. (♠ Krotności geometryczne i ich własności)

- Niech $\phi : V \rightarrow V$ będzie endomorfizmem i niech $\{\alpha_1, \alpha_2, \alpha_3\}$ będzie bazą V , przy czym $\phi(\alpha_1) = 2\alpha_1$, $\phi(\alpha_2) = \alpha_2$ i $\phi(\alpha_3) = 2\alpha_3$. Czy $\dim V_{(2)} = 2$?
- Czy istnieje endomorfizm $\phi : V \rightarrow V$ pięciowymiarowej przestrzeni liniowej V nad \mathbb{R} , taki że liczby 1, 4, 7 są wartościami własnymi ϕ oraz $\dim V_{(4)} = 4$?
- Czy istnieje endomorfizm rzeczywistej przestrzeni liniowej posiadający wektory własne α, β, γ o wartościach własnych 2, 5, -7, odpowiednio, spełniające: $\alpha + \beta + \gamma = 0$?
- Niech ϕ będzie endomorfizmem 7-wymiarowej przestrzeni liniowej V nad \mathbb{R} . Przypuśćmy, że 3 jest wartością własną endomorfizmu ϕ , przy czym $\dim V_{(3)} = 6$ oraz przypuśćmy, że ϕ nie jest monomorfizmem. Czy wynika stąd, że endomorfizm ϕ jest diagonalizowalny?
- Macierz $A \in M_5(\mathbb{R})$ spełnia $r(A - 2I) = 2$. Czy jest możliwe, aby $r(A + 2I) = 2$?
- Wykaż, że jeśli macierz $A \in M_n(K)$ ma dokładnie jedną wartość własną w K , to A jest diagonalizowalna nad K wtedy i tylko wtedy, gdy A jest diagonalna.
- Niech A oraz B będą macierzami rozmiaru $n \times n$. Wiadomo, że wektory $\alpha_1, \dots, \alpha_n$ są liniowo niezależnymi wektorami własnymi zarówno A , jak i B , i odpowiadają one kolejno wartościom własnym $\lambda_1, \dots, \lambda_n$. Czy wynika stąd, że $A = B$?

4. Endomorfizm $\phi : \mathbb{R}^n \rightarrow \mathbb{R}^n$ jest diagonalizowalny. Czy jest prawdą, że $\dim \text{im } \phi = \dim \text{im } \phi^3$?

5. Macierz rzeczywista A rozmiarów 2×2 ma wartości własne 1 i 2. Wyznacz $\det(A^3 - 3A^2 + A + 5I)$.

6. Niech $A \in M_{3 \times 3}(K)$ będzie niezerową macierzą diagonalizowalną nad ciałem K . Wykaż, że następujące dwie liczby są równe rzędowi macierzy A :

- $\max\{i : a_i \neq 0\}$, gdzie $w_A(\lambda) = -\lambda^3 + a_1\lambda^2 + a_2\lambda + a_3$,
- rozmiar największej odwracalnej macierzy kwadratowej powstałej z A przez wykreślenie wierszy i kolumn o tych samych indeksach.

Wykaż, że bez założenia o diagonalizowalności macierzy A teza zadania nie jest prawdziwa.

3.2 Uzupełnienie. Probabilistyka na sześcienniej kostce

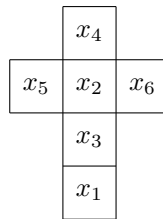
Diagonalizowalność macierzy służy także do badania przebiegu procesów „w dłuższej perspektywie”. Jest to niezwykle rozbudowana teoria zawierająca wiele istotnych wyników. Zobaczymy ją na przykładzie.

ZADANIE. Matematyk ma kostkę sześcienną, na której ścianach umieszczono liczby N_1, \dots, N_6 . Zapisuje on sobie, dla każdej ściany, średnią arytmetyczną liczb na sąsiednich czterech ścianach. Następnie zastępuje każdą z liczb N_i uzyskaną średnią, i powtarza tę procedurę. Jakie liczby pojawiają się na poszczególnych ścianach po wykonaniu bardzo wielu takich zmian?

Operacja opisana w zadaniu będzie przez nas przetłumaczona na język endomorfizmu przestrzeni liniowych. Ale jakich przestrzeni? Będzie to przestrzeń \mathbb{R}^6 złożona z ciągów

$$(x_1, x_2, x_3, x_4, x_5, x_6),$$

gdzie x_i to są liczby wpisane na ścianach kostki jak na rysunku poniżej.



Rozważmy przekształcenie liniowe $f : \mathbb{R}^6 \rightarrow \mathbb{R}^6$ zadane macierzą A

$$A = \frac{1}{4} \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

Przemnożenie tej macierzy przez wektor $x = (x_1, \dots, x_6)^T$ daje dokładnie operację, którą wykonuje się na ściankach kostki. Musimy tę operację wykonać wiele razy, więc interesuje nas jak wygląda, dla dużych n , wektor $A^n x$? Jest więc jasne, że trzeba diagonalizować macierz A . Można to zrobić i dostajemy sześć wektorów własnych:

- $v_1 = (1, 1, 1, 1, 1, 1)$, gdzie $f(v_1) = v_1$,
- $v_2 = (0, 0, 1, 1, -1, -1)$, gdzie $f(v_2) = -\frac{1}{2}v_2$,
- $v_3 = (-2, -2, 1, 1, 1, 1)$, gdzie $f(v_3) = -\frac{1}{2}v_3$,
- $v_4 = (0, 0, -1, 1, 0, 0)$, gdzie $f(v_4) = 0$,
- $v_5 = (0, 0, 0, 0, 1, -1)$, gdzie $f(v_5) = 0$,
- $v_6 = (-1, 1, 0, 0, 0, 0)$, gdzie $f(v_6) = 0$.

W bazie $\mathcal{A} = (v_1, v_2, \dots, v_6)$ endomorfizm f dany jest macierzą B :

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

Biorąc wektor $v = a_1v_1 + \dots + a_6v_6$ widzimy, że

$$B \cdot (a_1v_1 + \dots + a_6v_6) = a_1v_1 - \frac{1}{2}a_2v_2 - \frac{1}{2}a_3v_3.$$

A zatem dla całkowitych dodatnich n mamy

$$B^n = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & (-\frac{1}{2})^n & 0 & 0 & 0 & 0 \\ 0 & 0 & (-\frac{1}{2})^n & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Innymi słowy

$$B^n v \rightarrow a_1 v_1.$$

A jakie są współrzędne interesującego nas wektora (N_1, \dots, N_6) w bazie \mathcal{A} ? Trzeba sprawdzić, że pierwszą z nich jest

$$\frac{1}{6}(N_1 + N_2 + \dots + N_6).$$

Na pierwszy rzut oka może się wydawać, że policzenie tych współrzędnych jest trudne, ale za jakiś czas przekonamy się, że wektory v_i są prostopadłe i będzie nieco łatwiej. Natomiast konsekwencja jest taka:

$$B^n \cdot \begin{bmatrix} N_1 \\ N_2 \\ \vdots \\ N_6 \end{bmatrix} \rightarrow \frac{1}{6}(N_1 + N_2 + \dots + N_6) \cdot \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} = \frac{1}{6} \begin{bmatrix} N_1 + N_2 + \dots + N_6 \\ N_1 + N_2 + \dots + N_6 \\ \vdots \\ N_1 + N_2 + \dots + N_6 \end{bmatrix}.$$

A zatem dla dużych n stanie się to, czego się spodziewamy – nastąpi uśrednienie liczb wpisanych na każdej ścianie. A czy wiecie Państwo jak to pokazać bez takiej skomplikowanej matematyki?

Co to ma wspólnego z tytułową probabilistyką? Czytelnik zechce zauważyć, że wiersze i kolumny rozważanej przez nas macierzy przekształcenia f mają wyrazy nieujemne, których sumy są równe 1. Rozważmy następujący problem.

ZADANIE. Matematyk znalazł się na kostce sześcienniej, na ścianie z jednym oczkiem. W każdym ruchu przechodzi losowo na jedną z czterech sąsiednich ścian. Jakie jest prawdopodobieństwo, że po dziesiątym przejściu stanie na ścianie z trzema oczkami? Czy jeśli Matematyk wykona *dużo* takich przejść, to trafi z równym prawdopodobieństwem na dowolną ścianę?

Rozwiązanie pierwszej części problemu polega na przemnożeniu wektora $(1, 0, 0, 0, 0, 0)$ przez macierz A^{10} . Dlaczego? Rozważmy ogólny kontekst, związany z dyskretnymi procesami Markowa, czyli ciągami zdarzeń, w których prawdopodobieństwo kolejnego zdarzenia zależy jedynie od wyniku poprzedniego.

Założmy, że mamy skończony zbiór E oraz ciąg $X = (X_n)_{n \in \mathbb{N}}$ przyjmujący wartości w „zbiornie stanów” E . Przykładowo: E może być zbiorem ścianek kostki, zaś X_i – położeniem Matematyka po i -tym skoku. Powiemy (starając się nie narazić zbyt wiele Probabilistom takim spłyleniem), że dyskretnym łańcuchem Markowa jest taki ciąg X (zmiennych losowych), dla którego dla każdego $n \in \mathbb{N}$ spełniona jest zależność (trzeba sobie przypomnieć prawdopodobieństwo warunkowe):

$$\mathbb{P}(X_{n+1} = s_{n+1} \mid X_n = s_n, \dots, X_1 = s_1, X_0 = s_0) = \mathbb{P}(X_{n+1} = s_{n+1} \mid X_n = s_n).$$

Krótko mówiąc chodzi o sytuację, w której prawdopodobieństwo tego co się stanie w następnym kroku zależy wyłącznie od prawdopodobieństwa zajścia obecnego kroku, a bez uwzględnienia prawdopodobieństw zajścia wcześniejszych — jest to swego rodzaju „zapominanie o przeszłości”. Czytelnik w przyszłości pozna te problemy dokładniej. Co to ma wspólnego z naszą grą, macierzami i diagonalizacją?

Założmy, że chcemy wyznaczyć prawdopodobieństwo tego, że na początku Matematyk jest na ścianie s_0 , po pierwszym przejściu trafia na s_1 , a po drugim — na s_2 , czyli:

$$\mathbb{P}(X_0 = s_0, X_1 = s_1, X_2 = s_2).$$

Używając twierdzenia o prawdopodobieństwie całkowitym (szkolnego?) mamy:

$$\mathbb{P}(X_0 = s_0, X_1 = s_1, X_2 = s_2) = \mathbb{P}(X_0 = s_0) \cdot \mathbb{P}(X_1 = s_1 \mid X_0 = s_0) \cdot \mathbb{P}(X_2 = s_2 \mid X_0 = s_0, X_1 = s_1).$$

Teraz kluczowy jest warunek Markowa, który upraszcza rachunek wyżej, bowiem:

$$\mathbb{P}(X_2 = s_2 | X_0 = s_0, X_1 = s_1) = \mathbb{P}(X_2 = s_2 | X_1 = s_1)$$

dając nam

$$\mathbb{P}(X_0 = s_0, X_1 = s_1, X_2 = s_2) = q_0(s_0) \cdot p(s_0, s_1) \cdot p(s_1, s_2),$$

gdzie $q_0(s_i)$ to prawdopodobieństwo, że na początku jesteśmy w stanie s_i oraz

$$\mathbb{P}(X_{n+1} = s_{n+1} | X_n = s_n) = p(s_n, s_{n+1}).$$

Ogólnie można łatwo pokazać, że prawdopodobieństwo, iż w $n + 1$ -szym ruchu procesu Markowa znajdziemy się w stanie s_{n+1} równe jest:

$$q_{n+1}(s_{n+1}) = \sum_{s \in E} p(s, s_{n+1}) \cdot q_n(s).$$

Czy Państwo widzą tu mnożenie macierzy? Rozważmy dowolny zbiór dopuszczalnych stanów $E = \{e_1, \dots, e_k\}$. Wówczas

$$\begin{bmatrix} q_n(e_1) & \dots & q_n(e_k) \end{bmatrix} \cdot \begin{bmatrix} p(e_1, e_1) & \dots & p(e_1, e_n) \\ \vdots & \ddots & \vdots \\ p(e_n, e_1) & \dots & p(e_n, e_n) \end{bmatrix} = \begin{bmatrix} q_{n+1}(e_1) & \dots & q_{n+1}(e_k) \end{bmatrix}.$$

To oznacza, że do zrozumienia dynamiki procesu Markowa wystarczy znajomość wektora prawdopodobieństw zajścia odpowiednich stanów na początku procesu, oraz tzw. macierz przejścia, czyli:

$$\begin{bmatrix} q_0(e_1) & \dots & q_0(e_k) \end{bmatrix} \cdot \begin{bmatrix} p(e_1, e_1) & \dots & p(e_1, e_n) \\ \vdots & \ddots & \vdots \\ p(e_n, e_1) & \dots & p(e_n, e_n) \end{bmatrix}^n = \begin{bmatrix} q_{n+1}(e_1) & \dots & q_{n+1}(e_k) \end{bmatrix}.$$

Czy nasz proces skakania po kalendarzu jest procesem Markowa, dla $E = \{1, 2, 3, 4, 5, 6\}$? To zależy od naszego Matematyka, ale jeśli przyjmiemy, że błąka się on rzeczywiście w sposób „losowy” po naszej kostce, zapominając (lub nie przejmując się) gdzie był krok wcześniej — wówczas możemy działać.

Jeśli na przykład przyjmiemy, że Matematyk wylądował na ściance z jednym oczkiem, to jak policzyć dokąd może dojść? Mówi o tym macierz A . Z prawdopodobieństwem $1/4$ może przejść na pola z odpowiednio trzema, czterema, pięcioma lub sześcioma oczkami (patrz rysunek kostki na początku). A zatem po dziesiątym ruchu wektor prawdopodobieństw położenia Matematyka dla poszczególnych ścian na kostce to:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 & 0,25 & 0,25 & 0,25 & 0,25 \\ 0 & 0 & 0,25 & 0,25 & 0,25 & 0,25 \\ 0,25 & 0,25 & 0 & 0 & 0,25 & 0,25 \\ 0,25 & 0,25 & 0 & 0 & 0,25 & 0,25 \\ 0,25 & 0,25 & 0,25 & 0,25 & 0 & 0 \\ 0,25 & 0,25 & 0,25 & 0,25 & 0 & 0 \end{bmatrix}^{10}.$$

Trudno to policzyć? Trudno. Ale jeśli umielibyśmy zapisać wektor $(1, 0, 0, 0, 0, 0)$ w bazie $\mathcal{A} = (v_1, v_2, \dots, v_6)$ to historia by była całkiem inna, bowiem do policzenia mielibyśmy iloczyn pewnego wektora przez dziesiątą potęgę znanej nam już macierzy diagonalnej. To by nam ułatwiło zrozumienie losów Matematyka.

O rozważanym tu temacie mówić można naprawdę bardzo dużo. Macierze rzeczywiste rozważane przez nas wyżej nazywamy PODWÓJNIE STOCHASTYCZNYMI, a ich rozmaite własności oraz związane z nimi niezwykle głębokie i ważne twierdzenia poznać można na przykład poprzez lekturę artykułu

Ciesielska, Kowalczyk, *Twierdzenie Perrona-Frobeniusa i jego zastosowanie w algorytmie Page Rank*,
Prace Koła Matematyków Uniwersytetu Pedagogicznego w Krakowie
<https://pracekm.up.krakow.pl/article/view/2712/2379>

Algorytm Page Rank pojawia się nieprzypadkowo. W tym świetnym artykule popularyzującym zagadnienie macierzy o nieujemnych współczynnikach znajdziecie Państwo łańcuchy Markowa (z wieloma przykładami), wspomniane w innym dodatku macierze sąsiedztwa, metody ustalania rankingów, tzw. problemy kontroli sił, modele przeżycia (muchy i żaby to tylko początek tej opowieści) oraz właśnie tytułowy Page Rank, opatentowany w 1998 roku przez dwóch doktorantów Uniwersytetu Stanforda, służący określeniu „wartości” stron internetowych i sporządzanie ich rankingów. Zachęcam do lektury (zamiast dodatków)!

Rozdział 4

Sformułowanie twierdzenia Jordana

Klasa endomorfizmów diagonalizowalnych obejmuje wiele sytuacji istotnych z punktu widzenia zastosowań algebry liniowej. Chcąc jednak zrozumieć jak działają inne endomorfizmy, a w szczególności jak wyglądać mogą klasy podobieństwa macierzy kwadratowych, wyróżnimy dziś¹ pewne specjalne macierze górnorójkątne, które nie są wzajemnie do siebie podobne. Zagadnienie to jest głębokie i prowadzi do ważnego twierdzenia tego kursu – twierdzenia Jordana. Aby je sformułować potrzebujemy kilku definicji.

Definicja 4.1: Klatki Jordana

Niech $a \in K$. KLATKĄ JORDANA o wartości własnej a i rozmiarze n nazywamy macierz postaci

$$M = \begin{bmatrix} a & 1 & 0 & \dots & 0 \\ 0 & a & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & a \end{bmatrix} \in M_n(K),$$

przy czym $M = [a]$, gdy $n = 1$. Innymi słowy wyrazy m_{ij} macierzy M spełniają warunki:

$$m_{ij} = \begin{cases} a, & \text{gdy } i = j, \\ 1, & \text{gdy } j - i = 1, \\ 0, & \text{w pozostałych przypadkach.} \end{cases}$$

Powyższe macierze są górnorójkątne, ale nie są one diagonalizowalne nad ciałem K , dla $n > 1$. Oczywiście $w_M(\lambda) = (a - \lambda)^n$, Widzimy więc, że krotność algebraiczna wartości własnej a wynosi n , podczas gdy jej krotność geometryczna wynosi 1, czyli równa jest wymiarowi przestrzeni rozwiązań układu o macierzy:

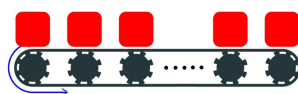
$$M - aI = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & 0 \end{bmatrix}.$$

Jedyną wartością własną macierzy wyżej jest zero. Jest ona macierzą w bazach standardowych endomorfizmu $\phi \in \text{End}(K^n)$ postaci:

$$\phi((x_1, \dots, x_n)) = (x_2, x_3, \dots, x_n, 0).$$

Endomorfizm ϕ zachowuje się jak taśma, która przy każdej iteracji „zrzuca” jedną zmienną. Mamy:

$$\phi^2((x_1, \dots, x_n)) = (x_3, \dots, x_n, 0, 0), \dots, \phi^{n-1}((x_1, \dots, x_n)) = (x_n, 0, \dots, 0), \phi^n((x_1, \dots, x_n)) = (0, 0, \dots, 0).$$



¹Ostatnia aktualizacja: 07.05.2023 r.

Aby zobaczyć jakie macierze możemy „budować” z klatek Jordana powiedzmy o macierzach blokowych.

Definicja 4.2: Macierz w postaci blokowej

Niech $A \in M_n(K)$ oraz $n = n_1 + n_2 + \dots + n_k$, dla pewnych całkowitych $n_1, \dots, n_k, k > 0$. Niech macierz $D_{ij} \in M_{n_i \times n_j}(K)$, zwana dalej BLOKIEM A względem podziału $n = n_1 + n_2 + \dots + n_k$, powstaje z macierzy A przez:

- usunięcie wszystkich wierszy poza wierszami o indeksach

$$\underbrace{n_1 + \dots + n_{i-1} + 1, \dots, n_1 + \dots + n_{i-1} + n_i}_{n_i \text{ nieusuniętych wierszy}}$$

- usunięcie wszystkich kolumn poza kolumnami o indeksach

$$\underbrace{n_1 + \dots + n_{j-1} + 1, \dots, n_1 + \dots + n_{j-1} + n_j}_{n_j \text{ nieusuniętych kolumn}}$$

przy czym przyjmujemy $n_0 = 0$. Wówczas mówimy, że macierz A jest w POSTACI BLOKOWEJ (D_{ij}) (względem rozbitcia $n = n_1 + n_2 + \dots + n_k$), co oznaczamy często w następujący sposób:

$$A = \begin{array}{c|c|c|c} D_{11} & D_{12} & \dots & D_{1k} \\ \hline D_{21} & D_{22} & \dots & D_{2k} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline D_{k1} & D_{k2} & \dots & D_{kk} \end{array} \quad \text{lub prościej} \quad A = \begin{bmatrix} D_{11} & D_{12} & \dots & D_{1k} \\ D_{21} & D_{22} & \dots & D_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ D_{k1} & D_{k2} & \dots & D_{kk} \end{bmatrix}.$$

Macierz A nazywamy BLOKOWO DIAGONALNĄ, jeśli $D_{ij} = 0$, dla wszystkich $i \neq j$.

Oto przykłady blokowo-diagonalnych macierzy rozmiaru 4 o wyrazach rzeczywistych:

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

Przejdźmy do owej specjalnej rodziny macierzy górnotrójkątnych, o której mówić będzie tytułowy rezultat. Jest to rodzina pewnych macierzy blokowo-diagonalnych.

Definicja 4.3: Macierz w postaci Jordana

Mówimy, że macierz $A \in M_n(K)$ jest w POSTACI JORDANA, jeśli istnieją takie liczby całkowite dodatnie n_1, n_2, \dots, n_k oraz macierze

$$J_1 \in M_{n_1}(K), \quad J_2 \in M_{n_2}(K), \quad \dots, \quad J_k \in M_{n_k}(K)$$

będące klatkami Jordana takimi, że $n = n_1 + n_2 + \dots + n_k$ oraz

$$A = \begin{bmatrix} J_1 & 0 & 0 & \dots & 0 \\ 0 & J_2 & 0 & \dots & 0 \\ 0 & 0 & J_3 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & J_k \end{bmatrix}, \quad (*),$$

czyli A jest macierzą blokową diagonalną o blokach diagonalnych J_1, \dots, J_k . Dla danej wartości własnej λ macierzy A te klatki Jordana J_i , które na swojej przekątnej mają wartość λ nazywamy KLATKAMI JORDANA ODPOWIADAJĄCYMI WARTOŚCI WŁASNEJ λ w postaci (*).

Oto przykład sytuacji, w której rozważamy endomorfizm ϕ przestrzeni wymiaru 16 mający (parami różne) wartości własne $\lambda_1 = 1, \lambda_2 = 3$ o krotnościach algebraicznych $a_1 = 8, a_2 = 8$, gdzie:

$$M(\phi)_{st}^{st} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 \end{bmatrix} \in M_{16}(\mathbb{R}). \quad (*)$$

Macierz $M(\phi)_{st}^{st}$ ma zatem postać Jordana o:

- trzech kłatkach odpowiadających wartości własnej 1; klatki te mają rozmiary 4, 3, 1,
- trzech kłatkach odpowiadających wartości własnej 3; klatki te mają rozmiary 3, 3, 2.

Główny rezultat dotyczący macierzy w postaci Jordana jest następujący.

Twierdzenie 4.1: Twierdzenie Jordana

Niech V będzie przestrzenią skończenie wymiarową nad ciałem K oraz niech $\phi \in \text{End}(V)$. Jeżeli wielomian charakterystyczny endomorfizmu ϕ rozkłada się nad ciałem K na czynniki liniowe to istnieje baza \mathcal{A} przestrzeni V zwana BAZĄ JORDANA, w której macierz ϕ ma postać Jordana.

W szczególności jeśli ciało K jest algebraicznie domknięte, wówczas każdy endomorfizm $\phi \in \text{End}(V)$ ma w pewnej bazie przestrzeni liniowej V macierz w postaci Jordana. Macierze $A, B \in M_n(K)$ będące w postaci Jordana są podobne wtedy i tylko wtedy, gdy różnią się co najwyżej kolejnością kłatek w postaci (*).

Nie wykażemy tego twierdzenia, ale spróbujemy zrozumieć o czym ono mówi i w jaki sposób je stosować. Zwróćmy uwagę na warunek mówiący o rozkładalności wielomianu $w_\phi(\lambda)$ na czynniki stopnia nie większego niż 1. Jak pokazujemy w uzupełnieniu, jest on równoważny istnieniu bazy, w której endomorfizm ma macierz górnotrójkątną (to fakt znacznie łatwiejszy od twierdzenia Jordana). Zaczniemy jednak od pokazania, że macierze rozmiaru n o wyrazach w ciele K będące w postaci Jordana są – podobnie jak macierze diagonalne – podobne wtedy i tylko, gdy różnią się kolejnością kłatek.

Twierdzenie 4.2

Niech $A \in M_n(K)$ i niech a będzie wartością własną macierzy A . Dla każdego $m = 1, 2, \dots$ niech

$$q_m = r(A - aI)^{m-1} - r(A - aI)^m.$$

Przyjmujemy też $(A - aI)^0 = I$. Wówczas jeśli $B \in M_n(K)$ jest macierzą w postaci Jordana podobną do A , to w macierzy B :

- (1) suma rozmiarów kłatek odpowiadających wartości własnej a jest krotnością algebraiczną a .
- (2) Liczba kłatek Jordana rozmiaru $\geq m$ odpowiadających a wynosi q_m .
- (3) Liczba kłatek Jordana rozmiaru m odpowiadających a wynosi $q_m - q_{m+1}$.

Dowód. Macierze A i B są podobne, więc mają ten sam wielomian charakterystyczny. Stwierdzenie (1) wynika od razu z tego, że wszystkimi pierwiastkami wielomianu charakterystycznego macierzy (górnoróżkowej) w postaci Jordana są elementy z przekątnej. Suma rozmiarów klatek odpowiadających wartości własnej a równa jest sumie wystąpień a na przekątnej macierzy B . Dowodzimy (2), (3). Zaczniemy od sprawdzenia, że jeśli A jest macierzą rozmiaru n nad K , oraz B jest podobną do niej macierzą w postaci Jordana, to dla każdego $a \in K$ mamy

$$r(A - aI)^k = r(B - aI)^k.$$

Rzeczywiście, skoro $B = C^{-1}AC$, dla pewnej macierzy odwracalnej C , to:

$$C^{-1}(A - aI)C = C^{-1}AC - C^{-1}aIC = B - aI.$$

W szczególności macierze $A - aI$ oraz $B - aI$ są podobne. Mamy więc:

$$\begin{aligned} (B - aI)^k &= (C^{-1}(A - aI)C)^k = \\ &= \underbrace{C^{-1}(A - aI)C \cdot C^{-1}(A - aI)C \cdot \dots \cdot C^{-1}(A - aI)C}_k \\ &= C^{-1}(A - aI)^k C. \end{aligned}$$

Skoro macierze $(B - aI)^k$ oraz $(A - aI)^k$ są podobne, to oczywiście ich rzędy są równe. Zajmiemy się zatem wyznaczeniem rzędów potęg odpowiednich macierzy powstałych z macierzy w postaci Jordana.

Zauważmy, że dla macierzy blokowo-diagonalnej B mamy:

$$B = \begin{bmatrix} J_1 & 0 & 0 & \dots & 0 \\ 0 & J_2 & 0 & \dots & 0 \\ 0 & 0 & J_3 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & J_k \end{bmatrix} \implies B^m = \begin{bmatrix} J_1^m & 0 & 0 & \dots & 0 \\ 0 & J_2^m & 0 & \dots & 0 \\ 0 & 0 & J_3^m & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & J_k^m \end{bmatrix}.$$

W szczególności:

$$r(B^m) = r(J_1^m) + r(J_2^m) + \dots + r(J_k^m).$$

Po drugie, zauważmy, że jeśli B jest blokowo-diagonalna, to również $B - aI$ jest blokowo diagonalna. Skoro B jest w postaci Jordana z klatkami J_1, J_2, \dots, J_k odpowiadającymi wartościom własnym a_1, \dots, a_k , to $B - aI$ ma klatki Jordana $J_1 - aI, J_2 - aI, \dots, J_k - aI$ o wartościach własnych $a_1 - a, a_2 - a, \dots, a_n - a$ (i tych samych rozmiarach). Stąd:

$$r(B - aI)^m = r(J_1 - aI)^m + r(J_2 - aI)^m + \dots + r(J_k - aI)^m.$$

Chcemy wyznaczyć rząd potęgi macierzy postaci:

$$J_i - aI = \begin{bmatrix} a_i - a & 1 & 0 & \dots & 0 & 0 \\ 0 & a_i - a & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & a_i - a & 1 \\ 0 & 0 & 0 & \dots & 0 & a_i - a \end{bmatrix}.$$

Oczywiście jeśli $a_i - a \neq 0$, to rząd każdej potęgi tej klatki równy jest jej rozmiarowi, powiedzmy s_i . Jeśli jednak $a_i - a = 0$, to dostajemy macierz mającą jedynki nad przekątną samych zer. A zatem jeśli (po ewentualnym przenumerowaniu) przyjmiemy, że $a_i - a = 0$ dla $i = 1, 2, 3, \dots, s$, gdzie s to liczba klatek Jordana macierzy B odpowiadających wartości własnej a , to mamy:²

$$r(B - aI)^{m-1} - r(B - aI)^m = \sum_{i=1}^s r(J_i - aI)^{m-1} - r(J_i - aI)^m.$$

²Dla $i > s$, czyli dla klatek J_i nie odpowiadających wartości własnej a mamy

$$r(J_i - aI)^{m-1} = r(J_i - aI)^m = s_i.$$

Założmy, że J_i ma rozmiar s_i . Ile wynosi składnik opisany wyżej? Przypomnijmy, że

$$J_i - aI = \begin{bmatrix} 0 & \mathbf{1} & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & \mathbf{1} \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \end{bmatrix} \in M_{s_i}(K).$$

Innymi słowy $J_i - aI$ jest macierzą w bazach standardowych (znanego nam już) endomorfizmu $\phi \in \text{End}(K^{s_i})$ postaci $\phi(x_1, \dots, x_{s_i}) = (x_2, x_3, \dots, x_{s_i}, 0)$. Jest zatem jasne, że

$$\dim \text{im } \phi^m = r(J_i - aI)^m = \begin{cases} s_i - m, & m \leq s_i \\ 0, & m \geq s_i. \end{cases}$$

Stąd dla $i = 1, 2, \dots, s$ mamy:

$$r(J_i - aI)^{m-1} - r(J_i - aI)^m \in \{0, 1\},$$

przy czym różnica ta równa jest

- 0 dokładnie wtedy, gdy $m > s_i$, czyli gdy klatka J_i ma rozmiar $< m$,
- 1 dokładnie wtedy, gdy $m \leq s_i$, czyli gdy klatka J_i ma rozmiar $\geq m$.

W szczególności mamy:

- $r(B - aI)^0 - r(B - aI)^1$ to liczba kl. Jordana macierzy B odp. wart. własnej a rozmiaru ≥ 1 ,
- $r(B - aI)^1 - r(B - aI)^2$ to liczba kl. Jordana macierzy B odp. wart. własnej a rozmiaru ≥ 2 ,
- $r(B - aI)^2 - r(B - aI)^3$ to liczba kl. Jordana macierzy B odp. wart. własnej a rozmiaru ≥ 3 , itd.

□

Powyższe rozważania pozwalają sformułować wniosek, wynikający oczywiście z twierdzenia Jordana.

Wniosek 4.1

Niech K będzie ciałem algebraicznie domkniętym oraz niech $A, B \in M_n(K)$. Następujące warunki są równoważne:

- macierze A, B są podobne,
- dla każdego $a \in K$ oraz dla każdego $k \geq 1$ mamy: $r(A - aI)^k = r(B - aI)^k$.

Rozważmy przykład macierzy $A \in M_{16}(\mathbb{R})$ postaci (*). Po pierwsze, $w_A(\lambda) = (1 - \lambda)^8(3 - \lambda)^8$. Zatem krotność algebraiczna każdej z wartości własnych 1 i 3 wynosi 8. Tyle też wynosi suma rozmiarów klatek odpowiadającej każdej z wartości własnych. Poznajmy ich rozmiary, zaczynając od wartości własnej 1.

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

4.1 Zadania do samodzielnej pracy

Zadania ilustrujące umiejętności niezbędne do zaliczenia przedmiotu oznaczone są symbolem ♠. Przy tych zadaniach dodany jest opis umiejętności, które sprawdzają.

1. (♠ Rozstrzygnięcie czy macierze są podobne)

Dla każdej pary i, j , gdzie $1 \leq i < j \leq 4$, zbadaj czy macierze $A_i, A_j \in M_3(\mathbb{R})$ są podobne.

$$A_1 = \begin{bmatrix} 2 & 0 & 1 \\ 1 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 2 & 0 & 0 \\ 1 & 2 & 1 \\ 0 & 0 & 2 \end{bmatrix}, \quad A_3 = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 1 & 2 \end{bmatrix}, \quad A_4 = \begin{bmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 1 & 2 \end{bmatrix}.$$

2. (♠ Znajdowanie postaci Jordana)

Znajdź postać Jordana poniższych macierzy o wyrazach z \mathbb{R} :

$$A_1 = \begin{bmatrix} 4 & -1 & 5 \\ 1 & 2 & 7 \\ 0 & 0 & 3 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 5 & 1 & 0 & 0 \\ -1 & 3 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 3 & 1 & 2 & 4 \end{bmatrix}, \quad A_3 = \begin{bmatrix} 5 & 0 & 0 & 0 & 0 & 0 \\ 2 & 5 & 2 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 & 0 \\ 3 & 0 & 3 & 5 & 0 & 0 \\ 0 & 2 & 0 & 4 & 5 & 0 \\ 1 & 0 & 1 & 0 & 1 & 5 \end{bmatrix}.$$

3. (♠ Znajdowanie postaci Jordana – zadania z parametrem)

Wyznacz macierz w postaci Jordana podobną do macierzy X_s o wyrazach rzeczywistych, w zależności od parametru s , gdzie X_s równa jest jednej z poniższych macierzy

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 1 \\ -1 & 0 & s & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}, \quad \begin{bmatrix} 1 & -1 & -2 & s \\ 0 & 0 & -2 & 3 \\ 0 & 1 & 1 & -1 \\ 0 & 0 & -1 & 2 \end{bmatrix}, \quad \begin{bmatrix} -2 & -2 & 0 & 0 \\ s & s & 0 & 0 \\ 0 & 0 & -4 & 4 \\ 0 & 0 & -s & s \end{bmatrix}.$$

4. Endomorfizm $\phi: \mathbb{R}^4 \rightarrow \mathbb{R}^4$ dany jest następującym wzorem

$$\phi((x_1, x_2, x_3, x_4)) = (3x_1, x_1 + 3x_2 - x_4, -3x_1 + 3x_3 + 3x_4, 2x_1 + x_2 + x_4).$$

Dla jakich $s \in \mathbb{R}$ istnieje baza \mathcal{A} przestrzeni \mathbb{R}^4 , że $M(\phi)_{\mathcal{A}}^{\mathcal{A}} = B_s$, gdzie

$$B_s = \begin{bmatrix} 2 & 1 & 1 & 2 \\ 0 & 3 & 0 & 1 \\ 0 & 0 & 3 & s \\ 0 & 0 & 0 & 2 \end{bmatrix} \in M_4(\mathbb{R})?$$

5. Pewna macierz $A \in M_7(\mathbb{C})$ spełnia równanie $(A - I)^3 = 0$. Wiadomo też, że $r(A - I)^2 = 2$. Wykaż, że jedyną wartością własną macierzy A jest 1. Opisz postać Jordana macierzy A .
6. Wielomian charakterystyczny endomorfizmu ϕ równy jest $(1 - \lambda)^{10}$, przy czym $\dim \ker(\phi - \text{id}) = 5$, $\dim \ker(\phi - \text{id})^2 = 8$ oraz $\dim \ker(\phi - \text{id})^3 = 9$. Podaj macierz endomorfizmu ϕ w bazie Jordana.
7. Endomorfizm ϕ skończenie wymiarowej przestrzeni liniowej V spełnia warunek $\phi^4 = \phi^3$. Pokaż, że macierz ϕ w bazie Jordana zawiera tylko klatki rozmiaru ≤ 3 .
8. Macierz $A \in M_n(\mathbb{C})$ spełnia równanie $A^2 = I$. Pokaż, że jest to macierz diagonalizowalna. Jakie wartości własne może mieć ta macierz?
9. Udowodnij, że każda macierz $M \in M_n(\mathbb{C})$ jest podobna do transponowanej do niej macierzy M^T .
10. Niech V będzie przestrzenią liniową wymiaru n nad ciałem \mathbb{C} oraz niech $\phi \in \text{End}(V)$. Wykaż, że następujące warunki są równoważne:
- endomorfizm ϕ jest diagonalizowalny nad ciałem \mathbb{C} ,
 - dla każdego $a \in \mathbb{C}$ mamy $\ker(\phi - a \cdot \text{id})^2 = \ker(\phi - a \cdot \text{id})$,
 - dla każdego $a \in \mathbb{C}$ mamy $\text{im}(\phi - a \cdot \text{id}) \cap \ker(\phi - a \cdot \text{id}) = 0$.

4.2 Endomorfizmy triangularyzowalne

Klasa endomorfizmów diagonalizowalnych obejmuje wiele sytuacji istotnych z punktu widzenia zastosowań algebry liniowej. Chcąc jednak zrozumieć jak działają dowolne endomorfizmy, a w szczególności jak wyglądają klasy podobieństwa macierzy kwadratowych, musimy wrócić do „powodów”, dla których endomorfizm ϕ przestrzeni n -wymiarowej V nad ciałem K może nie być diagonalizowalny. Oto one.

- Wielomian charakterystyczny $w_\phi(\lambda)$ może mieć mniej niż n pierwiastków w ciele K . Skoro łączna liczba tych pierwiastków (licząc krotności) jest nie mniejsza niż suma krotności geometrycznych wartości własnych, to suma tych ostatnich nie może być równa n , czego wymaga kryterium diagonalizowalności. Krótko mówiąc — powodem jest sam wielomian charakterystyczny.
- Wielomian $w_\phi(\lambda)$ ma n pierwiastków, ale mimo wszystko suma krotności geometrycznych wartości własnych ϕ jest mniejsza niż n . Innymi słowy — powodem są wymiary podprzestrzeni własnych.

Możemy próbować „usunąć” pierwszą przeszkodę i zakładać, że wielomiany charakterystyczne rozważanych endomorfizmów mają dokładnie tyle pierwiastków, ile wynosi ich stopień. W takim przypadku $w_\phi(\lambda)$ rozkłada się na czynniki liniowe. Punktem wyjścia naszych rozważań jest następujące twierdzenie.

Twierdzenie 4.3

Niech V będzie skończenie wymiarową przestrzenią liniową nad ciałem K oraz niech $\phi \in \text{End}(V)$. Następujące warunki są równoważne:

- (1) wielomian $w_\phi(\lambda)$ rozkłada się na czynniki stopnia nie większego niż 1 (liniowe),
- (2) istnieje baza \mathcal{A} , w której macierz $M(\phi)_{\mathcal{A}}^{\mathcal{A}}$ jest górnotrójkątna.

Dowód. Dowiedzimy (1) \Rightarrow (2) przez indukcję ze względu na $\dim(V)$. Dla $\dim(V) = 1$ teza jest oczywista, bowiem wtedy $\deg w_\phi(\lambda) = 1$. Jak wygląda zatem krok indukcyjny? Z faktu, że $w_\phi(\lambda)$ rozkłada się na czynniki liniowe wynika, że co najmniej jeden z tych czynników jest stopnia 1, a więc zgodnie z twierdzeniem Bezout wielomian ten ma pierwiastek c . W szczególności, endomorfizm ϕ ma wektor własny $\alpha \neq 0$ o wartości własnej c .

Dopełnijmy wektor α do dowolnej bazy \mathcal{A} przestrzeni V wektorami $(\beta_1, \dots, \beta_{n-1})$. Wówczas w bazie \mathcal{A} macierz $M(\phi)_{\mathcal{A}}^{\mathcal{A}}$ ma postać:

$$M(\phi)_{\mathcal{A}}^{\mathcal{A}} = \begin{bmatrix} c & A \\ 0 & B \end{bmatrix},$$

gdzie $A \in M_{1 \times (n-1)}(K)$ oraz $B \in M_{n-1}(K)$. Innymi słowy — pierwsza kolumna macierzy $M(\phi)_{\mathcal{A}}^{\mathcal{A}}$ ma, poza elementem c na przekątnej, same zerowe wyrazy.

Niech $B = M(\psi)_{st}^{st}$, dla pewnego endomorfizmu ψ przestrzeni $n-1$ wymiarowej $V' = \text{lin}(\beta_1, \dots, \beta_{n-1})$. Z rozwinięcia Laplace’a względem pierwszej kolumny wynika natychmiast, że

$$w_\phi(\lambda) = \det \begin{bmatrix} c - \lambda & A \\ 0 & B - \lambda I \end{bmatrix} = (c - \lambda) \cdot w_\psi(\lambda).$$

Skoro założyliśmy, że $w_\phi(\lambda)$ rozkłada się na czynniki liniowe, a $w_\psi(\lambda)$ jest dzielnikiem $w_\phi(\lambda)$, to on też³ $w_\psi(\lambda)$ rozkłada się na czynniki liniowe. Z założenia indukcyjnego istnieje zatem baza \mathcal{B} przestrzeni V' (wymiaru $n-1$), że endomorfizm ψ ma w niej macierz górnotrójkątną B' . W języku macierzy oznacza to, że istnieje macierz odwracalna S rozmiaru $n-1$ taka, że $B' = S^{-1}BS$. Rozważmy macierz S' rozmiarów $n \times n$ postaci

$$\begin{bmatrix} 1 & 0 \\ 0 & S \end{bmatrix},$$

gdzie w pierwszym wierszu i w pierwszej kolumnie poza przekątną stoją zera. Jest jasne, że:

$$S'^{-1} \cdot M(\phi)_{\mathcal{A}}^{\mathcal{A}} \cdot S' = \begin{bmatrix} 1 & 0 \\ 0 & S^{-1} \end{bmatrix} \cdot \begin{bmatrix} c & A \\ 0 & B \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & S \end{bmatrix} = \begin{bmatrix} c & A \\ 0 & S^{-1}B \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & S \end{bmatrix} = \begin{bmatrix} c & AS \\ 0 & B' \end{bmatrix}.$$

³Tu znowu korzystamy z faktu, że jeśli wielomian o współczynnikach w ciele rozkłada się na czynniki stopnia 1, to rozkład ten jest jednoznaczny z dokładnością do stałej i kolejności czynników.

Stąd macierz $M(\phi)_A^A$ jest podobna do macierzy górnotrójkątnej, co jest równoważne z istnieniem bazy, w której ϕ ma macierz górnotrójkątną.

Implikacja (2) \Rightarrow (1). Zauważmy, że jeśli $A = [a_{ij}]$ jest górnotrójkątna, to jej wielomian charakterystyczny jest (jako wyznacznik macierzy górnotrójkątnej $A - \lambda I$) postaci $(a_{11} - \lambda)(a_{22} - \lambda) \dots (a_{nn} - \lambda)$. \square

Definicja 4.4: Endomorfizm triangularyzowalny

Powiemy, że endomorfizm ϕ przestrzeni skończenie wymiarowej V nad ciałem K jest TRIANGULARYZOWALNY, jeśli w pewnej bazie tej przestrzeni ma on macierz górnotrójkątną.

Oczywiście każdy endomorfizm diagonalizowalny jest triangularyzowalny. Co więcej, kryterium triangularyzowalności jest znacznie słabsze niż diagonalizowalności. Wymaga ono jedynie, żeby wielomian charakterystyczny endomorfizmu rozkładał się na czynniki stopnia nie większego niż 1. W ten sposób uzyskujemy ważny wniosek dla przestrzeni liniowych nad poznaną na początku semestru klasą ciał.

Wniosek 4.2

Każdy endomorfizm skończenie wymiarowej przestrzeni liniowej V nad ciałem algebraicznie domkniętym K jest triangularyzowalny.

Powyższy rezultat prowadzi, na mocy Zasadniczego Twierdzenia Algebry, do ważnego wniosku.

Wniosek 4.3

Każda macierz $A \in M_n(\mathbb{C})$ jest podobna do macierzy górnotrójkątnej. W szczególności każdy endomorfizm skończenie wymiarowej przestrzeni zespolonej jest triangularyzowalny.

Jeśli ciało K nie jest algebraicznie domknięte – powyższy ten nie jest prawdą, czego przykładem jest standardowo obrót dwuwymiarowej przestrzeni rzeczywistej o 90 stopni. Co więcej, macierze rzeczywiste nie muszą być triangularyzowalne, jeśli ich wielomiany charakterystyczne nie rozkładają się na czynniki, jak w przypadku wielomianu charakterystycznego macierzy:

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

Z jednej strony rezultat powyższy jest zadowalający, bowiem wreszcie mamy sensowne ograniczenie tego, co w sposób geometryczny robi działanie dowolnego endomorfizmu przynajmniej w pewnych przestrzeniach skończenie wymiarowych. Ten geometryczny opis poznamy na wykładzie szóstym mówiąc o podprzestrzeni niezmienniczej. Z drugiej strony, rezultat wyżej nie jest zadowalający, ponieważ nie potrafimy tak łatwo jak w przypadku dwóch macierzy diagonalnych powiedzieć kiedy dwie macierze górnotrójkątne są podobne. W przypadku macierzy diagonalnych – wystarczy sprawdzić czy na diagonalu stoją, z dokładnością do kolejności, te same wyrazy. W przypadku macierzy górnotrójkątnych swoboda jest znacznie większa, a niezmienniki – bardzo subtelne. Stąd widać, że twierdzenie Jordana jest subtelnym wynikiem.

Na koniec warto zwrócić uwagę na związki pomiędzy reprezentacją endomorfizmu w postaci macierzy górnotrójkątnej oraz pojęciem przestrzeni ilorazowej. Poniżej proponuję alternatywny dowód Twierdzenia 4.3 uwzględniający właśnie proste konstrukcje omawiane w dodatkach do notatek w pierwszym semestrze.

ALTERNATYWNY DOWÓD TWIERDZENIA 4.3. Rozumujemy przez indukcję ze względu na n . Przypadek $n = 1$ jest oczywisty. Niech $n > 1$ i niech $\lambda_1, \dots, \lambda_n$ będą wartościami własnymi endomorfizmu ϕ (niekoniecznie różnymi). Wybierzmy wektor własny v_1 odpowiadający wartości własnej λ_1 i niech $U = \text{lin}(v_1)$. Rozważamy przekształcenie liniowe $\bar{\phi} : V/U \rightarrow V/U$ indukowane przez ϕ i zadane wzorem $\bar{\phi}(v + U) = \phi(v) + U$. Nietrudno widzieć, że wartościami własnymi tego przekształcenia są $\lambda_2, \dots, \lambda_n$. Z założenia indukcyjnego zatem możemy znaleźć bazę $\mathcal{B} = (v_2 + U, \dots, v_n + U)$ przestrzeni V/U taką, że $\bar{\phi}$ ma w tej bazie macierz górnotrójkątną. To jednak znaczy, z definicji macierzy przekształcenia liniowego, że dla $i \geq 2$ mamy $\bar{\phi}(v_i + U) = \phi(v_i) + U \subseteq \text{lin}(v_2 + U, \dots, v_i + U)$. Rozważając teraz bazę $\mathcal{A} = (v_1, v_2, \dots, v_n)$ widzimy zatem, że dla $i \geq 1$ mamy $\phi(v_i) \in \text{lin}(v_1, \dots, v_i)$, czyli macierz $M(\phi)_A^A$ jest górnotrójkątna.

4.3 Dodatek. Podobieństwo nad ciałami nieskończonymi

Ten materiał poświęcimy krótkiej informacji na temat badania podobieństwa macierzy, które nie są triangularyzowalne, a więc nie są podobne do żadnej macierzy górnotrójkątnej (i co za tym idzie nie są podobne do macierzy w postaci Jordana). Chciałbym w nim podkreślić dwa aspekty sprawy, a więc dwa podejścia do stwierdzania czy macierze są podobne.

Jedno podejście mówi, że można próbować określać inne typy „postaci kanonicznych”, do których można by próbować sprowadzać dowolną macierz, niekoniecznie triangularyzowalną. Postać Jordana jest typem „postaci kanonicznej” dla macierzy triangularyzowalnej – za jej pomocą można po prostu zliczać wszystkie klasy podobieństwa macierzy tego typu. Jest wiele innych form, ogólniejszych – w szczególności niegórnotrójkątnych. Najsłynniejszą jest zapewne postać kanoniczna (normalna) Frobeniusa, inną jest postać kanoniczna Weyra, a jest ich więcej. Czytelnik bez trudu znajdzie odpowiednie wyniki w literaturze.⁴

Warto pokazać przykład takich form kanonicznych dla macierzy nad ciałem liczb rzeczywistych. Zachęcam Czytelnika, by wychodząc od twierdzenia Jordana spróbował udowodnić następujący wynik.

Twierdzenie 4.4: Rzeczywista postać Jordana

Niech $\phi \in \text{End}(\mathbb{R}^n)$. Istnieje taka baza \mathcal{A} przestrzeni \mathbb{R}^n , że macierz $M(\phi)_{\mathcal{A}}^{\mathcal{A}}$ ma postać blokowo-diagonalną, w której bloki są klatkami Jordana lub uogólnionymi rzeczywistymi klatkami Jordana postaci

$$K_n(\alpha, \beta) = \begin{bmatrix} A & I & \cdots & 0 & 0 \\ 0 & A & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & A & I \\ 0 & 0 & \cdots & 0 & A \end{bmatrix} \in M_{2n}(\mathbb{R})$$

(blok A pojawia się $n \geq 1$ razy), zaś

$$A = \begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix}$$

dla pewnych $\alpha \in \mathbb{R}$ oraz $0 \neq \beta \in \mathbb{R}$.

Nietrudno zrozumieć ideę tego twierdzenia. Liczba nierezywista z jest wartością własną wielomianu charakterystycznego $w_\phi(\lambda) \in \mathbb{R}[\lambda]$ endomorfizmu $\phi \in \text{End}(\mathbb{R}^n)$, to \bar{z} też jest pierwiastkiem tego wielomianu. A zatem gdyby traktować macierz A endomorfizmu ϕ jako macierz rozmiaru n nad \mathbb{C} , to oczywiście znaleźlibyśmy takie $C \in M_n(\mathbb{C})$, że $C^{-1}AC$ jest w postaci Jordana. Chodzi jednak o to, by poprawić C do odwracalnej macierzy rzeczywistej. Jak to zrobić?

Drugi wynik, o którym wspomnimy stanowi rozwinięcie idei podanej wyżej. Mówi on coś bardzo zaskakującego. Mianowicie — podobieństwo macierzy nie zależy od ciała, nad którym je rozważamy. Co to znaczy?

Twierdzenie 4.5

Jeśli $K \subseteq L$ są ciałami oraz $A, B \in M_n(K)$, to jeśli A, B są podobne nad L , to są podobne nad K .

Przyjmijmy, że $K = \mathbb{R}$ oraz $L = \mathbb{C}$. Powyższy wynik mówi, że do sprawdzenia czy dwie macierze rzeczywiste są podobne nad \mathbb{R} nie potrzeba znajdowania ich rzeczywistych postaci Jordana i porównywania ich, ale wystarczy sprawdzić czy są one podobne jako macierze zespolone. Jeśli są, to muszą być podobne również nad \mathbb{R} . Podejście to więc zapewni jedynie istnienie macierzy podobieństwa, bez wskazywania jej.

Dowód tego rezultatu jest stosunkowo nietrudny, gdy K jest ciałem nieskończonym. Zachęcam do samodzielnego zastanowienia się nad nim. W przypadku, gdy K jest skończone wymaga osobnej, ciekawej teorii macierzy wielomianowych (znowu odsyłam do moich notatek dla potoku gwiazdkowego).

⁴Można też zajrzeć do mojego wykładu dla potoku gwiazdkowego, gdzie znajdują się opisy tych form i szkice dowodów: https://mimuw.edu.pl/~amecel/20211/gal21/GAL2+_AM_w6.pdf.

4.4 Trivia. Problem Collatza

Przy tak poważnym twierdzeniu jak twierdzenie Jordana nie wypada opowiadać o matematycznych zabawkach, a warto przytoczyć prawdziwy i otwarty od dawna problem badawczy. Będzie on dotyczył następującej prostej funkcji na zbiorze liczb naturalnych.

Definicja 4.5

Definiujemy następującą FUNKCJĘ COLLATZA $f : \mathbb{N} \rightarrow \mathbb{N}$:

$$f(n) = \begin{cases} 3n + 1, & \text{gdy } n \text{ jest nieparzyste,} \\ \frac{n}{2}, & \text{gdy } n \text{ jest parzyste.} \end{cases}$$

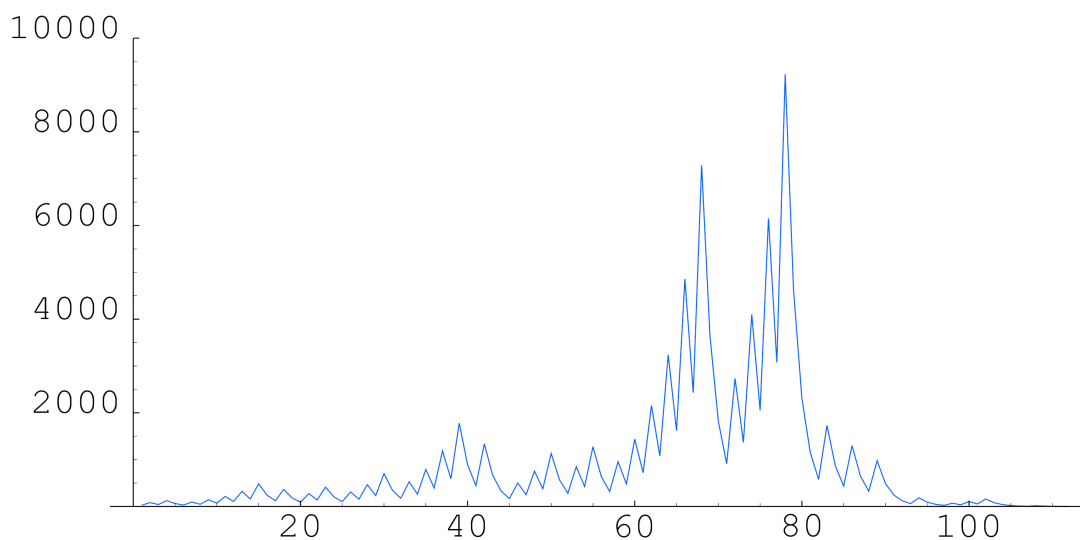
PROBLEM COLLATZA (1937). *Rozstrzygnąć czy dla każdego $k \in \mathbb{N}$ w ciągu $f^n(k)$ znajduje się liczba 1.*

Zagadnienie to było rozważane przez wielu słynnych matematyków, między innymi Ulama i Kakutaniego. Paul Erdős wypowiedział o nim słynne zdanie: „mathematics is not yet ready for such problems”.

Przyjrzyjmy się ciągom $(n, f(n), f^2(n), \dots)$ dla kilku liczb całkowitych:

$$(n, f(n), f^2(n), \dots) = \begin{cases} n = 5 : & (5, 16, 8, 4, 2, 1, 4, 2, 1, \dots) \\ n = 6 : & (6, 3, 10, 5, 16, 8, 4, 2, 1, 4, 2, 1, \dots) \\ n = 7 : & (7, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1, \dots) \\ n = 8 : & (8, 4, 2, 1, 4, 2, 1, \dots) \\ n = 9 : & (9, 28, 14, 7, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1, \dots) \\ n = 10 : & (10, 5, 16, 8, 4, 2, 1, 4, 2, 1, \dots) \end{cases}$$

Jak widzimy, ciągi te w końcu „schodzą” do 1, a potem powtarza się cykl (1, 4, 2). Można by spodziewać się, że ciągi te nie będą osiągały zawrotnych wartości w porównaniu do liczby początkowej.



Przebieg $f^k(27)$. Źródło: Wikipedia.

Tymczasem patrząc na $n = 27$ stwierdzamy, że $f^{36}(n) = 1186$, zaś $f^{77}(n) = 9232$. Okazuje się to jednak być największą wartością tego ciągu, a już $f^{111}(n) = 1$. Zachowanie $f^k(n)$ nie jest łatwo przewidywalne.

Gdy problem jest bardzo trudny matematycy próbują go przetłumaczyć na inny⁵ problem. Równoważnych sformułowań wielki problemów takich jak hipoteza Riemanna są dziesiątki, o ile nie setki. Problem Collatza może nie jest milenijny (choć Erdős oferował 500 dolarów za jego rozwiązanie), ale ma ładne przetłumaczenie na problem algebroliniowy, więc kto wie – może Państwo go rozwiązać?

⁵Zgodnie ze sloganem: jeśli chcesz zobaczyć co jest na szczycie góry wejdź na sąsiednią i popatrz przez lornetkę.

Definicja 4.6

Niech $f : \mathbb{N} \rightarrow \mathbb{N}$ będzie dowolną funkcją. Dla każdego $n \in \mathbb{N}$ określamy macierz^a $A_f(n) \in M_n(\mathbb{C})$ o wyrazach a_{ij} postaci:

$$a_{ij} = \begin{cases} 1, & \text{jeśli } i = f(j), \text{ dla pewnych } i, j \in \{1, \dots, n\}, \\ 0, & \text{w przeciwnym przypadku.} \end{cases}$$

Dla (przyspieszonej) funkcji Collatza macierze $A_f(n)$ oznaczamy jako A_n .

^aInnymi słowy $A_f(n)$ jest macierzą sąsiedztwa grafu skierowanego $\Gamma_f(n)$ o wierzchołkach $1, \dots, n$ oraz o krawędziach $i \rightarrow j$ występujących wtedy i tylko wtedy, gdy $i = f(j)$.

„Przyspieszona” funkcja Collatza opisuje ten sam proces, ale nieco skrócony:

$$f(n) = \begin{cases} \frac{3n+1}{2}, & \text{gdy } n \text{ jest nieparzyste,} \\ \frac{n}{2}, & \text{gdy } n \text{ jest parzyste.} \end{cases}$$

Przyjrzyjmy się jak wygląda macierz A_8 .

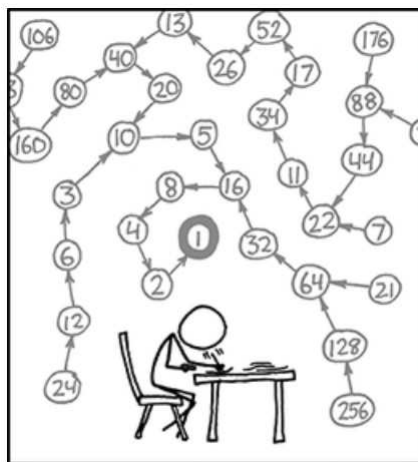
$$A_8 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}.$$

Zauważmy, że dla ustalonego $m \geq 2$ macierz A_m nie zawiera całej informacji o obrazach $f(i)$, dla $1 \leq i \leq m$. Na przykład dla $m = 5$ mamy $f(5) = 8$, a więc piąty wiersz macierzy A_5 jest zerowy. A zatem na przykład nie wiemy czym są $f^i(5)$, bo $3 \rightarrow 5 \rightarrow 8 \rightarrow 4 \rightarrow 2 \rightarrow 1$ oraz $8 > 5$. Tymczasem $f^i(4)$ mogą być całkowicie odczytane z A_5 .

Przeformułowanie problemu Collatza na problem algebry liniowej można znaleźć w pracy studenckiej „*The Jordan Canonical Form for a Class of Zero-One Matrices*” autorstwa Cardona i Tuckfielda⁶. W szczególności w rozwiązaniu problemu bardzo przydałaby się znajomość wielomianu charakterystycznego $w_A(x)$ macierzy A_n . Hipoteza studentów mówi, że jest on równy

$$(-1)^n \cdot x^{n-2} \cdot (x^2 - 1).$$

Może Państwo to pokazać?



⁶https://repository.upenn.edu/cgi/viewcontent.cgi?article=1314&context=oid_papers

Rozdział 5

Wyznaczanie bazy Jordana

Dzisiejszy¹ wykład poświęcimy próbie zrozumienia jak działa endomorfizm zadany przez macierz w postaci Jordana. W ten sposób będziemy w stanie wyznaczać bazy Jordana endomorfizmów.

Twierdzenie 5.1: Twierdzenie Jordana

Niech V będzie przestrzenią skończenie wymiarową nad ciałem K oraz niech $\phi \in \text{End}(V)$. Jeżeli wielomian charakterystyczny endomorfizmu ϕ rozkłada się nad ciałem K na czynniki liniowe to istnieje baza \mathcal{A} przestrzeni V zwana BAZĄ JORDANA, w której macierz ϕ ma postać Jordana.

Zajmiemy się teraz ilustracjami metody wyznaczania bazy Jordana endomorfizmu. Nie podamy ogólnego algorytmu, ale zilustrujemy kilka problemów².

PRZYKŁAD. Niech $\phi \in \text{End}(\mathbb{R}^4)$ zadany będzie w bazie standardowej macierzą

$$A = M(\phi)_{st}^{st} = \begin{bmatrix} 1 & 2 & 1 & 1 \\ 0 & 1 & 3 & 2 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Oczywiście wielomianem charakterystycznym tego endomorfizmu jest $(1 - \lambda)^4$. Skoro rozkłada się on nad \mathbb{R} na iloczyn czynników liniowych, to zgodnie z twierdzeniem Jordana istnieje baza, w której ϕ ma macierz w postaci Jordana. Wyznamy ją przez badanie potęg macierzy $A - I = M(\phi - \text{id})_{st}^{st}$. Mamy:

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

A zatem $r(A) = 3$ i stąd $q_1 = r(A - I)^0 - r(A - I) = 4 - 3 = 1$. A zatem ϕ ma w bazie Jordana \mathcal{J} macierz o jednej klatce rozmiaru ≥ 1 odpowiadającą wartości własnej 1. Skoro suma rozmiarów klatek odpowiadających tej wartości własnej równa jest krotności algebraicznej wartości własnej 1 (a ich liczba równa jest wymiarowi przestrzeni własnej odpowiadającej wartości własnej 1, czyli jej krotności geometrycznej), czyli 4, to owa jedna klatka ma rozmiar 4×4 . W rezultacie:

$$M(\phi)_{\mathcal{J}}^{\mathcal{J}} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Mamy zatem macierz przekształcenia ϕ w bazie Jordana $\mathcal{J} = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ i odczytujemy z niej, że

$$\begin{aligned} \phi(\alpha_1) &= \alpha_1, \\ \phi(\alpha_2) &= \alpha_1 + \alpha_2, \\ \phi(\alpha_3) &= \alpha_2 + \alpha_3, \\ \phi(\alpha_4) &= \alpha_3 + \alpha_4. \end{aligned}$$

¹Ostatnia aktualizacja: 07.05.2023 r.

²Zamiast czytać można również obejrzeć film z czasów pandemicznych: <https://youtu.be/ayIYqL26MNY>.

Wyznamy najpierw wektor własny α_1 , a później napiszemy na podstawie warunków wyżej układ równań, który pozwoli wyznaczyć wektor α_2 i kolejne. Wiemy, że każdy wektor własny x o współrzędnych w bazie standardowej (x_1, x_2, x_3, x_4) spełnia warunek $(\phi - \text{id})(x) = 0$, czyli

$$\begin{bmatrix} 0 & 2 & 1 & 1 \\ 0 & 0 & 3 & 2 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix},$$

czyli $(x_1, x_2, x_3, x_4) \in \text{lin}((1, 0, 0, 0))$. Możemy zatem wybrać $\alpha_1 = (6, 0, 0, 0)$ i przejść do wyznaczenia α_2 o współrzędnych (y_1, y_2, y_3, y_4) z warunku $\phi(\alpha_2) = \alpha_1 + \alpha_2$, czyli $(\phi - \text{id})(\alpha_2) = \alpha_1$. Dostajemy układ:

$$\begin{bmatrix} 0 & 2 & 1 & 1 \\ 0 & 0 & 3 & 2 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} = \begin{bmatrix} 6 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

Przykładowym rozwiązaniem jest wektor $\alpha_2 = (5, 3, 0, 0)$. Analogicznie wyznaczamy α_3 i α_4 rozwiązując kolejno układy:

$$\begin{bmatrix} 0 & 2 & 1 & 1 \\ 0 & 0 & 3 & 2 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{bmatrix} = \begin{bmatrix} 5 \\ 3 \\ 0 \\ 0 \end{bmatrix},$$

co prowadzi do uzyskania np. wektora $\alpha_3 = (1, 2, 1, 0)$ i wreszcie, rozwiązujemy czwarty układ:

$$\begin{bmatrix} 0 & 2 & 1 & 1 \\ 0 & 0 & 3 & 2 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 1 \\ 0 \end{bmatrix},$$

dostajemy przykładowe rozwiązanie $\alpha_4 = (0, 0, 0, 1)$. W prostych sytuacjach przedstawiony algorytm pozwala wyznaczać bazę Jordana (tzn. w sytuacjach, gdy wprowadzisz wartości własnych może być wiele, ale każdej odpowiada jedna klatka). Metoda ta ma jednak wady gdy danej wartości własnej odpowiada więcej klatek. Zaczniemy jednak od omówienia sytuacji, gdy jest więcej wartości własnych.

PRZYKŁAD. Rozważmy macierz

$$X = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 1 \\ -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix} \in M_4(\mathbb{R}).$$

Znaleźć macierz J w postaci Jordana podobną do macierzy X oraz taką macierz odwracalną $C \in M_4(\mathbb{R})$, że $J = C^{-1}XC$.

Wielomian charakterystyczny macierzy X ma postać:

$$w_X(\lambda) = \begin{vmatrix} 1-\lambda & 0 & 0 & 0 \\ 0 & 1-\lambda & -1 & 1 \\ -1 & 0 & 1-\lambda & 0 \\ 0 & 0 & 0 & 2-\lambda \end{vmatrix} = (1-\lambda)^3(2-\lambda).$$

Endomorfizm $\phi \in \text{End}(\mathbb{R}^4)$ dany w bazie standardowej macierzą X ma zatem wartości własne 1, 2. Mamy

$$r(X - I) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = 3.$$

Macierz X można zatem sprowadzić do macierzy w postaci Jordana o jednej klatce rozmiaru 3×3 odpowiadającej wartości własnej 1 oraz o jednej klatce rozmiaru 1×1 odpowiadającej wartości własnej 2.

Endomorfizm ϕ ma wartości własne 1, 2 i zgodnie z rachunkami wyżej wiemy, że ϕ ma w pewnej bazie $\mathcal{J} = \{\beta_1, \beta_2, \beta_3, \beta_4\}$ macierz:

$$M(\phi)_{\mathcal{J}} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}.$$

Widzimy, że $(0, 1, 0, 0)$ jest wektorem własnym ϕ o wartości własnej 1 i możemy przyjąć $\beta_1 = (0, 1, 0, 0)$. Aby wyznaczyć β_2 rozwiązujemy układ:

$$(X - I) \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix},$$

Mamy zatem $\beta_2 = (0, 0, -1, 0)$. Dalej rozwiązujemy równanie $(X - I)\beta_3 = \beta_2$, uzyskując na przykład $\beta_3 = (1, 0, 0, 0)$. Następnie znajdujemy wektor własny o wartości własnej 2, na przykład $\beta_4 = (0, 1, 0, 1)$.

Przejdźmy do przykładu, gdy zaprezentowana metoda może nie zadziałać.

PRZYKŁAD. Weźmy endomorfizm $\psi : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ dany w bazie standardowej macierzą

$$A = M(\psi)_{st}^{st} = \begin{bmatrix} 4 & -1 & 0 \\ 4 & 0 & 0 \\ 8 & -4 & 2 \end{bmatrix}.$$

Mam nadzieję, że uwierzycie mi Państwo, że $w_\psi(\lambda) = (2 - \lambda)^3$ oraz, że $r(A - 2I) = 1$, a zatem macierz ψ w bazie Jordana ma 2 bloki rozmiaru ≥ 1 , czyli w pewnej bazie $\mathcal{J} = (\alpha_1, \alpha_2, \alpha_3)$ mamy:

$$M(\psi)_{\mathcal{J}} = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}.$$

Jak teraz wyznaczą Państwo α_1 ? Sprawdzamy, że

$$V_{(2)} = \text{lin}((1, 2, 0), (0, 0, 1)).$$

Czy można przyjąć za α_1 dowolny wektor własny, choćby $(1, 2, 0)$? Wówczas koniecznie $\psi(\alpha_2) = \alpha_1 + 2\alpha_2$, czyli

$$(\psi - 2 \text{id})(\alpha_2) = \alpha_1.$$

Jeśli $\alpha_2 = (x_1, x_2, x_3)$, to mamy:

$$\begin{bmatrix} 2 & -1 & 0 \\ 4 & -2 & 0 \\ 8 & -4 & 0 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}.$$

Nietrudno sprawdzić, że układ ten nie ma rozwiązania! A zatem wybór wektora własnego $(1, 2, 0)$ był nieprawidłowy. Wektor α_1 powinien być innym elementem $V_{(2)}$. Jakim? Wyznamy najpierw α_2 , bowiem $(\psi - 2 \text{id})(\alpha_2) = \alpha_1$. Skoro tak, to

$$(\psi - 2 \text{id})^2(\alpha_2) = (\psi - 2 \text{id})(\alpha_1) = 0.$$

A zatem $\alpha_2 \in \ker(\psi - 2 \text{id})^2 \setminus \ker(\psi - 2 \text{id})$. Jednak $\ker(\psi - 2 \text{id})^2 = \mathbb{R}^3$, bo

$$M((\psi - 2 \text{id})^2)_{st}^{st} = \begin{bmatrix} 2 & -1 & 0 \\ 4 & -2 & 0 \\ 8 & -4 & 0 \end{bmatrix} \cdot \begin{bmatrix} 2 & -1 & 0 \\ 4 & -2 & 0 \\ 8 & -4 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

A zatem α_2 może być wybrany jako dowolny niezerowy wektor nie-własny. Na przykład $\alpha_2 = (0, 1, 0)$. Wówczas mamy: $\alpha_1 = (\psi - 2 \text{id})(\alpha_2)$, czyli $\alpha_1 = (-1, -2, -4)$. Teraz możemy DOBRAĆ do wektora α_1 wektor własny α_3 . Wybór α_3 zależy więc od wyboru wektora nie-własnego α_2 , a nie tylko od liniowej niezależności z α_1 . Czy widzicie Państwo jak wyglądałaby sytuacja, gdyby było to przekształcenie $\mathbb{R}^4 \rightarrow \mathbb{R}^4$ i jego postać Jordana miałaby dwie klatki 2×2 odpowiadające tej samej wartości własnej?

Spróbujmy nieco wyjaśnić o co chodzi z „dobieraniem” wektorów, które zaprezentowaliśmy powyżej. Niech V będzie przestrzenią wymiaru n oraz niech $\phi \in \text{End}(V)$. Niech $\mathcal{J} = (\beta_1, \dots, \beta_n)$ oraz

$$M(\phi)_{\mathcal{J}} = \begin{bmatrix} a & 1 & 0 & \dots & 0 & 0 \\ 0 & a & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & a & 1 \\ 0 & 0 & 0 & \dots & 0 & a \end{bmatrix},$$

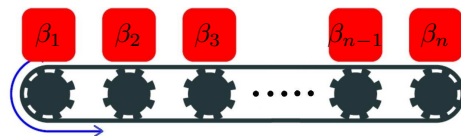
Wynika stąd, że mamy:

$$\begin{aligned} \phi(\beta_1) &= a \cdot \beta_1 \\ \phi(\beta_2) &= \beta_1 + a \cdot \beta_2 \\ \phi(\beta_3) &= \beta_2 + a \cdot \beta_3 \\ &\vdots \\ \phi(\beta_n) &= \beta_{n-1} + a \cdot \beta_n. \end{aligned}$$

Rozważając odwzorowanie $\phi - a \cdot \text{id}$ mamy:

$$\begin{aligned} (\phi - a \cdot \text{id})(\beta_1) &= 0 \\ (\phi - a \cdot \text{id})(\beta_2) &= \beta_1 \\ (\phi - a \cdot \text{id})(\beta_3) &= \beta_2 \\ &\vdots \\ (\phi - a \cdot \text{id})(\beta_n) &= \beta_{n-1}. \end{aligned}$$

Widzimy zatem, że przy kolejnych działaniach $\phi - a \text{id}$ wszystkie wektory β_1, \dots, β_n ustawiają się (w odwrotnej kolejności) w łańcuch, w którym każdy następny (poza pierwszym, czyli β_n) jest obrazem poprzedniego, a ostatni (czyli β_1) zamienia się w zero: $\beta_n \mapsto \beta_{n-1} \mapsto \beta_{n-2} \mapsto \dots \mapsto \beta_2 \mapsto \beta_1 \mapsto 0$. Widzimy zatem, że działanie endomorfizmu $\phi - a \cdot \text{id}$ można przedstawić za pomocą grafiki:



Ta grafika ilustruje nam, że kolejne iteracje $\phi - a \text{id}$ mają w jądrach kolejne wektory β_i :

$$(\phi - a \text{id})^n(\beta_n) = 0, \quad (\phi - a \text{id})^{n-1}(\beta_{n-1}) = 0, \quad (\phi - a \text{id})^{n-2}(\beta_{n-2}) = 0, \quad \dots \quad (\phi - a \text{id})(\beta_1) = 0.$$

Wiedząc jednocześnie, że $(\phi - a \text{id})(\beta_i) = \beta_{i-1}$, dla $i > 1$ mamy:

$$\begin{aligned} \beta_n &\in \ker(\phi - a \text{id})^n \setminus \ker(\phi - a \text{id})^{n-1}, \\ \beta_{n-1} &\in \ker(\phi - a \text{id})^{n-1} \setminus \ker(\phi - a \text{id})^{n-2}, \\ \beta_{n-2} &\in \ker(\phi - a \text{id})^{n-2} \setminus \ker(\phi - a \text{id})^{n-3}, \\ &\vdots \\ \beta_2 &\in \ker(\phi - a \text{id})^2 \setminus \ker(\phi - a \text{id}), \\ \beta_1 &\in \ker(\phi - a \text{id}). \end{aligned}$$

Najważniejsze jest jednak to, że znając β_n wyznaczamy jednoznacznie pozostałe β_i , które są obrazami β_n przy kolejnych iteracjach $(\phi - a \text{id})$. Jak to stosować w praktyce? Wróćmy do pierwszego przykładu, czyli endomorfizmu danego w bazie Jordana macierzą o jednej klatce 4×4 :

$$M(\phi)_{\mathcal{J}} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Widzimy zatem, że tym razem wektory bazy Jordana endomorfizmu ϕ układają się w trzy łańcuchy, odpowiadające wynikom działań endomorfizmu $\phi - a \cdot \text{id}$:

$$\beta_5 \mapsto \beta_4 \mapsto \beta_3 \mapsto \beta_2 \mapsto \beta_1 \mapsto 0, \quad \beta_9 \mapsto \beta_8 \mapsto \beta_7 \mapsto \beta_6 \mapsto 0, \quad \beta_{11} \mapsto \beta_{10} \mapsto 0.$$

Gdyby naszym zadaniem było znalezienie bazy Jordana, moglibyśmy to zrobić poprzez staranne wybieranie wektorów z baz jąder odpowiednio wysokich iteracji endomorfizmu $\phi - a \text{id}$. W rozważanym przypadku wybralibyśmy najpierw dowolny wektor β_5 z różnicy zbiorów $\ker(\phi - a \text{id})^5 \setminus \ker(\phi - a \text{id})^4$. Następnie wyznaczylibyśmy wektory $\beta_4, \beta_3, \beta_2, \beta_1$ jak wyżej, rozwiązując warunek $(\phi - a \text{id})(\beta_i) = \beta_{i-1}$.

Skąd wzięlibyśmy β_9 ? Otóż jest to wektor z $(\phi - a \text{id})^4 \setminus \ker(\phi - a \text{id})^3$ i to liniowo niezależny z już znalezionym wektorem β_3 , który jest w tym samym zbiorze. Gdy taki wektor wybierzemy, wyznaczamy β_8, β_7 i β_6 .

Wreszcie, wektor β_{11} wybieramy z $\ker(\phi - a \text{id})^2 \setminus \ker(\phi - a \text{id})$ tak, by układ $\{\beta_2, \beta_7, \beta_{10}\}$ był liniowo niezależny (β_2 dobieramy więc do β_7 i β_{10}), bo te wszystkie wektory są w tej różnicy. W ten sposób wyznaczymy β_{11} . Wydać, że rachunki są w takim przypadku niezwykle żmudne.

* * *

Wreszcie, należy przyrzeć się ogólnej sytuacji, gdy endomorfizm ϕ ma (parami różne) wartości własne $\lambda_1, \lambda_2, \dots, \lambda_s$ o krotnościach algebraicznych t_1, t_2, \dots, t_s i krotnościach geometrycznych r_1, r_2, \dots, r_s .

Oto przykładowa sytuacja, gdy $\lambda_1 = 1, \lambda_2 = 3$, zaś $t_1 = 8, t_2 = 6, t_3 = 2$ oraz $r_1 = 3, r_2 = 2, r_3 = 1$. Weźmy $A \in M_{16}(\mathbb{R})$ postaci:

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

Jeśli przyjmiemy, że jest to macierz endomorfizmu $\phi \in \mathbb{R}^{16}$ w bazie Jordana $(\beta_1, \dots, \beta_{16})$, to dla każdej wartości własnej rozważyć można diagramy opisujące działania odpowiednich endomorfizmów:

- endomorfizm $\phi - 1 \cdot \text{id}$ ograniczony do przestrzeni rozpiętej na $\{\beta_1, \dots, \beta_8\}$ przekształca te wektory zgodnie ze schematem $\beta_4 \mapsto \beta_3 \mapsto \beta_2 \mapsto \beta_1 \mapsto 0, \quad \beta_7 \mapsto \beta_6 \mapsto \beta_5 \mapsto 0, \quad \beta_8 \mapsto 0$.
- endomorfizm $\phi - 3 \cdot \text{id}$ ograniczony do przestrzeni rozpiętej na $\{\beta_9, \dots, \beta_{14}\}$ przeprowadza te wektory zgodnie ze schematem $\beta_{11} \mapsto \beta_{10} \mapsto \beta_9 \mapsto 0, \quad \beta_{14} \mapsto \beta_{13} \mapsto \beta_{12} \mapsto 0$
- endomorfizm $\phi - 2 \cdot \text{id}$ ograniczony do przestrzeni rozpiętej na $\{\beta_{15}, \beta_{16}\}$ przeprowadza te wektory zgodnie ze schematem $\beta_{16} \mapsto \beta_{15} \mapsto 0$.

Dla każdej z powyższych wartości własnych wykonać byśmy musieli serię operacji opisanych wyżej dla pojedynczych wartości. Dla wartości własnej 1 wyznaczalibyśmy trzy łańcuchy wektorów, dla wartości własnej 3: dwa łańcuchy i dla wartości własnej 2: jeden łańcuch. Procedurę taką należałoby już oczywiście wykonać za pomocą narzędzi komputerowych.

Nie jest naszym celem uczenie Państwa ogólnych algorytmów wyznaczania bazy Jordana, choć są one opisane i można je wywnioskować na podstawie powyższych przykładów. Na ćwiczeniach i kolokwiach obowiązują przykłady o stopniu trudności występującym w skrypcie dra Koźniewskiego i na kolokwiach.

5.1 Zadania do samodzielnej pracy

Zadania ilustrujące umiejętności niezbędne do zaliczenia przedmiotu oznaczone są symbolem ♠. Przy tych zadaniach dodany jest opis umiejętności, które sprawdzają.

1. (♠ Wyznaczanie bazy Jordana)

- Wyznacz bazę Jordana dla endomorfizmu $\phi : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ o wielomianie charakterystycznym $w_\phi(\lambda) = -(1 + \lambda)^3$, danego wzorem $\phi((x_1, x_2, x_3)) = (x_2, -x_1 - x_2 + x_3, x_1 - 2x_3)$.
- Wyznacz bazę \mathcal{J} przestrzeni \mathbb{R}^3 , w której macierz $M(\phi)_{\mathcal{J}}$ endomorfizmu $\phi : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ danego wzorem $\phi(x_1, x_2, x_3) = (-3x_1 - 2x_2, 2x_1 + x_2, 3x_1 + 3x_2 - x_3)$ ma postać Jordana.
- Niech $A \in M_3(\mathbb{R})$ będzie macierzą postaci:

$$A = \begin{bmatrix} -6 & 6 & 6 \\ 0 & 2 & 0 \\ -8 & 8 & 8 \end{bmatrix}.$$

Znajdź taką macierz C , że macierz $C^{-1}AC$ jest w postaci Jordana.

- Znajdź bazę Jordana endomorfizmu $\phi \in \text{End}(\mathbb{R}^4)$ danego w bazie standardowej macierzą:

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

- Znajdź bazę Jordana endomorfizmu $\phi \in \text{End}(\mathbb{R}^5)$ danego w bazie standardowej macierzą:

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

2. Dla każdej z poniższych macierzy A_i o wyrazach z \mathbb{R} oblicz $(A_i)^{123}$, korzystając przy tym z zależności $A^n = C^{-1}J^nC$, gdzie J jest macierzą w postaci Jordana.

$$A_1 = \begin{bmatrix} 0 & -1 \\ 4 & 4 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \quad A_3 = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$

3. Ciąg (a_n) dany jest rekurencją $a_1 = 1, a_2 = 5$ oraz $a_n = 4a_{n-1} - 4a_{n-2}$, dla $n \geq 3$.

- Znajdź macierz $A \in M_2(\mathbb{R})$, dla której

$$A \cdot \begin{bmatrix} a_{n-1} \\ a_n \end{bmatrix} = \begin{bmatrix} a_n \\ a_{n+1} \end{bmatrix}.$$

- Wyznacz A^n oraz wzór ogólny na n -ty wyraz ciągu (a_n) .

4. Poniższe zadanie dotyczy problemu wyznaczania pierwiastków z macierzy w łatwych sytuacjach.

- Dla $a \in \mathbb{C}$ rozważamy macierz

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

Dla jakich $a \in \mathbb{C}$ istnieją macierze $B \in M_2(\mathbb{C})$ takie, że $B^2 = J$? Wypisz te macierze.

- Znajdź macierz J w postaci Jordana podobną do macierzy

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

oraz macierz odwracalną C , taką że $C^{-1}JC = M$. Jaki jest związek między macierzami typu \sqrt{A} , a macierzami typu \sqrt{J} ? Wyznacz wszystkie „zespolone” pierwiastki z macierzy A .

5.2 Uzupełnienie. Trudniejsze zadania o postaci i bazie Jordana

Przedstawione na wykładzie przykłady wyznaczania baz Jordana obejmują bardzo podstawowe sytuacje, ilustrując w zasadzie sposób odczytywania macierzy zapisanej w bazie Jordana. Szereg krótszych i dłuższych zadań stawia nam wyzwanie zebrania całej wiedzy dotyczącej endomorfizmów i zastosowania jej w sposób nie zawsze oczywisty. W tym uzupełnieniu prezentujemy przykłady takich zadań, pochodzące zarówno z kolokwium na potoku zwykłym, jak i gwiazdkowym.

Zadanie 5.1. *Pewna macierz $A \in M_{7 \times 7}(\mathbb{C})$ spełnia równanie $(A - I)^3 = 0$. Wiemy też, że $r(A - I)^2 = 2$. Wykaż, że jedyną wartością własną macierzy A jest 1. Opisz postać Jordana macierzy A .*

ROZWIĄZANIE. Niech $Av = \lambda v$, dla pewnego niezerowego wektora v oraz $\lambda \in \mathbb{C}$. Mamy zatem $(A - I)v = (\lambda - 1)v$, czyli $(A - I)^3 v = (\lambda - 1)^3 v$. Ale $(A - I)^3 v = 0v = 0$, a zatem skoro $v \neq 0$ mamy $(\lambda - 1)^3 = 0$, czyli $\lambda = 1$. A zatem A można sprowadzić do postaci Jordana, w której wszystkie klatki odpowiadają wartości własnej 1. Wyznaczamy teraz stałe $q_k = r(A - I)^{k-1} - r(A - I)^k$ opisujące liczby klatek rozmiaru $\geq k$.

Skoro $(A - I)^3 = 0$, to $r(A - I)^3 = 0$. A zatem $q_3 = 2 - 0 = 2$. Oczywiście $q_4 = r(A - I)^3 - r(A - I)^4 = 0 - 0 = 0$. Zatem w postaci Jordana J macierzy A są dwie klatki rozmiaru nie mniejszego niż 3 i zero klatek rozmiaru nie mniejszego niż 4. A zatem J ma dwie klatki rozmiaru 3×3 , i żadnej większej. Skoro A (a więc i J) jest rozmiarów 7×7 , to suma rozmiarów klatek Jordana macierzy J to 7. Postać Jordana macierzy A ma zatem jedną klatkę 1×1 oraz dwie klatki 3×3 , odpowiadające wartości własnej 1. ■

Zadanie 5.2. *Niech $A \in M_{n \times n}(\mathbb{C})$. Pokaż, że jeśli $A^3 = A$, to $r(A) = \text{tr } A^2$.*

ROZWIĄZANIE. Niech J będzie macierzą w postaci Jordana podobną do A . Wiemy, że $r(A) = r(J)$ oraz $\text{tr } A^2 = \text{tr } J^2$. Macierz J jest górnotrójkątna i na jej przekątnej stoją wartości własne macierzy A . Podobnie macierz J^2 jest górnotrójkątna i na jej przekątnej stoją kwadraty wartości własnych macierzy A , czyli wartości własne macierzy A^2 . Twierdzimy, że wartości własne macierzy A wynosić mogą jedynie $-1, 0, 1$. Istotnie, jeśli $Av = \lambda v$, dla pewnego wektora niezerowego v , to $A^3 v = \lambda^3 v$. A zatem równość $A^3 = A$ pociąga za sobą równość $A^3 v = Av$, czyli $(\lambda^3 - \lambda)v = 0$. Skoro $v \neq 0$, to $\lambda^3 - \lambda = 0$, a więc $\lambda \in \{-1, 0, 1\}$. A zatem elementy na przekątnej macierzy J to jedynie $-1, 0$ lub 1 . Stąd elementy na przekątnej J^2 mogą wynosić jedynie $0, 1$. Reszta tezy wynika z faktu, że A jest diagonalizowalna. Jak to pokazać?

Skoro $A^3 = A$, to też $J^3 = J$ (też było na wykładzie). Potęgowanie macierzy Jordana polega zaś na potęgowaniu poszczególnych jej klatek. To oznacza, że wszystkie klatki w J są rozmiarów 1×1 , bo tylko wtedy trzecia potęga klatki może być równa niej samej (nad \mathbb{C}). Zatem liczba niezerowych elementów na przekątnej macierzy J^2 jest jednocześnie rzędem tej macierzy. Skoro te niezerowe elementy muszą wynosić 1, to liczba ta jest też również śladem J^2 . A zatem $r(J^2) = \text{tr}(J^2)$, czyli $r(A^2) = \text{tr}(A^2)$. Skoro J i J^2 są diagonalne, to jest jasne, że $r(A) = r(J) = r(J^2)$. Czyli $r(A) = \text{tr}(A^2)$. ■

Zadanie 5.3. *Macierz $A \in M_{n \times n}(\mathbb{C})$ spełnia równanie $A^2 = I$. Pokaż, że jest to macierz diagonalizowalna. Jakie wartości własne może mieć ta macierz?*

ROZWIĄZANIE. Każdą kwadratową macierz zespoloną można sprowadzić do postaci Jordana. Niech J będzie macierzą w postaci Jordana podobną do A . Wówczas istnieje macierz odwracalna P taka, że $P^{-1}AP = J$. A zatem $J^2 = P^{-1}A^2P = P^{-1}P = I$. Oznacza to, że każda z klatek Jordana macierzy J po podniesieniu do kwadratu jest macierzą identity. Załóżmy, że w J istnieje klatka rozmiaru co najmniej 2×2 odpowiadająca wartości własnej a . Wówczas:

$$\begin{bmatrix} a & 1 & 0 & \dots & 0 \\ 0 & a & 1 & \dots & 0 \\ 0 & 0 & a & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & a \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix}.$$

A zatem dostajemy warunki: $a^2 = 1$ oraz $2a = 0$, co oznacza, że powyższe równanie macierzowe jest sprzeczne. Wszystkie klatki Jordana J są zatem rozmiaru 1×1 , a zatem A jest diagonalizowalna. Oczywiście jeśli $a \in \mathbb{C}$ jest wartością własną A , to a^2 jest wartością własną I , a zatem $a^2 = 1$. Równanie to ma w liczbach zespolonych jedynie pierwiastki -1 oraz 1 . To jedyne możliwe wartości własne macierzy A . ■

Zadanie 5.4. Rozważmy endomorfizm ϕ przestrzeni V wymiaru 14 nad ciałem algebraicznie domkniętym, przy czym $\dim \ker \phi = 9$ oraz $\text{im } \phi \subseteq \ker \phi$. Znajdź możliwe postaci Jordana endomorfizmu ψ takiego, że $\phi = \psi^3$.

ROZWIĄZANIE. Warunek $\text{im } \phi \subseteq \ker \phi$ oznacza, że $\phi^2 = 0$. Stąd wszystkie wartości własne ϕ są równe 0. W istocie wielomian charakterystyczny ϕ musi być³ postaci $\lambda^{14} = 0$. Mamy również $\psi^6 = 0$, a zatem również ψ ma wielomian charakterystyczny $\lambda^{14} = 0$. Mamy zatem

$$\dim \ker \psi^3 = 9, \quad \dim \ker \psi^6 = 14.$$

A zatem jeśli B jest macierzą ψ , to

$$r(B^3) = 5, \quad r(B^6) = 0.$$

Oczywiście $r(B^0) = 14$, więc mamy:

$$q_1 + q_2 + q_3 = r(B^0) - r(B) + r(B) - r(B^2) + r(B^2) - r(B^3) = 9, \quad q_4 + q_5 + q_6 = r(B^3) - r(B^6) = 5.$$

Mamy jednak $q_1 \leq q_2 \leq q_3 \leq q_4 \leq q_5 \leq q_6$. Nasza macierz może mieć co najwyżej trzy klatki rozmiaru co najmniej 3. A zatem możliwe trójki (q_4, q_5, q_6) to $(3, 2, 0)$, $(3, 1, 1)$, $(2, 2, 1)$. Uwzględniając pierwszy warunek widzimy, że możliwe konfiguracje klatek Jordana macierzy B są następujące:

- dwie klatki rozmiaru 5×5 oraz jedna klatka rozmiaru 4×4 ,
- jedna klatka rozmiaru 6×6 oraz dwie klatki rozmiaru 4×4 ,
- po jednej klatce rozmiaru 6×6 , 5×5 oraz 3×3 ,
- po jednej klatce rozmiaru 6×6 , 5×5 , 2×2 oraz 1×1 ,
- po jednej klatce rozmiaru 6×6 , 5×5 oraz trzy klatki rozmiaru 1×1 .

■

Zadanie 5.5. Znajdź postać Jordana endomorfizmu $\phi \in \text{End}(\mathbb{C}^{10})$ spełniającego:

$$\begin{cases} \text{tr } \phi = 20 \\ \dim \ker(\phi - 2 \text{id})^2 = 5 \\ \dim \ker(\phi - 2 \text{id})^4 = 8 \\ \det(\phi - 3 \text{id}) = 0. \end{cases}$$

ROZWIĄZANIE. Jeśli A jest macierzą endomorfizmu ϕ , mamy $r(A - 2I)^2 = 5$ oraz $r(A - 2I)^4 = 2$. Zatem

$$q_1 + q_2 = r(I) - r(A - 2I) + r(A - 2I) + r(A - 2I)^2 = 5,$$

skąd możliwe wartości (q_1, q_2) to $(5, 0)$, $(4, 1)$ lub $(3, 2)$. Mamy też:

$$q_3 + q_4 = r(A - 2I)^2 - r(A - 2I)^3 + r(A - 2I)^3 - r(A - 2I)^4 = 3.$$

Oczywiście $q_1 \leq q_2 \leq q_3 \leq q_4$. A zatem musi być $q_3 = 2$ i wtedy $q_4 = 1$. W rezultacie mamy dokładnie jedną klatkę rozmiaru 3 i co najmniej jedną klatkę rozmiaru 4 — czyli dokładnie jedną, bo więcej się nie zmieści. Jedyna konfiguracja, która tu pasuje to oczywiście $q_1 = 3$ oraz $q_2 = 2$. Stąd mamy jedną klatkę o rozmiarze jeden i wiemy, że wielomian charakterystyczny A dzieli się co najmniej przez $(\lambda - 2)^8$.

Endomorfizm ten ma jednak także wartość własną 3. A zatem może mieć jeszcze jedną wartość własną i ma, bowiem ich suma razem z krotnościami równa jest śladowi, czyli liczbie 20. Mamy zatem $20 = 8 \cdot 2 + 3 + x$, czyli $x = 1$ jest ostatnią szukaną wartością własną. A zatem postać Jordana endomorfizmu ϕ ma 5 klatek:

- trzy klatki odpowiadające wartości własnej 2 rozmiarów 4×4 , 3×3 oraz 1×1 ,
- po jednej klatce rozmiaru 1×1 odpowiadającej wartości własnej 1 oraz 3.

■

Ostatnie zadanie dotyczy będzie wyznaczania bazy Jordana oraz potęg macierzy niediagonalizowalnej.

³To jest prawdziwe dla endomorfizmu przestrzeni nad dowolnym ciałem, o czym wspominamy w dodatku.

Zadanie 5.6. Rozważmy endomorfizm ϕ przestrzeni \mathbb{C}^4 dany w bazie standardowej macierzą:

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

Wyznacz macierz ϕ w postaci Jordana. Wyznacz A^{100} .

ROZWIĄZANIE. Macierz A jest blokowo górnotrójkątna i oczywiście jej wielomian charakterystyczny to $(\lambda^2 + 1)^2 = (x - i)^2(x + i)^2$. A zatem ϕ ma wartości własne i oraz $-i$. Mamy też:

$$A - iI = \begin{bmatrix} -i & 1 & 1 & 0 \\ -1 & -i & 0 & 1 \\ 0 & 0 & -i & 1 \\ 0 & 0 & -1 & -i \end{bmatrix}, \quad (A - iI)^2 = \begin{bmatrix} -2 & -2i & -2i & 2 \\ 2i & -2 & -2 & -2i \\ 0 & 0 & -2 & -2i \\ 0 & 0 & 2i & -2 \end{bmatrix},$$

co oznacza, że $r(A - iI) = 3$, $r(A - iI)^2 = 2$. A zatem mamy jedną klatkę Jordana rozmiaru 2 odpowiadającą wartości własnej $-i$. Również wartości własnej i odpowiada klatka rozmiaru 2.

Druga część wymaga użycia postaci Jordana a także wyznaczenia bazy Jordana. Pokażmy jak to zrobić, a potem jak można było tego uniknąć. Jak skorzystać z postaci Jordana J macierzy A ? Zapiszemy $A = C^{-1}JC$, gdzie J jest postacią Jordana A , zaś C^{-1} jest macierzą mającą w kolumnie wektory bazy Jordana. Wtedy $A^{100} = C^{-1}J^{100}C$. Czasami podnoszenie macierzy w postaci Jordana do wysokiej potęgi jest znośne. Są resztką ogólne (dość istotne) wzory, które pozwalają to robić w dowolnej sytuacji.

Trzeba zacząć od wyznaczenia bazy Jordana. W skrócie, mamy:

$$\begin{aligned} \ker(\phi - i \text{id})^2 &= \text{lin}((1, i, 0, 0), (0, 0, 1, i)), & (\phi - i \text{id})(0, 0, 1, i) &= (1, i, 0, 0), \\ \ker(\phi + i \text{id})^2 &= \text{lin}((1, -i, 0, 0), (0, 0, 1, -i)), & (\phi + i \text{id})(0, 0, 1, -i) &= (1, -i, 0, 0). \end{aligned}$$

A zatem po krótkich rachunkach:

$$C^{-1} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ i & 0 & -i & 0 \\ 0 & 1 & 0 & 1 \\ 0 & i & 0 & -i \end{bmatrix}, \quad C = \frac{1}{2} \begin{bmatrix} 1 & -i & 0 & 0 \\ 0 & 0 & 1 & -i \\ 1 & i & 0 & 0 \\ 0 & 0 & 1 & i \end{bmatrix}$$

Teraz podnosimy do potęgi 100 klatki Jordana J_1, J_2 macierzy Jordana J endomorfizmu ϕ , aby dalej skorzystać z zależności:

$$J^{100} = \begin{bmatrix} J_1^{100} & 0 \\ 0 & J_2^{100} \end{bmatrix}.$$

Nietrudno widzieć, że:

$$J_1^n = \begin{bmatrix} i & 1 \\ 0 & i \end{bmatrix}^n = \begin{bmatrix} i^n & i^{n-1}n \\ 0 & i^n \end{bmatrix}, \quad J_2^n = \begin{bmatrix} i & 1 \\ 0 & i \end{bmatrix}^n = \begin{bmatrix} (-i)^n & (-i)^{n-1}n \\ 0 & (-i)^n \end{bmatrix},$$

czyli:

$$A^{100} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ i & 0 & -i & 0 \\ 0 & 1 & 0 & 1 \\ 0 & i & 0 & -i \end{bmatrix} \cdot \begin{bmatrix} 1 & -100i & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 100i \\ 0 & 0 & 0 & 1 \end{bmatrix} \cdot \frac{1}{2} \begin{bmatrix} 1 & -i & 0 & 0 \\ 0 & 0 & 1 & -i \\ 1 & i & 0 & 0 \\ 0 & 0 & 1 & i \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & -100 \\ 0 & 1 & 100 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Czy można inaczej? Zauważmy, że kładąc: $C = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ mamy $A = \begin{bmatrix} C & I \\ 0 & C \end{bmatrix}$ oraz:

$$A^n = \begin{bmatrix} C^n & nC^{n-1} \\ 0 & C^n \end{bmatrix}$$

Macierz C to tymczasem macierz obrotu o $3\pi/2$, czyli jej setna potęga to macierz obrotu o kąt 150π , czyli I . A nawet jeśli nie widzieliśmy tego obrotu, to widać, że $C^2 = -I$. Mamy więc $C^{99} = -C$, czyli:

$$A^{100} = \begin{bmatrix} 1 & 0 & 0 & -100 \\ 0 & 1 & 100 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

■

5.3 Dodatek. Endomorfizmy nilpotentne i ich geometria

Podprzestrzenie pierwiastkowe

Na wykładzie rozważaliśmy endomorfizm $\phi - a \text{id}$ przestrzeni n wymiarowej V w sytuacji, gdy ϕ ma w bazie Jordana $\mathcal{J} = (\beta_{n-1}, \dots, \beta_1)$ jedną klatkę odpowiadającą wartości własnej a postaci:

$$M(\phi)_{\mathcal{J}} = \begin{bmatrix} a & 1 & 0 & \dots & 0 & 0 \\ 0 & a & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & a & 1 \\ 0 & 0 & 0 & \dots & 0 & a \end{bmatrix}.$$

Wynioskowaliśmy stąd, że mamy:

$$(\phi - a \text{id})^n(\beta_n) = 0, \quad (\phi - a \text{id})^{n-1}(\beta_{n-1}) = 0, \quad (\phi - a \text{id})^{n-2}(\beta_{n-2}) = 0, \quad \dots \quad (\phi - a \text{id})(\beta_1) = 0.$$

Oczywiście nietrudno wnioskować stąd także, że dla dowolnego wektora $v \in V$ mamy $(\phi - a \text{id})^n(v) = 0$. Tego typu własność ma kluczowe znaczenie dla zrozumienia działań endomorfizmów.

Definicja 5.1: Endomorfizm nilpotentny

Endomorfizm ϕ skończenie wymiarowej przestrzeni liniowej V nazywamy NILPOTENTNYM, jeśli istnieje liczba całkowita $k > 0$ taka, że

$$\phi^k = 0. \quad (\heartsuit)$$

Najmniejsze k spełniające (\heartsuit) nazywamy STOPNIEM NILPOTENTNOŚCI ϕ . Macierz $A \in M_n(K)$ nazywamy NILPOTENTNĄ STOPNIA k , jeśli $A^k = 0$ oraz $A^{k-1} \neq 0$.

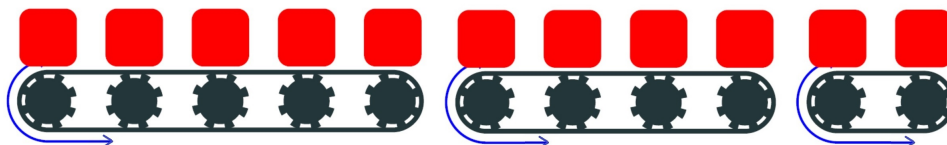
Zauważmy, że dla dowolnego endomorfizmu nilpotentnego stopnia n postaci $\phi \in \text{End}(V)$ istnieje niezerowy wektor $v \in V$ taki, że $\phi^n(v) = 0$ oraz $\phi^{n-1}(v) \neq 0$. Gdyby okazało się, że sama przestrzeń jest wymiaru n , to ciąg wektorów $\phi^{n-1}(v), \phi^{n-2}(v), \dots, \phi(v), v$ staje się bazą przestrzeni V , w której endomorfizm ϕ ma macierz

$$\begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & 0 & \dots & 0 & 0 \end{bmatrix} \in M_n(K). \quad (*)$$

Zauważmy, że nilpotentność może działać w bardziej subtelny sposób. Biorąc endomorfizm nilpotentny stopnia 5 przestrzeni 11-wymiarowej dany w bazie standardowej macierzą

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

widzimy, że w istocie działa on „niezależnie” na podprzestrzeniach $\text{lin}(\epsilon_1, \dots, \epsilon_5)$, $\text{lin}(\epsilon_6, \dots, \epsilon_9)$ oraz $\text{lin}(\epsilon_{10}, \epsilon_{11})$, co można ilustrować za pomocą trzech działających jednocześnie taśmociągów.



Źródło: <http://qirui.li/> – polecam slajdy z bardzo pomysłowymi poglądowymi ilustracjami tematów z algebry liniowej.

Z naszego punktu widzenia macierze czy endomorfizmy nilpotentne można traktować jako endomorfizmy *zupełnie innej natury geometrycznej* niż diagonalizowalne. Endomorfizm nilpotentny zabija (czyli zerem), po dostatecznej liczbie aplikacji, dowolny niezerowy wektor przestrzeni, na której działa. Wartością własną endomorfizmu nilpotentnego jest jedynie 0. Proszę sprawdzić, że endomorfizm diagonalizowalny, który jest jednocześnie nilpotentny musi być zerowy. Nietrudno w istocie pokazać, że wielomian charakterystyczny endomorfizmu nilpotentnego jest postaci $\pm \lambda^n$, co oznacza, że jest to zawsze endomorfizm triangularyzowalny. Jednym z kluczowych punktów dowodu twierdzenia Jordana jest pokazanie, że każda macierz nilpotentna jest podobna do macierzy w postaci Jordana. Innym kluczowym wynikiem teorii endomorfizmów jest twierdzenie o addytywnym rozkładzie Jordana-Chevalleya, które mówi, co następuje.

Twierdzenie 5.2: Twierdzenie Jordana-Chevalleya

Niech V będzie skończenie wymiarową przestrzenią liniową nad K oraz niech $\phi \in \text{End}(V)$ będzie triangularyzowalny. Wówczas istnieje jednoznaczny rozkład

$$\phi = \phi_S + \phi_N, \quad (*)$$

- gdzie ϕ_S jest diagonalizowalny,
- ϕ_N jest nilpotentny,
- oraz $\phi_S \circ \phi_N = \phi_N \circ \phi_S$.

Co więcej ϕ_S, ϕ_N należą do algebry endomorfizmu ϕ (są wielomianami od ϕ).

W twierdzeniu istotna jest przemienność ϕ_S, ϕ_N , inaczej da się znaleźć wiele rozkładów na endomorfizm diagonalizowalny i nilpotentny, np.:

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix},$$

a przecież ϕ zadane macierzą A jest diagonalizowalne.

Niech $D_n(K)$ oraz $N_n(K)$ oznaczają odpowiednio zbiory macierzy diagonalizowalnych nad K oraz nilpotentnych nad K . Żaden z tych zbiorów nie jest podprzestrzenią $M_n(K)$, np:

$$\begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \notin D_2(K) \quad \text{oraz} \quad \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \notin N_2(K).$$

Zagadka: czym są podprzestrzenie $\text{lin}(D_n(K))$ i $\text{lin}(N_n(K))$. Czy to $M_n(K)$?

Opis endomorfizmów nilpotentnych jest w istocie kluczowym punktem w dowodzie twierdzenia Jordana. Wyjaśnieniem tego faktu jest rozważanie tzw. podprzestrzeni pierwiastkowych.

Definicja 5.2: Podprzestrzeń pierwiastkowa

Niech $\phi \in \text{End}(V)$. Dla każdego $a \in K$ przez $V_{[a]}$ oznaczamy podprzestrzeń złożoną ze wszystkich $\alpha \in V$, dla których istnieje n takie, że

$$(\phi - a \text{id})^n(\alpha) = 0.$$

Przestrzeń $V_{[a]}$ nazywamy PODPRZESTRZENIĄ PIERWIASTKOWĄ endomorfizmu ϕ lub UOGÓLNIONĄ PODPRZESTRZENIĄ WŁASNĄ odpowiadającą wartości własnej a .

Przykład. Jeśli $\phi \in \text{End}(\mathbb{C}^4)$ oraz $w_\phi(\lambda) = (\lambda - 1)^2(\lambda - 4)^2$, to w celu opisu przestrzeni $V_{[1]}$ rozważamy endomorfizm $\phi - \text{id}$, który ograniczony do $V_{[1]}$ jest w kwadracie zerowy, czyli $(\phi - \text{id})^2|_{V_{[1]}} = 0$, np. dla $M(\phi)_{st}^{st} = (x_1 + x_2, x_2, 4x_3 + x_4, 4x_4)$ mamy $V_{[1]} = \text{lin}(\epsilon_1, \epsilon_2)$ oraz:

$$M(\phi - \text{id})_{st}^{st} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 3 \end{bmatrix}, \quad M((\phi - \text{id})^2)_{st}^{st} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 9 & 6 \\ 0 & 0 & 0 & 9 \end{bmatrix}.$$

Mówiąc pogłębienie, dla endomorfizmu ϕ przestrzeni V rozważać możemy jego przesunięcia $\phi - a\phi$ i zastanawiać się czy są podprzestrzenie V , na których to przesunięcie działa jak endomorfizm nilpotentny. Okazuje się, co jest niezwykle istotnym wynikiem, że jeśli wielomian charakterystyczny endomorfizmu rozkłada się na czynniki liniowe, to przestrzeń V jest sumą prostą podprzestrzeni pierwiastkowych. Innymi słowy macierz $\phi|_{V[a_i]}$ ma mieć w bazie \mathcal{J}_i wszystkie klatki Jordana odpowiadające wartości własnej a_i w postaci Jordana macierzy całego endomorfizmu ϕ – i tylko te klatki. Oczywiście może być ich wiele. A więc można powiedzieć, że twierdzenie Jordana orzeka, że dla dowolnego endomorfizmu triangularyzowalnego przestrzeni V , możemy napisać, że V jest sumą prostą przestrzeni, które pogrupować można w mniejsze sumy proste stanowiące podprzestrzenie pierwiastkowe odpowiadające wartościom własnym ϕ .

Oto przykład. Niech $\phi \in \text{End}(K^{16})$ ma bazie $\mathcal{B} = (\beta_1, \dots, \beta_{16})$ macierz:

$$M(\phi)_{\mathcal{B}}^{\mathcal{B}} = \begin{bmatrix} 1 & 1 & 0 & 0 & & & & & & & & & & & & & \\ 0 & 1 & 1 & 0 & & & & & & & & & & & & & \\ 0 & 0 & 1 & 1 & & & & & & & & & & & & & \\ 0 & 0 & 0 & 1 & & & & & & & & & & & & & \\ & & & & 1 & 1 & 0 & & & & & & & & & & \\ & & & & 0 & 1 & 1 & & & & & & & & & & \\ & & & & 0 & 0 & 1 & & & & & & & & & & \\ & & & & & & & 1 & & & & & & & & & \\ & & & & & & & & 3 & 1 & 0 & & & & & & \\ & & & & & & & & 0 & 3 & 1 & & & & & & \\ & & & & & & & & 0 & 0 & 3 & & & & & & \\ & & & & & & & & & & & 3 & 1 & 0 & & & \\ & & & & & & & & & & & 0 & 3 & 1 & & & \\ & & & & & & & & & & & 0 & 0 & 3 & & & \\ & & & & & & & & & & & & & & 3 & 1 & \\ & & & & & & & & & & & & & & 0 & 3 & \end{bmatrix}$$

Czym są podprzestrzenie pierwiastkowe tego endomorfizmu? Ma on wielomian charakterystyczny postaci $(\lambda - 1)^8 \cdot (\lambda - 3)^8$, ale $\dim V_{(1)} = 3$ oraz $\dim V_{(3)} = 3$. Nie jest to więc endomorfizm diagonalizowalny. Tymczasem dysponując wiedzą nabytą na wykładzie możemy łatwo stwierdzić, że: $V_{[1]} = \text{lin}(\beta_1, \dots, \beta_8)$ oraz $V_{[3]} = \text{lin}(\beta_9, \dots, \beta_{16})$.

Twierdzenie 5.3: Twierdzenie o rozkładzie na podprzestrzenie pierwiastkowe

Niech $\phi \in \text{End}(V)$ i niech a_1, \dots, a_k będą parami różnymi wartościami własnymi ϕ . Następujące warunki są równoważne.

- Endomorfizm ϕ jest triangularyzowalny.
- $\dim V = \dim V_{[a_1]} + \dim V_{[a_2]} + \dots + \dim V_{[a_k]}$.
- $V = V_{[a_1]} \oplus V_{[a_2]} \oplus \dots \oplus V_{[a_k]}$.

Jeśli zachodzi dowolny z warunków wyżej oraz

$$w_\phi(\lambda) = (a_1 - \lambda)^{t_1} \cdot \dots \cdot (a_k - \lambda)^{t_k},$$

to

- (1) $V_{[a_j]} = \ker(\phi - a_j \text{id})^{t_j}$.
- (2) $\text{im}((\phi - a_j \text{id})^{t_j}) = \bigoplus_{i \neq j} V_{[a_i]}$
- (3) $w_{\phi|_{V_{[a_i]}}}(\lambda) = (a_j - \lambda)^{t_j}$,
- (4) $\dim V_{[a_j]} = t_j$.

Widzimy, że pierwsze trzy równoważne warunki w powyższym twierdzeniu nawiązują bezpośrednio do twierdzenia o endomorfizmach diagonalizowalnych. Mówiąc inaczej, dla endomorfizmu triangularyzowalnego podprzestrzenie pierwiastkowe odgrywają analogiczną rolę do podprzestrzeni własnych.

Rozdział 6

Podprzestrzenie niezmiennicze Twierdzenie Cayleya-Hamiltona

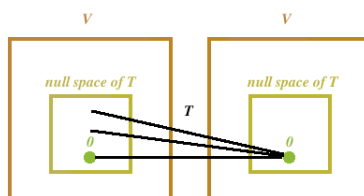
Na ostatnim wykładzie omówiliśmy twierdzenie Jordana opisujące endomorfizmy w przestrzeni skończonego wymiaru nad ciałem algebraicznie domkniętym, a także pozwalające w wielu sytuacjach stwierdzać kiedy macierze są podobne. Dziś, kończąc temat endomorfizmów, przyjrzymy się tak zwanym podprzestrzeniom niezmienniczym endomorfizmów. Ich zrozumienie pozwoli nam zobaczyć z nowej perspektywy omówione wcześniej wyniki. Każda podprzestrzeń własna endomorfizmu ϕ przestrzeni liniowej V ma tę własność, że nie zmienia się (jako cała przestrzeń) przy działaniu ϕ , to znaczy: $\phi(V_{(a)}) = V_{(a)}$. Uogólnieniem tej własności jest pojęcie podprzestrzeni niezmienniczej, któremu poświęcony jest ten wykład¹.

Definicja 6.1: Podprzestrzeń niezmiennicza względem endomorfizmu

Niech ϕ będzie endomorfizmem przestrzeni liniowej V nad ciałem K . Podprzestrzeń $W \subseteq V$ nazywamy NIEZMIENNICZĄ WZGLĘDEM ϕ (lub ϕ -niezmienniczą) wtedy i tylko wtedy, gdy $\phi(W) \subseteq W$.

Przykłady.

- Niech $\phi \in \text{End}(V)$. Wówczas V oraz podprzestrzeń zerowa są zawsze niezmiennicze względem ϕ .



Jądro endomorfizmu jest zawsze podprzestrzenią niezmienniczą. Źródło: <http://mathonline.wikidot.com/>.

- Niech $\phi \in \text{End}(V)$. Wówczas $\ker(\phi)$ oraz $\text{im}(\phi)$ są niezmiennicze względem ϕ . Dość istotne dla różnych rozumowań jest również to, że $\ker(\phi^k)$ oraz $\text{im}(\phi^k)$ są ϕ -niezmiennicze, dla każdego $k \in \mathbb{N}$.
- Niech $\phi \in \text{End}(V)$ oraz niech $0 \neq \alpha \in V$ będzie wektorem własnym ϕ . Wówczas $\text{lin}(\alpha)$ jest podprzestrzenią ϕ -niezmienniczą.
- Niech a będzie wartością własną $\phi \in \text{End}(V)$. Wówczas $V_{(a)}$ jest podprzestrzenią ϕ -niezmienniczą.
- Niech $\phi \in \text{End}(\mathbb{R}^4)$ będzie zadany w bazie standardowej macierzą

$$M(\phi)_{st}^{st} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Łatwo widzieć, że $\text{lin}((1, 0, 0, 0), (0, 1, 0, 0))$ oraz $\text{lin}((0, 0, 1, 0), (0, 0, 0, 1))$ są (oczywiście nie jedynymi) podprzestrzeniami niezmienniczymi endomorfizmu ϕ . Nie są to też podprzestrzenie własne.

¹Ostatnia aktualizacja: 07.05.2023 r.

Definicja 6.2

Niech $\phi : V \rightarrow V$ będzie przekształceniem liniowym oraz niech $U \subseteq V$ będzie podprzestrzenią ϕ -niezmienniczą.^a Przez $\phi|_U$ rozumiemy endomorfizm przestrzeni U zadany wzorem:

$$\phi|_U(u) = \phi(u),$$

dla każdego $u \in U$.

^aOznaczenie to sugeruje, że mowa jest o obcięciu przekształcenia f do podprzestrzeni U , ale obcięcie jest formalnie definiowane jako przekształcenie z U do V . Nam natomiast zależy na tym, żeby macierz endomorfizmu $\phi|_U$ była kwadratowa, co oczywiście ma sens w przypadku podprzestrzeni niezmienniczych. Taka konwencja jest przyjmowana w wielu źródłach, mimo pewnego braku precyzji (którą oczywiście da się, przy większym formalizmie, uzyskać).

Tak jak endomorfizm ma wektor własny wtedy i tylko wtedy, gdy jego wielomian charakterystyczny ma pierwiastek, tak istnienie nietrywialnych (różnych od zera i całości) podprzestrzeni niezmienniczych zależy od rozkładalności wielomianu ϕ w ciele K na czynniki oraz od możliwości przedstawienia macierzy przekształcenia ϕ w bazie w odpowiedniej postaci blokowej.

Obserwacja 6.1

Niech V będzie skończenie wymiarową przestrzenią liniową nad ciałem K , niech $\phi \in \text{End}(V)$ oraz niech U będzie podprzestrzenią V , różną od 0 i V . Następujące warunki są równoważne:

- (1) $U \subseteq V$ jest podprzestrzenią ϕ -niezmienniczą,
- (2) istnieje baza \mathcal{A} przestrzeni V oraz taka macierz $A \in M_{\dim U}(K)$, że

$$M(\phi)_{\mathcal{A}}^{\mathcal{A}} = \begin{bmatrix} A & B \\ 0 & C \end{bmatrix},$$

gdzie A jest macierzą $\phi|_U$ w pewnej bazie przestrzeni U .

Gdy spełniony jest jeden z warunków wyżej, wówczas istnieje $g \in K[\lambda]$, że:^a

$$w_{\phi}(\lambda) = w_{\phi|_U}(\lambda) \cdot g(\lambda).$$

^aW dodatku omówimy fundamentalny problem odwrotny: kiedy rozkład wielomianu charakterystycznego implikuje rozkład związany z podprzestrzeniami niezmienniczymi. Czytelnik może jednak zadać sobie pytanie jak zrozumieć przypadek, gdy $B = 0$? Co wiemy o $g \in K[\lambda]$?

Dowód. Załóżmy (1). Niech $\mathcal{A}' = (\alpha_1, \dots, \alpha_k)$ będzie bazą U oraz niech $(\alpha_{k+1}, \dots, \alpha_n)$ będzie dopełnieniem bazy \mathcal{A}' do bazy \mathcal{A} przestrzeni V . Obrazy wektorów $\alpha_1, \dots, \alpha_k$ po zastosowaniu ϕ należą do U , a więc do $\text{lin}(\alpha_1, \dots, \alpha_k)$. A zatem pierwsze k kolumn macierzy $M(\phi)_{\mathcal{A}}^{\mathcal{A}}$ może mieć niezerowe wyrazy jedynie w pierwszych k wierszach. W szczególności istnieją takie macierze $A \in M_k(K)$, $B \in M_{k \times (n-k)}(K)$ oraz $C \in M_{n-k}(K)$, że:

$$M(\phi)_{\mathcal{A}}^{\mathcal{A}} = \begin{bmatrix} A & B \\ 0 & C \end{bmatrix}.$$

Uzyskaliśmy zatem (2). Odwrotna implikacja (2) \Rightarrow (1) jest teraz jasna. Co więcej,

$$w_{\phi}(\lambda) = \det \begin{bmatrix} A - \lambda I_k & B \\ 0 & C - \lambda I_{n-k} \end{bmatrix}.$$

A zatem $w_{\phi}(\lambda) = \det(A - \lambda I_k) \det(C - \lambda I_{n-k})$. Jednak $\det(A - \lambda I_k)$ to wielomian charakterystyczny endomorfizmu $\phi|_U$. Dowód jest zakończony. \square

Zajmiemy się teraz wykorzystaniem następującej obserwacji. Jeśli v należy do podprzestrzeni ϕ -niezmienniczej U przestrzeni V , to do U należą również kolejne iteracje ϕ na v

$$\phi(v), \quad \phi^2(v), \quad \phi^3(v), \quad \dots$$

Definicja 6.3: Podprzestrzeń cykliczna

Niech $\phi \in \text{End}(V)$. Podprzestrzenią CYKLIČNĄ przestrzeni V względem ϕ rozpiętą przez wektor α nazywamy:

$$V_\alpha = \text{lin}(\phi^n(\alpha) \mid n \in \mathbb{N}) = \text{lin}(\alpha, \phi(\alpha), \phi^2(\alpha), \phi^3(\alpha), \dots).$$

Przykłady.

- Niech ϕ będzie jednokładnością o skali λ na V (w tym identycznością, dla $\lambda = 1$). Wówczas dla każdego $\alpha \in V$ mamy $V_\alpha = \text{lin}(\alpha)$, gdyż dla dodatniej liczby całkowitej k mamy $\phi^k(\alpha) = \lambda^k \cdot \alpha$.
- Niech ϕ będzie symetrią \mathbb{R}^2 względem $\text{lin}(1, 0)$ wzdłuż $\text{lin}(0, 1)$. Wówczas z jednej strony mamy $(1, 0) = \phi(1, 0) = \phi^2(1, 0) = \dots$, a z drugiej: $\phi((1, 1)) = (1, -1)$, $\phi((1, -1)) = (1, 1), \dots$, czyli $V_{(1,0)} = \text{lin}(1, 0)$, $V_{(0,1)} = \text{lin}(0, 1)$ ale $V_{(1,1)} = \mathbb{R}^2$.
- Niech $\phi \in \text{End}(K^n)$ dany będzie wzorem $\phi((x_1, x_2, \dots, x_n)) = (x_2, x_3, \dots, x_n, 0)$. Wówczas

$$\begin{aligned}\phi(1, 1 \dots, 1, 1, 1) &= (1, 1, \dots, 1, 1, 0), \\ \phi^2(1, 1 \dots, 1, 1, 1) &= \phi(1, 1 \dots, 1, 1, 0) = (1, 1, \dots, 1, 0, 0), \\ \phi^3(1, 1 \dots, 1, 1, 1) &= \phi^2(1, 1 \dots, 1, 1, 0) = \phi(1, 1 \dots, 1, 0, 0) = (1, 1, \dots, 0, 0, 0), \\ &\vdots \\ \phi^{n-1}(1, 1 \dots, 1, 1, 1) &= \phi^{n-2}(1, 1 \dots, 1, 0) = \dots = \phi(1, 1 \dots, 0, 0) = (1, 0, \dots, 0, 0), \\ \phi^n(1, 1 \dots, 1, 1, 1) &= (0, 0, 0, \dots, 0, 0).\end{aligned}$$

Zatem $V_{(1,1,1,\dots,1,1)} = K^n$. Ten endomorfizm jest nam dobrze znany, a jego macierz to

$$M(\phi)_{st}^{st} = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & 0 & \dots & 0 & 0 \end{bmatrix} \in M_n(K).$$

- Jeśli $(\alpha_1, \dots, \alpha_n)$ jest bazą przestrzeni V , w której macierz endomorfizmu ϕ jest klatką Jordana odpowiadającą wartości własnej a , wówczas $\text{lin}(\alpha_1, \dots, \alpha_n)$ jest podprzestrzenią cykliczną endomorfizmu (nilpotentnego) $\phi - a \text{id}$ rozpiętą przez wektor α_n . Mamy bowiem

$$\begin{aligned}\alpha_{n-1} &= (\phi - a \text{id})(\alpha_n), \\ \alpha_{n-2} &= (\phi - a \text{id})^2(\alpha_n), \\ &\vdots \\ \alpha_1 &= (\phi - a \text{id})^{n-1}(\alpha_n) \\ 0 &= (\phi - a \text{id})^k(\alpha_n), \text{ dla } k \geq n.\end{aligned}$$

Ogólnie, baza Jordana endomorfizmu ϕ (o ile istnieje) rozbija się na podzbiory rozłączne złożone z baz podprzestrzeni cyklicznych endomorfizmów $\phi - a_i \text{id}$, gdzie a_i są wartościami własnymi ϕ .

Jednym z ważnych twierdzeń teorii endomorfizmów, którego tu nie dowodzimy, jest następujący rezultat².

Twierdzenie 6.1: O rozkładzie na podprzestrzenie cykliczne

Niech ϕ będzie endomorfizmem skończonej wymiarowej przestrzeni liniowej V . Jeżeli wielomian charakterystyczny ϕ rozkłada się na czynniki liniowe, to V jest sumą prostą (skończenie wielu) przestrzeni cyklicznych.

Kluczowe dla naszych dalszych rozważań jest zauważenie, że podprzestrzeń cykliczna ϕ rozpięta przez wektor v składa się z wartości v na wszystkich wielomianach od endomorfizmu ϕ . O czym mowa?

²Dowód w notatkach dr. A. Strojnowskiego: https://www.mimuw.edu.pl/~stroa/Gal_Dodatki/Dodatki.html.

Definicja 6.4

Niech $w \in K[\lambda]$ będzie postaci $a_0 + a_1\lambda + \dots + a_n\lambda^n$. Niech $\phi \in \text{End}(V)$, gdzie V jest nad ciałem K oraz niech $A \in M_s(K)$. Definiujemy:

$$w(\phi) = a_0 \cdot \text{id}_V + a_1 \cdot \phi + \dots + a_n \cdot \phi^n \in \text{End}(V), \quad w(A) = a_0 I + a_1 A + \dots + a_n A^n \in M_s(K).$$

OBSERWACJA. Jeśli dla $w, v, z \in K[\lambda]$ mamy $w = v + z$, to $w(\phi) = v(\phi) + z(\phi)$, a jeśli $w = v \cdot z$, to $w(\phi) = v(\phi) \circ z(\phi) = z(\phi) \circ v(\phi) = vz(\phi) = zv(\phi)$.

Definicja 6.5: Algebra endomorfizmu

Niech $\phi \in \text{End}(V)$, gdzie V jest przestrzenią liniową nad ciałem K . Podprzestrzeń

$$E(\phi) = \{w(\phi) \mid w \in K[\lambda]\} \subseteq \text{End}(V)$$

nazywamy ALGEBRĄ ENDOMORFIZMU ϕ .

Możemy teraz napisać, że dla endomorfizmu ϕ podprzestrzeń cykliczna rozpięta przez wektor v złożona jest ze wszystkich wektorów postaci $V_v = \{f(v), f \in E(\phi)\}$. Zauważmy także, że jeśli $A = M(\phi)|_A^A$, to dla dowolnego $w \in K[\lambda]$ mamy $w(A) = M(w(\phi))|_A^A$.

Sformułujemy teraz kilka zadań, które są nietrudnymi, ale bardzo pouczającymi ćwiczeniami. Są one niezbędne do dowodu twierdzenia Cayleya-Hamiltona, które zaraz sformułuję (ale na wykładzie nie będzie ono dowodzone). Samo stosowanie twierdzenia wlicza się do materiału. Oto te ćwiczenia.

ĆWICZENIE. Własności podprzestrzeni ϕ -cyklicznej V_α , dla $\phi \in \text{End}(V)$.

- V_α jest NAJMNIEJSZĄ WZGLĘDEM INKLUZJI podprzestrzenią ϕ -niezmienniczą zawierającą wektor α .
- Jeśli $0 \neq \alpha$, to bazą V_α jest układ

$$\mathcal{B} = (\alpha, \phi(\alpha), \phi^2(\alpha), \phi^3(\alpha), \dots, \phi^{k-1}(\alpha)) \quad \text{gdzie } k = \dim V_\alpha.$$

- Niech $k = \dim V_\alpha$ oraz niech $c_0, \dots, c_{k-1} \in K$ spełniają

$$c_0\alpha + c_1\phi(\alpha) + \dots + c_{k-1}\phi^{k-1}(\alpha) + \phi^k(\alpha) = 0.$$

Wówczas

$$M(\phi|_{V_\alpha})_{\mathcal{B}}^{\mathcal{B}} = \begin{bmatrix} 0 & 0 & \dots & 0 & -c_0 \\ 1 & 0 & \dots & 0 & -c_1 \\ 0 & 1 & \dots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -c_{k-1} \end{bmatrix}. \quad (*)$$

Co więcej:

$$w_{\phi|_{V_\alpha}}(\lambda) = (-1)^k \cdot (c_0 + c_1\lambda + \dots + c_{k-1}\lambda^{k-1} + \lambda^k).$$

Jesteśmy gotowi sformułować twierdzenie Cayleya-Hamiltona. Twierdzenie nosi nazwisko wielkich matematyków XIX wieku. Pokazali oni w połowie tamtego stulecia jedynie pewne szczególne przypadki. Co znamienne, Cayley nie widział powodu ani sensu szukania dowodu dla macierzy dowolnego rozmiaru. Zostało ono udowodnione przez Frobeniusa w 1878 roku, który uświadomił sobie dopiero w 1896 roku, że ktoś już o tym problemie myślał przed nim. Zgodnie z ówczesnym zwyczajem przyznał pierwszeństwo swoim słynnym poprzednikom.

Twierdzenie 6.2: Twierdzenie Cayleya-Hamiltona

Jeśli $A \in M_n(K)$ oraz $w = w_A(\lambda)$ jest wielomianem charakterystycznym macierzy A , to $w(A) = 0$.

Zanim przedstawię dowód zobaczmy jak użyteczne i zaskakujące twierdzenie mamy przed sobą. Mówi ono, że dla każdej macierzy rozmiaru n macierz A^n jest kombinacją liniową swoich niższych potęg.

Dla przykładu: jeśli A to macierz 3×3 o wielomianie charakterystycznym $-\lambda^3 + 1$, to na mocy twierdzenia Cayleya-Hamiltona mamy $-A^3 + I = 0$. Stąd $A^3 = I$. A zatem chcąc wyliczyć na przykład A^{1000} mamy po prostu

$$A^{1000} = (A^3)^{333} A = A.$$

Istnieją też bardziej wyrafinowane zastosowania tej metody³.

Twierdzenie to pozwala także w ciekawy sposób odwracać niektóre macierze. Jeśli wiemy, dla przykładu, że macierz odwracalna A ma wielomian charakterystyczny $\lambda^5 + \lambda - 1$, to oczywiście $A^5 + A - I = 0$. Mnożąc tę równość z dowolnej strony przez A^{-1} dostajemy warunek: $A^4 + I - A^{-1} = 0$. A zatem $A^{-1} = A^4 + I$. W niektórych przypadkach twierdzenie Cayleya-Hamiltona znacznie ułatwia odwracanie macierzy.

Dowód. Niech $\phi \in \text{End}(V)$ oraz $A = M(\phi)_{st}^{st}$, przy czym $\dim(V) = n$. Aby pokazać, że $w_A(A) = 0$ wystarczy pokazać, że dla dowolnego $\alpha \in V$ zachodzi równość

$$w_\phi(\phi)(\alpha) = 0.$$

Weźmy więc dowolny niezerowy wektor $\alpha \in V$. Rozważamy podprzestrzeń cykliczną V_α wymiaru k . Mamy więc liczby $a_0, a_1, \dots, a_{k-1} \in K$, że

$$0 = a_0\alpha + a_1\phi(\alpha) + \dots + a_{k-1}\phi^{k-1}(\alpha) + \phi^k(\alpha),$$

bo baza V_α złożona jest z $\alpha, \dots, \phi^{k-1}(\alpha)$ (patrz ćwiczenie wyżej). Niech

$$q(\lambda) = a_0 + a_1\lambda + \dots + a_{k-1}\lambda^{k-1} + \lambda^k \in K[\lambda].$$

Rozszerzamy bazę V_α do bazy \mathcal{A} całego V . Wówczas, zgodnie z twierdzeniem o macierzy przekształcenia mającego podprzestrzeń ϕ -niezmienniczą mamy macierze $X \in M_k(K)$, $Y \in M_{k \times n-k}(K)$, $Z \in M_{n-k}(K)$, że:

$$M(\phi)_{\mathcal{A}}^{\mathcal{A}} = \begin{bmatrix} X & Y \\ 0 & Z \end{bmatrix}.$$

Opiszmy blok X tej macierzy wiedząc co robi ϕ z pierwszymi k wektorami $\alpha, \phi(\alpha), \phi^2(\alpha), \dots, \phi^{k-1}(\alpha)$ bazy \mathcal{A} :

$$X = \begin{bmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_{k-1} \end{bmatrix}.$$

Rzeczywiście

$$\phi(\alpha) = \phi(\alpha), \quad \phi(\phi(\alpha)) = \phi^2(\alpha), \quad \dots, \quad \phi(\phi^{k-1}(\alpha)) = \phi^k(\alpha) = -(a_0\alpha + a_1\phi(\alpha) + \dots + a_{k-1}\phi^{k-1}(\alpha)).$$

Cóż nam to wszystko dało? Otóż wiemy, że wielomian charakterystyczny $\phi|_{V_\alpha}$ jest dzielnikiem wielomianu charakterystycznego ϕ , bo V_α jest niezmiennicza. Ale macierz $\phi|_{V_\alpha}$ w bazie $\alpha, \dots, \phi^{k-1}(\alpha)$ ma dokładnie postać X . A więc wielomian charakterystyczny X jest dzielnikiem wielomianu charakterystycznego endomorfizmu ϕ . Wielomian charakterystyczny tej macierzy to $q(\lambda)$, czyli (jak wiemy z innego z ćwiczeń) $(-1)^k(a_0 + a_1\lambda + \dots + a_{k-1}\lambda^{k-1} + \lambda^k)$. A zatem wiemy, że $w_\phi(\lambda) = q(\lambda) \cdot h(\lambda) = h(\lambda) \cdot q(\lambda)$, dla pewnego $h \in K[\lambda]$. Jednocześnie

$$w_\phi(\phi)(\alpha) = (-1)^k(a_0\alpha + a_1\phi(\alpha) + \dots + a_{k-1}\phi^{k-1}(\alpha) + \phi^k(\alpha)) = 0.$$

W szczególności mamy $w_\phi(\phi)(\alpha) = hq(\phi)(\alpha) = (h(\phi) \circ q(\phi))(\alpha) = h(\phi)(0) = 0$. Zatem $w_\phi(\phi) = 0$. \square

³Więcej przykładów i agitacji w filmie z czasów pandemicznych: <https://youtu.be/wSGW9E06Wg8>.

6.1 Zadania do samodzielnej pracy

Zadania ilustrujące umiejętności niezbędne do zaliczenia przedmiotu oznaczone są symbolem ♠. Przy tych zadaniach dodany jest opis umiejętności, które sprawdzają.

1. (♠ Wyznaczanie potęg i odwrotności macierzy/endomorfizmów z twierdzenia Cayleya-Hamiltona)

- Wyznacz B^{100} , gdzie $B = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & -1 \\ 0 & 1 & 1 \end{bmatrix} \in M_3(\mathbb{C})$.
- Wyznacz takie $a, b, c \in \mathbb{R}$, że $A^{-1} = aA^2 + bA + cI$, gdzie

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

- Załóżmy, że macierz $A \in M_2(\mathbb{R})$ ma dwie wartości własne: -1 oraz 3 . Dla każdej dodatniej liczby całkowitej n znajdź a_n oraz b_n , takie że $A^{n+1} = a_n A + b_n I$.
- Niech ϕ będzie endomorfizmem przestrzeni \mathbb{R}^3 danym wzorem

$$\phi((x_1, x_2, x_3)) = (-3x_1 - 4x_2 - 4x_3, 2x_1 + 2x_2 + x_3, x_2 + 2x_3).$$

Udowodnij, że $\phi^{2n} = n \cdot \phi^2 - (n-1) \cdot \text{id}$.

2. Macierze $A, B \in M_2(\mathbb{C})$ spełniają zależność $A = AB - BA$.

- Wykaż, że $\text{tr}(A) = 0$.
- Wykaż, że $A^2 = -\det(A)I$.
- Zapisz A^2 na dwa sposoby jako iloczyn i udowodnij, że $A^2 = 0$.

3. Macierze $A, B \in M_2(\mathbb{C})$ spełniają zależność $(AB)^2 = 0$.

- Udowodnij, że $\det(AB) = \text{tr}(AB) = 0$.
- Wykaż, że $(BA)^2 = 0$.

4. Endomorfizm ϕ przestrzeni liniowej V wymiaru n ma tę własność, że dowolna podprzestrzeń V wymiaru $n-1$ jest ϕ -niezmiennicza. Wykaż, że każdy niezerowy wektor przestrzeni V jest własny.

5. Opisz wszystkie podprzestrzenie ϕ -niezmiennicze endomorfizmu $\phi \in \text{End}(\mathbb{C}^2)$, danego wzorem $\phi((x_1, x_2)) = (3x_1 + 2x_2, x_2)$. Ile maksymalnie podprzestrzeni niezmienniczych może mieć endomorfizm $g \in \text{End}(\mathbb{C}^2)$, który nie jest homotetią?

6. Opisz wszystkie podprzestrzenie ϕ -niezmiennicze endomorfizmu $\phi \in \text{End}(\mathbb{R}^4)$, danego wzorem $\phi((x_1, x_2, x_3, x_4)) = (x_2, x_3, x_4, 0)$.

7. Endomorfizm $\phi \in \text{End}(\mathbb{R}^3)$ dany jest w bazie standardowej macierzą:

$$M(\phi)_{st}^{st} = \begin{bmatrix} 4 & -2 & 2 \\ 2 & 0 & 2 \\ -1 & 1 & 1 \end{bmatrix}.$$

Wykaż, że wszystkie 2-wymiarowe podprzestrzenie ϕ -niezmiennicze przestrzeni \mathbb{R}^3 są albo równe $U = \text{lin}((1, 1, 0), (1, 0, -1))$, albo równe $\text{lin}((2, 2, -1), \alpha)$, gdzie $\alpha \in U$.

8. Endomorfizm $\phi \in \text{End}(\mathbb{R}^3)$ dany jest w bazie standardowej macierzą:

$$M(\phi)_{st}^{st} = \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 2 \end{bmatrix}.$$

Uzasadnij, że $W = \text{lin}((1, 0, 0), (0, 1, 0))$ jest podprzestrzenią ϕ -niezmienniczą. Czy istnieje podprzestrzeń ϕ -niezmiennicza $W' \neq W$, taka że $\dim(W') = 2$? Wskazówka: załóżmy, że istnieje taka W' . Czy $W' \cap W$ jest ϕ -niezmiennicza? Jaki ma wymiar?

9. Endomorfizm $\phi \in \text{End}(\mathbb{R}^4)$ dany jest wzorem $\phi((x_1, x_2, x_3, x_4)) = (x_2 + x_3, x_3, 0, 0)$. Wyznacz ϕ^3 . Czy istnieją takie ϕ -niezmiennicze podprzestrzenie $U, V \subseteq \mathbb{R}^4$, że $\dim U = \dim V$ oraz $\mathbb{R}^4 = U \oplus V$?

10. Niech $A, B \in M_n(\mathbb{C})$. Załóżmy, że $r(AB - BA) = 1$. Niech λ będzie wartością własną macierzy B . Wykaż, że obraz lub jądro endomorfizmu $\psi - \lambda \text{id}$ jest podprzestrzenią ϕ -niezmienniczą.

6.2 Uzupełnienie. Rozkłady ϕ -niezmiennicze

Niezwykle istotny wgląd w teorię endomorfizmów daje badanie ich nie tylko z perspektywy macierzy przekształceń, ale wynikających z niej rozkładów przestrzeni liniowych, na których działają. Przypomnijmy kluczową definicję, wspominaną w uzupełnieniach do wykładów w pierwszym semestrze.

Definicja 6.6: Suma prosta

Niech V_1, V_2, \dots, V_k będą podprzestrzeniami przestrzeni V . Powiemy, że V jest SUMĄ PROSTĄ PODPRZESTRZENI V_1, V_2, \dots, V_k , co oznaczamy jako $V = V_1 \oplus V_2 \oplus \dots \oplus V_k$, jeśli zachodzi jeden z dwóch równoważnych warunków:

- (1) każdy wektor $v \in V$ rozkłada się w sposób jednoznaczny na sumę postaci $v_1 + v_2 + \dots + v_k$, gdzie $v_i \in V_i$.
- (2) $V = V_1 + V_2 + \dots + V_k$ oraz jeśli W_i oznacza sumę podprzestrzeni V_1, \dots, V_k z wyłączeniem składnika V_i , to $V_i \cap W_i = \{0\}$, dla $i = 1, \dots, k$.

Z Obserwacji 6.1 wynika następujący fundamentalny fakt.

Obserwacja 6.2

Niech $V = V_1 \oplus \dots \oplus V_k$ oraz niech $\phi \in \text{End}(V)$ będzie taki, że V_1, \dots, V_k są podprzestrzeniami ϕ -niezmienniczymi w V . Wówczas ϕ ma w pewnej bazie \mathcal{A} macierz blokowo-diagonalną postaci

$$M(\phi)_{\mathcal{A}}^{\mathcal{A}} = \begin{bmatrix} A_1 & 0 & 0 & \dots & 0 \\ 0 & A_2 & 0 & \dots & 0 \\ 0 & 0 & A_3 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & A_k \end{bmatrix}, \quad \text{gdzie } A_i \in M_{\dim(V_i)}(K).$$

Niestety uzyskiwanie rozkładów przestrzeni liniowych na sumy proste podprzestrzeni niezmienniczych bywa bardzo trudne. Zauważmy, że kryterium diagonalizowalności macierzy dotyczy dokładnie sytuacji, gdy V jest sumą prostą podprzestrzeni własnych. Skąd jednak wiadomo, że taki warunek zachodzi? Niestety nie jest prawdą nad każdym ciałem, że jeśli $W \subseteq V$ jest podprzestrzenią niezmienniczą względem $\phi \in \text{End}(V)$, to istnieje podprzestrzeń ϕ -niezmiennicza W' taka, że $W \oplus W' = V$. Wybór odpowiednich podprzestrzeni (i ciał!), dla których takie dopełnienia da się uzyskać jest treścią głębokich twierdzeń.⁴

Twierdzenie, któremu poświęcimy to uzupełnienie opowiada o pięknym i zaskakującym związku pomiędzy rozkładami na sumy proste, rozkładalnością wielomianu charakterystycznego oraz geometrią.

Definicja 6.7: Rozkład ϕ -niezmienniczy

Niech $\phi \in \text{End}(V)$. Niech V będzie sumą prostą postaci

$$V = V_1 \oplus \dots \oplus V_r \quad (*).$$

Powiemy, że ROZKŁAD (*) JEST ϕ -NIEZMIENNICZY, jeśli każda z podprzestrzeni V_i jest ϕ -niezmiennicza.

Przykłady:

- jeśli $\phi \in \text{End}(V)$ jest rzutem, to rozkład $V = \ker(\phi) \oplus \text{im}(\phi)$ jest ϕ -niezmienniczy,
- jeśli $\phi \in \text{End}(V)$ jest diagonalizowalny, to rozkład V na sumę prostą podprzestrzeni własnych jest ϕ -niezmienniczy.
- jeśli $\phi \in \text{End}(V)$ jest triangularyzowalny, to rozkład V na sumę prostą podprzestrzeni pierwiastkowych jest ϕ -niezmienniczy.

⁴Jest to w istocie jeden z centralnych problemów algebry, leżący u podstaw tzw. teorii reprezentacji.

KLUCZOWA IDEA. Jeśli znajdziemy rozkład ϕ -niezmienniczy postaci $V = V_1 \oplus \dots \oplus V_r$, to badanie działania ϕ na V sprowadza się do badania *niezależnych działań* ϕ na każdym z V_i . Podsumujmy.

Obserwacja 6.3

Niech V będzie wymiaru n nad ciałem K . Niech $\phi \in \text{End}(V)$. Załóżmy, że mamy rozkład ϕ -niezmienniczy $V = V_1 \oplus \dots \oplus V_r$. Istnieje baza \mathcal{A} przestrzeni V , że:

(1) macierz $M(\phi)_{\mathcal{A}}^{\mathcal{A}}$ ma postać BLOKOWO-DIAGONALNĄ

$$\begin{bmatrix} A_1 & 0 & \dots & 0 \\ 0 & A_2 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & A_r \end{bmatrix}, \quad \text{gdzie } A_i \in M_{\dim V_i}(K), \quad (*)$$

(2) $w_{\phi}(\lambda) = w_{A_1}(\lambda) \cdot \dots \cdot w_{A_r}(\lambda)$.

Prawdziwy *cud* polega na tym, że odpowiednia rozkładalność wielomianu charakterystycznego gwarantuje rozkłady ϕ -niezmiennicze. Przyjrzymy się tej sprawie, przywołując wiedzę z materiałów uzupełniających z pierwszego semestru.

Definicja 6.8: Wielomian (nie)rozkładalny

Niech K będzie ciałem.

- wielomian $f \in K[x]$ nazywamy ROZKŁADALNYM, jeśli istnieją wielomiany $p, q \in K[x]$ stopnia mniejszego niż f takie, że

$$f(x) = p(x)q(x).$$

Niezerowy wielomian, który nie jest rozkładalny nazywamy wielomianem NIEROZKŁADALNYM.

- NAJWIĘKSZY WSPÓLNY DZIELNIK wielomianów p_1, \dots, p_n należących do $K[x]$ nazywamy wielomian najwyższego możliwego stopnia dzielący wszystkie te wielomiany. Jeśli 1 jest największym wspólnym dzielnikiem p_1, \dots, p_n , wówczas mówimy, że wielomiany te są WZGLĘDNIE PIERWSZE.

Niezwykle istotny wynik związany z rozkładami ϕ -niezmienniczymi wiąże je z rozkładalnością wielomianów należących do algebry endomorfizmu.

Twierdzenie 6.3: Twierdzenie o rozkładzie prymarnym

Niech $p \in K[\lambda]$ będzie wielomianem o rozkładzie^a

$$p = p_1 \dots p_k,$$

gdzie p_1, \dots, p_k są czynnikami względnie pierwszymi. Niech $\phi \in \text{End}(V)$. Wówczas ma miejsce rozkład

$$\ker p(\phi) = \ker p_1(\phi) \oplus \dots \oplus \ker p_k(\phi)$$

na sumę prostą ϕ -niezmienniczych podprzestrzeni w V .

^aDwie kluczowe intuicje dotyczące powyższego fundamentalnego wyniku.

- Jeśli V jest skończenie wymiarową przestrzenią nad ciałem K , to dla każdego $\phi \in \text{End}(V)$ mamy $w_{\phi}(\phi) = 0$ (twierdzenie Cayleya-Hamiltona), czyli $\ker p(\phi) = V$ dla $p = w_{\phi}(\lambda)$.
- Nawet jeśli $\dim V = \infty$, ale mimo to $\phi \in \text{End}(V)$ spełnia równanie wielomianowe, np. rzut $\phi \in \text{End}(V)$ spełnia $(\phi^2 - \phi)(\alpha) = 0$, dla $\alpha \in V$, to twierdzenie działa.

Zobaczmy przykłady takich rozkładów.

- Rozważmy $\phi \in \text{End}(\mathbb{R}^4)$ dany macierzą:

$$M(\phi)_{st}^{st} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Oczywiście $w_\phi(\lambda) = (1 - \lambda)^4$, ale ϕ nie jest diagonalizowalny, bo $\dim V_{(1)} = \dim \ker(\phi - \text{id}) = 2$. Z drugiej strony biorąc wektory bazowe $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4$ mamy:

$$\begin{aligned} \phi(\epsilon_1) &= \epsilon_1 && \Rightarrow (\phi - \text{id})(\epsilon_1) = 0, \\ \phi(\epsilon_2) &= \epsilon_1 + \epsilon_2 && \Rightarrow (\phi - \text{id})(\epsilon_2) = \epsilon_1 \Rightarrow (\phi - \text{id})^2(\epsilon_2) = 0, \\ \phi(\epsilon_3) &= \epsilon_2 + \epsilon_3 && \Rightarrow (\phi - \text{id})(\epsilon_3) = \epsilon_2 \Rightarrow (\phi - \text{id})^3(\epsilon_3) = 0, \\ \phi(\epsilon_4) &= \epsilon_4 && \Rightarrow (\phi - \text{id})(\epsilon_4) = 0. \end{aligned}$$

⁵ Zatem $\mathbb{R}^4 = \ker(\phi - \text{id})^3$. Co ciekawe, $\ker(\phi - \text{id})^3$ rozkłada się.

- Rozważmy $\phi \in \text{End}(\mathbb{R}^4)$ dany macierzą:

$$M(\phi)_{st}^{st} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \end{bmatrix}.$$

Łatwo widzieć, że $w_\phi(\lambda) = \lambda^4 + 1$. A zatem $w_\phi(\lambda)$ nie ma pierwiastków w \mathbb{R} . Mamy jednak⁶

$$\mathbb{R}^4 = \ker(\phi^4 + \text{id}) = \ker(\phi^2 - 2\phi + 2\text{id}) \oplus \ker(\phi^2 + 2\phi + 2\text{id}),$$

zatem mimo, że ϕ nie jest triangularyzowalny, istnieje baza \mathcal{A} przestrzeni \mathbb{R}^4 , w której ϕ ma macierz blokowo-diagonalną:

$$\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}, \quad \text{dla pewnych } A, B \in M_2(\mathbb{R}).$$

Być może jeszcze jeden obrazek pomoże nieco zrozumieć rozkłady niezmiennicze. Jeśli $\phi \in \text{End}(V)$ jest triangularyzowalny i $M(\phi)_{\mathcal{A}}^{\mathcal{A}}$ jest górnotrójkątna dla bazy $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$ przestrzeni V , to mamy następujący WSTĘPUJĄCY ŁAŃCUCH $n + 1$ PODPRZESTRZENI ϕ -niezmienniczych:

$$\{0\} \subset \text{lin}(\alpha_1) \subset \text{lin}(\alpha_1, \alpha_2) \subset \text{lin}(\alpha_1, \alpha_2, \alpha_3) \subset \dots \subset \text{lin}(\alpha_1, \dots, \alpha_{n-1}) \subset V.$$

Intuicyjnie V wraz ze wskazanymi podprzestrzeniami przypomina przekrój drzewa, w którym koncentrycznie układają się kolejne słoje reprezentujące kolejne podprzestrzenie. Endomorfizm ϕ działa na V w taki sposób, że jeśli znajdowaliśmy się w *obszarze ograniczonym danym słojem*, to ϕ nas z niego nie wyprowadzi. W przypadku, gdy ϕ jest diagonalizowalny, wówczas mamy rozkład ϕ -niezmienniczy $V = \text{lin}(\alpha_1) \oplus \text{lin}(\alpha_2) \oplus \dots \oplus \text{lin}(\alpha_n)$ i wtedy możemy stwierdzić, że pomiędzy każdymi dwoma „słojami” przekształcenie działa w sposób niezależny od pozostałych obszarów.



⁵Ale o tym mówi nam już twierdzenie Jordana. W rozkładzie wielomianu $w_\phi(\lambda)$ mamy jeden czynnik, z dokładnością do wzgl. pierwszości, czyli $p_1 = (1 - \lambda)^4$.

⁶Inaczej mówiąc $w_\phi(\lambda) = p_1 p_2$, gdzie $p_1 = \lambda^2 - 2\lambda + 2$, $p_2 = \lambda^2 + 2\lambda + 2$.

6.3 Dodatek. Rodziny endomorfizmów przemiennych

Wspólna diagonalizowalność i triangularyzowalność

Niech $D_n(K)$ będzie podzbiorem $M_n(K)$ złożonym z macierzy diagonalizowalnych nad K . Wiemy, że zbiór ten jest sumą rozłączną pewnej liczby klas abstrakcji relacji podobieństwa na zbiorze $M_n(K)$. Nie należą tu nigdy (dla $n > 1$) wszystkie klasy, ale pokazaliśmy na wykładzie, że zbiór ten jest stosunkowo złożony. Okazuje się, że suma PRZEMIENNYCH endomorfizmów diagonalizowalnych z $\text{End}(V)$ jest diagonalizowalna.

Definicja 6.9: Endomorfizmy wspólnie diagonalizowalne

Niech V będzie przestrzenią skończonego wymiaru nad ciałem K . Powiemy, że rodzina endomorfizmów $\{\phi_t \in \text{End}(V), t \in T\}$ jest **WSPÓLNIE DIAGONALIZOWALNA** nad K , jeśli istnieje baza \mathcal{A} przestrzeni V , w której dla każdego $t \in T$ macierz $M(\phi_t)_{\mathcal{A}}$ jest diagonalna (czyli \mathcal{A} to baza złożona z wektorów własnych tych ϕ_t).

Naszym celem jest dowód zaskakującego twierdzenia.

Twierdzenie 6.4

Niech V będzie przestrzenią skończonego wymiaru nad ciałem K oraz niech $\{\phi_t \in \text{End}(V), t \in T\}$ będzie rodziną endomorfizmów **diagonalizowalnych**. Następujące warunki są równoważne:

- (1) Dowolne dwa elementy rodziny $\{\phi_t \in \text{End}(V), t \in T\}$ są przemiennie.
- (2) Rodzina $\{\phi_t \in \text{End}(V), t \in T\}$ jest **wspólnie diagonalizowalna**.

Typowym przykładem przemiennych rodzin są elementy algebry endomorfizmu, która jest przemienna. Innymi słowy dla dowolnych wielomianów $w, v \in K[\lambda]$ oraz endomorfizmu ϕ mamy równość:

$$w(\phi) \circ v(\phi) = v(\phi) \circ w(\phi) = vw(\phi).$$

Oczywiście nie zawsze te endomorfizmy przemiennie muszą być diagonalizowalne (to zależy od ϕ). Ciekawym przykładem rodziny przemiennych macierzy diagonalizowalnych są tak zwane macierze cykliczne.

Definicja 6.10: Macierze cykliczne rozmiaru n

Dla dowolnych $a_0, \dots, a_{n-1} \in K$ macierz rozmiaru n o wyrazach z K postaci

$$C(a_0, \dots, a_{n-1}) = \begin{bmatrix} a_0 & a_1 & a_2 & \dots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \dots & a_{n-3} & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \dots & a_{n-4} & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_2 & a_2 & a_4 & \dots & a_0 & a_1 \\ a_1 & a_2 & a_3 & \dots & a_{n-1} & a_0 \end{bmatrix}.$$

nazywamy macierzą cykliczną rozmiaru n nad K . Zbiór takich macierzy oznaczamy jako $Cykl_n(K)$.

Zachęcam do sprawdzenia co robi macierz cykliczna z wektorem o współrzędnych będących kolejnymi pierwiastkami stopnia n z 1. Jak się okazuje istnieje taka macierz $P \in M_n(K)$, że dla dowolnych $a_0, \dots, a_{n-1} \in K$ mamy $C(a_0, \dots, a_{n-1}) = w(P)$, dla pewnego wielomianu $w \in K[\lambda]$. Wniosujemy stąd, że $Cykl_n(K)$ to podprzestrzeń liniowa w $M_n(K)$, że iloczyn macierzy z $Cykl_n(K)$ jest w $Cykl_n(K)$ oraz, że mnożenie macierzy w $Cykl_n(K)$ jest przemiennie. Jak to pokazać?

Rzeczywiście, rozważmy endomorfizm $\phi \in \text{End}(K^n)$ zadany na bazie standardowej wzorem $\phi(\epsilon_i) = \epsilon_{n-1}$, przy czym $\phi(\epsilon_1) = \epsilon_n$. Niech P będzie macierzą tego endomorfizmu w bazie standardowej:

$$P = M(\phi)_{st}^{st} = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{bmatrix}.$$

Zachęcam Czytelnika do sprawdzenia jak zachowują się endomorfizmy ϕ^i i do wywnioskowania, że dla $f(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} \in K[x]$ mamy $f(P) = C(a_0, \dots, a_{n-1})$. Okazuje się, że macierze cykliczne są wspólnie diagonalizowalne nad \mathbb{C} , a ich wartościami własnymi są pierwiastki stopnia n z 1.

Dowód Twierdzenia 6.3 zaczniemy od następującej obserwacji.

Obserwacja 6.4

Jeśli endomorfizm $\phi : V \rightarrow V$ jest diagonalizowalny i W jest podprzestrzenią ϕ -niezmienniczą przestrzeni V , to endomorfizm $\phi|_W : W \rightarrow W$ jest również diagonalizowalny.

Dowód. Niech $\lambda_1, \dots, \lambda_r$ będą parami różnymi wartościami własnymi ϕ . Wynika stąd, że V jest sumą prostą podprzestrzeni własnych $V_{(\lambda_i)}$, zatem dla każdego $w \in W$ możemy zapisać

$$w = v_1 + \dots + v_r, \text{ gdzie } v_i \in V_{(\lambda_i)}. \quad (\dagger)$$

Pokazujemy, że $v_i \in W$, co będzie oznaczało, że $W = W_1 \oplus \dots \oplus W_r$, gdzie $W_i = V_{(\lambda_i)} \cap W$. Oczywiście dla $i \neq j$ mamy $W_i \cap W_j = \{0\}$.

Weźmy najmniejsze r takie, że dla pewnego w w rozkładzie (\dagger) pewne v_i nie należy do W . Mamy

$$\phi(w) - \lambda_1 w = (\lambda_2 - \lambda_1)v_2 + \dots + (\lambda_k - \lambda_1)v_k \in W.$$

Z minimalności r mamy $(\lambda_i - \lambda_1)v_i \in W$, dla $1 < i < k$. Ale $\lambda_i - \lambda_1 \neq 0$, czyli $v_2, \dots, v_r \in W$. Na mocy (\dagger) także $v_1 \in W$. Dostaliśmy zatem sprzeczność z wyborem w . Stąd W jest sumą prostą W_i , czyli $\phi|_W$ jest diagonalizowalny. \square

Przechodzimy do dowodu implikacji $(1) \Rightarrow (2)$. Zaczniemy od sytuacji, gdy $T = \{1, 2, \dots, r\}$ jest zbiorem skończonym. Stosujemy indukcję po r . Dla $r = 1$ teza jest jasna. Załóżmy więc, że $r \geq 2$.

Skoro ϕ_r jest diagonalizowalny, to V jest sumą prostą podprzestrzeni własnych $V_{(\lambda)}$ względem ϕ_r , gdzie λ to wartość własna ϕ_r . Dla $i \neq r$ mamy $\phi_i \circ \phi_r = \phi_r \circ \phi_i$, zatem jeśli $v \in V_{(\lambda)}$, to

$$\phi_r(\phi_i(v)) = \phi_i(\phi_r(v)) = \phi_i(\lambda v) = \lambda \cdot \phi_i(v).$$

Zatem $V_{(\lambda)}$ jest ϕ_i -niezmiennicza ($v \in V_{(\lambda)} \Rightarrow \phi_i(v) \in V_{(\lambda)}$). Oczywiście endomorfizmy $\phi_1|_{V_{(\lambda)}}, \dots, \phi_{r-1}|_{V_{(\lambda)}}$ są przemienne. Zatem z powyższej Obserwacji pomocniczej każde z tych przekształceń jest diagonalizowalne. Z założenia indukcyjnego endomorfizmy te są wspólnie diagonalizowalne przez pewną bazę \mathcal{A}_λ przestrzeni $V_{(\lambda)}$ (czyli $\phi_r|_{V_{(\lambda)}}$ też się w niej diagonalizuje). Skoro $V = V_{(\lambda_1)} \oplus \dots \oplus V_{(\lambda_r)}$, gdzie λ_i to wartości własne ϕ_i , to biorąc bazę $(\mathcal{A}_{(\lambda_1)}, \dots, \mathcal{A}_{(\lambda_r)})$ przestrzeni V dostajemy wspólną bazę wektorów własnych dla wszystkich ϕ_i , dla $i = 1, \dots, r$. To kończy krok indukcyjny i dowód dla zbiorów skończonych.

Przypadek ogólny jest teraz oczywisty. niech $U = \text{lin}(\{\phi_t \in \text{End}(V), t \in T\}) \subseteq \text{End}(V)$. Skoro $\text{End}(V)$ jest skończenie wymiarowa, to U też. A zatem wspólna diagonalizowalność rodziny U zależy jedynie od tego, czy wspólnie diagonalizowalne są jej elementy bazowe, których jest skończenie wiele.

Dowód implikacji $(2) \Rightarrow (1)$. Załóżmy, że dla $A, B \in M_n(K)$ istnieje macierz odwracalna P , że

$$P^{-1}D_1P = A, \quad P^{-1}D_2P = B,$$

gdzie D_1, D_2 są diagonalne. Jest jasne, że $D_1D_2 = D_2D_1$, zatem

$$\underbrace{(P^{-1}D_1P)}_A \underbrace{(P^{-1}D_2P)}_B = P^{-1}D_1D_2P = P^{-1}D_2D_1P = \underbrace{(P^{-1}D_2P)}_B \underbrace{(P^{-1}D_1P)}_A.$$

Uwaga. Bardzo ważny w algebrze jest również problem wspólnej triangulizowalności. Można pokazać, że endomorfizmy triangulizowalne są wspólnie triangulizowalne, gdy są przemienne, ale odwrotna implikacja nie zachodzi! Wspólna triangulizowalność zachodzi w wielu innych sytuacjach i prowadzi do ważnych twierdzeń (patrz H. Radjavi, P. Rosenthal, *Simultaneous Triangularization*, Springer, 2014).

Obserwacja 6.5

Niech A_1, A_2, \dots, A_k będą przemiennymi macierzami rozmiaru $n \times n$ nad ciałem algebraicznie domkniętym F . Wówczas A_1, A_2, \dots, A_k są jednocześnie triangulizowalne, tzn. istnieje macierz odwracalna $C \in M_n(F)$ taka, że $C^{-1}AC$ jest górnotrójkątna, dla $i = 1, 2, \dots, k$

Powyższy fakt jest dość trudnym ćwiczeniem. Aby jednak przekonać Czytelnika, że zagadnienie to może być przydatne, przywołamy istotne zadanie związane z tak zwanymi równaniami macierzowym Sylwestera, istotnymi w wielu zastosowaniach. Wykorzystamy w jego rozwiązaniu powyższy wynik.

Zadanie 6.1. Niech F będzie ciałem algebraicznie domkniętym oraz niech $A \in M_n(F)$, $B \in M_m(F)$. Rozważmy endomorfizmy T_A, T_B przestrzeni liniowej $V = M_{n \times m}(F)$ dane wzorami:

$$T_A(X) = AX, \quad T_B(X) = XB, \quad \text{dla każdych } X \in V.$$

- Pokaż, że T_A, T_B są jednocześnie triangulizowalne.
- Pokaż, że jeśli A, B nie mają wspólnej wartości własnej, to równanie $AX - XB = C$ ma dokładnie jedno rozwiązanie $X \in M_{n \times m}(F)$.

Zanim przedstawimy dowód powiedzmy nieco o równaniu macierzowym $AX - XB = C$. Do równań macierzowych można podchodzić w języku endomorfizmów i wartości własnych. Jednoznaczność rozwiązania prostego równania postaci $AX = Y$ lub $XB = Y$ wymaga, aby A (odpowiednio B) było macierzą odwracalną, a więc by jej wartości własne nie były zerowe. Odpowiada to intuicji ze świata równań: równanie $ax = y$ ma rozwiązanie tylko, gdy $a \neq 0$ (nad ciałem). Analogia ta przenosi się na równania $AX - XB = Y$. Gdybyśmy mieli do rozwiązania równanie $ax - xb = y$, wówczas jest ono jednoznaczne gdy $a - b \neq 0$. Podobnie, gdyby macierze A, B były diagonalne, wówczas równanie to ma jednoznaczne rozwiązanie $X = [x_{ij}]$ postaci $x_{ij} = y_{ij}/(\lambda_i - \mu_j)$, zakładając, że $\lambda_i - \mu_j \neq 0$, dla wszystkich $i, j \neq 0$, gdzie $Y = [y_{ij}]$, zaś na diagonalach A, B są odpowiednio λ_i oraz μ_j . Wszystko to można przetłumaczyć też tak: równanie $AX - XB$ mają jednoznaczne rozwiązanie, gdy A, B nie mają wspólnej wartości własnej. Cud polega na tym, że A oraz B wcale nie muszą być diagonalizowalne.

ROZWIĄZANIE.⁷ Najpierw udowodnimy, że T_A, T_B są jednocześnie triangulizowalne. Z Obserwacji 6.5 wynika, że wystarczy pokazać, iż są one przemienne (jesteśmy nad ciałem algebraicznie domkniętym). Dla każdego $X \in M_{n \times m}(F)$ mamy jednak

$$T_A(T_B(X)) = T_A(XB) = AXB = T_B(AX) = T_B(T_A(X)),$$

bo mnożenie macierzy jest łączne, a to kończy dowód jednoczesnej triangulizowalności.

Niech $T \in \text{End}(V)$ będzie dane wzorem $T = T_A - T_B$, zaś $\mathcal{A} = \{\alpha_1, \dots, \alpha_{nm}\}$ będzie taką bazą przestrzeni V , w której zarówno macierz T_A , jak i macierz T_B mają postać górnotrójkątną (z poprzedniego akapitu wiemy, że takowa istnieje). Niech

$$M(T_A)_{\mathcal{A}}^{\mathcal{A}} = \begin{bmatrix} a_1 & * & \dots & * \\ 0 & a_2 & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_{nm} \end{bmatrix}, \quad M(T_B)_{\mathcal{A}}^{\mathcal{A}} = \begin{bmatrix} b_1 & * & \dots & * \\ 0 & b_2 & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & b_{nm} \end{bmatrix},$$

gdzie $a_i, b_i \in F$, zaś $*$ oznaczają dowolne elementy F . Wówczas

$$M(T)_{\mathcal{A}}^{\mathcal{A}} = M(T_A - T_B)_{\mathcal{A}}^{\mathcal{A}} = M(T_A)_{\mathcal{A}}^{\mathcal{A}} - M(T_B)_{\mathcal{A}}^{\mathcal{A}} = \begin{bmatrix} a_1 - b_1 & * & \dots & * \\ 0 & a_2 - b_2 & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_{nm} - b_{nm} \end{bmatrix}.$$

⁷Autorem tego ładnego rozwiązania jest Mieszko Grodzicki.

Pokażemy, że dla $i = 1, 2, \dots, nm$ mamy $a_i - b_i \neq 0$. Załóżmy w tym celu nie wprost, że $a_i = b_i$ dla pewnego $1 \leq i \leq nm$. Oznaczmy $c = a_i = b_i$. Zauważmy, że

$$\begin{aligned} w_{T_A}(\lambda) &= (a_1 - \lambda)(a_2 - \lambda)\dots(a_{nm} - \lambda), \\ w_{T_B}(\lambda) &= (b_1 - \lambda)(b_2 - \lambda)\dots(b_{nm} - \lambda), \end{aligned}$$

zatem c jest wartością własną zarówno T_A , jak i T_B . Istnieją więc niezerowe macierze $K, L \in M_{n \times m}(F)$ takie, że

$$\begin{aligned} T_A(K) &= cK, & T_B(L) &= cL, \\ AK &= cK, & LB &= cL. \end{aligned}$$

W szczególności, jeśli przez k, l oznaczymy odpowiednio dowolną niezerową kolumnę K i dowolny niezerowy wiersz L (istnieją, skoro K, L są niezerowe), to

$$Ak = ck, \quad lB = cl.$$

Z pierwszej równości wynika, że c jest wartością własną macierzy A . Z drugiej dostajemy

$$B^T l^T = (lB)^T = (cl)^T = c \cdot l^T,$$

czyli c jest wartością własną macierzy B^T . Ale to oznacza, że jest też wartością własną macierzy B , ponieważ $w_B(\lambda) = \det(B - \lambda I) = \det(B - \lambda I)^T = \det(B^T - \lambda I) = w_{B^T}(\lambda)$. To jest jednak wbrew założeniu, że A i B nie mają wspólnej wartości własnej. Otrzymana sprzeczność kończy dowód tego, że $a_i - b_i \neq 0$ dla każdego $i = 1, 2, \dots, nm$.

Wiemy więc, że macierz $M(T)_{\mathcal{A}}^{\mathcal{A}}$ jest górnotrójkątna, a na przekątnej ma wszystkie wyrazy różne od 0. To oznacza, że $r(M(T)_{\mathcal{A}}^{\mathcal{A}}) = nm$, czyli macierz ta jest odwracalna, a więc T jest izomorfizmem przestrzeni V . Wobec tego dla dowolnego $C \in V$ istnieją dokładnie jedno takie $X \in V$, że $T(X) = C$, czyli dokładnie jedno rozwiązanie równania $AX - XB = C$. ■

Równanie Sylwestera stosować można choćby do badania podobieństwa macierzy blokowych. Rozważmy macierze blokowe rozmiaru $2n \times 2n$ o blokach $n \times n$ postaci:

$$\begin{bmatrix} A & C \\ 0 & B \end{bmatrix}, \quad \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}.$$

Kiedy takie dwie macierze blokowe są podobne? Zauważmy, że dla dowolnej macierzy $X \in M_n(K)$ mamy:

$$\begin{bmatrix} I & X \\ 0 & I \end{bmatrix}^{-1} = \begin{bmatrix} I & -X \\ 0 & I \end{bmatrix}.$$

A zatem dwie macierze blokowe wyżej będą podobne, jeśli znajdziemy X spełniające:

$$\begin{bmatrix} A & C \\ 0 & B \end{bmatrix} \cdot \begin{bmatrix} I & X \\ 0 & I \end{bmatrix} = \begin{bmatrix} I & X \\ 0 & I \end{bmatrix} \cdot \begin{bmatrix} A & C \\ 0 & B \end{bmatrix}.$$

Wymnażając te macierze dostajemy cztery równości, z których tylko jedna nie jest automatycznie spełniona: $AX + C = XB$, czyli $AX - XB = -C$. A zatem zadanie wyżej daje nam wniosek.

Wniosek 6.1

Jeśli $A, B \in M_n(K)$, gdzie K jest ciałem algebraicznie domkniętym oraz jeśli A, B nie mają wspólnych wartości własnych, to dla każdej macierzy $C \in M_n(K)$ poniższe macierze są podobne

$$\begin{bmatrix} A & C \\ 0 & B \end{bmatrix}, \quad \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}.$$

Można udowodnić, że powyższy warunek jest konieczny i wystarczający, nawet po opuszczeniu założenia, że ciało K jest algebraicznie domknięte (W. E. Roth, *The equations $AX - YB = C$ and $AX - XB = C$ in matrices*, Proc. Amer. Math. Soc. 3 (1952) 392–396).

6.4 Trivia. Twierdzenie Cayleya-Hamiltona na konkursach

Warto wspomnieć, że studenci mogą brać udział w wielu konkursach na poziomie pierwszych lat studiów matematycznych. Do najstarszych i najsłynniejszych należy amerykański Putnam, największy zasięg i globalny prestiż ma IMC (International Mathematics Competition for University Students), a nie brakuje także konkursów lokalnych. W niektórych krajach np. w Rumunii zadania z analizy matematycznej oraz algebry liniowej i abstrakcyjnej występują na najwyższych poziomach krajowej olimpiady. Zachęcam do pracy z ciekawymi problemami z tych konkursów. Potrafi to dać wiele satysfakcji — bywa i frustrujące. Zacząć można od forum AOPS: https://artofproblemsolving.com/community/c15_undergraduate_contests, ale przydatne w tym kontekście będą również książki⁸ Titu Andreescu lub Fuzhena Zhanga.

Na zawodach bardzo często korzystać należy z następującej, prostej wersji twierdzenia Cayleya-Hamiltona związanej z Obserwacją 2.2 i dotyczącej macierzy $X \in M_2(K)$, która mówi, że zachodzi równość

$$X^2 - \operatorname{tr}(X)X + \det(X)I = 0.$$

Dowód to po prostu bezpośredni rachunek. Jeśli

$$X = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

to macierz $X^2 - \operatorname{tr}(X)X + \det(X)I$ równa jest:

$$\begin{bmatrix} a^2 + bc & ab + bd \\ ac + cd & bc + d^2 \end{bmatrix} - \begin{bmatrix} (a+d)a & (a+d)b \\ (a+d)c & (a+d)d \end{bmatrix} + \begin{bmatrix} ad - bc & 0 \\ 0 & ad - bc \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Oto trzy przykładowe zadania, gdzie wykorzystywany jest powyższy fakt. Są to niestandardowe problemy konkursowe, zwłaszcza zadanie drugie, ale warto docenić jak sprytnie korzysta się ze znanych nam faktów (nie tylko z tego semestru).

ZADANIE 1. Niech $A, B \in M_2(K)$, gdzie $\det A = \det B = 1$. Pokaż, że

$$\operatorname{tr}(AB) - \operatorname{tr}(A)\operatorname{tr}(B) + \operatorname{tr}(AB^{-1}) = 0.$$

ROZWIĄZANIE. Z twierdzenia wyżej mamy

$$B^2 - (\operatorname{tr} B)B + I_2 = 0,$$

co po przemnożeniu przez AB^{-1} z lewej daje

$$AB - \operatorname{tr}(B)A + AB^{-1} = 0. \quad (\dagger)$$

Teraz trzeba zauważyć, że dla dowolnych macierzy kwadratowych $X, Y \in M_n(K)$ oraz $\lambda \in K$ mamy

$$\operatorname{tr}(X + Y) = \operatorname{tr}(X) + \operatorname{tr}(Y) \quad \text{oraz} \quad \operatorname{tr}(\lambda X) = \lambda \operatorname{tr}(X).$$

Zatem obkładając równość (\dagger) funkcją tr otrzymujemy tezę. ■

ZADANIE 2. Pokaż, że $\det(X) = 0$, gdzie $X \in M_2(\mathbb{R})$ spełnia, dla pewnego całkowitego $n > 2$, równanie:

$$X^n + X^{n-2} = \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}.$$

Pokaż, że istnieje tylko jedna macierz $X \in M_2(\mathbb{Z}_5)$ taka, że:

$$X^5 = \begin{bmatrix} 4 & 2 \\ 4 & 1 \end{bmatrix}.$$

ROZWIĄZANIE. Pierwsza część zadania dotyczy teorii wyznaczników, ale jest bardzo interesująca i użyjemy w niej twierdzenia Cayleya-Hamiltona. Aby pokazać, że $\det(X) = 0$ obłożymy wyjściową równość wyznacznikiem. Mamy:

$$\det(X^n + X^{n-2}) = \det(X)^{n-2} \det(X^2 + I) = 0.$$

⁸T. Andreescu, *Essential Linear Algebra with Applications. A Problem-Solving Approach*, Birkhauser, 2014; F. Zhang, *Linear Algebra. Challenging Problems for Students* (2nd ed.), Johns Hopkins Studies in the Mathematical Sciences, 1996.

Jeśli jednak $\det(X^2 + I) = 0$, to przechodząc do wielomianów zespolonych mamy: $\det(X - iI) \det(X + iI)$. A zatem i lub $-i$ są wartościami własnymi X . To jednak oznacza, że obydwie te liczby są pierwiastkami wielomianu charakterystycznego X , który jest rzeczywisty. Wielomian ten ma stopień 2, a więc musi mieć postać $\lambda^2 + 1$. Stąd jednak mielibyśmy, na mocy twierdzenia Cayleya-Hamiltona, $X^2 + I = 0$, co znaczyłoby, że lewa strona wyjściowego równania to macierz 0, co jest niemożliwe.

Uwaga. Teraz możliwe jest rozwiązanie wyjściowego równania (zadanie pochodzi z Olimpiady w Rumunii). Otóż stwierdzamy, że wobec $\det(X) = 0$ wielomian charakterystyczny macierzy X ma postać $\lambda^2 - \text{tr}(X)\lambda$, czyli na mocy tw. C-H mamy $X^2 = \text{tr}(X)X$. Zatem mamy: $X^n + X^{n-2} = (\text{tr}(X)^{n-1} - \text{tr}(X)^{n-3})X$. Przechodzimy do śladu macierzy po obydwu stronach. Po lewej ślad wynosi 2 (patrz wyjściowe równanie), a po prawej jest to oczywiście $\text{tr}(X)^n - \text{tr}(X)^{n-2}$. A zatem liczba $\text{tr}(X)$ jest pierwiastkiem wielomianu $x^n + x^{n-2} - 2$. Teraz już przechodzimy do analizy. Dla n parzystego okazuje się, że $\text{tr}(X)$ może być równe jedynie -1 oraz 1 (dlaczego?). Dla n nieparzystych jedynym zerem rozważanego wielomianu jest 1 . A zatem wyznaczyliśmy ślad i wyznacznik macierzy X , co daje trzy rozwiązania wyjściowego równania.

Przechodzimy do części drugiej. Rozwiążemy zadanie na trzy sposoby.

Sposób 1. Zauważmy, że ślad i wyznacznik macierzy $A = \begin{bmatrix} 4 & 2 \\ 4 & 1 \end{bmatrix}$ to odpowiednio: 0 oraz 1. Szukamy macierzy rozmiaru 2×2 , która w piątej potędze ma taki ślad i wyznacznik. To oznacza, na mocy twierdzenia Cayleya-Hamiltona, że

$$(X^5)^2 + I = 0.$$

Zatem $A^2 + I = 0$. Czyli $A^5 = A$. Zatem A jest rozwiązaniem postawionego równania. Zauważmy dalej, że $\det X^5 = 1$, a równanie $x^5 = 1$ ma w \mathbb{Z}^5 jedynie rozwiązanie $x = 1$. Zatem równanie Cayleya-Hamiltona dla macierzy X ma postać: $X^2 - \text{tr}(X)X + I = 0$. Podnosimy całość do potęgi piątej:

$$X^{10} = (\text{tr}(X) - I)^5,$$

co nad ciałem \mathbb{Z}_5 jest równe po prostu $\text{tr}(X)^5 X - I$ (bo I jest przemienna z X oraz zachodzi cudowna tożsamość $(x+y)^5 = x^5 + y^5$). Co więcej, w ciele \mathbb{Z}^5 mamy $x^5 = x$, więc tak naprawdę $X^{10} = \text{tr}(X)X - I$. Ale przecież $X^{10} = A^2 = -I$, czyli $\text{tr}(X)X = 0$, co oznacza $\text{tr}(X) = 0$. A zatem $X^2 = -I$, czyli $X^5 = X = A$.

Sposób 2. Biorąc $m = \text{tr}(X)$, iterujemy trzykrotnie znane nam równanie $X^2 - mX + I = 0$ dostając:

$$X^5 = X^3(mX - I) = mX^4 - X^3 = mX^2(mX - I) - X(mX - I) = \dots = (m^4 - 3m^2 + 1)X - (m^3 - 2m)I. \quad (\dagger)$$

Przechodzimy do śladu macierzy po obydwu stronach. Mamy

$$\text{tr}(X^5) = m(m^4 - 3m^2 + 1) - 2(m^3 - 2m) = m^5 = m,$$

skąd $m = 0$ (wiemy ile wynosi ślad X^5). Zatem wracając do (\dagger) mamy $X^5 = X$, czyli $X = A$.

Sposób 3. Skoro A spełnia wyjściowe równanie to można pokazać, że dowolne inne rozwiązanie X musi mieć te same wartości własne, co macierz A (stwierdzamy najpierw, że X ma te same wartości własne, co X^5). Ale A ma dwie różne wartości własne: 2, 3. A zatem X musi być również diagonalizowalna. Natomiast dla macierzy diagonalizowalnej X nad \mathbb{Z}_5 mamy $X^5 = X$, co daje znowu $X = A$. ■

ZADANIE 3. Niech $A, B \in M_2(\mathbb{R})$ spełniają warunek

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

Wyznacz $((BA)^{-1} + BA)^{2019}$.

ROZWIĄZANIE. Korzystając z faktu, że dla dowolnych macierzy kwadratowych X, Y zachodzą równości $\text{tr}(XY) = \text{tr}(YX)$, $\det(XY) = \det(YX)$ widzimy, że

$$\text{tr}(BA) = \text{tr}(AB) = 3, \quad \det(BA) = \det(AB) = 1.$$

Zatem na mocy twierdzenia Cayleya-Hamiltona:

$$(BA)^2 - 3(BA) + I = 0.$$

Mnożąc uzyskaną równość przez $(BA)^{-1}$ dostajemy:

$$BA + (BA)^{-1} = 3I. \quad \blacksquare$$

Rozdział 7

Przestrzenie afiniczne w przestrzeniach liniowych

Tym wykładem¹ rozpoczynamy nowy etap poznawania geometrii z punktu widzenia algebry związany z tzw. przestrzeniami afinicznymi. Wśród wielu alternatywnych podejść do tego tematu realizujemy najpierw najbardziej elementarny, polegający na wzbogaceniu struktury przestrzeni liniowych dodatkową operacją. Przypisywać ona będzie każdej parze wektorów (v, w) nowy wektor: $w - v$, który oznaczamy będziemy jako \vec{vw} . Wydaje się to na pierwszy rzut oka banalne, a jednak doprowadzi do nowego spojrzenia na geometrię choćby przestrzeni K^n , gdzie K jest ciałem. Struktura afiniczna pozwoli na mówienie o punktach, prostych, czy trójkątach, a także na interpretację znanych pojęć odległości czy równoległości. Zobaczymy też, że ów nowy typ struktury na przestrzeni liniowej pozwala badać nie tylko jej podprzestrzenie liniowe, ale także podzbiory będące zbiorami rozwiązań układów niejednorodnych, traktując je jako tzw. podprzestrzenie afiniczne. Gdy oswoimy się z nowym językiem na gruncie przestrzeni liniowych, poznamy również aksjomatykę przestrzeni afinicznych, obejmującą nie tylko podzbiory przestrzeni liniowych z dodatkową strukturą.²

Definicja 7.1: Wektor łączący

Niech V będzie przestrzenią liniową nad ciałem K . Wartość funkcji $\omega : V \times V \rightarrow V$ przypisującej parze (α, β) wektor

$$\omega(\alpha, \beta) = \beta - \alpha,$$

nazywamy WEKTOREM ŁĄCZĄCYM α z β , albo krócej WEKTOREM OD α DO β i oznaczamy jako $\vec{\alpha\beta}$.

Zauważmy, że zbiór „wektorów łączących” w przestrzeni V pokrywa się po prostu ze zbiorem elementów V . O co więc tu chodzi? Po co nam taka dodatkowa kopia V ? Pierwsza motywacja jest następująca: rozróżnienie to jest wygodne dla opisu zbiorów rozwiązań układów równań niejednorodnych.

Z pierwszego semestru pamiętamy, że jeśli U jest układem niejednorodnym równań liniowych, a U' odpowiadającym mu układem jednorodnym, to zbiór rozwiązań układu U jest postaci

$$H = v + W = \{v + w \mid w \in W\},$$

gdzie v jest pewnym wektorem z V spełniającym U oraz W jest przestrzenią rozwiązań układu jednorodnego U' . Pamiętajmy, że zbiór H nie jest podprzestrzenią liniową, o ile $v \neq 0$. Używając języka wprowadzonego wyżej możemy powiedzieć, że zbiór rozwiązań układu U to

$$\{v + \vec{vw} \mid w \in H\}.$$

Po co nam taki opis?

¹Ostatnia aktualizacja: 14.05.2023 r.

²Pod względem koncepcyjnym jest to stosunkowo skomplikowany temat, a powodów należałoby zapewne szukać w niezwykle skomplikowanej historii geometrii. Choć sam język mówiący o przestrzeniach afinicznych jest bardzo elegancki, to ustępuje jak się wydaje pod względem znaczenia językowi, który poznał Państwo na Topologii, mówiąc o przestrzeniach metrycznych. Niemal każdy podręcznik algebry liniowej podchodzi do tematu przestrzeni afinicznych nieco inaczej. Zasadniczo opieramy się – jak wcześniej – na podejściu ze skryptu wydziałowego „Wykłady z algebry liniowej II”

PRZYKŁAD. Rozwiązaniem równania

$$x_1 + x_2 + x_3 = 3$$

w \mathbb{R}^3 jest np. zbiór

$$(3, 0, 0) + \text{lin}((0, 1, -1), (-1, 0, 1)).$$

Jest to zbiór wektorów łączących wektor $(3, 0, 0)$ oraz dowolny wektor z $\text{lin}((0, 1, -1), (-1, 0, 1))$. Dlaczego „na przykład”? Nie jest to bowiem jedyny opis. Rozwiązania układu U można także opisać jako zbiór

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

Po prostu wybieramy inne rozwiązanie układu U . Oczywiście dowolne dwa rozwiązania układu U wyznaczają pewien wektor łączący należący do $\text{lin}((0, 1, -1), (-1, 0, 1))$. Prowadzi to do następującej definicji.

Definicja 7.2: Warstwa podprzestrzeni

Niech W będzie podprzestrzenią przestrzeni liniowej V nad ciałem K i niech $\alpha \in V$. Zbiór

$$\alpha + W = \{\alpha + \gamma, \gamma \in W\}$$

nazywamy WARSTWĄ PODPRZESTRZENI W w przestrzeni V .

Obserwacja 7.1

Niech W będzie podprzestrzenią przestrzeni liniowej V i niech $\alpha, \beta \in V$. Wówczas:

- (i) $\alpha + W = \beta + W \Leftrightarrow \alpha - \beta \in W$,
- (ii) $(\alpha + W) \cap (\beta + W) \neq \emptyset \Leftrightarrow \alpha + W = \beta + W$.

Dowód. Dowiedzimy (i). Jeśli $\alpha + W = \beta + W$, to $\alpha \in \beta + W$, więc $\alpha = \beta + \gamma$, dla pewnego $\gamma \in W$. Zatem $\alpha - \beta \in W$. Na odwrót: jeśli $\alpha - \beta = \gamma \in W$, to $\alpha = \beta + \gamma$. Wówczas dla każdego $\gamma' \in W$ mamy

$$\alpha + \gamma' = \beta + \gamma + \gamma' \in \beta + W,$$

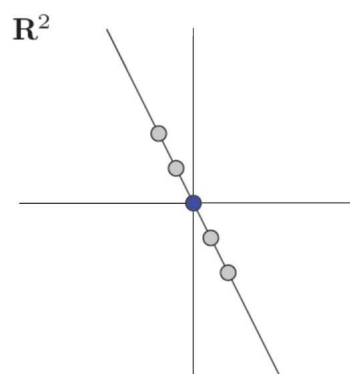
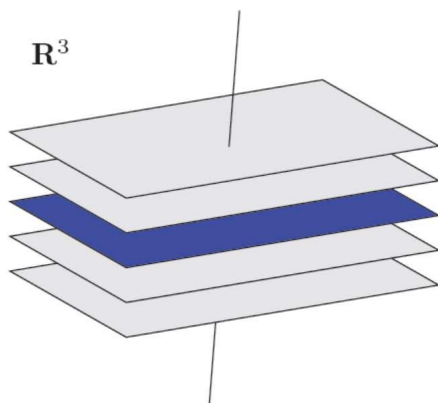
bo $\gamma + \gamma' \in W$. Stąd $\alpha + W \subseteq \beta + W$. Analogicznie dowodzimy $\beta + W \subseteq \alpha + W$.

Dowodzimy (ii). Niech $(\alpha + W) \cap (\beta + W) \neq \emptyset$. Zatem istnieje $\delta \in (\alpha + W) \cap (\beta + W)$. Stąd

$$\alpha + \gamma_1 = \delta = \beta + \gamma_2,$$

dla pewnych $\gamma_1, \gamma_2 \in W$. Wówczas $\alpha - \beta = \gamma_2 - \gamma_1 \in W$, więc na mocy (i) mamy $\alpha + W = \beta + W$. \square

Wniosek z punktu (i) jest taki, że dwie warstwy $\alpha + W, \beta + W$ podprzestrzeni W są równe wtedy i tylko wtedy, gdy $\vec{\beta\alpha}$ należy do W .



Warstwy podprzestrzeni wymiaru 2 w \mathbb{R}^3 interpretować będziemy w postaci równoległych płaszczyzn. Warstwy podprzestrzeni wymiaru 0 w \mathbb{R}^2 interpretować będziemy jako punkty. W pokazanym przypadku punkty te należą akurat do wybranej prostej.

Obserwacja 7.2

Podzbiór $H \subseteq K^n$ jest warstwą podprzestrzeni $W \subseteq K^n$ wtedy i tylko wtedy,^a gdy H jest zbiorem rozwiązań niesprzecznego układu równań liniowych o n niewiadomych i współczynnikami w K .

^aTo był jeden z punktów twierdzenia Kroneckera-Capellego.

Co to wszystko ma wspólnego z dodatkową strukturą wektorów łączących wprowadzoną na początku wykładu? Otóż warstwa nie jest sama w sobie podprzestrzenią liniową, ale jest zamknięta na operację ω , którą wprowadziliśmy w V .

Definicja 7.3: Przestrzeń afiniczna, przestrzeń styczna, punkty

Niech V będzie przestrzenią liniową nad ciałem K .

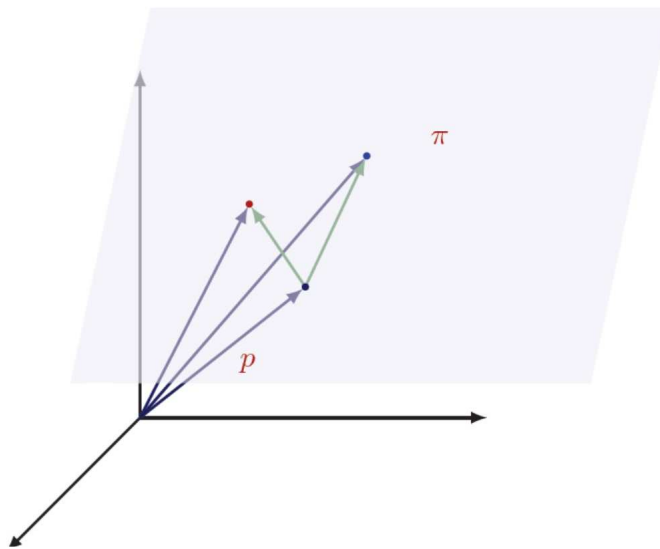
- Mówimy, że podzbiór $H \subseteq V$ jest PRZESTRZENIĄ AFINICZNĄ NAD K , jeśli H jest warstwą pewnej podprzestrzeni w V .
- Elementy przestrzeni afinicznej H nazywamy PUNKTAMI.
- Podprzestrzeń liniową W , której warstwą jest H nazywamy PRZESTRZENIĄ STYCZNĄ lub PRZESTRZENIĄ WEKTORÓW SWOBODNYCH do przestrzeni afinicznej H i oznaczamy $T(H)$.
- Mówimy, że przestrzenie afiniczne $H_1, H_2 \subseteq V$ są RÓWNOLEGŁE, jeśli $T(H_1) = T(H_2)$.

PRZYKŁADY.

- Przestrzeń liniowa V ma strukturę przestrzeni afinicznej – jest to warstwa podprzestrzeni $W = V$ postaci $0 + V$. Dla każdego $q \in V$ zbiór $\{q\}$ jest przestrzenią afiniczną jako warstwa $q + 0$.
- Zbiór $H = \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1 - x_2 = 4, x_2 - 2x_3 = 5\}$ jest przestrzenią afiniczną. Mamy

$$T(H) = \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1 - x_2 = 0, x_2 - 2x_3 = 0\} = \text{lin}((2, 2, 1)),$$

a więc $H = (11, 7, 1) + \text{lin}((2, 2, 1))$.



Komentarz. Wybierając dowolny punkt p na płaszczyźnie π (tzn. odpowiedni wektor w \mathbb{R}^3) możemy traktować π jako zbiór wektorów postaci: $p + T(\pi)$. Zbiór $T(\pi)$ składa się z wektorów swobodnych, ale można je interpretować jako wektory łączące p ze wszystkimi punktami π . Kluczowe jest to, że niezależnie od wyboru punktu p na π mamy równość $\pi = p + T(\pi)$.

Przyjmijmy umowę notacyjną. Elementy przestrzeni afinicznej W zawartej w przestrzeni liniowej V , czyli punkty, oznaczamy małymi literami naszego alfabetu, a więc p, q, r, s itd. Wektory swobodne będziemy oznaczać literami greckimi: α, β, γ itd.

Jako, że zarówno punkty jak i wektory są w istocie elementami V , to w przypadku działania w przestrzeni współrzędnych $V = K^n$ będziemy zarówno współrzędne punktów, jak i wektorów zapisywać jednakowo w okrągłych nawiasach. Stosunkowo delikatnie będziemy natomiast mówić o wykonywaniu operacji mnożenia przez skalar i dodawania wektorów, która jest w przestrzeni V . Wiąże się to z tym, że jeśli punkty p, q należą do przestrzeni afinicznej W , to ani $2p$, ani $p + q$ nie muszą do niej należeć, choć same napisy mają sens, bo działamy w przestrzeni liniowej. Musimy określić kiedy stosowanie tych operacji jest przydatne. Motywacja pochodzi z pierwszego wykładu o układach równań.

Obserwacja 7.3

Rozważmy układ m równań liniowych na zbiorze $X = \{x_1, \dots, x_n\}$ o współczynnikach w ciele K postaci:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1 \\ \dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = b_m. \end{cases}$$

Założmy, że powyższy układ nie jest jednorodny. Wówczas jeśli wektory v_0, \dots, v_s są rozwiązaniami tego układu, to dla dowolnych $t_0, \dots, t_s \in K$ kombinacja liniowa $t_0v_0 + \dots + t_s v_s$ jest rozwiązaniem tego układu wtedy i tylko wtedy, gdy $t_0 + \dots + t_s = 1$.

Dowód. Zapiszmy nasz układ w postaci macierzowej

$$A = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{bmatrix}, \quad b = \begin{bmatrix} b_1 \\ \vdots \\ v_n \end{bmatrix}.$$

Wówczas to, że v_0, \dots, v_s są rozwiązaniami powyższego układu zapisać możemy w postaci:

$$Av_0 = b, \quad \dots, \quad Av_s = b.$$

Zatem dla dowolnych $t_0, \dots, t_s \in K$ mamy:

$$A(t_0v_0 + \dots + t_s v_s) = t_0Av_0 + \dots + t_s Av_s = t_0b + \dots + t_s b.$$

Wektor $t_0v_0 + \dots + t_s v_s$ jest zatem rozwiązaniem powyższego układu równań wtedy i tylko wtedy, gdy $(t_0 + \dots + t_s)b = b$. Skoro $b \neq 0$, to zachodzi równość $t_0 + \dots + t_s = 1$. \square

Dla przykładu: wiedząc, że punkty $(1, 1)$, $(2, 3)$ są rozwiązaniami pewnego układu równań liniowych

$$a_{11}x_1 + a_{12}x_2 = b_1, \quad a_{21}x_1 + a_{22}x_2 = b_2$$

widzimy, że:

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}, \quad \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 3 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}.$$

A zatem każdy z punktów postaci $t(1, 1) + (1 - t)(2, 3)$ również jest rozwiązaniem tego układu równań.

Definicja 7.4: Kombinacja afiniczna, wagi

Niech V będzie przestrzenią liniową nad ciałem K . Dla każdych punktów $p_0, p_1, \dots, p_n \in V$ i każdych $a_0, a_1, \dots, a_n \in K$ spełniających

$$a_0 + a_1 + \dots + a_n = 1$$

sumę:

$$a_0p_0 + a_1p_1 + \dots + a_np_n \in V$$

nazywamy KOMBINACJĄ AFINICZNĄ PUNKTÓW p_0, \dots, p_n Z WAGAMI a_0, \dots, a_n .

Kombinacje afiniczne są specjalnym typem kombinacji liniowych, w których suma współczynników to 1.

Przykłady:

- Dla $V = \mathbb{R}^3$ i $p_0 = (1, 2, 1), p_1 = (1, -1, -1), p_2 = (0, 1, 3)$ mamy

$$2p_0 + 3p_1 - 4p_2 = 2(1, 2, 1) + 3(1, -1, -1) - 4(0, 1, 3) = (5, -3, -13),$$

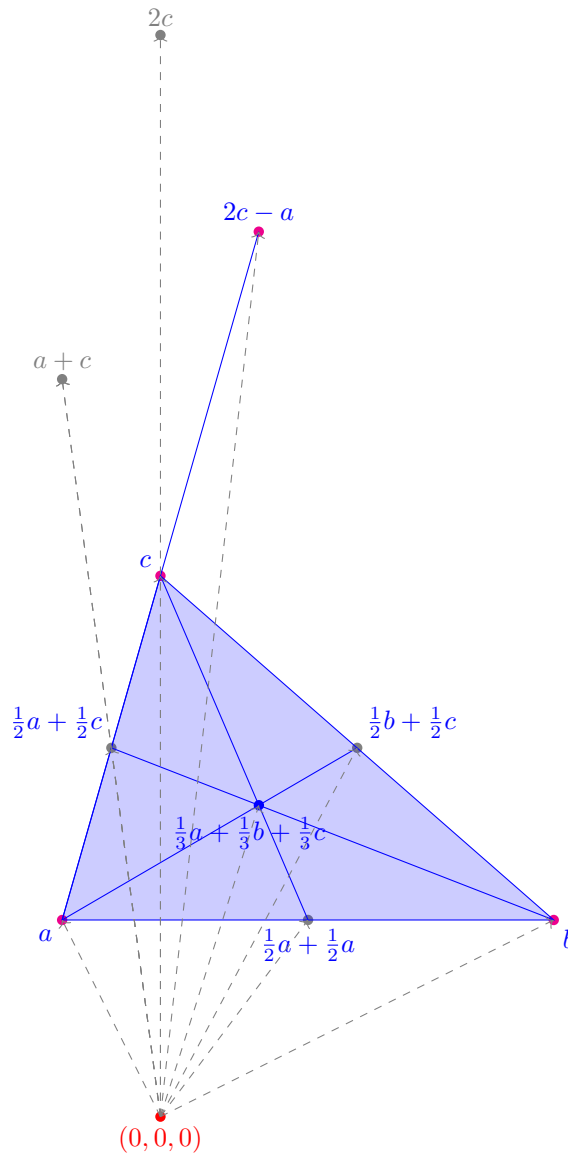
więc $p = (5, -3, -13)$ jest kombinacją afiniczną punktów p_0, p_1, p_2 z wagami 2, 3, -4.

- Dla dowolnych punktów $x, y \in V$ oraz dowolnego $\lambda \in K$ punkt $\lambda x + (1 - \lambda)y$ jest kombinacją afiniczną punktów x, y z wagami $\lambda, 1 - \lambda$. W interpretacji geometrycznej punkty te należą do prostej zawierającej punkty x i y . Gdy $K = \mathbb{R}$ oraz $\lambda \in [0, 1]$, zbiór punktów postaci $\{\lambda x + (1 - \lambda)y\}$ interpretować będziemy jako odcinek w przestrzeni afinicznej o końcach w x i y .



- Dla dowolnych punktów $p, q, r \in V$ punkt $\frac{1}{3}p + \frac{1}{3}q + \frac{1}{3}r$ jest kombinacją afiniczną punktów p, q, r . W interpretacji nad \mathbb{R} jest to środek ciężkości trójkąta o wierzchołkach w punktach p, q, r .

Spójrzmy na rysunek. Weźmy punkty a, b, c w przestrzeni afinicznej \mathbb{R}^3 (wierzchołki szarego trójkąta). Na niebiesko zaznaczone są pewne ich kombinacje afiniczne. Punkty $2c$ oraz $a + c$ nie są kombinacjami afinicznymi a, b, c , o ile $a, c \neq (0, 0, 0)$. Niebieskie odcinki oznaczają kombinacje afiniczne o dodatnich wagach (tzw. kombinacje wypukłe, mające sens nad \mathbb{R}) łączących je punktów. To co jest kluczowe to fakt, że z punktu widzenia tej konfiguracji nie ważne gdzie leży punkt $p_0 = (0, 0, 0)$, a kombinacje afiniczne (tylko one, bo liniowe – nie) punktów a, b, c są jednoznacznie wyznaczone.



Będziemy wielokrotnie korzystać z następującej obserwacji. Wyraża ona wagi a_1, \dots, a_k kombinacji afinicznej $p = a_0 p_0 + a_1 p_1 + \dots + a_k p_k$ jako współczynniki w przedstawieniu wektora $\overrightarrow{p_0 p}$ w postaci kombinacji liniowej wektorów $\overrightarrow{p_0 p_1}, \dots, \overrightarrow{p_0 p_k}$.

Obserwacja 7.4

Dla każdych $p_0, p_1, \dots, p_k, p \in V$ oraz $a_0, \dots, a_k \in K$ spełniających $a_0 + \dots + a_k = 1$ zachodzi:

$$p = a_0 p_0 + a_1 p_1 + \dots + a_k p_k \iff \overrightarrow{p_0 p} = a_1 \overrightarrow{p_0 p_1} + \dots + a_k \overrightarrow{p_0 p_k}.$$

Dowód. Jeśli $p = a_0 p_0 + \dots + a_k p_k$, to

$$\begin{aligned} \overrightarrow{p_0 p} &= p - p_0 = \\ &= a_0 p_0 + \dots + a_k p_k - p_0 = \\ &= a_0 p_0 + \dots + a_k p_k - \underbrace{(a_0 + \dots + a_k)}_1 p_0 = \\ &= a_0 (p_0 - p_0) + \dots + a_k (p_k - p_0) = \\ &= a_1 \overrightarrow{p_0 p_1} + \dots + a_k \overrightarrow{p_0 p_k}. \end{aligned}$$

Na odwrót, jeśli $\overrightarrow{p_0 p} = a_1 \overrightarrow{p_0 p_1} + \dots + a_k \overrightarrow{p_0 p_k}$, to:

$$\begin{aligned} p &= p_0 + \overrightarrow{p_0 p} \\ &= \underbrace{(a_0 + \dots + a_k)}_1 p_0 + a_1 \overrightarrow{p_0 p_1} + \dots + a_k \overrightarrow{p_0 p_k} = \\ &= a_0 p_0 + a_1 (p_0 + \overrightarrow{p_0 p_1}) + \dots + a_k (p_0 + \overrightarrow{p_0 p_k}) = \\ &= a_0 p_0 + a_1 p_1 + \dots + a_k p_k. \end{aligned}$$

□

Zauważmy, że wybór punktu p_0 w powyższej uwadze jest zupełnie arbitralny. Można zamiast niego wziąć dowolny z punktów p_1, \dots, p_k , odpowiednio modyfikując sformułowanie.

PRZYKŁAD. Dla układu punktów w \mathbb{R}^3

$$p_0 = (1, 2, 1), p_1 = (1, -1, -1), p_2 = (0, 1, 3), p = (5, -3, -13)$$

mamy $p = 2p_0 + 3p_1 - 4p_2$, a więc równoważnie $\overrightarrow{p_0 p} = 3\overrightarrow{p_0 p_1} - 4\overrightarrow{p_0 p_2}$, a także $\overrightarrow{p_1 p} = 2\overrightarrow{p_1 p_0} - 4\overrightarrow{p_1 p_2}$ oraz $\overrightarrow{p_2 p} = 2\overrightarrow{p_2 p_0} + 3\overrightarrow{p_2 p_1}$.

Omówimy teraz podstawowe własności kombinacji afinicznych.

Obserwacja 7.5

Niech q_0, \dots, q_r będzie układem punktów, z których każdy jest kombinacją afiniczną punktów p_0, \dots, p_k . Wówczas każda kombinacja afiniczna punktów q_0, \dots, q_r jest też kombinacją afiniczną punktów p_0, \dots, p_k .

Dowód. Dla każdego $i = 1, \dots, r$ mamy $q_i = a_{i0} p_0 + \dots + a_{ik} p_k$, dla pewnych wag a_{i0}, \dots, a_{ik} . Stąd dla każdego układu wag a_0, \dots, a_r otrzymujemy:

$$\begin{aligned} a_0 q_0 + \dots + a_r q_r &= a_0 (a_{00} p_0 + \dots + a_{0k} p_k) + \dots + a_r (a_{r0} p_0 + \dots + a_{rk} p_k) = \\ &= (a_0 a_{00} + \dots + a_r a_{r0}) p_0 + \dots + (a_0 a_{0k} + \dots + a_r a_{rk}) p_k \end{aligned}$$

Wystarczy pokazać, że suma współczynników występujących przy p_i w ostatnim wierszu ciągu równości powyżej wynosi 1. Mamy jednak:

$$\begin{aligned} &(a_0 a_{00} + \dots + a_r a_{r0}) + \dots + (a_0 a_{0k} + \dots + a_r a_{rk}) = \\ &a_0 \underbrace{(a_{00} + \dots + a_{0k})}_1 + \dots + a_r \underbrace{(a_{r0} + \dots + a_{rk})}_1 = \\ &a_0 + \dots + a_r = 1. \end{aligned}$$

□

Definicja 7.5: Podzbiór zamknięty ze względu na kombinacje afiniczne

Niech V będzie przestrzenią liniową nad K . Mówimy, że podzbiór $H \subseteq V$ JEST ZAMKNIĘTY ZE WZGLĘDU NA KOMBINACJE AFINICZNE, jeśli dla każdego punktu $p_0, \dots, p_k \in H$ i każdego wag a_0, \dots, a_k zachodzi $a_0 p_0 + \dots + a_k p_k \in H$.

Poniższe twierdzenie wiąże pojęcia wprowadzone na dzisiejszym wykładzie, stanowiąc jednocześnie alternatywną definicję dla przestrzeni afinicznych (jako podzbiorów przestrzeni liniowych).

Obserwacja 7.6

Niech H będzie niepustym podzbiorem przestrzeni liniowej V nad K . Następujące warunki są równoważne.

- (i) H jest zamknięty ze względu na kombinacje afiniczne,
- (ii) H jest warstwą podprzestrzeni przestrzeni V ,
- (iii) H jest przestrzenią afiniczną.

Dowód. Oczywiście równoważność (ii) i (iii) wynika z definicji przestrzeni afinicznej.

Dowodzimy (i) \Rightarrow (ii). Załóżmy, że H jest zamknięty ze względu na kombinacje afiniczne. Wybieramy $p_0 \in H$. Niech $W = \{\overrightarrow{p_0 p} \mid p \in H\}$. Wykażemy, że W jest podprzestrzenią przestrzeni V . Weźmy dowolne $\alpha_1, \alpha_2 \in W$, czyli pewne $\overrightarrow{p_0 p_1}, \overrightarrow{p_0 p_2}$, dla pewnych $p_1, p_2 \in H$. Weźmy też dowolne $a_1, a_2 \in K$. Niech $a_0 = 1 - a_1 - a_2$. Zbiór H jest zamknięty ze względu na kombinacje afiniczne, więc

$$p = a_0 p_0 + a_1 p_1 + a_2 p_2 \in H.$$

Stąd wektor $\overrightarrow{p_0 p}$ należy do W . Ale $\overrightarrow{p_0 p} = a_1 \overrightarrow{p_0 p_1} + a_2 \overrightarrow{p_0 p_2} = a_1 \alpha_1 + a_2 \alpha_2$. Stąd $a_1 \alpha_1 + a_2 \alpha_2 \in W$, co wobec dowolności $a_1, a_2, \alpha_1, \alpha_2$ dowodzi, że W jest podprzestrzenią przestrzeni V . Ponadto $H = p_0 + W$ na mocy definicji W . Zatem H jest warstwą podprzestrzeni W w V .

Dowodzimy (ii) \Rightarrow (i). Załóżmy, że $H = q + W$, dla pewnego $q \in V$ oraz pewnej podprzestrzeni W przestrzeni V . Niech $p_0, \dots, p_k \in H$ oraz $a_0, \dots, a_k \in K$, przy czym $a_0 + \dots + a_k = 1$. Wówczas $p_i = q + \alpha_i$, dla pewnych $\alpha_i \in W$, gdzie $i = 0, \dots, k$. Zatem

$$\sum_{i=0}^k a_i p_i = \sum_{i=0}^k a_i (q + \alpha_i) = \sum_{i=0}^k a_i q + \sum_{i=0}^k a_i \alpha_i = q + \gamma,$$

gdzie $\gamma = a_0 \alpha_0 + \dots + a_k \alpha_k$ jest kombinacją liniową wektorów przestrzeni W , więc należy do W . Stąd $a_0 p_0 + \dots + a_k p_k = q + \gamma \in q + W = H$. Zatem H jest zamknięty ze względu na kombinacje afiniczne. \square

Definicja 7.6: Podprzestrzeń przestrzeni afinicznej

Niech H_1, H_2 będą przestrzeniami afinicznymi w przestrzeni liniowej V . Jeśli $H_1 \subseteq H_2$, to mówimy, że H_1 jest PODPRZESTRZENIĄ PRZESTRZENI AFINICZNEJ H_2 .

Obserwacja 7.7

Niech p_0, \dots, p_k będą punktami przestrzeni afinicznej H . Wówczas zbiór wszystkich kombinacji afinicznych punktów p_0, \dots, p_k jest podprzestrzenią przestrzeni afinicznej H .

Definicja 7.7: Podprzestrzeń rozpięta na układzie punktów

Niech p_0, \dots, p_k będą punktami przestrzeni afinicznej H . Wówczas zbiór wszystkich kombinacji afinicznych punktów p_0, \dots, p_k nazywamy PODPRZESTRZENIĄ AFINICZNĄ ROZPIĘTĄ NA p_0, \dots, p_k (lub PODPRZESTRZENIĄ GENEROWANĄ przez p_0, \dots, p_k) i oznaczamy $\text{af}(p_0, \dots, p_k)$.

Podobnie jak przestrzeń liniowa może być rozpięta przez dowolny układ wektorów, podobnie i rozważać można podprzestrzenie afiniczne rozpięte przez dowolne układy punktów.

Definicja 7.8

Niech $X \subseteq V$. Przez $\text{af}(X)$ rozumiemy zbiór kombinacji afinicznych elementów zbioru X .

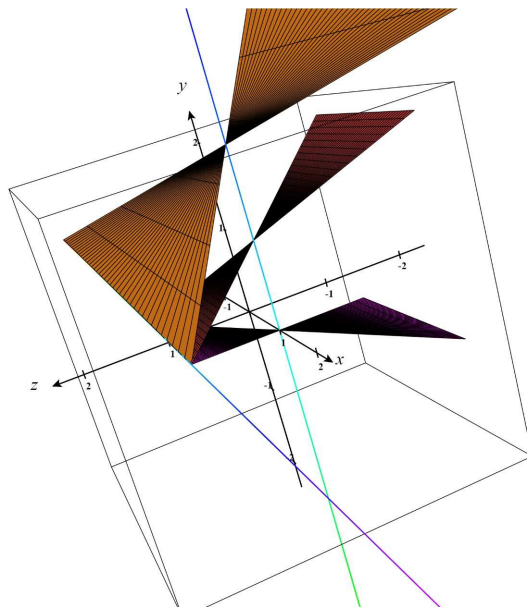
Przykłady:

- Dla dowolnej przestrzeni liniowej V mamy $\text{af}(V) = V$.
- Dla dwóch różnych punktów p, q zbiór $\text{af}(p, q)$ jest prostą.
- Rozważmy proste l_1, l_2 zadane w \mathbb{R}^3 układami postaci: $l_1 : x_1 = 0, x_2 = 0, l_2 : x_1 = 1, x_3 = 0$. Te dwie proste nie mają punktu wspólnego – są to tzw. proste skośne. Każdy punkt na prostej l_1 ma postać $(0, 0, s)$, gdzie $s \in \mathbb{R}$, a każdy punkt na l_2 ma postać $(1, t, 0)$, gdzie $t \in \mathbb{R}$. A zatem do prostych tych należą na przykład punkty $(0, 0, 0), (0, 0, 1), (1, 0, 0)$ oraz $(1, 1, 0)$. Dowolny punktu $(x, y, z) \in \mathbb{R}^3$ jest ich kombinacją afiniczną:

$$(x, y, z) = (x - y)(1, 0, 0) + y(1, 1, 0) + z(0, 0, 1) + (1 - x - z)(0, 0, 0).$$

A zatem $\text{af}(l_1 \cup l_2) = \mathbb{R}^3$.

Od razu chciałbym przestrzec Czytelnika przed różnymi uproszczeniami. Przestrzeń afiniczna rozpięta na układzie punktów nie jest tym samym co zbiór prostych łączących poszczególne punkty. Proszę rozważyć przykład, który kilka razy pojawiał się na kolokwiach. Dla podzbiorów H_1, H_2 przestrzeni afinicznej \mathbb{R}^3 definiujemy zbiór $H_3 = \{tp + (1 - t)q \mid p \in H_1, q \in H_2, t \in \mathbb{R}\}$. Wówczas dla $H_1 = (0, 0, 1) + \text{lin}((1, 0, 0))$ oraz $H_2 = (1, 0, 0) + \text{lin}((0, 1, 0))$ zbiór H_3 nie jest równy \mathbb{R}^3 , a nawet nie jest podprzestrzenią afiniczną.



Idea jest taka: wybierzmy punkt na prostej H_2 i połączmy go prostymi ze wszystkimi punktami z prostej skośnej H_1 (dla ustalonych $p \in H_1, q \in H_2$ zbiór $\{tp + (1 - t)q \mid t \in \mathbb{R}\}$ jest prostą). Dostajemy *prawie płaszczyznę* (bez jednej prostej). Można w ten sposób uzyskać *prawie wszystkie* *prawie płaszczyzny* zawierające H_1 poza jedną – równoległą do H_2 . Łącznie dostajemy \mathbb{R}^3 bez dwóch *prawie płaszczyzn*.

7.1 Zadania do samodzielnej pracy

Zadania ilustrujące umiejętności niezbędne do zaliczenia przedmiotu oznaczone są symbolem ♠. Przy tych zadaniach dodany jest opis umiejętności, które sprawdzają.

1. (♠ Rozstrzygnięcie czy podzbiór jest przestrzenią afiniczną)
 - Czy podzbiór $X = \{A \in M_n(\mathbb{R}) : \text{tr}(A) = 1\}$ jest podprzestrzenią afiniczną w $M_n(\mathbb{R})$?
 - Czy podzbiór $Y = \{w \in \mathbb{R}[x] : w(0) = 1\}$ jest podprzestrzenią afiniczną w $\mathbb{R}[x]$?
 - Niech x_1, \dots, x_n będą parami różnymi liczbami rzeczywistymi oraz c_1, c_2, \dots, c_n – dowolnymi liczbami rzeczywistymi. Czy podzbiór $Z = \{f \in F(\mathbb{R}, \mathbb{R}) : f(x_1) = c_1, \dots, f(x_n) = c_n\}$ jest podprzestrzenią afiniczną w $\mathbb{R}[x]$?
2. (♠ Sprawdzanie czy punkty są kombinacjami afinicznymi innych)
 - (a) Czy punkt $(1, 2, 1) \in \mathbb{R}^3$ jest kombinacją afiniczną punktów $(1, 0, 0), (0, 1, 0), (0, 0, 1)$?
 - (b) Dla jakich wartości $t \in \mathbb{R}$ mamy $(5, t, 4, 3) \in \text{af}((1, 0, 1, 0), (1, 1, 2, 1), (0, 1, 1, 0)) \subset \mathbb{R}^4$?
 - (c) Niech $p_0 = (1, 1, 0), p_1 = (0, 1, 2), q_0 = (3, 1, 3), q_1 = (1, 0, 1)$. Czy istnieje punkt $p \in \mathbb{R}^3$, który jest kombinacją afiniczną punktów p_0, p_1 i jest też kombinacją afiniczną punktów q_0, q_1 ?
3. (♠ Wyznaczanie warstw względem podprzestrzeni i układów równań je opisujących)
 - (a) Znajdź układ równań opisujący podprzestrzeń afiniczną
$$\text{af}((1, 0, 0, 1), (2, 1, 0, 2), (1, 1, 1, 1), (2, 2, 1, 3)) \subset \mathbb{R}^4.$$
 - (b) Znajdź układ równań liniowych, którego zbiorem rozwiązań jest warstwa podprzestrzeni
$$W = \text{lin}((1, 3, 0, 1), (2, 9, 4, 2)) \subset \mathbb{R}^4$$
zawierająca wektor $\alpha = (1, 1, -1, 2)$.
 - (c) Czy podprzestrzenie afiniczne $\text{af}((0, 1, 1), (0, 1, 2), (1, 1, 1))$ oraz $\text{af}((2, 1, 1), (0, 1, 0), (2, 1, 2))$ przestrzeni afinicznej \mathbb{R}^3 są równoległe?
 - (d) Niech $H = \text{af}((1, 1, 0), (2, 1, 1), (1, 2, 0))$. Znajdź równanie podprzestrzeni afinicznej P równoległej do H i zawierającej punkt $(-1, 2, -3)$.
 - (e) Znajdź równanie opisujące podprzestrzeń afiniczną $H \subseteq \mathbb{R}^3$ zawierającą punkt $(2, 3, 1)$ oraz taką, że $T(H) = T(P_1) \cap T(P_2)$, gdzie P_1, P_2 to podprzestrzenie afiniczne \mathbb{R}^3 dane równaniami $P_1 : -4x_1 + x_2 - 3x_3 = 1$ oraz $P_2 : -x_1 - 3x_2 + 2x_3 = 1$.
 - (f) Dane są podzbiory przestrzeni \mathbb{R}^3 postaci
$$H_1 = (1, 0, 1) + \text{lin}((1, 1, 0)) \quad \text{oraz} \quad H_2 = (1, 1, 2) + \text{lin}((1, 1, 0))$$
Wyznacz równanie podprzestrzeni afinicznej $\text{af}(H_1 \cup H_2)$.
 - (g) Niech $K = \mathbb{Z}_2$ i niech $V = K^4$. Dla $W = \text{lin}((1, 0, 1, 0), (0, 1, 1, 1)) \subseteq V$ wyznacz wszystkie warstwy podprzestrzeni W .
 - (h) Ile jest podprzestrzeni afinicznych w przestrzeni afinicznej \mathbb{Z}_p^2 ?
4. Niech $H \subseteq K^n$ będzie przestrzenią afiniczną. Czy istnieje układ równań liniowych U o n niewiadomych, taki że zbiór rozwiązań U pokrywa się z H ?
5. Niech X, Y będą podprzestrzeniami przestrzeni afinicznej H . Niech $p \in X, q \in Y$. Wykaż, że
$$\text{af}(X \cup Y) = \text{af}(p, q) + T(X) + T(Y).$$
6. W przestrzeni afinicznej K^n nad ciałem K dane są punkty

$$p_1 = (a_{11}, \dots, a_{1n}), \quad p_2 = (a_{21}, a_{22}, \dots, a_{2n}), \quad \dots \quad p_n = (a_{n1}, a_{n2}, \dots, a_{nn}).$$

Kiedy podprzestrzeń $\text{af}(p_1, p_2, \dots, p_n)$ opisana jest jednym równaniem liniowym postaci

$$\det \begin{bmatrix} 1 & x_1 & x_2 & \dots & x_n \\ 1 & a_{11} & a_{12} & \dots & a_{1n} \\ 1 & a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} = 0?$$

7.2 Uzupełnienie. Geometria afiniczna, czyli jaka?

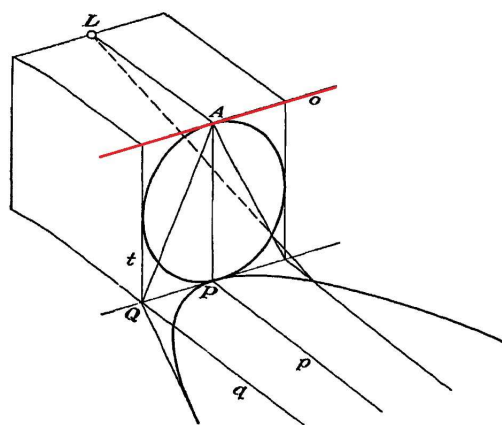
Pojęcie przestrzeni afinicznej jest na tyle istotnym i delikatnym punktem naszego programu, że warto poświęcić mu nieco mniej matematyczny fragment naszych rozważań, niebędący jednak tylko dodatkiem historycznym, ale tekstem bliższym wykładowi. Koncepcja przestrzeni afinicznej i jej związków z otaczającym nas światem jest punktem zwrotnym kursu. Zaczniemy od idei prostej, podkreślonej pięknie przez jednego z polskich autorów, Jacka Komorowskiego, w świetnej (i bardzo polecanej) książce *Od liczb zespolonych do tensorów, spinorów, algebr Liego i kwadryk*, gdzie pojawia się następujący argument³.

Nie wydaje się naturalne przyjmowanie przestrzeni wektorowej jako ośrodka, w którym będzie uprawiana geometria. Taki wybór, aczkolwiek wygodny ze względów rachunkowych, jest niefortunny ze światopoglądowego punktu widzenia; przecież w otaczającym nas świecie, którego modelem ma być geometria, brak jest np. wyróżnionego punktu, „pępka świata”, jakim w przestrzeni wektorowej jest zero.

Warto napisać kilka zdań o geometrycznych źródłach geometrii afinicznej, będących w zasadzie tłumaczeniem (bez większego komentarza) fragmentu rozważań jednego z głównych autorytetów XX-wiecznej geometrii – H. S. M. Coxetera. Pochodzą one z książki *The Real and Projective Plane*.

Zwykła geometria, którą poznawaliśmy w szkole, zajmowała się okręgami, kątami, prostymi równoległymi, trójkątami podobnymi itd., zwana jest geometrią euklidesową⁴, ponieważ została ona po raz pierwszy usystematyzowana przez Euklidesa, żyjącego ok. 300 r. p.n.e. Jego dzieło – *Elementy*, Do dziś, przy odpowiednim języku i redakcji, jest to pozycja zawierająca wzorcowe podejście ilustrującej stosowanie metody dedukcyjnej. W XIX wieku pojawiła się tendencja do wyciągania z geometrii euklidesowej pewnych fundamentalnych idei, zwłaszcza takich, które nie wymagają mierzenia odległości lub kątów, i do wykorzystywania tych idei do budowania ogólniejszych spojrzeń na geometrię.

Skąd się bierze nazwa geometrii afinicznej? Weźmy dwie figury znajdujące się na dwóch różnych płaszczyznach. Powiemy, że jedną figurę można uzyskać z drugiej przez rzut równoległy, jeśli odpowiednie punkty znajdujące się na tych figurach można połączyć za pomocą równoległych prostych. To jest ta sytuacja, która ma miejsce gdy słońce rzuca cień na ziemię, np. okrągła moneta rzuca eliptyczny cień. Jeśli dwie płaszczyzny są równoległe, dwie figury będą przystające; w przeciwnym przypadku będą miały wprawdzie nieco inne kształty, ale linie proste pozostaną proste, styczne do krzywych pozostaną stycznymi, proste równoległe pozostaną równoległe, odcinki przecięte na pół pozostaną takie po rzutowaniu itd.

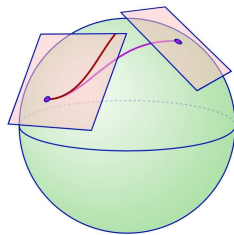


Słowo „afiniczne” (*affinis* – z łac. podobieństwo, powinowactwo) zostało użyte po raz pierwszy przez Eulera w drugim tomie *Introductio in Analysis Infinitorum* z 1748 roku, w kontekście stycznych do krzywej. Niedługo później zostało podjęte przez Möbiusa i Monge’a, który dali początek ogólniejszej teorii – geometrii rzutowej. Stawia ona mniej restrykcyjne wymagania, ograniczając się do tych własności, które nie zmieniają się przy rzucie środkowym. Tu pojawiają się dodatkowe wyzwania, bo nie każda prosta przechodzi na prostą, tak jak czerwona prosta na rysunku powyżej.

³Argument ten stosowany również przez inne nauki, na przykład fizyczne, o czym wspomina znakomity podręcznik prof. A. Herdegena z Uniwersytetu Jagiellońskiego: http://eigenspace.pl/herdegen_algebra.pdf.

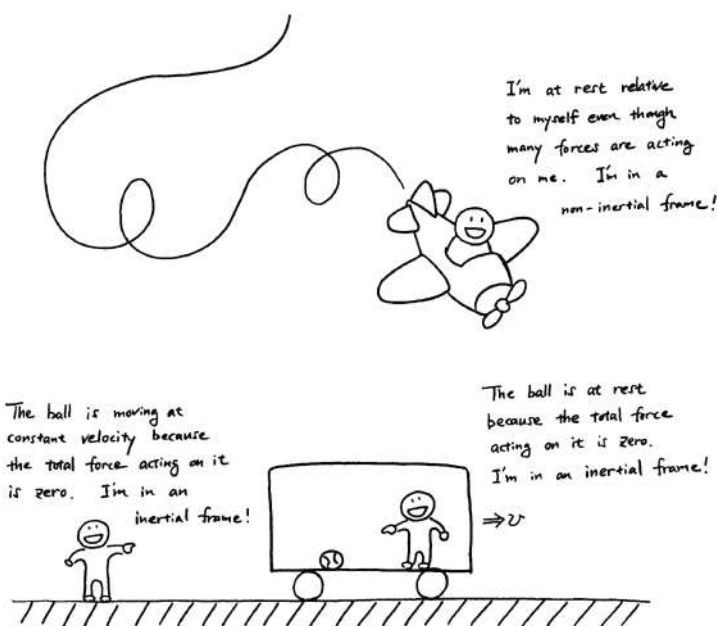
⁴Za kilka wykładów poznamy tzw. przestrzenie euklidesowe, która mają być bezpośrednim obiektem realizującym geometrię euklidesową w kontekście przestrzeni liniowych.

Na wykładzie zdefiniowaliśmy przestrzenie afiniczne będące warstwami w przestrzeniach liniowych. Jest to podejście bliskie naszej geometrycznej intuicji i dogodne w licznych zastosowaniach – nie jest ono jednak wystarczające. Jeden z powodów jest następujący: w przyszłości będziecie Państwo badać obiekty nieliniowe i ich własności przypisując im „lokalnie” pewne obiekty liniowe i afiniczne.



Nie zawsze wygodne będzie zanurzanie owych nieliniowych obiektów w przestrzeń liniową z jednym ustalonym „układem współrzędnych” i rozpatrywanie w ramach tej przestrzeni złożonych problemów analitycznych. Stąd potrzeba, by móc w jakiś alternatywny sposób określić przestrzeń afiniczną. Nakreślę dwa podstawowe podejścia prowadzące do owych alternatywnych definicji. Jedno z nich oparte jest o abstrakcyjną definicję aksjomatyczną przestrzeni afinicznej, a drugie oparte jest o ideę „obiektów niezmienniczych”. Jest to stosowny moment, by na podstawie naszych dotychczasowych doświadczeń opowiedzieć Państwu o różnych spojrzeniach na zagadnienia geometryczne. Będzie to również zapowiedź tego, że na kolejnych latach studiów matematycznych poznamy problemy geometryczne „z wyższego punktu widzenia”.

W geometrii afinicznej badamy obiekty odnoszące się silnie do „rzeczywistości”. Bardziej niż w przypadku przestrzeni liniowych, strukturze afinicznej przypisujemy miano „geometrii świata” – co prowadzi naturalnie do wielu trudnych pytań. Rzecz jasna aksjomatyka przestrzeni liniowych czerpie z intuicji fizycznych, ale pojawiają się pewne ograniczenia. Związane są one ze sformułowaną przez Galileusza tzw. *zasadą względności* mówiącą poglądowo, że prawa fizyki w dwóch inercjalnych układach odniesienia są takie same. Choć w różnych układach odniesienia prawa fizyki mają być te same, ich „postrzeganie” i „opisywanie” stawia wielkie matematyczne wyzwania. Opis zjawisk fizycznych chętnie czerpał z geometrii analitycznej Kartezjusza i Fermata, i możliwości przedstawiania obiektów w układach współrzędnych, a następnie pracowicie tworzył sposoby przechodzenia z jednego układu odniesienia do drugiego. W tym kluczu możemy między innymi interpretować przestrzeń liniowe i ich endomorfizmy – przechodząc z macierzy przekształcenia w jednej bazie do innej „zmieniamy układ odniesienia”. Zawsze jednak istniało napięcie związane z pytaniem: czy istnieje „uniwersalny układ inercjalny”, albo z jego nieprecyzyjną, ale obrazową wersją: czy ktokolwiek we Wszechświecie jest w stanie stwierdzić czy się porusza, czy nie?



Przykład. Rozważmy podzbiór P przestrzeni afinicznej \mathbb{R}^2 postaci

$$P = \{(x, x^2), | x \in \mathbb{R}\}.$$

Jest to wykres funkcji kwadratowej lub inaczej mówiąc: parabola. Nie jest to z pewnością warstwa względem podprzestrzeni liniowej w \mathbb{R}^2 , a jednak łatwo można wprowadzić w niej strukturę do złudzenia przypominającą afiniczną. Wystarczy rozważyć bijekcję: $f : P \rightarrow \mathbb{R}$ postaci $(x, x^2) \mapsto (x, 0)$ i przyjmując za „przestrzeń wektorów swobodnych” przestrzeni P podprzestrzeń liniową $\text{lin}(1, 0)$. Definiujemy dalej operację dodawania do punktu $(x, x^2) \in P$ wektora $\alpha \in \text{lin}(1, 0)$ w następujący sposób:

$$(x, x^2) \boxplus (a, 0) = ((x + a), (x + a)^2).$$

Krótko mówiąc przenosimy na P strukturę afiniczną prostej afinicznej $(0, 0) + \text{lin}(1, 0)$, czyli P jest zbiorem punktów, a $\text{lin}(\alpha)$ jest jakby przestrzenią wektorów swobodnych. Jeśli ktoś powie, że to oszustwo, bo ta struktura nie mówi nic o zakrzywieniu P odpowiem – cóż z tego? Nie używam dodawania w \mathbb{R}^2 , ale jakiegoś innego – ok, ale skutek wydaje się ten sam. Czy jestem w stanie powyższą strukturę zrealizować jako warstwę podprzestrzeni w pewnej przestrzeni liniowej? Mogę, ale po co miałbym to robić? Już jako podzbiór w \mathbb{R}^2 zbiór P z dodatkową strukturą dodawania \boxplus do elementu $p \in P$ wektora $\alpha \in \text{lin}(1, 0)$ dostatecznie przypomina przestrzeń afiniczną.

Problem 2. Przypuśćmy, że interesuje nas zbiór wszystkich przekształceń afinicznych $A(H_1, H_2)$ z przestrzeni afinicznej H_1 do przestrzeni afinicznej H_2 , przy czym zakładamy, że przestrzenie te są zawarte w przestrzeniach liniowych V, W nad ciałem K . W przypadku przekształceń liniowych wiemy, że $L(V, W)$ ma również strukturę przestrzeni liniowej. Czy zbiór $A(H_1, H_2)$ ma strukturę przestrzeni afinicznej? Czy jest to po prostu warstwa w $L(V, W)$?

Definicja 7.9: Aksjomatyczna definicja przestrzeni afinicznej

Niech W będzie przestrzenią liniową nad ciałem K . PRZESTRZENIĄ AFINICZNĄ nad ciałem K o PRZESTRZENI WEKTORÓW SWOBODNYCH W nazywamy niepusty zbiór H wraz z odwzorowaniem:

$$H \times W \longrightarrow H, \quad (p, \alpha) \mapsto p \boxplus \alpha,$$

zwanym DODAWANIEM WEKTORA DO PUNKTU, przy czym spełnione są następujące warunki, zwane aksjomatami przestrzeni afinicznej.

(1) Dla każdych $\alpha, \beta \in W$ i każdego $p \in H$ mamy:

$$p \boxplus 0 = p, \quad p \boxplus (\alpha + \beta) = (p \boxplus \alpha) \boxplus \beta.$$

(2) Dla każdych $p, q \in H$ istnieje dokładnie jeden $\alpha \in W$ taki, że $p \boxplus \alpha = q$.

Elementy przestrzeni H nazywamy PUNKTAMI przestrzeni H .

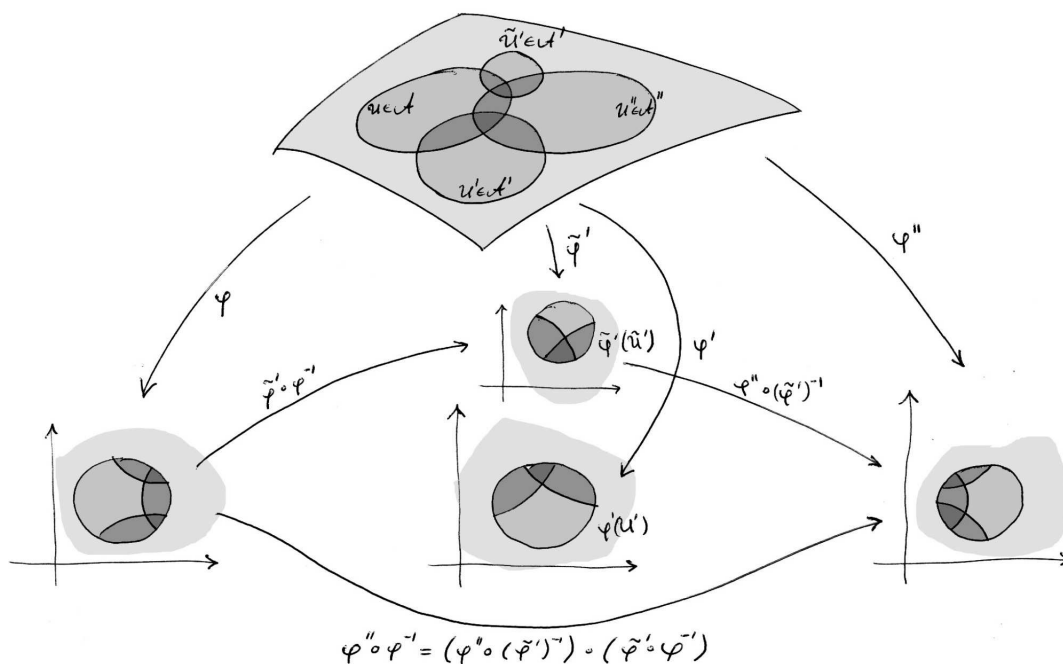
Przykłady:

- Przestrzenie afiniczne rozpatrywane dotąd jako warstwy podprzestrzeni liniowych w przestrzeniach liniowych są przestrzeniami afinicznymi w sensie powyższej definicji. Jeśli $H \subseteq V$ jest warstwą podprzestrzeni W przestrzeni liniowej V , to dla każdego $p \in H$ i każdego $\alpha \in W$ mamy $p + \alpha \in H$, więc rolę odwzorowania $\boxplus : H \times W \longrightarrow H$ gra tu po prostu dodawanie wektorów zapożyczony z V .
- Jeśli H_1, H_2 są przestrzeniami afinicznymi nad K , to $H_1 \times H_2 = \{(p_1, p_2) | p_1 \in H_1, p_2 \in H_2\}$ jest przestrzenią afiniczną nad K . Jeśli W_1, W_2 są przestrzeniami wektorów swobodnych przestrzeni H_1, H_2 , odpowiednio, to $W_1 \times W_2$ jest przestrzenią wektorów swobodnych przestrzeni $H_1 \times H_2$.
- Niech H będzie przestrzenią afiniczną nad K i niech $X \neq \emptyset$. Wówczas $P(X, H) = \{\text{funkcje } X \rightarrow H\}$ jest przestrzenią afiniczną nad K . Jeśli W jest przestrzenią wektorów swobodnych przestrzeni H , to $F(X, W)$ jest przestrzenią wektorów swobodnych przestrzeni $F(X, H)$.
- Struktura $(P, \text{lin}(1, 0), \boxplus)$ rozważana w problemie pierwszym jest przestrzenią afiniczną.

Zarówno podejście aksjomatyczne do geometrii afinicznej, jak i podejście oparte na traktowaniu przestrzeni afinicznych jako warstwy ma pewne zauważalne już wady. W ujęciu aksjomatycznym wydajemy się mieć za dużą swobodę, mogąc choćby tak jak w problemie pierwszym przypisać strukturę afiniczną niemal dowolnemu obiektowi. W ujęciu „warstwowym” – zasadniczo nie tracimy nic ze swobody, jaką daje nam podejście aksjomatyczne⁵, ale trafiamy do drugiego ekstremum: musimy traktować „liniowo” obiekty, które jako takie nie mają natury liniowej. Tak było w przypadku paraboli opisanej w problemie pierwszym. Parabola jest jednak niedoskonałym przykładem, bo choć nie jest warstwą, to jednak jej „naturę” odczytujemy stąd, że jest opisana w afinicznym układzie współrzędnych na płaszczyźnie. Gdybyśmy nie wiedzieli, że P składa się z punktów postaci (x, x^2) , słabiej byśmy oponowali przeciwko myśleniu o $(P, \text{lin}(1, 0), \boxplus)$ jako o prostej afinicznej.

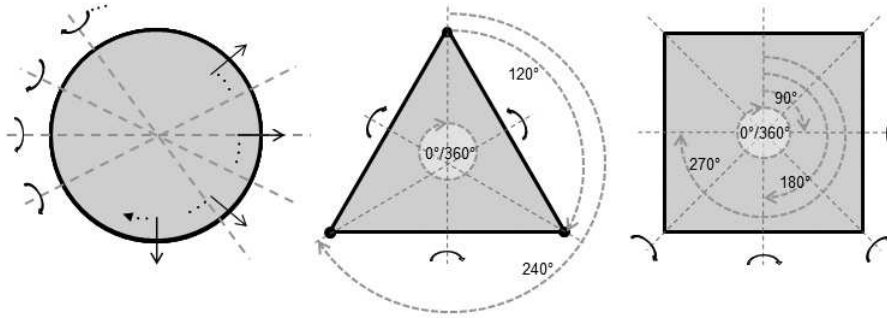
Problem ten rozważa się także w ogólnej sytuacji: mamy pewien zbiór X i nie mamy w nim struktury liniowej. Czasem nie chcemy myśleć o naszym obiekcie jako zanurzonej w przestrzeni liniowej z układem współrzędnych, nawet w ten sposób, w jaki parabola P z problemu pierwszego była związana z \mathbb{R}^2 . Naprawdę nie traktujemy X jako części większej całości tylko jako obiekt sam w sobie. Co można powiedzieć o jego geometrii? To wbrew pozorom niezwykle ważne pytanie, zwłaszcza gdy ze zbiorem X związane są pewne funkcje, przez których badanie możemy wypowiadać się o naturze geometrycznej tego zbioru. Pięknie o tym pisze prof. Toruńczyk w swoich notatkach (<https://duch.mimuw.edu.pl/~torunczy/GAL/011-12/Wyk/VIII-AFI.pdf>), mówiąc o intuicji pojęcia, zwanego ROZMAITOŚCIĄ.

„Przypuśćmy, że grono osób bada niedostępny obiekt \mathbb{A} (np. powierzchnię niewidocznej strony Księżyca), mając do dyspozycji pewien zbiór jego map, rozdzielonych między badających. Jeśli ktoś zaproponuje nazwanie zbioru $X \subseteq \mathbb{A}$ elipsą, gdy na jego mapie zbiór ten jest odzwierciedlony jako elipsa, to natychmiast pojawia się pytanie, czy na innych mapach też jest on tak odzwierciedlony. Oznaczmy przez S_i przekształcenie, które punktowi zbioru \mathbb{A} przyporządkowuje jego obraz na i -tej mapie. Wówczas $S_j S_i^{-1}$ przyporządkowuje punktom i -tej mapy odpowiadające im punkty mapy j -tej. Możliwość uzgodnienia przez badających, jakie zbiory \mathbb{A} nazwać elipsami, zależy od tego, czy wszystkie PRZEKSZTAŁCENIA ZMIANY MAP przeprowadzają elipsy na elipsy. Ogólniej, badający zdołają uzgodnić te pojęcia dotyczące obiektu \mathbb{A} , które są niezmiennicze względem wszystkich tych przekształceń. (Zostawiamy tu pewne niedopowiedzenie.) [...] Materiał ten jest ważny i dlatego, że stwarza pewien zakres pojęć umożliwiających badanie przestrzeni, w której żyjemy – co było zadaniem geometrii od jej początków. Zadanie to o tyle sobie ułatwiamy, że istnienie odpowiednio zgodnych map przyjmujemy, podczas gdy ważnym osiągnięciem geometrii klasycznej było odkrycie ich istnienia i wskazanie sposobów konstrukcji.”



⁵Każdej przestrzeni afinicznej zdefiniowanej przez aksjomaty można w sposób jednoznaczny przypisać izomorficzną z nią – czyli identyczną pod względem abstrakcyjnej struktury afinicznej – warstwę pewnej podprzestrzeni. Służy temu konstrukcja tzw. przestrzeni uniwersalnej.

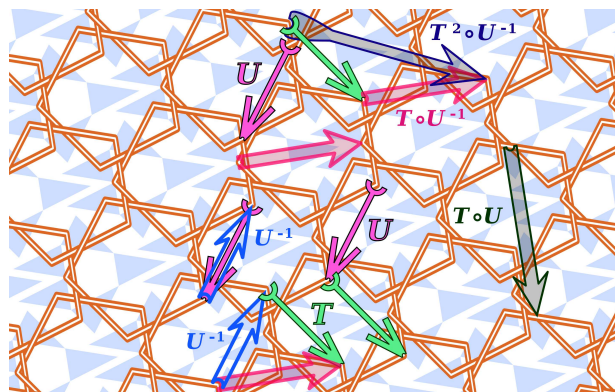
Zaczęliśmy rozważania tego wykładu od nadania paraboli w sposób sztuczny struktury afinicznej przez przypisanie jej jednej tylko „mapy”. To skrajny przykład zaprzeczający idei powyższych rozważań. „Poprawne” nadanie paraboli P zestawu funkcji $S_i : P \rightarrow \mathbb{R}^2$, które jednoznacznie **wyróżniają ją** w zbiorze innych (pewnych) podzbiorów \mathbb{R}^2 , opisanych innymi zestawami map (i opisanie sposobów na porównywanie „zestawów map”) – to jest właściwy problem. Unikam tu jak mogę precyzyjnego języka – kiedyś na analizie i geometrii różniczkowej poznacie Państwo szczegóły. Powiem tylko, że podejście to pozwala na jeszcze inną definicję przestrzeni afinicznej wymiaru n nad ciałem K – mianowicie jako zbioru \mathbb{A} z wyróżnioną rodziną bijekcji $M_{\mathbb{A}}$ idących z \mathbb{A} do K^n takich, że dla $f_1, f_2 \in M_{\mathbb{A}}$ odwzorowanie $f_1 f_2^{-1}$ należy do przestrzeni przekształceń afinicznych $A(K^n, K^n)$. Podejście to, opisane w notatkach prof. Toruńczyka, pozwala widzieć rozmaite obiekty geometryczne jako „niezmiennicze” przy działaniu pewnych „grup przekształceń”. Sposób ten promował F. Klein w tzw. programie erlangenkim (1872 r.). Nie sposób wejść w szczegóły, ale chciałbym przynajmniej powiedzieć co rozumieć przez „obiekty niezmiennicze”.



IZOMETRIE WŁASNE OKRĘGU, TRÓJKĄTA RÓWNOBOCZNEGO I KWADRATU. Źródło: Michael J Richardson.

W matematyce możemy badać obiekty poprzez ich zbiory przekształceń, na przykład zbiory symetrii w sobie. Zbiory te wyglądają inaczej dla różnych obiektów geometrycznych. Interesujące jest jednak podejście, w którym to nie obiekt definiuje swoje przekształcenia, ale to zbiór przekształceń definiuje obiekt! Weźmy zbiór X bez żadnej „odziedziczonej” struktury. Do badania X będziemy mieli do dyspozycji zestaw przekształceń \mathcal{F} zbioru X w siebie. Umówimy się, że jeśli dla pewnego podzbioru $O \subseteq X$ mamy $f(O) = O$, dla każdego $f \in \mathcal{F}$, to zbiór O nazywamy \mathcal{F} -okręgiem. Uwaga: nic nie wiemy ani o zbiorze O , ani o X (może to np. zbiór Cantora), a nawet nic wstępnie nie zakładamy o \mathcal{F} . Przy tak minimalistycznym podejściu wydaje się, że zbieżność nazewnictwa \mathcal{F} -okręgu z „prawdziwymi okręgami” (czyli czym?) jest zupełnie przypadkowa i bezzasadna. Czy rzeczywiście?

Umówmy się zatem, że jeśli w zbiorze X istnieje inny podzbiór: P taki, że tylko dwa przekształcenia z \mathcal{F} (a nie wszystkie) zachowują P , to P nazywamy \mathcal{F} -prostokątem. Nonsens? Pojęcia \mathcal{F} -okręgu i \mathcal{F} -prostokąta pozbawione są być może na pozór geometrycznego sensu – ale można pytać co nas dokładnie interesowało? Myślenie geometryczne polegające na rozróżnianiu obiektów ze względu na pewne niezmienniki jest niezwykle ciekawe i prowadzi do głębokich pytań, zupełnie innych jakościowo od pytań geometrii szkolnej. Proces formułowania problemów bywa nie mniej fascynujący, co samo poszukiwanie na nie rozwiązania. Ot choćby: jak wysłowić różnicę między preclem, a pączkiem, czyli między torusem i sferą (dwuwymiarowymi)? Przecież „widzimy” tę różnicę („dziura”), ale jak ująć tę różnicę w pojęcia matematyczne i sformułować odpowiedni wynik? Pytanie to dotyczy niezwykle ważnych problemów.



7.3 Dodatek. Kombinacje i zbiory wypukłe

Na wykładzie powiedzieliśmy o zbiorach zamkniętych na kombinacje afiniczne, co pozwala znacznie poszerzyć spektrum badanych obiektów w przestrzeni K^n . Na kolejnych wykładach będziemy mówić o punktach, prostych, płaszczyznach, równoległości, dalej o prostopadłości, kątach itd. Jest to kierunek mający ostatecznie na celu odpowiedzenie sobie na pytanie: jak różnić własności geometryczne zbiorów opisywanych równaniami (liniowymi i nie tylko). W tym dodatku powiemy o własności będącej nieco z boku tych rozważań, mającej jednak bardzo geometryczny charakter i bardzo istotny wpływ na wiele dziedzin matematyki (w tym analizę, teorię liczb, kombinatorykę itd.). Jest to teoria zbiorów (oraz funkcji) wypukłych. W kilku najbliższych dodatkach opowiemy o pewnych, raczej rekreacyjnych, jej aspektach. Teoria ta dotyczy (z naszego punktu widzenia) rzeczywistych przestrzeni afinicznych, choć można ją rozszerzać i na inne ciała.

Definicja 7.10: Podzbiór wypukły

Niepusty podzbiór X przestrzeni afinicznej \mathbb{R}^n nazywamy WYPUKŁYM jeśli dla dowolnych $x, y \in X$ oraz $\lambda \in [0, 1]$ mamy:

$$(1 - \lambda)x + \lambda y \in X.$$

Zbiór pusty również uznajemy za wypukły.

Oczywistymi przykładami zbiorów wypukłych są: cała przestrzeń afiniczna \mathbb{R}^n oraz każdy punkt tej przestrzeni. Podstawowymi przykładami są natomiast sympleksy i półprzestrzenie.

Definicja 7.11

SYMPEKSEM n -wymiarowym rozpiętym na afinicznie niezależnym układzie punktów p_0, \dots, p_n nazywamy zbiór $S(p_0, \dots, p_n)$ określony warunkami:

$$S(p_0, \dots, p_n) = \{a_0 p_0 + \dots + a_n p_n \in \mathbb{R}^n \mid a_0 + \dots + a_n = 1, a_i \geq 0\}.$$

Sympleks jednowymiarowy nazywamy ODCINKIEM, dwuwymiarowy – TRÓJKĄTEM, a trójwymiarowy – CZWOROŚCIANEM. Punkty p_0, \dots, p_n nazywamy też WIERZCHOŁKAMI sympleksu.

Sympleks jest oczywiście zbiorem wypukłym. Jeśli $p = a_0 p_0 + \dots + a_n p_n$ oraz $q = a'_0 p_0 + \dots + a'_n p_n$, gdzie $a_i, a'_i \geq 0$ oraz $a_0 + \dots + a_n = a'_0 + \dots + a'_n = 1$. to

$$t(a_0 p_0 + \dots + a_n p_n) + (1 - t)(a'_0 p_0 + \dots + a'_n p_n) = (ta_0 + (1 - t)a'_0)p_0 + \dots + (ta_n + (1 - t)a'_n)p_n.$$

Oczywiście mamy $ta_i + (1 - t)a'_i \geq 0$. Natomiast suma owych nieujemnych wag jest równa 1, tzn.

$$(ta_0 + (1 - t)a'_0) + \dots + (ta_n + (1 - t)a'_n) = t(a_0 + \dots + a_n) + (1 - t)(a'_0 + \dots + a'_n) = t + 1 - t = 1.$$

Definicja 7.12: Półprzestrzeń w \mathbb{R}^n

PÓLPRZESTRZENIĄ w \mathbb{R}^n nazywamy zbiór H rozwiązań nietrywialnej nierówności liniowej postaci:

$$H = \{(x_1, \dots, x_n) \in \mathbb{R}^n \mid a_1 x_1 + a_2 x_2 + \dots + a_n x_n \leq b, \text{ gdzie } (a_1, a_2, \dots, a_n) \neq 0\}.$$

Półprzestrzeń jest zbiorem wypukłym. Istotnie, niech $p = (p_1, \dots, p_n)$ oraz $q = (q_1, q_2, \dots, q_n) \in H$ oraz niech $t \in [0, 1]$ Należy wykazać, że $tp + (1 - t)q \in H$. Mamy $a_1 p_1 + a_2 p_2 + \dots + a_n p_n \leq b$ oraz $a_1 q_1 + a_2 q_2 + \dots + a_n q_n \leq b$. Stąd

$$a_1(tp_1) + a_2(tp_2) + \dots + a_n(tp_n) \leq tb, \quad a_1(1 - t)q_1 + a_2(1 - t)q_2 + \dots + a_n(1 - t)q_n \leq (1 - t)b.$$

W rezultacie:

$$\sum_{i=1}^n a_i(tp_i + (1 - t)q_i) \leq b, \quad \text{oraz} \quad tp + (1 - t)q \in H.$$

Bez trudu sprawdzamy (zostawiam to jako ćwiczenie), że zbiorem wypukłym jest również (standardowa euklidesowa) KULA $K_{p,r} \subseteq \mathbb{R}^n$ o środku w punkcie $p = (p_1, \dots, p_n)$ i promieniu $r \geq 0$, czyli zbiór postaci

$$K_{p,r} = \{(x_1, \dots, x_n) \in \mathbb{R}^n \mid (x_1 - p_1)^2 + \dots + (x_n - p_n)^2 \leq r^2\}.$$

Obserwacja 7.8

Część wspólna zbiorów wypukłych jest zbiorem wypukłym.

Dowód. Niech $A = \bigcap_i A_i$ będzie przecięciem rodziny zbiorów wypukłych A_i . Weźmy $p, q \in A$. Wtedy dla każdego i mamy $p \in A_i$ oraz $q \in A_i$, co z wypukłości A_i oznacza, że dla każdego $t \in [0, 1]$ mamy $tp + (1-t)q \in A_i$. W szczególności $tp + (1-t)q \in A$. \square

Definicja 7.13: Kombinacja wypukła, otoczka wypukła

Niech x_0, \dots, x_k będą punktami w przestrzeni afinicznej \mathbb{R}^n oraz a_0, \dots, a_k będzie układem wag, czyli $a_0 + \dots + a_k = 1$. Kombinację afiniczną $a_0x_0 + \dots + a_kx_k$ nazywamy KOMBINACJĄ WYPUKŁĄ, jeśli $a_0, a_1, \dots, a_k \geq 0$. Niech $X \subset \mathbb{R}^n$. Zbiór wszystkich kombinacji wypukłych punktów z X nazywamy UWYPUKLIENIEM lub OTOCZKĄ WYPUKŁĄ zbioru X , oznaczaną jako $\text{conv}(X)$.

Zgodnie z powyższą definicją $S(p_0, \dots, p_n) = \text{conv}(\{p_0, \dots, p_n\})$. Wykażemy następujący fakt.

Obserwacja 7.9

Zbiór $\text{conv}(X)$ jest najmniejszym (względem inkluzji) zbiorem wypukłym zawierającym X .

Dowód. Wypukłość zbioru $\text{conv}(X)$ uzasadnia się identycznie jak wypukłość sympleksu. Pozostaje więc uzasadnić minimalność. Niech C będzie zbiorem wypukłym zawierającym X . Wykażemy przez indukcję względem długości $k+1$ zapisu kombinacji wypukłej, że każdy punkt $p \in \text{conv}(X)$ należy do C . Niech $p = a_0p_0 + \dots + a_kp_k \in \text{conv}(X)$, gdzie $p_i \in X$, $a_0 + \dots + a_k = 1$ oraz $a_i \geq 0$.

Jeśli $k=0$, to $p = p_0 \in X \subseteq C$. Przechodzimy do kroku indukcyjnego. Założymy, że $k > 0$ oraz, że każda kombinacja wypukła $\leq k$ punktów z X należy do C . Niech $p = a_0p_0 + \dots + a_kp_k$. Jeśli dowolna z wag a_i tej kombinacji równa jest 1, to ponownie opisuje ona punkt ze zbioru X . Załóżmy więc, że mamy $a_k < 1$. Dla $i = 0, 1, 2, \dots, k-1$ niech

$$a'_i = \frac{a_i}{1 - a_k}.$$

Wówczas $a'_i \geq 0$ oraz

$$a'_0 + \dots + a'_{k-1} = \frac{a_0}{1 - a_k} + \dots + \frac{a_{k-1}}{1 - a_k} = \frac{a_0 + \dots + a_{k-1}}{1 - a_k} = 1.$$

Zatem na mocy założenia indukcyjnego punkt $p' = a'_0p_0 + \dots + a'_{k-1}p_{k-1}$ należy do C . Co więcej

$$p = a_0p_0 + \dots + a_kp_k = (1 - a_k)(a'_0p_0 + \dots + a'_{k-1}p_{k-1}) + a_kp_k = (1 - a_k)p' + a_kp_k,$$

czyli z definicji zbioru wypukłego C skoro $p' \in C$ oraz $p_k \in X \subseteq C$, to $p \in C$. \square

Wniosek 7.1

Następujące warunki są równoważne dla podzbioru $X \subseteq \mathbb{R}^n$:

- X jest wypukły,
- X jest zamknięty na kombinacje wypukłe, tzn. $\text{conv}(X) = X$.

Pięknym i ważnym aspektem teorii zbiorów wypukłych jest ich związek z dodawaniem zbiorów (rozumianych w sensie przestrzeni liniowych). Operacja ta ma w kontekście tej teorii nazwę sumy Minkowskiego.

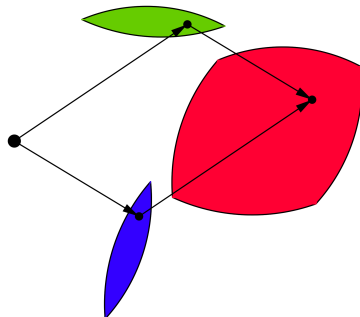
Definicja 7.14: Suma i iloczyn Minkowskiego

Dla podzbiorów A, B przestrzeni liniowej \mathbb{R}^n SUMĄ MINKOWSKIEGO tych podzbiorów nazywamy:

$$A + B = \{a + b \mid a \in A, b \in B\}.$$

Dla podzbioru $A \subseteq \mathbb{R}^n$ przez ILOCZYN ZBIORU A PRZEZ SKALAR $t \in \mathbb{R}$ określamy zbiór

$$tA = \{ta \mid a \in A\}.$$



Suma Minkowskiego zbioru niebieskiego i zielonego to zbiór czerwony.

Zachęcam Czytelnika do uzasadnienia prostych obserwacji:

- zbiór $\{0\}$ jest elementem neutralnym dodawania Minkowskiego,
- suma Minkowskiego jest działaniem łącznym i przemianym,
- mnożenie przez skalar jest rozdzielne względem dodawania,
- suma i mnożenie przez skalar w sensie Minkowskiego zachowują inkluzje, tzn. jeśli $A_1 \subseteq B_1$ oraz $A_2 \subseteq B_2$, to $A_1 + A_2 \subseteq B_1 + B_2$ oraz $tA_1 \subseteq tB_1$.

Obserwacja 7.10

Jeśli A, B są zbiorami wypukłymi, to $A + B$ oraz tA są wypukłe, dla każdego $t \in \mathbb{R}$. Co więcej, dla dowolnych podzbiorów $A, B \subseteq \mathbb{R}^n$ mamy:

$$\text{conv}(A) + \text{conv}(B) = \text{conv}(A + B).$$

Dowód. Oczywiście tA jest obrazem zbioru A przy jednokładności o środku 0 i skali t , więc jest to zbiór wypukły. Również suma Minkowskiego zachowuje wypukłość. Jeśli zbiory A_1, A_2 są wypukłe to niech $p, q \in A_1 + A_2$. Wówczas $p = p_1 + p_2$ oraz $q = q_1 + q_2$, dla pewnych $p_i, q_i \in A_i$. Ponieważ A_i jest zbiorem wypukłym, to $S(p_i, q_i) \subseteq A_i$. Zatem:

$$S(p, q) \subseteq \{(1-t)p_1 + tq_1 \mid t \in [0, 1]\} + \{(1-t)p_2 + tq_2 \mid t \in [0, 1]\} \subseteq S(p_1, q_1) + S(p_2, q_2) \subseteq A_1 + A_2.$$

□

* * *

Wprowadzone wyżej operacje mają liczne proste własności analityczne i topologiczne. Czytelnika zainteresowanego tymi własnościami odsyłam do podręcznika prof. M. Moszyńskiej *Geometria zbiorów wypukłych*. Sumy Minkowskiego mają istotne znaczenie w zastosowaniach, m.in. w tomografii czy robotyce. O zbiorach wypukłych wspomnimy poniżej w kontekście twierdzenia Helly'ego oraz w kontekście wielościanów, w dodatku do przekształceń afinicznych.

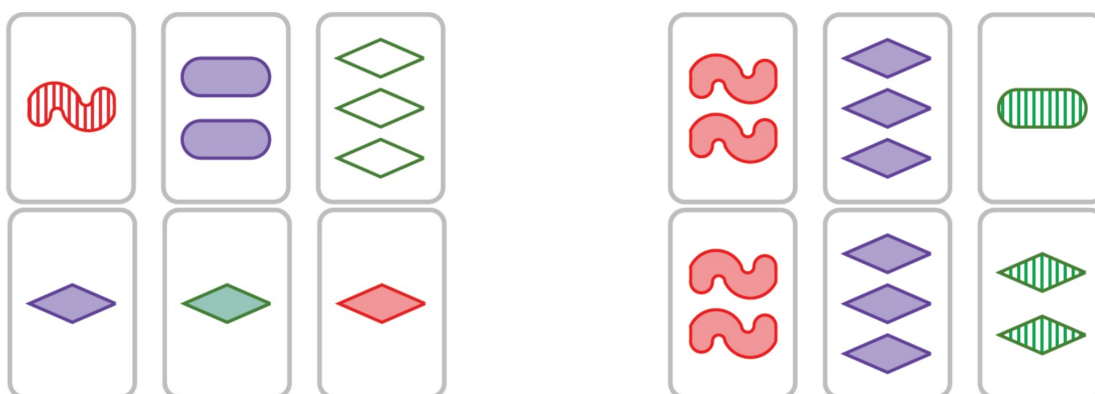
7.4 Trivia. SET, czyli przestrzeń afiniczna nad \mathbb{Z}_3

SET jest szybką i dość wciągającą grą karcianą polegającą na rozpoznawaniu prawidłowości, bardzo popularną wśród studentów i entuzjastów matematyki⁶. Zadaniem jest identyfikowanie trzech kart z obiektami, które spełniają określone zasady – taki zbiór to właśnie Set.

Zasady⁷ są następujące. Dana jest talia 81 kart. Każda karta jest określona przez cztery cechy, z których każda ma jedną z trzech możliwych wartości zgodnie z poniższą tabelą (sprawę \mathbb{Z}_3 wyjaśnimy dalej).

cecha/element \mathbb{Z}_3	0	1	2
liczba	raz	dwa	trzy
wypełnienie	puste	częściowe	pełne
kolor	czerwony	zielony	fioletowy
kształt	romb	elipsa	fala

Na początku rozgrywki rozkładamy na stole 12 kart (3 rzędy po 4 kolumny). Celem jest zebranie **Setów**, czyli 3 kart na których każda pojedyncza cecha jest różna lub taka sama. Kiedy któryś z graczy go zauważy mówi głośno „Set”, gra się zatrzymuje i sprawdzamy czy jest on poprawny. Każdy Set jest wart 3 punkty, jednak kiedy wytypujemy zły Set tracimy jedną kartę. Następnie karty uzupełniane są do 12.



Po lewej – dwa Sety, po prawej – dwa nie-Sety.

Proszę zauważyć, że jeśli mamy dowolne dwie karty, to istnieje dokładnie jedna karta w zestawie, która tworzy z nimi Set. To się kojarzy z własnością:

Przez dowolne dwa punkty można przeprowadzić prostą.

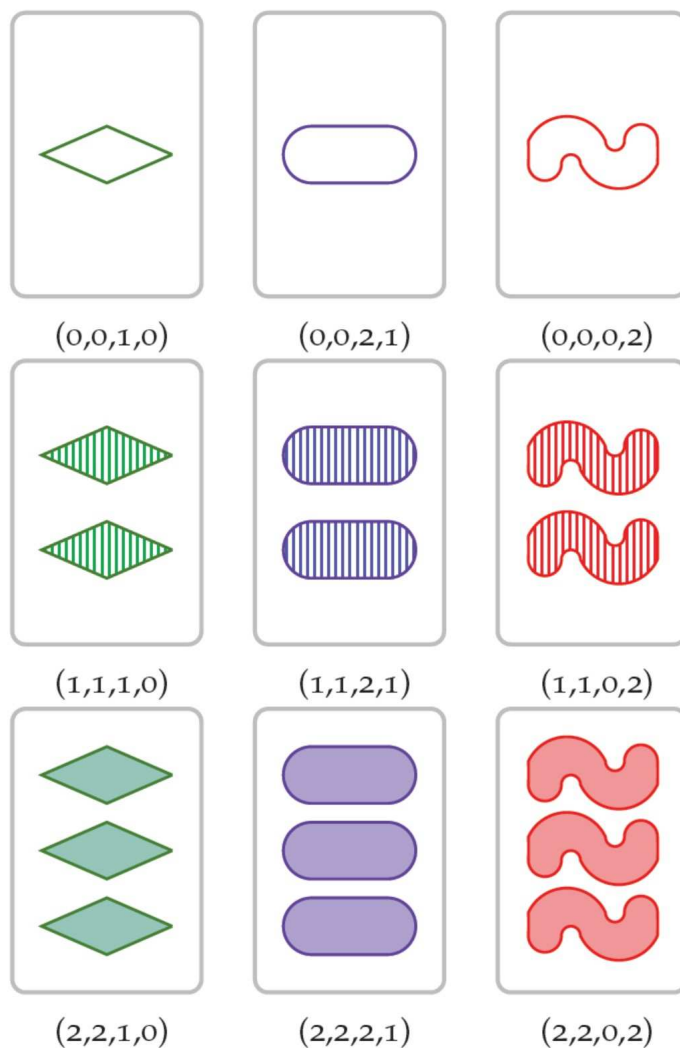
Pomysł jest taki, że rozważamy przestrzeń \mathbb{Z}_3^4 traktowaną jako przestrzeń afiniczna i w tej przestrzeni karty są punktami, a Sety – prostymi. Jak to działa? Mamy po prostu punkty o współrzędnych (x_1, x_2, x_3, x_4) , które oznaczają kolejno: liczbę, wypełnienie, kolor, kształt, a liczby 0, 1, 2 z ciała \mathbb{Z}_3 przypisujemy kolejno tak jak w tabeli wyżej. A zatem np. elementowi $(0, 1, 0, 2)$ przypisujemy kartę:



⁶Podstawą merytoryczną jest artykuł *Algebra From Geometry in the Card Game SET* autorstwa Timothy E. Goldberga, The College Mathematics Journal, Vol. 47, No. 4, pp. 265-273 oraz materiały prof. J. Wiśniewskiego

⁷Zasady przytoczone za stronę <https://boardtime.pl/2012/11/set-recenzja.html>. W Seta można zagrać także online: https://smart-games.org/en/set/submit_set.

Wyobraźmy sobie teraz np. zbiór rozwiązań układu równań liniowych $x_1 - x_2 = 0, x_3 - x_4 = 1$. Jest to warstwa dwuwymiarowej przestrzeni liniowej nad \mathbb{Z}_3 , a dokładniej zbiór 9 kart. Poniżej znajdują się te karty i odpowiadające im punkty. Wyraźnie widzimy, że jest to płaszczyzna afiniczna w przestrzeni \mathbb{Z}_3^4 złożona z 12 prostych (proszę wskazać).



Zauważmy też, że mamy operacje w tej przestrzeni, na przykład dodawanie do punktów wektorów:

$$\begin{array}{c}
 \begin{array}{|c|} \hline \text{Two purple figure-eight shapes with vertical stripes} \\ \hline \end{array} + \begin{array}{|c|c|} \hline \xrightarrow{\hspace{1cm}} \\ \hline \begin{array}{|c|} \hline \text{Green diamond} \\ \hline \end{array} \begin{array}{|c|} \hline \text{Two purple figure-eight shapes with vertical stripes} \\ \hline \end{array} \\ \hline \end{array} = \begin{array}{|c|} \hline \text{Three red rounded rectangles} \\ \hline \end{array} \\
 (1,1,2,2) + \overrightarrow{(0,0,1,0)(1,1,2,2)} = (2,2,0,1)
 \end{array}$$

Nie chcę przywoływać rozważań teoretycznych⁸ dotyczących gry Set, ale mam nadzieję, że to spojrzenie u przyjemni Państwu myślenie o przestrzeniach afinicznych także w kontekście matematyki dyskretnej. Przede wszystkim natomiast polecam Set — jakże popularny wśród matematyków.

⁸No dobrze, przywołam jedno: ile można wyłożyć kart, by nie było wśród nich żadnego Seta? Odpowiedź w artykule: <http://homepages.warwick.ac.uk/staff/D.Maclagan/papers/set.pdf>

Rozdział 8

Afiniczna niezależność, bazy punktowe i układy bazowe

Na poprzednim wykładzie zapoznaliśmy się z pojęciem przestrzeni afinicznej. Podobnie jak dla przestrzeni liniowych, do badania przestrzeni afinicznych potrzebne jest rozważanie „podstruktur”. W przeciwieństwie do podprzestrzeni liniowych, interesują nas zbiory zamknięte na szczególny typ kombinacji – tak zwane kombinacje afiniczne. Naszym dzisiejszym celem¹ będzie opis podprzestrzeni rozpiętych na układach punktów, a w szczególności – opis minimalnych układów generujących podprzestrzeń afiniczną. Jak się okaże własności tych układów są ściśle związane z minimalnymi układami wektorów rozpinających (czyli bazami) jej przestrzeni stycznej. Pozwala to m.in. na mówienie o wymiarze przestrzeni afinicznej.

Obserwacja 8.1

Niech p_0, \dots, p_k będą punktami przestrzeni afinicznej H . Następujące warunki są równoważne:

- (1) $H = \text{af}(p_0, \dots, p_k)$,
- (2) $T(H) = \text{lin}(\overrightarrow{p_0p_1}, \dots, \overrightarrow{p_0p_k})$.

Dowód. Dowodzimy (1) \Rightarrow (2). Skoro H jest przestrzenią afiniczną, to zgodnie z dowodem faktu charakteryzującego przestrzenie afiniczne jako podzbiory zamknięte na kombinacje afiniczne wiemy, że dla każdego $q \in H$ mamy

$$T(H) = \{\overrightarrow{qp} \mid p \in H\}.$$

Jeśli $H = \text{af}(p_0, \dots, p_k)$, to biorąc $q = p_0$ otrzymujemy

$$\begin{aligned} T(H) &= \{\overrightarrow{p_0p} \mid p \in H\} = \\ &= \{\overrightarrow{p_0p} \mid \text{dla wszystkich } p = a_0p_0 + \dots + a_kp_k, \text{ gdzie } a_0 + \dots + a_k = 1\} = \\ &= \{a_1\overrightarrow{p_0p_1} + \dots + a_k\overrightarrow{p_0p_k} \mid a_1, \dots, a_k \in K\} = \\ &= \text{lin}(\overrightarrow{p_0p_1}, \dots, \overrightarrow{p_0p_k}). \end{aligned}$$

Na odwrót: jeśli $T(H) = \text{lin}(\overrightarrow{p_0p_1}, \dots, \overrightarrow{p_0p_k})$, to już wiemy, że dla każdego $p \in H$ mamy

$$\overrightarrow{p_0p} = a_1\overrightarrow{p_0p_1} + \dots + a_k\overrightarrow{p_0p_k},$$

dla pewnych $a_1, \dots, a_k \in K$. Chcemy, by $p \in \text{af}(p_0, \dots, p_k)$. Przyjmując $a_0 = 1 - a_1 - \dots - a_k$ otrzymujemy

$$p = p_0 + \overrightarrow{p_0p} = (a_0 + \dots + a_k)p_0 + a_1(p_1 - p_0) + \dots + a_k(p_k - p_0).$$

Po uproszczeniu dostajemy $p = a_0p_0 + \dots + a_kp_k$. Wobec dowolności p otrzymujemy stąd (1). \square

PRZYKŁAD. W przestrzeni $V = \mathbb{R}^3$ niech $H = \text{af}((1, 0, 2), (2, 1, 3), (4, 1, 1))$. Wówczas przestrzeń styczna $T(H)$ to $\text{lin}((1, 1, 1), (3, 1, -1)) = \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1 - 2x_2 + x_3 = 0\}$. Stąd sama podprzestrzeń H opisana jest jako zbiór rozwiązań układu złożonego z pojedynczego równania $x_1 - 2x_2 + x_3 = 3$.

¹Ostatnia aktualizacja 15:05.2023 r.

Definicja 8.1: Układ afinicznie zależny/niezależny

Niech p_0, \dots, p_k będzie układem punktów przestrzeni afinicznej H nad ciałem K .

- Mówimy, że układ p_0, \dots, p_k jest **AFINICZNIE ZALEŻNY** (albo, że jest w **POŁOŻENIU SZCZEGÓLNYM**), jeśli jeden z punktów tego układu jest kombinacją afiniczną pozostałych.
- Mówimy, że układ p_0, \dots, p_k jest **AFINICZNIE NIEZALEŻNY** (albo, że jest w **POŁOŻENIU OGÓLNYM**), jeśli nie jest on w położeniu szczególnym.

PRZYKŁAD. W przestrzeni $H = \mathbb{R}^3$ układ $((3, 7, 4), (1, 9, 7), (5, 5, 1))$ jest afinicznie zależny, bo mamy $(1, 9, 7) = 2(3, 7, 4) - 1(5, 5, 1)$. Układ $(3, 1, 1), (1, 2, 1)$ jest natomiast afinicznie niezależny w \mathbb{R}^3 .

Afiniczna (nie)zależność układu punktów nie zależy od kolejności punktów układu. Każdy podukład układu afinicznie niezależnego jest afinicznie niezależny. Łatwo widzieć, że istnieje zależność pomiędzy afiniczną niezależnością układu punktów i liniową niezależnością odpowiadającego mu układu wektorów. Układ $k + 1$ punktów jest afinicznie niezależny wtedy i tylko wtedy, gdy układ k wektorów o początkach w jednym z tych punktów łączących go z pozostałymi punktami układu jest liniowo niezależny.

Obserwacja 8.2

Niech p_0, \dots, p_k będą punktami przestrzeni afinicznej H nad K . Równoważne są warunki:

- (1) układ p_0, \dots, p_k jest afinicznie niezależny,
- (2) układ wektorów $\overrightarrow{p_0p_1}, \dots, \overrightarrow{p_0p_k}$ jest liniowo niezależny.

Dowód. Załóżmy, że (2) nie jest prawdą i układ $\overrightarrow{p_0p_1}, \dots, \overrightarrow{p_0p_k}$ jest liniowo zależny. Wówczas któryś z wektorów tego układu jest liniową kombinacją pozostałych. Ewentualnie przenumerowując p_1, \dots, p_k możemy zakładać, że

$$\overrightarrow{p_0p_k} = a_1\overrightarrow{p_0p_1} + \dots + a_{k-1}\overrightarrow{p_0p_{k-1}},$$

dla pewnych $a_1, \dots, a_{k-1} \in K$. Niech $a_0 = 1 - a_1 - \dots - a_{k-1}$. Wówczas

$$\begin{aligned} a_0p_0 + a_1p_1 + \dots + a_{k-1}p_{k-1} &= a_0(p_0 + \overrightarrow{p_0p_0}) + a_1(p_0 + \overrightarrow{p_0p_1}) + \dots + a_{k-1}(p_0 + \overrightarrow{p_0p_{k-1}}) = \\ &= \underbrace{(a_0 + a_1 + \dots + a_{k-1})}_{=1}p_0 + \underbrace{a_1\overrightarrow{p_0p_1} + \dots + a_{k-1}\overrightarrow{p_0p_{k-1}}}_{=\overrightarrow{p_0p_k}} = \\ &= p_0 + \overrightarrow{p_0p_k} = p_k. \end{aligned}$$

A zatem p_k jest kombinacją afiniczną punktów p_0, \dots, p_{k-1} . A zatem (1) \Rightarrow (2).

Na odwrót: przypuśćmy, że układ p_0, \dots, p_k jest afinicznie zależny (znowu z zaprzeczenia chcemy wywieść zaprzeczenie). Chcemy wykazać liniową zależność specyficznego zbioru wektorów (o początkach w p_0). Rozważamy dwa przypadki.

- Punkt p_0 jest kombinacją afiniczną punktów p_1, \dots, p_k . Niech $p_0 = a_1p_1 + \dots + a_kp_k$, przy czym $a_1 + \dots + a_k = 1$. Mamy więc

$$0 = \overrightarrow{p_0p_0} = \overrightarrow{p_0(a_1p_1 + \dots + a_kp_k)} = a_1\overrightarrow{p_0p_1} + \dots + a_k\overrightarrow{p_0p_k}.$$

Zatem układ $\overrightarrow{p_0p_1}, \dots, \overrightarrow{p_0p_k}$ jest liniowo zależny, i mamy sprzeczność z założeniem, że zachodzi (2).

- Punkt p_0 nie jest kombinacją afiniczną² punktów p_1, \dots, p_k . Wówczas skoro układ p_0, \dots, p_k jest afinicznie zależny, to jeden z punktów p_1, \dots, p_k jest kombinacją afiniczną pozostałych. Po ewentualnym przenumerowaniu p_1, \dots, p_k możemy założyć, że p_k jest kombinacją afiniczną p_0, \dots, p_{k-1} . W szczególności $p_k = a_0p_0 + \dots + a_{k-1}p_{k-1}$, gdzie $a_0 + \dots + a_{k-1} = 1$. A zatem:

$$\overrightarrow{p_0p_k} = a_0\overrightarrow{p_0p_0} + a_1\overrightarrow{p_0p_1} + \dots + a_{k-1}\overrightarrow{p_0p_{k-1}} = a_1\overrightarrow{p_0p_1} + \dots + a_{k-1}\overrightarrow{p_0p_{k-1}},$$

czyli układ $\overrightarrow{p_0p_1}, \dots, \overrightarrow{p_0p_k}$ jest liniowo zależny, co przeczy (2). A zatem (2) \Rightarrow (1). □

²Np. układ punktów $p_0 = (1, 2), p_1 = (2, 2), p_2 = (3, 3), p_3 = (4, 4)$ jest afinicznie zależny w \mathbb{R}^2 , ale $p_0 \notin \text{af}(p_1, p_2, p_3)$.

Definicja 8.2: Baza punktowa

Mówimy, że układ punktów p_0, \dots, p_k punktów przestrzeni afinicznej H jest BAZĄ PUNKTOWĄ przestrzeni H , jeśli spełnia następujące dwa warunki:

- układ p_0, \dots, p_k jest afinicznie niezależny,
- $H = \text{af}(p_0, \dots, p_k)$, czyli układ p_0, \dots, p_k ROZPINA H .

Obserwacja 8.3

Niech p_0, \dots, p_k będą punktami przestrzeni afinicznej H . Układ p_0, \dots, p_k jest bazą punktową przestrzeni H wtedy i tylko wtedy, gdy układ wektorów $\overrightarrow{p_0p_1}, \dots, \overrightarrow{p_0p_k}$ jest bazą przestrzeni $T(H)$. W szczególności każde dwie skończone bazy punktowe przestrzeni afinicznej są równoliczne.

Powyższy wniosek uzasadnia następującą definicję.

Definicja 8.3: Wymiar przestrzeni afinicznej; proste, płaszczyzny

WYMIAREM przestrzeni afinicznej H nazywamy wymiar jej przestrzeni stycznej $T(H)$. Wymiar przestrzeni H oznaczamy $\dim H$. Przestrzenie afiniczne wymiaru 1 nazywamy PROSTYMI, przestrzenie wymiaru 2 – PŁASZCZYZNAMI.

- Układ $0, \epsilon_1, \dots, \epsilon_n$, wektorów przestrzeni liniowej K^n , gdzie $\epsilon_1, \dots, \epsilon_n$ są wektorami bazy standardowej, tworzy bazę punktową przestrzeni afinicznej K^n . Przestrzeń ta ma wymiar równy n .
- Niech $H = \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1 - x_2 + 3x_3 = 6\}$. Wówczas $T(H)$ opisać można jako zbiór

$$\{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1 - x_2 + 3x_3 = 0\} = \text{lin}((1, 1, 0), (0, 3, 1)).$$

A zatem $\dim H = 2$. Weźmy teraz $p_0 = (1, 1, 2) \in H$ i niech $p_1 = p_0 + (1, 1, 0) = (2, 2, 2)$ oraz $p_2 = p_0 + (0, 3, 1) = (1, 4, 3)$. Wówczas układ p_0, p_1, p_2 jest bazą punktową przestrzeni H .

- Dla $M = \text{af}((1, 2, 3), (5, 4, 1), (-3, 0, 5), (2, 1, 4)) \subseteq \mathbb{R}^3$ znajdujemy opis przestrzeni $T(M)$ jako

$$\text{lin}((4, 2, -2), (-4, -2, 2), (1, -1, 1)) = \text{lin}((4, 2, -2), (1, -1, 1)).$$

Zatem $\dim M = 2$. Układ trzech punktów: $(1, 2, 3)$, $(1, 2, 3) + (4, 2, -2)$, $(1, 2, 3) + (1, -1, 1)$ jest więc bazą punktową przestrzeni M .

Następujące własności baz punktowych są konsekwencjami odpowiednich własności baz przestrzeni liniowych oraz powyższego wniosku.

Obserwacja 8.4

Każda przestrzeń afiniczna ma bazę punktową. Jeśli $\dim H = k$, to każda baza punktowa przestrzeni H ma $k+1$ punktów. Układ p_0, \dots, p_k punktów w przestrzeni afinicznej H nad K jest bazą punktową przestrzeni H wtedy i tylko wtedy, dla każdego $p \in H$ istnieje dokładnie jeden układ wag $a_0, \dots, a_k \in K$ taki, że $p = a_0p_0 + \dots + a_kp_k$.

Definicja 8.4: Współrzędne barycentryczne

Niech H będzie przestrzenią afiniczną nad K i niech p_0, \dots, p_k będzie bazą punktową przestrzeni H . WSPÓLRZĘDNymi (BARYCENTRYCZNYMI) punktu $p \in H$ w BAZIE PUNKTOWEJ p_0, \dots, p_k nazywamy układ wag $a_0, \dots, a_k \in K$ taki, że $p = a_0p_0 + \dots + a_kp_k$.

Definicja 8.5: Układ bazowy i współrzędne w nim

Niech H będzie przestrzenią afiniczną nad K .

- Jeśli p_0 jest punktem przestrzeni H oraz $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$ jest bazą przestrzeni $T(H)$, to układ $p_0; \alpha_1, \dots, \alpha_n$ nazywamy UKŁADEM BAZOWYM dla przestrzeni H .
- Dla punktu p przestrzeni H układ a_1, \dots, a_n elementów ciała K taki, że $p = p_0 + a_1\alpha_1 + \dots + a_n\alpha_n$ nazywamy WSPÓLRZĘDNYMI PUNKTU p W UKŁADZIE BAZOWYM $p_0; \mathcal{A}$.

Odwzorowanie $K^n \rightarrow H$ opisane wzorem:

$$(s_1, \dots, s_n) \mapsto p_0 + s_1\alpha_1 + s_2\alpha_2 + \dots + s_n\alpha_n,$$

nazywamy PARAMETRYZACJĄ przestrzeni H .

Pojęcie parametryzacji stosuje się także w analizie np. przy opisie krzywych. Funkcja $t \mapsto (\cos t, \sin t)$ jest parametryzacją okręgu na płaszczyźnie, ale oczywiście nie jest to parametryzacja w sensie algebry liniowej. W przeciwieństwie do podanej parametryzacji okręgu, parametryzacje przestrzeni afinicznej opisane w powyższej definicji są zawsze bijekcjami. Oczywiście jasny jest także następujący wniosek.

Obserwacja 8.5

Układ p_0, \dots, p_n jest bazą punktową przestrzeni H wtedy i tylko wtedy, gdy układ $p_0; \overrightarrow{p_0p_1}, \dots, \overrightarrow{p_0p_n}$ jest układem bazowym przestrzeni H .

PRZYKŁAD. Niech $H = \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid 2x_1 - x_2 + 3x_3 = 5\}$. Wówczas $(1, 0, 1) \in H$ oraz

$$T(H) = \{(x_1, x_2, x_3) \mid 2x_1 - x_2 + 3x_3 = 0\} = \text{lin}((1, 2, 0), (0, 3, 1)).$$

Stąd $(1, 0, 1); (1, 2, 0), (0, 3, 1)$ jest układem bazowym w H , zaś przyporządkowanie

$$\mathbb{R}^2 \ni (s_1, s_2) \mapsto (1, 0, 1) + s_1(1, 2, 0) + s_2(0, 3, 1) = (s_1 + 1, 2s_1 + 3s_2, s_2 + 1) \in H$$

jest parametryzacją przestrzeni H .

Powyższe definicje afinicznej niezależności układu punktów, bazy punktowej i układu bazowego poprowadzą nas, podobnie jak w przypadku przestrzeni liniowych, do pojęcia przekształcenia afinicznego. Wcześniej jednak warto odnotować jeszcze szereg pojęć geometrycznych, które można określić już na początku pracy z przestrzeniami afinicznymi. Najważniejszym jest równoległość przestrzeni afinicznych, o którym mówiliśmy ostatnio. W zadaniach dotyczących przestrzeni afinicznych stosujemy specyficzną dla geometrii elementarnej nomenklaturę. Mówimy chociażby o tym, że

- PUNKT p LEŻY NA prostej/płaszczyźnie, co oznacza, że należy do tej prostej/płaszczyzny,
- prosta, płaszczyzna lub przestrzeń afiniczna PRZECHODZI PRZEZ DANY PUNKT, co znaczy, że ten punkt do niej należy,
- proste, płaszczyzny lub przestrzenie afiniczne PRZECINAJĄ SIĘ mając na myśli to, że odpowiednie przestrzenie afiniczne mają punkt wspólny (lub nie!),
- punkt p LEŻY POMIĘDZY PUNKTAMI q, r , jeśli $p = tq + (1 - t)r$, gdzie $0 < t < 1$ (tutaj nad \mathbb{R}),
- punkty p, q, r są WSPÓLLINIOWE, jeśli leżą na jednej prostej,
- podprzestrzenie F_1, F_2 SA SKOŚNE, to znaczy: $F_1 \cap F_2 = \emptyset$ oraz $T(F_1) \cap T(F_2) = \{0\}$.

Widzimy wyraźnie, że język geometrii afinicznej korzysta obficie ze znanego nam ze szkoły nazewnictwa obecnego w geometrii elementarnej płaszczyzny czy przestrzeni. Do pełni „geometrycznej operatywności” brakuje nam rzecz jasna kątów oraz odległości, a także izometrii. Te obiekty wprowadzimy rozważając strukturę przestrzeni euklidesowej w przestrzeni afinicznej. Wcześniej poznamy podstawy algebraicznego opisu przekształceń afinicznych³ – bardzo atrakcyjnych również z geometrycznego punktu widzenia.

³Książeczka dr. Jerzego Bednarczuka zawierająca podejście geometryczne do przekształceń afinicznych mówi nawet o „Uroku przekształceń afinicznych” (Biblioteczka Matematyczna, tom 36).

8.1 Afiniczna niezależność, baza punktowa, układ bazowy

Zadania ilustrujące umiejętności niezbędne do zaliczenia przedmiotu oznaczone są symbolem ♠. Przy tych zadaniach dodany jest opis umiejętności, które sprawdzają.

1. (♠ Wyznaczanie parametryzacji przestrzeni afinicznej)

- Znajdź bazę punktową oraz parametryzację płaszczyzny w \mathbb{R}^4 przechodzącej przez punkt $(3, 1, 2, 1)$ i równoległej do płaszczyzny H opisanej układem

$$\begin{cases} x_1 + x_2 - 2x_3 + x_4 = 2 \\ 2x_1 + 3x_2 - 2x_3 + x_4 = 3 \end{cases}$$

- Podaj parametryzację prostej zawartej w przestrzeni afinicznej \mathbb{R}^n przechodzącej przez dwa różne punkty $p_0 = (a_1, \dots, a_n)$ oraz $p_1 = (b_1, \dots, b_n)$.

2. (♠ Wyznaczanie współrzędnych barycentrycznych)

- Wyznacz współrzędne barycentryczne punktu $(4, 2)$ względem bazy punktowej $(1, 0), (6, 5), (6, -5)$ przestrzeni afinicznej \mathbb{R}^2 .
- Niech $p = (1, 0, i) \in \mathbb{C}^3$ oraz $p_0 = (1, 0, 1), p_1 = (2, i, 1), p_2 = (1 + i, 0, 2), p_3 = (1, i, 1)$. Wyznacz współrzędne barycentryczne punktu p w bazie punktowej $\{p_0, p_1, p_2, p_3\}$.

3. (♠ Znajdowanie przecięć przestrzeni afinicznych)

- W \mathbb{R}^3 znaleźć prostą L przechodzącą przez punkt $(2, 1, 4)$ i przecinającą proste L_1, L_2 zadane przez parametryzacje

$$L_1 : (0, 1, 1) + t(1, -1, 1), \quad L_2 : (2, 0, 1) + t(1, 3, 0).$$

- W \mathbb{R}^3 dane są: płaszczyzna $H : x_1 + x_2 + 2x_3 = 1$, prosta $L = (-2, 4, -3) + \text{lin}(0, 1, -2)$ oraz punkt $p = (1, 1, 0)$. Niech M będzie taką prostą, która przechodzi przez punkt p , przecina prostą L i nie przecina płaszczyzny H . Znaleźć punkt $L \cap M$.

- Niech $p = (-1, -1, 1) \in \mathbb{R}^3$ oraz

$$L_1 = (2, 3, 5) + \text{lin}((1, 2, 1)), \quad L_2 = \{(x_1, x_2, x_3 \in \mathbb{R}^3, | x_1 - x_2 + x_3 = 7, 3x_1 - 2x_2 + 2x_3 = 17\}.$$

Pokaż, że istnieje prosta $L \subseteq \mathbb{R}^3$ zawierająca punkt p i przecinająca obie proste L_1 oraz L_2 . Wyznacz punkty przecięcia prostej L z prostymi L_1 oraz L_2 .

- Niech H_1, H_2 będą nierównoległymi podprzestrzeniami afinicznymi \mathbb{R}^4 wymiaru 3. Czy jest prawdą, że $H_1 \cap H_2 \neq \emptyset$? Jeśli tak, to jakiego wymiaru jest przestrzeń afiniczna $H_1 \cap H_2$?

4. Niech H będzie przestrzenią afiniczną i $p_0, \dots, p_k \in H$. Załóżmy, że $q \in H$ jest takim punktem nienależącym do $\text{af}(p_0, p_1, \dots, p_k)$, że układ wektorów $\overrightarrow{qp_0}, \overrightarrow{qp_1}, \dots, \overrightarrow{qp_k}$ jest liniowo niezależny. Czy układ punktów p_0, p_1, \dots, p_k może być afinicznie zależny?

5. Układ p_0, p_1, \dots, p_k jest bazą punktową przestrzeni afinicznej H . Niech $\alpha \in T(H)$. Czy układ $p_0 + \alpha, p_1 + \alpha, \dots, p_k + \alpha$ również tworzy bazę punktową H ?

6. Niech p_0, p_1, \dots, p_n będzie bazą przestrzeni afinicznej H . Wykaż, że jeśli punkt $p \in H$ ma w tej bazie współrzędne a_0, a_1, \dots, a_n , to p ma w układzie bazowym $p_0; \overrightarrow{p_0 p_1}, \dots, \overrightarrow{p_0 p_n}$ współrzędne a_1, \dots, a_n .

7. Niech $B = \{p_0, p_1, \dots, p_n\}$ będzie bazą punktową przestrzeni afinicznej $H \subset K^n$. Udowodnij, że zbiór B jest bazą przestrzeni $\text{lin}(H)$ wtedy i tylko wtedy wektor zerowy (w K^n) należy do H .

8. Niech $H_1 \subset H_2$ będą podprzestrzeniami afinicznymi skończonego wymiaru. Wykaż, że jeśli zachodzi $\dim H_1 \geq \dim H_2$, to $H_1 = H_2$.

9. W przestrzeni afinicznej K^n nad ciałem K dane są punkty

$$p_1 = (a_{11}, \dots, a_{1n}), \quad p_2 = (a_{21}, a_{22}, \dots, a_{2n}), \quad \dots \quad p_s = (a_{s1}, a_{s2}, \dots, a_{sn}).$$

Niech $A = [a_{ij}] \in M_{s \times n}(K)$. Wykaż, że zachodzi nierówność

$$r(A) - 1 \leq \dim \text{af}(p_1, \dots, p_s) \leq r(A).$$

Pod jakimi warunkami w nierównościach tych zachodzą równości?

10. Niech z_1, z_2, \dots, z_n będą pierwiastkami stopnia n z 1. Wykaż, że jeśli liczby $w_1 \cdot w_2$ należą do wielokąta foremego W o wierzchołkach z_1, z_2, \dots, z_n , to liczba $w_1 \cdot w_2$ też należy do W .

8.2 Uzupełnienie. Wymiar przecięcia przestrzeni afinicznych

Wzajemne położenie przestrzeni afinicznych jest bardziej skomplikowane niż w przypadku przestrzeni liniowych, co odczytujemy choćby przez obecność nieprzecinających się prostych w przestrzeni trójwymiarowej. W trzech wymiarach nie pojawiają się poważniejsze komplikacje dotyczące położenia przestrzeni afinicznych. Jednak już dokonanie klasyfikacji wzajemnego położenia płaszczyzn w przestrzeni czterowymiarowej nie jest trywialnym zadaniem i prowadzi do pięciu konfiguracji. W zrozumieniu tych zależności pomóc nam może analog formuły Grassmanna w przestrzeniach afinicznych.

Twierdzenie 8.1: Formuła Grassmanna w przestrzeniach afinicznych

Niech H_1 oraz H_2 będą przestrzeniami afinicznymi w przestrzeni liniowej V . Wówczas:

- jeśli $H_1 \cap H_2 \neq \emptyset$, to

$$\dim(H_1 + H_2) = \dim(\text{af}(H_1, H_2)) = \dim H_1 + \dim H_2 - \dim(H_1 \cap H_2),$$

- jeśli $H_1 \cap H_2 = \emptyset$, to

$$\dim(H_1 + H_2) = \dim(\text{af}(H_1, H_2)) = \dim H_1 + \dim H_2 - \dim(T(H_1) \cap T(H_2)) + 1.$$

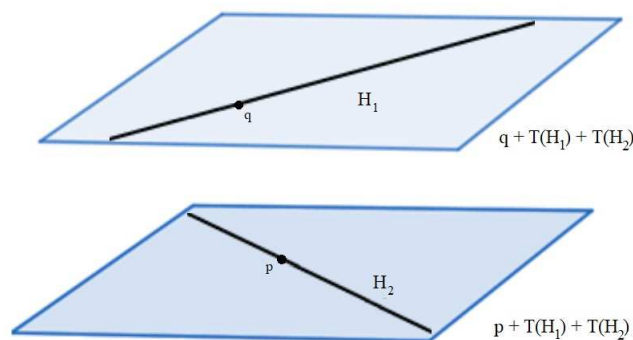
Uzasadnienie rozpoczniemy od następującego lematu.

Obserwacja 8.6

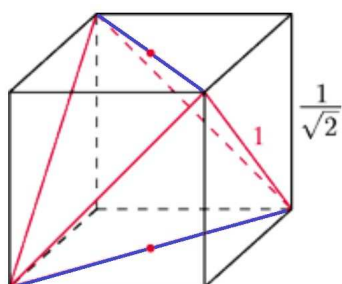
Jeśli dane są w przestrzeni liniowej przestrzenie afiniczne $H_1 = p_1 + T(H_1)$ oraz $H_2 = p_2 + T(H_2)$, to

$$H_1 \cap H_2 \neq \emptyset \iff \overrightarrow{p_1 p_2} \in T(H_1) + T(H_2).$$

Rozważmy poniższą ilustrację. Pokazuje ona typową sytuację: dwie proste skośne H_1, H_2 w przestrzeni \mathbb{R}^3 . Zwłaszcza w (przyszłym) kontekście liczenia odległości pomiędzy prostymi, bardzo wygodne jest zawarcie owych prostych w równoległych płaszczyznach, których przestrzenią styczną jest $T(H_1) + T(H_2)$



Oto przykład zastosowania tego spojrzenia dla szkolnego rachunku⁴ polegającego na wyznaczeniu odległości pomiędzy środkami przeciwległych krawędzi czworobocianu foremnego o krawędzi długości 1.



⁴Więcej: <https://www.deltami.edu.pl/temat/matematyka/geometria/stereometria/2014/01/31/2014-02-k25.pdf>.

Dowód. Jeśli istnieje punkt $r = p_1 + \alpha_1 = p_2 + \alpha_2$, gdzie $\alpha_1 \in T(H_1)$ oraz $\alpha_2 \in T(H_2)$, to

$$\overrightarrow{p_1 p_2} = \overrightarrow{p_1 r} + \overrightarrow{r p_2} = \alpha_1 - \alpha_2 \in T(H_1) + T(H_2).$$

Z drugiej strony, jeśli $\overrightarrow{p_1 p_2} \in T(H_1) + T(H_2)$, to $\overrightarrow{p_1 p_2} = \alpha_1 + \alpha_2$, gdzie $\alpha_1 \in T(H_1)$, $\alpha_2 \in T(H_2)$, co daje nam

$$p_2 = p_1 + \overrightarrow{p_1 p_2} = p_1 + \alpha_1 + \alpha_2,$$

a stąd

$$p_1 + \alpha_1 = p_2 - \alpha_2 \in (p_1 + T(H_1)) \cap (p_2 + T(H_2)).$$

□

Obserwacja 8.7

Jeśli dane są w przestrzeni liniowej przestrzenie afiniczne $H_1 = p_1 + T(H_1)$ oraz $H_2 = p_2 + T(H_2)$, to

$$r \in H_1 \cap H_2 \implies H_1 \cap H_2 = r + (T(H_1) \cap T(H_2)).$$

Dowód. Na mocy Obserwacji 7.1 wiemy, że $p_1 + T(H_1) = r + T(H_1)$ oraz $p_2 + T(H_2) = r + T(H_2)$. Stąd

$$H_1 \cap H_2 = (r + T(H_1)) \cap (r + T(H_2)) = r + (T(H_1) \cap T(H_2)).$$

□

Dla dowodu formuły Grassmanna niezbędne jest określenie sumy przestrzeni afinicznych.

Definicja 8.6: Suma podprzestrzeni afinicznych

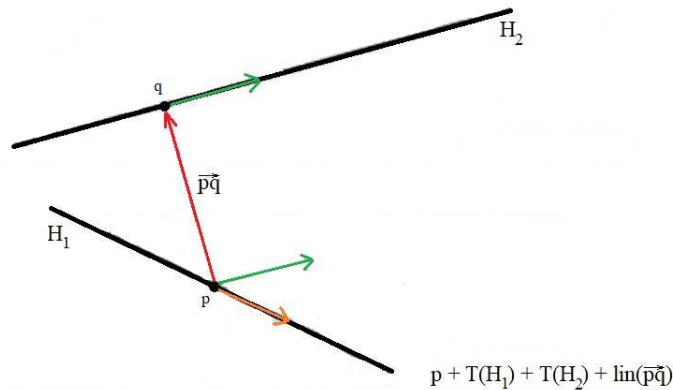
Jeśli H_1, H_2 są przestrzeniami afinicznymi w przestrzeni liniowej V , wówczas przez $H_1 + H_2$ definiujemy najmniejszą podprzestrzeń afiniczną zawierającą H_1 oraz H_2 , czyli $\text{af}(H_1, H_2)$.

Opis sumy podprzestrzeni jest bardzo prosty.

Obserwacja 8.8

Jeśli dane są w przestrzeni liniowej przestrzenie afiniczne $H_1 = p_1 + T(H_1)$ oraz $H_2 = p_2 + T(H_2)$, to

$$H_1 + H_2 = p_1 + (T(H_1) + T(H_2) + \text{lin}(\overrightarrow{p_1 p_2})).$$



Dowód. Załóżmy, że L jest przestrzenią afiniczną zawierającą H_1 oraz H_2 . Skoro p_1, p_2 należą do L , to istnieje podprzestrzeń W taka, że $L = p_1 + W = p_2 + W$ oraz $\text{lin}(\overrightarrow{p_1 p_2}) \subseteq W$. Jednak $H_1 \subseteq L$ implikuje $T(H_1) \subseteq W$ i podobnie $H_2 \subseteq L$ implikuje $T(H_2) \subseteq W$. A zatem

$$T(H_1) + T(H_2) + \text{lin}(\overrightarrow{p_1 p_2}) \subseteq W$$

oraz $p_1 + (T(H_1) + T(H_2) + \text{lin}(\overrightarrow{p_1 p_2})) \subseteq L$. A zatem $p_1 + (T(H_1) + T(H_2) + \text{lin}(\overrightarrow{p_1 p_2}))$ zawarta jest w $\text{af}(H_1, H_2)$. Z drugiej strony $\text{af}(H_1, H_2) \subseteq p_1 + (T(H_1) + T(H_2) + \text{lin}(\overrightarrow{p_1 p_2}))$, co daje tezę. □

Jesteśmy gotowi na dowód formuły Grassmanna. Załóżmy najpierw, że $H_1 \cap H_2 \neq \emptyset$. Zgodnie z Obserwacją 8.6 mamy

$$T(H_1) + T(H_2) + \text{lin}(\overrightarrow{p_1 p_2}) = T(H_1) + T(H_2),$$

a zatem zgodnie z Obserwacją 8.8 mamy:

$$H_1 + H_2 = p_1 + T(H_1) + T(H_2).$$

Zatem:

$$\begin{aligned} \dim(H_1 + H_2) &= \dim(T(H_1) + T(H_2)) \\ &= \dim T(H_1) + \dim T(H_2) - \dim(T(H_1) \cap T(H_2)) \\ &= \dim H_1 + \dim H_2 - \dim(H_1 \cap H_2), \end{aligned}$$

bo zgodnie z Obserwacją 8.7 mamy $\dim(H_1 \cap H_2) = \dim(T(H_1) \cap T(H_2))$.

Dowodzimy tezę w przypadku, gdy $H_1 \cap H_2 = \emptyset$. Wówczas zgodnie z Obserwacją 8.6 mamy

$$(T(H_1) + T(H_2)) \cap \text{lin}(\overrightarrow{p_1 p_2}) = 0,$$

a zatem zgodnie z Obserwacją 8.8 mamy

$$\begin{aligned} \dim(H_1 + H_2) &= \dim(T(H_1) + T(H_2) + \text{lin}(\overrightarrow{p_1 p_2})) \\ &= \dim(T(H_1) + T(H_2)) + \dim(\text{lin}(\overrightarrow{p_1 p_2})) \\ &= \dim T(H_1) + \dim T(H_2) - \dim(T(H_1) \cap T(H_2)) + 1 \\ &= \dim H_1 + \dim H_2 - \dim(T(H_1) \cap T(H_2)) + 1 \end{aligned}$$

* * *

Zauważmy, że w drugiej części rozumowania nie można wymienić $\dim(T(H_1) \cap T(H_2))$ na $\dim(H_1 \cap H_2)$. Zauważmy, że biorąc w \mathbb{R}^4 :

$$\begin{aligned} H_1 &= (0, 0, 0, 0) + \text{lin}((1, 0, 0, 0), (0, 1, 0, 0)) \\ H_2 &= (0, 0, 0, 1) + \text{lin}((0, 1, 0, 0), (0, 0, 1, 0)) \end{aligned}$$

widzimy, że $H_1 \cap H_2 = \emptyset$, ale płaszczyzny te nie są równoległe. Mamy przy tym

$$\dim(H_1 + H_2) = 2 + 2 - \dim(T(H_1) \cap T(H_2)) + 1 = 5 - 1 = 4.$$

Ogólne możliwe konfiguracje par płaszczyzn w przestrzeni wymiaru 4 opisuje poniższy wniosek. Zachęcam do wskazania przykładów odpowiednich konfiguracji.

Wniosek 8.1

Jeśli dane są w przestrzeni \mathbb{K}^4 przestrzenie afiniczne $H_1 = p_1 + T(H_1)$ oraz $H_2 = p_2 + T(H_2)$, przy czym $\dim H_1 = \dim H_2 = 2$, to:

1. Jeśli $H_1 \cap H_2 \neq \emptyset$, to $\dim(H_1 + H_2) = 2 + 2 - \dim(H_1 \cap H_2) = 4 - \dim(H_1 \cap H_2)$, przy czym
 - jeśli $\dim(H_1 \cap H_2) = 0$, to $H_1 \cap H_2$ jest punktem,
 - jeśli $\dim(H_1 \cap H_2) = 1$, to $H_1 \cap H_2$ jest prostą,
 - jeśli $\dim(H_1 \cap H_2) = 2$, to $H_1 = H_2$.
2. Jeśli $H_1 \cap H_2 = \emptyset$, to $\dim(H_1 + H_2) = 2 + 2 - \dim(T(H_1) \cap T(H_2)) + 1 = 5 - \dim(T(H_1) \cap T(H_2))$, przy czym
 - jeśli $\dim(T(H_1) \cap T(H_2)) = 1$, są to płaszczyzny skośne,
 - jeśli $\dim(T(H_1) \cap T(H_2)) = 2$, są to płaszczyzny równoległe.

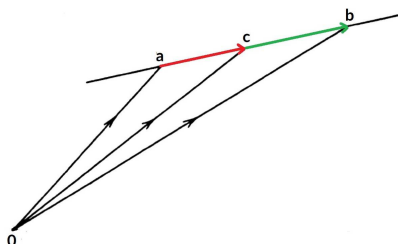
8.3 Dodatek. Współliniowość, współrzędne barycentryczne oraz intuicje i twierdzenia geometrii elementarnej

Przy pomocy rachunku wektorowego w przestrzeni afinicznej dowodzić można klasyczne twierdzenia geometrii⁵. Przyjrzyjmy się przede wszystkim pojęciu współliniowości w rzeczywistej przestrzeni afinicznej. Mówimy o trójkach punktów, które są albo w położeniu ogólnym, co najczęściej kwitujemy mówiąc, że tworzą one trójkąt niezdegenerowany, albo są współliniowe — są w położeniu szczególnym (w tym równe).

Obserwacja 8.9

Jeśli c jest dowolnym punktem na prostej wyznaczonej przez dwa różne punkty a, b w przestrzeni afinicznej nad \mathbb{R} (czyli $\text{af}(a, b)$), który jest od nich różny, to istnieje $\lambda \in \mathbb{R}$ takie, że $c = (1 - \lambda)a + \lambda b$, przy czym zachodzi równość

$$\vec{cb} = \frac{\lambda}{1 - \lambda} \cdot \vec{ac}.$$



Dowód. Skoro c jest kombinacją afiniczną punktów a, b , to niech $c = (1 - \lambda)a + \lambda b$. Zatem $c - a = \lambda(b - a)$, co w konsekwencji daje $\vec{ac} = \lambda \vec{ab}$. Z drugiej strony $b - c = (1 - \lambda)(b - a)$, czyli $\vec{cb} = (1 - \lambda)\vec{ab}$. \square

Spójrzmy na powyższą równość w inny sposób.

Obserwacja 8.10

Jeśli punkty a, b, c przestrzeni afinicznej nad \mathbb{R} są współliniowe, to istnieją liczby $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$, nie wszystkie równe 0, spełniające warunki:

$$\lambda_1 + \lambda_2 + \lambda_3 = 0 \quad \text{oraz} \quad \lambda_1 a + \lambda_2 b + \lambda_3 c = 0.$$

Dowód. Jeśli $a = b = c$, to teza jest oczywista. Załóżmy, że a, b są różne. Wówczas zgodnie z poprzednią obserwacją możemy zapisać $c = (1 - \lambda)a + \lambda b$, dla pewnego λ . Mamy zatem:

$$(1 - \lambda)a + \lambda b + (-1)c = 0,$$

czyli biorąc $\lambda_1 = 1 - \lambda$, $\lambda_2 = \lambda$ oraz $\lambda_3 = -1$ dostajemy tezę. \square

Kluczowe jest odwrócenie powyższego faktu.

Obserwacja 8.11

Jeśli dane są punkty a, b, c oraz liczby rzeczywiste $\lambda_1, \lambda_2, \lambda_3$, nie wszystkie równe 0, dla których $\lambda_1 + \lambda_2 + \lambda_3 = 0$ oraz $\lambda_1 a + \lambda_2 b + \lambda_3 c = 0$, wówczas punkty a, b, c są współliniowe.

Dowód. Ewentualnie zmieniając nazwy punktów możemy założyć, że $\lambda_1 \neq 0$. Możemy zapisać:

$$a = -\frac{\lambda_2}{\lambda_1}b - \frac{\lambda_3}{\lambda_1}c.$$

Skoro $\lambda_1 + \lambda_2 + \lambda_3 = 0$, to $-\frac{\lambda_2}{\lambda_1} - \frac{\lambda_3}{\lambda_1} = 1$. A zatem kładąc $\lambda = -\frac{\lambda_3}{\lambda_1}$, to $1 - \lambda = -\frac{\lambda_2}{\lambda_1}$ uzyskujemy

$$a = (1 - \lambda)b + \lambda c.$$

Jeśli b, c nie są różne, to oczywiście a, b, c są współliniowe. Jeśli natomiast b, c są różne, to $a \in \text{af}(b, c)$. \square

⁵Tekst na podstawie książki D. Pedoe, *Geometry, a comprehensive course*, Dover Publications 1988.

Wniosek 8.2

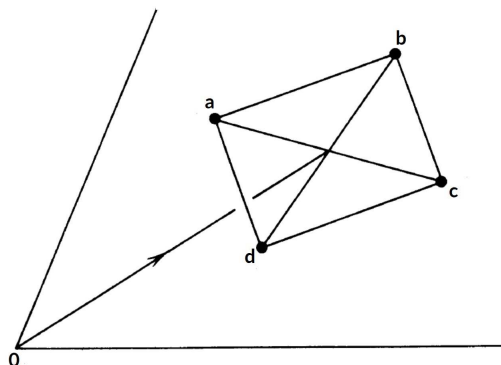
Jeśli a, b, c są niewspółliniowymi punktami oraz jeśli istnieją liczby rzeczywiste λ_1, λ_2 oraz λ_3 takie, że $\lambda_1 + \lambda_2 + \lambda_3 = 0$ oraz $\lambda_1 a + \lambda_2 b + \lambda_3 c = 0$, to $\lambda_1 = \lambda_2 = \lambda_3 = 0$.

Zobaczmy kilka zastosowań.

Obserwacja 8.12

Założmy, że a, b, c, d są parami różne. Następujące warunki są równoważne:

- czworokąt a, b, c, d jest równoległobokiem, tzn. $\vec{ab} = \vec{dc}$ (równoważnie $\vec{ad} = \vec{bc}$),
- $af(a, c) \cap af(b, d) = \frac{1}{2}a + \frac{1}{2}c = \frac{1}{2}b + \frac{1}{2}d$, tzn. przekątne czworokąta $abcd$ przecinają się w połowie.



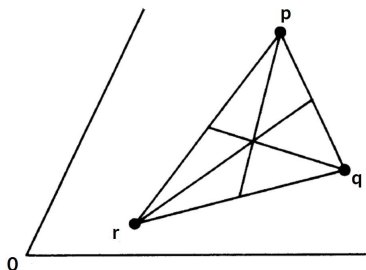
Dowód. Mamy równoważności $\vec{ab} = \vec{dc} \iff b - a = c - d \iff b + d = c + a \iff \frac{1}{2}b + \frac{1}{2}d = \frac{1}{2}c + \frac{1}{2}a$. \square

Obserwacja 8.13

W trójkącie o wierzchołkach p, q, r środkowe przecinają się w jednym punkcie

$$\frac{1}{3}p + \frac{1}{3}q + \frac{1}{3}r,$$

który dzieli je w stosunku 1 : 2.



Dowód. Kładąc $\lambda = \frac{2}{3}$ we wzorze $z = (1 - \lambda)x + \lambda y$ widzimy, że punkt, który dzieli wektor \vec{xy} w stosunku 2 : 1 to punkt $z = \frac{1}{3}x + \frac{2}{3}y$. Środkiem odcinka qr jest $p' = \frac{1}{2}q + \frac{1}{2}r$ i punkt, który dzieli wektor $\vec{pp'}$ w stosunku 1 : 2 to

$$\frac{2}{3} \left(\frac{q + r}{2} \right) + \frac{p}{3} = \frac{p + q + r}{3}.$$

Symetria tego rozumowania daje zatem tezę. \square

Przejdziemy teraz do znanego faktu konkursowego, zapewne niepokazywanego w szkole.

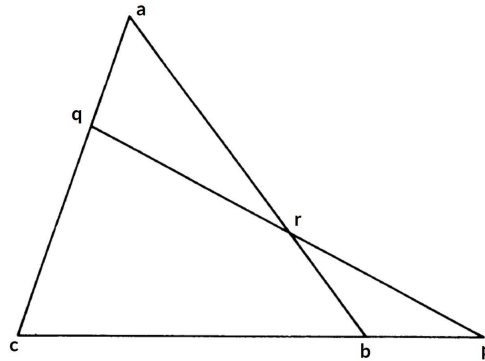
Twierdzenie 8.2: Menelaos

Pewna prosta przecina proste $af(b, c)$, $af(c, a)$, $af(a, b)$ (zawierające boki trójkąta abc) w punktach p, q, r . Wówczas jeśli dla pewnych $x_1, x_2, x_3, y_1, y_2, y_3 \in \mathbb{R}$ spełniających $x_1 + y_1 = 1, x_2 + y_2 = 1$ oraz $x_3 + y_3 = 1$ mamy:

$$p = x_1b + y_1c, \quad q = x_2c + y_2a, \quad r = x_3a + y_3b,$$

wówczas $x_1x_2x_3 = -y_1y_2y_3$, czyli równoważnie^a:

$$\frac{\vec{bp}}{\vec{pc}} \cdot \frac{\vec{cq}}{\vec{qa}} \cdot \frac{\vec{ar}}{\vec{rb}} = -1.$$



^aPorównujemy stosunki podziałów wektorów, czyli pisząc $\lambda = \frac{\vec{a}}{\vec{b}}$, mamy na myśli $\vec{a} = \lambda \cdot \vec{b}$,

Dowód. Skorzystamy z Obserwacji 8.7. Skoro p, q, r są współliniowe, to istnieją liczby rzeczywiste $\lambda_1, \lambda_2, \lambda_3$, nie wszystkie równe 0, takie że $\lambda_1 + \lambda_2 + \lambda_3 = 0$ oraz $\lambda_1p + \lambda_2q + \lambda_3r = 0$. Stąd

$$\lambda_1(x_1b + y_1c) + \lambda_2(x_2c + y_2a) + \lambda_3(x_3a + y_3b) = 0,$$

czyli równoważnie

$$(\lambda_1x_1 + \lambda_3y_3)b + (\lambda_2x_2 + \lambda_1y_1)c + (\lambda_3x_3 + \lambda_2y_2)a = 0.$$

Zauważmy, że suma współczynników powyższej kombinacji to

$$(\lambda_1x_1 + \lambda_3y_3) + (\lambda_2x_2 + \lambda_1y_1) + (\lambda_3x_3 + \lambda_2y_2) = \lambda_1(x_1 + y_1) + \lambda_2(x_2 + y_2) + \lambda_3(x_3 + y_3) = \lambda_1 + \lambda_2 + \lambda_3 = 0.$$

Biorąc pod uwagę, że punkty a, b, c nie są współliniowe jako wierzchołki trójkąta (układ afinicznie niezależny), na mocy Wniosku 8.1 mamy zatem

$$\lambda_1x_1 + \lambda_3y_3 = \lambda_2x_2 + \lambda_1y_1 = \lambda_3x_3 + \lambda_2y_2 = 0.$$

Stąd

$$(\lambda_1x_1)(\lambda_2x_2)(\lambda_3x_3) = (-\lambda_3y_3)(-\lambda_1y_1)(-\lambda_2y_2).$$

Pozostaje rozważyć kilka przypadków.

- Jeśli żadna z liczb $\lambda_1, \lambda_2, \lambda_3$ nie jest równa 0, to od razu dostajemy tezę $x_1x_2x_3 = -y_1y_2y_3$.
- Skoro nie wszystkie z liczb $\lambda_1, \lambda_2, \lambda_3$ mogą być równe 0, to nie więcej niż jedna jest równa 0. Załóżmy, że $\lambda_1 = 0$. Wówczas $\lambda_2 + \lambda_3 = 0$, to $\lambda_2 = -\lambda_3 \neq 0$, i z równości $\lambda_2q + \lambda_3r = 0$, więc $q = r$. Zakładamy jednak, że p, q, r są różne. Inaczej bowiem tego teza jest oczywista.

□

Zachęcam Czytelnika do zastanowienia się nad możliwymi konfiguracjami punktów p, q, r . Niekoniecznie leżą one na bokach trójkąta a, b, c . Proszę pomyśleć też o sformułowaniu twierdzenia odwrotnego i spróbować je udowodnić.

Współrzędne barycentryczne punktu w bazie punktowej przestrzeni afinicznej pozwalają wprowadzić swego rodzaju wewnętrzny układ współrzędnych na przestrzeni afinicznej. Przyjrzymy się temu w przypadku rozważanej już sytuacji, gdy dany jest układ trzech punktów w położeniu ogólnym — trójkąt abc , którego wierzchołki określają nowy „układ współrzędnych”. Przypomnijmy fakt z wykładu w tymże języku.

Obserwacja 8.14

Jeśli punkty a, b, c rzeczywistej przestrzeni afinicznej są niewspółliniowe (są afinicznie niezależne), to każdy punkt p płaszczyzny $af(a, b, c)$ można zapisać w postaci

$$p = \lambda_1 a + \lambda_2 b + \lambda_3 c, \quad \text{gdzie } \lambda_1 + \lambda_2 + \lambda_3 = 1.$$

Dla danego punktu p liczby $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$ są wyznaczone jednoznacznie.

Pomyślmy o naszych współrzędnych jak o trójkach postaci $(\lambda_1 : \lambda_2 : \lambda_3)$. Wówczas mamy

$$a = (1 : 0 : 0), \quad b = (0 : 1 : 0), \quad c = (0 : 0 : 1).$$

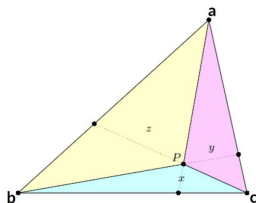
Czy wiemy coś jeszcze? Owszem, środek odcinka ab to $(\frac{1}{2} : \frac{1}{2} : 1)$, zaś środek odcinka bc to $(0 : \frac{1}{2} : \frac{1}{2})$. Jeśli Czytelnikowi wydaje się, że to mało, zachęcam do sprawdzenia⁶, że również inne punkty szczególne w trójkącie wyrażają się elegancko w tych współrzędnych. Jeśli $|a|, |b|, |c|$ to długości boków trójkąta abc , zaś α, β, γ to miary kątów wewnętrznych w tym trójkącie (kąt α naprzeciw a itd.) to:

- współrzędne środka ciężkości trójkąta abc to $(\frac{1}{3} : \frac{1}{3} : \frac{1}{3})$,
- współrzędne środka okręgu wpisanego to $(\frac{|a|}{|a|+|b|+|c|} : \frac{|b|}{|a|+|b|+|c|} : \frac{|c|}{|a|+|b|+|c|})$,
- współrzędne przecięcia wysokości (ortocentrum) to $(\frac{\text{tg } \alpha}{\text{tg } \alpha + \text{tg } \beta + \text{tg } \gamma} : \frac{\text{tg } \beta}{\text{tg } \alpha + \text{tg } \beta + \text{tg } \gamma} : \frac{\text{tg } \gamma}{\text{tg } \alpha + \text{tg } \beta + \text{tg } \gamma})$.

Te współrzędne nie wyglądają na pierwszy rzut oka zachęcająco, więc być może warto powiedzieć kilka słów o ich genezie związanej z masami, ciężarami i wyporami, pochodzącej od Ferdinanda Möbiusa. Cytujemy tu świetny artykuł prof. Marka Kordosa⁷. Pomyślmy jakie ciężary należy umieścić w wierzchołkach trójkąta, aby jego środek ciężkości znalazł się we wskazanym punkcie w jego wnętrzu? To może dziwne pytanie, ale jeśli postawimy analogiczne pytanie dla odcinka o końcach w punktach (różnych) a, b i zadamy punkt x , na którym znajdować się ma równowaga po przyłożeniu odpowiednio do a, b mas $\frac{m_a}{m_b}$ oraz m_b , to zachodzić musi znane z fizyki prawo (Archimedes) dźwigni $m_a \cdot \vec{ax} = m_b \cdot \vec{xb}$, czyli $\frac{m_a}{m_b} = \frac{\vec{xb}}{\vec{ax}}$.

Można tu pytać jak interpretować ujemne współczynniki? Czy chodzi o masy ujemne? Już Archimedes wiedział, że efektywna siła ciężkości może działać zarówno w dół, jak i do góry. Ta druga sytuacja ma miejsce na przykład przy unoszeniu się balonu, albo podczas unoszenia się na powierzchni wody statku. Owe „ujemne ciężary” można nazwać *wyporem*. Tu dochodzimy do związku naszych zagadnień z wypukłością. Otóż okazuje się, że punkt o wszystkich nieujemnych współrzędnych barycentrycznych leżeć musi wewnątrz lub na obwodzie trójkąta abc , a więc jest elementem powłoki wypukłej $\text{conv}(a, b, c)$.

Chcąc jeszcze bardziej namieszać Czytelnikowi w głowie mogę dodać (choć jeszcze nie wiemy co to jest pole), że współrzędne barycentryczne nazywano kiedyś współrzędnymi arealnymi. Wiąże się to z faktem, że punkt p o współrzędnych barycentrycznych $(\lambda_1 : \lambda_2 : \lambda_3)$ wyznacza trójkąty pcb, pba, pac o polach (skierowanych, cokolwiek to znaczy), których stosunek do pola trójkąta abc to odpowiednio $\lambda_1, \lambda_2, \lambda_3$.



Spróbujmy przekonać Czytelnika, że współrzędne barycentryczne mogą mu się do czegoś przydać.

⁶... lub przeczytania, np. pod adresem <https://web.evanchen.cc/handouts/bary/bary-full.pdf>.

⁷<https://www.deltami.edu.pl/temat/matematyka/geometria/planimetria/2012/02/29/wypory.pdf>.

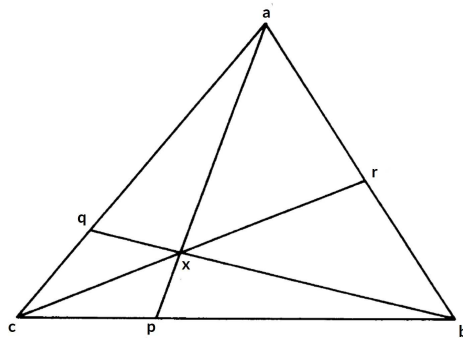
Twierdzenie 8.3: Ceva

Dany jest trójkąt abc i punkt $x \in \text{af}(a, b, c)$. Proste $\text{af}(a, x)$, $\text{af}(b, x)$, $\text{af}(c, x)$ przecinają boki bc , ca , ab trójkąta abc w punktach p , q , r . Niech $x_1, x_2, x_3, y_1, y_2, y_3 \in \mathbb{R}$ będą takimi liczbami spełniającymi $x_1 + y_1 = 1, x_2 + y_2 = 1$ oraz $x_3 + y_3 = 1$, że:

$$p = x_1b + y_1c, \quad q = x_2c + y_2a, \quad r = x_3a + y_3b.$$

Wówczas $x_1x_2x_3 = y_1y_2y_3$, czyli równowaznie:

$$\frac{\vec{bp}}{\vec{pc}} \cdot \frac{\vec{cq}}{\vec{qa}} \cdot \frac{\vec{ar}}{\vec{rb}} = 1.$$



Dowód. Zapiszmy $x = \lambda_1a + \lambda_2b + \lambda_3c$, gdzie $\lambda_1 + \lambda_2 + \lambda_3 = 1$. Możemy również napisać:

$$x = \lambda_1a + (\lambda_2 + \lambda_3)y,$$

gdzie

$$y = (\lambda_2b + \lambda_3c)/(\lambda_2 + \lambda_3).$$

Na mocy pierwszego z równań wyżej punkty x, a, y są współliniowe, zaś na mocy drugiego — punkty y, b, c są współliniowe. Zatem punkt y leży na ap oraz leży na bc . Zatem mamy $y = p = x_1b + y_1c$. Stąd:

$$\frac{x_1}{y_1} = \frac{\lambda_1}{\lambda_2}.$$

Stąd natychmiast wynika teza. □

Warto pokazać jeszcze pewien alternatywny dowód, pokazujący więcej narzędzi stosowanych w rozwiązywaniu zadań olimpijskich⁸. Zachęcam Czytelnika do przeprowadzenia dowodu poniższej obserwacji.

Obserwacja 8.15

Rozważmy płaszczyznę $\text{af}(a, b, c)$, gdzie a, b, c są afinicznie niezależne. Wówczas dla każdego układu liczb u, v, w , gdzie $(u, v, w) \neq (0, 0, 0)$ zbiór punktów o współrzędnych barycentrycznych $(\lambda_1, \lambda_2, \lambda_3)$ takich, że

$$u\lambda_1 + v\lambda_2 + w\lambda_3 = 0 \quad (*)$$

jest prostą.

Aby Czytelnik poczuł ideę, zauważmy, że równanie prostej zawierającej punkty a, b to po prostu $\lambda_3 = 0$, bowiem równanie $(*)$ muszą spełniać punkty $a = (1 : 0 : 0)$ oraz $b = (0 : 1 : 0)$. Wracając do twierdzenia Ceva i jego dowodu — zachęcam Czytelnika do pokazania, że jeśli $p = (0, d, 1 - d)$, $q = (1 - e, 0, e)$ oraz $r = (f, 1 - f, 0)$, wówczas proste $\text{af}(a, p)$, $\text{af}(b, q)$, $\text{af}(c, r)$ mają równania odpowiednio

$$\lambda_3 = \frac{1-d}{d}\lambda_2, \quad \lambda_1 = \frac{1-e}{e}\lambda_3, \quad \lambda_2 = \frac{1-f}{f}\lambda_1.$$

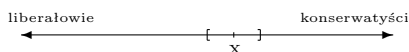
Kiedy te proste mają punkt wspólny (o pewnych współrzędnych barycentrycznych)?

⁸Nie sposób nie odesłać tu do Evana Chena: <https://web.evanchen.cc/handouts/bary/bary-full.pdf>.

8.4 Trivia. Twierdzenie Helly’ego

Kiedy możliwe jest porozumienie? Jak decyzja grupy ludzi zależy od indywidualnych preferencji? W określonych warunkach odpowiedzi na te pytania dostarczyć może klasyczny już dziś rezultat teorii zbiorów wypukłych należący do austriackiego matematyka z przełomu XIX. i XX. wieku – Eduarda Helly’ego.

Każdy ma swoje „idealne” preferencje. W imię koniecznego kompromisu jesteśmy jednak zdolni do zaakceptowania opcji dostatecznie „bliskich” naszym oczekiwaniom. Klasyczną sytuacją jest tu uproszczony model głosowania z jednowymiarowym spektrum, w którym konserwatystów umieszczamy po prawej stronie osi, liberałów zaś po lewej tak, jak na rysunku poniżej.



Każdy punkt naszego modelu oznacza pewien możliwy wybór. Każdemu wyborcy X przyporządkowujemy przedział I_X akceptowalnych przez niego kandydatów. Załóżmy, że na karcie wyborczej wolno mu zaznaczyć cały przedział I_X .⁹ Przy jakich warunkach możemy określić kiedy społeczeństwo „zgodzi” się na określonego kandydata?

Odpowiedzi na postawione wyżej pytania mogą być dość zaskakujące. Okazuje się, że jeśli każdych dwóch wyborców skłonnych będzie zaakceptować pewną kandydaturę, to wybrana zostanie osoba akceptowana przez całe społeczeństwo!¹⁰ Wydaje się to nieprawdopodobne, ale jeśli wysłowimy tę obserwację w języku matematyki stojącej za tym modelem dostaniemy całkiem intuicyjny fakt.

Obserwacja 8.16

Dana jest rodzina \mathcal{I} przedziałów domkniętych w \mathbb{R} , przy czym $|\mathcal{I}| > 1$. Jeśli dla każdych $I, J \in \mathcal{I}$ zachodzi warunek $I \cap J \neq \emptyset$, to przecięcie wszystkich elementów rodziny \mathcal{I} jest niepuste.

Podaliśmy w ten sposób najprostszy możliwy, bo jednowymiarowy, przypadek twierdzenia Helly’ego. Aby go udowodnić nie potrzeba żadnej skomplikowanej technologii. Przedstawiona wyżej interpretacja społeczna jest naturalnie jedną z wielu możliwych. Czytelnik zachęcony powyższym przykładem będzie w stanie wskazać wiele innych „z życia wziętych” sytuacji, do których fakt idealnie pasuje. Można też przy pomocy twierdzenia Helly’ego rozwiązywać nietrywialne zadania geometryczne.

Zadanie 8.1. Na płaszczyźnie położona jest dowolna skończona rodzina wielokątów \mathcal{F} (niekoniecznie wypukłych) o tej własności, że każde dwa jej elementy mają punkt wspólny. Pokaż, że dla dowolnego punktu P na płaszczyźnie istnieje okrąg o środku w P mający punkt wspólny z każdym wielokątem z \mathcal{F} .

Rozwiązanie. Wybieramy P i ustalamy dowolną półprostą l przechodzącą przez ten punkt. Rozważamy przekształcenie $f : \mathbb{R}^2 \rightarrow l$ zadane w następujący sposób: każdy okrąg O_r o środku w P i promieniu $r \geq 0$ przeprowadzamy na punkt $O_r \cap l$. Nietrudno widzieć¹¹, że każdy z wielokątów należących do \mathcal{F} przejdzie na pewien odcinek domknięty na l . Z założenia $f(W_1) \cap f(W_2) \neq \emptyset$, gdzie $W_1, W_2 \in \mathcal{F}$. Z twierdzenia Helly’ego przecięcie wszystkich odcinków postaci $f(W)$, $W \in \mathcal{F}$ jest niepuste. Wiadomo już zatem jaki okrąg wybrać, prawda?

Wróćmy jeszcze na moment do interpretacji społecznych. Czasami do podjęcia decyzji potrzeba więcej niż jednej informacji. Na przykład: nasz idealny kandydat¹² powinien nie tylko być po „właściwej stronie”. Chcemy też wiedzieć czy jest raczej pacyfistą, czy może pragnie wojen? Czy zamierza dużo podróżować, czy raczej nie? W naszym modelu dodajemy więc kolejne osie – spektrum wyboru staje się przestrzenią wymiaru 2, 3, a czasem i większego. Wyborca X ma w nim już nie przedział, ale n – wymiarowy zbiór I_X akceptowalnych przez siebie opcji. Okazuje się, że im więcej wymiarów, tym bardziej zgodnego społeczeństwa potrzebujemy. Przy jednym parametrze jedynie każdych dwóch wyborców musiało się zgadzać. Przy dwóch parametrach potrzeba, by kompromis osiągało każdych trzech. W trójwymiarowym modelu zgodni muszą być dowolni czterej, itd. Samo to nie wystarcza jeszcze do jednomyślnego rozstrzygnięcia.

⁹W podobny sposób wybierają swoje władze matematycy w USA...

¹⁰A na jakie poparcie może liczyć potencjalny zwycięzca, jeśli spośród każdych trzech wyborców tylko dwóm udaje się wypracować wspólne stanowisko?

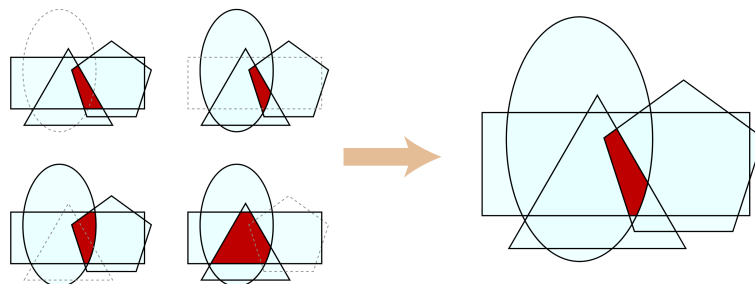
¹¹Czy przez dowolny punkt P można przeprowadzić pewną prostą przecinającą każdy wielokąt z \mathcal{F} ?

¹²Serwis randkowy *eHarmony* używa przestrzeni wymiaru 29...

Trzeba coś założyć o zbiorach I_X . I tu możliwości jest wiele. Każda z nich to pewna odmiana twierdzenia Helly'ego. Najbardziej klasycznym założeniem jest wypukłość.

Twierdzenie 8.4: Helly, 1913

Dana jest skończona rodzina \mathcal{I} zbiorów wypukłych w \mathbb{R}^n , przy czym $|\mathcal{I}| > n$. Jeśli każde $n + 1$ z nich ma niepuste przecięcie, to przecięcie wszystkich elementów rodziny \mathcal{I} jest niepuste.



Twierdzenie to ukazuje swoistą sztywność zbiorów wypukłych. Jako ilustrację proponujemy zadanie.

Zadanie 8.2. Na płaszczyźnie leży n punktów $A_1, A_2, A_3, \dots, A_n$, przy czym $n \geq 3$. Dla każdych trzech punktów z tego zbioru istnieje koło o promieniu 1, które je zawiera. Udowodnij, że wszystkie te punkty leżą w pewnym kole o promieniu 1.

ROZWIĄZANIE. Niech k_1, k_2, k_3 będą kołami o środkach w punktach A_1, A_2, A_3 i promieniach równych 1. Zgodnie z założeniem istnieje koło k o promieniu 1 i środku a , że $A_1, A_2, A_3 \in k$. Równoważnie: $a \in k_1 \cap k_2 \cap k_3 \neq \emptyset$. Zatem rodzina kół $\{k_i\}_{i \in \{1, 2, 3, \dots, n\}}$ o środkach w A_i i promieniu 1 spełnia założenia twierdzenia Helly'ego w przypadku dwuwymiarowym: jest to rodzina zbiorów wypukłych, w której każde trzy elementy mają niepuste przecięcie. Istnieje więc punkt wspólny wszystkich kół z tej rodziny. Łatwo widzieć, że jego odległość od każdego z punktów $A_1, A_2, A_3, \dots, A_n$ równa jest co najwyżej o 1. ■

Czytelników zainspirowanych tym zadaniem zachęcamy, by zastanowić się jakie jest najmniejsze możliwe koło potrzebne do przykrycia dowolnych n punktów $A_1, A_2, A_3, \dots, A_n$ położonych na płaszczyźnie w ten sposób, że $|A_i A_j| \leq 1$, gdzie $1 \leq i < j \leq n$.

Istnieją też interesujące zadania dla trójwymiarowej wersji twierdzenia Helly'ego.

Zadanie 8.3. W przestrzeni trójwymiarowej dana jest pewna ilość (co najmniej 4) półprzestrzeni (trójwymiarowy analog półprostej na prostej i półpłaszczyzny na płaszczyźnie). Półpłaszczyzny te wypełniają w sumie całą przestrzeń. Pokazać, że tak naprawdę już pewne cztery z nich wypełniają całą przestrzeń.

Zadanie 8.4. Na płaszczyźnie leży n punktów $\{a_1, a_2, \dots, a_n\}$, gdzie $n \geq 3$. Dla każdych trzech z nich istnieje koło o promieniu 1, który je zawiera. Udowodnij, że wszystkie te punkty zawarte są w pewnym kole o promieniu 1.

ROZWIĄZANIE. Niech c_1, c_2, c_3 będą kołami o promieniach równych 1 i środkach w punktach a_1, a_2, a_3 . Wówczas zgodnie z założeniem istnieje koło c o promieniu 1 i środku a_0 , że $a_1, a_2, a_3 \in c$. Równoważnie: $c_1 \cap c_2 \cap c_3 \neq \emptyset$. Z twierdzenia Helly'ego zastosowanego do rodziny kół $\{c_1, c_2, \dots, c_n\}$ o promieniach 1 i środkach w $\{a_1, a_2, \dots, a_n\}$ mamy: $c_1 \cap c_2 \cap \dots \cap c_n \neq \emptyset$. Niech x należy do przecięcia tej rodziny kół. Zgodnie z definicją $\{a_1, a_2, \dots, a_n\}$ są odległe od x o co najwyżej 1. Istnieje zatem koło o środku w x i promieniu 1, zawierający je wszystkie. ■

Dowód jest oczywiście prawdziwy gdy zamiast kół o promieniach równych 1 rozważymy koła o promieniach równych pewnemu ustalonemu $r > 0$. Pokażmy pewne ciekawe zastosowanie poprzedniego ćwiczenia.

Zadanie 8.5. Niech z_1, z_2, \dots, z_n będą punktami płaszczyzny takimi, że dowolne dwa są odległe od siebie nie więcej niż o 1. Wtedy wszystkie te punkty można pokryć kołem o promieniu $\frac{1}{\sqrt{3}}$.

ROZWIĄZANIE. Wystarczy pokazać, że każde trzy punkty z rozważanego zbioru można przykryć kołem o promieniu $\frac{1}{\sqrt{3}}$. Dla trzech punktów mamy następujące możliwości położenia: punkty te są wierzchołkami trójkąta ostrokątnego/prostokątnego, rozwartokątnego lub punkty te są współliniowe.

W trzech ostatnich przypadkach nie ma żadnego problemu. Wystarczy wziąć środek najdłuższego z trzech odcinków powstałych z połączenia rozważanych punktów i umieścić w tym punkcie okrąg o promieniu $\frac{1}{2}$. Pokryje on z pewnością wszystkie punkty. Pozostaje problem trójkąta ostrokątnego. Załóżmy, że rozważamy punkty A, B, C . Niech O będzie środkiem okręgu opisanego na ABC . Bez straty ogólności możemy założyć, że kąt ABC jest największym z kątów tego trójkąta (a więc jego miara jest nie mniejsza niż 60°). Niech P będzie rzutem O na AC . Wówczas przez α oznaczymy kąt AOP . Mamy:

$$|AP| = \frac{1}{2}|AC| \leq \frac{1}{2}, \quad \alpha = \angle ABC = \angle AOP = \frac{1}{2}\angle AOC \geq 60^\circ.$$

Stąd:

$$|AO| = \frac{|AP|}{\sin \alpha} = \frac{|AC|}{2 \sin \alpha} \leq \frac{1}{2 \sin \alpha} \leq \frac{1}{2 \sin 60^\circ} \leq \frac{1}{\sqrt{3}}.$$

■

Zadanie 8.6. Na płaszczyźnie leży n prostokątów o bokach równoległych do osi OX i OY : P_1, P_2, \dots, P_n o tej własności, że dowolne dwa mają punkt wspólny. Pokaż, że wszystkie prostokąty mają punkt wspólny.

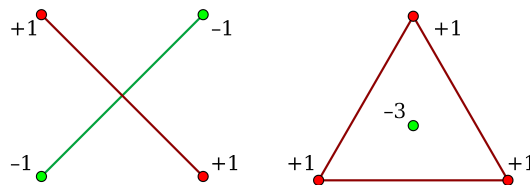
ROZWIĄZANIE. Zrzutujemy te prostokąty na osie układu współrzędnych. Obraz każdego prostokąta po zrzutowaniu na dowolną z osi jest odcinkiem. Niech f, g będą tymi zrzutowaniami. Wówczas dla dowolnych dwóch prostokątów P_1, P_2 rozważanej rodziny mamy: $f(P_1) \cap f(P_2) \neq \emptyset$. Podobnie dla g . Stosując na osi OX twierdzenie Helly'ego do rodziny $f(P_i)$ dostajemy, że istnieje $x \in OX$, że $x \in \bigcap f(P_i)$. Podobnie na osi OY istnieje punkt $y \in OY$, który zawiera się w przecięciu $g(P_i)$. Zatem punkt (x, y) należy do przecięcia wszystkich tych prostokątów. ■

Widzimy zatem, że można układać całkiem nietrywialne zadania związane z twierdzeniem Helly'ego. Zanim udowodnimy to twierdzenie potrzebujemy dwóch faktów z teorii zbiorów wypukłych.

Obserwacja 8.17: Radon

Niech $S = \{x_1, x_2, \dots, x_r\}$ będzie zbiorem punktów przestrzeni \mathbb{R}^n , gdzie $r \geq n+2$. Wówczas można S podzielić na dwa niepuste i rozłączne podzbiory S_1, S_2 o tej własności, że:

$$\text{conv}(S_1) \cap \text{conv}(S_2) \neq \emptyset.$$



Dowód. Rozważmy punkty $y_i = (x_i, 1) \in \mathbb{R}^{n+1}$. Mamy $r \geq n+2$ wektorów w $n+1$ wymiarowej przestrzeni liniowej, więc istnieją $\lambda_1, \dots, \lambda_r$, nie wszystkie równe zero, że

$$\lambda_1 y_1 + \dots + \lambda_r y_r = 0.$$

Niech $S_1 = \{i \mid \lambda_i \geq 0\}$ oraz niech $S_2 = \{i \mid \lambda_i < 0\}$. Skoro ostatnia współrzędna b_i równa jest 1, mamy:

$$\sum_{i \in S_1} \lambda_i = - \sum_{j \in S_2} \lambda_j = \lambda \neq 0.$$

W szczególności punkt

$$\sum_{i \in S_1} \frac{\lambda_i}{\lambda} x_i = \sum_{j \in S_2} \frac{-\lambda_j}{\lambda} x_j$$

należy zarówno do $\text{conv}(S_1)$ jak i do $\text{conv}(S_2)$, co kończy dowód. □

Można udowodnić także odwrotną wersję tego lematu: jeśli S jest dowolnym skończonym podzbiorem \mathbb{R}^n , afinicznie niezależnym, wówczas dla każdego podziału S na dwa niepuste i rozłączne podzbiory S_1, S_2 mamy $\text{conv } S_1 \cap \text{conv } S_2 \neq \emptyset$. Dowodzi się go analogicznie.

Przystąpmy do zasadniczego dowodu tw. Helly'ego. Niech $\mathcal{F} = \{B_1, B_2, \dots, B_r\}$. Dowód to indukcja ze względu na r . Dla $r = n + 1$ teza jest oczywista. Załóżmy teraz, że moc rozważanej rodziny to $r > n + 1$. Zgodnie z założeniem indukcyjnym, istnieją takie punkty x_1, x_2, \dots, x_r , że:

$$x_i \in B_1 \cap B_2 \cap \dots \cap B_{i-1} \cap B_{i+1} \cap \dots \cap B_r.$$

Skoro $r \geq n + 2$ możemy zaaplikować do tego zbioru punktów (nazwijmy go S) lemat Radona i stwierdzić bez straty ogólności, że istnieje $S_1 = \{x_1, x_2, \dots, x_k\}$, że $\text{conv } S_1 \cap \text{conv}(S \setminus S_1) \neq \emptyset$. Niech więc:

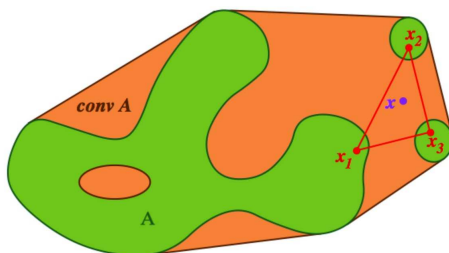
$$x \in \text{conv}(x_1, x_2, \dots, x_k) \cap \text{conv}(x_{k+1}, x_{k+2}, \dots, x_r).$$

Wówczas twierdzimy, że x jest w przecięciu wszystkich B_i (to da tezę). Istotnie, $x \in \text{conv}(x_1, x_2, \dots, x_k)$, a więc na mocy wypukłości zbiorów B_i mamy: $x \in B_{k+1} \cap B_{k+2} \cap \dots \cap B_r$. Podobnie w drugą stronę: $x \in \text{conv}(x_{k+1}, x_{k+2}, \dots, x_r)$, a więc $x \in B_1 \cap B_2 \cap \dots \cap B_{k-1}$. Zatem x leży w przecięciu wszystkich B_i .

Łatwo pokazać, że założenie tw. Helly'ego nie da się w żadnym przypadku istotnie poprawić. Nie można oczywiście opuścić założenia wypukłości (prosty kontrprzykład). Nie jest też możliwe obniżenie założenia, że przecinać się (w \mathbb{R}^n) musi każda podrodzina $n + 1$ zbiorów. Inaczej bowiem boki dowolnego trójkąta stanowią kontrprzykład do tego twierdzenia. Ciekawym rezultatem, ważnym dla teorii zbiorów wypukłych, jest również następujący wynik. Zachęcam Państwa do wykazania go (jest on też w linkowanych plikach).

Twierdzenie 8.5: Caratheodory

Jeśli A jest niepustym podzbiorem przestrzeni afinicznej \mathbb{R}^n oraz $x \in \text{conv}(A)$, wówczas x jest kombinacją wypukłą afinicznie niezależnych punktów w A ,



Twierdzenie Helly'ego było pierwszym rezultatem tzw. **dyskretnej geometrii kombinatorycznej**. Typowe zagadnienia tej dziedziny związane są między innymi z kolorowaniem obiektów geometrycznych, z najlepszymi pokryciami, upakowaniami lub wypełnieniami, z podziałami i rozkładami figur, z ich symetriami. Choć znakomita większość problemów do niej należących da się wysłowić w sposób całkowicie elementarny, ich dowody nie należą zawsze do łatwych. Oto kilka zadań z tego typu geometrii¹³.

Zadanie 8.7. Na płaszczyźnie dane jest pięć punktów. Żadne trzy z nich nie są współliniowe. Wówczas można z nich wybrać cztery będące wierzchołkami czworokąta wypukłego.

Zadanie 8.8. Na płaszczyźnie dane jest sześć punktów. Żadne trzy z nich nie są współliniowe. Wówczas można utworzyć dwa rozłączne trójkąty o wierzchołkach w tych sześciu punktach.

Zadanie 8.9. Na płaszczyźnie dane jest siedem punktów. Wówczas istnieją takie punkty A, B (niekoniecznie spośród danych siedmiu), że jeśli pewien zbiór wypukły X zawiera przynajmniej cztery z wybranych siedmiu punktów, to X zawiera też A lub B .

Zadanie 8.10. Na płaszczyźnie dane jest osiem punktów. Żadne trzy z nich nie są współliniowe. Czy można zawsze utworzyć dwa trójkąty o wierzchołkach wybranych spośród tych punktów tak, by odcinek łączący pozostałe dwa punkty przechodził przez ich wnętrze?

¹³Zachęcam też do zajrzenia do poniższych notatek <https://pi.math.cornell.edu/~eranevo/homepage/ConvNote.pdf>.

Rozdział 9

Przekształcenia afiniczne

W tym rozdziale omawiamy pojęcie przekształcenia afinicznego, czyli z geometrycznego punktu widzenia: takiego przekształcenia pomiędzy przestrzeniami afinicznymi, które zachowuje kombinacje afiniczne. Przekształcenie takie przeprowadza choćby trójki punktów współliniowych na trójki punktów współliniowych. Z algebraicznego punktu widzenia można szukać innej motywacji: mamy w pewnych przestrzeniach liniowych V, W zawarte przestrzenie afiniczne H i M szukamy przekształceń $f : H \rightarrow M$, które zachowują operację wektora łączącego zdefiniowaną na V oraz W . Oznacza to, że z przekształceniem f stowarzyszone jest przekształcenie liniowe $\phi : T(H) \rightarrow T(M)$ takie, że dla każdego $p_1 \in H$ oraz $p_2 \in M$ mamy

$$\phi(\overrightarrow{p_1 p_2}) = \overrightarrow{f(p_1) f(p_2)}.$$

Wykażemy, że są to podejścia równoważne. Zaczniemy od podejścia algebraicznego.

Obserwacja 9.1

Niech H, M będą przestrzeniami afinicznymi nad ciałem K i niech $\phi : T(H) \rightarrow T(M)$ będzie przekształceniem liniowym. Dla dowolnej funkcji $f : H \rightarrow M$ następujące warunki są równoważne:

- (1) istnieją punkty $p_0 \in H, q_0 \in M$ takie, że dla każdego punktu $p \in H$ zachodzi

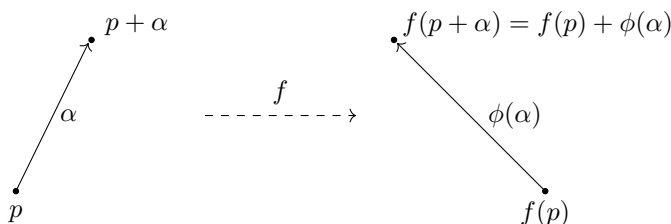
$$f(p) = q_0 + \phi(\overrightarrow{p_0 p}),$$

- (2) dla każdego $p \in H$ i każdego $\alpha \in T(H)$:

$$f(p + \alpha) = f(p) + \phi(\alpha),$$

- (3) dla każdego $p, p' \in H$ mamy:

$$\phi(\overrightarrow{pp'}) = \overrightarrow{f(p)f(p')}.$$



Powyższa obserwacja daje nam dwa warunki charakteryzujące ów związek pomiędzy poszukiwanymi (i jeszcze niezdefiniowanymi) przekształceniami przestrzeni afinicznych, a odpowiadającymi im przekształceniami liniowymi zachowującymi wektory łączące (to dokładnie wyraża warunek (3)).

Punkt (1) podaje wprost „przepis” na znalezienie każdego takiego przekształcenia $f : H \rightarrow M$ mając dane przekształcenie $\phi : T(H) \rightarrow T(M)$. Warunek ten mówi, że po ustaleniu na co ma przechodzić jeden wybrany punkt z przestrzeni H możemy, wykorzystując ϕ , określić jednoznacznie przekształcenie f .

Dowód. Dowiedzimy (1) \Rightarrow (2). Z (1) wynika, że $f(p_0) = q_0$. Co więcej, dla każdego $p \in H$ oraz $\alpha \in T(H)$ mamy

$$p + \alpha = p_0 + \overrightarrow{p_0 p} + \alpha.$$

Stąd ponownie na mocy (1) oraz z liniowości ϕ :

$$f(p + \alpha) = f(p_0 + \overrightarrow{p_0 p} + \alpha) \stackrel{(1)}{=} q_0 + \overrightarrow{\phi(p_0)(p_0 + \overrightarrow{p_0 p} + \alpha)} = q_0 + \overrightarrow{\phi(p_0 p) + \alpha} = q_0 + \overrightarrow{\phi(p_0 p)} + \phi(\alpha) = f(p) + \phi(\alpha).$$

Dowodzimy (2) \Rightarrow (3). Weźmy dowolne punkty $p, p' \in H$ i niech $\alpha = \overrightarrow{pp'}$. Wówczas $p' = p + \alpha$, więc:

$$f(p') = f(p + \alpha) \stackrel{(2)}{=} f(p) + \phi(\alpha) = f(p) + \overrightarrow{\phi(p p')}.$$

$$\text{Stąd } \overrightarrow{\phi(p p')} = f(p') - f(p) = \overrightarrow{f(p) f(p')}.$$

Dowodzimy (3) \Rightarrow (1). Weźmy dowolny punkt $p_0 \in H$ i przyjmijmy $q_0 = f(p_0)$. Wówczas dla każdego $p \in H$ mamy

$$\overrightarrow{\phi(p_0 p)} \stackrel{(3)}{=} \overrightarrow{f(p_0) f(p)} = \overrightarrow{q_0 f(p)},$$

więc

$$f(p) - q_0 = \overrightarrow{\phi(p_0 p)} \Rightarrow f(p) = q_0 + \overrightarrow{\phi(p_0 p)}.$$

□

Drugie, bardzo naturalne z geometrycznego punktu widzenia podejście każe szukać przekształceń, które zachowują kombinacje afiniczne punktów (czyli także ich współrzędne barycentryczne w układzie bazowym). Poniższe twierdzenie mówi, że przekształcenia te uzyskiwane są jedynie w sposób opisany wyżej.

Twierdzenie 9.1

Niech H, M będą przestrzeniami afinicznymi nad ciałem K . Wówczas dla funkcji $f : H \rightarrow M$ następujące warunki są równoważne:

(1) dla każdych punktów $p_0, \dots, p_k \in H$ oraz układu wag $a_0, \dots, a_k \in K$ mamy

$$f(a_0 p_0 + \dots + a_k p_k) = a_0 f(p_0) + \dots + a_k f(p_k),$$

(2) istnieje przekształcenie liniowe $\phi : T(H) \rightarrow T(M)$ oraz punkty $p_0 \in H$ i $q_0 \in M$ takie, że dla każdego $p \in H$ mamy

$$f(p) = q_0 + \overrightarrow{\phi(p_0 p)}.$$

Dowód. Wykażemy (1) \Rightarrow (2). Wybierzmy $p_0 \in H$ i określmy przekształcenie $\phi : T(H) \rightarrow T(M)$ wzorem

$$\phi(\alpha) = \overrightarrow{f(p_0) f(p_0 + \alpha)} = f(p_0 + \alpha) - f(p_0).$$

Wykażemy, że ϕ jest liniowe. Niech $\alpha, \beta \in T(H)$. Wówczas $p_0 + \alpha + \beta$ jest kombinacją afiniczną punktów $p_0, p_0 + \alpha, p_0 + \beta$ z wagami $-1, 1, 1$ postaci:

$$p_0 + \alpha + \beta = -p_0 + (p_0 + \alpha) + (p_0 + \beta).$$

Z warunku (1) dostajemy więc, że:

$$f(p_0 + \alpha + \beta) = -f(p_0) + f(p_0 + \alpha) + f(p_0 + \beta).$$

A zatem z definicji ϕ mamy:

$$\begin{aligned} \phi(\alpha + \beta) &= \overrightarrow{f(p_0) f(p_0 + \alpha + \beta)} = \\ &= f(p_0 + \alpha + \beta) - f(p_0) = \\ &= -f(p_0) + f(p_0 + \alpha) + f(p_0 + \beta) - f(p_0) = \\ &= f(p_0 + \alpha) - f(p_0) + f(p_0 + \beta) - f(p_0) = \\ &= \overrightarrow{f(p_0) f(p_0 + \alpha)} + \overrightarrow{f(p_0) f(p_0 + \beta)} = \\ &= \phi(\alpha) + \phi(\beta). \end{aligned}$$

Pozostaje pokazać, że $\phi(a\alpha) = a\phi(\alpha)$, dla każdego $\alpha \in T(H)$ oraz dla każdego $a \in K$. Jednak również wektor $p_0 + a\alpha$ możemy przedstawić jako kombinację afiniczną postaci

$$p_0 + a\alpha = a(p_0 + \alpha) + (1 - a)p_0,$$

otrzymując stąd równość:

$$f(p_0 + a\alpha) = af(p_0 + \alpha) + (1 - a)f(p_0).$$

W rezultacie opierając się ponownie na definicji ϕ mamy:

$$\begin{aligned} \phi(a\alpha) &= \overrightarrow{f(p_0)f(p_0 + a\alpha)} = \\ &= f(p_0 + a\alpha) - f(p_0) = \\ &= af(p_0 + \alpha) + (1 - a)f(p_0) - f(p_0) = \\ &= a(f(p_0 + \alpha) - f(p_0)) = \\ &= a\phi(\alpha). \end{aligned}$$

Pokazaliśmy zatem, że zdefiniowane przez nas ϕ jest przekształceniem liniowym. Trzeba jeszcze sprawdzić, że spełnia ono wymagania postawione w (2). Z definicji ϕ mamy jednak: $f(p_0 + \alpha) = f(p_0) + \phi(\alpha)$, dla każdego $\alpha \in T(H)$. Przyjmując więc $q_0 = f(p_0)$ dostajemy:

$$f(p) = f(p_0 + \overrightarrow{p_0p}) = f(p_0) + \phi(\overrightarrow{p_0p}) = q_0 + \phi(\overrightarrow{p_0p}).$$

Dowodzimy (2) \Rightarrow (1). Przypuśćmy więc, że istnieje przekształcenie liniowe $\phi : T(H) \rightarrow T(M)$ oraz punkty $s_0 \in H, t_0 \in M$ takie, że dla każdego $p \in H$ zachodzi $f(p) = t_0 + \phi(\overrightarrow{s_0p})$ (w szczególności $f(s_0) = t_0$). Wówczas dla każdego punktu $p_0, \dots, p_k \in H$ i wag $a_0, \dots, a_k \in K$ mamy:

$$a_0p_0 + \dots + a_kp_k = s_0 - (a_0 + \dots + a_k)s_0 + a_0p_0 + \dots + a_kp_k = s_0 + a_0\overrightarrow{s_0p_0} + \dots + a_k\overrightarrow{s_0p_k},$$

$$\begin{aligned} \text{Zatem} \quad f(a_0p_0 + \dots + a_kp_k) &= f(s_0 + a_0\overrightarrow{s_0p_0} + \dots + a_k\overrightarrow{s_0p_k}) = \\ &\stackrel{\text{Obs. 9.1 (2)}}{=} t_0 + \phi(a_0\overrightarrow{s_0p_0} + \dots + a_k\overrightarrow{s_0p_k}) = \\ &= t_0 + a_0\phi(\overrightarrow{s_0p_0}) + \dots + a_k\phi(\overrightarrow{s_0p_k}) = \\ &\stackrel{\text{Obs. 9.1 (3)}}{=} t_0 + a_0\overrightarrow{f(s_0)f(p_0)} + \dots + a_k\overrightarrow{f(s_0)f(p_k)} = \\ &= t_0 + a_0\overrightarrow{t_0f(p_0)} + \dots + a_k\overrightarrow{t_0f(p_k)} = \\ &= a_0(t_0 + \overrightarrow{t_0f(p_0)}) + \dots + a_k(t_0 + \overrightarrow{t_0f(p_k)}) = \\ &= a_0f(p_0) + \dots + a_kf(p_k). \end{aligned}$$

□

Powyższe twierdzenie motywuje sformułowanie definicji przekształcenia afinicznego.

Definicja 9.1: Przekształcenie afiniczne

Niech H, M będą przestrzeniami afinicznymi nad ciałem K . Mówimy, że funkcja $f : H \rightarrow M$ jest PRZEKSZTAŁCENIEM AFINICZNYM, jeśli f spełnia jeden z równoważnych warunków:

- (1) dla każdego punktu $p_0, \dots, p_k \in H$ oraz układu wag $a_0, \dots, a_k \in K$ zachodzi równość $f(a_0p_0 + \dots + a_kp_k) = a_0f(p_0) + \dots + a_kf(p_k)$,
- (2) istnieje przekształcenie liniowe $\phi : T(H) \rightarrow T(M)$ oraz punkty $p_0 \in H$ i $q_0 \in M$ takie, że dla każdego $p \in H$ mamy $f(p) = q_0 + \phi(\overrightarrow{p_0p})$.

Przekształcenie liniowe $\phi : T(H) \rightarrow T(M)$ z warunku (2) nazywamy POCHODNĄ (albo PRZEKSZTAŁCENIEM WEKTORÓW SWOBODNYCH) przekształcenia afinicznego f i oznaczamy f' .

Z pierwszego udowodnionego dziś twierdzenia wynika, że ϕ jest przekształceniem wyznaczonym jednoznacznie przez f , niezależnie od wyboru p_0 i $q_0 = f(p_0)$. Rozważmy kilka przykładów.

- Rozważmy przyporządkowanie $f : \mathbb{R}^2 \rightarrow \mathbb{R}^3$ zadane wzorem $f((x_1, x_2)) = (x_1 + 2, x_2 + 1, x_2)$. Jest to przekształcenie afiniczne, gdyż mamy przekształcenie liniowe $\phi : \mathbb{R}^2 \rightarrow \mathbb{R}^3$ dane wzorem $\phi((x_1, x_2)) = (x_1, x_2, x_2)$ oraz punkty $p_0 = (0, 0), q_0 = (2, 1, 0)$ takie, że

$$f((x_1, x_2)) = (2, 1, 0) + \phi(x_1 - 0, x_2 - 0) = (2, 1, 0) + \phi((x_1, x_2)).$$

- Niech

$$H = \{(x_1, x_2, x_3) \in K^3 \mid x_1 + x_2 + x_3 = 1\}, \quad M = \{(x_1, x_2) \in K^2 \mid x_1 - x_2 = 2\}.$$

Funkcja $f : H \rightarrow M$ dana wzorem $f((x_1, x_2, x_3)) = (x_1, -x_2 - x_3 - 1)$ jest przekształceniem afinicznym. Mamy

$$T(H) = \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1 + x_2 + x_3 = 0\}, \quad T(M) = \{(x_1, x_2) \in \mathbb{R}^2 \mid x_1 - x_2 = 0\}.$$

Zauważmy, że $\phi(T(H)) = T(M)$, gdzie $\phi : \mathbb{R}^3 \rightarrow \mathbb{R}^2$ dane jest wzorem

$$\phi((x_1, x_2, x_3)) = (x_1, -x_2 - x_3).$$

A zatem możemy określić $f' = \phi|_{T(H)} : T(H) \rightarrow T(M)$ oraz przyjąć $p_0 = (0, -1, 2), q_0 = (0, -2)$.

- Niech V, Z będą przestrzeniami liniowymi nad K . Każde przekształcenie liniowe $\phi : V \rightarrow Z$ jest przekształceniem afinicznym, przy czym $\phi' = \phi$. Każde przekształcenie afiniczne $f : V \rightarrow Z$ jest postaci $f(\alpha) = f(0 + \alpha) = f(0) + f'(\alpha)$.
- Każda parametryzacja $K^n \rightarrow H$ przestrzeni afinicznej H jest przekształceniem afinicznym.

Wniosek 9.1

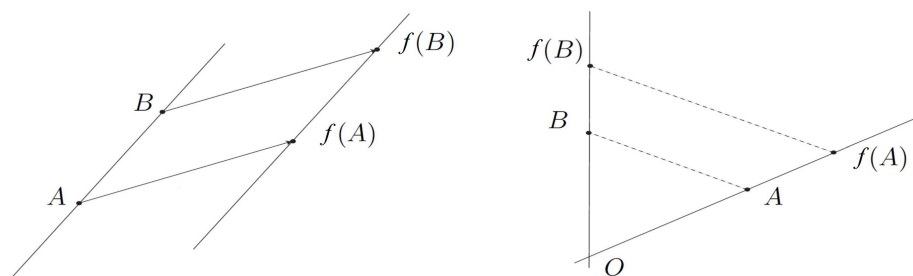
Każde przekształcenie afiniczne $f : K^n \rightarrow K^m$ jest zadane wzorem:

$$f((x_1, \dots, x_n)) = (a_{11}x_1 + \dots + a_{1n}x_n + b_1, \dots, a_{m1}x_1 + \dots + a_{mn}x_n + b_m),$$

gdzie $(b_1, \dots, b_m) = f((0, \dots, 0))$ oraz f' to przekształcenie liniowe o macierzy $M(f')_{st} = A = [a_{ij}]$.

Omówmy kilka ważnych klas przekształceń afinicznych.

- Dla dowolnych przestrzeni afinicznych H, M nad K i każdego $q \in M$ PRZEKSZTAŁCENIE STAŁE $f : H \rightarrow M$, o wartości $f(p) = q$, dla każdego $p \in H$, jest afiniczne. Przy tym $f' = 0$.
- Niech H będzie przestrzenią afiniczną nad K i niech $\alpha \in T(H)$. Przekształcenie $f : H \rightarrow H$ spełniające $f(p) = p + \alpha$, dla każdego $p \in H$ jest afiniczne. Nazywamy je PRZESUNIĘCIEM (TRANSLACJĄ) O WEKTOR α i oznaczamy τ_α . Zatem $(\tau_\alpha)' = \text{id}$.
- Niech H będzie przestrzenią afiniczną nad K , $p_0 \in H$ i $a \in K$. Przekształcenie afiniczne $f : H \rightarrow H$ takie, że $f(p_0) = p_0$ oraz $f' = a \cdot \text{id}$ nazywamy JEDNOKŁADNOŚCIĄ O ŚRODKU p_0 I SKALI a .



Ilustracja przesunięcia (po lewej) i homotetii o środku O (po prawej).

- Niech H będzie przestrzenią afiniczną nad K oraz $T(H) = W_1 \oplus W_2$. Dla $p_1, p_2 \in H$ określamy podprzestrzenie afiniczne $H_1 = p_1 + W_1, H_2 = p_2 + W_2$. Przekształcenie afiniczne $f : H \rightarrow H$ takie, że f' jest RZUTEM na W_1 wzdłuż W_2 oraz $f(p_1) = p_1$ nazywamy RZUTEM na H_1 wzdłuż H_2 . Przekształcenie afiniczne $g : H \rightarrow H$ takie, że $g(p_1) = p_1$ oraz g' jest SYMETRIĄ względem W_1 wzdłuż W_2 nazywamy SYMETRIĄ względem H_1 wzdłuż H_2 .

Obserwacja 9.2: Jednoznaczność przekształcenia afinicznego na bazie punktowej

Niech H, M będą przestrzeniami afinicznymi nad ciałem K .

- Jeśli p_0, \dots, p_n jest bazą punktową przestrzeni H oraz q_0, \dots, q_n jest dowolnym układem punktów przestrzeni M , to istnieje dokładnie jedno przekształcenie afiniczne $f : H \rightarrow M$ takie, że $f(p_i) = q_i$, dla $i = 0, \dots, n$. Jest ono zadane przez:

$$f(a_0 p_0 + \dots + a_n p_n) = a_0 q_0 + \dots + a_n q_n, \quad \text{dla dowolnych wag } a_0, \dots, a_n \in K.$$

- Jeśli $p_0; \alpha_1, \dots, \alpha_n$ jest układem bazowym przestrzeni H oraz $q_0 \in M$, a β_1, \dots, β_n jest dowolnym układem wektorów w $T(M)$, to istnieje dokładnie jedno przekształcenie afiniczne $f : H \rightarrow M$ takie, że $f(p_0) = q_0$ oraz $f'(\alpha_i) = \beta_i$, dla $i = 1, \dots, n$. Jest ono zadane wzorem

$$f(p_0 + a_1 \alpha_1 + \dots + a_n \alpha_n) = q_0 + a_1 \beta_1 + \dots + a_n \beta_n, \quad \text{dla dowolnych skalarów } a_1, \dots, a_n \in K.$$

W geometrii elementarnej powyższa obserwacja daje ważne wnioski:

- dla każdej trójki punktów niewspółliniowych na płaszczyźnie H istnieje izomorfizm afiniczny, który przeprowadza te punkty na wierzchołki trójkąta równobocznego,
- dla każdej czwórki punktów będących wierzchołkami równoległoboku na płaszczyźnie H istnieje izomorfizm afiniczny, który przeprowadza te punkty na wierzchołki kwadratu,
- dla każdej czwórki punktów niewspółpłaszczyznowych w przestrzeni trójwymiarowej H istnieje izomorfizm afiniczny, który przeprowadza te punkty na wierzchołki czworościanu foremnego.

Prosty przykład zastosowania. Jeśli chcemy udowodnić, że w dowolnym trójkącie środkowe przecinają się w jednym punkcie i dzielą w stosunku 2 : 1, licząc od wierzchołka, to wystarczy wiedzieć, że trójkąt równoboczny ma żądane własności. Dowolny inny trójkąt jest jego obrazem przy pewnym przekształceniu afinicznym, które zachowuje środki boków, a więc także środkowe, ich współpękowość oraz stosunek podziału. Podobnie argumentować można np. dowód twierdzenia Cevy czy Menelaosa.

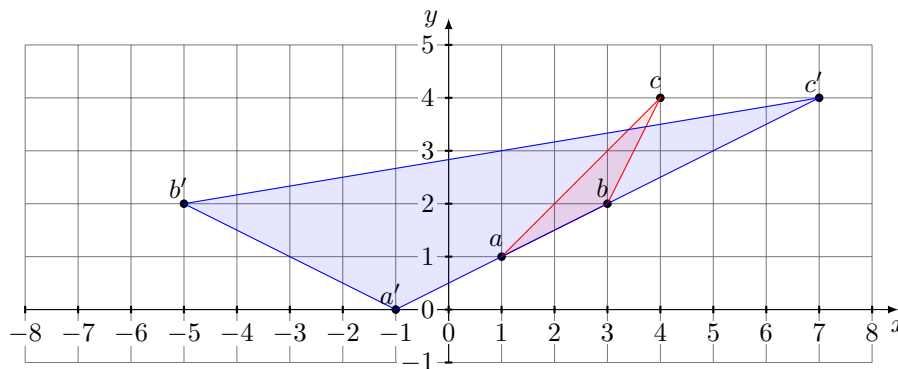
Przykład. Znajdź (jedyne) przekształcenie afiniczne $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$, które przeprowadza punkty $a = (1, 1), b = (3, 2), c = (4, 4)$ odpowiednio na punkty $a' = (-1, 0), b' = (-5, 2)$ oraz $c' = (7, 4)$.

Rozważmy układy bazowe $a; \vec{ab}, \vec{ac}$, czyli $(1, 1); (2, 1), (3, 3)$ oraz $a'; \vec{a'b'}, \vec{a'c'}$, czyli $(-1, 0); (-4, 2), (8, 4)$. Stąd f' jest przeprowadzając $(2, 1)$ w $(-4, 2)$ oraz $(3, 3)$ w $(8, 4)$. Zatem (jak w pierwszym semestrze):

$$f'((x_1, x_2)) = \left(-\frac{20}{3}x_1 + \frac{28}{3}x_2, \frac{2}{3}x_1 + \frac{2}{3}x_2 \right).$$

Biorąc dowolne $p = (x_1, x_2)$ oraz $p_0 = (1, 1), q_0 = f(p_0) = (-1, 0)$ mamy:

$$\begin{aligned} f((x_1, x_2)) &= q_0 + f(\overrightarrow{p_0 p}) = (-1, 0) + f'(\overrightarrow{(1, 1), (x_1, x_2)}) = (-1, 0) + f'((x_1 - 1, x_2 - 1)) \\ &= (-1, 0) + \left(-\frac{20}{3}(x_1 - 1) + \frac{28}{3}(x_2 - 1), \frac{2}{3}(x_1 - 1) + \frac{2}{3}(x_2 - 1) \right) = \left(-\frac{20}{3}x_1 + \frac{28}{3}x_2 - \frac{11}{3}, \frac{2}{3}x_1 + \frac{2}{3}x_2 - \frac{4}{3} \right). \end{aligned}$$



Opisane przekształcenie przeprowadza trójkąt abc na trójkąt $a'b'c'$. Dokładniej, punkt o współrzędnych barycentrycznych (x, y, z) w bazie punktowej a, b, c przechodzi na punkt o współrzędnych barycentrycznych (x, y, z) w bazie punktowej a', b', c' .

Definicja 9.2: Izomorfizm afiniczny

Niech H, M będą przestrzeniami afinicznymi nad ciałem K . Mówimy, że przekształcenie afiniczne $f : H \rightarrow M$ jest **IZOMORFIZMEM**, jeśli f jest różnowartościowe i „na”. Mówimy, że przestrzenie H, M są **IZOMORFICZNE**, jeśli istnieje izomorfizm $f : H \rightarrow M$.

Poniższa charakteryzacja izomorfizmów przestrzeni afinicznych jest bezpośrednią konsekwencją odpowiedniej charakteryzacji izomorfizmów przestrzeni liniowych i związku między nimi.

Obserwacja 9.3

Niech H, M będą przestrzeniami afinicznymi nad K i niech $f : H \rightarrow M$ będzie przekształceniem afinicznym. Następujące warunki są równoważne:

- f jest izomorfizmem,
- f przeprowadza pewną (każdą) bazę punktową H na bazę punktową M ,
- istnieje przekształcenie afiniczne $g : M \rightarrow H$ takie, że $g \circ f = \text{id}_H$ oraz $f \circ g = \text{id}_M$,
- $f' : T(H) \rightarrow T(M)$ jest izomorfizmem przestrzeni liniowych.

Przesunięcia równoległe, jednokładności o skalach różnych od 0, symetrie – są przykładami izomorfizmów afinicznych. Skończenie wymiarowe przestrzenie liniowe nad K są izomorficzne wtedy i tylko wtedy, gdy mają ten sam wymiar. Stąd wynika wniosek.

Wniosek 9.2

Niech H, M będą skończenie wymiarowymi przestrzeniami afinicznymi nad K . Przestrzenie H, M są izomorficzne wtedy i tylko wtedy, gdy $\dim T(H) = \dim T(M)$. W szczególności każda n -wymiarowa przestrzeń afiniczna nad K jest izomorficzna z przestrzenią afiniczną K^n .

Przyjrzymy się związkom pomiędzy przekształceniami afinicznymi i macierzami ich pochodnych.

Obserwacja 9.4

Niech H, M będą przestrzeniami afinicznymi nad K , niech $p_0; \mathcal{A}$ będzie układem bazowym przestrzeni H oraz niech $q_0; \mathcal{B}$ będzie układem bazowym przestrzeni M , przy czym $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$, $\mathcal{B} = (\beta_1, \dots, \beta_m)$. Niech $f : H \rightarrow M$ będzie przekształceniem afinicznym, przy czym:

- $f(p_0) = q_0 + w_1\beta_1 + \dots + w_m\beta_m$, dla pewnych w_1, \dots, w_m ,
- $M(f')_{\mathcal{A}}^{\mathcal{B}} = A$.

Wówczas dla każdego $p \in H$: jeśli p ma w układzie bazowym $p_0; \mathcal{A}$ współrzędne a_1, \dots, a_n oraz $f(p)$ ma w układzie bazowym $q_0; \mathcal{B}$ współrzędne b_1, \dots, b_m , to:

$$\begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix} = A \cdot \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} + \begin{bmatrix} w_1 \\ \vdots \\ w_m \end{bmatrix}. \quad (*)$$

W szczególności jeśli $H = M$ oraz $f = \text{id}$, dostajemy następujący związek między współrzędnymi $a_1, \dots, a_n, b_1, \dots, b_n$ punktu $p \in H$ odpowiednio w układach bazowych $p_0; \mathcal{A}, q_0; \mathcal{B}$:

$$\begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = C \cdot \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} + \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix}, \quad \text{gdzie} \quad C = M(\text{id})_{\mathcal{A}}^{\mathcal{B}} \text{ oraz } p_0 = q_0 + w_1\beta_1 + \dots + w_n\beta_n.$$

Dowód. Skoro $A = M(f')_{\mathcal{A}}^{\mathcal{B}}$, to dla d_1, \dots, d_m spełniających

$$\begin{bmatrix} d_1 \\ \vdots \\ d_m \end{bmatrix} = A \cdot \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$$

mamy $f'(a_1\alpha_1 + \dots + a_n\alpha_n) = d_1\beta_1 + \dots + d_m\beta_m$. Skoro $p = p_0 + a_1\alpha_1 + \dots + a_n\alpha_n$, to:

$$\begin{aligned} f(p) &= f(p_0) + f'(a_1\alpha_1 + \dots + a_n\alpha_n) = \\ &= q_0 + w_1\beta_1 + \dots + w_m\beta_m + d_1\beta_1 + \dots + d_m\beta_m = \\ &= q_0 + (w_1 + d_1)\beta_1 + \dots + (w_m + d_m)\beta_m \end{aligned}$$

Wobec równości $f(p) = q_0 + b_1\beta_1 + \dots + b_m\beta_m$ mamy $\begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix} = \begin{bmatrix} d_1 \\ \vdots \\ d_m \end{bmatrix} + \begin{bmatrix} w_1 \\ \vdots \\ w_m \end{bmatrix} = A \cdot \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} + \begin{bmatrix} w_1 \\ \vdots \\ w_m \end{bmatrix}$. \square

Uwaga. Stosuje się niekiedy następującą wygodną notację blokową zapisującą skróto formułę (*):

$$\begin{bmatrix} b_1 \\ \vdots \\ b_m \\ 1 \end{bmatrix} = \left[\begin{array}{ccc|c} a_{11} & \dots & a_{1n} & w_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m1} & \dots & a_{mn} & w_m \\ \hline 0 & \dots & 0 & 1 \end{array} \right] \cdot \begin{bmatrix} a_1 \\ \vdots \\ a_n \\ 1 \end{bmatrix}.$$

Wprowadzimy element nieobowiązkowy: macierz przekształcenia afinicznego w układach bazowych¹.

Definicja 9.3

Niech H, M będą przestrzeniami afinicznymi nad K , niech $p_0; \mathcal{A}$ będzie układem bazowym przestrzeni H oraz niech $q_0; \mathcal{B}$ będzie układem bazowym przestrzeni M , przy czym $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$, $\mathcal{B} = (\beta_1, \dots, \beta_m)$. MACIERZĄ PRZEKSZTAŁCENIA AFINICZNEGO $f : H \rightarrow M$ W UKŁADACH BAZOWYCH $p_0; \mathcal{A}$, $q_0; \mathcal{B}$ nazywamy macierz blokową

$$M(f)_{p_0; \mathcal{A}}^{q_0; \mathcal{B}} = \left[\begin{array}{c|c} A & w \\ \hline 0 & 1 \end{array} \right],$$

gdzie $A = M(f')_{\mathcal{A}}^{\mathcal{B}}$ spełnia (*) oraz w jest wektorem współrzędnych $f(p_0)$ w układzie bazowym $q_0; \mathcal{B}$

Wróćmy do rozważanego już wcześniej przekształcenia afinicznego przeprowadzającego trójkąty o wierzchołkach $a = (1, 1), b = (3, 2), c = (4, 4)$ trójkąta abc odpowiednio na wierzchołki trójkąta $a'b'c'$ postaci $a' = (-1, 0), b' = (-5, 2), c' = (7, 4)$ Popatrzymy na f w dwóch sytuacjach.

- W układach bazowych: $\mathcal{X} = \{a; \vec{ab}, \vec{ac}\}$ oraz $\mathcal{Y} = \{a'; \vec{a'b'}, \vec{a'c'}\}$ mamy $f(a) = a' + 0 \cdot \vec{a'b'} + 0 \cdot \vec{a'c'}$, czyli współrzędne $f(a)$ w układzie bazowym \mathcal{Y} wynoszą $w_1 = 0, w_2 = 0$. A zatem

$$M(f)_{\mathcal{X}}^{\mathcal{Y}} = \left[\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \hline 0 & 0 & 1 \end{array} \right].$$

- W standardowych układach bazowych $st = \{(0, 0), (1, 0), (0, 1)\}$ mamy $f(a) = a' = (-1, 0)$. Mamy też $f'((1, 0)) = (-\frac{20}{3}, \frac{2}{3})$ oraz $f'((0, 1)) = (\frac{28}{3}, \frac{2}{3})$. A zatem

$$M(f)_{st}^{st} = \left[\begin{array}{cc|c} -\frac{20}{3} & \frac{28}{3} & -1 \\ \frac{2}{3} & \frac{2}{3} & 0 \\ \hline 0 & 0 & 1 \end{array} \right].$$

¹Pojęcie to nie jest standardowym elementem kursu, ale pojawia się u wielu autorów i prowadzi do nieco łatwiejszych rachunków, gdy składamy przekształcenia afiniczne. Wtedy bowiem dla przekształceń afinicznych $f : H_1 \rightarrow H_2$ oraz $g : H_2 \rightarrow H_3$ oraz układów bazowych $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ odpowiednio w H_1, H_2, H_3 mamy

$$M(f \circ g)_{\mathcal{X}}^{\mathcal{Z}} = M(g)_{\mathcal{Y}}^{\mathcal{Z}} \cdot M(f)_{\mathcal{X}}^{\mathcal{Y}}.$$

Warto również wspomnieć, że zbiór przekształceń afinicznych $A(H, M)$ z H do M jest izomorficzny z przestrzenią $M_{\dim H + 1 \times \dim M}(K)$ wymiaru $(\dim H + 1) \dim M$.

Przykład. W przestrzeni afinicznej \mathbb{R}^3 rozważamy podprzestrzenie afiniczne

$$L = \text{af}((1, 1, 1), (3, 5, 4)), \quad H : x_1 + 2x_2 - 2x_3 = 4.$$

Niech $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ będzie rzutem na H wzdłuż L oraz niech $g : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ będzie jednokładnością o środku $(5, 5, 5)$ i skali 3. Wyznaczyć wzór przekształcenia f .

Rozwiązanie 1. Mamy $T(L) = \text{lin}(2, 4, 3)$, zaś $T(H)$ jest opisana równaniem $x_1 + 2x_2 - 2x_3 = 0$, czyli np. $T(H) = \text{lin}((0, 1, 1), (2, 0, 1))$. Mamy zatem bazę \mathcal{A} przestrzeni \mathbb{R}^3 , której pierwszy element rozpinia $T(L)$, a kolejne dwa rozpinają $T(H)$: $\mathcal{A} = ((2, 4, 3), (0, 1, 1), (2, 0, 1))$. Pochodna f' jest rzutem \mathbb{R}^3 na $T(H)$ wzdłuż $T(L)$, czyli

$$M(f')_{\mathcal{A}}^{\mathcal{A}} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Wyznaczamy $M(f')_{st}^{st}$ ze wzoru $M(f')_{st}^{st} = M(\text{id})_{\mathcal{A}}^{st} \cdot M(f')_{\mathcal{A}}^{\mathcal{A}} \cdot M(\text{id})_{st}^{\mathcal{A}}$. Mamy:

$$M(\text{id})_{\mathcal{A}}^{st} = \begin{bmatrix} 2 & 0 & 2 \\ 4 & 1 & 0 \\ 3 & 1 & 1 \end{bmatrix} \quad \text{oraz} \quad M(\text{id})_{st}^{\mathcal{A}} = (M(\text{id})_{\mathcal{A}}^{st})^{-1} = \begin{bmatrix} \frac{1}{4} & \frac{1}{2} & -\frac{1}{2} \\ -1 & -1 & 2 \\ \frac{1}{4} & -\frac{1}{2} & \frac{1}{2} \end{bmatrix}.$$

Zatem:

$$M(f')_{st}^{st} = \begin{bmatrix} 2 & 0 & 2 \\ 4 & 1 & 0 \\ 3 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} \frac{1}{4} & \frac{1}{2} & -\frac{1}{2} \\ -1 & -1 & 2 \\ \frac{1}{4} & -\frac{1}{2} & \frac{1}{2} \end{bmatrix} = \begin{bmatrix} 0 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} \frac{1}{4} & \frac{1}{2} & -\frac{1}{2} \\ -1 & -1 & 2 \\ \frac{1}{4} & -\frac{1}{2} & \frac{1}{2} \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & -1 & 1 \\ -1 & -1 & 2 \\ -\frac{3}{4} & -\frac{3}{2} & \frac{5}{2} \end{bmatrix}$$

Oczywiście f przeprowadza każdy punkt z H na siebie, a więc mamy na przykład $f((4, 0, 0)) = (4, 0, 0)$. Mamy więc, dla dowolnego punktu $(x_1, x_2, x_3) \in \mathbb{R}^3$:

$$\begin{aligned} f(x_1, x_2, x_3) &= (4, 0, 0) + f'((x_1, x_2, x_3) - (4, 0, 0)) = (4, 0, 0) + f'(x_1 - 4, x_2, x_3) = \\ &= (4, 0, 0) + \left(\frac{1}{2}(x_1 - 4) - x_2 + x_3, -(x_1 - 4) - x_2 + 2x_3, -\frac{3}{4}(x_1 - 4) - \frac{3}{2}x_2 + \frac{5}{2}x_3 \right) = \\ &= \left(\frac{1}{2}x_1 - x_2 + x_3 + 2, -x_1 - x_2 + 2x_3 + 4, -\frac{3}{4}x_1 - \frac{3}{2}x_2 + \frac{5}{2}x_3 + 3 \right) \end{aligned}$$

Rozwiązanie 2 (mniej rachunkowe). Obrazem punktu (x_1, x_2, x_3) przy rzucie f jest taki punkt

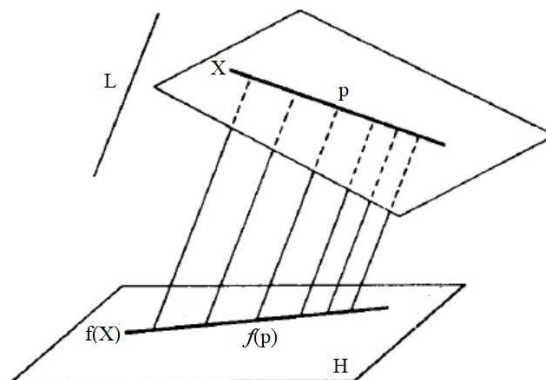
$$f((x_1, x_2, x_3)) = (x_1, x_2, x_3) + t(2, 4, 3),$$

który należy do H . A zatem wyznaczamy t za pomocą x_1, x_2, x_3 rozwiązując równanie

$$(x_1 + 2t) + 2(x_2 + 4t) - 2(x_3 + 3t) = 4,$$

czyli równoważnie $4t = 4 - x_1 - 2x_2 + 2x_3$. Zatem $f((x_1, x_2, x_3)) = (x_1, x_2, x_3) + (1 - \frac{x_1}{4} - \frac{x_2}{2} + \frac{x_3}{2})(2, 4, 3)$.

Morał jest taki: pomocne jest rozumienie geometrii przekształcenia. Wyjaśnienie drugiego sposobu jest widoczne gdy patrzymy na geometrię rzutu, nazywanego czasem w geometrii rzutem równoległym. Rzut w kierunku pewnej prostej L w przestrzeni \mathbb{R}^3 na płaszczyznę H polega na tym, że wybierając punkt $(x_1, x_2, x_3) \in \mathbb{R}^3$ poruszamy się po prostej równoległej do L przechodzącej przez ten punkt. Zapisanie tej prostej w postaci parametrycznej ułatwia sprawdzanie które z jej punktów trafiają na H .



Przykład. Niech $s : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ będzie symetrią względem płaszczyzny $H : x_1 + x_2 - x_3 = 2$ wzdłuż prostej $L = (0, 1, 0) + \text{lin}((2, 1, 2))$. Znajdziemy $s((1, 0, 1))$ oraz wyznaczmy wzór przekształcenia s .

Niech $p = (1, 0, 1)$. Dla $r \in \mathbb{R}^3$ mamy $s(p) = s(r + \vec{rp}) = s(r) + s'(\vec{rp})$. Płaszczyzna H opisana jest układem bazowym

$$\underbrace{(1, 1, 0)}_{\in H}; \underbrace{(1, 0, 1), (0, 1, 1)}_{\in T(H)}.$$

Zatem obraz punktu $r = (1, 1, 0) \in H$ w tej symetrii to $s(r) = (1, 1, 0)$. Rozważmy wektor \vec{rp} równy $(0, -1, 1)$. Znajdźmy współrzędne tego wektora w bazie $(1, 0, 1), (0, 1, 1), (2, 1, 2)$ przestrzeni \mathbb{R}^3 (pierwsze dwa wektory rozpinają $T(H)$, a ostatni $T(L)$). Mamy:

$$(0, -1, 1) = 4(1, 0, 1) + 1(0, 1, 1) - 2(2, 1, 2).$$

A zatem z definicji symetrii liniowej s' :

$$\begin{aligned} s'((0, 1, -1)) &= 4s'((1, 0, 1)) + 1s'((0, 1, 1)) - 2s'((2, 1, 2)) = \\ &= 4(1, 0, 1) + 1(0, 1, 1) + 2(2, 1, 2) = (8, 3, 9). \end{aligned}$$

Zatem

$$s(p) = s(r) + s'(\vec{rp}) = (1, 1, 0) + (8, 3, 9) = (9, 4, 9).$$

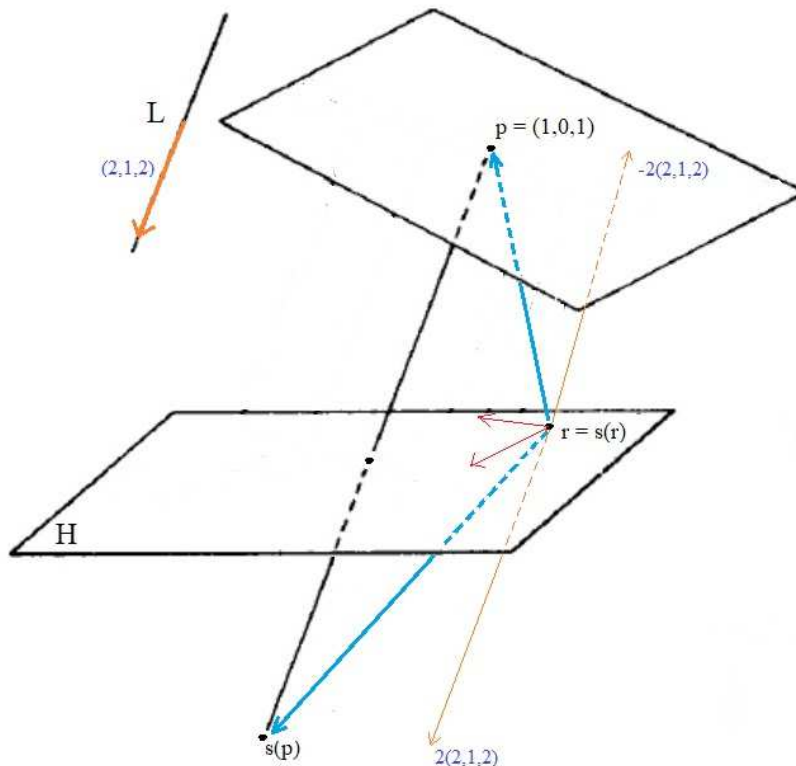
Przejdźmy do wyznaczenia wzoru na s . Układem bazowym płaszczyzny H jest $(1, 1, 0); (1, 0, 1), (0, 1, 1)$. Zatem obraz punktu $r = (1, 1, 0) \in H$ w tej symetrii równy jest $s(r) = (1, 1, 0)$. Dla $x \in \mathbb{R}^3$ mamy zatem $s(x) = s(r) + s'(\vec{rx})$, czyli w bazie standardowej:

$$s \left(\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \right) = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + M(s')_{st}^{st} \left(\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} - \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \right).$$

Oczywiście biorąc bazę $\mathcal{A} = ((1, 0, 1), (0, 1, 1), (2, 1, 2))$ przestrzeni \mathbb{R}^3 (pierwsze dwa wektory rozpinają $T(H)$, a ostatni $T(L)$) wyznaczamy macierz

$$M(s')_{\mathcal{A}}^{\mathcal{A}} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

i stąd potem (znanymi metodami) wyznaczamy $M(s')_{st}^{st}$.



9.1 Zadania do samodzielnej pracy

Zadania ilustrujące umiejętności niezbędne do zaliczenia przedmiotu oznaczone są symbolem ♠.

Przy tych zadaniach dodany jest opis umiejętności, które sprawdzają.

1. (♠ Znajdowanie obrazów przekształceniach afinicznych)

- Znajdź obraz punktu $p = (1, 1, 1)$ w symetrii względem $W = \text{lin}((1, 1, 0, 0), (1, 0, 0, 1))$.
- Niech $H = \text{af}((1, 1, 0), (2, 1, 1), (1, 2, 0))$ i $L = (1, 1, 1) + \text{lin}((-1, 1, 1))$ będą podprzestrzeniami afinicznymi \mathbb{R}^3 . Wyznacz obrazy punktu $(4, -2, -1)$ przy rzucie na H wzdłuż L i przy symetrii względem H wzdłuż L .
- Niech $s : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ będzie symetrią względem płaszczyzny $H : x_1 + x_2 - x_3 = 2$ wzdłuż prostej $L = (0, 1, 0) + \text{lin}((2, 1, 2))$. Znajdź obraz $s(p)$ punktu $p = (1, 0, 1)$ przy symetrii s . Znajdź bazę punktową obrazu $s(M)$ przestrzeni $M = \text{af}(p, p_1, p_2)$, gdzie $p_1 = (1, 2, 2), p_2 = (1, 6, 4)$, przy symetrii s .
- W przestrzeni afinicznej \mathbb{R}^3 rozważamy podprzestrzenie afiniczne

$$L = \text{af}((1, 1, 1), (3, 5, 4)), \quad H : x_1 + 2x_2 - 2x_3 = 4.$$

Niech $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ będzie rzutem na H wzdłuż L oraz niech $g : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ będzie jednokładnością o środku $(5, 5, 5)$ i skali 3. Znajdź obraz punktu $(g \circ f)((0, 1, 1))$.

2. (♠ Znajdowanie wzoru na przekształcenie afiniczne)

- Znajdź wzór przekształcenia afinicznego $f : \mathbb{R}^3 \rightarrow \mathbb{R}^4$ spełniającego warunki

$$\begin{aligned} f((1, 1, 1)) &= (2, 0, 1, 0), & f((2, 1, 1)) &= (0, 1, 3, 3) \\ f((1, 2, 1)) &= (0, 0, 1, 3), & f((1, 1, 2)) &= (0, 1, 0, 1). \end{aligned}$$

- Niech $H \subset \mathbb{R}^3$ będzie płaszczyzną o równaniu $x_1 + 2x_2 - x_3 = 1$. Znajdź wzór na takie przekształcenie afiniczne $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$, że $f(H) = \{(1, 1, 4)\}$ oraz $f((1, 1, 1)) = (0, 0, 1)$.
- Znajdź wzór na symetrię $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ względem prostej $K = (2, 1, 0) + \text{lin}((1, -1, -1))$ wzdłuż płaszczyzny $H = (1, 0, 0) + \text{lin}((1, 1, -2), (0, 1, -1))$.
- W przestrzeni afinicznej \mathbb{R}^3 dana jest prosta $L = (2, 1, 0) + \text{lin}((1, 0, -1))$ oraz płaszczyzna $M = \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1 + 2x_2 - x_3 = 2\}$. Znajdź wzór na przekształcenie afiniczne $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ będące rzutem na L wzdłuż $W = \text{lin}((1, 1, 1), (0, 1, 3))$. Wyznacz parametryzację obrazu płaszczyzny M w jednokładności o środku $(0, 0, 1)$ i skali 2.
- Niech $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ będzie jednokładnością o środku $(1, 1, 1)$ i skali 3, niech $g : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ będzie przesunięciem o wektor $(3, 2, 1)$ oraz niech $h : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ będzie rzutem na podprzestrzeń $L = (0, 1, 0) + \text{lin}(1, 1, 2)$ wzdłuż $H : x_1 + 4x_2 + 3x_3 = 2$. Znajdź wzory na przekształcenia

$$f \circ g \circ h, \quad g \circ h \circ h \circ f, \quad h \circ f \circ f \circ g \circ g.$$

- Niech $f : H \rightarrow H$ będzie rzutem na podprzestrzeń $H_1 \subseteq H$ wzdłuż $W \subseteq T(H)$. Załóżmy, że $\dim W = k$. Czy istnieje $k+1$ różnych punktów p_0, p_1, \dots, p_k , takich że $f(p_0) = f(p_1) = \dots = f(p_k)$?
- Dana jest skończona wymiarowa przestrzeń afiniczna H oraz izomorfizm afiniczny $f : H \rightarrow H$ taki, że $f(M) \subseteq M$, dla pewnej podprzestrzeni afinicznej $M \subseteq H$. Czy wynika stąd, że $f(M) = M$?
- Załóżmy, że przekształcenie afiniczne $f : H \rightarrow H$ ma dokładnie jeden punkt stały, tzn. istnieje dokładnie jeden punkt $p_0 \in H$ taki, że $f(p_0) = p_0$. Pokaż, że nie istnieje niezerowy wektor $v \in T(H)$, że $f'(v) = v$.
- W \mathbb{R}^n dana jest podprzestrzeń afiniczna opisana równaniem $c_1x_1 + c_2x_2 + \dots + c_nx_n + c_{n+1} = 0$ oraz dany jest izomorfizm afiniczny $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$ określony wzorem:

$$f(x_1, x_2, \dots, x_n) = (a_{11}x_1 + \dots + a_{1n}x_n + b_1, a_{21}x_1 + \dots + a_{2n}x_n + b_2, \dots, a_{n1}x_1 + \dots + a_{nn}x_n + b_n).$$

Wykaż, że obrazem L w izomorfizmie f jest podprzestrzeń afiniczna L opisana równaniem

$$\det \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 - x_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 - x_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} & b_n - x_n \\ c_1 & c_2 & \dots & c_n & c_{n+1} \end{bmatrix} = 0.$$

Definicja 9.5: Hiperpłaszczyzna podpierająca, brzeg bryły wielościennej

Niech $W \subseteq \mathbb{R}^n$ będzie zbiorem wypukłym. Powiemy, że $n - 1$ -wymiarowa podprzestrzeń afiniczna $H \subset \mathbb{R}^n$ jest HIPERPLASZCZYZNĄ PODPIERAJĄCĄ zbiór W w punkcie $p = (p_1, \dots, p_n) \in W$, jeżeli H jest opisana równaniem $a_1x_1 + a_2x_2 + \dots + a_nx_n = b$, gdzie $(a_1, \dots, a_n) \in \mathbb{R}^n$, $b \in \mathbb{R}$ spełniają:

- zbiór W „leży po jednej stronie” H , czyli dla każdego $x = (x_1, \dots, x_n) \in W$ zachodzi nierówność $a_1x_1 + a_2x_2 + \dots + a_nx_n \leq b$,
- punkt p należy do H , czyli $a_1p_1 + a_2p_2 + \dots + a_np_n = b$.

Niech W będzie bryłą wielościnną. Zbiór punktów $p \in W$, dla których istnieje płaszczyzna podpierająca W w punkcie p nazwiemy BRZEGIEM W .

Z uwagi na to, że nie chcemy wprowadzać elementów analitycznych, definiujemy brzeg jedynie dla bryły wielościennej, co pozwala na użycie płaszczyzny podpierającej, zamiast pojęć metrycznych. Można udowodnić, że dla brzegu ∂W zdefiniowanego w sposób analityczny² zachodzi twierdzenie: jeśli W jest zbiorem wypukłym i domkniętym oraz $p \in \partial W$, to istnieje hiperpłaszczyzna podpierająca W w punkcie p .

Definicja 9.6: Ściana, krawędź, wierzchołek zbioru wypukłego

ŚCIANĄ zbioru wypukłego W nazwiemy zbiór $W \cap H$, gdzie H jest hiperpłaszczyzną podpierającą W . WYMIAREM ŚCIANY $W \cap H$ nazywamy liczbę $\dim \text{af}(W \cap H)$. Ścianę wymiaru 0 nazywamy WIERZCHOŁKIEM zbioru W , zaś ścianę wymiaru 1 nazywamy KRAWĘDZIĄ.

Pojęcie wymiaru ściany jest oczywiście dobrze określone (np. punkt wewnętrzny krawędzi nie jest wierzchołkiem). Dla opisu ścian brył wielościennej przydatne jest pojęcie półprzestrzeni dopełniającej.

Definicja 9.7: Półprzestrzeń dopełniająca

Niech $H = \{(x_1, \dots, x_n) \in \mathbb{R}^n \mid a_1x_1 + \dots + a_nx_n \leq b\}$ będzie półprzestrzenią. PÓŁPRZESTRZENIĄ DOPEŁNIAJĄCĄ H nazywamy półprzestrzeń $H^- = \{(x_1, \dots, x_n) \in \mathbb{R}^n \mid a_1x_1 + \dots + a_nx_n \geq b\}$.

Odnotujmy następujące łatwe w dowodzie obserwacje. Zostawiamy je jako ćwiczenie.

- Jeśli H jest półprzestrzenią w \mathbb{R}^n , to $\mathbb{R}^n = H \cup H^-$, natomiast $H \cap H^-$ jest brzegiem zarówno H , jak i H^- . Zbiór ten jest, zgodnie z definicją wyżej, jedyną ścianą półprzestrzeni H .
- Niech $W = \bigcap_{i=1}^t H_i$ będzie bryłą wielościnną, gdzie H_i są półprzestrzeniami. Wówczas $W \cap H^-$ jest ścianą W lub zbiorem pustym (patrz np. $H_1 \cap H_2^-$, gdzie $H_1 : x_1 \in \mathbb{R} : x_1 \geq 2, H_2 : x_1 \in \mathbb{R} : x_1 \geq 1$). Co więcej, jeśli dla pewnego s zbiór $S = W \cap \bigcap_{i=1}^s H_i$ jest niepusty, to jest on ścianą W .

Obserwacja 9.5: Opis ścian brył wielościennej

Niech $p = (p_1, \dots, p_n)$ będzie punktem bryły wielościennej $W \subset \mathbb{R}^n$ będącej przecięciem t półprzestrzeni postaci $H_i = \{(x_1, \dots, x_n) \in \mathbb{R}^n \mid a_{i1}x_1 + \dots + a_{in}x_n \leq b_i\}$, dla $1 \leq i \leq t$, przy czym zakładamy, że punkt p należy do brzegu dokładnie s pierwszych półprzestrzeni, tzn.

$$\begin{aligned} a_{i1}p_1 + \dots + a_{in}p_n &= b_i, \text{ dla każdego } 1 \leq i \leq s, \\ a_{j1}p_1 + \dots + a_{jn}p_n &< b_j, \text{ dla każdego } s+1 \leq j \leq t. \end{aligned}$$

Rozważmy macierz $A_p = [a_{ij}] \in M_{t \times n}(\mathbb{R})$. Wówczas zbiór $S = W \cap \bigcap_{i=1}^s H_i^-$ jest ścianą wymiaru $n - r(A_p)$ zawierającą p .

²Tzn. $\partial W = \{p \in \mathbb{R}^n : \forall \epsilon > 0 \exists q_1, q_2 \ q_1 \in K(p, \epsilon) \cap W, q_2 \in K(p, \epsilon) \setminus W\}$, gdzie $K(p, \epsilon)$ jest kulą o środku p i promieniu ϵ .

Dowód. Jeśli przez H określimy zbiór rozwiązań układu s równań postaci $a_{i1}x_1 + \dots + a_{in}x_n = b_i$, to na mocy tw. Kroneckera-Capellego zbiór H jest przestrzenią afiniczną wymiaru $n - r(A_p)$. Mamy też $H = \bigcap_{i \leq s} H_i \cap \bigcap_{i \leq s} H_i^-$. Oczywiście $S \subseteq H$, więc $\dim S \leq n - r(A_p)$.

Niech $m = n - r(A_p)$ i niech układ $\alpha_1, \dots, \alpha_m$ wektorów w \mathbb{R}^n stanowi bazę przestrzeni liniowej $T(H)$. Uzupełnijmy ten układ do bazy $\alpha_1, \dots, \alpha_n$ całej przestrzeni \mathbb{R}^n . Wówczas w układzie bazowym $p; \alpha_1, \dots, \alpha_n$ punkt należy do H wtedy i tylko wtedy, gdy ma ostatnie $n - m$ współrzędnych zerowych. Skoro dla $j > s$ punkt p należy do każdej z półprzestrzeni H_j i nie leży na jej brzegu – mamy bowiem $a_{j1}p_1 + \dots + a_{jn}p_n < b_j$ – to dla każdego $i \leq m$ istnieje dostatecznie małe r_i , że $p + r_i\alpha_i$ również należy do przecięcia wszystkich H_j , dla $t \geq j > s$. Jednocześnie $p + r_i\alpha_i$ jest w H , ponieważ jego ostatnie $n - m$ współrzędnych w układzie bazowym $p; \alpha_1, \dots, \alpha_n$ to zera. A zatem zbiór S zawiera układ $m + 1$ afinicznie niezależnych punktów $\{p, p + r_1\alpha_1, \dots, p + r_m\alpha_m\}$, czyli $\dim S \geq m$. W rezultacie $\dim S = m$. \square

Uzyskany wynik pozwala sprawdzać kiedy punkt przestrzeni afinicznej jest wierzchołkiem wielościanu. W tym sensie możemy uzyskać prosty algorytm szukania wierzchołków czy krawędzi wielościanu – istotny dla rozwiązywania praktycznych problemów programowania liniowego. Naszym celem będzie natomiast dowód twierdzenia strukturalnego, wymagającego zastosowania tzw. teorii dualności.

Twierdzenie 9.2: Twierdzenie strukturalne – Minkowski, Steinitz, Weyl

Następujące warunki są równoważne dla podzbioru $\Delta \subseteq \mathbb{R}^n$.

- (1) podzbiór Δ jest wielościanem wypukłym,
- (2) $\Delta = \text{conv}(p_0, \dots, p_r)$, dla pewnego układu punktów p_1, \dots, p_r w \mathbb{R}^n .

Definicja 9.8: Stożek

Dla dowolnego podzbioru $X \subseteq \mathbb{R}^n$ definiujemy STOŻEK WYPUKŁY $\text{cone}(X)$ rozpięty (generowany) przez X jako zbiór nieujemnych kombinacji liniowych układów punktów z X :

$$\text{cone}(X) = \{a_1p_1 + \dots + a_r p_r \mid p_1, \dots, p_r \in X, a_1, \dots, a_r \geq 0\}.$$

Definiujemy też WYMIAR STOŻKA jako $\dim \text{lin}(\text{cone}(X))$. Jeśli X jest zbiorem skończonym to stożek $\text{cone}(X)$ nazywamy SKOŃCZENIE GENEROWANYM.

Jak widzimy, definicja wykorzystuje wektor zerowy w \mathbb{R}^n . Alternatywnie można definiować stożek $C \subseteq \mathbb{R}^n$ tak, aby dla każdego niezerowego $x \in C$ zachodziło $\{tx \in C \mid t \geq 0\}$. Innymi słowy, stożek jest sumą półprostych. Jest jasne, że stożek jest zbiorem wypukłym. Wykażemy, że w istocie stożek skończenie generowany jest bryłą wielościanową, a nawet przecięciem skończenie wielu półprzestrzeni przechodzących przez 0. Teoria dowolnych stożków wymaga bardziej zaawansowanych narzędzi.

Twierdzenie 9.3: Twierdzenie Fouriera-Motzkina

Obraz bryły wielościennej Δ przy rzutowaniu $p : \mathbb{R}^n \rightarrow \mathbb{R}^{n-1}$, danym wzorem $p(x_1, \dots, x_n) = (x_1, \dots, x_{n-1})$, jest bryłą wielościanową.

Dowód. Załóżmy, że bryła wielościennej Δ zadana jest układem m nierówności postaci

$$a_{i1}x_1 + a_{i2}x_2 + \dots + a_{in}x_n \leq b_i. \quad (\dagger)$$

Popatrzmy na współczynniki w n -tej kolumnie macierzy $A = [a_{ij}]$ i rozważmy trzy zbiory postaci

$$P = \{i : a_{in} > 0\}, \quad N = \{j : a_{jn} < 0\}, \quad Z = \{k : a_{kn} = 0\}.$$

Dla indeksów i, j należących do $P \cup N$ przyjmujemy, po podzieleniu odpowiednich nierówności przez a_{in} :

$$\begin{aligned} x_n &\leq a'_{i1}x_1 + \dots + a'_{i,n-1}x_{n-1} + b'_i, \text{ dla } i \in P \\ a'_{j1}x_1 + \dots + a'_{j,n-1}x_{n-1} + b'_j &\leq x_n, \text{ dla } j \in N. \end{aligned}$$

W konsekwencji, warunek $(x_1, \dots, x_{n-1}) \in p(\Delta)$ można zapisać za pomocą układu nierówności³

$$a'_{j_1}x_1 + \dots + a'_{j_{n-1}}x_{n-1} + b'_j \leq x_n \leq a_{i_1}x_1 + \dots + a_{i_{n-1}}x_{n-1} + b'_i,$$

gdzie $i \in P$ oraz $j \in N$. Oznacza to, że zbiór $p(\Delta)$ jest zadany za pomocą $|P| \cdot |N|$ nierówności postaci:

$$(a'_{j_1} - a_{i_1})x_1 + \dots + (a'_{j_{n-1}} - a_{i_{n-1}})x_{n-1} \leq (b'_i - b'_j)$$

oraz nierówności typu (\dagger) , dla których $a_{in} = 0$ (które nie zawierają x_n), mających indeksy spoza zbioru $P \cup N$. Stąd $p(\Delta)$ jest bryłą wielościenneą. \square

Udowodnione twierdzenie jest podstawą tzw. algorytmu Fouriera-Motzkina rozwiązywania układów nierówności liniowych. Możemy rozważyć układ m nierówności liniowych od n zmiennych x_1, \dots, x_n , przy czym zmienna x_n ma być wyeliminowana. Wyjściowy układ nierówności ma rozwiązanie $(s_1, \dots, s_{n-1}, s_n)$, które jest punktem bryły wielościennej Δ wtedy i tylko wtedy, gdy po redukcji punkt (s_1, \dots, s_{n-1}) jest rozwiązaniem układu opisującego $p(\Delta)$. W ten sposób eliminujemy kolejne zmienne. Na końcu stwierdzamy, że nierówności typu $a \leq x_1$ oraz $x_1 \leq b$ mają rozwiązanie wtedy i tylko wtedy, gdy $a \leq b$.

Rozważmy układ nierówności od zmiennych x_1, x_2, x_3 postaci:

$$\begin{cases} -5x_1 + 4x_2 + 2x_3 & \leq 12 \\ -4x_1 + 3x_2 + 3x_3 & \leq 9 \\ 5x_1 - 2x_2 - x_3 & \leq -7 \\ 2x_1 + 6x_2 - 3x_3 & \leq 12 \end{cases}$$

Aby wyeliminować zmienną x_3 zapisujemy nierówności w równoważnej postaci:

$$\begin{cases} x_3 & \leq \frac{12+5x_1-4x_2}{2} \\ x_3 & \leq \frac{9+4x_1-3x_2}{3} \\ x_3 & \geq 7 + 5x_1 - 2x_2 \\ x_3 & \geq \frac{-12+2x_1+6x_2}{3} \end{cases}$$

Mamy zatem dwie nierówności \leq oraz dwie \geq . Zatem rozważany układ ma rozwiązanie jeśli prawa strona każdej nierówności \leq jest równa co najmniej prawej stronie każdej nierówności \geq . To prowadzi do układu:

$$\begin{cases} 7 + x_1 - 2x_2 & \leq \frac{12+5x_1-4x_2}{2} \\ 7 + 5x_1 - 2x_2 & \leq \frac{9+4x_1-3x_2}{3} \\ \frac{-12+2x_1+6x_2}{3} & \leq \frac{12+5x_1-4x_2}{2} \\ \frac{-12+2x_1+6x_2}{3} & \leq \frac{9+4x_1-3x_2}{3} \end{cases}$$

Czytelnika zainteresowanego większą liczbą przykładów i związkami algorytmu Fouriera z klasyczną eliminacją Gaussa, odsyłam do świetnego elementarnego tekstu Nielsa Lauritzena w „Undergraduate Convexity”: https://www.worldscientific.com/doi/suppl/10.1142/8527/suppl_file/8527_chap01.pdf.

Zastosujmy powyższe twierdzenie dla stożków.

Obserwacja 9.6

W przestrzeni afinicznej \mathbb{R}^{n+1} złożonej z punktów postaci (x_0, \dots, x_n) rozważmy przestrzeń afiniczną H zadaną równaniem $x_0 = 1$. Dla dowolnego $X \subseteq H$ zachodzi

$$\text{conv}(X) = \text{cone}(X) \cap H.$$

Dowód. Inkluzja $\text{conv}(X) \subseteq \text{cone}(X) \cap H$ jest jasna, bo $\text{cone}(X)$ oraz H są wypukłe. Załóżmy, że dla $i = 1, \dots, r$ mamy punkty $p_i = (1, b_{i1}, \dots, b_{in}) \in \mathbb{R}^{n+1}$. Wówczas wektor $a_1p_1 + \dots + a_r p_r$ ma na zerowej współrzędnej sumę $a_1 + \dots + a_r$. Stąd kombinacjom liniowym punktów p_i w \mathbb{R}^{n+1} odpowiadają kombinacje afiniczne p_i w H , a nieujemnym kombinacjom w \mathbb{R}^{n+1} – kombinacje wypukłe w H . \square

³Jeśli $P = \emptyset$ lub $N = \emptyset$, to $p(\Delta)$ opisany jest nierównościami (\dagger) , dla $i \in Z$. Jeśli również Z jest zbiorem pustym, to $p(\Delta)$ jest przestrzenią afiniczną wymiaru $n - 1$. Np. dla półprzestrzeni $\Delta = \{(x_1, x_2) \in \mathbb{R}^2 \mid x_1 + x_2 \leq 0\}$ zbiór $p(\Delta)$ jest prostą.

Twierdzenie 9.4: Skończenie generowane stożki są bryłami wielościennymi

Dla dowolnego układu r wektorów $v_i = (b_{1i}, \dots, b_{ni})$ w przestrzeni \mathbb{R}^n , gdzie $1 \leq i \leq r$, stożek $\sigma = \text{cone}(v_1, \dots, v_r)$ jest bryłą wielościenną. Co więcej, stożek ten jest opisany układem skończenie wielu nierówności typu

$$a_{i1}x_1 + \dots + a_{in}x_n \leq 0.$$

Dowód. Naszym celem będzie wykazanie, że stożek σ jest obrazem pewnej bryły wielościennej przy rzutowaniu $p : \mathbb{R}^{n+r} \rightarrow \mathbb{R}^n$ (a w istocie przy złożeniu r rzutowań).

Niech $B \in M_{n \times r}(\mathbb{R})$ będzie macierzą, której i -ta kolumna zawiera współrzędne v_i w bazie standardowej, czyli b_{ki} . W przestrzeni \mathbb{R}^{n+r} ze współrzędnymi $(x, y) = (x_1, \dots, x_n, y_1, \dots, y_r)$ rozpatrzmy bryłę wielościenną Δ zadaną układem nierówności, który można zapisać skrótowo w postaci

$$(x, y) \in \Delta \iff x = By \text{ oraz } y \geq 0$$

czyli po zapisaniu we współrzędnych $(x_1, \dots, x_n, y_1, \dots, y_r)$ chodzi o układ nierówności

$$\begin{cases} x_i - b_{i1}y_1 - b_{i2}y_2 - \dots - b_{ir}y_r & \leq 0, \text{ dla } 1 \leq i \leq n, \\ b_{j1}y_1 + b_{j2}y_2 + \dots + b_{jr}y_r - x_j & \leq 0, \text{ dla } 1 \leq j \leq n, \\ -y_k & \leq 0, \text{ dla } 1 \leq k \leq r. \end{cases}$$

Wówczas rzutowanie $p : \mathbb{R}^{n+r} \rightarrow \mathbb{R}^n$ określone wzorem $p(x, y) = x$ oczywiście przeprowadza Δ na σ , czyli

$$p(\Delta) = \text{cone}(v_1, \dots, v_r) = \sigma.$$

Z drugiej strony z twierdzenia Fouriera-Motzkina wiemy, że σ jest bryłą wielościenną, czyli spełnia pewien układ nierówności postaci

$$a_{i1}x_1 + \dots + a_{in}x_n \leq b_i.$$

Pozostaje zatem wykazać, że $b_i = 0$. Wiemy jednak, że $0 \in \text{cone}(v_1, \dots, v_r)$, więc wszystkie b_i są nieujemne. Z drugiej strony, gdyby $b_i > 0$, dla pewnego i , wówczas mielibyśmy wektor $v = (x_1, \dots, x_n) \in \sigma$, że

$$0 < a_{i1}x_1 + \dots + a_{in}x_n \leq b_i.$$

Skoro jednak dla każdego $c \in \mathbb{R}$ mamy $cv \in \sigma$, to dla $c \gg 0$ dostalibyśmy sprzeczność. □

Dowód twierdzenia wyżej pozwala udowodnić jedną z implikacji w twierdzeniu strukturalnym.

Wniosek 9.3

Dla układu punktów $X = \{p_0, \dots, p_r\}$ w przestrzeni \mathbb{R}^n zbiór $\text{conv}(X)$ jest wielościannem wypukłym.

Dowód. Rozważmy układ $Y \subset \mathbb{R}^{n+1}$ złożony z punktów postaci

$$y_i = (1, p_i), \text{ gdzie } 1 \leq i \leq r.$$

Wówczas $\text{cone}(Y)$ jest, jako stożek skończenie generowany, bryłą wielościenną. Stąd

$$\text{conv}(Y) = \text{cone}(Y) \cap H$$

jest wielościannem, gdzie $H : \{(1, x), x \in \mathbb{R}^n\}$. Po zrzutowaniu $p : \mathbb{R}^{n+1} \rightarrow \mathbb{R}^n$ postaci

$$p((x_0, \dots, x_n)) \mapsto (x_1, \dots, x_n)$$

mamy zatem $p(\text{conv}(Y)) = \text{conv}(X)$. Z twierdzenia Fouriera-Motzkina wynika więc, że $\text{conv}(X)$ jest bryłą wielościenną. Jest jasne, że $\text{conv}(X)$ jest zbiorem ograniczonym, co kończy dowód. □

Uwaga. Warto uzasadnić samodzielnie wniosek opisujący dokładnie nierówności spełniane przez dowolny sympleks n -wymiarowy (mający oczywiście $n + 1$ ścian wymiaru $n - 1$).

Wniosek 9.4

Niech p_0, \dots, p_n będzie afinicznie niezależnym układem punktów w \mathbb{R}^n , takim że

$$\det \begin{bmatrix} p_0 & 1 \\ p_1 & 1 \\ \vdots & \vdots \\ p_n & 1 \end{bmatrix} > 0.$$

Wówczas $W = \text{conv}(p_0, p_1, \dots, p_n)$ jest wielościanem złożonym z punktów $x = (x_1, \dots, x_n)$ spełniających układ $n + 1$ nierówności:

$$\det \begin{bmatrix} x & 1 \\ p_1 & 1 \\ \vdots & \vdots \\ p_n & 1 \end{bmatrix} \geq 0, \quad \det \begin{bmatrix} x & 1 \\ p_1 & 1 \\ \vdots & \vdots \\ p_n & 1 \end{bmatrix} \geq 0, \quad \det \begin{bmatrix} p_0 & 1 \\ x & 1 \\ \vdots & \vdots \\ p_n & 1 \end{bmatrix} \geq 0, \quad \det \begin{bmatrix} p_0 & 1 \\ p_1 & 1 \\ \vdots & \vdots \\ x & 1 \end{bmatrix} \geq 0.$$

Co więcej, dla każdego j punkt p_j spełnia wszystkie nierówności wyżej, za wyjątkiem j -tej, czyli jest wierzchołkiem wielościanu.

Jeśli Państwo myślą, że nic ciekawego nie wynika z takiego opisu, warto przypomnieć sobie dodatek 5.4 ze skryptu z GAL I. Opisywał on – choć wtedy nie można było tego powiedzieć – jak wygląda wielościan rozpięty na wszystkich macierzach permutacyjnych rozmiaru n . Okazuje się, że jest to zbiór macierzy podwójnie stochastycznych, czyli takich, gdzie wiersze i kolumny mają sumy wyrazów równe 1, co udowodnił w 1946 roku Birkhoff (i do czego Państwa zachęcam). Fakt ten ma wiele zastosowań.

Aby uzasadnić, że każdy wielościan wypukły jest uwypukleniem skończonego zbioru punktów, będziemy potrzebowali uzasadnić wcześniej fakt mówiący, że bryła wielościennej pewnej szczególnej postaci jest stożkiem. W tym celu wprowadzimy podstawowe narzędzia teorii dualności.

Wcześniej jednak wzmocnijmy nieco geometryczne intuicje stojące za wykazywanymi rezultatami, tak by wprowadzenie do naszych rozumowań funkcjonałów wydało się naturalne. Intuicje te związane są bezpośrednio z faktem, że każdy funkcjonał odpowiada geometrycznie pewnej podprzestrzeni kowymiaru 1. Oto *podstawowy rezultat teorii nierówności liniowych*.

Twierdzenie 9.5: Lemat Farkasa

Niech v_1, \dots, v_m, b będą wektorami w przestrzeni \mathbb{R}^n . Wówczas zachodzi alternatywa wyłączająca:

- (1) albo $b \in \text{cone}(v_1, \dots, v_m)$,
- (2) albo istnieje funkcjonał $\lambda \in (\mathbb{R}^n)^*$, taki że $\lambda(b) > 0$ oraz $\lambda(v_1) \leq 0, \dots, \lambda(v_m) \leq 0$.

Punkt (2) można sformułować geometrycznie, mianowicie: istnieje podprzestrzeń afiniczna H wymiaru $n - 1$ (hiperpowierzchnia), która „rozdziela” stożek $\text{cone}(v_1, \dots, v_m)$ oraz prostą $\text{lin}(b)$. Co to znaczy? Jeśli H opisana jest równaniem $a_1x_1 + a_2x_2 + \dots + a_nx_n = 0$, to dla wektorów $(s_1, s_2, \dots, s_n) \in \text{cone}(v_1, \dots, v_m)$ mamy $a_1s_1 + \dots + a_ns_n \leq 0$, zaś dla wektora $b = (b_1, \dots, b_n)$ mamy $a_1b_1 + a_2b_2 + \dots + a_nb_n > 0$.

Prostą ilustrację dają choćby układ wektorów $v_1 = (1, 0)$, $v_2 = (1, 1)$ oraz $b = (0, 1)$. Nie ma wątpliwości, że $b \notin \text{cone}(v_1, v_2)$. Lemat powyżej mówi, że istnieje prosta rozdzielająca $\text{cone}(v_1, v_2)$ od $\text{lin}(b)$. Wystarczy wziąć prostą $y = \text{lin}(-1, 1)$. Odpowiada jej funkcjonał $\lambda \in (\mathbb{R}^2)^*$ dany wzorem $\lambda(x_1, x_2) = -x_1 + x_2$. Oczywiście $\lambda(v_1) = -1$, $\lambda(v_2) = 0$, zaś $\lambda(b) = 1$.

Aby udowodnić powyższy lemat wykorzystamy jeszcze jedną ważną konwencję. Niech $v_i = (a_{i1}, \dots, a_{in})$ i niech $A = [a_{ij}] \in M_{n \times m}(\mathbb{R})$. Punkt pierwszy lematu mówi, że istnieje $x \in \mathbb{R}^m$, $x \geq 0$ (nieujemne współrzędne), że

$$Ax = b.$$

Drugi punkt można natomiast przepisać w postaci: istnieje $y = (a_1, \dots, a_n) \in \mathbb{R}^n$, że

$$A^T y \leq 0 \quad \text{oraz} \quad b^T y > 0.$$

Oczywiście y ma być taki, że $\lambda(x_1, \dots, x_n) = a_1 x_1 + \dots + a_n x_n$. Widać po przemnożeniu macierzy, że dostajemy warunki równoważne opisanym w lemacie. Można powyższe warunki interpretować także w języku funkcjonałów. Rozważmy przekształcenie liniowe $\phi : \mathbb{R}^m \rightarrow \mathbb{R}^n$ dane macierzą A . Macierz A^T jest macierzą przekształcenia sprzężonego $\phi^* : (\mathbb{R}^n)^* \rightarrow (\mathbb{R}^m)^*$. Warunek $A^T y \leq 0$ oznacza, dokładnie tyle, że obraz każdego z v_i jest przy λ niedodatni, dla $1 \leq i \leq m$. Zauważmy jeszcze, że używając języka macierzowego można przeformułować Obserwację 10.3 w następujący sposób: dla dowolnego stożka C w przestrzeni \mathbb{R}^n generowanego przez r wektorów istnieje macierz $A \in M_{m \times n}(\mathbb{R})$, że

$$C = \{v \in \mathbb{R}^n \mid Av \leq 0\}.$$

Dowód Lematu Farkasa. Jeśli zachodzi pierwszy warunek, to

$$b^T y = (Ax)^T y = (x^T A^T) y = x^T (A^T y) \leq 0,$$

jeśli $y^T A \leq 0$ oraz $x \geq 0$. Ostatnia nierówność przeczy warunkowi $y^T b > 0$. Trudniej wykazać, że drugi warunek zachodzi, gdy nie zachodzi pierwszy.

Niech C będzie stożkiem generowanym przez kolumny macierzy A . Na mocy Obserwacji 10.3 istnieje macierz Y , taka że $C = \{v \in \mathbb{R}^n \mid Yv \leq 0\}$. Jeśli pierwszy warunek nie zachodzi, to $b \notin C$. To oznacza, że $Yb \not\leq 0$, czyli istnieje wektor wierszowy y w macierzy Y , że $y^T b > 0$. Jeśli v_i jest wektorem kolumnowym w A , to z definicji C mamy jednak $y^T v_i \leq 0$. Stąd $y^T A \leq 0$ i dowód jest zakończony.

* * *

Definicja 9.9: Stożek dualny

Dla dowolnego zbioru $X \subseteq \mathbb{R}^n$ definiujemy tzw. stożek dualny do $\text{cone}(X)$ postaci:

$$\text{cone}^*(X) = \{\lambda \in (\mathbb{R}^n)^* \mid \forall v \in X \lambda(v) \geq 0\}.$$

Podobnie dla $Y \subseteq (\mathbb{R}^n)^*$ definiujemy

$$\text{cone}^*(Y) = \{v \in \mathbb{R}^n \mid \forall \lambda \in Y \lambda(v) \geq 0\}.$$

Czasami definiujemy stożek dualny do stożka $\text{cone}(X)$ jako podzbiór \mathbb{R}^n złożony z takich wektorów (a_1, \dots, a_n) , że dla każdego wektora $(x_1, \dots, x_n) \in \text{cone}(X)$ mamy $a_1 x_1 + \dots + a_n x_n \geq 0$.

Zachęcam Czytelnika do prostego dowodu następujących wartości stożków.

Obserwacja 9.7: Własności stożków dualnych

Niech X będzie podzbiorem \mathbb{R}^n .

- (i) Jeśli $X \subseteq Y \subseteq \mathbb{R}^n$, to $\text{cone}^*(X) \supseteq \text{cone}^*(Y)$.
- (ii) $\text{cone}^*(\text{conv}(X)) = \text{cone}^*(X)$.
- (iii) $\text{cone}^*(\text{cone}(X)) = \text{cone}^*(X)$.
- (iv) $\text{cone}^*(\text{cone}^*(X)) = \text{cone}(X)$.

Przechodzimy do naszkicowania twierdzenia o dualności. Dla uproszczenia notacji przyjmijmy, że jeśli $\sigma = \text{cone}(X)$ w przestrzeni V lub V^* , to $\text{cone}^*(\sigma)$ oznaczamy przez σ^* . Wówczas kluczowy czwarty punkt powyższej obserwacji sprowadza się do stwierdzenia, że $(\sigma^*)^* = \sigma$.

Twierdzenie 9.6: Dualność stożków – Farkas, Minkowski, Weyl

Następujące warunki są równoważne dla podzbiorów $\sigma \subseteq \mathbb{R}^n$ oraz $\sigma^* \subseteq (\mathbb{R}^n)^*$.

- (a) σ jest skończenie generowany, czyli $\sigma = \text{cone}(v_1, \dots, v_r)$,
- (a') σ^* jest skończenie generowany,
- (b) σ jest bryłą wielościanową, czyli jest rozwiązaniem układu $Ax \leq 0$.
- (b') σ^* jest bryłą wielościanową.

Dowód. Implikacje (a) \Rightarrow (b) oraz (a') \Rightarrow (b') są już nam znane. Jeśli σ spełnia warunek (b), to wiemy już, że jest opisana układem r nierówności $a_{i1}x_1 + \dots + a_{in}x_n \leq 0$. Biorąc więc funkcjonały $\lambda_i : \mathbb{R}^n \rightarrow \mathbb{R}$ dane wzorami $\lambda_i(x_1, \dots, x_n) = a_{i1}x_1 + \dots + a_{in}x_n$ bez trudu stwierdzamy, że $\sigma^* = \text{cone}(-\lambda_1, \dots, -\lambda_r)$, co daje (a'). Równoważności (a) oraz (a') wynikają natomiast wprost z uwag wyżej. \square

Jesteśmy gotowi na wykazanie finalnej implikacji w twierdzeniu strukturalnym.

Jeśli mamy wielościan Δ zadany przez układ nierówności postaci $a_{i1}x_1 + \dots + a_{in}x_n \leq b_i$, to bierzemy stożek $\sigma \in \mathbb{R}^{n+1}$ taki, aby $p(\sigma \cap H) = \Delta$, czyli zadany nierównościami $-b_ix_0 + a_{i1}x_1 + \dots + a_{in}x_n \leq 0$. Na mocy twierdzenia o dualności stożków stwierdzamy, że σ jest stożkiem rozpiętym na pewnym układzie wektorów v_1, \dots, v_r , gdzie $v_i = (c_{i0}, \dots, c_{in})$. Rozpatrujemy trzy przypadki, w zależności od znaku c_{i0} .

Jeśli dla każdego i mamy $c_{i0} > 0$, to kładąc $p_i = \frac{1}{c_{i0}}v_i$ widzimy, że $p(\sigma) = \Delta = \text{conv}(p_1, \dots, p_r)$. Jeśli σ zawiera niezerowy wektor $v = (0, c_1, \dots, c_n)$, to $\Delta \subset \Delta + tv$, dla $t > 0$, co jest sprzeczne z tym, że Δ jest ograniczony. Jeśli wreszcie $v = (c_0, \dots, c_n) \in \sigma$, gdzie $c_0 < 0$, to łącząc punkty wielościanu $\Delta \subset H = \{x_0 = 1\}$ z punktem odpowiadającym wektorowi v dostajemy wektor z zerową współrzędną i wracamy do poprzedniego przypadku. Twierdzenie strukturalne jest udowodnione.

Zachęcam Czytelnika do docenienia uzyskanego twierdzenia strukturalnego poprzez zauważenie, że poniższe obserwacje są zwykle trywialne przy jednym opisie wielościanu, a zdecydowanie nie – przy drugim.

- Przecięcie bryły wielościennej z podprzestrzenią afiniczną jest bryłą wielościanową.
- Przecięcie bryły wielościennej z bryłą wielościanową jest bryłą wielościanową.
- Suma Minkowskiego dwóch brył wielościanowych jest bryłą wielościanową.
- Każdy wielościan wypukły jest sumą Minkowskiego sympleksów.
- Każdy wielościan wypukły jest obrazem sympleksu przy pewnym rzucie afinicznym.

Można udowodnić ogólniejsze twierdzenie, związane z operacją sumy Minkowskiego.

Twierdzenie 9.7

Podzbiór W przestrzeni afinicznej \mathbb{R}^n jest bryłą wielościanową wtedy i tylko wtedy, gdy istnieje przedstawienie:

$$W = \text{conv}(V) + \text{cone}(Y),$$

gdzie V oraz Y są zbiorami skończonymi. Innymi słowy każda bryła wielościanowa jest sumą wielościanu wypukłego i stożka skończenie generowanego.

* * *

Teoria wielościanów związana jest nie tylko z optymalizacją liniową czy teorią zbiorów wypukłych, ale także z osiągnięciami tzw. rzeczywistej geometrii algebraicznej i jej aktywnie uprawianymi dziedzinami. Czytelnika zainteresowanego tekstem popularyzującym jeden z możliwych kierunków dalszego pogłębienia tematu odsyłam do artykułu Davida A. Coxa: *Mirror Symmetry and Polar Duality of Polytopes*, pod adres: <https://www.mdpi.com/2073-8994/7/3/1633>. Zainteresowanych natomiast monografią prezentującą dogłębnie algebraiczną teorię wielościanów i ich kombinatorykę, odsyłam do klasycznego już podręcznika Zieglera *Lectures on Polytopes*; GTM 152, Springer, 1995.

Rozdział 10

Formy dwuliniowe i iloczyn skalarny

Klasyfikacja wszystkich endomorfizmów (nad ciałem algebraicznie domkniętym) w języku postaci Jordana mimo niewątpliwego uroku ma też swoje wady – wiemy wprawdzie coś o geometrii każdego endomorfizmu z osobna, ale nie rozumiemy zbyt dobrze „struktury algebraicznej” stojącej za tym opisem geometrycznym. Mówiąc prościej: mając dwa endomorfizmy ϕ, ψ przestrzeni V , na przykład nad ciałem \mathbb{C} , możemy wyznaczyć bazy (i postaci) Jordana $\mathcal{J}_1, \mathcal{J}_2$ każdego z tych endomorfizmów. Uzyskamy informację geometryczną o każdym z nich. Nie wiemy natomiast czym jest z geometrycznego punktu widzenia $\phi \circ \psi$. Jego macierzą nie musi być przecież iloczyn macierzy w postaci Jordana $M(\psi)_{\mathcal{J}_2} \cdot M(\phi)_{\mathcal{J}_1}$, który nie musi mieć nawet postaci Jordana. Nie znamy relacji baz Jordana dla złożień innych niż wielomian od endomorfizmu. Takie podejście niestety nie zadziała. Określimy jednak nowy rodzaj baz, wymagający rozważania dodatkowej struktury na przestrzeni liniowej, który umożliwi to w istotnych sytuacjach. Struktura ta pozwoli między innymi na mówienie o prostopadłości wektorów, i to nie tylko w kontekście geometrycznym.

Definicja 10.1: Forma dwuliniowa

Niech V będzie przestrzenią liniową nad ciałem K . Funkcję:

$$h : V \times V \rightarrow K$$

nazywamy FORMĄ DWULINIOWĄ (albo FUNKCJONALEM DWULINIOWYM) na przestrzeni V , jeśli dla każdych $\alpha, \beta, \gamma, \delta \in V$ i $a, b, c, d \in K$ zachodzi:

- (1) $h(a \cdot \alpha + b \cdot \beta, \gamma) = a \cdot h(\alpha, \gamma) + b \cdot h(\beta, \gamma)$ liniowość względem pierwszej zmiennej,
- (2) $h(\alpha, c \cdot \gamma + d \cdot \delta) = c \cdot h(\alpha, \gamma) + d \cdot h(\alpha, \delta)$ liniowość względem drugiej zmiennej,

Zobaczmy kilka przykładów.

- Dla $V = K^2$ funkcja $h : V \times V \rightarrow \mathbb{R}$ dana wzorem:

$$h((x_1, x_2), (y_1, y_2)) = x_1 y_1 - x_2 y_2$$

jest formą dwuliniową. Mamy bowiem:

$$\begin{aligned} h(a \cdot (x_1, x_2) + b \cdot (x'_1, x'_2), (y_1, y_2)) &= h((ax_1 + bx'_1, ax_2 + bx'_2), (y_1, y_2)) \\ &= (ax_1 + bx'_1)y_1 - (ax_2 + bx'_2)y_2 = a(x_1 y_1 - x_2 y_2) + b(x'_1 y_1 - x'_2 y_2) \\ &= a \cdot h((x_1, x_2), (y_1, y_2)) + b \cdot h((x'_1, x'_2), (y_1, y_2)). \end{aligned}$$

- Dla $V = K^n$ oraz $A = [a_{ij}] \in M_n(K)$ dwuliniowa jest forma $h_A : V \times V \rightarrow K$ zadana wzorem

$$h_A((x_1, \dots, x_n), (y_1, \dots, y_n)) = \begin{bmatrix} x_1 & x_2 & \dots & x_n \end{bmatrix} \cdot \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \cdot \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \sum_{1 \leq i, j \leq n} a_{ij} x_i y_j \quad (\dagger)$$

Wynika to z rozdzielności mnożenia względem dodawania dla macierzy $V_1, V_2 \in M_{1 \times n}(K)$ oraz $W_1, W_2 \in M_{n \times 1}(K)$:

$$(V_1 + V_2)AW = V_1AW + V_2AW \quad \text{oraz} \quad VA(W_1 + W_2) = VAW_1 + VAW_2.$$

- Dla dowolnej pary wektorów $(a_1, a_2), (b_1, b_2) \in K^2$ określamy:

$$h((a_1, a_2), (b_1, b_2)) = \det \begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \end{bmatrix}.$$

Rzeczywiście, dla dowolnych $a_1, a_2, b_1, b_2, a'_1, a'_2, b'_1, b'_2 \in K$ mamy:

$$\begin{aligned} \det \begin{bmatrix} a_1 + a'_1 & b_1 \\ a_2 + a'_2 & b_2 \end{bmatrix} &= \det \begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \end{bmatrix} + \det \begin{bmatrix} a'_1 & b_1 \\ a'_2 & b_2 \end{bmatrix}, \\ \det \begin{bmatrix} a_1 & b_1 + b'_1 \\ a_2 & b_2 + b'_2 \end{bmatrix} &= \det \begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \end{bmatrix} + \det \begin{bmatrix} a_1 & b'_1 \\ a_2 & b'_2 \end{bmatrix}. \end{aligned}$$

- Dla $V = M_n(K)$ oraz dowolnych $A, B \in V$ określamy:

$$h((A, B)) = \text{tr}(AB^T).$$

- Dla $V = F_c[0, 1]$ – funkcji „całkowalnych” z $[0, 1]$ do \mathbb{R} , określamy:

$$h(f, g) = \int_0^1 f(x)g(x)dx.$$

- Dla przestrzeni $V = (P(X), \Delta, \emptyset)$ nad \mathbb{Z}_2 oraz $A, B \in V$ określamy:

$$h(A, B) = |A \cap B| \pmod{2}.$$

Odnotujmy kilka własności dowolnej formy dwuliniowej h na przestrzeni V nad ciałem K .

- $h(a \cdot \alpha, b \cdot \beta) = ab \cdot h(\alpha, \beta)$, dla dowolnych $a, b \in K$ oraz $\alpha, \beta \in V$,
- $h(\alpha, 0) = h(\alpha, \alpha - \alpha) = h(\alpha, \alpha) - h(\alpha, \alpha) = 0$, dla dowolnego $\alpha \in V$,
- $h(\alpha + \beta, \alpha + \beta) = h(\alpha, \alpha) + h(\alpha, \beta) + h(\beta, \alpha) + h(\beta, \beta)$, dla dowolnych $\alpha, \beta \in V$.

Obserwacja 10.1

Każda forma dwuliniowa h na przestrzeni K^n zadana jest wzorem:

$$h((x_1, \dots, x_n), (y_1, \dots, y_n)) = \sum_{1 \leq i, j \leq n} a_{ij} x_i y_j,$$

dla pewnych $a_{ij} \in K$.

Dowód. Niech h będzie formą dwuliniową na K^n oraz niech $(\epsilon_1, \epsilon_2, \dots, \epsilon_n)$ będzie bazą standardową. Dla każdego $i, j = 1, 2, \dots, n$ niech też $a_{ij} = h(\epsilon_i, \epsilon_j) \in K$. Wówczas mamy:

$$\begin{aligned} h((x_1, \dots, x_n), (y_1, \dots, y_n)) &= h(x_1 \epsilon_1 + x_2 \epsilon_2 + \dots + x_n \epsilon_n, y_1 \epsilon_1 + y_2 \epsilon_2 + \dots + y_n \epsilon_n) = \\ &\stackrel{(1)}{=} x_1 \cdot h(\epsilon_1, y_1 \epsilon_1 + y_2 \epsilon_2 + \dots + y_n \epsilon_n) + \dots + x_n \cdot h(\epsilon_n, y_1 \epsilon_1 + y_2 \epsilon_2 + \dots + y_n \epsilon_n) = \\ &\stackrel{(2)}{=} x_1 y_1 \cdot h(\epsilon_1, \epsilon_1) + \dots + x_1 y_n \cdot h(\epsilon_1, \epsilon_n) + \dots + x_n y_1 \cdot h(\epsilon_n, \epsilon_1) + \dots + x_n y_n \cdot h(\epsilon_n, \epsilon_n) = \\ &= a_{11} x_1 y_1 + a_{12} x_1 y_2 + \dots + a_{1n} x_1 y_n + \dots + a_{n1} x_n y_1 + a_{n2} x_n y_2 + \dots + a_{nn} x_n y_n. \end{aligned}$$

Wynika stąd, że h zadana jest wzorem (\dagger) , czyli jest dwuliniowa zgodnie z wcześniejszym rachunkiem. \square

Przez kilka wykładów zajmować się będziemy jedynie przestrzeniami liniowymi nad ciałem liczb rzeczywistych. Dlaczego? Dla ilustracji rozmaitych zagadnień potrzebujemy odróżniać skalary dodatnie od ujemnych. Później przyjrzymy się analogicznym strukturom definiowanym nad dowolnymi ciałami. Poprowadzi nas to do pięknych i głębokich rezultatów geometrycznych.

Definicja 10.2: Iloczyn skalarny

Niech V będzie przestrzenią liniową nad ciałem \mathbb{R} . Formę dwuliniową

$$\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{R}$$

nazywamy ILOCZYNEM SKALARNYM NA PRZESTRZENI V , jeśli

- $\langle \cdot, \cdot \rangle$ jest SYMETRYCZNA, to znaczy dla dowolnych $\alpha, \beta \in V$ mamy $\langle \alpha, \beta \rangle = \langle \beta, \alpha \rangle$,
- $\langle \cdot, \cdot \rangle$ jest DODATNIO OKREŚLONA, to znaczy dla niezerowego $\alpha \in V$ mamy $\langle \alpha, \alpha \rangle > 0$.

Możliwych iloczynów skalarnych na danej przestrzeni jest oczywiście wiele. Zobaczmy kilka przykładów na przestrzeni $V = \mathbb{R}^n$. Zaczniemy od fundamentalnego.

- Definiujemy $f : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$ wzorem:

$$\langle (x_1, \dots, x_n), (y_1, \dots, y_n) \rangle = x_1 y_1 + x_2 y_2 + \dots + x_n y_n$$

zadaje iloczyn skalarny na przestrzeni \mathbb{R}^n , który nazywać będziemy STANDARDOWYM ILOCZYNEM SKALARNYM i oznaczamy jako $\langle \cdot, \cdot \rangle_{st}$. Dzięki (standardowemu) iloczynowi skalarnemu odczytamy w nowym języku wiele poznanych wcześniej konfiguracji. Jest to również podstawowy obiekt w elementarnej geometrii analitycznej, choć niestety już nie geometrii uczonej w szkole.

Rozważmy układ równań o współczynnikach rzeczywistych postaci:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1 \\ \dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = b_m. \end{cases}$$

Przyjmijmy, że $v = (x_1, \dots, x_n)$ oraz $\alpha_i = (\alpha_{i1}, \dots, \alpha_{in})$ są elementami \mathbb{R}^n , dla $1 \leq i \leq m$. Wówczas powyższy układ równań liniowych zapisać możemy w postaci układu warunków:

$$\langle \alpha_1, v \rangle_{st} = b_1, \quad \dots, \quad \langle \alpha_m, v \rangle_{st} = b_m.$$

Zauważmy, że jeśli $\epsilon_1, \dots, \epsilon_n$ jest bazą standardową przestrzeni \mathbb{R}^n , to mamy:

$$\langle \epsilon_i, \epsilon_j \rangle = \begin{cases} 1, & \text{dla } i = j, \\ 0, & \text{dla } i \neq j. \end{cases}$$

- Funkcja $\langle \cdot, \cdot \rangle : \mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R}$ dana wzorem

$$\langle (x_1, x_2, x_3), (y_1, y_2, y_3) \rangle = x_1 y_1 + 2x_1 y_2 + 2x_2 y_1 + 9x_2 y_2 + 4x_3 y_3$$

jest dwuliniową formą symetryczną, zgodnie z obserwacją wyżej. Warunek dodatniej określoności jest spełniony, bo wyrażenie $\langle (x_1, x_2, x_3), (x_1, x_2, x_3) \rangle$ zapisuje się jako:

$$x_1^2 + 2x_1 x_2 + 2x_2 x_1 + 9x_2^2 + 4x_3^2 = (x_1 + 2x_2)^2 + 5x_2^2 + 4x_3^2.$$

- Funkcja $f : \mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R}$ dana wzorem

$$f((x_1, x_2, x_3), (y_1, y_2, y_3)) = x_1 y_1 + 4x_1 y_2 + 4x_2 y_1 + 5x_2 y_2$$

jest dwuliniowa symetryczna, ale nie jest dodatnio określona, bowiem

$$f((1, -1, 0), (1, -1, 0)) = 1 \cdot 1 + 4 \cdot 1 \cdot (-1) + 4 \cdot (-1) \cdot 1 + 5 \cdot (-1) \cdot (-1) = -2,$$

więc nie jest ona iloczynem skalarnym na \mathbb{R}^3 .

Iloczyny skalarne pełnią fundamentalną rolę w badaniu ważnych klas przestrzeni nieskończonego wymiaru. Ograniczmy się w tym miejscu do podania dwóch przykładów ze skryptu.

- W przestrzeni \mathbb{R}^∞ rozpatrujemy podprzestrzeń l^2 złożoną ze wszystkich ciągów (x_i) takich, że

$$\sum_{i=1}^{\infty} x_i^2 < \infty.$$

Wówczas (i to trzeba udowodnić) funkcja $\langle , \rangle : l^2 \times l^2 \rightarrow \mathbb{R}$ dana wzorem

$$\langle (x_i), (y_i) \rangle = \sum_{i=1}^{\infty} x_i y_i$$

jest iloczynem skalarnym na l^2 .

- Niech $C[a, b]$ oznacza przestrzeń wszystkich funkcji ciągłych określonych na przedziale $[a, b]$ o wartościach w \mathbb{R} . Funkcja $\langle , \rangle : C[a, b] \times C[a, b] \rightarrow \mathbb{R}$ dana wzorem

$$\langle f, g \rangle = \int_a^b f(x)g(x)dx$$

jest iloczynem skalarnym na przestrzeni $C[a, b]$.

Widzimy, że w obydwu przypadkach wprowadzenie iloczynu skalarnego wymaga nietrywialnych definicji i faktów analitycznych (i nie tylko). Stąd też rozważania na temat nieskończone wymiarowe przestrzeni liniowych (m.in.) z iloczynem skalarnym stanowią przedmiot semestralnego wykładu na wyższych latach.

Definicja 10.3: Przestrzeń euklidesowa (liniowa)

Parę (V, \langle , \rangle) gdzie V jest skończenie wymiarową przestrzenią liniową nad \mathbb{R} , zaś \langle , \rangle jest iloczynem skalarnym na V nazywamy PRZESTRZENIĄ EUKLIDESOWĄ LINIOWĄ.

Przejdźmy do zasadniczych pojęć geometrycznych.

Definicja 10.4: Długość/norma wektora

Niech \langle , \rangle będzie iloczynem skalarnym na przestrzeni V . DŁUGOŚCIĄ (albo NORMĄ) wektora $\alpha \in V$ nazywamy liczbę $\|\alpha\| = \sqrt{\langle \alpha, \alpha \rangle}$.

Norma zależy od wyboru iloczynu skalarnego. Wektor $(3, 4)$ ma:

- normę $\sqrt{3^2 + 4^2} = 5$, jeśli \langle , \rangle to standardowy iloczyn skalarny,
- normę $\sqrt{3^2 + (2 \cdot 4)^2} = \sqrt{73}$, jeśli $\langle (x_1, x_2), (y_1, y_2) \rangle = x_1 y_1 + 2 x_2 y_2$.

Nowo zdefiniowana funkcja „zachowuje” się jak znana ze szkoły długość, co wyrażają następujące fakty.

Obserwacja 10.2: Podstawowe własności normy

Niech \langle , \rangle będzie iloczynem skalarnym na przestrzeni V . Wówczas dla każdych $\alpha, \beta \in V$ oraz $a \in \mathbb{R}$ zachodzi:

- $\|\alpha + \beta\|^2 = \|\alpha\|^2 + \|\beta\|^2 + 2 \langle \alpha, \beta \rangle$,
- $\|a \cdot \alpha\| = |a| \cdot \|\alpha\|$,
- $\|\alpha\| = 0 \iff \alpha = 0$.

Twierdzenie 10.1: Uogólnienia nierówności szkolnych

Niech $\langle \cdot, \cdot \rangle$ będzie iloczynem skalarnym na przestrzeni V . Wówczas dla każdych $\alpha, \beta \in V$ zachodzi:

- (1) nierówność Schwarz'a: $|\langle \alpha, \beta \rangle| \leq \|\alpha\| \cdot \|\beta\|$,
- (2) nierówność trójkąta: $\|\alpha + \beta\| \leq \|\alpha\| + \|\beta\|$,
- (3) twierdzenie Pitagorasa: $\langle \alpha, \beta \rangle = 0 \implies \|\alpha\|^2 + \|\beta\|^2 = \|\alpha + \beta\|^2$.

Dowód. Dowód (1). Jeśli $\alpha = 0$, to obie strony nierówności są zerami. W przypadku, gdy $\alpha \neq 0$ rozważamy funkcję $f: \mathbb{R} \rightarrow \mathbb{R}$ zadaną wzorem $f(t) = \|t\alpha + \beta\|^2$. Zatem

$$\begin{aligned} f(t) &= \langle t\alpha + \beta, t\alpha + \beta \rangle = \\ &= t \langle \alpha, t\alpha + \beta \rangle + \langle \beta, t\alpha + \beta \rangle = \\ &= t^2 \langle \alpha, \alpha \rangle + t \langle \alpha, \beta \rangle + t \langle \beta, \alpha \rangle + \langle \beta, \beta \rangle = \\ &= t^2 \|\alpha\|^2 + 2t \langle \alpha, \beta \rangle + \|\beta\|^2. \end{aligned}$$

Na mocy dodatniej określoności iloczynu skalarnego dla każdego $t \in \mathbb{R}$ mamy $f(t) \geq 0$, a zatem wyróżnik trójkątnianu kwadratowego

$$t^2 \|\alpha\|^2 + 2 \langle \alpha, \beta \rangle t + \|\beta\|^2$$

musi być niedodatni, tj. $\Delta \leq 0$, gdzie

$$\Delta = (2 \langle \alpha, \beta \rangle)^2 - 4 \|\alpha\|^2 \|\beta\|^2 = 4 \langle \alpha, \beta \rangle^2 - 4 \|\alpha\|^2 \|\beta\|^2.$$

Stąd wynika (1). Do dowodu (2) i (3) wykorzystujemy przydatną w rachunkach tożsamość, wypisaną wcześniej w Obserwacji 10.2 $\|\alpha + \beta\|^2 = \|\alpha\|^2 + 2 \langle \alpha, \beta \rangle + \|\beta\|^2$, którą wyprowadza się jak powyżej. Wówczas na mocy (1) mamy:

$$\|\alpha + \beta\|^2 \leq \|\alpha\|^2 + 2\|\alpha\| \cdot \|\beta\| + \|\beta\|^2 = (\|\alpha\| + \|\beta\|)^2.$$

□

Gorąco zachęcam Czytelnika do przeanalizowania kiedy w nierównościach wyżej zachodzą równości. Wymaga to chwili namysłu i jest istotnym ćwiczeniem na analizę dowodu wyżej.

Z nierówności Schwarz'a wynika natychmiast, że dla każdej pary niezerowych wektorów $\alpha, \beta \in V$ mamy:

$$-1 \leq \frac{\langle \alpha, \beta \rangle}{\|\alpha\| \cdot \|\beta\|} \leq 1.$$

Dla każdej liczby rzeczywistej $r \in [-1, 1]$ istnieje dokładnie jedna liczba $\theta \in [0, \pi]$, że $\cos \theta = r$.

Definicja 10.5: Kąt między wektorami

Niech $\langle \cdot, \cdot \rangle$ będzie iloczynem skalarnym na przestrzeni V . Niech α, β będą niezerowymi wektorami przestrzeni V . Liczbę $\theta \in [0, \pi]$ taką, że

$$\frac{\langle \alpha, \beta \rangle}{\|\alpha\| \cdot \|\beta\|} = \cos \theta$$

nazywamy (niezorientowanym) KĄTEM MIĘDZY WEKTORAMI α i β .

Przykład. Wyznacz kosinus kąta θ pomiędzy wektorami $\alpha = (2, 1, -4)$ oraz $\beta = (1, -1, 3)$ w przestrzeni $(\mathbb{R}^3, \langle \cdot, \cdot \rangle)$, gdzie $\langle \cdot, \cdot \rangle$ jest iloczynem skalarnym postaci $h((x_1, x_2, x_3), (y_1, y_2, y_3)) = x_1 y_1 + 2x_2 y_2 + 3x_3 y_3$.

ROZWIĄZANIE. Szukany kosinus równy jest $-\frac{2}{\sqrt{5}}$. Wyznaczamy go z zależności $\|\alpha\| \cdot \|\beta\| \cdot \cos \theta = \langle \alpha, \beta \rangle$. Mamy $\|\alpha\| = \sqrt{1 \cdot 2^2 + 2 \cdot 1^2 + 3 \cdot (-4)^2} = \sqrt{54}$ oraz $\|\beta\| = \sqrt{1 \cdot 1^2 + 2 \cdot (-1)^2 + 3 \cdot 3^2} = \sqrt{30}$, a także $\langle \alpha, \beta \rangle = 2 \cdot 1 + 2 \cdot 1 \cdot (-1) + 3 \cdot (-4) \cdot 3 = -36$. Stąd

$$\cos \theta = \frac{-36}{\sqrt{30} \cdot \sqrt{54}} = -\frac{2}{\sqrt{5}}.$$

10.1 Zadania do samodzielnej pracy

Zadania ilustrujące umiejętności niezbędne do zaliczenia przedmiotu oznaczone są symbolem ♠. Przy tych zadaniach dodany jest opis umiejętności, które sprawdzają.

1. Czy dana funkcja jest iloczynem skalarnym?
 - $f : \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}$, gdzie $f((x_1, x_2), (y_1, y_2)) = |x_1 y_1| + |x_2 y_2|$,
 - $g : \mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R}$, gdzie $g((x_1, x_2, x_3), (y_1, y_2, y_3)) = x_1 y_1 + x_3 y_3$.
2. (♠ Podstawowe rachunki w przestrzeni euklidesowej) W przestrzeni \mathbb{R}^3 ze standardowym iloczynem skalarnym rozpatrujemy wektory $\alpha = (-1, 2, 2)$, $\gamma_t = (2, 1, t)$. Dla jakich wartości parametru t kąt między wektorami α i γ_t wynosi $2\pi/3$?
3. (♠ Podstawowe rachunki w przestrzeni euklidesowej) O wektorach występujących w poniższych zadaniach zakładamy, że należą do rzeczywistej przestrzeni liniowej z iloczynem skalarnym $\langle \cdot, \cdot \rangle$
 - Załóżmy, że $\langle u, v \rangle = -1$ oraz $\|u\| = 2$. Oblicz $\langle u + v, 2u \rangle$ oraz $\langle 4u, 3u - 2v \rangle$.
 - Wektory v, w spełniają warunek $\langle v, w \rangle = 0$ i mają normy równe 1. Wyznacz $\|x - y\| + \|x + y\|$.
 - Niech $\|u\| = 3$, $\|v + w\| = 4$ oraz $\|u - v\| = 6$. Oblicz $\|v\|$.
 - Załóżmy $\|v\| = 1$, $\|w\| = 2$, przy czym kąt między wektorami v i w wynosi $\frac{\pi}{3}$. Oblicz $\|v - 2w\|$.
 - Wiedząc, że $\|u + v\| = 3$, $\|u - v\| = 2$, $\cos \angle(u, v) = \frac{1}{2}$, oblicz $\|u\| + \|v\|$ oraz $\|u\| \cdot \|v\|$.
 - Uzasadnij, że jeśli wektory u oraz v mają równe normy, to $\langle u + v, u - v \rangle = 0$.
 - Niech $\|u\| = \|v\| = 1$ oraz $\langle u, v \rangle = 1$. Wykaż, że $u = v$.

4. Uzasadnij, że następujące warunki są równoważne dla $u, v \in (V, \langle \cdot, \cdot \rangle)$:

$$(a) \|u\| + \|v\| = \|u + v\| \quad (b) |\langle u, v \rangle| = \|u\| \cdot \|v\|, \quad (c) u \in \text{lin}(v) \text{ lub } v \in \text{lin}(u).$$

5. Niech $(V, \langle \cdot, \cdot \rangle)$ oraz niech $u, v \in V$. Wykaż, że równoważne są warunki:

$$(a) \|u\| = \|v\|, \quad (b) \|au + bv\| = \|bu + av\|, \text{ dla } \text{każdych } a, b \in \mathbb{R}.$$

6. (Korzystanie z dodatniej określoności, nierówności trójkąta i nierówności Schwarz'a)

- Niech $S = \{\langle u, v \rangle + \langle v, w \rangle + \langle w, u \rangle \mid u, v, w \in \mathbb{R}^2, \text{ gdzie } \|u\| = \|v\| = \|w\| = 1\} \subset \mathbb{R}$. Wyznacz najmniejszy i największy element zbioru S .
- Niech α, β będą liniowo niezależnymi wektorami w przestrzeni euklidesowej $(V, \langle \cdot, \cdot \rangle)$ takimi, że $\|\alpha\| = \|\beta\| = 1$. Pokaż, że dla każdego $t \in (0, 1)$ zachodzi nierówność $\|(1-t)\alpha + t\beta\| < 1$.
- Wykaż, że $\langle u, v \rangle = 0$ wtedy i tylko wtedy, gdy $\|u\| \leq \|u + av\|$, dla każdego $a \in \mathbb{R}$.
- Niech $\|u\| \leq 1$ oraz $\|v\| \leq 1$. Wykaż, że

$$\sqrt{1 - \|u\|^2} \sqrt{1 - \|v\|^2} \leq 1 - |\langle u, v \rangle|.$$

- Wektory u, v, z mają normę 1 i $\langle u, v \rangle = a$ oraz $\langle v, z \rangle = b$. Wykaż, że

$$\langle z, u \rangle \geq ab - \sqrt{1 - a^2} \sqrt{1 - b^2}.$$

- Załóżmy, że wektory $v_1, v_2, v_3, v_4 \in \mathbb{R}^4$ spełniają $\langle v_i, v_j \rangle < 0$ dla $i \neq j$. Udowodnij, że pewne trzy spośród nich są liniowo niezależne.

7. Wykaż, że w przestrzeni liniowej z iloczynem skalarnym zachodzi tożsamość równoległoboku:

$$\|u + v\|^2 + \|u - v\|^2 = 2(\|u\|^2 + \|v\|^2).$$

Czy istnieje iloczyn skalarny na \mathbb{R}^2 , w którym norma ma postać $\|(x, y)\| = \max\{|x|, |y|\}$?

8. Dana jest przestrzeń euklidesowa $(\mathbb{R}^n, \langle \cdot, \cdot \rangle)$ oraz $\phi \in \text{End}(\mathbb{R}^n)$. Wykaż, że funkcja $f : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$ dana wzorem $f(v, w) = \langle \phi(v), \phi(w) \rangle$ jest iloczynem skalarnym wtedy i tylko wtedy, gdy $\ker \phi = 0$.
9. Na przestrzeni $V = M_n(\mathbb{R})$ definiujemy funkcjonal dwuliniowy $\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{R}$ dany wzorem:

$$\langle A, B \rangle = \text{tr}(B^T A).$$

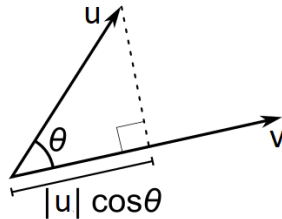
- (a) Udowodnij, że $\langle \cdot, \cdot \rangle$ jest iloczynem skalarnym.
- (b) Niech $(\mathbb{R}^n, \langle \cdot, \cdot \rangle_{st})$ będzie przestrzenią euklidesową ze standardowym iloczynem skalarnym. Wykaż, że dla dowolnych $A \in M_n(\mathbb{R})$ oraz $v \in \mathbb{R}^n$ zachodzi nierówność $\|Av\| \leq \|A\| \cdot \|v\|$.
- (c) Wykaż, że dla każdej rzeczywistej wartości własnej λ macierzy A zachodzi $|\lambda| \leq \|A\|$.

10.2 Uzupełnienie. Dlaczego cosinus?

Powiedzieliśmy, że liczbę $\theta \in [0, \pi]$ taką, że

$$\frac{\langle u, v \rangle}{\|u\| \cdot \|v\|} = \cos \theta$$

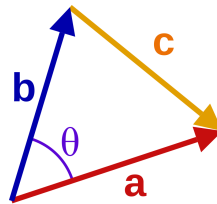
nazywamy (niezorientowanym) kątem między wektorami u i v . Czy taka definicja ma coś wspólnego z geometrią i tym, co znamy jako cosinus? Na poziomie intuicji dać można następującą odpowiedź: jeśli chcielibyśmy pomnożyć dwa wektory poprzez mnożenie ich długości, wypadaloby aby wektory te miały ten sam zwrot. Rozważmy następujący rysunek



Zauważmy, że z definicji kąta wynika równość $\langle u, v \rangle = \|u\| \cdot \|v\| \cdot \cos \theta$, a liczba $\|u\| \cdot |\cos \theta|$ równa jest długości rzutu prostopadłego wektora u na podprzestrzeń $\text{lin}(v)$. O prostopadłości powiemy więcej na następnym wykładzie (a o rzutach — za dwa wykłady). Jednak już teraz możemy powiedzieć, że jeśli u_v jest długością rzutu wektora u na $\text{lin}(v)$ oraz v_u jest długością rzutu v na $\text{lin}(u)$, to zachodzi równość:

$$|\langle u, v \rangle| = u_v \cdot \|v\| = v_u \cdot \|u\|.$$

Bardzo nas ta równość nie dziwi, bowiem $\sqrt{\|u\|^2 - u_v^2} \cdot \|v\| = \sqrt{\|v\|^2 - v_u^2} \cdot \|u\|$ równe jest polu równoległoboku rozpiętego przez wektory u, v (wysokość razy podstawa). Z geometrycznego punktu widzenia równość wyżej może być traktowana jako definicja iloczynu skalarnego, o ile wiemy czym jest kosinus (lub pole). Rozważmy kolejny rysunek



Zauważmy, że posługując się wprowadzoną definicją kąta możemy wykazać twierdzenie cosinusów. Istotnie, dla trójkąta wyżej, wyznaczonego przez kierunki a, b oraz $c = a - b$ mamy:

$$\|c\|^2 = \langle c, c \rangle = \langle a - b, a - b \rangle = \|a\|^2 - 2\langle a, b \rangle + \|b\|^2 = \|a\|^2 + \|b\|^2 - 2\|a\| \cdot \|b\| \cdot \cos \theta.$$

Jaki ma to związek ze współrzędnymi i definicjami iloczynu skalarnego za pomocą różnych form dwuliniowych? Zobaczmy to zagadnienie w \mathbb{R}^3 ze standardowym iloczynem skalarnym. Jeśli $a = (x_1, y_1, z_1)$ oraz $b = (x_2, y_2, z_2)$, to $a - b = (x_1 - x_2, y_1 - y_2, z_1 - z_2)$. Stąd (przyjmując standardową normę) mamy:

$$\|c\| = \|a - b\| = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2 + (z_1 - z_2)^2}.$$

Jeżeli wystartujemy od twierdzenia cosinusów zapisanego w postaci następujących równości $2\langle a, b \rangle = 2\|a\| \cdot \|b\| \cdot \cos \theta = \|a\|^2 + \|b\|^2 - \|c\|^2$, to otrzymamy:

$$\begin{aligned} 2\langle a, b \rangle &= 2\|a\| \cdot \|b\| \cdot \cos \theta = (x_1^2 + y_1^2 + z_1^2) + (x_2^2 + y_2^2 + z_2^2) - ((x_1 - x_2)^2 + (y_1 - y_2)^2 + (z_1 - z_2)^2) = \\ &= 2(x_1x_2 + y_1y_2 + z_1z_2). \end{aligned}$$

A zatem $\langle a, b \rangle = x_1x_2 + y_1y_2 + z_1z_2$. Widzimy więc ponownie — można określać kąt (i za chwilę również pole) za pomocą iloczynu skalarnego i to jest podejście ważne z punktu widzenia naszego kursu. Ze szkolnego punktu widzenia można określić iloczyn skalarny za pomocą podstawowych narzędzi geometrii elementarnej, dowodząc wcześniej twierdzenie cosinusów — odsyłam do tekstu dra Krycha wspomnianego w zasadniczym tekście wykładu. Wiadomo jest jednak, że szkolne definicje kąta czy funkcji trygonometrycznej mają w sobie pewne przemilczenia (np. czym dokładnie jest *miara łukowa* czy *pole*). Stąd nasz „kierunek definicji” jest w pewnym sensie odwrotny do „szkolnego”. W naszym ujęciu startujemy od abstrakcji (aksjomaty) i idziemy do intuicyjnie znanych obiektów: najpierw wektory i przestrzenie liniowe, potem punkty i przestrzenie afiniczne: proste, płaszczyzny itd., dalej abstrakcyjny iloczyn skalarny, a z nim: kąty, odległości, pole, a jeszcze dalej: odcinki, trójkąty, okręgi, parabole, hiperbole itd.

10.3 Dodatek. Iloczyn skalarny i funkcjonały

Na wykładzie wspomnieliśmy o związkach pomiędzy iloczynem skalarnym na przestrzeni liniowej oraz o przestrzeni sprzężonej. Rozwińmy nieco ten wątek.

Obserwacja 10.3: Twierdzenie Riesz'a o reprezentacji

Niech $(V, \langle \cdot, \cdot \rangle)$ będzie liniową przestrzenią euklidesową wymiaru n . Każdemu wektorowi $v \in V$ przyporządkujemy funkcjonal $f_v \in V^*$ określony wzorem:

$$f_v(u) = \langle u, v \rangle, \text{ gdzie } u \in V.$$

Przyporządkowanie $\Phi : V \rightarrow V^*$ zadane wzorem $\Phi(v) = f_v$ jest izomorfizmem przestrzeni liniowych. Jeśli $\mathcal{V} = (v_1, \dots, v_n)$ jest bazą ortonormalną w V , to układ $(f_{v_1}, \dots, f_{v_n})$ jest bazą dualną do \mathcal{V} .

Dowód. Przekształcenie f_v jest oczywiście liniowe dla każdego $v \in V$, bo $f_v(au) = \langle au, v \rangle = a \langle u, v \rangle = a \cdot f_v(u)$ oraz $f_v(u_1 + u_2) = \langle u_1 + u_2, v \rangle = \langle u_1, v \rangle + \langle u_2, v \rangle = f_v(u_1) + f_v(u_2)$. A zatem rzeczywiście $f_v \in V^*$. Także przyporządkowanie Φ jest liniowe, ponieważ $f_{av}(u) = \langle u, av \rangle = a \langle u, v \rangle = a \cdot f_v(u)$, czyli funkcjonały $\Phi(av)$ oraz $a \cdot \Phi(v)$ są identyczne na V . Także $f_{v_1+v_2}(u) = \langle u, v_1 + v_2 \rangle = \langle u, v_1 \rangle + \langle u, v_2 \rangle = f_{v_1}(u) + f_{v_2}(u)$, czyli funkcjonały $\Phi(v_1 + v_2)$ oraz $\Phi(v_1) + \Phi(v_2)$ są równe. Skoro V oraz V^* są tego samego wymiaru to do wykazania, że Φ jest izomorfizmem wystarczy pokazać, że Φ to monomorfizm. Jeśli mamy $\Phi(v) = 0$, to f_v jest tożsamościowo równe 0. W szczególności $f_v(v) = \langle v, v \rangle = \|v\|^2 = 0$. Zatem $v = 0$. Czyli Φ jest izomorfizmem. Ostatnie stwierdzenie dotyczące baz dualnych jest oczywiste (z definicji). \square

Niech V będzie przestrzenią liniową skończonego wymiaru oraz V^* niech będzie przestrzenią dualną do V . Wiemy, że przestrzenie V oraz V^* są tego samego wymiaru, a więc istnieje między nimi izomorfizm. Żaden izomorfizm nie jest jednak wyróżniony lub „naturalny”. Dlaczego? Można wprawdzie wybrać bazę w V oraz bazę w V^* i zażądać przekształcenia liniowego $i : V \rightarrow V^*$, które przeprowadza jedną bazę w drugą. Jest jednak pewien problem. Załóżmy, że mamy dwie skończone wymiarowe przestrzenie liniowe V_1 oraz V_2 oraz przekształcenie liniowe $\lambda : V_1 \rightarrow V_2$. Wiemy, że indukuje ono przekształcenie liniowe $\lambda^* : V_2^* \rightarrow V_1^*$. Chciałoby się uważać, że skoro V i V^* są izomorficzne, to istnieje jakiś naturalny sposób przechodzenia z endomorfizmów V do endomorfizmów V^* . Okazuje się, że nie musi istnieć izomorfizm $i : V \rightarrow V^*$ taki, że dla każdego odwracalnego λ spełniona jest równość:

$$\begin{array}{ccc} V & \xrightarrow{i} & V^* \\ \lambda \downarrow & & \lambda^* \uparrow \\ V & \xrightarrow{i} & V^* \end{array}$$

Oczywiście jeśli wybierzemy pewien izomorfizm $V \rightarrow V^*$ w dolnym wierszu tego diagramu, to można określić i górny, znając λ . Ale nie dobierzemy JEDNEGO izomorfizmu i do WSZYSTKICH λ . Pokazanie tego to stosunkowo trudne ćwiczenie z niesymetrycznych form dwuliniowych¹. Inaczej mają się sprawy, gdy V jest przestrzenią euklidesową, czyli jest parą $(V, \langle \cdot, \cdot \rangle)$. Wówczas, jak można pokazać, każdemu endomorfizmowi $\lambda : V \rightarrow V$ odpowiada jednoznacznie endomorfizm sprzężony $\lambda' : V \rightarrow V$ taki, że

$$\langle \lambda(v), w \rangle = \langle v, \lambda'(w) \rangle.$$

Dzięki niemu mamy naturalną odpowiedniość między $End(V)$ i $End(V^*)$:

$$\begin{array}{ccc} V & \xrightarrow{i} & V^* \\ \uparrow \lambda' & & \lambda^* \uparrow \\ V & \xrightarrow{i} & V^* \end{array}$$

Rzeczywiście, dzięki izomorfizmowi Φ możemy o każdym funkcjonałe z V^* myśleć jako o pewnym f_v (dla pewnego wektora v). A zatem: bierzemy taki funkcjonal f_v , wykonujemy na nim ϕ^* i dostajemy znowu funkcjonal z V^* , czyli pewien funkcjonal $f_{v'}$ (bo tak nakazuje Φ). Co mają ze sobą wspólnego v oraz v' ? Musimy mieć $\phi^*(f_v) = f_{v'}$, czyli dla każdego $u \in V$ mamy $\phi^*(f_v)(u) = f_v(\phi(u)) = f_{v'}(u)$. A zatem z definicji funkcjonałów f_v oraz $f_{v'}$ mamy $\langle \phi(u), v \rangle = \langle u, v' \rangle$.

¹<https://www.ams.org/journals/tran/1945-058-00/S0002-9947-1945-0013131-6/S0002-9947-1945-0013131-6.pdf>, str. 4.

10.4 Trivia. Zastosowania nierówności Cauchy-ego Schwarza

Nierówność Cauchy'ego Schwarza ma liczne zastosowania algebraiczne, w tym konkursowe. Wykorzystuje się zwłaszcza wersję dla pary wektorów w przestrzeni \mathbb{R}^n ze standardowym iloczynem skalarnym.

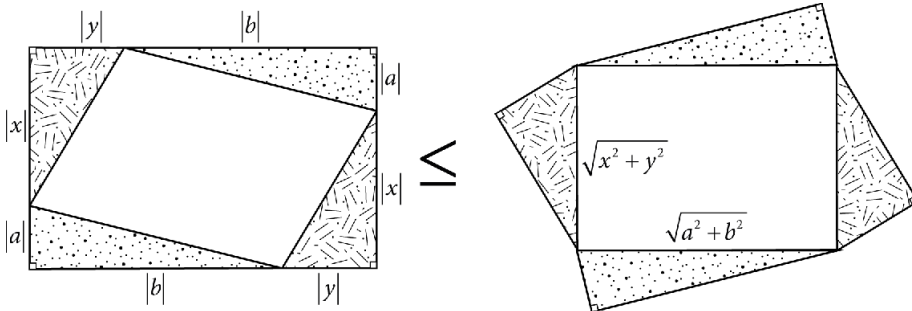
Obserwacja 10.4

Dla dowolnych liczb rzeczywistych a_1, \dots, a_n oraz b_1, \dots, b_n mamy:

$$(a_1 b_1 + \dots + a_n b_n)^2 \leq (a_1^2 + \dots + a_n^2)(b_1^2 + \dots + b_n^2),$$

przy czym równość zachodzi wtedy i tylko wtedy, gdy istnieje $\lambda \in \mathbb{R}$ taka, że $a_i = \lambda b_i$, dla wszystkich i lub $b_i = \lambda a_i$, dla wszystkich i .

Poniższy rysunek ilustruje możliwą geometryczną interpretację nierówności powyżej na płaszczyźnie (po spierwiastkowaniu obydwu stron).



Źródło. Proofs without words, R. Nielsen.

Bezpośrednim zastosowaniem powyższej nierówności jest dla $a_i = \sqrt{x_i}$ oraz $b_i = 1/\sqrt{x_i}$, gdzie $x_i \geq 0$, nierówność między średnią arytmetyczną i harmoniczną (a raczej jej równoważna forma).

$$(x_1 + \dots + x_n) \left(\frac{1}{x_1} + \dots + \frac{1}{x_n} \right) \geq n^2.$$

Biorąc $b_i = 1$ uzyskujemy nierówność między średnią kwadratową i arytmetyczną

$$\sqrt{\frac{a_1^2 + \dots + a_n^2}{n}} \geq \frac{a_1 + \dots + a_n}{n}.$$

Jeszcze innym zastosowaniem jest nierówność Minkowskiego (to w zasadzie nierówność trójkąta):

$$\sqrt{x_1^2 + \dots + x_n^2} + \sqrt{y_1^2 + \dots + y_n^2} \geq \sqrt{(x_1 + y_1)^2 + \dots + (x_n + y_n)^2}.$$

Oto przykład z I etapu LXXIV OM. Pokazać, że dla dowolnych liczb dodatnich a, b, c mamy:

$$\sqrt{ab^2(b+c)} + \sqrt{bc^2(c+a)} + \sqrt{ca^2(a+b)} \leq \frac{1}{2} \sqrt{(a+b+c)^4 - (a^2 + b^2 + c^2)^2}.$$

Przyjmijmy $x_1 = \sqrt{ab}$, $x_2 = \sqrt{bc}$, $x_3 = \sqrt{ca}$ oraz

$$y_1 = \sqrt{b(b+c)}, \quad y_2 = \sqrt{c(c+a)}, \quad y_3 = \sqrt{a(a+b)}.$$

Wówczas teza wynika natychmiast z nierówności Cauchy'ego-Schwarza, bowiem:

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 &= ab + bc + ca \\ y_1^2 + y_2^2 + y_3^2 &= a^2 + b^2 + c^2 + ab + bc + ca \\ x_1 y_1 + x_2 y_2 + x_3 y_3 &= \sqrt{ab^2(b+c)} + \sqrt{bc^2(c+a)} + \sqrt{ca^2(a+b)} \end{aligned}$$

Z drugiej strony korzystając ze wzorów skróconego mnożenia (wzór na różnicę kwadratów) mamy:

$$(a+b+c)^4 - (a^2 + b^2 + c^2)^2 = 4(a^2 + b^2 + c^2 + ab + bc + ca)(ab + bc + ca).$$

Zachęcam Czytelnika do poszukania ciekawych wniosków z nierówności Cauchy'ego Schwarza dla niestandardowych iloczynów skalarnych na \mathbb{R}^n oraz dla innych przestrzeni euklidesowych.

Rozdział 11

Prostopadłość

Badanie form dwuliniowych na przestrzeniach liniowych jest ciekawe, ponieważ wśród układów liniowo niezależnych szczególnie miejsce mają układy wektorów, które nazwiemy prostopadłymi lub ortogonalnymi. Bazy złożone z takich układów są kluczem do całej dalszej teorii. Samo pojęcie prostopadłości jest centralnym motywem całej matematyki, który odkrywać będziecie Państwo w rozmaitych kontekstach.

Definicja 11.1: Wektory prostopadłe, dopełnienie ortogonalne podzbioru

Niech h będzie formą dwuliniową na przestrzeni liniowej V .

1. Mówimy, że wektory $\alpha, \beta \in V$ są PROSTOPADŁE, ozn. $\alpha \perp \beta$, jeśli

$$h(\alpha, \beta) = 0.$$

2. Dla podzbioru $X \subseteq V$ definiujemy jego DOPEŁNIENIE ORTOGONALNE

$$X^\perp = \{\alpha \in V : \alpha \perp \beta, \text{ dla każdego } \beta \in X\}.$$

Powyższa definicja obejmuje oczywiście także iloczyny skalarne, określone na przestrzeniach rzeczywistych. Różnym formom dwuliniowym na tej samej przestrzeni liniowej V odpowiadają różne pojęcia prostopadłości. Wektory bazy standardowej

$$(1, 0, 0), (0, 1, 0)$$

są prostopadłe przy standardowym iloczynie skalarnym na przestrzeni \mathbb{R}^3 , ale $\langle (1, 0, 0), (0, 1, 0) \rangle = 2$, jeśli iloczyn skalarnym \langle, \rangle jest określony na tej samej przestrzeni \mathbb{R}^3 wzorem

$$\langle (x_1, x_2, x_3), (y_1, y_2, y_3) \rangle = x_1y_1 + 2x_1y_2 + 2x_2y_1 + 9x_2y_2 + 4x_3y_3.$$

Obserwacja 11.1

Dla każdego podzbioru $X \subseteq V$ zbiór X^\perp jest podprzestrzenią V .

Dowód. Dla dowolnych $a, b \in \mathbb{R}$, $\alpha, \beta \in X^\perp$ oraz dla dowolnego $x \in X$ mamy:

$$\langle x, a\alpha + b\beta \rangle = a\langle x, \alpha \rangle + b\langle x, \beta \rangle = 0.$$

□

Odnotujmy też, że wyznaczanie podprzestrzeni X^\perp ma wiele wspólnego z rozwiązywaniem układów równań liniowych. Jeśli na przykład $X = \{(1, 1, 2), (1, 2, 0)\}$ i szukamy w \mathbb{R}^3 zbioru X^\perp przy standardowym iloczynie skalarnym, to każdy wektor (x_1, x_2, x_3) należący do tego zbioru spełniać musi układ równań:

$$\begin{cases} \langle (x_1, x_2, x_3), (1, 1, 2) \rangle = 0 \\ \langle (x_1, x_2, x_3), (1, 2, 0) \rangle = 0 \end{cases} \iff \begin{cases} x_1 + x_2 + 2x_3 = 0 \\ x_2 + 2x_2 = 0 \end{cases}$$

Definicja 11.2: Układ prostopadły, baza ortogonalna

Niech h będzie formą dwuliniową na przestrzeni liniowej V .

1. Układ wektorów $X \subseteq V$ nazwiemy PROSTOPADŁYM (albo ORTOGONALNYM), jeśli $\alpha \perp \beta$, dla każdych $\alpha, \beta \in X$.
2. Układ prostopadły będący bazą przestrzeni V nazywamy BAZĄ PROSTOPADŁĄ (albo ortogonalną) przestrzeni V względem h .

Zobaczmy kilka przykładów.

- Jeśli $\langle \cdot, \cdot \rangle_{st}$ jest standardowym iloczynem skalarnym na przestrzeni \mathbb{R}^n , to baza standardowa tej przestrzeni jest bazą prostopadłą.
- Układ $(1, 1, 2), (2, 2, -2), (1, -1, 0)$ jest bazą prostopadłą przestrzeni \mathbb{R}^3 ze standardowym iloczynem skalarnym.
- Jeśli $\langle \cdot, \cdot \rangle$ jest iloczynem skalarnym na przestrzeni V oraz $W \subseteq V$ jest podprzestrzenią, to ograniczenie $\langle \cdot, \cdot \rangle|_W : W \times W \rightarrow \mathbb{R}$ dane wzorem $\langle w_1, w_2 \rangle|_W = \langle w_1, w_2 \rangle$ jest iloczynem skalarnym na W .

Niech $V = \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1 + 2x_2 - 2x_3 = 0\}$. Na przestrzeni V rozważyć możemy ograniczenie standardowego iloczynu skalarnego z przestrzeni \mathbb{R}^3 . Wówczas układ $(0, 1, 1), (4, -1, 1)$ jest bazą prostopadłą przestrzeni $(V, \langle \cdot, \cdot \rangle|_V)$.

- Funkcja $\langle (x_1, x_2, x_3), (y_1, y_2, y_3) \rangle = x_1y_1 + 2x_1y_2 + 2x_2y_1 + 9x_2y_2 + 4x_3y_3$ jest, jak już wiemy, iloczynem skalarnym na \mathbb{R}^3 . Układ $(1, 0, 0), (2, -1, 0), (0, 0, 1)$ jest bazą prostopadłą przestrzeni \mathbb{R}^3 z tym iloczynem skalarnym.
- Warunek dodatniej określoności iloczynu skalarnego wymusza, aby w przestrzeni z iloczynem skalarnym niezerowy wektor nie był prostopadły do siebie samego. Dla dowolnej formy dwuliniowej jest to jednak możliwe. Na przykład: dla formy $h : \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}$ zadanej wzorem

$$h((x_1, x_2), (y_1, y_2)) = x_1y_2 + x_2y_1$$

mamy $(1, 0) \perp (1, 0)$ oraz $(0, 1) \perp (0, 1)$. To rodzi następujące pytanie: czy w przestrzeni (\mathbb{R}^2, h) istnieje baza ortogonalna? Okazuje się, że tak — wystarczy obrać układ $((1, 1), (1, -1))$.

Układy i bazy prostopadłe można teoretycznie rozważać zarówno w przestrzeniach skończonego, jak i nieskończonego wymiaru, ale tylko pierwsza z możliwości daje istotne dla nas wyniki. W przestrzeniach nieskończonego wymiaru problem istnienia bazy ortogonalnej nie jest taki prosty, jak się wydaje¹.

Rozważmy podprzestrzeń $X \subseteq \mathbb{R}^\infty$ złożoną z ciągów ograniczonych (a_1, a_2, \dots) z iloczynem skalarnym $\langle \cdot, \cdot \rangle$ danym wzorem:

$$\langle (a_n), (b_n) \rangle = \sum_{n=1}^{\infty} \frac{a_n b_n}{n^2}.$$

Niech U będzie podprzestrzenią X złożoną z ciągów o skończonej liczbie niezerowych wyrazów. Wówczas ciągi $(\epsilon_i)_n$ dane wzorami

$$(\epsilon_i)_n = \begin{cases} n, & n = i \\ 0, & n \neq i \end{cases}$$

tworzą bazę ortogonalną U . Jednak $U^\perp = \{0\}$ (sprawdź!) To pokazuje, że układ $\{\epsilon_i\}_{i \in \mathbb{N}}$ jest maksymalnym układem ortogonalnym² w X , ale nie jest bazą X . Okazuje się, że X takiej bazy nie ma!

¹W analizie funkcjonalnej wprowadza się pojęcie bazy ortogonalnej, ale nie jest to *zwykle* baza w sensie algebry liniowej.

²Dostaliśmy przykład tzw. **zupełnego układu wektorów** w przestrzeni V nad \mathbb{R} , który nie jest bazą w sensie algebry liniowej, tzn. układu wektorów $(\alpha_1, \alpha_2, \dots)$ takiego, że dla każdego $\beta \in V$ zachodzi

$$\forall i \in \mathbb{N} \langle \beta, \alpha_i \rangle = 0 \Rightarrow \beta = 0.$$

W dalszym ciągu zajmujemy się jedynie przestrzeniami euklidesowymi. Do rozważań dotyczących przestrzeni z dowolną formą dwuliniową wrócimy za kilka wykładów. Zaczniemy od obserwacji wskazującej na to, że układy ortogonalne niezerowych wektorów w przestrzeni euklidesowej są liniowo niezależne.

Obserwacja 11.2

Niech $X \subseteq V$ będzie prostopadłym układem niezerowych wektorów przestrzeni V z iloczynem skalarnym $\langle \cdot, \cdot \rangle$. Wówczas układ X jest liniowo niezależny.

Dowód. Weźmy dowolny skończony podukład X , np. $\{\alpha_1, \dots, \alpha_n\}$. Wystarczy pokazać, że jest on liniowo niezależny. Przypuśćmy, że $\sum_{i=1}^n a_i \alpha_i = 0$, dla pewnych a_1, \dots, a_n . Wówczas dla każdego j :

$$0 = \langle 0, \alpha_j \rangle = \left\langle \sum_{i=1}^n a_i \alpha_i, \alpha_j \right\rangle = \sum_{i=1}^n a_i \langle \alpha_i, \alpha_j \rangle = a_j \langle \alpha_j, \alpha_j \rangle,$$

bo $\langle \alpha_i, \alpha_j \rangle = 0$, dla $i \neq j$. Wobec $\langle \alpha_j, \alpha_j \rangle > 0$ dostajemy $a_j = 0$, dla każdego $j = 1, \dots, n$. \square

Obserwacja 11.3

Każda przestrzeń euklidesowa ma bazę prostopadłą.

Dowód. Stosujemy indukcję ze względu na wymiar przestrzeni liniowej. Dla przestrzeni wymiaru 1 twierdzenie jest oczywiste, bo każdy jej niezerowy wektor stanowi bazę prostopadłą.

Założmy, że wykazaliśmy twierdzenie dla przestrzeni wymiaru mniejszego od n . Niech $(V, \langle \cdot, \cdot \rangle)$ będzie n -wymiarową przestrzenią euklidesową. Wybierzmy dowolny niezerowy wektor $\alpha \in V$. Pokażemy najpierw, że zachodzi rozkład:

$$V = \text{lin}(\alpha) \oplus \text{lin}(\alpha)^\perp.$$

W tym celu trzeba uzasadnić kolejno równości $\text{lin}(\alpha) \cap \text{lin}(\alpha)^\perp = \{0\}$ oraz $\text{lin}(\alpha) + \text{lin}(\alpha)^\perp = V$.

Założmy zatem, że jakiś niezerowy wektor v należy zarówno do $\text{lin}(\alpha)$ jak i do podprzestrzeni $\text{lin}(\alpha)^\perp$ ortogonalnej do $\text{lin}(\alpha)$. Zatem $v = a\alpha$, dla pewnego $0 \neq a \in \mathbb{R}$. Skoro wektor $a\alpha$ należy także do $\text{lin}(\alpha)^\perp$ to $\langle a\alpha, \alpha \rangle = 0$. Wobec tego, że $\langle a\alpha, \alpha \rangle = a \langle \alpha, \alpha \rangle$ oraz, że $\langle \alpha, \alpha \rangle > 0$, dla każdego $0 \neq \alpha$, dostajemy sprzeczność z wyborem a , bo iloczyn dwóch niezerowych z założenia wartości $a \langle \alpha, \alpha \rangle$ daje zero. Pokazaliśmy zatem, że żaden niezerowy wektor nie może należeć do $\text{lin}(\alpha) \cap \text{lin}(\alpha)^\perp$.

Aby pokazać równość $\text{lin}(\alpha) + \text{lin}(\alpha)^\perp = V$ musimy rozłożyć dowolny wektor $\beta \in V$ na sumę wektorów, z których pierwszy należy do $\text{lin}(\alpha)$, a drugi do $\text{lin}(\alpha)^\perp$. Oto ten rozkład:

$$\beta = \frac{\langle \beta, \alpha \rangle}{\langle \alpha, \alpha \rangle} \alpha + \left(\beta - \frac{\langle \beta, \alpha \rangle}{\langle \alpha, \alpha \rangle} \alpha \right).$$

Pokażemy, że drugi składnik powyższej sumy jest prostopadły do α . Mamy:

$$\left\langle \beta - \frac{\langle \beta, \alpha \rangle}{\langle \alpha, \alpha \rangle} \alpha, \alpha \right\rangle = \langle \beta, \alpha \rangle - \frac{\langle \beta, \alpha \rangle}{\langle \alpha, \alpha \rangle} \langle \alpha, \alpha \rangle = \langle \beta, \alpha \rangle - \langle \beta, \alpha \rangle = 0.$$

Pokazaliśmy, że $V = \text{lin}(\alpha) \oplus \text{lin}(\alpha)^\perp$. Z twierdzenia o wymiarze sumy prostej $\dim \text{lin}(\alpha)^\perp = n - 1$. Przyjmijmy $W = \text{lin}(\alpha)^\perp$ i rozważmy przekształcenie $\langle \cdot, \cdot \rangle|_W : W \times W \rightarrow \mathbb{R}$ zadane wzorem $\langle w, w' \rangle|_W = \langle w, w' \rangle$, dla dowolnych $w, w' \in W$. Jest to obcięcie przekształcenia $\langle \cdot, \cdot \rangle$ do zbioru $W \times W$, będące oczywiście iloczynem skalarnym. A zatem z założenia indukcyjnego $(W, \langle \cdot, \cdot \rangle|_W)$ ma bazę prostopadłą, powiedzmy $\beta_1, \dots, \beta_{n-1}$. Zgodnie z definicją $\langle \cdot, \cdot \rangle|_W$ jest to również układ ortogonalny w V . Co więcej każdy z jego elementów jest prostopadły do α . Zatem układ ortogonalny $\alpha, \beta_1, \dots, \beta_{n-1}$ jest liniowo niezależny i tworzy bazę ortogonalną V . \square

Ważną jest znów interpretacja w języku układów równań. Zauważmy, że gdy $\alpha = (a_1, \dots, a_n) \in \mathbb{R}^n$ oraz gdy $\langle \cdot, \cdot \rangle$ jest standardowym iloczynem skalarnym na \mathbb{R}^n , to $\text{lin}(\alpha)^\perp$ złożona jest z wektorów (x_1, \dots, x_n) spełniających

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = 0.$$

W tym sensie twierdzenie formułowane wyżej jest po prostu innym sformułowaniem twierdzenia Kroneckera-Capellego. Dla pełnego obrazu należałoby powiedzieć, że dla dowolnej bazy $\alpha_1, \dots, \alpha_n$ przestrzeni \mathbb{R}^n istnieje iloczyn skalarny na \mathbb{R}^n , względem którego jest to baza prostopadła. Czy Państwo widzą, że wyznaczenie tego iloczynu skalarnego ma jakiś związek z szukaniem bazy dualnej do powyższej bazy?

Obserwacja 11.4

Jeśli $\alpha_1, \dots, \alpha_n$ jest bazą podprzestrzeni $W \subseteq V$, to następujące warunki są równoważne dla $v \in V$:

- (i) $v \in W^\perp$,
- (ii) $\langle v, \alpha_i \rangle = 0$, dla każdego i .

Dowód. Implikacja (i) \Rightarrow (ii) jest jasna. W drugą stronę: chcemy, by $v \in V$ był prostopadły do każdego wektora z W , a każdy taki wektor jest postaci $w = a_1\alpha_1 + \dots + a_n\alpha_n$. Zatem

$$\langle v, w \rangle = \sum_i a_i \langle v, \alpha_i \rangle = 0.$$

□

Kluczowa dla powyższego dowodu obserwacja o tym, że mamy rozkład $V = \text{lin}(\alpha) \oplus \text{lin}(\alpha)^\perp$ znajduje swoje uogólnienie w następującym fakcie.

Obserwacja 11.5

Niech $(V, \langle \cdot, \cdot \rangle)$ będzie n wymiarową przestrzenią euklidesową i niech W będzie podprzestrzenią przestrzeni V . Wówczas:

- (a) $V = W \oplus W^\perp$,
- (b) jeśli $\dim(W) = k$, to $\dim(W^\perp) = n - k$,
- (c) $(W^\perp)^\perp = W$.

Dowód. Dowiedzimy (a). Podobnie jak w dowodzie twierdzenia o istnieniu bazy prostopadłej musimy wykazać, że $W \cap W^\perp = \{0\}$ oraz, że $W + W^\perp = V$. Pierwszy punkt jest oczywisty. Jeśli $w \in W \cap W^\perp$, to $\langle w, w \rangle = 0$, czyli $w = 0$. Niech $\alpha_1, \dots, \alpha_k$ będzie bazą prostopadłą W , czyli $\langle \alpha_i, \alpha_j \rangle = 0$, dla $i \neq j$ (już wiemy, że taka baza istnieje). Dla każdego wektora $\alpha \in V$ definiujemy:

$$\alpha' = \sum_{i=1}^k \frac{\langle \alpha, \alpha_i \rangle}{\langle \alpha_i, \alpha_i \rangle} \alpha_i.$$

Wówczas oczywiście $\alpha' \in W$. Co więcej, okazuje się, że $\alpha - \alpha' \in W^\perp$. Sprawdźmy to pokazując, że $\alpha - \alpha'$ jest prostopadły do każdego wektora bazowego w W . Istotnie, dla każdego $j = 1, \dots, k$ mamy:

$$\begin{aligned} \langle \alpha - \alpha', \alpha_j \rangle &= \langle \alpha - \sum_{i=1}^k \frac{\langle \alpha, \alpha_i \rangle}{\langle \alpha_i, \alpha_i \rangle} \alpha_i, \alpha_j \rangle = \langle \alpha, \alpha_j \rangle - \sum_{i=1}^k \frac{\langle \alpha, \alpha_i \rangle}{\langle \alpha_i, \alpha_i \rangle} \langle \alpha_i, \alpha_j \rangle = \\ &= \langle \alpha, \alpha_j \rangle - \frac{\langle \alpha, \alpha_j \rangle}{\langle \alpha_j, \alpha_j \rangle} \langle \alpha_j, \alpha_j \rangle = \langle \alpha, \alpha_j \rangle - \langle \alpha, \alpha_j \rangle = 0. \end{aligned}$$

A zatem każdy wektor $\alpha \in V$ ma rozkład $\alpha = \alpha' + (\alpha - \alpha') \in W + W^\perp$. Stąd wynika punkt (a). Oczywiście (b) jest natychmiastową konsekwencją (a). Jeśli chodzi o (c) zauważmy, że mamy $W \subseteq (W^\perp)^\perp$, bo każdy wektor z W jest prostopadły do każdego wektora z W^\perp . Zauważmy jednak, że stosując (b) mamy $\dim(W^\perp)^\perp = n - \dim(W^\perp) = n - (n - \dim W) = \dim W$. Zatem $W = (W^\perp)^\perp$. □

Twierdzenie to pozwala opisywać zbiory ortogonalne i jego teza jest szczególnie przejrzysta gdy weźmiemy przestrzeń \mathbb{R}^n ze standardowym iloczynem skalarnym i w niej podprzestrzeń W opisaną układem równań jednorodnych o macierzy $A \in M_{m \times n}(K)$. Jeśli przez $\alpha_1, \dots, \alpha_m$ oznaczymy wiersze macierzy A , to $W^\perp = \text{lin}(\alpha_1, \dots, \alpha_m)$. Oczywiście gdy iloczyn skalarny nie jest standardowy tak nie musi być.

Zobaczymy przykład wyznaczania bazy prostopadłej oparty o pokazany dowód. Niech V będzie przestrzenią \mathbb{R}^5 z iloczynem skalarnym $\langle \cdot, \cdot \rangle$ zadanym wzorem:

$$\langle (x_1, x_2, x_3, x_4, x_5), (y_1, y_2, y_3, y_4, y_5) \rangle = 2x_1y_1 + x_1y_4 + x_2y_2 + 2x_3y_3 + x_4y_1 + 2x_4y_4 + x_5y_5$$

Niech $W \subseteq \mathbb{R}^5$ będzie opisana układem równań:

$$\begin{cases} 3x_1 + x_2 + 3x_3 + 2x_4 = 0 \\ 2x_1 + x_2 + 2x_3 + 3x_4 = 0 \end{cases}$$

Nietrudno widzieć, że W jest trójwymiarowa. Weźmiemy dowolny niezerowy wektor α do niej należący, powiedzmy

$$\alpha = (-1, 0, 1, 0, 1)$$

i wyznaczmy przestrzeń $\text{lin}(\alpha)^\perp$. Zawiera ona wszystkie wektory $v \in \mathbb{R}^5$ postaci $(x_1, x_2, x_3, x_4, x_5)$ takie, że $\langle \alpha, v \rangle = 0$, czyli (pamiętajmy — $\langle \cdot, \cdot \rangle$ nie jest standardowy iloczyn skalarny):

$$2 \cdot (-1) \cdot x_1 + 1 \cdot (-1) \cdot x_4 + 1 \cdot 0 \cdot x_2 + 2 \cdot 1 \cdot x_3 + 1 \cdot 0 \cdot x_1 + 2 \cdot 0 \cdot x_4 + 1 \cdot 1 \cdot x_5 = 0.$$

A zatem przestrzeń $\text{lin}(\alpha)^\perp$ opisana jest równaniem:

$$-2x_1 + 2x_3 - x_4 + x_5 = 0.$$

Wektory β, γ , które mają dopełnić α do bazy ortogonalnej W pochodzą z $\text{lin}(\alpha)^\perp$, oraz oczywiście są elementami W . A zatem β, γ należą do przestrzeni $W' = \text{lin}(\alpha)^\perp \cap W$ opisanej układem:

$$\begin{cases} 3x_1 + x_2 + 3x_3 + 2x_4 = 0 \\ 2x_1 + x_2 + 2x_3 + 3x_4 = 0 \\ -2x_1 + 2x_3 - x_4 + x_5 = 0 \end{cases}$$

Widzimy zatem, że dowolne dwa wektory prostopadłe z W' dopełnią α do bazy W . Jak je zatem znaleźć? Tak, jakbyśmy startowali od W' . Bierzemy dowolne niezerowe $\beta \in W'$ i szukamy wektora $\gamma \neq 0$ w podprzestrzeni $\text{lin}(\beta)^\perp \cap W'$. Jest jasne, że

$$\text{lin}(\beta)^\perp \cap W' = \text{lin}(\alpha)^\perp \cap \text{lin}(\beta)^\perp \cap W.$$

A zatem biorąc $\beta = (-1, 0, 1, 0, -4)$ widzimy, że $\text{lin}(\beta)^\perp$ opisana jest równaniem $-x_1 + x_3 - x_5 = 0$. Stąd brakujący wektor γ szukanej bazy leży w przestrzeni $\text{lin}(\beta)^\perp \cap W'$ opisanej układem:

$$\begin{cases} 3x_1 + x_2 + 3x_3 + 2x_4 = 0 \\ 2x_1 + x_2 + 2x_3 + 3x_4 = 0 \\ -2x_1 + 2x_3 - x_4 + x_5 = 0 \\ -x_1 + x_3 - x_5 = 0 \end{cases}$$

A zatem baza tworzona jest krok po kroku: zaczynamy od $\alpha \in W$, potem bierzemy wektor $\beta \in \text{lin}(\alpha)^\perp \cap W$, potem (tak naprawdę) wektor $\gamma \in \text{lin}(\alpha, \beta)^\perp \cap W$. Odrobinę prostszym zadaniem jest prośba o wyznaczenie dowolnej bazy prostopadłej przestrzeni \mathbb{R}^5 przy zadanym iloczynie skalarnym. Idea jest wówczas taka sama, przy czym przyjmujemy $W = \mathbb{R}^5$.

Na kolejnym wykładzie przyjrzymy się geometrycznej interpretacji rozkładu na sumę prostopadłą. Chodzi przede wszystkim o wprowadzenie pojęć rzutu i symetrii prostopadłej oraz związanych z nimi istotnych procedur ortogonalizacji, czyli szukania bazy prostopadłej przestrzeni liniowej, zwłaszcza pochodzącej od zadanej z góry bazy tej przestrzeni.

11.1 Zadania do samodzielnej pracy

Zadania ilustrujące umiejętności niezbędne do zaliczenia przedmiotu oznaczone są symbolem ♠.

Przy tych zadaniach dodany jest opis umiejętności, które sprawdzają.

1. (♠ Wyznaczanie wektora prostopadłego)

- W przestrzeni \mathbb{R}^2 ze standardowym iloczynem skalarnym znajdź wektory u, v , spełniające warunki $u \in \text{lin}((1, 3)), v \in \text{lin}((1, 3))^\perp$ oraz $(1, 2) = u + v$.
- W przestrzeni \mathbb{R}^4 ze standardowym iloczynem skalarnym dane są wektory $v = (1, 2, 0, 3)$ oraz $w = (2, 3, -1, 0)$. Wyznacz takie $a, b \in \mathbb{R}$, aby $z = (0, 0, 1, 1) + av + bw \in \text{lin}(v, w)^\perp$.

2. (♠ Opis dopełnienia ortogonalnego podprzestrzeni \mathbb{R}^n)

- Niech $W = \text{lin}((0, 1, 2, 1), (1, 3, 2, 2), (2, 1, -6, -1)) \subset \mathbb{R}^4$. Znajdź bazę przestrzeni W^\perp zarówno w przestrzeni euklidesowej \mathbb{R}^4 ze standardowym iloczynem skalarnym, jak i bazę w przestrzeni \mathbb{R}^4 z iloczynem skalarnym $\langle \cdot, \cdot \rangle$ danym wzorem

$$\langle (x_1, x_2, x_3, x_4), (y_1, y_2, y_3, y_4) \rangle = x_1y_1 - x_1y_2 - x_2y_1 + 4x_2y_2 + 2x_3y_3 - x_3y_4 - x_4y_3 + 2x_4y_4.$$

- W przestrzeni \mathbb{R}^3 ze standardowym iloczynem skalarnym znajdź układ równań opisujący przestrzeń W^\perp , gdzie $W = \{(x_1, x_2, x_3, x_4) \in \mathbb{R}^4 \mid x_1 - x_2 + x_3 - x_4 = 0\}$.

3. (♠ Wyznaczanie bazy prostopadłej podprzestrzeni w \mathbb{R}^n)

- Znajdź bazę prostopadłą przestrzeni \mathbb{R}^3 z iloczynem skalarnym $\langle \cdot, \cdot \rangle$ zadany wzorem

$$\langle (x_1, x_2, x_3), (y_1, y_2, y_3) \rangle = x_1y_1 + 2x_1y_2 + 2x_2y_1 + 7x_2y_2 + x_2y_3 + x_3y_2 + 10x_3y_3.$$

- Niech $W = \text{lin}((1, 1, 2, 1), (2, 3, 1, 3), (3, 5, 0, 5))$ i niech Z będzie podprzestrzenią \mathbb{R}^4 opisaną układem równań

$$\begin{cases} x_1 + x_2 - x_3 + 2x_4 = 0 \\ -x_1 + x_2 + 2x_3 - x_4 = 0 \end{cases}.$$

Znajdź bazę prostopadłą przestrzeni W oraz bazę ortonormalną przestrzeni Z :

- w \mathbb{R}^4 ze standardowym iloczynem skalarnym,
- w \mathbb{R}^4 z iloczynem skalarnym danym wzorem

$$\langle (x_1, x_2, x_3, x_4), (y_1, y_2, y_3, y_4) \rangle = 2x_1y_1 + x_1y_4 + x_2x_4 + 2x_3y_3 + x_4y_1 + 2x_4y_4.$$

- Wskaż za pomocą wzoru przykład iloczynu skalarnego $\langle \cdot, \cdot \rangle : \mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R}$, takiego by układ wektorów $\alpha_1 = (1, 0, 0)$, $\alpha_2 = (0, -1, 0)$, $\alpha_3 = (1, 0, 1)$ był bazą ortonormalną $(\mathbb{R}^3, \langle \cdot, \cdot \rangle)$.

4. W przestrzeni $\mathbb{R}_{\leq n}[x]$ iloczyn skalarny wielomianów $f = a_0x + \dots + a_nx^n$, $g = b_0x + \dots + b_nx^n$ określony jest wzorem: $\langle f, g \rangle = a_0b_0 + a_1b_1 + \dots + a_nb_n$. Znajdź dopełnienie ortogonalne:

- podprzestrzeni wielomianów, dla których $f(1) = 0$,
- podprzestrzeni wszystkich wielomianów parzystego stopnia.

5. W przestrzeni $l^2 \subset \mathbb{R}^\infty$ złożonej z ciągów (x_i) , takich że $\sum_{i=1}^{\infty} x_i^2 < \infty$ rozważamy iloczyn skalarny

$$\langle \cdot, \cdot \rangle : l^2 \times l^2 \rightarrow \mathbb{R} \text{ dany wzorem } \langle (x_i), (y_i) \rangle = \sum_{i=1}^{\infty} x_i y_i. \text{ Rozważmy w tej przestrzeni podprzestrzeń } W$$

ciągów, które mają jedynie skończenie wiele niezerowych wyrazów. Znajdź W^\perp . Czy $l^2 = W \oplus W^\perp$?

6. Dwa ciągi wektorów (v_1, \dots, v_n) oraz (w_1, \dots, w_n) w przestrzeni euklidesowej spełniają warunki $\langle v_i, w_j \rangle = 0$, dla $i \neq j$ oraz $\langle v_i, w_i \rangle = 1$. Wykaż, że układ v_1, \dots, v_n jest liniowo niezależny.

7. Niech V będzie przestrzenią euklidesową oraz niech W_1, W_2 będą podprzestrzeniami V spełniającymi warunek $\dim W_1 < \dim W_2$. Pokazać, że istnieje niezerowy wektor $v \in W_2$ taki, że $v \in W_1^\perp$.

8. Załóżmy, że $(V, \langle \cdot, \cdot \rangle)$ jest przestrzenią euklidesową. Niech układ $\{e_1, \dots, e_n\}$ wektorów z V będzie ortonormalny. Wykaż, że następujące warunki są równoważne:

- $v \in \text{lin}(e_1, \dots, e_m)$,
- $\|v\|^2 = |\langle v, e_1 \rangle|^2 + \dots + |\langle v, e_m \rangle|^2$.

9. Znajdź największe m , dla którego istnieje układ m wektorów $\alpha_1, \dots, \alpha_m$ w n -wymiarowej przestrzeni euklidesowej liniowej, że $\langle \alpha_i, \alpha_j \rangle < 0$, dla $1 \leq i < j \leq n$.

11.2 Trivia. Czy względna pierwszość to prostopadłość?

Jak wiemy każda dodatnia liczba naturalna n może być jednoznacznie przedstawiona jako iloczyn

$$n = \prod_p p^{v_p(n)},$$

gdzie v_p są nieujemnymi liczbami naturalnymi. Wspominaliśmy o tym choćby w podrozdziale o liczbach p -adycznych. Liczby $v_p(n)$ nazywamy wykładnikami p -adycznymi liczby n . Są takie liczby całkowite k , że $p^k \mid n$ oraz $p^{k+1} \nmid n$. Wprawdzie powyższy iloczyn jest nieskończony, ale jedynie skończenie wiele z jego czynników jest różnych od 1. Przypomnijmy kilka elementarnych własności wykładnika.

Obserwacja 11.6

Niech p będzie liczbą pierwszą, zaś a, b niech będą dodatnimi liczbami całkowitymi.

- $v_p(ab) = v_p(a) + v_p(b)$ oraz $v_p(a/b) = v_p(a) - v_p(b)$,
- $v_p(a^n) = nv_p(a)$,
- $v_p(\text{NDW}(a, b)) = \min\{v_p(a), v_p(b)\}$ oraz $v_p(\text{NWW}(a, b)) = \max\{v_p(a), v_p(b)\}$,
- $v_p(a \pm b) \geq \min\{v_p(a), v_p(b)\}$. Gdy $v_p(a) \neq v_p(b)$, wówczas mamy równość.

Co więcej następujące warunki są równoważne.

- $x \mid y$,
- dla każdej liczby pierwszej p zachodzi nierówność $v_p(x) \leq v_p(y)$

W szczególności $x = y$ wtedy i tylko wtedy, gdy $v_p(x) = v_p(y)$, dla każdej liczby pierwszej p .

Przykładowe proste zastosowania powyższego faktu.

Zadanie 11.1. Niech p będzie liczbą pierwszą. Wykaż, że równanie $x^2 - py^2 = 0$ nie ma rozwiązań w liczbach całkowitych.

ROZWIĄZANIE. Aby zachodziła równość $x^2 = py^2$ konieczne jest, aby $v_p(x^2) = v_p(py^2)$. Jedna strona tej równości jest liczbą parzystą $2v_p(x)$, druga zaś – liczbą nieparzystą $2v_p(y) + 1$, co jest niemożliwe. ■

Zadanie 11.2. Dla dodatnich liczb całkowitych a, b mamy $\text{NDW}(a, b) \cdot \text{NWW}(a, b) = a \cdot b$.

ROZWIĄZANIE. Policzmy wartość wyrażenia $v_p(\text{NDW}(a, b) \cdot \text{NWW}(a, b)) - v_p(ab)$. Zgodnie z własnościami podanymi wyżej wyrażenie to jest równe $\min\{v_p(a), v_p(b)\} + \max\{v_p(a), v_p(b)\} - v_p(a) - v_p(b)$. Jest jasne, że uzyskane wyrażenie jest zawsze równe 0. ■

Na potrzeby tego dodatku stosować będziemy notację przyjętą przez Ronalda L. Grahama, Donalda D. Knutha i Orena Patashnika w książce *Matematyka Konkretna*, oznaczając liczby względnie pierwsze symbolem prostopadłości \perp , tzn. $n \perp m \iff \text{NDW}(n, m) = 1$. Jaka jest motywacja tego podejścia?

Podstawowe własności wektorów prostopadłych można podsumować w następującym wyliczeniu. Niech v, w będą wektorami w przestrzeni rzeczywistej. Wówczas:

- dla każdego \vec{v} istnieje \vec{w} , że $\vec{v} \perp \vec{w}$,
- dla każdych \vec{v}, \vec{w} mamy $\vec{v} \perp \vec{w} \Rightarrow \vec{w} \perp \vec{v}$,
- dla każdego $\vec{v} \neq 0$ mamy $\vec{v} \not\perp \vec{v}$,
- dla każdych $\vec{v}, \vec{w}, \vec{z}$ mamy:

$$\begin{cases} \vec{v} \perp \vec{w} \\ \vec{v} \perp \vec{z} \end{cases} \Rightarrow \vec{v} \perp (\vec{w} + \vec{z})?$$

Czy te własności spełnione są przez pary liczb względnie pierwszych? Pierwsze dwie – oczywiście tak. Każda dodatnia liczba całkowita ma choć jedną względnie pierwszą z nią (a nawet nieskończenie wiele). Relacja względnej pierwszości jest symetryczna. A pozostałe dwa?

Warunek trzeci może budzić wątpliwość, bo w ogóle nie rozważamy na razie niezerowych liczb. Ma on jednak sens o tyle, że jedyną dodatnią liczbą całkowitą względnie pierwszą ze sobą jest 1 — ta liczba gra więc rolę zera.

A warunek czwarty? Odpowiedź jest pozytywna, jeśli działanie $+$ jest **mnożeniem**! Jak to rozumieć?

Rozważamy podzbiór przestrzeni ciągów \mathbb{R}^∞ złożony z ciągów postaci:

$$n \mapsto v(n) = (v_2(n), v_3(n), v_5(n), v_7(n), v_{11}(n), \dots),$$

Zobaczmy przykłady:

$$80 = 2^4 \cdot 3^0 \cdot 5^1 \cdot 7^0 \cdot \dots \rightsquigarrow (4, 0, 1, 0, 0, \dots)$$

$$189 = 2^0 \cdot 3^3 \cdot 5^0 \cdot 7^1 \cdot \dots \rightsquigarrow (0, 3, 0, 1, 0, \dots)$$

W tej konfiguracji oczywiście liczba 1 przechodzi na wektor zerowy:

$$1 = 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^0 \cdot \dots \rightsquigarrow (0, 0, 0, 0, 0, \dots).$$

Jasna jest również interpretacja liczb pierwszych – są to kolejne „wersory”, np.

$$5 = 2^0 \cdot 3^0 \cdot 5^1 \cdot 7^0 \cdot \dots \rightsquigarrow (0, 0, 1, 0, 0, \dots)$$

Zauważmy, że w istocie można rozszerzyć powyższe przypisanie na dowolne dodatnie liczby wymierne, przyjmując $v(p/q) = v(p) - v(q)$, na przykład:

$$80/27 = 2^4 \cdot 3^{-3} \cdot 5^1 \cdot 7^0 \cdot \dots \rightsquigarrow (4, -3, 1, 0, 0, \dots)$$

$$189/25 = 2^0 \cdot 3^3 \cdot 5^{-2} \cdot 7^1 \cdot \dots \rightsquigarrow (0, 3, -2, 1, 0, \dots)$$

$$3/7 = 2^0 \cdot 3^1 \cdot 5^0 \cdot 7^{-1} \cdot \dots \rightsquigarrow (0, 1, 0, -1, 0, \dots)$$

Gdybyśmy mogli tu używać języka teorii grup, powiedzielibyśmy, że mamy izomorfizm grupy mnożymy liczb wymiernych z grupą addytywną wielomianów o współczynnikach całkowitych. Oczywiście nie otrzymujemy podprzestrzeni liniowej (ale otrzymujemy pewien podmoduł...). Zauważmy, że przyjmując w wymienionych wyżej ciągach naturalne działania dodawania wektorów i mnożenia przez skalar widzimy, że

$$v(nm) = v(n) + v(m), \quad v(n^k) = k \cdot v(n).$$

Oto ilustracja dla iloczynu $80 \cdot 189$ oraz dla liczby $3920^3 = 2^{12} \cdot 5^3 \cdot 7^6$:

$$(4, 0, 1, 0, 0, \dots) + (0, 3, 0, 1, 0, \dots) = (4, 3, 1, 1, 0, \dots), \quad 3 \cdot (4, 0, 1, 2, 0, \dots) = (12, 0, 3, 6, 0, \dots).$$

We wprowadzonej konwencji rozważać można również kombinacje liniowe wektorów:

$$\vec{a} = 3, \quad \vec{b} = 10, \quad \vec{a} + 2\vec{b} = 3 \cdot 10^2 = 300.$$

Jest wreszcie jasne, że względna pierwszość liczb całkowitych odpowiada prostopadłości, przy przyjęciu „standardowego iloczynu skalarnego” w \mathbb{R}^∞ , np.

$$\langle 80, 189 \rangle = 4 \cdot 0 + 0 \cdot 3 + 1 \cdot 0 + 0 \cdot 1 + \dots = 0.$$

Podobnie zdefiniować można normę oraz kąt, np.

$$\|432\| = \sqrt{2^4 \cdot 3^3, 2^4 \cdot 3^3} = \sqrt{4^2 + 3^2} = 5, \quad \cos \angle(6, 10) = \frac{\langle 6, 10 \rangle}{\|6\| \cdot \|10\|} = \frac{1}{\sqrt{2} \cdot \sqrt{2}} = \frac{1}{2}.$$

Można więc powiedzieć, że pary liczb względnie pierwszych można traktować w tej konwencji jako liczby prostopadłe, a potęgi tej samej liczby całkowitej – jako liczby równoległe. Zachęcam Czytelnika do przemyślenia dlaczego w ramach tej konwencji „trójkąt” o wierzchołkach 6, 10, 15 jest „równoboczny”.

Czy to wszystko przekłada się na jakiegokolwiek zastosowania? Okazuje się, że tak, gdy rozważamy powyższe wektory jako elementy \mathbb{Z}_2^∞ , ale to już inna historia...

Rozdział 12

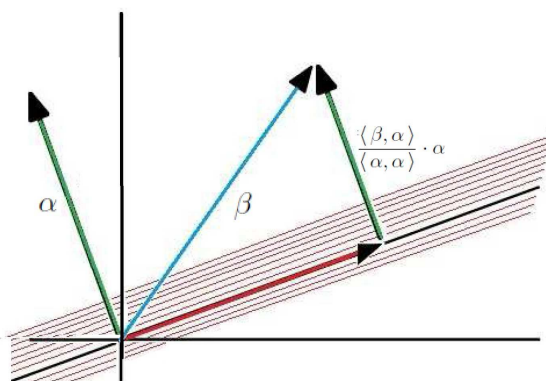
Rzut prostopadły i ortogonalizacja

Na poprzednim wykładzie wprowadziliśmy pojęcie prostopadłości pary wektorów, a także pojęcie dopełnienia ortogonalnego. W kontekście przestrzeni euklidesowych pojęcia te mają szczególnie przejrzysty opis. Wykazaliśmy, że każda taka przestrzeń posiada bazę prostopadłą oraz pokazaliśmy, dla dowolnej podprzestrzeni W przestrzeni euklidesowej V ma miejsce rozkład $V = W \oplus W^\perp$. Dziś kontynuujemy te rozważania, wychodząc od następującej obserwacji, poczynionej na poprzednim wykładzie.

Obserwacja 12.1

Jeśli α jest niezerowym wektorem w przestrzeni liniowej V z iloczynem skalarnym $(V, \langle \cdot, \cdot \rangle)$ oraz $\beta \in V$, to mamy rozkład, w którym drugi składnik należy do $\text{lin}(\alpha)^\perp$

$$\beta = \frac{\langle \beta, \alpha \rangle}{\langle \alpha, \alpha \rangle} \cdot \alpha + \left(\beta - \frac{\langle \beta, \alpha \rangle}{\langle \alpha, \alpha \rangle} \cdot \alpha \right),$$



Obserwacja 12.2

Niech $\mathcal{A} = \{\alpha_1, \dots, \alpha_n\}$ będzie bazą prostopadłą przestrzeni euklidesowej $(V, \langle \cdot, \cdot \rangle)$. Wówczas dla każdego wektora $\alpha = a_1\alpha_1 + \dots + a_n\alpha_n \in V$ jego współrzędne w bazie \mathcal{A} wynoszą:

$$a_1 = \frac{\langle \alpha, \alpha_1 \rangle}{\langle \alpha_1, \alpha_1 \rangle}, \quad a_2 = \frac{\langle \alpha, \alpha_2 \rangle}{\langle \alpha_2, \alpha_2 \rangle}, \quad \dots, \quad a_n = \frac{\langle \alpha, \alpha_n \rangle}{\langle \alpha_n, \alpha_n \rangle}.$$

Dowód. Dla każdego $i = 1, \dots, n$ oraz dla każdego $j \neq i$ mamy $\langle \alpha_j, \alpha_i \rangle = 0$, czyli:

$$\begin{aligned} \langle \alpha, \alpha_i \rangle &= \langle a_1\alpha_1 + a_2\alpha_2 + \dots + a_n\alpha_n, \alpha_i \rangle = \\ &= a_1 \langle \alpha_1, \alpha_i \rangle + \dots + a_i \langle \alpha_i, \alpha_i \rangle + \dots + a_n \langle \alpha_n, \alpha_i \rangle = a_i \langle \alpha_i, \alpha_i \rangle. \end{aligned}$$

Stąd $a_i = \frac{\langle \alpha, \alpha_i \rangle}{\langle \alpha_i, \alpha_i \rangle}$. □

Powyższe rozważania prowadzą do następującej definicji.

Definicja 12.1: Rzut i symetria prostopadła

Niech $(V, \langle \cdot, \cdot \rangle)$ będzie przestrzenią euklidesową i niech $W \subseteq V$ będzie podprzestrzenią.

- Przekształcenie liniowe $\phi : V \rightarrow V$ będące rzutem na W wzdłuż W^\perp nazywamy RZUTEM PROSTOPADŁYM na W .
- Przekształcenie liniowe $\psi : V \rightarrow V$ będące symetrią względem W wzdłuż W^\perp nazywamy SYMETRIĄ PROSTOPADŁĄ względem W .

Z opisu współrzędnych w bazie prostopadłej wynika natychmiast następująca obserwacja.

Obserwacja 12.3: Rzut prostopadły

Niech $W \subseteq V$ będzie podprzestrzenią przestrzeni euklidesowej $(V, \langle \cdot, \cdot \rangle)$, niech $(\alpha_1, \dots, \alpha_k)$ będzie bazą prostopadłą przestrzeni W oraz niech $(\alpha_{k+1}, \dots, \alpha_n)$ niech będzie bazą prostopadłą przestrzeni W^\perp . Wówczas dla każdego wektora $\alpha \in V$:

- rzut prostopadły $\phi(\alpha)$ wektora α na W wynosi:

$$\phi(\alpha) = \sum_{i=1}^k \frac{\langle \alpha, \alpha_i \rangle}{\langle \alpha_i, \alpha_i \rangle} \alpha_i,$$

- symetria prostopadła $\psi(\alpha)$ wektora α względem W wynosi:

$$\psi(\alpha) = \sum_{i=1}^k \frac{\langle \alpha, \alpha_i \rangle}{\langle \alpha_i, \alpha_i \rangle} \alpha_i - \sum_{j=k+1}^n \frac{\langle \alpha, \alpha_j \rangle}{\langle \alpha_j, \alpha_j \rangle} \alpha_j.$$

Rzut prostopadły ma ważną interpretację dotyczącą szacowania norm, o licznych zastosowaniach.

Obserwacja 12.4

Niech W będzie podprzestrzenią przestrzeni euklidesowej V oraz niech $v \in V$ rozkłada się (jednoznacznie) na sumę $v' + v''$, gdzie $v' \in W$ oraz $v'' \in W^\perp$. Wówczas

$$\|v - v'\| = \min_{w \in W} \|v - w\|.$$

Dowód. Dowód wynika z definicji normy i twierdzenia Pitagorasa. Dla każdego $w \in W$ mamy:

$$\begin{aligned} \|v - v'\|^2 &\leq \|v - v'\|^2 + \|v' - w\|^2 \\ &= \|(v - v') + (v' - w)\|^2 = \|v - w\|^2. \end{aligned}$$

□

Do opisu rzutów i symetrii prostopadłych, a także szerszej klasy przekształceń, którą poznamy niebawem, przydatne będzie rozważanie baz prostopadłych złożonych z wektorów jednostkowych.

Definicja 12.2: Układ ortonormalny

Mówimy, że układ $\alpha_1, \dots, \alpha_n$ wektorów przestrzeni euklidesowej $(V, \langle \cdot, \cdot \rangle)$ jest PROSTOPADŁY UNORMOWANY (albo ORTONORMALNY), jeśli $\alpha_1, \dots, \alpha_n$ jest układem prostopadłym oraz $\|\alpha_i\| = 1$, dla każdego $i = 1, \dots, n$. Układ prostopadły unormowany będący bazą przestrzeni V nazywamy BAZĄ ORTONORMALNĄ przestrzeni $(V, \langle \cdot, \cdot \rangle)$.

Przykłady.

- Baza standardowa w \mathbb{R}^n jest bazą ortonormalną $(\mathbb{R}^n, \langle \cdot, \cdot \rangle_{st})$.
- Poniższy układ jest bazą ortonormalną przestrzeni $(\mathbb{R}^3, \langle \cdot, \cdot \rangle_{st})$:

$$\left(\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}} \right), \quad \left(-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0 \right), \quad \left(\frac{1}{\sqrt{6}}, \frac{1}{\sqrt{6}}, -\frac{2}{\sqrt{6}} \right).$$

Wniosek 12.1

Każda przestrzeń euklidesowa $(V, \langle \cdot, \cdot \rangle)$ ma bazę ortonormalną.

Dowód. Niech $\alpha_1, \dots, \alpha_n$ będzie bazą prostopadłą przestrzeni $(V, \langle \cdot, \cdot \rangle)$. Wówczas układ $\frac{1}{\|\alpha_1\|}\alpha_1, \dots, \frac{1}{\|\alpha_n\|}\alpha_n$ jest w sposób oczywisty ortonormalny, bo z definicji iloczynu skalarnego mamy $\|a\alpha\| = |a| \cdot \|\alpha\|$, dla każdego $a \in \mathbb{R}$ oraz $\alpha \in V$. \square

Dysponując bazami ortonormalnymi wiele rozważanych wcześniej wzorów i rozumowań jest czytelniejszych, bowiem nie ma konieczności wpisywania do mianowników wyrażeń typu $\langle \alpha_i, \alpha_i \rangle$. Współrzędne wektora α w bazie ortonormalnej $(\alpha_1, \dots, \alpha_n)$ to po prostu $\langle \alpha, \alpha_1 \rangle, \dots, \langle \alpha, \alpha_n \rangle$. Wynikają stąd również bardziej przejrzyste wzory na rzut i symetrię prostopadłą.

* * *

Bazę prostopadłą przestrzeni euklidesowej $(V, \langle \cdot, \cdot \rangle)$ można otrzymać nie tylko poprzez wyliczenie dopełnień ortogonalnych, ale też przez odpowiednią modyfikację dowolnej bazy zadanej przestrzeni V . Metoda ta nazywa się ortogonalizacją Grama-Schmidta i posiada liczne zastosowania. Geometrycznie polega ona na zastąpieniu bazy $\gamma_1, \dots, \gamma_n$ bazą $\alpha_1, \dots, \alpha_n$, w której dla $i = 2, \dots, n$ wektor α_i jest rzutem prostopadłym wektora γ_i na podprzestrzeń $\text{lin}(\gamma_1, \dots, \gamma_{i-1})^\perp$.

Twierdzenie 12.1: Ortogonalizacja Grama-Schmidta

Jeśli $(V, \langle \cdot, \cdot \rangle)$ jest przestrzenią euklidesową oraz $\gamma_1, \dots, \gamma_n$ jest bazą przestrzeni V , to układ $\alpha_1, \dots, \alpha_n$ zadany indukcyjnie wzorami $\alpha_1 = \gamma_1$ oraz dla $j > 1$:

$$\alpha_j = \gamma_j - \sum_{i=1}^{j-1} \frac{\langle \gamma_j, \alpha_i \rangle}{\langle \alpha_i, \alpha_i \rangle} \alpha_i$$

jest bazą prostopadłą przestrzeni V . Ponadto dla każdego $j = 1, \dots, n$ mamy:

$$\text{lin}(\alpha_1, \dots, \alpha_j) = \text{lin}(\gamma_1, \dots, \gamma_j).$$

Uwaga. Bardzo istotne jest założenie $V_s = \text{lin}(\alpha_1, \dots, \alpha_s) = \text{lin}(\gamma_1, \dots, \gamma_s)$, które mówi, że w $s+1$ -wszym kroku algorytmu, gdy udało nam się już zamienić bazę $\gamma_1, \dots, \gamma_s$ przestrzeni V_s na bazę prostopadłą $\alpha_1, \dots, \alpha_s$ - rzutujemy γ_{s+1} na $\text{lin}(\alpha_1, \dots, \alpha_s)^\perp$ i w ten sposób dostajemy α_{s+1} , uzupełniający $\alpha_1, \dots, \alpha_s$ do bazy prostopadłej V_{s+1} .

Przykład. Rozważmy $(\mathbb{R}^3, \langle \cdot, \cdot \rangle_{st})$ z bazą $\gamma_1 = (1, -1, 1)$, $\gamma_2 = (1, 0, 1)$, $\gamma_3 = (1, 1, 2)$. Zaprezentujemy algorytm ortogonalizacji.

$$\alpha_1 = (1, -1, 1), \quad \alpha_2 = (1, 0, 1) - \frac{\langle (1, 0, 1), (1, -1, 1) \rangle}{\langle (1, -1, 1), (1, -1, 1) \rangle} (1, -1, 1) = \left(\frac{1}{3}, \frac{2}{3}, \frac{1}{3} \right),$$

$$\alpha_3 = (1, 1, 2) - \frac{\langle (1, 1, 2), (1, -1, 1) \rangle}{\langle (1, -1, 1), (1, -1, 1) \rangle} (1, -1, 1) - \frac{\langle (1, 1, 2), (\frac{1}{3}, \frac{2}{3}, \frac{1}{3}) \rangle}{\langle (\frac{1}{3}, \frac{2}{3}, \frac{1}{3}), (\frac{1}{3}, \frac{2}{3}, \frac{1}{3}) \rangle} \left(\frac{1}{3}, \frac{2}{3}, \frac{1}{3} \right) = \left(\frac{-1}{2}, 0, \frac{1}{2} \right).$$

Dostaliśmy bazę prostopadłą $(1, -1, 1), (\frac{1}{3}, \frac{2}{3}, \frac{1}{3}), (\frac{-1}{2}, 0, \frac{1}{2})$.

Czytelnika zainteresowanego większą liczbą przykładów wyznaczania baz prostopadłych odsyłam do filmu: <https://youtu.be/sh0Ck6nQFGE>.

Dowód. Stosujemy indukcję względem n . Dla $n = 1$ teza jest oczywista. Załóżmy, że wykazaliśmy twierdzenie dla $n - 1$ i dowodzimy dla n . Niech $W = \text{lin}(\gamma_1, \dots, \gamma_{n-1})$. Na mocy założenia indukcyjnego wzory określone w tezie określają bazę prostopadłą $\alpha_1, \dots, \alpha_{n-1}$ przestrzeni W . Stąd mamy rozkład wektora γ_n na sumę wektorów z W oraz W^\perp , której składnikami są

$$\sum_{i=1}^{n-1} \frac{\langle \gamma_n, \alpha_i \rangle}{\langle \alpha_i, \alpha_i \rangle} \alpha_i \in W \quad \text{oraz} \quad \gamma_n - \sum_{i=1}^{n-1} \frac{\langle \gamma_n, \alpha_i \rangle}{\langle \alpha_i, \alpha_i \rangle} \alpha_i \in W^\perp.$$

Drugi z tych wektorów jest niezerowy, bo $\gamma_n \notin \text{lin}(\gamma_1, \dots, \gamma_{n-1}) = \text{lin}(\alpha_1, \dots, \alpha_{n-1})$ (tu wykorzystujemy ponownie założenie indukcyjne, tym razem wobec do drugiej części tezy). A zatem układ:

$$\alpha_1, \dots, \alpha_{n-1}, \gamma_n - \sum_{i=1}^{n-1} \frac{\langle \gamma_n, \alpha_i \rangle}{\langle \alpha_i, \alpha_i \rangle} \alpha_i$$

składa się z n niezerowych wektorów. Jest to więc baza prostopadła V . □

Odnotujemy istotny wniosek.

Wniosek 12.2

Niech $(V, \langle \cdot, \cdot \rangle)$ będzie przestrzenią euklidesową.^a Wówczas każdy układ prostopadły (odp. ortonormalny) dopełnić można do bazy prostopadłej przestrzeni V .

^aA co się w zasadzie dzieje, gdy próbujemy wykonać proces ortogonalizacji na układzie liniowo zależnym? Otóż stanie się to, że w trakcie procesu dostaniemy wektor zerowy. Innymi słowy, proces ortogonalizacji można stosować do rozpoznawania układów liniowo zależnych. Proszę to sprawdzić na układzie wektorów w $(\mathbb{R}^4, \langle \cdot, \cdot \rangle_{st})$:

$$\begin{aligned} \gamma_1 &= (1, -1, 1, -1) \\ \gamma_2 &= (1, 1, 3, -1) \\ \gamma_3 &= (-3, 7, 1, 3) \end{aligned}$$

Dowód. Niech $\alpha_1, \dots, \alpha_k$ będzie układem prostopadłym w V . Na mocy tw. Steinitza możemy dopełnić ten układ do bazy V wektorami $\gamma_{k+1}, \dots, \gamma_n$. Stosujemy proces ortogonalizacji do rozszerzonego przez nas układu $\alpha_1, \dots, \alpha_k, \gamma_{k+1}, \dots, \gamma_n$ i uzyskujemy bazę prostopadłą $\alpha_1, \dots, \alpha_k, \alpha_{k+1}, \dots, \alpha_n$. Rzeczywiście, w pierwszych k krokach dostaniemy po prostu układ prostopadły $\alpha_1, \dots, \alpha_k$. □

Końcową część poświęcimy nieobowiązkowemu, ale ważnemu komentarzowi do teorii endomorfizmów. Przypomnijmy, że macierz $A = (a_{ij}) \in M_n(K)$ nazywamy górnotrójkątną, jeśli $a_{ij} = 0$, dla $i < j$. Niech ϕ będzie endomorfizmem skończenie wymiarowej przestrzeni liniowej V . Jednym z rozważanych przez nas problemów było pytanie czy istnieje baza V , w której ϕ ma macierz górnotrójkątną? O takiej sytuacji mówimy, że ϕ jest triangularyzowalny. W ramach teorii endomorfizmów ustaliliśmy, że warunkiem koniecznym i dostatecznym jego triangularyzowalności jest to, by wielomian charakterystyczny endomorfizmu ϕ rozkładał się na czynniki liniowe.

Obserwacja 12.5

Niech $(V, \langle \cdot, \cdot \rangle)$ będzie przestrzenią euklidesową oraz niech $\phi \in \text{End}(V)$ będzie triangularyzowalny. Wówczas istnieje baza prostopadła przestrzeni V , w której macierz ϕ jest górnotrójkątna.

Dowód. Niech $\mathcal{A} = (\gamma_1, \dots, \gamma_n)$ będzie bazą taką, że $M(\phi)_{\mathcal{A}}^{\mathcal{A}}$ jest górnotrójkątna. Wiemy, że dla każdego $1 \leq j \leq n$ przestrzeń $\text{lin}(\gamma_1, \dots, \gamma_j)$ jest ϕ -niezmiennicza. Stosując procedurę Grama-Schmidta dostajemy bazę prostopadłą $\alpha_1, \dots, \alpha_n$ przestrzeni V taką, że $\text{lin}(\gamma_1, \dots, \gamma_j) = \text{lin}(\alpha_1, \dots, \alpha_j)$. A zatem $\text{lin}(\alpha_1, \dots, \alpha_j)$ jest również ϕ -niezmiennicza, dla każdego j . To oznacza, że ϕ ma w bazie $\{\alpha_1, \dots, \alpha_n\}$ macierz górnotrójkątną. □

Uwaga: zauważmy, że powyższy fakt nie stosuje się koniecznie do macierzy diagonalizowalnych. Czy Czytelnik potrafi pokazać odpowiedni przykład? Kwestię diagonalizowalności endomorfizmów przestrzeni euklidesowych poruszemy później. Ma ona fundamentalne znaczenie dla zastosowań matematyki.

12.1 Zadania do samodzielnej pracy

Zadania ilustrujące umiejętności niezbędne do zaliczenia przedmiotu oznaczone są symbolem ♠.

Przy tych zadaniach dodany jest opis umiejętności, które sprawdzają.

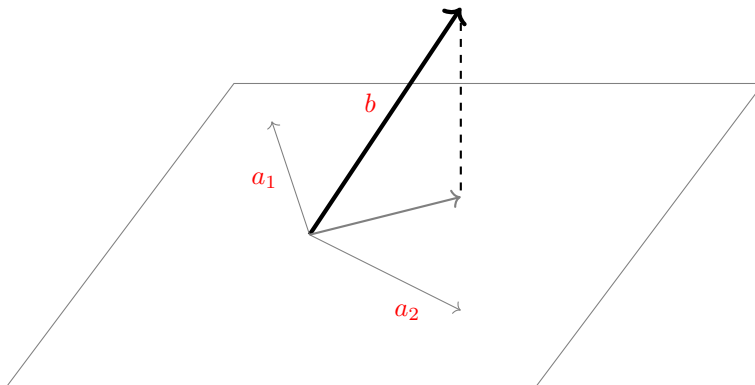
1. (♠ Stosowanie ortogonalizacji Grama-Schmidta)
 - W przestrzeni liniowej \mathbb{R}^4 ze standardowym iloczynem skalarnym rozważmy wektory $v_1 = (2, -1, 0, -2)$, $v_2 = (4, 1, 4, -4)$, $v_3 = (0, 0, 1, 0)$, $v_4 = (0, 0, 0, 1)$. Stosując algorytm ortogonalizacji Grama-Schmidta wyznacz taką bazę ortonormalną $\{e_1, e_2, e_3, e_4\}$ przestrzeni \mathbb{R}^4 , że $\text{lin}(e_1, e_2, e_3, e_4) = \text{lin}(v_1, v_2, v_3, v_4)$.
 - W przestrzeni liniowej \mathbb{R}^4 ze standardowym iloczynem skalarnym rozważmy podprzestrzeń $W = \text{lin}((1, 1, 0, 1), (1, 0, 1, 0), (0, 1, 1, 1))$. Znajdź bazę przestrzeni W otrzymaną z bazy $(1, 1, 0, 1), (1, 0, 1, 0), (0, 1, 1, 1)$ za pomocą ortogonalizacji Grama-Schmidta.
2. (♠ Obraz wektora przy rzucie lub symetrii prostopadłej)
 - W przestrzeni euklidesowej liniowej \mathbb{R}^4 ze standardowym iloczynem skalarnym znajdź rzuty prostopadłe wektora $(0, 1, 1, 1)$ na przestrzenie W oraz W^\perp , gdzie W jest podprzestrzenią opisaną równaniem $2x_1 + 2x_2 - x_3 + x_4 = 0$.
 - Znajdź obraz wektora $(1, -2, 0, 1)$ przy symetrii prostopadłej względem podprzestrzeni $\text{lin}(1, 2, 2, -1)^\perp$ przestrzeni \mathbb{R}^4 ze standardowym iloczynem skalarnym.
 - W przestrzeni \mathbb{R}^4 dany jest standardowy iloczyn skalarny. Niech $\alpha_t = (t^2, 0, 1, t)$ i niech β_t będzie rzutem prostopadłym wektora α_t na prostą $\text{lin}((1, 1, 1, 1))$. Dla jakich $t \in \mathbb{R}$ długość wektora β_t jest najmniejsza?
 - W \mathbb{R}^3 ze standardowym iloczynem skalarnym niech $\alpha_1 = (1, 2, 1)$, $\alpha_2 = (0, 1, -2)$, $\alpha_3 = (0, t, 1)$. Niech β będzie rzutem prostopadłym wektora α_3 na $\text{lin}(\alpha_1, \alpha_2)^\perp$. Dla jakich $t \in \mathbb{R}$ wektor β ma najmniejszą długość?
 - W przestrzeni liniowej \mathbb{R}^4 ze standardowym iloczynem skalarnym dana jest podprzestrzeń $U = \text{lin}((1, 1, 0, 0), (1, 1, 1, 2))$. Znajdź $\alpha \in U$ taki, że norma $\|\alpha - (1, 2, 3, 4)\|$ jest minimalna.
 - W przestrzeni euklidesowej liniowej $(V, \langle \cdot, \cdot \rangle)$ dana jest baza ortonormalna $\beta_1, \beta_2, \beta_3$ oraz wektory $\alpha = a_1\beta_1 + a_2\beta_2 + a_3\beta_3$ i $\beta = b_1\beta_1 + b_2\beta_2 + b_3\beta_3$, dla pewnych $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{R}$. Wyznacz rzut prostopadły wektora β na $\text{lin}(\alpha)$.
3. (♠ Wzór rzutu/symetrii prostopadłej)
 - W przestrzeni \mathbb{R}^4 ze standardowym iloczynem skalarnym dana jest podprzestrzeń
$$W = \text{lin}((2, 1, 0, 1), (1, 0, 0, 1)).$$
Znajdź wzór na rzut prostopadły na W oraz na symetrię prostopadłą względem W^\perp .
 - W przestrzeni \mathbb{R}^4 ze standardowym iloczynem skalarnym dana jest podprzestrzeń W opisana równaniem $x_1 + x_2 - x_3 + 2x_4 = 0$. Wyznacz wzór na symetrię prostopadłą względem W .
4. W przestrzeni \mathbb{R}^n ze standardowym iloczynem skalarnym rozpatrzmy układ wektorów $\alpha_1, \dots, \alpha_k$, gdzie $\alpha_j = (a_{1j}, a_{2j}, \dots, a_{nj})$, dla $j = 1, \dots, k$, i rozpatrzmy odpowiadającą im macierz postaci $A = [a_{ij}] \in M_{n \times k}(\mathbb{R})$. Niech $p_W : \mathbb{R}^n \rightarrow \mathbb{R}^n$ będzie rzutem prostopadłym na $W = \text{lin}(\alpha_1, \dots, \alpha_k)$. Wykaż, że jeśli $\alpha_1, \dots, \alpha_k$ jest układem ortonormalnym, to $M(p_W)_{st}^s = AA^T$.
5. Niech $(V, \langle \cdot, \cdot \rangle)$ będzie przestrzenią euklidesową liniową. Wykaż, że jeśli $\phi : V \rightarrow V$ spełnia warunek $\phi^2 = \phi$ oraz każdy wektor w $\ker \phi$ jest prostopadły do każdego wektora w $\text{im } \phi$, to ϕ jest rzutem prostopadłym na pewną podprzestrzeń V .
6. Niech $(V, \langle \cdot, \cdot \rangle)$ będzie przestrzenią euklidesową liniową. Wykaż, że jeśli $\phi : V \rightarrow V$ jest rzutem, który dla każdego $\alpha \in V$ spełnia $\|\phi(\alpha)\| \leq \|\alpha\|$, to ϕ jest rzutem prostopadłym na pewną podprzestrzeń.
7. Niech ϕ będzie endomorfizmem przestrzeni euklidesowej liniowej $(V, \langle \cdot, \cdot \rangle)$. Niech U będzie podprzestrzenią V . Wykaż, że następujące warunki są równoważne:
 - podprzestrzeń U jest ϕ -niezmiennicza,
 - $p_U \circ \phi \circ p_U = \phi \circ p_U$, gdzie p_U jest rzutem prostopadłym na U .
8. Niech $(V, \langle \cdot, \cdot \rangle)$ będzie przestrzenią euklidesową liniową oraz v_1, \dots, v_m – liniowo niezależnym układem wektorów w V . Wykaż, że istnieje dokładnie 2^m układów ortonormalnych (e_1, \dots, e_m) takich, że $\text{lin}(v_1, \dots, v_j) = \text{lin}(e_1, \dots, e_j)$, dla wszystkich $j \in \{1, \dots, m\}$.

12.2 Uzupełnienie. Metoda najmniejszych kwadratów

Zacznijmy od układów równań¹. Jeśli $A \in M_{m \times n}(\mathbb{R})$ oraz $b \in \mathbb{R}^m$, to układ $Ax = b$ może nie mieć rozwiązania $x \in \mathbb{R}^n$. Jeśli jednak rozważamy strukturę przestrzeni euklidesowej $(\mathbb{R}^n, \langle \cdot, \cdot \rangle)$, to możemy zastanawiać się czy jest jakiś wektor, który byłby „najbliższy” rozwiązaniu. Rozważmy przykład:

$$\begin{bmatrix} 1 & 2 \\ 1 & 3 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 4 \\ 5 \\ 6 \end{bmatrix} \iff x_1 \cdot \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + x_2 \cdot \begin{bmatrix} 2 \\ 3 \\ 0 \end{bmatrix} = \begin{bmatrix} 4 \\ 5 \\ 6 \end{bmatrix}.$$

Nietrudno widzieć, że równanie to nie ma rozwiązań, bo wektor $(4, 5, 6)$ nie jest kombinacją liniową wektorów $a_1 = (1, 1, 0)$, $a_2 = (2, 3, 0)$. Zobaczmy rysunek w przestrzeni \mathbb{R}^3



Zaznaczona „płaszczyzna” to przestrzeń rozpięta przez kolumny a_1, a_2 macierzy naszego układu. Każdy wektor na tej płaszczyźnie jest postaci $x_1 a_1 + x_2 a_2$, dla pewnych $x_1, x_2 \in \mathbb{R}$. To są właśnie wektory Ax . Linia przerywaną oznaczony jest wektor opisujący $Ax - b$. Niestety może on nigdy nie być zerowy. Ale skoro jesteśmy w przestrzeni euklidesowej, to możemy próbować minimalizować wyrażenie $\|Ax - b\|$.

Przypomnijmy Obserwację z wykładu, która mówiła, że jeśli W jest podprzestrzenią przestrzeni euklidesowej V oraz v' jest rzutem prostopadłym wektora $v \in V$ na W , wówczas $\|v - v'\| = \min_{w \in W} \|v - w\|$.

W naszym przypadku podprzestrzeń $W = \{Ax, \text{ gdzie } x \in \mathbb{R}^3\}$ jest przestrzenią kolumnową macierzy A . Zatem wektor \hat{x} , który minimalizuje $\|Ax - b\|$ jest rzutem wektora b na podprzestrzeń kolumnową A .

Jak wyznaczyć ten rzut? Popatrzmy na tzw. wektor błędu $b - A\hat{x}$. Wektor ten musi być prostopadły do każdej kolumny a_1, \dots, a_n macierzy A , co możemy zapisać schematycznie w postaci:

$$\begin{cases} \langle a_1^T, b - A\hat{x} \rangle = 0 \\ \vdots \\ \langle a_n^T, b - A\hat{x} \rangle = 0 \end{cases},$$

co w przypadku standardowego iloczynu skalarnego przepisać można do postaci $A^T(b - A\hat{x}) = 0$. Innymi słowy, wektor \hat{x} jest w tym przypadku rozwiązaniem tzw. równania normalnego $A^T A \hat{x} = A^T b$, powstającego przez pomnożenie wyjściowego równania przez A^T . Zachodzi następujące twierdzenie.

Obserwacja 12.6

Jeśli równanie $Ax = b$ nie ma rozwiązań w przestrzeni euklidesowej $(\mathbb{R}^n, \langle \cdot, \cdot \rangle_{st})$, to $\|Ax - b\|$ jest minimalna dla $x = \hat{x}$, będącego rozwiązaniem równania $A^T A \hat{x} = A^T b$. Macierz $A^T A$ jest odwracalna wtedy i tylko wtedy, gdy kolumny A są liniowo niezależne. Wówczas:

$$\hat{x} = (A^T A)^{-1} A^T b.$$

Zachęcam Czytelnika do dowodu tego faktu. Proszę przy okazji pokazać, że jednorodny układ równań liniowych zadane macierzami A oraz $A^T A$ mają ten sam zbiór rozwiązań.

¹Ten dodatek napisany jest na podstawie znakomitej książki Gilberta Stranga „Linear algebra and its applications”.

Przejdźmy na koniec do naszego przykładu. Rzut prostopadły (standardowy) wektora $b = (4, 5, 6)$ na przestrzeń kolumnową macierzy o kolumnach $(1, 1, 0)^T$ oraz $(2, 3, 0)^T$ to po prostu rzut prostopadły na przestrzeń $\text{lin}((1, 0, 0), (0, 1, 0))$, i jest to oczywiście $(4, 5, 0)$. Potwierdza się to przy wyliczeniach proponowanych przez fakt wyżej:

$$A^T A = \begin{bmatrix} 1 & 1 & 0 \\ 2 & 3 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 \\ 1 & 3 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 5 \\ 5 & 13 \end{bmatrix}$$

$$\hat{x} = (A^T A)^{-1} A^T b = \begin{bmatrix} 13 & -5 \\ -5 & 2 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 0 \\ 2 & 3 & 0 \end{bmatrix} \cdot \begin{bmatrix} 4 \\ 5 \\ 6 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \end{bmatrix}, \quad A\hat{x} = \begin{bmatrix} 1 & 2 \\ 1 & 3 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 4 \\ 5 \\ 0 \end{bmatrix}.$$

Co to wszystko ma wspólnego z zastosowaniami matematyki? Załóżmy, że wykonaliśmy serię eksperymentów i oczekujemy, że wynik b będzie funkcją liniową argumentu t . Szukamy zatem prostej o równaniu $C + Dt = b$. Przykłady:

- Wyznaczamy odległość satelity od Marsa. W tym przypadku t jest zmienną czasową, a b – dystansem od planety. O ile nie wyłączy się silnika i o ile grawitacja nie będzie bardzo silna, satelita powinien poruszać się z mniej więcej stałą prędkością v , czyli $b = b_0 + vt$.
- W teorii elastyczności badamy rozszerzenie b struny obciążonej określoną masą t . O ile obciążenie nie jest nadmierne, rozważa się liniową zależność $b = C + Dt$.
- Koszt produkcji t książek jest niemal liniową funkcją $b = C + Dt$, gdzie C jest kosztem przygotowania, a D jest kosztem każdej dodatkowej książki

Jak wyznaczyć C i D ? Jeśli nie ma błędu, wówczas każde dwa pomiary b powinny określać prostą $b = C + Dt$. Ale jeśli jest błąd, wówczas musimy być gotowi na znajdowanie „optymalnej” prostej przybliżającej te rozwiązania. Wykonujemy te pomiary dostając układ równań:

$$\begin{cases} C + Dt_1 & = b_1 \\ C + Dt_2 & = b_2 \\ & \vdots \\ C + Dt_m & = b_m. \end{cases}$$

Ten układ zawiera nadmiarowe informacje: mamy m równań i tylko dwie niewiadome C, D . Jeśli wystąpiły błędy, układ ten nie ma rozwiązania. Jeśli wystąpiły, to najlepsze rozwiązanie $\hat{x} = (\hat{C}, \hat{D})^T$, przybliżające błąd (w normie $\|\cdot\|_{st}$) ma minimalizować wyrażenie:

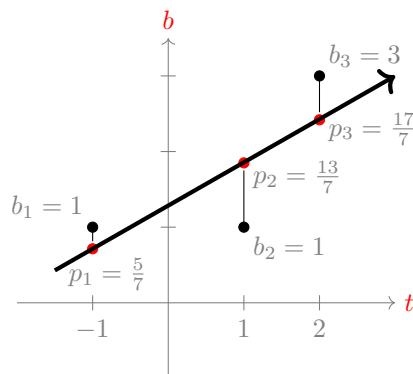
$$\|Ax - b\| = (b_1 - C - Dt_1)^2 + \dots + (b_m - C - Dt_m)^2.$$

Wektor $p = (p_1, p_2, p_3) = A\hat{x}$ jest „tak blisko” $b = (b_1, b_2, b_3)$, jak to możliwe, tzn. suma kwadratów różnic $p_i - b_i$ jest minimalna.

Dla przykładu: biorąc $b_1 = 1, t_1 = 1, b_2 = 1, t_2 = 1, b_3 = 3, t_3 = 2$ widzimy, że punkty (b_i, t_i) nie leżą na jednej prostej. Istnieje jednak prosta $\hat{C} + \hat{D}t = \frac{9}{7} + \frac{4}{7}t$, która „najlepiej” przybliży rozwiązania układu

$$\begin{cases} C - D & = 1 \\ C + D & = 1 \\ C + 2D & = 3 \end{cases}$$

Rysunek poniżej przedstawia uzyskaną prostą i „punkty pomiarowe”.



Rozdział 13

Macierze form dwuliniowych. Kryterium Sylwestera

Na ostatnim wykładzie omówione zostały podstawowe metody wyznaczania bazy ortogonalnej przestrzeni euklidesowej. Dziś przekonamy się, że z iloczynem skalarnym i układem wektorów przestrzeni euklidesowej $(V, \langle \cdot, \cdot \rangle)$ związać można pewne bardzo istotne macierze, tzw. macierze formy dwuliniowej. W języku wyznaczników związanych z tymi macierzami sformułujemy kryterium wyróżniające iloczyny skalarne spośród funkcji $h : V \times V \rightarrow \mathbb{R}$ liniowych ze względu na każdą ze zmiennych i symetrycznych, nazwane imieniem Jacoba Sylwestera. Zaczniemy od następującej definicji.

Definicja 13.1

Niech $h : V \times V \rightarrow K$ będzie formą dwuliniową na przestrzeni V i niech $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$ będzie bazą przestrzeni V . MACIERZĄ FORMY h W BAZIE \mathcal{A} nazywamy macierz:

$$G(h; \mathcal{A}) = [h(\alpha_i, \alpha_j)] \in M_n(K)$$

Rozważmy kilka przykładów

- Niech $h : \mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R}$ dana będzie wzorem $h((x_1, x_2, x_3), (y_1, y_2, y_3)) = x_1y_1 + x_2y_2 - x_3y_3$. Wówczas:

$$G(h; st) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}.$$

- Niech $h : \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}$ dana będzie wzorem $h((x_1, x_2), (y_1, y_2)) = x_1y_1 - 2x_1y_2 + 3x_2y_1 + 5x_2y_2$. Wówczas jeśli $\mathcal{A} = ((1, 1), (0, 4))$, to

$$G(h; st) = \begin{bmatrix} 1 & -2 \\ 3 & 5 \end{bmatrix}, \quad G(h; \mathcal{A}) = \begin{bmatrix} 7 & 12 \\ 32 & 80 \end{bmatrix}.$$

Przypominamy formułę wynikającą z definicji macierzy formy.

Obserwacja 13.1

Jeśli $h : V \times V \rightarrow K$ jest formą dwuliniową, zaś $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$ jest bazą przestrzeni V , to dla dowolnych wektorów $\alpha = x_1\alpha_1 + \dots + x_n\alpha_n$, oraz $\beta = y_1\alpha_1 + \dots + y_n\alpha_n$ przestrzeni V zachodzi:

$$h(\alpha, \beta) = [x_1 \quad \dots \quad x_n] \cdot G(h; \mathcal{A}) \cdot \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}.$$

Dowód. Z rozważań prowadzonych na poprzednich wykładach wiemy, że jeśli $G(h; \mathcal{A}) = [a_{ij}]$, to

$$\begin{aligned} [x_1 \ \dots \ x_n] \cdot G(h; \mathcal{A}) \cdot \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} &= \sum_{1 \leq i, j \leq n} a_{ij} x_i y_j = \sum_{1 \leq i, j \leq n} h(\alpha_i, \alpha_j) x_i y_j = \sum_{1 \leq j \leq n} h(x_1 \alpha_1 + \dots + x_n \alpha_n, \alpha_j) y_j \\ &= h(x_1 \alpha_1 + \dots + x_n \alpha_n, y_1 \alpha_1 + \dots + y_n \alpha_n) = h(\alpha, \beta). \end{aligned}$$

□

Odnotujmy kluczowy wniosek dla iloczynów skalarnych.

Wniosek 13.1

Niech h będzie formą dwuliniową na przestrzeni skończenie wymiarowej V nad ciałem \mathbb{R} . Wówczas następujące warunki są równoważne:

- (i) dla pewnej bazy \mathcal{A} przestrzeni V mamy $G(h; \mathcal{A}) = I$,
- (ii) h jest iloczynem skalarnym na V .

Dowód. Implikacja (ii) \Rightarrow (i) jest oczywista — wystarczy przyjąć, że \mathcal{A} jest bazą ortonormalną (V, h) . W drugą stronę — aby pokazać, że h jest iloczynem skalarnym, należy uzasadnić jej symetryczność i dodatnią określoność. Symetria jest oczywista, bo dla dowolnych wektorów $\alpha = x_1 \alpha_1 + \dots + x_n \alpha_n$, $\beta = y_1 \alpha_1 + \dots + y_n \alpha_n$ przestrzeni V mamy

$$h(\alpha, \beta) = [x_1 \ \dots \ x_n] \cdot I \cdot \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = \sum_{1 \leq i \leq n} x_i y_i = [y_1 \ \dots \ y_n] \cdot I \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = h(\beta, \alpha).$$

Dodatnia określoność również jest jasna. Dla dowolnego niezerowego wektora $\alpha = x_1 \alpha_1 + \dots + x_n \alpha_n$ mamy

$$h(\alpha, \alpha) = [x_1 \ \dots \ x_n] \cdot I \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \sum_{1 \leq i \leq n} x_i^2.$$

Ostatnia suma jest większa od 0, bowiem co najmniej jeden z wyrazów x_i jest niezerowy. □

Intuicja powyższego faktu jest następująca: wszystkie iloczyny skalarne na przestrzeni wymiaru n nad ciałem \mathbb{R} działają „w ten sam sposób” jak iloczyn standardowy, oczywiście w pewnej bazie. Innymi słowy, jeśli $\alpha_1, \dots, \alpha_n$ jest bazą ortonormalną przestrzeni euklidesowej $(V, \langle \cdot, \cdot \rangle)$, to dla dowolnych wektorów $\alpha = x_1 \alpha_1 + \dots + x_n \alpha_n$, $\beta = y_1 \alpha_1 + \dots + y_n \alpha_n$ przestrzeni V zachodzi:

$$\langle \alpha, \beta \rangle = x_1 y_1 + \dots + x_n y_n.$$

Widzimy już jak ważnym wątkiem naszych rozważań będzie badanie macierzy form dwuliniowych w różnych bazach. Odnotujmy podstawową uwagę.

Obserwacja 13.2

Niech $h : V \times V \rightarrow K$ będzie formą dwuliniową oraz niech $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$, $\mathcal{B} = (\beta_1, \dots, \beta_n)$ będą bazami przestrzeni V . Jeśli $A = G(h; \mathcal{A})$, $B = G(h; \mathcal{B})$ oraz $C = M(\text{id})_{\mathcal{B}}^{\mathcal{A}}$, to

$$B = C^T A C.$$

Dowód. Niech $C = [c_{ij}]$. Opiszmy wyraz z i -tego wiersza i j -tej kolumny macierzy $C^T A C$. Nietrudno widzieć (bo tak jest dla dowolnego iloczynu trzech macierzy), że wyraz ten powstaje przez przemnożenie i -tego wiersza macierzy C^T , macierzy A oraz j -tej kolumny macierzy C . Mnożymy więc w rezultacie współrzędne i -tego oraz j -tego elementu bazy \mathcal{B} zapisanych w bazie \mathcal{A} przez macierz formy h w bazie \mathcal{A} . A zatem zgodnie z poprzednią uwagą wyraz ten wynosi $h(\beta_i, \beta_j)$. Dokładnie tej samej postaci jest także z definicji wyraz w i -tym wierszu i j -tej kolumnie macierzy $B = G(h; \mathcal{B})$. □

Uwaga ta motywuje wprowadzenie następującego ważnego pojęcia.

Definicja 13.2

Mówimy, że macierze $A, B \in M_n(K)$ są KONGRUENTNE NAD K jeśli istnieje macierz odwracalna $C \in M_n(K)$ taka, że

$$B = C^T A C.$$

Przykład. Macierze $A_1, A_2 \in M_3(K)$ postaci

$$A_1 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \quad A_2 = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

są kongruentne nad dowolnym ciałem charakterystyki różnej od 2, ponieważ:

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

Obserwacja 13.3

Macierze $A, B \in M_n(K)$ są kongruentne wtedy i tylko wtedy, gdy są macierzami tej samej formy dwuliniowej (w pewnych bazach).

Dowód. Jeśli istnieje forma dwuliniowa $h : V \times V \rightarrow K$ na n wymiarowej przestrzeni liniowej V nad K oraz bazy \mathcal{A}, \mathcal{B} przestrzeni V takie, że $A = G(h, \mathcal{A})$, $B = G(h, \mathcal{B})$, to macierze A, B są kongruentne na mocy uwagi wyżej. Na odwrót, niech $B = C^T A C$, dla pewnej macierzy odwracalnej $C \in M_n(K)$. Niech $A = [a_{ij}]$. Określmy formę dwuliniową $h : K^n \times K^n \rightarrow K$ warunkiem $G(h; st) = A$. To znaczy:

$$h((x_1, \dots, x_n), (y_1, \dots, y_n)) = \sum_{i,j}^n a_{ij} x_i y_j.$$

Niech $B = (\beta_1, \dots, \beta_n)$ będzie bazą przestrzeni K^n zadaną przez $M(\text{id})_{\mathcal{B}}^{st} = C$. Wówczas z dowodu poprzedniej uwagi wynika natychmiast, że $B = G(h; \mathcal{B})$. \square

Dla (rozważanej wcześniej) formy $h : \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}$ zadanej wzorem

$$h((x_1, x_2), (y_1, y_2)) = x_1 y_1 - 2x_1 y_2 + 3x_2 y_1 + 5x_2 y_2$$

wyliczyliśmy

$$G(h; st) = \begin{bmatrix} 1 & -2 \\ 3 & 5 \end{bmatrix}, \quad G(h; \mathcal{A}) = \begin{bmatrix} 7 & 12 \\ 32 & 80 \end{bmatrix},$$

więc macierze te są kongruentne nad \mathbb{R} . Przestrzeń (\mathbb{R}^2, h) nie jest jednak euklidesowa, bo $G(h; st)$ nie jest nawet symetryczna.

Kongruentność, podobnie jak podobieństwo, jest relacją równoważności w zbiorze $M_n(K)$. Rzeczywiście:

- zwrotność relacji kongruencji wynika z faktu, że $A = I^T A I$,
- symetryczność relacji kongruencji wynika z tego, że jeśli $A = C^T B C$, dla pewnej macierzy odwracalnej C , to $B = (C^{-1})^T A C^{-1}$,
- przechodniość relacji kongruencji wynika z tego, że jeśli $A = X^T B X$, $B = Y^T C Y$, to

$$A = X^T Y^T C Y X = (Y X)^T C (Y X).$$

Stwierdzenie kiedy macierze są kongruentne może być bardzo trudnym zadaniem. Jednym z celów całego kursu jest dokonać takiej klasyfikacji dla macierzy symetrycznych nad ciałem liczb rzeczywistych i zespolonych. Sformułujmy teraz kilka warunków koniecznych, aby macierze były kongruentne.

Obserwacja 13.4

Jeśli macierze $A, B \in M_n(K)$ są kongruentne nad K , to:

- $r(A) = r(B)$,
- $\det(A) \cdot \det(B)$ jest kwadratem w ciele K .

Dowód. Skoro istnieje macierz odwracalna C taka, że $B = C^T A C$, to $r(B) = r(C^T A C) = r(A)$, bo mnożenie przez macierz odwracalną (z dowolnej strony) nie zmienia rzędu. Mamy również:

$$\det(A) \cdot \det(B) = \det(A) \cdot \det(C^T A C) = (\det A \cdot \det C)^2.$$

□

Intuicyjnie, problem badania kongruencji macierzy nad K jest tym trudniejszy, im więcej elementów ciała K nie można utożsamić za pomocą kwadratu. Stąd na przykład klasyfikacja macierzy kongruentnych nad ciałem \mathbb{Q} jest bardzo skomplikowana, w porównaniu do ciał \mathbb{C} oraz \mathbb{R} . Przede wszystkim jednak, interesuje nas ograniczenie się do badania form i macierzy symetrycznych. Przypomnijmy definicję.

Wniosek 13.2

Jeśli h jest iloczynem skalarnym na przestrzeni liniowej V ciałem \mathbb{R} oraz \mathcal{A} jest dowolną bazą V , to

$$\det G(h; \mathcal{A}) > 0.$$

Dowód. Rzeczywiście, macierz $G(h; \mathcal{A})$ jest kongruentna do macierzy identycznościowej. Innymi słowy, istnieje macierz odwracalna $C \in M_n(\mathbb{R})$, że:

$$G(h; \mathcal{A}) = C^T \cdot I \cdot C.$$

Wynika stąd, że $\det G(h; \mathcal{A}) = (\det C)^2 > 0$, bo C jest macierzą odwracalną.

□

Definicja 13.3: Macierz symetryczna

Macierz $A \in M_n(K)$ nazywamy SYMETRYCZNĄ, jeśli $A = A^T$, czyli jeśli $A = [a_{ij}]$, to $a_{ij} = a_{ji}$, dla dowolnych $1 \leq i, j \leq n$.

Na dzisiejszym wykładzie skupimy się jedynie nad wykorzystaniem pojęcia kongruencji do rozróżnienia macierzy iloczynów skalarnych spośród wszystkich macierzy symetrycznych form dwuliniowych na skończone wymiarowych przestrzeniach liniowych nad ciałem \mathbb{R} .

Definicja 13.4: Główne minory wiodące macierzy kwadratowej

Dla dowolnej macierzy $A \in M_n(K)$ oraz dla $i = 1, \dots, n$ niech $A^{(i)} \in M_i(K)$ oznacza macierz powstałą z A przez usunięcie ostatnich $n - i$ wierszy i ostatnich $n - i$ kolumn. Wyznacznik tej macierzy nazywamy WIODĄCYM MINOREM GŁÓWNYM STOPNIA i macierzy A .

Przykład dla macierzy symetrycznej $A \in M_3(\mathbb{R})$ w postaci

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

mamy 3 główne minory wiodące, równe $\det A^{(1)} = 4$, $\det A^{(2)} = 1$, $\det A^{(3)} = 3$, będące wyznacznikami macierzy:

$$A^{(1)} = [4], \quad A^{(2)} = \begin{bmatrix} 4 & 1 \\ 1 & 2 \end{bmatrix}, \quad A^{(3)} = \begin{bmatrix} 4 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

Twierdzenie 13.1: Kryterium Sylwestera

Niech h będzie symetryczną formą dwuliniową na n -wymiarowej przestrzeni liniowej V nad ciałem \mathbb{R} oraz niech $A = G(h; \mathcal{A})$ będzie macierzą tej formy w bazie \mathcal{A} . Następujące warunki są równoważne:

- (i) h jest iloczynem skalarnym na przestrzeni V ,
- (ii) $\det A^{(i)} > 0$, dla $i = 1, \dots, n$.

Przykład: niech $h : \mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R}$, gdzie

$$h((x_1, x_2, x_3), (y_1, y_2, y_3)) = (4 - r)x_1y_1 + x_1y_2 + x_1y_3 + x_2y_1 + x_2y_2 + x_2y_3 + x_3y_1 + x_3y_2 + rx_3y_3.$$

- Dla jakich $r \in \mathbb{R}$ funkcja h jest iloczynem skalarnym na \mathbb{R}^3 ?
- Dla jakich $r \in \mathbb{R}$ funkcja $h|_W$ jest iloczynem skalarnym na przestrzeni $W = \text{lin}((1, 1, -1), (0, 1, 1))$?

Rozwiązanie. Funkcja h jest dwuliniowa i symetryczna, a zatem możemy zastosować kryterium Sylwestera. Bierzemy bazę standardową $(\epsilon_1, \epsilon_2, \epsilon_3)$ przestrzeni \mathbb{R}^3 i macierz o wyrazach $h(\epsilon_i, \epsilon_j)$ postaci:

$$\begin{bmatrix} 4 - r & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & r \end{bmatrix}.$$

Aby macierz ta była macierzą iloczynu skalarnego potrzeba i wystarcza, aby:

$$4 - r > 0, \quad \begin{vmatrix} 4 - r & 1 \\ 1 & 1 \end{vmatrix} > 0,$$

oraz

$$\begin{vmatrix} 4 - r & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & r \end{vmatrix} > 0.$$

A zatem dostajemy układ warunków:

$$4 > r, \quad 3 > r, \quad -r^2 + 4r - 3 = -(r - 1)(r - 3) > 0.$$

Stąd h jest iloczynem skalarnym na \mathbb{R}^3 wtedy i tylko wtedy, gdy $r \in (1, 3)$.

Odpowiedzmy na drugie pytanie. Bierzemy

$$\alpha_1 = (1, 1, -1), \quad \alpha_2 = (0, 1, 1).$$

Wyznaczamy macierz o wyrazach $h(\alpha_i, \alpha_j)$. Ma ona postać:

$$\begin{bmatrix} 3 & 3 - r \\ 3 - r & 3 + r \end{bmatrix}.$$

A zatem jest ona macierzą iloczynu skalarnego wtedy i tylko wtedy, gdy $3(3 + r) - (3 - r)^2 > 0$, co daje $-r^2 + 9r > 0$, czyli $r(9 - r) > 0$. A zatem w tym przypadku $r \in (0, 9)$.

Dowód. Dowiedzimy (i) \Rightarrow (ii). Jeśli h jest iloczynem skalarnym na V , to oczywiście A jest macierzą formy h w bazie $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$. Ograniczenie $h|_{W_i}$ do podprzestrzeni $W_i = \text{lin}(\alpha_1, \dots, \alpha_i)$ jest iloczynem skalarnym na przestrzeni W_i , dla każdego $i = 1, \dots, n$. A zatem macierze $A^{(i)} = G(\alpha_1, \dots, \alpha_i)$ mają dodatnie wyznaczniki, na mocy Wniosku 13.2.

Zakładamy, że dla bazy \mathcal{A} macierz $G(h; \mathcal{A})$ ma dodatnie główne minory wiodące. Rozważmy postać blokową powyższej macierzy postaci:

$$G(h; \mathcal{A}) = \begin{bmatrix} G(h; \mathcal{A})^{(n-1)} & \alpha \\ \alpha^T & b \end{bmatrix}, \quad \text{gdzie } \alpha \in \mathbb{R}^{n-1}, b \in \mathbb{R}.$$

Główne minory wiodące macierzy $G(h; \mathcal{A})^{(n-1)}$ są głównymi minorami wiodącymi macierzy $G(h; \mathcal{A})$. Zatem z założenia indukcyjnego forma $g = h|_{W_{n-1}}$ jest iloczynem skalarnym na przestrzeni $W_{n-1} = \text{lin}(\alpha_1, \dots, \alpha_{n-1})$.

Jeśli $\mathcal{C} = (\beta_1, \dots, \beta_{n-1})$ jest bazą W_{n-1} , to w bazie $\mathcal{B} = (\beta_1, \dots, \beta_{n-1}, \alpha_n)$ przestrzeni V macierz $G(h; \mathcal{B})$ ma postać:

$$G(h; \mathcal{B}) = \begin{bmatrix} G(g; \mathcal{C}) & \gamma \\ \gamma^T & b \end{bmatrix}, \text{ gdzie } \gamma \in \mathbb{R}^{n-1}$$

i skoro $G(h; \mathcal{B}) = C^T G(h; \mathcal{A}) C$, dla pewnej macierzy odwracalnej C , to wobec założenia $\det G(h; \mathcal{A}) > 0$ (to jeden z minorów) mamy $\det G(h; \mathcal{B}) > 0$. Przyjmijmy dalej, że baza \mathcal{C} jest ortonormalna.

Wobec tego macierz formy h w bazie $(\beta_1, \dots, \beta_{n-1}, \alpha_n)$ ma postać

$$G(h; \mathcal{B}) = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & a_1 \\ 0 & 1 & 0 & \dots & 0 & a_2 \\ 0 & 0 & 1 & \dots & 0 & a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & a_{n-1} \\ a_1 & a_2 & a_3 & \dots & a_{n-1} & b \end{bmatrix}.$$

Niech P^T będzie macierzą powstałą przez zamianę ostatniego wiersza w macierzy identyfikacyjnej $I_n \in M_n(\mathbb{R})$ na wiersz

$$[-a_1 \quad -a_2 \quad -a_3 \quad \dots \quad -a_{n-1} \quad 1],$$

czyli macierzą postaci:

$$P^T = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ -a_1 & -a_2 & -a_3 & \dots & -a_{n-1} & 1 \end{bmatrix}.$$

Łatwo sprawdzić patrząc jakie operacje elementarne związane są z mnożeniem przez P oraz P^T , że iloczyn $P^T X$ powstaje z X przez

- odjęcie od ostatniego wiersza wiersza pierwszego pomnożonego przez $-a_1$,
- odjęcie od ostatniego wiersza wiersza drugiego pomnożonego przez $-a_2$,
- ...,
- odjęcie od ostatniego wiersza wiersza $n - 1$ -wszego pomnożonego przez $-a_{n-1}$.

Analogicznie macierz XP powstaje z X przez operacje kolumnowe:

- odjęcie od ostatniej kolumny kolumny pierwszej pomnożonej przez $-a_1$,
- odjęcie od ostatniej kolumny kolumny drugiej pomnożonej przez $-a_2$,
- ...,
- odjęcie od ostatniej kolumny kolumny $n - 1$ -wszej pomnożonej przez $-a_{n-1}$.

Wynika stąd, że istnieje $d \in \mathbb{R}$, że:

$$P^T G(h; \mathcal{B}) P = \begin{bmatrix} I_{n-1} & 0 \\ 0 & d \end{bmatrix}.$$

Skoro zaś uzyskana macierz jest to kolejna macierz formy h (znowu dokonaliśmy zmiany bazy), to musi mieć dodatni wyznacznik (bo największy minor jest dodatni). Zatem $d > 0$ i h jest w sposób oczywisty iloczynem skalarnym. \square

W dalszych wykładach wrócimy do pojęcia macierzy formy dwuliniowej i do ważnej relacji kongruencji. Wpierw jednak skupimy się na geometrycznych aspektach macierzy układów wektorów na przestrzeni z iloczynem skalarnym — tak zwanej macierzy Grama. Poprowadzą nas one w kierunku pojęcia objętości.

13.1 Zadania do samodzielnej pracy

Zadania ilustrujące umiejętności niezbędne do zaliczenia przedmiotu oznaczone są symbolem ♠. Przy tych zadaniach dodany jest opis umiejętności, które sprawdzają.

1. (♠ Wyznaczanie macierzy formy dwuliniowej w bazie)

- Rozpatrzmy formę dwuliniową $h : \mathbb{R}^4 \times \mathbb{R}^4 \rightarrow \mathbb{R}$ zadaną wzorem:

$$h((x_1, x_2, x_3, x_4), (y_1, y_2, y_3, y_4)) = 2x_1y_1 - x_1y_2 + 5x_1y_4 + 6x_2y_3 - 4x_2y_4 + 7x_3y_3 - 3x_4y_1 + 8x_4y_3.$$

Niech $\mathcal{A} = ((2, 0, 1, 0), (0, 3, 0, 1), (1, 2, 0, 0), (0, 0, 1, 1))$. Znajdź $G(h; st)$ oraz $G(h; \mathcal{A})$.

- Niech $h : \mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R}$ będzie formą dwuliniową, która w bazie $\mathcal{A} = ((1, 1, 0), (0, 1, 0), (1, 1, 1))$ ma macierz

$$G(h; \mathcal{A}) = \begin{bmatrix} 1 & 4 & 2 \\ 1 & 3 & 0 \\ 0 & 5 & 2 \end{bmatrix}$$

Znajdź macierz $G(h; \mathcal{B})$ dla bazy $\mathcal{B} = ((2, 3, 1), (3, 4, 2), (0, 1, 2))$ oraz znajdź wzór formy h .

2. (♠ Stosowanie kryterium Sylwestera)

- Rozpatrzmy funkcję $\langle \cdot, \cdot \rangle : \mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R}$ daną wzorem

$$\langle (x_1, x_2, x_3), (y_1, y_2, y_3) \rangle = (4-r)x_1y_1 + x_1y_2 + x_1y_3 + x_2y_1 + x_2y_2 + x_2y_3 + x_3y_1 + x_3y_2 + rx_3y_3.$$

Dla jakich $r \in \mathbb{R}$ funkcja $\langle \cdot, \cdot \rangle$ jest iloczynem skalarnym na przestrzeni \mathbb{R}^3 ? Dla jakich $r \in \mathbb{R}$ funkcja $\langle \cdot, \cdot \rangle|_{W \times W}$ jest iloczynem skalarnym na $W = \text{lin}((1, 0, 0), (1, 1, 0))$?

- W przestrzeni euklidesowej \mathbb{R}^4 podprzestrzeń W dana jest równaniem $2x_1 + 2x_2 - x_3 + x_4 = 0$. Niech $h : \mathbb{R}^4 \times \mathbb{R}^4 \rightarrow \mathbb{R}$ będzie formą dwuliniową daną wzorem

$$h((x_1, x_2, x_3, x_4), (y_1, y_2, y_3, y_4)) = x_1y_1 + x_3y_3 + x_4y_4.$$

Czy $h|_{W \times W}$ jest iloczynem skalarnym na przestrzeni W ?

- Rozpatrzmy funkcję $h : \mathbb{R}^4 \times \mathbb{R}^4 \rightarrow \mathbb{R}$ daną wzorem

$$f((x_1, x_2, x_3, x_4), (y_1, y_2, y_3, y_4)) = 3x_1y_1 + ax_1y_2 + ax_2y_1 + 3x_2y_2 + ax_3y_3 + x_3y_4 + bx_4y_3 + 3x_4y_4.$$

Dla jakich wartości parametrów a, b funkcja ta jest iloczynem skalarnym na przestrzeni \mathbb{R}^4 ? Dla $a = b = 1$ znajdź bazę prostopadłą przestrzeni $(W, f|_{W \times W})$, gdzie W jest zadana równaniem $x_1 + 3x_2 + x_3 + x_4 = 0$.

- Dane są macierze symetryczne $A, B \in M_n(\mathbb{R})$ spełniające $B = C^T A C$ dla pewnej macierzy odwrotnej $C \in M_n(\mathbb{R})$. Przypuśćmy, że A spełnia kryterium Sylwestera, czyli jej główne minory wiodące $\det A^{(i)}$ są dodatnie, dla $i = 1, \dots, n$. Czy wynika stąd, że B spełnia kryterium Sylwestera?
- Założmy, że macierz symetryczna $A \in M_n(\mathbb{R})$ jest macierzą iloczynu skalarnego. Czy wynika stąd, że macierz A^2 jest macierzą iloczynu skalarnego? Czy zachodzi implikacja odwrotna?
- Niech $A \in M_n(\mathbb{R})$. Wykaż, że macierz $A^T A$ jest macierzą iloczynu skalarnego.
- Założmy, że macierz $A = [a_{ij}] \in M_n(\mathbb{R})$ jest macierzą iloczynu skalarnego. Wykaż, że dla $n \leq 3$ wynika stąd, że także macierz $B = [b_{ij}]$ o wyrazach $b_{ij} = |a_{ij}|$ jest macierzą iloczynu skalarnego.
- Rozważmy, dla $a \in \mathbb{R}$ macierz $A_n \in M_n(\mathbb{R})$ postaci:

$$A_n = \begin{bmatrix} a & 1 & 0 & \dots & 0 & 0 \\ 1 & a & 1 & \dots & 0 & 0 \\ 0 & 1 & a & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & a & 1 \\ 0 & 0 & 0 & \dots & 1 & a \end{bmatrix}.$$

Kiedy A_n jest macierzą iloczynu skalarnego?

- Macierz $A = [a_{ij}] \in M_n(\mathbb{R})$ spełnia warunki $a_{ii} = 1$ oraz $a_{ij} = a$, dla $i \neq j$ oraz pewnego $a \in \mathbb{R}$. Kiedy A jest macierzą iloczynu skalarnego?

13.2 Uzupełnienie. Kryterium Sylwestera ze skryptu

Czytelnika pracującego ze skrypcem wydziałowym zachęcam do prześledzenia alternatywnego dowodu tam przedstawionego, opartego o pojęcie macierzy Grama, które dopiero poznamy. Poniżej przedstawiam ten dowód w wersji nieco rozszerzonej w języku już poznanych faktów.

Nie dowodzimy implikacji (i) \Rightarrow (ii), ponieważ bez pojęcia kongruencji nie mamy chwilowo dobrego narzędzia do wykazania, że wyznacznik macierzy iloczynu skalarnego w dowolnej bazie jest dodatni. W skrypcie czyni się to za pomocą macierzy Grama, w pewnym sensie powtarzając główne argumenty wypisane wyżej w sposób ogólny — mianowicie pokazujemy, że macierz Grama jest iloczynem macierzy $C^T C$, dla pewnej macierzy odwracalnej C .

Dowodzimy implikację (ii) \Rightarrow (i) przez indukcję po wymiarze n przestrzeni V . Trzeba jedynie pokazać, że h jest dodatnio określona, tzn. $h(\alpha, \alpha) > 0$ dla dowolnego $0 \neq \alpha \in V$.

Dla $n = 1$ teza jest jasna, bo $V = \text{lin}(\alpha_1)$ oraz $A = [a_{11}]$, przy czym $a_{11} > 0$ (bo to jest $\det A^{(1)}$). A zatem dla każdego niezerowego $a\alpha_1 \in V$

$$h(a\alpha_1, a\alpha_1) = a^2 a_{11} > 0.$$

Zatem h jest iloczynem skalarnym. Załóżmy, że dowodzona implikacja jest prawdziwa dla $n - 1$. Dowodzimy tezę dla n . Niech $W = \text{lin}(\alpha_1, \dots, \alpha_{n-1})$.

Z założenia indukcyjnego $(W, h|_W)$ jest przestrzenią euklidesową. Niech $\beta_1, \dots, \beta_{n-1}$ będzie bazą prostopadłą W otrzymaną z bazy $\alpha_1, \dots, \alpha_{n-1}$ metodą Grama-Schmidta. W szczególności $h(\beta_i, \beta_j) = 0$, dla $i \neq j$. Definiujemy wektor β_n postaci:

$$\beta_n = \alpha_n - \sum_{i=1}^{n-1} \frac{h(\alpha_n, \beta_i)}{h(\beta_i, \beta_i)} \beta_i.$$

Wówczas nowo zdefiniowany wektor spełnia $h(\beta_n, \beta_i) = 0$, dla wszystkich $i = 1, \dots, n - 1$ (sprawdzamy to podobnie jak w dowodach z poprzedniego wykładu, stosując dwuliniowość oraz symetryczność h).

Rozpatrzmy teraz macierz $B = [b_{ij}] \in M_n(\mathbb{R})$, gdzie $b_{ij} = h(\beta_i, \beta_j)$, dla $i, j = 1, \dots, n$, czyli:

$$B = \begin{bmatrix} h(\beta_1, \beta_1) & 0 & \dots & 0 \\ 0 & h(\beta_2, \beta_2) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & h(\beta_n, \beta_n) \end{bmatrix}.$$

Teraz udowodnimy coś intuicyjnie jasnego, ale technicznego w dowodzie. W istocie macierz B powstaje z macierzy A przez wykonanie operacji elementarnych typu (1) na wierszach i kolumnach (dodawanie wiersza pomnożonego przez stałą do innego wiersza, analogicznie dla kolumn). Dlaczego to wystarczy?

Otóż operacje elementarne typu (1) nie zmieniają wyznacznika. Więc $\det A = \det B$. Wiemy też, że B jest diagonalna i ma na diagonalu wyrazy $h(\beta_1, \beta_1), \dots, h(\beta_n, \beta_n)$. Ich iloczyn to wyznacznik macierzy B . Wiemy z założenia indukcyjnego, że $h(\beta_1, \beta_1), \dots, h(\beta_{n-1}, \beta_{n-1})$ są dodatnie, bo $h|_W$ jest iloczynem skalarnym i korzystamy z (i) \Rightarrow (ii). Ostatni element diagonalni $h(\beta_n, \beta_n)$ też musi być jednak dodatni, bo z (ii) mamy

$$\det A^{(n)} = \det A > 0.$$

To oznacza, że h jest iloczynem skalarnym, bowiem biorąc $0 \neq \alpha = x_1\beta_1 + \dots + x_n\beta_n$ i korzystając z warunku $h(\beta_i, \beta_j) = 0$, dla $i \neq j$, mamy

$$h(\alpha, \alpha) = \sum_{i=1}^n x_i^2 h(\beta_i, \beta_i) > 0,$$

co zakończy dowód.

Dowód wymaga dwóch kroków. Po pierwsze zajmijmy się macierzą $X_{\mathcal{A}}$ mającą w wierszach wektory $\alpha_1, \dots, \alpha_n$ bazy \mathcal{A} , a następnie dopiero popatrzymy na minory macierzy A . Po pierwsze twierdzimy, że macierz $X_{\mathcal{B}}$ mająca w kolejnych wierszach wektory¹ β_1, \dots, β_n powstaje z macierzy $X_{\mathcal{A}}$ poprzez operacje typu (1) na wierszach.

Pokażmy przez indukcję ze względu na m , że sprowadzenie pierwszych m wierszy macierzy $X_{\mathcal{A}}$ do pierwszych m wierszy macierzy $X_{\mathcal{B}}$ wymaga stosowania jedynie operacji (1) na pierwszych m wierszach.

Dla $m = 1$ ² mamy $\beta_1 = \alpha_1$, więc teza jest jasna, bo nie trzeba wykonywać żadnych operacji. Natomiast jeśli wiemy, że jest tak dla $m - 1$, to bierzemy macierz $X_{\mathcal{A}}$. Zamieniamy pierwsze $m - 1$ wierszy z założenia indukcyjnego na $\beta_1, \dots, \beta_{m-1}$ operacjami (1) wykonywanymi w obrębie $m - 1$ pierwszych wierszy. Dostajemy macierz $X_{\mathcal{A}'}$ której pierwsze $m - 1$ wierszy to $\beta_1, \dots, \beta_{m-1}$, a kolejne to $\alpha_m, \dots, \alpha_n$.

$$\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_{m-1} \\ \alpha_m \\ \vdots \\ \alpha_n \end{bmatrix} \xrightarrow{m-1 \text{ operacji}} \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_{m-1} \\ \alpha_m \\ \vdots \\ \alpha_n \end{bmatrix}$$

Z twierdzenia o ortogonalizacji oraz z definicji wektora β_n mamy

$$\beta_m = \alpha_m - c_1\beta_1 - c_2\beta_2 - \dots - c_{m-1}\beta_{m-1}, \text{ gdzie } c_i = h(\alpha_m, \beta_i)/h(\beta_i, \beta_i).$$

A zatem od wiersza m -tego $X_{\mathcal{A}'}$ odejmujemy c_1 razy pierwszy wiersz. Od uzyskanego m -tego wiersza odejmujemy c_2 razy drugi wiersz itd, na końcu odejmując c_{m-1} razy wiersz $m - 1$ od wiersza m -tego. W rezultacie dostajemy macierz $X_{\mathcal{B}'}$, która w pierwszych m wierszach ma wektory β_1, \dots, β_m , uzyskane przez stosowanie operacji (1) na pierwszych m wierszach, a dalej (jeśli są) wektory $\alpha_{m+1}, \dots, \alpha_n$. To kończy dowód indukcyjny, że $X_{\mathcal{B}}$ można uzyskać z $X_{\mathcal{A}}$ przez operacje (1).

Niech A' będzie macierzą formy h w bazie $\beta_1, \dots, \beta_{m-1}, \alpha_m, \dots, \alpha_n$ oraz niech B' niech będzie macierzą formy h bazy $\beta_1, \dots, \beta_m, \alpha_{m+1}, \dots, \alpha_n$.

Do dowodu, że B jest uzyskiwana z A przez operacje elementarne wierszowe i kolumnowe typu (1) wystarczy pokazać, że B' można uzyskać z A' przez operacje typu (1) zmieniające jedynie wiersze i kolumny o indeksie m . Wynika to z faktu, że macierze A' oraz B' mają identyczne wyrazy poza m -tym wierszem i m -tą kolumną, bo układy $\beta_1, \dots, \beta_{m-1}, \alpha_m, \dots, \alpha_n$ oraz $\beta_1, \dots, \beta_m, \alpha_{m+1}, \dots, \alpha_n$ różnią się tylko m -tym elementem. Zobaczmy:

$$A' = \begin{bmatrix} & \dots & h(\beta_1, \beta_{m-1}) & h(\beta_1, \alpha_m) & \dots \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ h(\beta_{m-1}, \beta_1) & \dots & h(\beta_{m-1}, \beta_{m-1}) & h(\beta_{m-1}, \alpha_m) & \vdots & h(\beta_{m-1}, \alpha_n) \\ h(\alpha_m, \beta_1) & \dots & h(\alpha_m, \beta_{m-1}) & h(\alpha_m, \alpha_m) & \vdots & h(\alpha_m, \alpha_n) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ & \dots & h(\alpha_n, \beta_{m-1}) & h(\alpha_n, \alpha_m) & \dots \end{bmatrix}$$

$$B' = \begin{bmatrix} & \dots & h(\beta_1, \beta_{m-1}) & h(\beta_1, \beta_m) & \dots \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ h(\beta_{m-1}, \beta_1) & \dots & h(\beta_{m-1}, \beta_{m-1}) & h(\beta_{m-1}, \beta_m) & \vdots & h(\beta_{m-1}, \alpha_n) \\ h(\beta_m, \beta_1) & \dots & h(\beta_m, \beta_{m-1}) & h(\beta_m, \beta_m) & \vdots & h(\beta_m, \alpha_n) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ & \dots & h(\alpha_n, \beta_{m-1}) & h(\alpha_n, \beta_m) & \dots \end{bmatrix}$$

¹Mała delikatność: jeszcze nie wiemy czy układ β_1, \dots, β_n jest bazą V , bo nie wiemy czy h to iloczyn skalarny na V .

²Intuicja: wykonujemy na kolejnych wierszach $X_{\mathcal{A}}$ te same operacje, co przy ortogonalizacji G-S, choć nie wiemy czy h to iloczyn skalarny. Na i -tym wierszu stosujemy $i - 1$ operacji (1), co zamienia α_i na $\beta_i = \alpha_i - c_1\beta_1 - \dots - c_{i-1}\beta_{i-1}$.

Wiemy, że $\beta_m = \alpha_m - c_1\beta_1 - c_2\beta_2 - \dots - c_{m-1}\beta_{m-1}$, dla znanych c_i . Macierz $X_{B'}$ uzyskiwaliśmy z $X_{A'}$ przez wykonanie $m - 1$ operacji odjęcia od m -tego wiersza wielokrotności c_i wiersza i -tego. Aby uzyskać macierz B' z A' trzeba wykonać $2m - 2$ operacji typu (1). Pierwsze dwie to: odjęcie od m -tego wiersza c_1 razy wiersz pierwszy, potem od kolumny m -tej trzeba odjąć c_1 razy kolumnę pierwszą. Oto rezultat:

$$\begin{bmatrix} \dots & h(\beta_1, \beta_{m-1}) & h(\beta_1, \alpha_m - c_1\beta_1) & \dots \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ h(\beta_{m-1}, \beta_1) & \dots & h(\beta_{m-1}, \beta_{m-1}) & h(\beta_{m-1}, \alpha_m - c_1\beta_1) & \vdots & h(\beta_{m-1}, \alpha_n) \\ h(\alpha_m - c_1\beta_1, \beta_1) & \dots & h(\alpha_m - c_1\beta_1, \beta_{m-1}) & h(\alpha_m - c_1\beta_1, \alpha_m - c_1\beta_1) & \vdots & h(\alpha_m - c_1\beta_1, \alpha_n) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \dots & h(\alpha_n, \beta_{m-1}) & h(\alpha_n, \alpha_m - c_1\beta_1) & \dots \end{bmatrix}$$

Następne dwie operacje to: od m -tego wiersza odjąć c_2 razy drugi wiersz i potem od m -tej kolumny odjąć c_2 razy kolumnę drugą:

$$\begin{bmatrix} \dots & h(\beta_1, \alpha_m - c_1\beta_1 - c_2\beta_2) & \dots \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ h(\alpha_m - c_1\beta_1 - c_2\beta_2, \beta_2) & \dots & h(\alpha_m - c_1\beta_1 - c_2\beta_2, \alpha_m - c_1\beta_1 - c_2\beta_2) & \vdots & h(\alpha_m - c_1\beta_1 - c_2\beta_2, \alpha_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \dots & h(\alpha_n, \alpha_m - c_1\beta_1 - c_2\beta_2) & \dots \end{bmatrix},$$

i tak dalej. W ten sposób, korzystając z liniowości h względem każdej ze zmiennych dostajemy żadaną postać B' . Zauważmy wszak, że m -ty wiersz macierzy B' to kombinacja liniowa c_1 razy pierwszy wiersz + c_2 razy drugi wiersz + \dots + c_{m-1} razy $m - 1$ -wszy wiersz. Podobnie dla kolumn. Zatem pokazaliśmy, że B można dostać z A operacjami elementarnymi typu (1), co kończy dowód implikacji (ii) \Rightarrow (i).

* * *

Dowód był stosunkowo zawily, ale stanowi ilustrację poglądu, że można przeprowadzić go bez pojęcia kongruencji. Jeszcze inny elementarny dowód przytacza dr Krych w notatkach z Analizy II, cytując rozumowanie prof. Musielaka: <https://www.mimuw.edu.pl/~krych/matematyka/AM2skrypt/am2cz02L.pdf>.

Idea jest taka, by patrzeć na tzw. formę kwadratową q (definicję poznamy wkrótce) stowarzyszoną z formą dwuliniową h postaci $q((x_1, \dots, x_n)) = h((x_1, \dots, x_n), (x_1, \dots, x_n))$. Aby stwierdzić czy forma h jest dodatnio określona wystarczy pokazać, że $q(x) > 0$, dla każdego niezerowego $x \in \mathbb{R}^n$. A zatem badamy wyrażenie postaci $q((x_1, \dots, x_n)) = \sum_{1 \leq i, j \leq n} a_{ij}x_i x_j$, dla pewnych $a_{ij} \in \mathbb{R}$, przy czym $a_{ij} = a_{ji}$, bo

forma h jest symetryczna. Myślmy o q jak funkcji kwadratowej f zmiennej x_1 . Warunkiem koniecznym i dostatecznym na to, by $f(x_1) > 0$ jest $a_{11} > 0$ oraz to, by wyróżnik tego trójmianu był ujemny. Jak się okazuje, wyróżnik ten zależy jedynie od $n - 1$ zmiennych x_2, \dots, x_n , a nie zależy od x_1 . To pozwala przeprowadzić rozumowanie indukcyjne. Szczegóły — we wspomnianym wyżej tekście dra Krycha.

Ostatnia metoda ilustruje następującą myśl: czasem łatwiej pomyśleć niż korzystać z gotowych kryteriów. Rozważmy, dla $a \in \mathbb{R}$ macierz $A_n \in M_n(\mathbb{R})$ postaci:

$$A_n = G(h_a, st) = \begin{bmatrix} a & 1 & 0 & \dots & 0 & 0 \\ 1 & a & 1 & \dots & 0 & 0 \\ 0 & 1 & a & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & a & 1 \\ 0 & 0 & 0 & \dots & 1 & a \end{bmatrix}.$$

Czy h jest iloczynem skalarnym? Wystarczy sprawdzić dla jakich a dla dowolnego niezerowego wektora $v \in \mathbb{R}^n$ mamy $h_a(v, v) > 0$. Robimy to (niemal) wprost z definicji: niech $v = (v_1, \dots, v_n)$. Wtedy dla dowolnego a wartość $h_a(v, v) = v^T A_n v$ równa jest:

$$a(v_1^2 + \dots + v_n^2) + 2v_1v_2 + 2v_2v_3 + \dots + 2v_{n-1}v_n = (a-2)(v_1^2 + \dots + v_n^2) + v_1^2 + (v_1 + v_2)^2 + \dots + (v_{n-1} + v_n)^2 + v_n^2 > 0.$$

Jest więc jasne, że dla $a > 2$ forma h_a jest iloczynem skalarnym. Można też rozwiązać ten punkt korzystając z kryterium Sylwestera, wyprowadzając z rozwinięcia Laplace'a rekurencję $|A_n| = a|A_{n-1}| - |A_{n-2}|$.

13.3 Trivia. Inne kątomierze, czyli o aksonometrii

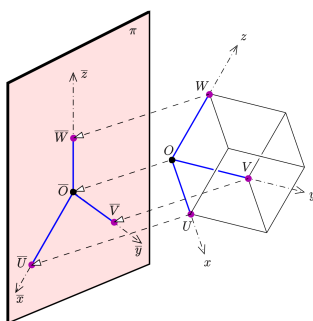
Widzieliście Państwo kiedyś kątomierz izometryczny? Czy wiecie, że na trzy rozłożone palce rzutować można sześcian? Jaki jest kąt pomiędzy $(1,0)$ a $(0,1)$ i jaki jest kierunek ich „dwusiecznej”? Spróbujmy powiązać te tematy tak, by uzyskać jeszcze jedno spojrzenie na iloczyny skalarne. Spójrzmy na poniższy rysunek



Twierdźmy, że kierunki wyznaczone przez trzy palce, z których żadne dwa nie są połączone wyznaczają sześcian. Co to znaczy? Jest to poglądowe wysłowienie następującego rezultatu, wspomnianego przez samego Hugona Steinhausa w *Kalejdoskopie Matematycznym*

Twierdzenie 13.2: Pohlke (1853), dowód – Schwarz (1864)

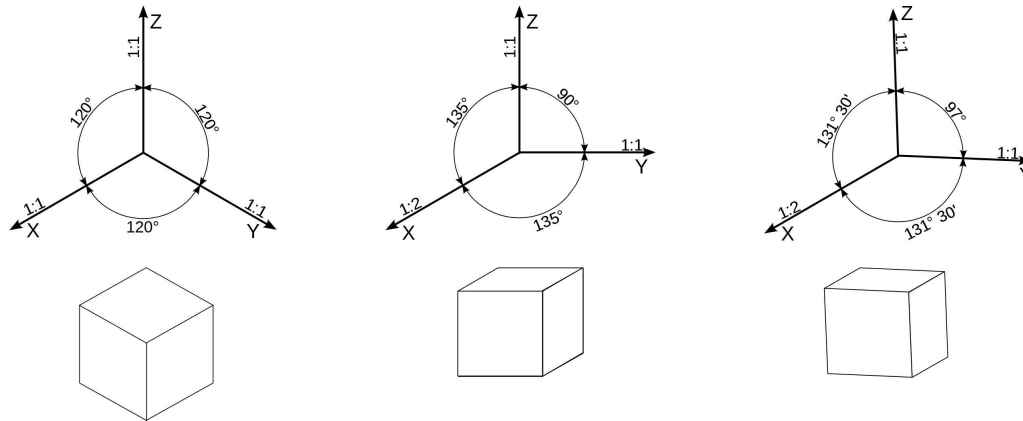
Trzy dowolne odcinki na płaszczyźnie wychodzące z jednego punktu, które nie leżą na jednej prostej można rozważać jako rzut równoległy krawędzi sześcianu.



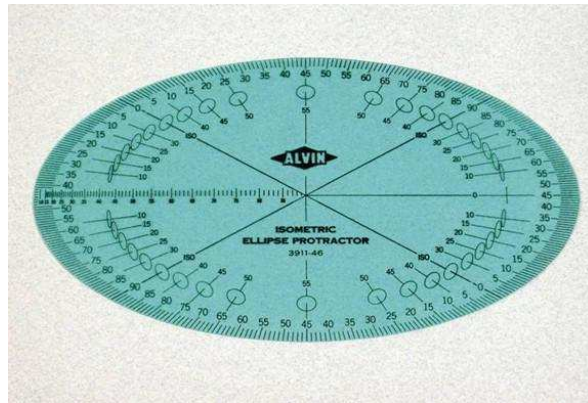
Nietrudny dowód tego rezultatu, wymagający jednak wiedzy, którą dopiero posiadziemy, znaleźć można w tekście <https://www.heldermann-verlag.de/jgg/jgg22/j22h2manf.pdf>. Postawmy sobie jednak inny problem: co to twierdzenie mówi o naszej percepcji kątów? Czy dla pary wektorów nierównoległych znaleźć można zawsze iloczyn skalarny taki, że kąt między nimi będzie prosty? Zagadnienia te mają związki z zastosowaniami matematyki w tzw. aksonometrii — dziedzinie mającej zastosowanie w rysunku technicznym, a dotyczącej odwzorowań przestrzeni na płaszczyznę z wykorzystaniem prostokątnego układu osi. Dąży się przy tym do zachowania prawdziwych wymiarów rzutowanych obiektów, przynajmniej w jednym wybranym kierunku. Trzy podstawowe typy aksonometrii to:

- izometria – wszystkie osie układu prostokątnego w przestrzeni tworzą jednakowy kąt z rzutnią i ich obrazy ulegają jednakowemu skrótovi – na rzutni powstaje obraz trzech osi tworzących pomiędzy sobą kąty po 120° , często na rysunkach izometrycznych pomija się wpływ skrótu;
- dimetria – dwie z osi układu prostokątnego tworzą z rzutnią jednakowe kąty (bywa, że są do niej równoległe), a zatem układ współrzędnych posiada jednakowe skróty na co najmniej dwóch osiach,
- trimetria (anizometria) – każda z osi układu prostokątnego tworzy z rzutnią inny kąt i podlega innemu skrótovi.

Oto przykładowe rzuty sześciianu i kąty pomiędzy ścianami przy tych typach odwzorowań.



Do rzutowania aksonometrycznego używa się specjalnych kątomierzy, podobnych do tego poniżej.



Aby dodać do naszej opowieści nieco matematyki, rozwiążmy prosty problem.

Zadanie. W przestrzeni euklidesowej $(\mathbb{R}^2, \langle \cdot, \cdot \rangle)$ dane są wektory $(1, 0)$, $(0, 1)$. Jaki może być, w zależności od $\langle \cdot, \cdot \rangle$ kąt między tymi wektorami? Opisać iloczyn skalarny na przestrzeni $(\mathbb{R}^2, \langle \cdot, \cdot \rangle)$, dla których kąt pomiędzy $(1, 0)$, a $(1, 1)$ wynosi $\frac{\pi}{2}$.

ROZWIĄZANIE. Ogólna postać iloczynu skalarnego wektorów $\langle (x_1, x_2), (y_1, y_2) \rangle$ w \mathbb{R}^2 to:

$$a_{11}x_1y_1 + a_{12}x_1y_2 + a_{21}x_2y_1 + a_{22}x_2y_2,$$

gdzie $a_{12} = a_{21} = \langle (1, 0), (0, 1) \rangle$, $a_{11} > 0$, $a_{11}a_{22} - a_{12}a_{21} > 0$.

Na przykład $\langle (1, 0), (0, 1) \rangle = 0$ zachodzi tylko dla iloczynu skalarnego postaci $ax_1y_1 + bx_2y_2$, dla $a, b > 0$. Natomiast $\langle (1, 0), (1, 1) \rangle = 0$ zachodzi tylko dla iloczynu skalarnego postaci $ax_1y_1 - ax_1y_2 - ax_2y_1 + bx_2y_2$, dla $b > a > 0$. A zatem $(1, 0)$ i $(1, 1)$ są prostopadłe dla każdego iloczynu skalarnego postaci:

$$\langle (x_1, x_2), (y_1, y_2) \rangle = x_1y_1 - x_1y_2 - x_2y_1 + bx_2y_2, \quad \text{gdzie } b > 1.$$

Zatem $\langle (1, 0), (0, 1) \rangle = -1$, $\|(1, 0)\| = \sqrt{\langle (1, 0), (1, 0) \rangle} = 1$ oraz $\|(0, 1)\| = \sqrt{\langle (0, 1), (0, 1) \rangle} = \sqrt{b}$. W zależności od b , cosinus kąta pomiędzy $(1, 0)$, a $(0, 1)$ wynosi:

$$\frac{-1}{\sqrt{b}} \in (-1, 0).$$

■

Pytania do samodzielnego przemyślenia.

1. Czy kąt pomiędzy $(1, 0)$, $(0, 1)$ może dla pewnego $\langle \cdot, \cdot \rangle$ wynosić π ?
2. Czy niezależnie od $\langle \cdot, \cdot \rangle$ suma kątów w trójkącie to π ?
3. Czy trójkąty wyznaczają iloczyny skalarny w \mathbb{R}^2 ?

Rozdział 14

Przestrzenie euklidesowe afiniczne

Celem dzisiejszego wykładu jest zaprezentowanie najprostszych pojęć związanych z rozważaniem na rzeczywistej przestrzeni afinicznej struktury przestrzeni euklidesowej. Uzyskamy w ten sposób „dostęp” do wielu obiektów geometrycznych znanych ze szkoły. Zaczniemy od intuicyjnej definicji.

Definicja 14.1: Przestrzeń euklidesowa afiniczna

Parę $(H, \langle \cdot, \cdot \rangle)$, gdzie H jest skończone wymiarową przestrzenią afiniczną nad ciałem \mathbb{R} , oraz gdzie $\langle \cdot, \cdot \rangle : T(H) \times T(H) \rightarrow \mathbb{R}$ jest iloczynem skalarnym na $T(H)$ nazywamy PRZESTRZENIĄ EUKLIDESOWĄ AFINICZNĄ

Każda przestrzeń euklidesowa liniowa jest przestrzenią euklidesową afiniczną. Jeśli M jest podprzestrzenią przestrzeni euklidesowej afinicznej $(H, \langle \cdot, \cdot \rangle)$, to $(M, \langle \cdot, \cdot \rangle|_{T(M)})$ jest przestrzenią euklidesową afiniczną. Każda podprzestrzeń afiniczna przestrzeni euklidesowej liniowej jest przestrzenią euklidesową afiniczną.

Definicja 14.2: Odległość

Niech $(H, \langle \cdot, \cdot \rangle)$ będzie przestrzenią euklidesową afiniczną. ODLEGŁOŚCIĄ punktów $p, q \in H$ nazywamy długość wektora łączącego p z q . Liczbę tę oznaczamy $\rho(p, q)$. Zatem $\rho(p, q) = \|\vec{pq}\|$.

To, co najczęściej nazywa się w potocznym matematycznym języku odległością euklidesową¹ punktów $a = (a_1, \dots, a_n)$, $b = (b_1, \dots, b_n)$ w przestrzeni \mathbb{R}^n , to norma wektora $\|\vec{ab}\|$ przy standardowym iloczynie skalarnym dana wzorem:

$$\rho(a, b) = \sqrt{(b_1 - a_1)^2 + \dots + (b_n - a_n)^2}.$$

Na przykład w \mathbb{R}^2 ze standardowym iloczynem skalarnym odległość punktów $(2, 3, 1)$, $(6, 1, 4)$ to

$$\rho((2, 3, 1), (6, 1, 4)) = \sqrt{(6 - 2)^2 + (1 - 3)^2 + (4 - 1)^2} = \sqrt{29}.$$

Obserwacja 14.1

Dla punktów p, q, r przestrzeni euklidesowej afinicznej mamy:

- (a) $\rho(p, q) = 0 \Leftrightarrow p = q$,
- (b) $\rho(p, q) = \rho(q, p)$,
- (c) $\rho(p, q) + \rho(q, r) \geq \rho(p, r)$.

Dowód. Dowód (a): $\|\vec{pq}\| = 0 \Leftrightarrow \vec{pq} = 0 \Leftrightarrow p = q$. Punkt (b) wynika z formuły: $\|\vec{pq}\| = \|\vec{qp}\|$, a punkt (c) z nierówności trójkąta dla przestrzeni euklidesowych liniowych, czyli: $\|\alpha\| + \|\beta\| \geq \|\alpha + \beta\|$. Mamy zaś: $\vec{pr} = \vec{pq} + \vec{qr}$, więc $\|\vec{pq}\| + \|\vec{qr}\| \geq \|\vec{pr}\|$. \square

¹Niestandardowe odległości euklidesowe wyrażają się „jakościowo” identycznymi wzorami. Dla nas umiejętność liczenia niestandardowej odległości w \mathbb{R}^n jest istotna, natomiast z szerszego punktu widzenia stosuje się jednolite nazewnictwo.

Na kolejnych latach studiów dowiedzie się Państwo, że wiele innych rzeczywistych funkcji (niż zdefiniowana wyżej norma różnicy wektorów zadająca „odległość euklidesową”) na zbiorze $X \times X$ spełnia warunki (a)-(c) podane wyżej. Funkcje te nazywane są ogólnie METRYKAMI. Wiele z nich można określić w \mathbb{R}^n . Przykładem jest „metryka miejska” – dla punktów $a = (a_1, \dots, a_n), b = (b_1, \dots, b_n)$ w \mathbb{R}^n określamy:

$$\mu(a, b) = |a_1 - b_1| + \dots + |a_n - b_n|.$$

Można liczyć „odległości” obiektów niekoniecznie przypominających geometryczne, na przykład definiując

- METRYKĘ RZĘDU: dla $A, B \in M_n(K)$ określamy $d(A, B) = r(A - B)$,
- ODLEGŁOŚĆ HAMMINGA dwóch słów długości n nad alfabetem Σ : liczba pozycji, na których słowa się różnią. Na przykład odległość między ZAGRABIĆ i ZATRĄBIĆ wynosi 3,
- ODLEGŁOŚĆ GEODEZYJNĄ wierzchołków grafu: długość najkrótszej ścieżki (geodezyjnej) między wierzchołkami grafu (jeśli dwa wierzchołki nie są połączone to za ich odległość przyjmuje się ∞).

Czytelnika zainteresowanego tym tematem, a także jego analitycznymi konsekwencjami, odsyłamy do artykułu dr Krycha w Delcie: <https://www.deltami.edu.pl/temat/matematyka/geometria/2019/03/25/2019-04-delta-metryka.pdf>, a także do wykładu z Topologii 1.

Kluczowym narzędziem w przestrzeniach euklidesowych liniowych są bazy prostopadłe i bazy ortonormalne. Podobnie jest w przestrzeniach afinicznych. Chcemy bowiem (choćby) wyznaczać odległości nie tylko pomiędzy punktami, ale też pomiędzy podzbiórami, a zwłaszcza podprzestrzeniami afinicznymi – na przykład odległość punktu od prostej, odległość dwóch prostych równoległych itd.

Definicja 14.3: Prostopadły układ bazowy

Mówimy, że układ $p_0; \alpha_1, \dots, \alpha_n$ jest UKŁADEM BAZOWYM PROSTOPADŁYM (odpowiednio: UKŁADEM BAZOWYM ORTONORMALNYM) przestrzeni euklidesowej afinicznej (H, \langle, \rangle) , jeśli p_0 jest punktem przestrzeni H oraz $\alpha_1, \dots, \alpha_n$ jest bazą prostopadłą (odpowiednio: bazą ortonormalną) przestrzeni euklidesowej liniowej $(T(H), \langle, \rangle)$.

Z istnienia baz prostopadłych i baz ortonormalnych przestrzeni euklidesowych liniowych wynika oczywiście istnienie układów bazowych prostopadłych i układów bazowych ortonormalnych przestrzeni euklidesowych afinicznych.

Przykład. Niech $H = \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid 2x_1 + x_2 - 3x_3 = 4\}$ i niech \langle, \rangle_{st} będzie standardowym iloczynem skalarnym w \mathbb{R}^3 . Wówczas

$$(1, 2, 0); (1, 1, 1), (4, -5, 1)$$

jest prostopadłym układem bazowym przestrzeni afinicznej $(H, \langle, \rangle|_H)$, a układ

$$(1, 2, 0); \frac{1}{\sqrt{3}}(1, 1, 1), \frac{1}{\sqrt{42}}(4, -5, 1)$$

jest ortonormalnym układem bazowym tej przestrzeni.

Definicja 14.4: Rzut i symetria prostopadła

Niech (H, \langle, \rangle) będzie przestrzenią euklidesową afiniczną i niech $M \subseteq H$ będzie podprzestrzenią przestrzeni H . RZUTEM PROSTOPADŁYM na M nazywamy przekształcenie afiniczne $f : H \rightarrow H$ będące rzutem na M wzdłuż $q + T(M)^\perp$, dla pewnego $q \in H$. SYMETRIĄ PROSTOPADŁĄ względem M nazywamy przekształcenie afiniczne $g : H \rightarrow H$ będące symetrią względem M wzdłuż $q + T(M)^\perp$, dla pewnego $q \in H$.

Zgodnie z definicją afinicznych rzutów i symetrii równoległych wybór punktu $q \in H$ jest tu dowolny; wynik jest ten sam dla wszystkich q . Zauważmy też, że jeśli $f : H \rightarrow H$ jest afinicznym rzutem prostopadłym na M , to jego pochodna $f' : T(H) \rightarrow T(H)$ jest rzutem prostopadłym na $T(M)$, podobnie dla symetrii.

Obserwacja 14.2

Niech $M \subseteq H$ będzie podprzestrzenią przestrzeni euklidesowej afinicznej $(H, \langle \cdot, \cdot \rangle)$. Niech p_0 będzie punktem przestrzeni M , niech $\alpha_1, \dots, \alpha_k$ będzie bazą prostopadłą przestrzeni $T(M)$ i niech $\alpha_{k+1}, \dots, \alpha_n$ będzie bazą przestrzeni $T(M)^\perp$. Wówczas dla każdego wektora $\alpha \in T(H)$ rzut prostopadły punktu $p_0 + \alpha$ na M wynosi:

$$p_0 + \frac{\langle \alpha, \alpha_1 \rangle}{\langle \alpha_1, \alpha_1 \rangle} \alpha_1 + \dots + \frac{\langle \alpha, \alpha_k \rangle}{\langle \alpha_k, \alpha_k \rangle} \alpha_k,$$

a obraz punktu $p_0 + \alpha$ w symetrii prostopadłej względem M wynosi:

$$p_0 + \left(\frac{\langle \alpha, \alpha_1 \rangle}{\langle \alpha_1, \alpha_1 \rangle} \alpha_1 + \dots + \frac{\langle \alpha, \alpha_k \rangle}{\langle \alpha_k, \alpha_k \rangle} \alpha_k \right) - \left(\frac{\langle \alpha, \alpha_{k+1} \rangle}{\langle \alpha_{k+1}, \alpha_{k+1} \rangle} \alpha_{k+1} + \dots + \frac{\langle \alpha, \alpha_n \rangle}{\langle \alpha_n, \alpha_n \rangle} \alpha_n \right).$$

Jeśli powyższy układ bazowy jest ortonormalny, to rzut prostopadły punktu $p_0 + \alpha$ na M wynosi:

$$p_0 + \langle \alpha, \alpha_1 \rangle \alpha_1 + \dots + \langle \alpha, \alpha_k \rangle \alpha_k,$$

zaś obraz punktu $p_0 + \alpha$ w symetrii prostopadłej względem M wynosi:

$$p_0 + (\langle \alpha, \alpha_1 \rangle \alpha_1 + \dots + \langle \alpha, \alpha_k \rangle \alpha_k) - (\langle \alpha, \alpha_{k+1} \rangle \alpha_{k+1} + \dots + \langle \alpha, \alpha_n \rangle \alpha_n).$$

Definicja 14.5: Odległość punktu od przestrzeni afinicznej

Niech $(H, \langle \cdot, \cdot \rangle)$ będzie przestrzenią euklidesową afiniczną. ODLEGŁOŚCIĄ PUNKTU $p \in H$ DO PODPRZESTRZENI $M \subseteq H$ nazywamy odległość punktu p od jego rzutu prostopadłego na M . Odległość tę oznaczamy $\rho(p, M)$.

Obserwacja 14.3

Jeśli M jest podprzestrzenią przestrzeni euklidesowej afinicznej H i p jest punktem przestrzeni H , to dla każdego punktu $q \in M$ zachodzi $\rho(p, q) \geq \rho(p, M)$.

Dowód. Niech p_0 będzie rzutem prostopadłym punktu p na M . Mamy zatem $\rho(p, M) = \rho(p, p_0)$. Przy tym $\overrightarrow{pp_0} \perp \overrightarrow{p_0q}$, dla każdego $q \in M$. Zatem z twierdzenia Pitagorasa $\|\overrightarrow{pq}\|^2 = \|\overrightarrow{pp_0}\|^2 + \|\overrightarrow{p_0q}\|^2$, a stąd

$$\rho(p, q) = \|\overrightarrow{pq}\| \geq \|\overrightarrow{pp_0}\| = \rho(p, p_0).$$

□

Przykład. W przestrzeni afinicznej $(\mathbb{R}^3, \langle \cdot, \cdot \rangle_{st})$ rozpatrzmy: prostą $M = (2, 3, 1) + \text{lin}((1, 2, -1))$ i punkt $p = (5, 4, 7) \notin M$. Mamy $p = (2, 3, 1) + (3, 1, 6)$, a więc rzut prostopadły p na M to

$$(2, 3, 1) + \frac{\langle (3, 1, 6), (1, 2, -1) \rangle}{\langle (1, 2, -1), (1, 2, -1) \rangle} (1, 2, -1) = (2, 3, 1) - \frac{1}{6} (1, 2, -1) = \left(\frac{11}{6}, \frac{16}{6}, \frac{7}{6} \right).$$

A zatem odległość punktu p od prostej M równa jest

$$\rho \left((5, 4, 7), \left(\frac{11}{6}, \frac{16}{6}, \frac{7}{6} \right) \right) = \left\| \frac{1}{6} (19, 8, 35) \right\| = \frac{\sqrt{1650}}{6} = \sqrt{\frac{275}{6}}$$

Udowodnijmy teraz wynikający z powyższych obserwacji wzór na odległość punktu od podprzestrzeni wymiaru o 1 mniejszego niż cała przestrzeń afiniczna. Uogólnia on znany ze szkoły wzór na odległość punktu od prostej na płaszczyźnie.

Obserwacja 14.4

W przestrzeni euklidesowej afinicznej $H = \mathbb{R}^n$ ze standardowym iloczynem skalarnym niech M będzie podprzestrzenią opisaną równaniem $a_1x_1 + \dots + a_nx_n = b$, gdzie $(a_1, \dots, a_n) \neq (0, \dots, 0)$. Wówczas odległość punktu $p = (y_1, \dots, y_n)$ od M wynosi:

$$\rho(p, M) = \frac{|a_1y_1 + \dots + a_ny_n - b|}{\sqrt{a_1^2 + \dots + a_n^2}}.$$

Wzór ten uogólnia się bez zmian na dowolną przestrzeń euklidesową afiniczną $(H, \langle \cdot, \cdot \rangle)$ i jej podprzestrzeń M wymiaru $\dim H - 1$ pod warunkiem, że

$$\begin{aligned} M &= \{p_0 + x_1\alpha_1 + \dots + x_n\alpha_n \mid a_1x_1 + \dots + a_nx_n = b\}, \\ p &= p_0 + y_1\alpha_1 + \dots + y_n\alpha_n \end{aligned}$$

dla pewnego ortonormalnego układu bazowego $p_0, \alpha_1, \dots, \alpha_n$ w H .

Dowód. Niech q będzie rzutem prostopadłym punktu p na M . Wówczas, jak wiemy z wcześniejszych wykładów $\rho(p, M) = \|p - q\|$. Jak wiadomo $p - q \in T(M)^\perp$. Przestrzeń $T(M)$ jest opisana równaniem $a_1x_1 + \dots + a_nx_n = 0$, a zatem wektor z $\mathbb{R}^n = T(H)$ należy do $T(M)$ wtedy i tylko wtedy gdy jest on prostopadły do wektora (a_1, \dots, a_n) (bo mamy standardowy iloczyn skalarny). Stąd

$$T(M) = \text{lin}((a_1, \dots, a_n))^\perp \quad \text{oraz} \quad T(M)^\perp = (\text{lin}((a_1, \dots, a_n))^\perp)^\perp = \text{lin}((a_1, \dots, a_n)).$$

Niech $q = (z_1, \dots, z_n)$. Skoro $p - q \in T(M)^\perp$, to istnieje takie $t \in \mathbb{R}$, że $p - q = t(a_1, \dots, a_n) = (y_1 - z_1, \dots, y_n - z_n)$. A zatem

$$\rho(p, M) = \|p - q\| = |t| \sqrt{a_1^2 + \dots + a_n^2}. \quad (\spadesuit)$$

Wyliczmy teraz wartość t :

$$\begin{aligned} t(a_1^2 + \dots + a_n^2) &= \langle t(a_1, \dots, a_n), (a_1, \dots, a_n) \rangle = \langle (y_1 - z_1, \dots, y_n - z_n), (a_1, \dots, a_n) \rangle = \\ &= a_1y_1 + \dots + a_ny_n - a_1z_1 - \dots - a_nz_n = a_1y_1 + \dots + a_ny_n - b, \end{aligned}$$

przy czym równość $a_1z_1 + \dots + a_nz_n = b$ wynika stąd, że $q \in M$. A więc

$$t = \frac{a_1y_1 + \dots + a_ny_n - b}{a_1^2 + \dots + a_n^2}.$$

Wstawiamy wyliczone $|t|$ do (\spadesuit) dostajemy

$$\rho(p, M) = \left| \frac{a_1y_1 + \dots + a_ny_n - b}{a_1^2 + \dots + a_n^2} \right| \cdot \sqrt{a_1^2 + \dots + a_n^2} = \frac{|a_1y_1 + \dots + a_ny_n - b|}{\sqrt{a_1^2 + \dots + a_n^2}}.$$

□

Definicja 14.6: Odległość podzbiorów przestrzeni afinicznej

Niech X, Y będą niepustymi podzbiórmi przestrzeni afinicznej euklidesowej $(H, \langle \cdot, \cdot \rangle)$. Odległością podzbiorów X, Y nazywamy liczbę:

$$\rho(X, Y) = \inf_{x \in X, y \in Y} \|x - y\|.$$

Ta definicja jest bardzo ogólna i dopuszcza sytuacje, gdy rozłączne podzbiory mają odległość zero. Wystarczy na prostej \mathbb{R} ze standardową odległością zadaną przez wartość bezwzględną przyjąć $X = \{0\}$ oraz $Y = (0, 1)$. W przypadku jednak, gdy X, Y są przestrzeniami afinicznymi taka sytuacja nie może mieć miejsca. Zachodzi następujący fakt.

Obserwacja 14.5

Załóżmy, że $A, B \neq \emptyset$ są podprzestrzeniami afinicznej przestrzeni euklidesowej X . Jeżeli $A \cap B = \emptyset$, to istnieje prosta $L \subseteq X$ prostopadła zarówno do A jak i do B , spełniająca

$$L \cap A \neq \emptyset, \quad L \cap B \neq \emptyset.$$

Dla dowolnych punktów $p \in L \cap A$ oraz $q \in L \cap B$ mamy $\rho(A, B) = \|\vec{pq}\|$.

Dowód. Twierdzimy, że skoro $A \cap B = \emptyset$, to $T(A) + T(B) \neq T(X)$. Inaczej bowiem biorąc dowolne punkty $a \in A$ oraz $b \in B$ mielibyśmy, że $\vec{ab} \in T(A) + T(B)$, czyli $\vec{ab} = v_a + v_b$, gdzie $v_a \in T(A)$ oraz $v_b \in T(B)$. Wtedy jednak $a + v_a = b - v_b$. Lewa strona należy do A , a prawa do B , co jest niemożliwe.

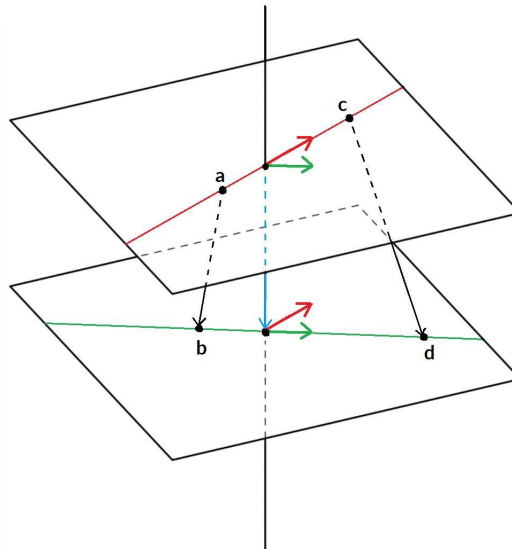
Weźmy $a \in A$ oraz $b \in B$ oraz zrzućmy wektor \vec{ab} na $(T(A) + T(B))^\perp$. Twierdzimy, że ten rzut nie zależy od wyboru a, b . Weźmy bowiem $c \in A$ oraz $d \in B$ i również zrzućmy \vec{cd} na $(T(A) + T(B))^\perp$. Dokładniej, niech $b - a = v_1 + v_2$ oraz $d - c = v'_1 + v'_2$, gdzie $v_1, v'_1 \in T(A) + T(B)$ oraz $v_2, v'_2 \in (T(A) + T(B))^\perp$. Wówczas:

$$b - a - (d - c) = (b - d) + (c - a) \in T(A) + T(B)$$

Jednak powyższa suma równa jest $v_1 + v_2 - v'_1 - v'_2$. Oznacza to, że $v_2 - v'_2 \in T(A) + T(B)$, a w konsekwencji: $v_2 - v'_2 = 0$, bo przecież $v_2 - v'_2 \in (T(A) + T(B))^\perp$. Dostaliśmy więc $v_2 = v'_2$. Ale v_2 to rzut \vec{ab} na $(T(A) + T(B))^\perp$, zaś v'_2 to rzut \vec{cd} na $(T(A) + T(B))^\perp$, czyli mamy to, co chcieliśmy: rzut nie zależy od wyboru $a \in A, b \in B$.

Wniosek jest taki, że jeśli $A \cap B = \emptyset$, to odległość pomiędzy podprzestrzeniami A oraz B jest długością rzutu wektora łączącego dowolny punkt z A z dowolnym punktem z B na $(T(A) + T(B))^\perp$. Dlaczego? Co z szukaną prostą? Wśród wszystkich możliwych wektorów łączących \vec{ab} , dla $a \in A, b \in B$, któryś jest w $(T(A) + T(B))^\perp$. Punkty, które łączy rozpinają szukaną prostą. Ich odległość to odległość A od B . \square

Geometrycznie sprawa jest prosta i można ją sobie zobrazować próbując wyznaczyć odległość dwóch nieprzecinających się prostych A oraz B w przestrzeni trójwymiarowej afinicznej. Proste te mogą być równoległe, czyli $T(A) = T(B)$ lub skośne, czyli $T(A) \cap T(B) = \{0\}$.



Mamy $A = a + T(A)$ oraz $B = b + T(B)$ i te przestrzenie afiniczne możemy zawrzeć w dwóch równoległych przestrzeniach:

$$A' = a + T(A) + T(B), \quad B' = b + T(A) + T(B).$$

W przypadku prostych skośnych podprzestrzenie A' oraz B' to płaszczyzny równoległe zawierające proste A oraz B . Odległość tych płaszczyzn wyznaczamy zgodnie z dowodem twierdzenia: zrzućmy dowolny wektor łączący $a \in A$ oraz $b \in B$ na $(T(A) + T(B))^\perp$ i bierzemy normę uzyskanego rzutu. Wynik nie zależy od wyboru a, b .

Przykład. W przestrzeni euklidesowej afinicznej \mathbb{R}^3 ze standardowym iloczynem skalarnym znajdź odległość prostych

$$\begin{aligned} L_1 &= (1, 2, 3) + \text{lin}((1, 0, 0)) \\ L_2 &= (0, 0, 0) + \text{lin}((0, 2, 4)). \end{aligned}$$

Rozwiązanie. Niech $p = (1, 2, 3)$ oraz $q = (0, 0, 0)$. Oczywiście $T(L_1) + T(L_2) = \text{lin}((1, 0, 0), (0, 2, 4))$. A zatem

$$(T(L_1) + T(L_2))^\perp = \text{lin}((0, 4, -2)).$$

Rozkładamy teraz wektor \vec{pq} na składowe z $T(L_1) + T(L_2)$ oraz $(T(L_1) + T(L_2))^\perp$. Po krótkich rachunkach mamy:

$$\vec{pq} = (-1, -2, -3) = -(1, 0, 0) - \frac{4}{5}(0, 2, 4) - \frac{1}{10}(0, 4, -2).$$

W szczególności wyznaczamy długość rzutu \vec{pq} na $(T(L_1) + T(L_2))^\perp$, czyli długość ostatniego składnika:

$$\rho(L_1, L_2) = \left| -\frac{1}{10}(0, 4, -2) \right| = \frac{\sqrt{5}}{5}.$$

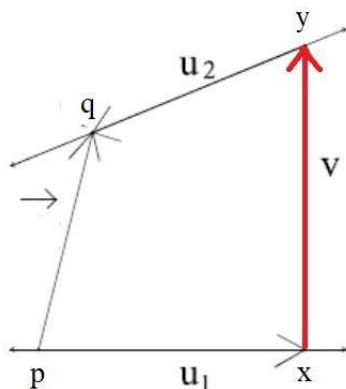
Szukając punktów x, y , dla których ta odległość jest osiągalna ustalmy, że jeśli

$$\vec{pq} = u_1 + u_2 + v,$$

gdzie $u_1 \in T(L_1), u_2 \in T(L_2), v \in (T(L_1) + T(L_2))^\perp$, to punkty te mają postać

$$x = p + u_1 \quad \text{oraz} \quad y = q - u_2$$

tak, by $\vec{xy} = v$, jak na rysunku poniżej.



W naszym przypadku mamy zatem $u_1 = (-1, 0, 0)$ oraz $u_2 = (0, -\frac{8}{5}, -\frac{16}{5})$. Stąd:

$$x = (1, 2, 3) + (-1, 0, 0) = (0, 2, 3), \quad y = (0, 0, 0) - \left(0, -\frac{8}{5}, -\frac{16}{5}\right) = \left(0, \frac{8}{5}, \frac{16}{5}\right).$$

Stąd $\rho(x, y) = \frac{\sqrt{5}}{5}$.

* * *

Zachęcam Czytelnika do samodzielnego odnalezienia odległości pomiędzy następującymi dwoma podprzestrzeniami afinicznymi w \mathbb{R}^4 postaci:

$$\begin{aligned} P_1 &= (0, 0, 0, 0) + \text{lin}((1, 0, 1, 0), (0, 1, 2, 3), (1, 0, 0, 1)) \\ P_2 &= (1, 1, 1, 1) + \text{lin}((2, 1, 3, 4)) \end{aligned}$$

a także do znalezienia punktów $p \in P_1$ oraz $q \in P_2$, dla których $\rho(p, q) = \rho(P_1, P_2)$.

14.1 Zadania do samodzielnej pracy

Zadania ilustrujące umiejętności niezbędne do zaliczenia przedmiotu oznaczone są symbolem ♠.

Przy tych zadaniach dodany jest opis umiejętności, które sprawdzają.

1. (♠ Wyznaczanie obrazu punktu przy rzucie i symetrii prostopadłej). W poniższych zadaniach rozważamy przestrzenie euklidesowe \mathbb{R}^n ze standardowym iloczynem skalarnym.

- Znajdź rzut prostopadły punktu $(0, 3, 1)$ na prostą $L_1 + \text{lin}((1, 1, -1))$.
- Wyznacz obraz punktu $(-2, 0, 0)$ przy rzucie prostopadłym na płaszczyznę P opisaną równaniem $4x_2 - 3x_3 + 25 = 0$ oraz symetrii prostopadłej względem P .
- Niech $H = \{(x_1, x_2, x_3, x_4) \in \mathbb{R}^4 \mid 3x_1 - x_2 + x_3 + 2x_4 = 1\}$ będzie podprzestrzenią w przestrzeni afinicznej \mathbb{R}^4 . Znajdź rzut prostopadły punktu $p = (4, 0, 0, 2)$ na przestrzeń H .
- W \mathbb{R}^n dany jest punkt $p = (y_1, \dots, y_n)$ oraz prosta $L = (b_1, \dots, b_n) + \text{lin}((a_1, \dots, a_n))$. Wykaż, że rzutem prostopadłym punktu p na prostą L jest punkt $q = (z_1, \dots, z_n)$, gdzie $z = b_i + ca_i$, dla $i = 1, \dots, n$, oraz

$$c = \frac{a_1(y_1 - b_1) + \dots + a_n(y_n - b_n)}{a_1^2 + \dots + a_n^2}.$$

2. (♠ Wyznaczanie odległości punktu od zbioru).

- Dana jest afiniczna przestrzeń euklidesowa \mathbb{R}^4 ze standardowym iloczynem skalarnym $\langle \cdot, \cdot \rangle$. Wyznacz odległość punkt $p = (2, 4, -4, 2)$ od podprzestrzeni afinicznej H opisanej układem

$$\begin{cases} x_1 + 2x_2 + x_3 - x_4 = 1 \\ x_1 + 3x_2 + x_3 - 3x_4 = 2 \end{cases}.$$

- W przestrzeni euklidesowej afinicznej \mathbb{R}^4 dany jest iloczyn skalarny $\langle \cdot, \cdot \rangle : \mathbb{R}^4 \times \mathbb{R}^4 \rightarrow \mathbb{R}$:

$$\langle (x_1, x_2, x_3, x_4), (y_1, y_2, y_3, y_4) \rangle = x_1y_1 + x_1y_2 + x_2y_1 + 4x_2y_2 + 2x_3y_3 + x_3y_4 + x_4y_3 + x_4y_4.$$

Znajdź odległość punktu $(3, 0, 0, 0)$ od $M = \{(x_1, x_2, x_3, x_4) \in \mathbb{R}^4 \mid x_1 + x_2 + x_3 + x_4 = 1\}$.

3. (♠ Znajdowanie odległości prostych)

- W przestrzeni euklidesowej \mathbb{R}^3 ze standardowym iloczynem skalarnym dane są dwie proste $L_1 = (2, 1, 1) + \text{lin}((1, 1, -1))$ oraz $L_2 = (-1, 1, 1) + \text{lin}((1, 2, 0))$. Dla jakich punktów $p \in L_1$ oraz $q \in L_2$ odległość $\rho(p, q)$ jest najmniejsza?
- W przestrzeni euklidesowej \mathbb{R}^3 ze standardowym iloczynem skalarnym dane są dwie proste: $K = (2, 0, 1) + \text{lin}((0, -2, 1))$ oraz L opisana układem równań $x_1 - x_3 = 0$ oraz $x_1 + x_3 = 2$. Znajdź odległość pomiędzy prostymi K i L .

4. W przestrzeni euklidesowej \mathbb{R}^3 ze standardowym iloczynem skalarnym $\langle \cdot, \cdot \rangle$ dane są dwie proste $L = (2, 0, 1) + \text{lin}((1, -2, 0))$ i $K = (0, 1, 1) + \text{lin}((-1, 1, 1))$.

- Znajdź parametryzację obrazu prostej L przy symetrii prostopadłej względem prostej K .
- Znajdź wzór rzutu prostopadłego $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ na prostą L .
- Znajdź odległość $\rho(L, K)$ między prostymi L i K .

5. W afinicznej przestrzeni euklidesowej \mathbb{R}^4 ze standardowym iloczynem skalarnym dana jest prosta $L = (0, 3, 0, 1) + \text{lin}((2, 0, 0, 1))$ oraz płaszczyzna $P = \text{af}((3, 1, 0, 0), (3, 2, 0, -1), (3, 0, 1, 1))$. Znajdź odległość między prostą L a płaszczyzną P .

6. W przestrzeni afinicznej $(\mathbb{R}^4, \langle \cdot, \cdot \rangle_{st})$ znajdź parametryzację obrazu rzutu prostej $\text{af}((1, 1, 0, 1), (1, 0, 0, -1))$ przy rzucie prostopadłym na podprzestrzeń W zadaną układem równań:

$$\begin{cases} x_1 + x_2 - x_3 - x_4 = 1 \\ x_1 + x_4 = 0 \end{cases}.$$

7. W przestrzeni euklidesowej afinicznej \mathbb{R}^3 ze standardowym iloczynem skalarnym wyznacz równanie płaszczyzny przechodzącej przez punkt $(4, 3, 5)$, której odległość od punktu $(0, 0, 0)$ jest największa.

8. Niech $(H, \langle \cdot, \cdot \rangle)$ będzie afiniczną przestrzenią euklidesową wymiaru $n > 2$ i niech $P \subset H$ będzie płaszczyzną. Czy jest prawdą, że dla każdego punktu $p \in P$ istnieje dokładnie jedna podprzestrzeń afiniczna $M \subset H$ wymiaru $n - 2$ prostopadła do P taka, że $M \cap P = \{p\}$.

14.2 Uzupełnienie. Dlaczego ogólny wzór na odległość działa?

Do Obserwacji 14.4 dodany został komentarz mówiący o odległości punktu od przestrzeni afinicznej wymiaru $n - 1$ opisanej równaniem zawierającym współrzędne w dowolnym układzie bazowym.

Obserwacja 14.6

W przestrzeni euklidesowej afinicznej $(H, \langle \cdot, \cdot \rangle)$ wymiaru n niech $p_0, \alpha_1, \dots, \alpha_n$ będzie ortonormalnym układem bazowym i niech M będzie zbiorem punktów

$$M = \{p_0 + x_1\alpha_1 + \dots + x_n\alpha_n \mid a_1x_1 + \dots + a_nx_n = b\}, \quad (a_1, \dots, a_n) \neq (0, \dots, 0).$$

Wówczas odległość punktu $p = p_0 + y_1\alpha_1 + \dots + y_n\alpha_n$ od M wynosi:

$$\rho(p, M) = \frac{|a_1y_1 + \dots + a_ny_n - b|}{\sqrt{a_1^2 + \dots + a_n^2}}.$$

Zanim przedstawimy dowód warto podać wyjaśnienie. Co to znaczy, że zapisujemy przestrzeń afiniczną za pomocą równania w innym układzie bazowym? Jeśli na przykład weźmiemy w \mathbb{R}^2 prostą o równaniu $x_1 - x_2 = 1$, czyli $(1, 0) + \text{lin}((1, 1))$, to biorąc na przykład układ bazowy $(1, 0); (1, 1), (1, -1)$ widzimy, że każdy punkt tej prostej zapisuje się w tym układzie bazowym w postaci $(1, 0) + y_1(1, 1)$, czyli każdy punkt tej prostej ma w nowym układzie bazowym współrzędne $(y_1, 0)$.

Opis podprzestrzeni afinicznych, a także ogólniej — zbiorów algebraicznych w przestrzeni afinicznej w współrzędnych w danym układzie bazowym ma kluczowe znaczenie w dalszych wykładach. Możliwość uzyskiwania „różnych równań” opisujących zbiory spełniające równania liniowe (a także wielomianowe) prowadzi do pytania: jak uzyskać „najprostsze” opisy zbiorów za pomocą równań.

Dowód. Niech q będzie rzutem prostokątnym punktu p na M . Wówczas, jak wiemy z wcześniejszych wykładów $\rho(p, M) = \|p - q\|$. Jak wiadomo $p - q \in T(M)^\perp$. Przestrzeń $T(M)$ jest złożona z wektorów postaci $x_1\alpha_1 + \dots + x_n\alpha_n$, które spełniają równanie $a_1x_1 + \dots + a_nx_n = 0$, bo układ $\alpha_1, \dots, \alpha_n$ jest ortonormalny, a zatem wektor z $T(H)$ należy do $T(M)$ wtedy i tylko wtedy gdy jest on prostokątny do wektora $a_1\alpha_1 + \dots + a_n\alpha_n$. Stąd

$$T(M)^\perp = \text{lin}(a_1\alpha_1 + \dots + a_n\alpha_n).$$

Niech $q = p_0 + z_1\alpha_1 + \dots + z_n\alpha_n$. Skoro $p - q \in T(M)^\perp$, to istnieje takie $t \in \mathbb{R}$, że

$$p - q = ta_1\alpha_1 + \dots + ta_n\alpha_n = (y_1 - z_1)\alpha_1 + \dots + (y_n - z_n)\alpha_n.$$

A zatem (znowu korzystamy z ortonormalności układu $\alpha_1, \dots, \alpha_n$):

$$\rho(p, M) = \|p - q\| = |t| \sqrt{a_1^2 + \dots + a_n^2}. \quad (\spadesuit)$$

Wyliczmy teraz wartość t :

$$\begin{aligned} t(a_1^2 + \dots + a_n^2) &= \langle ta_1\alpha_1 + \dots + ta_n\alpha_n, a_1\alpha_1 + \dots + a_n\alpha_n \rangle = \\ &= \langle (y_1 - z_1)\alpha_1 + \dots + (y_n - z_n)\alpha_n, a_1\alpha_1 + \dots + a_n\alpha_n \rangle = \\ &= a_1y_1 + \dots + a_ny_n - a_1z_1 - \dots - a_nz_n = a_1y_1 + \dots + a_ny_n - b, \end{aligned}$$

przy czym równość $a_1z_1 + \dots + a_nz_n = b$ wynika stąd, że $q \in M$. A więc

$$t = \frac{a_1y_1 + \dots + a_ny_n - b}{a_1^2 + \dots + a_n^2}.$$

Wstawiamy wyliczone $|t|$ do (\spadesuit) dostajemy

$$\rho(p, M) = \left| \frac{a_1y_1 + \dots + a_ny_n - b}{a_1^2 + \dots + a_n^2} \right| \cdot \sqrt{a_1^2 + \dots + a_n^2} = \frac{|a_1y_1 + \dots + a_ny_n - b|}{\sqrt{a_1^2 + \dots + a_n^2}}.$$

□

Rozdział 15

Macierz Grama. Miara n -wymiarowa

Na przedostatnim wykładzie wprowadzone zostało pojęcie macierzy formy dwuliniowej oraz jej macierzy w różnych bazach. Poprzez pojęcie kongruencji zobaczyliśmy jak wyróżnić iloczyny skalarne spośród rzeczywistych form dwuliniowych symetrycznych na przestrzeni skończonego wymiaru. Dziś przyjrzymy się kolejnemu zastosowaniu macierzy formy dwuliniowej, ograniczając się z jednej strony do iloczynów skalarnych, a rozszerzając z drugiej strony definicję na dowolne układy wektorów. Celem będzie mówienie o n -wymiarowej objętości. Zagadnienia „mierzenia” długości, pola, objętości bada tzw. teoria miary.

Definicja 15.1: Macierz i wyznacznik Grama układu wektorów

Niech $\alpha_1, \dots, \alpha_k$ będzie układem wektorów przestrzeni euklidesowej $(V, \langle \cdot, \cdot \rangle)$. MACIERZĄ GRAMA układu $\alpha_1, \dots, \alpha_k$ nazywamy macierz $G(\alpha_1, \dots, \alpha_k) \in M_k(\mathbb{R})$, która w i -tym wierszu i j -tej kolumnie ma wyraz $\langle \alpha_i, \alpha_j \rangle$. WYZNACZNIKIEM GRAMA układu $\alpha_1, \dots, \alpha_k$ nazywamy natomiast liczbę

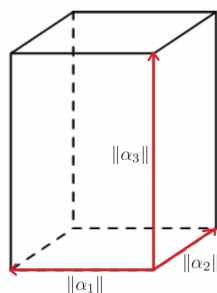
$$W(\alpha_1, \dots, \alpha_k) = \det G(\alpha_1, \dots, \alpha_k) \in \mathbb{R}.$$

Rozmiar macierzy Grama nie ma z założenia nic wspólnego z wymiarem przestrzeni V . W n -wymiarowej przestrzeni możemy rozpatrywać układ złożony choćby z dwóch wektorów i wyznaczyć jego macierz Grama rozmiarów 2×2 . Oto przykład. W przestrzeni euklidesowej $(\mathbb{R}^3, \langle \cdot, \cdot \rangle_{st})$ możemy rozważyć układ $\alpha_1 = (1, 0, 1), \alpha_2 = (1, 1, 2)$. Wówczas $\langle \alpha_1, \alpha_1 \rangle = 2, \langle \alpha_1, \alpha_2 \rangle = \langle \alpha_2, \alpha_1 \rangle = 3, \langle \alpha_2, \alpha_2 \rangle = 6$. Stąd:

$$G(\alpha_1, \alpha_2) = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 2 \end{bmatrix}.$$

Zobaczmy co wyznacznik Grama może mieć wspólnego z polem czy objętością. Wracając do przykładu wyżej możemy stwierdzić, że $\|(1, 0, 1)\| = \sqrt{2}$ oraz $\|(1, 1, 2)\| = \sqrt{6}$. Mamy też $\langle (1, 0, 1), (1, 1, 2) \rangle = 3$, zatem kosinus kąta pomiędzy rozważanymi wektorami to $3/\sqrt{12} = \sqrt{3}/2$, czyli kąt ten równy jest 30° . Z geometrii szkolnej wiemy zatem, że pole równoległoboku o bokach długości $\sqrt{2}, \sqrt{6}$ oraz kącie 30° pomiędzy nimi wynosi $\sqrt{2} \cdot \sqrt{6} \cdot \sin 30^\circ$, czyli $\sqrt{3}$. Wyznacznik macierzy wyżej jest kwadratem tego pola – wynosi 3. Nie jest to przypadek.

Oto inna charakterystyczna sytuacja, gdy macierz Grama wektorów $\alpha_1, \alpha_2, \alpha_3$ jest diagonalna. Czym są wyrazy na jej przekątnej? Są kwadratami długości wektorów α_i , czyli $\|\alpha_1\|^2, \|\alpha_2\|^2, \|\alpha_3\|^2$. Układ $\alpha_1, \alpha_2, \alpha_3$ jest prostopadły, bo macierz Grama jest diagonalna, a wyznacznik tej macierzy to oczywiście $\|\alpha_1\|^2 \|\alpha_2\|^2 \|\alpha_3\|^2$, czyli kwadrat objętości prostopadłościanu o krawędziach długości $\|\alpha_1\|, \|\alpha_2\|, \|\alpha_3\|$.



Jak przenieść powyższe intuicje na rozumowanie matematyczne? Zaczniemy od poniższego faktu ilustrującego jego wyliczanie wartości iloczynu skalarnego. Dowodzimy go podobnie jak na wcześniejszych wykładach.

Obserwacja 15.1

Macierz Grama $G(\alpha_1, \dots, \alpha_k)$ układu wektorów w (V, \langle, \rangle) wyznacza wartości iloczynu skalarnego na $\text{lin}(\alpha_1, \dots, \alpha_k)$: dla $v = a_1\alpha_1 + \dots + a_k\alpha_k$ oraz $w = b_1\alpha_1 + \dots + b_k\alpha_k$ mamy:

$$\langle a_1\alpha_1 + \dots + a_k\alpha_k, b_1\alpha_1 + \dots + b_k\alpha_k \rangle = [a_1 \quad \dots \quad a_k] \cdot G(\alpha_1, \dots, \alpha_k) \cdot \begin{bmatrix} b_1 \\ \vdots \\ b_k \end{bmatrix}.$$

W szczególności, jeśli β_1, \dots, β_n jest bazą ortonormalną (V, \langle, \rangle) , to dla dowolnych $\alpha, \beta \in V$ mamy

$$\langle \alpha, \beta \rangle = [\langle \alpha, \beta_1 \rangle \quad \dots \quad \langle \alpha, \beta_n \rangle] \cdot \begin{bmatrix} \langle \beta, \beta_1 \rangle \\ \vdots \\ \langle \beta, \beta_n \rangle \end{bmatrix}.$$

Teraz kluczowa kwestia: wyznacznik Grama rzeczywiście jest kwadratem. Dlaczego?

Wniosek 15.1

Dla układu wektorów $\alpha_1, \dots, \alpha_k$ przestrzeni euklidesowej (V, \langle, \rangle) oraz dla bazy ortonormalnej β_1, \dots, β_n tej przestrzeni niech A będzie macierzą rozmiaru $n \times k$ mającą w j -tej kolumnie współrzędne wektora α_j w bazie ortonormalnej β_1, \dots, β_n , to znaczy: $A = (a_{ij})$, gdzie $a_{ij} = \langle \alpha_j, \beta_i \rangle$, dla $i = 1, \dots, n, j = 1, \dots, k$. Wówczas:

$$G(\alpha_1, \dots, \alpha_k) = A^T A.$$

W szczególności dla $k = n$ mamy $W(\alpha_1, \dots, \alpha_n) = (\det A)^2$.

Dowód. Pierwsza część tezy wynika natychmiast z poprzedniego faktu, bowiem wyraz w i -tym wierszu oraz j -tej kolumnie $G(\alpha_1, \dots, \alpha_n)$ jest równy $\langle \alpha_i, \alpha_j \rangle$, czyli to iloczyn i -tego wiersza A^T przez macierz $G(\beta_1, \dots, \beta_n) = I$ oraz przez j -tą kolumnę macierzy A . Ta ostatnia zawiera współrzędne α_j w bazie β_1, \dots, β_n . Druga część tezy wynika z tego, że $\det A = \det A^T$, gdy $k = n$, a zatem z twierdzenia Cauchy'ego o wyznacznikach mamy $\det G(\alpha_1, \dots, \alpha_k) = \det A^T \det A = (\det A)^2$. \square

Obserwacja 15.2

Dla dowolnego układu $\alpha_1, \dots, \alpha_k$ wektorów przestrzeni euklidesowej (V, \langle, \rangle) zachodzi nierówność $W(\alpha_1, \dots, \alpha_k) \geq 0$. Co więcej następujące warunki są równoważne:

- (a) $\alpha_1, \dots, \alpha_k$ jest liniowo niezależny,
- (b) $W(\alpha_1, \dots, \alpha_k) > 0$.

Dowód. Niech $\mathcal{B} = \{\beta_1, \dots, \beta_n\}$ będzie bazą ortonormalną przestrzeni euklidesowej $W = \text{lin}(\alpha_1, \dots, \alpha_k)$ z iloczynem skalarnym $\langle, \rangle|_W$. Niech A ponownie macierzą rozmiaru $n \times k$ mającą w j -tej kolumnie współrzędne wektora α_j w bazie β_1, \dots, β_n . Zauważmy, że jeśli układ $\mathcal{A} = \{\alpha_1, \dots, \alpha_k\}$ jest liniowo niezależny, to jest on bazą W , czyli $k = n$ i macierz A jest odwracalną macierzą kwadratową postaci $M(\text{id})_{\mathcal{A}}^{\mathcal{B}}$. Skoro $G(\alpha_1, \dots, \alpha_k) = A^T A$, to w tym przypadku $W(\alpha_1, \dots, \alpha_k) = \det(A^T A) = \det(A)^2 > 0$.

Jeśli $\alpha_1, \dots, \alpha_k$ jest układem liniowo zależnym, to macierz A ma rząd mniejszy niż k . Rzeczywiście, warunkiem równoważnym liniowej zależności układu $\alpha_1, \dots, \alpha_k$ jest to, że jeden z wektorów α_i jest kombinacją liniową wektorów α_j , dla $i \neq j$. Niech to będzie

$$\alpha_i = \sum_{j \neq i} a_j \alpha_j.$$

Wówczas i -ta kolumna macierzy A zawierająca współrzędne α_i w bazie ortonormalnej \mathcal{B} ma postać:

$$\begin{bmatrix} \cdots & \langle \sum_{j \neq i} a_j \alpha_j, \beta_1 \rangle & \cdots \\ \vdots & \vdots & \ddots \\ \cdots & \langle \sum_{j \neq i} a_j \alpha_j, \beta_n \rangle & \cdots \end{bmatrix} = \sum_{j \neq i} a_j \begin{bmatrix} \cdots & \langle \alpha_j, \beta_1 \rangle & \cdots \\ \vdots & \vdots & \ddots \\ \cdots & \langle \alpha_j, \beta_n \rangle & \cdots \end{bmatrix}.$$

A zatem wykonując ciąg operacji elementarnych typu (1) polegających na odejmowaniu od i -tej kolumny j -tej przemnożonej przez a_j uzyskujemy wyzerowanie i -tej kolumny. Skoro rząd macierzy nie zmienia się przy operacjach elementarnych, to rząd macierzy A jest mniejszy niż k . Z pierwszego semestru wiemy, że dla dowolnych macierzy X, Y , dla których istnieje iloczyn XY , mamy¹

$$r(XY) \leq \min\{r(X), r(Y)\}.$$

Stąd $r(G(\alpha_1, \dots, \alpha_k)) = r(A^T A) \leq \min\{r(A^T), r(A)\} = r(A) < k$. Ostatecznie $W(\alpha_1, \dots, \alpha_k) = 0$. W szczególności pokazaliśmy też pierwszą część tezy (także dla macierzy, gdzie A nie jest kwadratowa). \square

Zobaczmy jak zmienia się wyznacznik Grama przy elementarnych modyfikacjach układu wektorów. Elementy poniższego dowodu wykorzystać można w dowodzie kryterium Sylwestera (uzup. wykładu 14).

Obserwacja 15.3

Niech $\alpha_1, \dots, \alpha_k$ będzie układem wektorów w przestrzeni euklidesowej $(V, \langle \cdot, \cdot \rangle)$. Wówczas jeśli układ β_1, \dots, β_k powstaje z $\alpha_1, \dots, \alpha_k$ za pomocą dowolnej z trzech poniższych operacji:

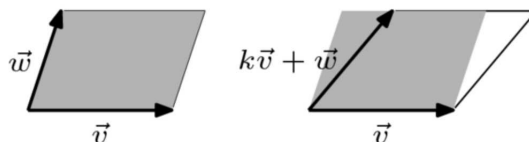
- przez dodanie do któregoś z wektorów α_i kombinacji liniowej pozostałych wektorów układu $\alpha_1, \dots, \alpha_k$,
- przez zmianę wektora z układu $\alpha_1, \dots, \alpha_k$ na wektor przeciwny,
- przez zamianę kolejności wektorów z układu $\alpha_1, \dots, \alpha_k$, to

$$W(\alpha_1, \dots, \alpha_k) = W(\beta_1, \dots, \beta_k).$$

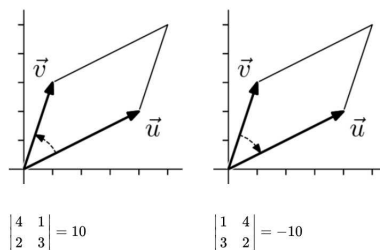
Jeśli β_1, \dots, β_k powstaje z $\alpha_1, \dots, \alpha_k$ przez przemnożenie jednego z wektorów α_i przez $a \in \mathbb{R}$, to

$$a^2 \cdot W(\alpha_1, \dots, \alpha_k) = W(\beta_1, \dots, \beta_k).$$

Powyższa obserwacja ma odniesienia geometryczne. Zobaczmy to na przykładzie pól równoległoboku.



Rysunek 1. Pole równoległoboku nie zmienia się co do modulu przy operacji (a). Źródło: Jim Hefferon, <https://hefferon.net/linearalgebra/>



Rysunek 3. Pole równoległoboku nie zmienia się co do modulu przy operacji (c). Źródło: Jim Hefferon, <https://hefferon.net/linearalgebra/>.

¹Przypominam — to wynika stąd, że kolumny macierzy XY są kombinacjami liniowymi kolumn macierzy Y .

Wiemy już, że wyznacznik Grama jest liczbą nieujemną (dodatnią, gdy układ jest liniowo niezależny). Chcielibyśmy myśleć o jego pierwiastku kwadratowym jako o liczbie przypisującej układowi wektorów „miarę” ich wzajemnego położenia w przestrzeni euklidesowej. Prowadzi to do definicji równoległościanu.

Definicja 15.2: Równoległościan w przestrzeni afinicznej

Niech H będzie przestrzenią euklidesową afiniczną. Podzbiór $R(p_0; \alpha_1, \dots, \alpha_k) \subset H$ postaci

$$\{p_0 + a_1\alpha_1 + \dots + a_k\alpha_k \mid a_1, \dots, a_k \in [0, 1]\}$$

gdzie $p_0 \in H$ oraz $\alpha_1, \dots, \alpha_k$ są liniowo niezależne w $T(H)$ nazywamy k -WYMIAROWYM RÓWNOLE-
GŁOŚCIANEM W H ROZPIĘTYM NA WEKTORACH $\alpha_1, \dots, \alpha_k$ ZACZEPIONYCH W PUNKCIE p_0 .

Wprowadzamy szczególne nazewnictwo dla równoległościanów w przestrzeniach niskich wymiarów.

- Równoległościan $R(p_0; \alpha_1)$ nazywamy ODCINKIEM o końcach w punktach $p_0, p_0 + \alpha_1$.
- Równoległościan $R(p_0; \alpha_1, \alpha_2)$ nazywamy RÓWNOLEGŁOBOKIEM.



Równoległobok oraz równoległościan. Źródło: materiały prof. Jarosława Wiśniewskiego

Dla równoległościanu $R(p_0; \alpha_1, \dots, \alpha_k) \subset H$ zbiór punktów postaci $p_0 + \epsilon_1\alpha_1 + \dots + \epsilon_k\alpha_k$, gdzie $\epsilon_i \in \{0, 1\}$ nazywamy często zbiorem WIERZCHOŁKÓW równoległościanu, a dla $k = 1$ – końcami odcinka.

Chcemy teraz określić objętość równoległościanu.

Definicja 15.3: Miara n -wymiarowa

Niech $R = R(p_0; \alpha_1, \dots, \alpha_k)$ będzie k -wymiarowym równoległościanem w afinicznej przestrzeni euklidesowej. Przez $\mu_n(R)$ określać będzie liczbę rzeczywistą zwaną n -WYMIAROWĄ MIARĄ (albo n -wymiarową objętością) równoległościanu R , przy czym

$$\mu_k(R) = \sqrt{W(\alpha_1, \dots, \alpha_k)}.$$

Ponadto przyjmujemy $\mu_n(R) = 0$, dla $n > k$ oraz $\mu_l(R) = \infty$, dla $n < k$.

Jednowymiarową miarę nazywamy długością, dwuwymiarową – polem, a trójwymiarową – objętością. Stwierdzenie z początku wykładu podaje szereg intuicji uzasadniających przyjętą przez nas definicję. Objętość nie zależy od kolejności wektorów ani zmiany zwrotu jednego z nich. Zmienia się ona proporcjonalnie do zmiany normy każdego z wektorów rozpinających równoległościan.

Zauważmy, że dla dowolnych wektorów $\alpha_1, \dots, \alpha_n$ przestrzeni liniowej \mathbb{R}^n ze standardowym iloczynem skalarnym zachodzi $W(\alpha_1, \dots, \alpha_n) = (\det A)^2$, bo możemy traktować macierz A jako macierz $M(\text{id})_A^{st}$. Stąd $|\det A|$ jest n -wymiarową objętością równoległościanu rozpiętego przez rozważany układ wektorów.

W przypadku, gdy układ $\alpha_1, \dots, \alpha_n$ wektorów rozpinających równoległościan równy jest wymiarowi n przestrzeni, w której się on znajduje, wówczas miara n -wymiarowa tego równoległościanu równa jest wyznacznikowi macierzy zawierającej w kolumnach współrzędne $\alpha_1, \dots, \alpha_n$ w dowolnej bazie ortonormalnej. Jest to też pojęcie intuicyjne z punktu widzenia szkolnego wzoru na pole jako „iloczynu podstawy i wysokości”, o czym mowa w kolejnym stwierdzeniu.

Twierdzenie 15.1: „Iloczyn pola podstawy i wysokości”

Niech $\alpha_1, \dots, \alpha_k$ będzie układem wektorów przestrzeni euklidesowej $(V, \langle \cdot, \cdot \rangle)$ i niech γ będzie rzutem prostopadłym α_k na $\text{lin}(\alpha_1, \dots, \alpha_{k-1})^\perp$.

$$W(\alpha_1, \dots, \alpha_k) = W(\alpha_1, \dots, \alpha_{k-1}) \cdot \|\gamma\|^2.$$

Dowód. Niech $W = \text{lin}(\alpha_1, \dots, \alpha_{k-1})$. Wiemy z wcześniejszych wykładów, że

$$V = W \oplus W^\perp \quad \text{oraz} \quad \alpha_k = \beta + \gamma,$$

dla pewnego $\beta \in W$. A zatem:

$$W(\alpha_1, \dots, \alpha_k) = \begin{vmatrix} \langle \alpha_1, \alpha_1 \rangle & \dots & \langle \alpha_1, \alpha_{k-1} \rangle & \langle \alpha_1, \beta + \gamma \rangle \\ \langle \alpha_2, \alpha_1 \rangle & \dots & \langle \alpha_2, \alpha_{k-1} \rangle & \langle \alpha_2, \beta + \gamma \rangle \\ \vdots & \ddots & \vdots & \vdots \\ \langle \alpha_{k-1}, \alpha_1 \rangle & \dots & \langle \alpha_{k-1}, \alpha_{k-1} \rangle & \langle \alpha_{k-1}, \beta + \gamma \rangle \\ \langle \beta + \gamma, \alpha_1 \rangle & \dots & \langle \beta + \gamma, \alpha_{k-1} \rangle & \langle \beta + \gamma, \beta + \gamma \rangle \end{vmatrix}$$

Skoro $\gamma \in \text{lin}(\alpha_1, \dots, \alpha_{k-1})^\perp$ oraz $\beta \perp \gamma$, to mamy:

$$W(\alpha_1, \dots, \alpha_k) = \begin{vmatrix} \langle \alpha_1, \alpha_1 \rangle & \dots & \langle \alpha_1, \alpha_{k-1} \rangle & \langle \alpha_1, \beta \rangle \\ \langle \alpha_2, \alpha_1 \rangle & \dots & \langle \alpha_2, \alpha_{k-1} \rangle & \langle \alpha_2, \beta \rangle \\ \vdots & \ddots & \vdots & \vdots \\ \langle \alpha_{k-1}, \alpha_1 \rangle & \dots & \langle \alpha_{k-1}, \alpha_{k-1} \rangle & \langle \alpha_{k-1}, \beta \rangle \\ \langle \beta, \alpha_1 \rangle & \dots & \langle \beta, \alpha_{k-1} \rangle & \langle \beta, \beta \rangle + \langle \gamma, \gamma \rangle \end{vmatrix}$$

Niech $\beta = a_1\alpha_1 + \dots + a_{k-1}\alpha_{k-1}$. Wtedy po odjęciu od n -tego wiersza i -tego wiersza przemnożonego przez a_i , dla wszystkich $1 \leq i \leq k-1$, wyznacznik się nie zmienia i dostajemy:

$$W(\alpha_1, \dots, \alpha_k) = \begin{vmatrix} \langle \alpha_1, \alpha_1 \rangle & \dots & \langle \alpha_1, \alpha_{k-1} \rangle & \langle \alpha_1, \beta \rangle \\ \langle \alpha_2, \alpha_1 \rangle & \dots & \langle \alpha_2, \alpha_{k-1} \rangle & \langle \alpha_2, \beta \rangle \\ \vdots & \ddots & \vdots & \vdots \\ \langle \alpha_{k-1}, \alpha_1 \rangle & \dots & \langle \alpha_{k-1}, \alpha_{k-1} \rangle & \langle \alpha_{k-1}, \beta \rangle \\ \langle 0, \alpha_1 \rangle & \dots & \langle 0, \alpha_{k-1} \rangle & \langle \gamma, \gamma \rangle \end{vmatrix}.$$

Po odjęciu od n -tej kolumny i -tej kolumny przemnożonej przez a_i , dla wszystkich $1 \leq i \leq k-1$, wyznacznik się nie zmienia i **ostatni wiersz się nie zmienia**, zaś ostatnia kolumna staje się *transpozycją* ostatniego wiersza, co oznacza, że:

$$W(\alpha_1, \dots, \alpha_k) = \begin{vmatrix} G(\alpha_1, \dots, \alpha_{k-1}) & 0 \\ 0 & \|\gamma\|^2 \end{vmatrix}.$$

□

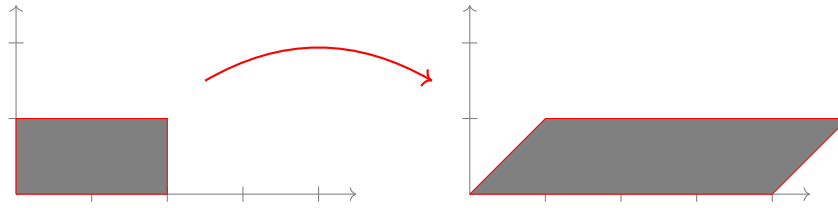
Powiedzmy o jeszcze jednym fundamentalnym dla naszej intuicji fakcie mającym olbrzymie znaczenie w interpretacji analitycznej: objętość równoległościanu zmienia przy endomorfizmie liniowym się tak, jak moduł wyznacznika tego endomorfizmu.

Obserwacja 15.4

Niech $\phi : V \rightarrow V$ będzie endomorfizmem przestrzeni euklidesowej $(V, \langle \cdot, \cdot \rangle)$. Dla dowolnej bazy $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$ w V zachodzi równość:

$$\sqrt{W(\phi(\alpha_1), \phi(\alpha_2), \dots, \phi(\alpha_n))} = |\det(\phi)| \cdot \sqrt{W(\alpha_1, \dots, \alpha_n)}.$$

Przykład. Bierzymy $\phi : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ dane wzorem $\phi(x, y) = (2x + y, y)$. Równoległoscian rozpięty na wektorach $(2, 0), (0, 1)$ przechodzi na równoległoscian rozpięty na wektorach $(4, 0), (1, 1)$.



Wyznacznik rozważanego przekształcenia liniowego to 2.

Dowód. Zakładamy, że $\dim V = n$. Niech \mathcal{B} będzie bazą ortonormalną przestrzeni $(V, \langle \cdot, \cdot \rangle)$. Wiemy, że:

$$G(\alpha_1, \dots, \alpha_n) = (M(\text{id})_{\mathcal{A}}^{\mathcal{B}})^T \cdot M(\text{id})_{\mathcal{A}}^{\mathcal{B}},$$

$$G(\phi(\alpha_1), \dots, \phi(\alpha_n)) = (M(\phi)_{\mathcal{A}}^{\mathcal{B}})^T \cdot M(\phi)_{\mathcal{A}}^{\mathcal{B}}.$$

Mamy też: $M(\phi)_{\mathcal{A}}^{\mathcal{B}} = M(\phi)_{\mathcal{B}}^{\mathcal{B}} \cdot M(\text{id})_{\mathcal{A}}^{\mathcal{B}}$, czyli $\det(M(\phi)_{\mathcal{A}}^{\mathcal{B}}) = \det(\phi) \cdot \det(M(\text{id})_{\mathcal{A}}^{\mathcal{B}})$. Zatem

$$W(\alpha_1, \dots, \alpha_n) = \det((M(\text{id})_{\mathcal{A}}^{\mathcal{B}})^T) \cdot \det(M(\text{id})_{\mathcal{A}}^{\mathcal{B}}) = (\det(M(\text{id})_{\mathcal{A}}^{\mathcal{B}}))^2$$

$$W(\phi(\alpha_1), \dots, \phi(\alpha_n)) = (\det(\phi) \cdot \det(M(\text{id})_{\mathcal{A}}^{\mathcal{B}}))^2.$$

□

Powyzszy fakt możemy przepisać w języku przekształceń afinicznych na równoległoscianach.

Obserwacja 15.5

Niech $f : V \rightarrow V$ będzie przekształceniem afinicznym przestrzeni euklidesowej afinicznej $(V, (V, \langle \cdot, \cdot \rangle))$ w siebie. Dla dowolnego układu bazowego $(p_0; \mathcal{A}) = (p_0; \alpha_1, \dots, \alpha_n)$ w V zachodzi równość:

$$\mu_n(R(f(p_0); f'(\alpha_1), \dots, f'(\alpha_n))) = |\det(f')| \cdot \mu_n(R(p_0; \alpha_1, \dots, \alpha_n)).$$

Przykład. Niech $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ dane wzorem $f(x, y) = (2x + y - 1, y)$. Równoległobok $R((1, 1); (2, 0), (0, 1))$ przechodzi na $R((2, 1); (4, 0), (1, 1))$, a jego pole zmienia się z 2 na 4, zgodnie z modułem wyznacznika pochodnej przekształcenia f .

Jeszcze jednym przykładem zbioru, który rozważamy w związku z objętością jest sympleks k -wymiarowy.

Definicja 15.4: Sympleks

Niech p_0, \dots, p_n będzie afinicznie niezależnym układem punktów. Zbiór kombinacji afinicznych punktów p_0, \dots, p_n o nieujemnych wagach oznaczamy przez $S(p_0, \dots, p_n)$ i nazywamy **n -WYMIAROWYM SYMPLEKSEM ROZPIĘTYM NA PUNKTACH (LUB: O WIERZCHOŁKACH) p_0, \dots, p_n** .

- Sympleks 1-miarowy nazywamy ODCINKIEM.
- Sympleks 2-wymiarowy nazywamy TRÓJKĄTEM.
- Sympleks 3-wymiarowy nazywamy CZWORÓŚCIANEM.



Trójkąt i czworoscian. Źródło: materiały prof. Jarosława Wiśniewskiego

Zarówno dla sympleksów, jak i dla równoległościanów można (także w kontekście afinicznym) mówić k -wymiarowej mierze (objętości) opartej o pojęcie wyznacznika Grama.

Definicja 15.5

Niech $S = S(p_0, \dots, p_k)$ będzie k -wymiarowym sympleksem w $(H, \langle \cdot, \cdot \rangle)$. Przez k -wymiarową miarę (lub k -wymiarową objętość) sympleksu S rozumiemy liczbę:

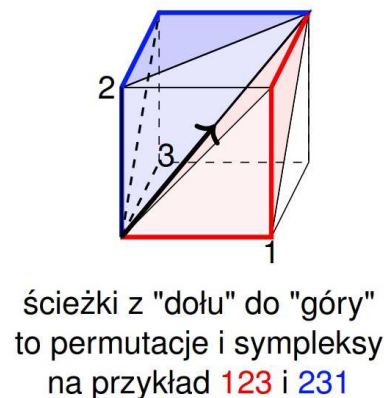
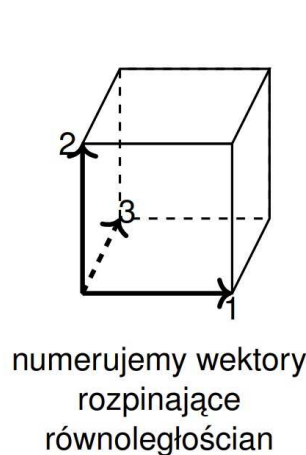
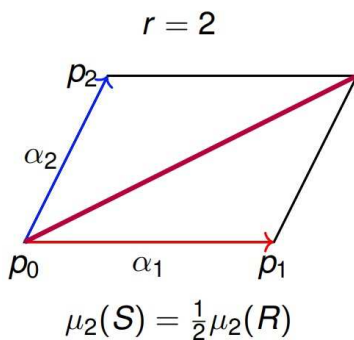
$$\mu_k(S) = \frac{1}{k!} \sqrt{W(\overrightarrow{p_0 p_1}, \dots, \overrightarrow{p_0 p_k})}.$$

Czytelnik powinien rozpoznać w powyższej formule wzory na pole trójkąta i objętość ostrosłupa trójkątnego. Sama definicja stawia jednak nowe pytania: czy „miara”, o której mówimy to jest „prawdziwe pole”? Albo pytając inaczej: czy miary określone osobno dla równoległościanów i sympleksów można rozszerzyć do miar obejmujących ogólniejsze rodziny zbiorów? A jeśli tak, to jakie to zbiory? To pytanie jest zaskakująco trudne, ale i niezwykle ważne. Skąd czynnik $1/k!$ w definicji miary k -wymiarowej sympleksu?

Rozumować można na wiele sposobów. W dodatku przedstawimy szkic podejścia wywodzącego się z analizy. Przedstamy podejście oparte o definicję. Mając równoległościan $R(p_0; \alpha_1, \dots, \alpha_k)$ możemy rozważyć wszystkie sympleksy rozpięte przez takie układy k wierzchołków tego równoległościanu, aby:

- układy te zawierały wierzchołek p_0 oraz przeciwległy, czyli $p_0 + \alpha_1 + \dots + \alpha_k$,
- aby zbiór wektorów łączących pary wierzchołków tego układu był wybrany ze zbioru $\overrightarrow{p_0 p_1}, \dots, \overrightarrow{p_0 p_k}$

Zgodnie z naszą definicją wszystkie te sympleksy mają tę samą objętość. A jest ich przecież $k!$ Czy Czytelnik wie jak to pokazać? Wybierając taki sympleks trzeba określić w jakiej kolejności poruszamy się po wierzchołkach równoległościanu w kierunkach k wektorów $\overrightarrow{p_0 p_1}, \dots, \overrightarrow{p_0 p_k}$. Innymi słowy: poruszamy się od wierzchołka $p_0 + 0 \cdot \overrightarrow{p_0 p_1} + \dots + 0 \cdot \overrightarrow{p_0 p_k}$ i w pewnej kolejności zamieniamy współczynniki 0 na współczynniki 1. W ten sposób po k krokach otrzymamy wierzchołek $p_0 + \alpha_1 + \dots + \alpha_k$. Oto przykłady:



Źródło: materiały prof. Jarosława Wiśniewskiego.

Inne podejście: k -wymiarową kostkę $[0, 1]^k$ „triangulować” możemy na $k!$ sympleksów postaci²:

$$S_\sigma = \{(x_1, \dots, x_k) \in \mathbb{R}^d \mid 0 \leq x_{\sigma(1)} \leq x_{\sigma(2)} \leq \dots \leq x_{\sigma(k)} \leq 1\}, \text{ gdzie } \sigma \in S_k.$$

Na kolejnym wykładzie przyjrzymy się pojęciu orientacji oraz iloczynowi wektorowego, stanowiących podstawowe narzędzia zaawansowanej geometrii analitycznej i różniczkowej. Mają one nie tylko ważne zastosowania w innych naukach, ale też wnoszą ważne intuicje do naszego rozumienia geometrii. Z elementarnego punktu widzenia pozwalają powiedzieć m.in. o tzw. mierze skierowanej (np. pole ze znakiem). Czytelnika zainteresowanego skarbcem ciekawych zagadnień geometrycznych dotyczącej miary odsyłam na stronę prof. Jacka Świątkowskiego (UWr): www.math.uni.wroc.pl/~swiatkow/Repozytorium/pole.html.

²Ogólną teorią takich działań zajmuje się topologiczna teoria tzw. kompleksów sympleksyjnych, patrz np. paragraf 5.1 w <https://ww2.ii.uj.edu.pl/~zglyczyn/dydaktyka/2013-14/top-obliczeniowa/topologia.pdf>.

15.1 Zadania do samodzielnej pracy

Zadania ilustrujące umiejętności niezbędne do zaliczenia przedmiotu oznaczone są symbolem ♠.

Przy tych zadaniach dodany jest opis umiejętności, które sprawdzają.

1. (♠ Pytania dotyczące macierzy Grama)

- Niech $\alpha_1 = (1, 2, 1, 3)$, $\alpha_2 = (3, 5, 1, 4)$, $\alpha_3 = (5, 8, s, 5)$. W \mathbb{R}^4 ze standardowym iloczynem skalarnym oblicz wyznacznik Grama układu $\alpha_1, \alpha_2, \alpha_3$. Dla jakich $s \in \mathbb{R}$ układ $\alpha_1, \alpha_2, \alpha_3$ jest liniowo niezależny?
- Czy istnieje 5-wymiarowa przestrzeń euklidesowa liniowa $(V, \langle \cdot, \cdot \rangle)$ zawierająca układ 7 wektorów $\alpha_1, \dots, \alpha_7$, którego wyznacznik Grama $W(\alpha_1, \dots, \alpha_7)$ jest dodatni?
- Niech $(V, \langle \cdot, \cdot \rangle)$ będzie przestrzenią euklidesową oraz niech \mathcal{A} będzie takim liniowo niezależnym układem wektorów w przestrzeni V , że macierz Grama $G(\mathcal{A})$ ma wyłącznie wyrazy równe 0 lub 1. Pokaż, że $G(\mathcal{A})$ jest wówczas macierzą identycznościową.
- Załóżmy, że $\alpha_1, \dots, \alpha_k, \alpha_{k+1}, \dots, \alpha_n$ są takimi wektorami liniowej przestrzeni euklidesowej $(V, \langle \cdot, \cdot \rangle)$ wymiaru n , że wyznacznik Grama $W(\alpha_{k+1}, \dots, \alpha_n)$ jest równy 0. Czy wyznacznik Grama $W(\alpha_1, \dots, \alpha_k, \alpha_{k+1}, \dots, \alpha_n)$ może być różny od zera?
- Niech $\alpha_1, \dots, \alpha_k$ będzie układem wektorów w przestrzeni euklidesowej $(V, \langle \cdot, \cdot \rangle)$, takim że układ $\alpha_1, \dots, \alpha_{k-1}$ jest ortonormalny i wyznacznik Grama układu $\alpha_1, \dots, \alpha_k$ wynosi 25. Niech γ będzie rzutem prostopadłym wektora α_k na przestrzeń $\text{lin}(\alpha_1, \dots, \alpha_{k-1})^\perp$. Wyznacz $\|\gamma\|$.
- Niech $\alpha_1, \dots, \alpha_n$ będzie bazą przestrzeni euklidesowej $(V, \langle \cdot, \cdot \rangle)$. Wykaż, że istnieje baza β_1, \dots, β_n przestrzeni V , że $(G(\alpha_1, \dots, \alpha_n))^{-1} = G(\beta_1, \dots, \beta_n)$. Opisz tę bazę w terminach wektorów α_i .
- Niech L_1, L_2, L_3 będą prostymi zawartymi w płaszczyźnie euklidesowej $(\mathbb{R}^2, \langle \cdot, \cdot \rangle)$. Niech α_{ij} będzie kątem pomiędzy wektorami rozpinającymi $T(L_i)$ oraz $T(L_j)$, dla $1 \leq i, j \leq 3$. Rozstrzygnij, czy wyznacznik macierzy $M \in M_3(\mathbb{R})$ o wyrazach $\cos(\alpha_{ij})$ może być niezerowy?

2. Korzystając z tego, że $W(\alpha_1, \alpha_2) \geq 0$ udowodnij nierówność Schwarza.

3. Wykaż, że dla dowolnych układów wektorów v_1, \dots, v_n oraz w_1, \dots, w_m przestrzeni euklidesowej liniowej $(V, \langle \cdot, \cdot \rangle)$ zachodzi nierówność $W(v_1, \dots, v_n, w_1, \dots, w_m) \leq W(v_1, \dots, v_n) \cdot W(w_1, \dots, w_m)$. Kiedy w powyższej nierówności zachodzi równość?

4. (♠ Znajdowanie pól i objętości)

- W afinicznej przestrzeni euklidesowej \mathbb{R}^3 zadany jest standardowy iloczyn skalarny oraz punkty $p_0 = (0, 1, 3)$, $p_1 = (1, 1, 2)$, $p_2 = (1, 3, 0)$ oraz $w_t = (t^2, 7, 3t)$, dla $t \in \mathbb{R}$. Znajdź pole trójkąta o wierzchołkach p_0, p_1, p_2 oraz rozstrzygnij, dla jakich $t \in \mathbb{R}$ czworościan $S(p_0, p_1, p_2, w_t)$ ma najmniejszą objętość.
- W afinicznej przestrzeni euklidesowej \mathbb{R}^3 zadany jest standardowy iloczyn skalarny. Rozważmy sympleks S rozpięty na punktach $p_0 = (0, 1, 0)$, $p_1 = (1, 2, 0)$, $p_2 = (1, 1, 1)$, $p_3 = (2, 3, 1)$. Znajdź objętość oraz pole powierzchni bocznej S . Rozważmy punkt $p = (10, 0, 0)$. Znajdź w S punkt najbliższy q .
- Niech $(\mathbb{R}^2, \langle \cdot, \cdot \rangle)$ będzie przestrzenią euklidesową. Wykaż, że miara 2-wymiarowa równoległoboku rozpiętego przez wektory $(1, 0)$ oraz $(0, 1)$ równa jest mierze 2-wymiarowej równoległoboku rozpiętego przez wektory $(1, 0)$ oraz $(1, 1)$.
- Podaj przykład iloczynu skalarnego na przestrzeni \mathbb{R}^2 , przy którym 2-wymiarowa miara równoległoboku rozpiętego przez wektory $(-1, 1)$ oraz $(1, 1)$ równa jest 3.
- Wykaż, że wśród wszystkich k -wymiarowych równoległocienów $R(p_0; \alpha_1, \dots, \alpha_k)$ w \mathbb{R}^n , takich że $\|\alpha_i\| = r_i$, dla $i = 1, \dots, k$ największą k -wymiarową objętość μ_k mają te, w których $\alpha_i \perp \alpha_j$, dla wszystkich $i \neq j$. Oblicz tę największą objętość.

5. Niech p_0, \dots, p_n będą punktami w przestrzeni euklidesowej afinicznej \mathbb{R}^n z iloczynem skalarnym $\langle \cdot, \cdot \rangle$ i niech $S = S(p_0, \dots, p_n)$. Niech też $\alpha_i = \overrightarrow{p_0 p_i}$, dla $i = 1, \dots, n$. Wówczas

$$\mu_n(S) = \frac{1}{n!} \sqrt{W(\alpha_1, \dots, \alpha_n)} = \frac{1}{n!} \left| \det \begin{bmatrix} | & | & \cdots & | \\ p_0 & p_1 & \cdots & p_n \\ | & | & & | \\ 1 & 1 & & 1 \end{bmatrix} \right|. \quad (*)$$

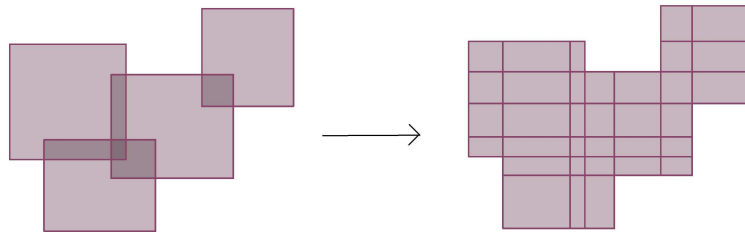
przy czym w kolumnach macierzy z prawej strony (*) są współrzędne p_0, \dots, p_n w dowolnym ortonormalnym układzie bazowym przestrzeni \mathbb{R}^n .

15.2 Dodatek. Miara Jordana i zasada Cavalieriego

Materiał przedstawiony w tym dłuższym niż zwykle dodatku, ma na celu wprowadzenie Państwa (bez szczegółów) w jedną z kluczowych obserwacji analitycznych prowadzących do wyznaczania objętości zbiorów... no właśnie, jakich? Zbiory te nazwiemy w tym dodatku mierzalnymi w sensie³ Jordana. Chciałbym pokazać jak wprowadzona przez nas definicja miary równoległościemu wiąże się z definicją miary sympleksu, oraz innych obiektów. Wyjaśnienie podane na końcu wykładu zyska w ten sposób szerszy kontekst.

Naszym celem jest określenie miary Jordana. Jest to sposób wyznaczania miary n -wymiarowej μ_n w przestrzeni \mathbb{R}^n , którą przypisujemy coraz bardziej skomplikowanym podzbiорom przestrzeni afinicznej, począwszy od równoległościemu. Robimy to w trzech krokach.

- **Krok 1.** Bierzemy przestrzeń \mathbb{R}^n i ustalamy w niej bazę \mathcal{A} . Niech P_1, \dots, P_s będzie zbiorem równoległościemu rozpiętych przez skalarne wielokrotności wektorów z \mathcal{A} o rozłącznych wnętrzach. Wówczas określamy $\mu_n(P_1 \cup \dots \cup P_s) = \mu_n(P_1) + \dots + \mu_n(P_s)$.
- **Krok 2.** Rozważamy zbiór równoległościemu P_1, \dots, P_s rozpiętych przez skalarne wielokrotności wektorów z \mathcal{A} , ale nie zakładamy, że ich wnętrza są rozłączne.

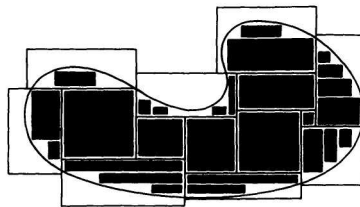


Przykład dekompozycji zbioru prostokątów o bokach równoległych do ustalonej bazy \mathbb{R}^2 .
Źródło: Wikipedia.

Nietrudno widzieć, że można dokonać ich dekompozycji na sumę prostokątów Q_1, \dots, Q_r o rozłącznych wnętrzach, jak w poprzednim kroku. Okazuje się, że niezależnie od wybranej dekompozycji wartość $\mu_n(Q_1 \cup \dots \cup Q_r)$ jest taka sama, co pozwala rozszerzyć definicję funkcję μ_n na zbiory $P_1 \cup \dots \cup P_s$.

Uzyskaliśmy zatem nową klasę zbiorów, na której mamy miarę μ_n – są to zbiory równoległościemu równoległych do ustalonej bazy \mathbb{R}^n . Czas na argument analityczny.

- **Krok 3.** Bierzemy podzbiór **ograniczony** $\Omega \subset \mathbb{R}^n$, to znaczy: Ω jest zawarty w pewnym równoległościemu.
– Przez **miarę zewnętrzną** zbioru Ω , ozn. $\overline{\mu_n(\Omega)}$, określamy infimum po wszystkich sumach skończonych $\mu_n(P_1) + \dots + \mu_n(P_s)$, gdzie P_1, \dots, P_s są równoległościemu (jak w poprzednich krokach) takimi, że $\Omega \subseteq P_1 \cup \dots \cup P_n$.



Źródło: K. Spindler Abstract Algebra With Applications, Chapman & Hall.

- Przez **miarę wewnętrzną** zbioru Ω , ozn. $\underline{\mu_n(\Omega)}$, określamy supremum po wszystkich sumach skończonych $\mu_n(Q_1) + \dots + \mu_n(Q_r)$, gdzie Q_1, \dots, Q_r są równoległościemu (jak w poprzednich krokach) takimi, że: $\Omega \supseteq Q_1 \cup \dots \cup Q_r$.

³W trakcie studiów poznają Państwo różne klasy zbiorów mierzalnych, zarówno w ramach kursu analizy, jak i teorii miary czy rachunku prawdopodobieństwa (najważniejszym będzie miara Lebesgue'a).

Definicja 15.6: Zbiór mierzalny w sensie Jordana

Mówimy, że zbiór ograniczony $\Omega \subseteq \mathbb{R}^n$ jest **mierzalny w sensie Jordana**, jeśli

$$\overline{\mu_n(\Omega)} = \underline{\mu_n(\Omega)}.$$

Liczbę powyżej nazywamy **miarą Jordana** zbioru Ω , ozn. $\mu_n(\Omega)$.

Mówiąc równoważnie: ograniczony zbiór $\Omega \subseteq \mathbb{R}^n$ jest mierzalny w sensie Jordana jeśli dla każdego $\epsilon > 0$ istnieją równoległościany P_1, \dots, P_m oraz R_1, \dots, R_s o rozłącznych wnętrzach rozpięte przez skalarne wielokrotności wektorów z bazy \mathcal{A} , że

$$P_1 \cup \dots \cup P_r \subseteq \Omega \subseteq R_1 \cup \dots \cup R_s \quad \text{oraz} \quad 0 \leq \sum_{j=1}^s \mu_n(R_j) - \sum_{i=1}^r \mu_n(P_i) < \epsilon.$$

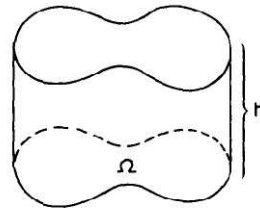
Czytelnika zainteresowanego szczegółami odsyłam do świetnego tekstu dra Michała Krycha: *Elementy teorii całkowania*, https://www.mimuw.edu.pl/~krych/staszic/skrypt27-calki_D.pdf.

Wymieńmy kilka własności miary, którą określiliśmy jako rozszerzenie zdefiniowanej na wykładzie miary.

- Suma skończenie wielu mierzalnych podzbiorów \mathbb{R}^n w sensie Jordana jest mierzalna w sensie Jordana, ale suma nieskończenie wielu – już niekoniecznie.
- Można pokazać, że dla zbiorów mierzalnych $\Omega_1 \subseteq \Omega_2$ mamy $\mu_n(\Omega_1) \leq \mu_n(\Omega_2)$.

Uogólnienia poznanych przez nas rezultatów, w tym niezwykle istotna zasada Cavalieriego.

- **Twierdzenie.** Niech $U \subseteq (\mathbb{R}^n, \langle \cdot, \cdot \rangle_{st})$ będzie podprzestrzenią afiniczną wymiaru $n - 1$, czyli tzw. hiperpłaszczyzną, oraz niech $v \in U^\perp$, gdzie $\|v\| = 1$. Niech μ_n oraz μ_{n-1} będą miarami Jordana na \mathbb{R}^n oraz na U . Dla dowolnego podzbioru $\Omega \subseteq U$ mierzalnego w sensie Jordana oraz dodatniej liczby $h > 0$ określamy **cylinder nad Ω wysokości h** jako zbiór $Cyl(\Omega, h) := \{x + tv \in \mathbb{R}^n \mid x \in \Omega, 0 \leq t \leq h\}$.

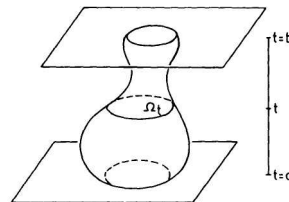


Cyl(Ω, h)

Źródło: K. Spindler Abstract Algebra With Applications, Chapman & Hall.

Wówczas $\mu_n(Cyl(\Omega, h)) = h \cdot \mu_{n-1}(\Omega)$.

- **Zasada Cavalieriego (1635).** Niech Ω będzie mierzalnym (w s. J.) podzbiorem $(\mathbb{R}^n, \langle \cdot, \cdot \rangle_{st})$, niech U będzie hiperpłaszczyzną i niech $n_0 \in U^\perp$ ma długość 1. Dla $t \in \mathbb{R}$ niech $\Omega_t := \Omega \cap (tn_0 + U)$.



Źródło: K. Spindler Abstract Algebra With Applications, Chapman & Hall.

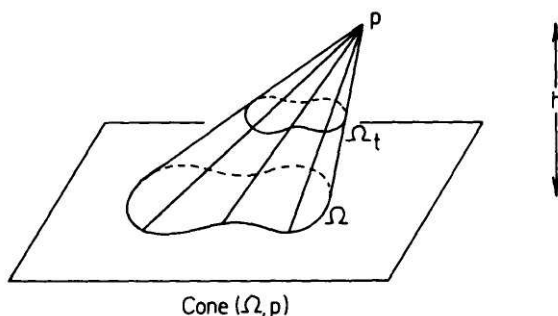
Jeśli Ω_t jest mierzalny (w sensie Jordana) dla $a \leq t \leq b$ oraz pusty dla pozostałych t , to:

$$\mu_n(\Omega) = \int_a^b \mu_{n-1}(\Omega_t) dt.$$

Czytelnik zechce wpisać w dowolną wyszukiwarkę hasło „zasada Cavalieriego”, a przekona się o jej licznych i pięknych zastosowaniach. Można też obejrzeć wiele przyjemnych filmów, np. <https://youtu.be/0xCe6LGWwJU>. Cytowany wyżej tekst da Państwu ścisły pogląd na te zagadnienia.

- **Wniosek.** Niech U będzie hiperpłaszczyzną w $(\mathbb{R}^n, \langle \cdot, \cdot \rangle_{st})$ i niech Ω będzie mierzalnym (w s. J) podzbiorem U . Dla każdego elementu $p \in V \setminus U$ przez **stożek nad Ω** określamy zbiór:

$$Cone(\Omega, p) := \{(1-t)x + tp \in \mathbb{R}^n \mid x \in \Omega, 0 \leq t \leq 1\},$$



Źródło: K. Spindler Abstract Algebra With Applications, Chapman & Hall.

czyli jest to suma wszystkich odcinków łączących elementy Ω z p . Jeśli h jest odległością p od U , to

$$\mu_n(Cone(\Omega, p)) = \frac{h}{n} \mu_{n-1}(\Omega).$$

Wykażmy ostatni wniosek. Zgodnie z zasadą Cavalieriego rozważamy zbiór

$$\Omega_t = \Omega \cap (tn_0 + U),$$

gdzie $0 \leq t \leq h$. Jest to obraz Ω przy jednokładności o środku w p o skali $\frac{h-t}{h}$. Zgodnie z twierdzeniem o zmianie miary przy przekształceniu afinicznym

$$\mu_{n-1}(\Omega_t) = \left(\frac{h-t}{h}\right)^{n-1} \mu_{n-1}(\Omega)$$

(zobacz macierz tej jednokładności). Zgodnie z zasadą Cavalieriego mamy zatem $\mu_n(Cone(\Omega, p))$ równe jest:

$$\int_0^h \left(\frac{h-t}{h}\right)^{n-1} \mu_{n-1}(\Omega) dt = h \cdot \mu_{n-1}(\Omega) \int_0^1 \tau^{n-1} d\tau = \frac{h}{n} \cdot \mu_{n-1}(\Omega).$$

Obserwacja 15.6: Wniosek – pole, wzór 1.

Niech $p_0, \dots, p_n \in (\mathbb{R}^n, (V, \langle \cdot, \cdot \rangle_{st}))$ i niech $S = S(p_0, \dots, p_n)$. Niech też $\alpha_i = \overrightarrow{p_0 p_i}$, dla $i = 1, \dots, n$. Wówczas^a:

$$\mu_n(S) = \frac{1}{n!} \sqrt{W(\alpha_1, \dots, \alpha_n)} \stackrel{*}{=} \frac{1}{n!} \left| \det \begin{bmatrix} | & | & \dots & | \\ p_0 & p_1 & \dots & p_n \\ | & | & \dots & | \\ 1 & 1 & \dots & 1 \end{bmatrix} \right|.$$

przy czym w kolumnach macierzy z prawej strony (*) są współrzędne p_0, \dots, p_n w dowolnym ortonormalnym układzie bazowym przestrzeni \mathbb{R}^n .

^a**Szczególny przypadek.** Dla standardowego układu bazowego w \mathbb{R}^2 dostajemy wzór na pole S trójkąta o wierzchołkach w punktach $(x_1, y_1), (x_2, y_2), (x_3, y_3)$ oraz warunek konieczny i wystarczający do współliniowości tych punktów. Dostajemy także równanie prostej przechodzącej przez dwa zadane punkty.

Dowód. Odejmując pierwszą kolumnę od wszystkich pozostałych dostajemy łatwo jedną z równości:

$$\begin{aligned} \det \begin{bmatrix} | & | & \cdots & | \\ p_0 & p_1 & \cdots & p_n \\ | & | & & | \\ 1 & 1 & & 1 \end{bmatrix}^2 &= \det \begin{bmatrix} | & \overrightarrow{p_0 p_1} & \cdots & \overrightarrow{p_0 p_n} \\ p_0 & 0 & \cdots & 0 \\ | & | & & | \\ 1 & 0 & & 0 \end{bmatrix}^2 = \\ &= \det \begin{bmatrix} | & \cdots & | \\ \alpha_1 & \cdots & \alpha_n \\ | & & | \end{bmatrix}^T \cdot \det \begin{bmatrix} | & \cdots & | \\ \alpha_1 & \cdots & \alpha_n \\ | & & | \end{bmatrix} = \\ &= \det \begin{bmatrix} \langle \alpha_1, \alpha_1 \rangle & \cdots & \langle \alpha_1, \alpha_n \rangle \\ \vdots & \ddots & \vdots \\ \langle \alpha_n, \alpha_1 \rangle & \cdots & \langle \alpha_n, \alpha_n \rangle \end{bmatrix} = W(\alpha_1, \dots, \alpha_n)^2. \end{aligned}$$

Indukcja ze względu na n . Dla $n = 1$ mamy z definicji (równoległocianu) $\mu_1(S(p_0, p_1)) = \sqrt{W(\alpha_1)}$.

Rozważmy zatem sympleks rozpięty na afinicznie niezależnym układzie p_0, \dots, p_{n+1} punktów w \mathbb{R}^n . Wiemy też (poprzedni fakt o mierze n -wymiarowej stożka), że

$$\mu_{n+1}(S(p_0, \dots, p_{n+1})) = \frac{h}{n+1} \mu_n(S(p_0, \dots, p_n)).$$

A zatem możemy wstawić uzyskaną wyżej formułę na $\mu_n(S(p_0, \dots, p_n))$ i dostajemy dwa przedstawienia szukanej objętości $\mu_{n+1}(S(p_0, \dots, p_{n+1}))$:

$$\frac{h}{(n+1)!} \left| \det \begin{bmatrix} | & | & \cdots & | \\ p_0 & p_1 & \cdots & p_n \\ | & | & & | \\ 1 & 1 & & 1 \end{bmatrix} \right| = \frac{1}{(n+1)!} \left| \det \begin{bmatrix} | & | & \cdots & | & | \\ p_0 & p_1 & \cdots & p_n & * \\ | & | & & | & | \\ 0 & 0 & \cdots & 0 & h \\ 1 & 1 & & 1 & 1 \end{bmatrix} \right|.$$

Powyższa równość wynika z rozwinięcia Laplace'a. Twierdzimy, że macierz (której wyznacznik liczymy) po prawej jest macierzą współrzędnych punktów p_0, \dots, p_n, p_{n+1} w pierwotnej bazie punktowej $p_0; \alpha_1, \dots, \alpha_n$ uzupełnionej o wektor $\frac{1}{h} \overrightarrow{p_{n+1} p_0}$. Mamy wtedy

$$p_{n+1} = p_0 + h \frac{1}{h} \overrightarrow{p_{n+1} p_0}$$

zaś punkty p_0, \dots, p_n mają w rozszerzonym układzie identyczne n współrzędnych, jak w pierwotnym (i ostatnie równe 0). \square

Widzicie zatem Państwo, że od dość ogólnych abstrakcyjnych rozważań przeszliśmy do bardzo konkretnych zastosowań. Jest ich więcej.

Obserwacja 15.7: Wniosek – pole, wzór 2.

Niech $p_0, \dots, p_n \in (\mathbb{R}^n, (V, \langle, \rangle)_{st})$ i niech $S = S(p_0, \dots, p_n)$. Niech też $\alpha_i = \overrightarrow{p_0 p_i}$, dla $i = 1, \dots, n$ oraz przyjmijmy $d_{ij} = \|p_i - p_j\|$, dla $0 \leq i, j \leq n$. Wówczas:

$$\mu_n(S)^2 = \frac{1}{2^n \cdot (n!)^2} \cdot \left| \det \begin{bmatrix} 0 & d_{01}^2 & \cdots & d_{0n}^2 & 1 \\ d_{10}^2 & 0 & \cdots & d_{1n}^2 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ d_{n0}^2 & d_{n1}^2 & \cdots & 0 & 1 \\ 1 & 1 & \cdots & 1 & 0 \end{bmatrix} \right|^2.$$

Przypadek szczególny. Wzór Herona. Niech Δ będzie trójkątem o bokach długości a, b, c i niech V będzie polem Δ . Dla $p = (a + b + c)/2$ mamy:

$$V^2 = \frac{1}{2^2 \cdot (2!)^2} \cdot \left| \det \begin{bmatrix} 0 & a^2 & c^2 & 1 \\ a^2 & 0 & b^2 & 1 \\ c^2 & b^2 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \right| = \frac{|-16p(p-a)(p-b)(p-c)|}{16}.$$

Dowód. Już wiemy, że

$$n! \cdot \mu_n(S) = \left| \det \begin{bmatrix} | & \dots & | \\ p_0 & \dots & p_n \\ | & \dots & | \\ 1 & \dots & 1 \end{bmatrix} \right| = \left| \det \begin{bmatrix} | & \dots & | \\ p_0 & \dots & p_n \\ | & \dots & | \\ 1 & \dots & 1 \end{bmatrix}^T \right|.$$

Możemy też zmodyfikować te macierze, nie zmieniając wyznaczników, i dostać:

$$n! \cdot \mu_n(S) = \left| \det \begin{bmatrix} - & p_0^T & - & 1 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ - & p_n^T & - & 1 & 0 \\ - & 0^T & - & 0 & 1 \end{bmatrix} \right| = \left| \det \begin{bmatrix} | & \dots & | & | \\ p_0 & \dots & p_n & 0 \\ | & \dots & | & | \\ 0 & \dots & 0 & 1 \\ 1 & \dots & 1 & 0 \end{bmatrix}^T \right|.$$

Mnożymy dwie macierze i na chwilę przypominamy sobie, że p_i to wektory. Zatem $(n! \cdot \mu_n(S))^2$ jest równe:

$$\left| \det \begin{bmatrix} \langle p_0, p_0 \rangle & \dots & \langle p_0, p_n \rangle & 1 \\ \vdots & & \vdots & \vdots \\ \langle p_n, p_0 \rangle & \dots & \langle p_n, p_n \rangle & 1 \\ 1 & \dots & 1 & 0 \end{bmatrix} \right| = 2^{-n} \cdot \left| \det \begin{bmatrix} 2\langle p_0, p_0 \rangle & \dots & 2\langle p_0, p_n \rangle & 1 \\ \vdots & & \vdots & \vdots \\ 2\langle p_n, p_0 \rangle & \dots & 2\langle p_n, p_n \rangle & 1 \\ 1 & \dots & 1 & 0 \end{bmatrix} \right|.$$

Dostaliśmy tę równość mnożąc pierwsze $n + 1$ wierszy przez 2 i jednocześnie dzieląc ostatnią kolumnę przez $\frac{1}{2}$. Teraz upraszczamy ten wyznacznik. Dla każdego k , gdzie $0 \leq k \leq n$ odejmujemy $\|p_k\|^2$ -razy ostatni wiersz od $(k + 1)$ -wszego wiersza, a jednocześnie odejmujemy $\|p_k\|^2$ -razy ostatnią kolumnę od kolumny $(k + 1)$ -wszej. Aby ogarnąć to, co powstanie wprowadzamy oznaczenia:

$$a_{ij} := 2\langle p_i, p_j \rangle - \|p_i\|^2$$

$$b_{ij} := 2\langle p_i, p_j \rangle - \|p_i\|^2 - \|p_j\|^2 = -\|p_i - p_j\|^2 = -d_{ij}^2.$$

Dostajemy (pamiętając, że $d_{ii} = \|p_i - p_i\| = 0$):

$$\begin{aligned} 2^n \cdot (n!)^2 \mu_n(S)^2 &= \left| \det \begin{bmatrix} 2\langle p_0, p_0 \rangle & \dots & 2\langle p_0, p_n \rangle & 1 \\ \vdots & & \vdots & \vdots \\ 2\langle p_n, p_0 \rangle & \dots & 2\langle p_n, p_n \rangle & 1 \\ 1 & \dots & 1 & 0 \end{bmatrix} \right| = \\ &= \left| \det \begin{bmatrix} a_{00} & \dots & a_{0n} & 1 \\ \vdots & & \vdots & \vdots \\ a_{n0} & \dots & a_{nn} & 1 \\ 1 & \dots & 1 & 0 \end{bmatrix} \right| = \left| \det \begin{bmatrix} b_{00} & \dots & b_{0n} & 1 \\ \vdots & & \vdots & \vdots \\ b_{n0} & \dots & b_{nn} & 1 \\ 1 & \dots & 1 & 0 \end{bmatrix} \right| = \\ &= \left| \det \begin{bmatrix} d_{00}^2 & \dots & d_{0n}^2 & -1 \\ \vdots & & \vdots & \vdots \\ d_{n0}^2 & \dots & d_{nn}^2 & -1 \\ 1 & \dots & 1 & 0 \end{bmatrix} \right| = \left| \det \begin{bmatrix} 0 & \dots & d_{0n}^2 & 1 \\ \vdots & & \vdots & \vdots \\ d_{n0}^2 & \dots & 0 & 1 \\ 1 & \dots & 1 & 0 \end{bmatrix} \right|. \end{aligned}$$

Obserwacja 15.8: Wniosek – pole, wzór 3.

Niech $p_0, \dots, p_n \in (\mathbb{R}^n, (V, \langle, \rangle)_{st})$ są równej długości: $\|p_i\| = r$ tzn. jeśli wszystkie wierzchołki p_i leżą na sferze o promieniu r o środku (gdzieś, czyli) w punkcie 0, to dla $S = S(p_0, \dots, p_n)$ mamy:

$$\mu_n(S)^2 = \frac{1}{2^{n+1}(n!)^2 r^2} \cdot \left| \det \begin{bmatrix} 0 & d_{01}^2 & \dots & d_{0n}^2 \\ d_{10}^2 & 0 & \dots & d_{1n}^2 \\ \vdots & \vdots & \ddots & \vdots \\ d_{n0}^2 & d_{n1}^2 & \dots & 0 \end{bmatrix} \right|.$$

Ilustracja. Niech \triangle będzie trójkątem o bokach długości a, b, c i niech V będzie polem \triangle . Jeśli r jest promieniem okręgu opisanego na trójkącie \triangle , to $4Vr = abc$.

$$V^2 = \frac{1}{2^{2+1} \cdot (2!)^2 \cdot r^2} \cdot \det \begin{bmatrix} 0 & a^2 & c^2 \\ a^2 & 0 & b^2 \\ c^2 & b^2 & 0 \end{bmatrix} = \frac{1}{2^{2+1} \cdot (2!)^2 \cdot r^2} \cdot 2a^2b^2c^2.$$

Dowód. Wiemy, że $r \cdot n! \cdot \mu_n(S)$ to (także):

$$r \cdot \left| \det \begin{bmatrix} | & & | \\ p_0 & \cdots & p_n \\ | & & | \\ 1 & & 1 \end{bmatrix} \right| = \left| \det \begin{bmatrix} | & & | \\ -p_0 & \cdots & -p_n \\ | & & | \\ r & & r \end{bmatrix} \right|.$$

A zatem $r \cdot n! \cdot \mu_n(S)$ równe jest:

$$r \cdot \left| \det \begin{bmatrix} - & p_0^T & - & 1 \\ & \vdots & & \vdots \\ - & p_n^T & - & 1 \end{bmatrix} \right| = \left| \det \begin{bmatrix} - & p_0^T & - & r \\ & \vdots & & \vdots \\ - & p_n^T & - & r \end{bmatrix} \right|.$$

$$r \cdot \left| \det \begin{bmatrix} | & & | \\ p_0 & \cdots & p_n \\ | & & | \\ 1 & & 1 \end{bmatrix} \right| = \left| \det \begin{bmatrix} | & & | \\ -p_0 & \cdots & -p_n \\ | & & | \\ r & & r \end{bmatrix} \right|.$$

A zatem wyznaczając:

$$(n!)^2 \cdot \mu_n(S)^2 \cdot r^2 = \left| \det \begin{bmatrix} r^2 - \|p_0\|^2 & r - \langle p_0, p_1 \rangle & \cdots & r^2 - \langle p_0, p_n \rangle \\ \vdots & \vdots & & \vdots \\ r^2 - \langle p_0, p_n \rangle & r^2 - \langle p_1, p_n \rangle & \cdots & r^2 - \|p_n\|^2 \end{bmatrix} \right|.$$

Stąd już wynika teza, bowiem mamy:

$$\begin{aligned} d_{ij}^2 &= \|p_i - p_j\|^2 = \|p_i\|^2 + \|p_j\|^2 - 2\langle p_i, p_j \rangle \\ &= r^2 + r^2 - 2\langle p_i, p_j \rangle \\ &= 2(r^2 - \langle p_i, p_j \rangle). \end{aligned}$$

Obserwacja 15.9: Wniosek - jeszcze jeden (ćwiczenie).

Niech p_0, \dots, p_{n+1} będą w \mathbb{R}^n . Wówczas dla $d_{ij} = \|p_i - p_j\|$ mamy:

$$-(-2)^n \det \underbrace{\begin{bmatrix} \|p_0\|^2 & p_0^T & 1 \\ \vdots & \vdots & \vdots \\ \|p_{n+1}\|^2 & p_{n+1}^T & 1 \end{bmatrix}}_A = \det \begin{bmatrix} 0 & d_{01}^2 & \cdots & d_{0n}^2 & 1 \\ d_{10}^2 & 0 & \cdots & d_{1n}^2 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ d_{n0}^2 & d_{n1}^2 & \cdots & 0 & 1 \\ 1 & 1 & \cdots & 1 & 0 \end{bmatrix}.$$

Co więcej, następujące warunki są równoważne.

- (1) Punkty v_0, \dots, v_{n+1} leżą na hiperpłaszczyźnie lub na sferze w \mathbb{R}^n .
- (2) Istnieją $a, c \in \mathbb{R}$, $b \in \mathbb{R}^n$ (nie wszystkie równe 0) takie, że $v = (v_0, \dots, v_{n+1})$ spełniają $a\|v\|^2 + 2\langle b, v \rangle + c = 0$;
- (3) $\det A = 0$.

Przykładowe zastosowanie: twierdzenie Ptolemeusza o czworokącie.

Jak Państwo widzicie, także z poziomu algebry liniowej (nie tylko analizy) dowodzić można szereg elementarnych rezultatów, także elementarnych. Można je traktować jako elementy geometrii analitycznej w n -wymiarach. Nie są one zasadniczą częścią wykładu, ponieważ zajmujemy się w nim strukturami i pojęciami przydatnymi nie tylko w geometrii, ale w i całej matematyce.

15.3 Trivia. Zastosowania macierzy Grama w zadaniach

Zadanie 1. *Miasteczko Nieparzystów liczy sobie n mieszkańców. Ich głównym zajęciem jest formowanie rozmaitych klubów, co grozi wielkim politycznym chaosem. Rada Nieparzystowa rozporządziła jednak, aby każdy klub miał nieparzystą liczbę członków. Co więcej każde dwa kluby muszą mieć parzystą liczbę wspólnych członków. Pokazać, że nie jest możliwe stworzenie więcej klubów, niż wynosi ludność Nieparzystowa.*

Liczba potencjalnych klubów, czyli podzbiorów zbioru n -elementowego wynosi 2^n , a więc więcej niż n . Ile wśród nich jest klubów o nieparzystej liczbie członków? Wydaje się, że również możliwe jest, żeby było ich więcej niż n . Gdy $n = 3$ mamy możliwe trzy kluby o jednym członku i jeden klub o trzech członkach, a więc więcej niż 3. Łatwo jednak sprawdzić, że konfiguracja taka nie może wystąpić w przypadku, gdy każde dwa kluby muszą mieć parzystą liczbę wspólnych członków. Jak to pokazać dla każdego n ?

Dowód. Ponumerujmy mieszkańców liczbami $1, 2, \dots, n$, a kluby nazwijmy C_1, \dots, C_m . Definiujemy macierz $A \in M_{n \times m}(\mathbb{R})$, w której kolumnach stoją „listy przynależności” do klubów. Dokładniej $A = (a_{ij})$:

$$a_{ij} = \begin{cases} 1, & \text{jeśli mieszkaniec } i \text{ należy do } C_j \\ 0, & \text{jeśli mieszkaniec } i \text{ nie należy do } C_j. \end{cases}$$

Przyjrzyjmy się teraz iloczynowi $A^T A$. Jest to macierz rozmiarów $m \times m$, której wyraz w wierszu i -tym oraz w kolumnie j -tej dostajemy ze wzoru: $\sum_{k=1}^n a_{ki} a_{kj}$. Co ta liczba oznacza?

Zauważmy, że i -ty wiersz macierzy A^T liczy sobie dokładnie n wyrazów i wyraz a_{ki} koduje przynależność k -tego mieszkańca do klubu C_i . Wyraz ten wynosi 1, jeśli k -ty mieszkaniec należy do klubu C_i oraz 0, jeśli nie należy. Mnożenie i -tego wiersza A^T oraz j -tego wiersza A to po prostu standardowy iloczyn skalarny „list przynależności” do klubów C_i i C_j . Proszę zauważyć, że iloczyn ten ma składniki równe 0 lub 1. Składnik $a_{ki} a_{kj}$ jest równy 1 wtedy i tylko wtedy gdy k -mieszkaniec jest członkiem zarówno klubu C_i jak i klubu C_j . A zatem wyraz macierzy $A^T A$ stojący w i -tym wierszu i j -tej kolumnie będący sumą takich $a_{ki} a_{kj}$ opisuje dokładnie liczbę wspólnych członków klubu i -tego i j -tego! To jest dokładnie macierz Grama układu wektorów opisujących „listy przynależności” do klubów od 1 do m . Zauważmy jeszcze, że można mówić o „prostopadłości” wektorów z listami klubów. Oznacza ona po prostu, że kluby nie mają wspólnych członków.

Co to oznacza dla naszego problemu? Prawo w Nieparzystowie implikuje, że na przekątnej naszej macierzy Grama $A^T A$ stoi nieparzysta liczba członków i -tego klubu (bo i -ty klub ma wszystkich członków wspólnych z i -tym klubem), a wszędzie indziej stoją liczby parzyste. Nietrudno pokazać, że macierz $A^T A$ rozmiaru $m \times m$ jest pełnego rzędu m . Wynika to stąd, że wyznacznik macierzy Grama jest liczbą całkowitą (wszystkie wyrazy są całkowite) zaś wyznacznik macierzy o współczynnikach całkowitych ma resztę z dzielenia przez 2 taką samą jak wyznacznik macierzy powstałej przez podmiany pierwotnych wyrazów przez ich reszty modulo 2. Można to pokazać na wiele sposobów. Natychmiast wynika to na przykład z wzoru permutacyjnego na wyznacznik. Np. dla zbadania parzystości wyznacznika macierzy całkowitoliczbowej:

$$\begin{vmatrix} 102495 & 550428 & 873298 & 660694 \\ 370628 & 909093 & 127450 & 925600 \\ 835044 & 601178 & 624653 & 263392 \\ 663780 & 487252 & 292276 & 593107 \end{vmatrix}$$

wystarczy wziąć każdy ze współczynników modulo 2 i dostajemy macierz I_4 , której wyznacznik jest nieparzysty.

W przypadku naszej „klubowej” macierzy Grama. Po wzięciu jej współczynników modulo 2 dostajemy I_m , a więc macierz $m \times m$ o niezerowym wyznaczniku 1. Zatem $r(A^T A) = m$. Na wykładzie przypomnieliśmy nierówność

$$m = r(A^T A) \leq r(A) = r(A^T) \leq n.$$

Klubów jest zatem nie więcej, niż mieszkańców. □

Podobnych zadań wykorzystujących „wektory przynależności” (lub wektory incydencji) jest znacznie więcej. Zachęcam Czytelnika do zmierzenia się z nimi.

Zadanie 2. Zbiór punktów $\{p_0, p_1, \dots, p_n\}$ przestrzeni euklidesowej afinicznej $(\mathbb{R}^n, \langle \cdot, \cdot \rangle)$ ma następującą własność: odległość dowolnych dwóch różnych punktów tego zbioru równa jest 1.

- Niech $\alpha_i = \overrightarrow{p_0 p_i}$, dla $i = 1, \dots, n$. Wyznacz macierz Grama $G(\alpha_1, \dots, \alpha_n)$.
- Pokaż, że układ punktów $\{p_0, p_1, \dots, p_n\}$ jest bazą punktową przestrzeni afinicznej $(\mathbb{R}^n, \langle \cdot, \cdot \rangle)$.
- Dla każdego $0 < k < n$ określamy $L_k = \text{af}(p_0, \dots, p_k)$, $S_k = \text{af}(p_{k+1}, \dots, p_n)$. Wykaż, że $L_k \cap S_k = \emptyset$.
- Dla $n = 3$ wyznacz odległość prostych $\text{af}(p_0, p_1)$ oraz $\text{af}(p_2, p_3)$.

ROZWIĄZANIE. Zaczniemy od (a). Zauważmy, że $\alpha_i - \alpha_j = \overrightarrow{p_0 p_i} - \overrightarrow{p_0 p_j} = \overrightarrow{p_j p_i}$. Przypomnijmy, że dla wektorów α, β przestrzeni euklidesowej mamy:

$$2\langle \alpha, \beta \rangle = \|\alpha\|^2 + \|\beta\|^2 - \|\alpha - \beta\|^2 \quad \Rightarrow \quad 2\langle \alpha_i, \alpha_j \rangle = \|\overrightarrow{p_0 p_i}\|^2 + \|\overrightarrow{p_0 p_j}\|^2 - \|\overrightarrow{p_j p_i}\|^2.$$

Dowodzimy (b). To, że $\{p_0, p_1, \dots, p_n\}$ jest bazą punktową \mathbb{R}^n jest równoważne temu, że $\alpha_1, \dots, \alpha_n$ jest bazą \mathbb{R}^n . Zgodnie z twierdzeniem z wykładu jest równoważne temu, że macierz Grama $G(\alpha_1, \dots, \alpha_n)$ jest odwracalna. To z kolei pokazujemy dowodząc, że $r(G(\alpha_1, \dots, \alpha_n)) = n$. Robimy to przez operacje elementarne. Wypisujemy macierz $2G(\alpha_1, \dots, \alpha_n)$ i odejmujemy ostatni wiersz od poprzednich. Dostajemy:

$$r \begin{bmatrix} 2 & 1 & \dots & 1 & 1 \\ 1 & 2 & \dots & 1 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & \dots & 2 & 1 \\ 1 & 1 & \dots & 1 & 2 \end{bmatrix} = r \begin{bmatrix} 1 & 0 & \dots & 0 & -1 \\ 0 & 1 & \dots & 0 & -1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -1 \\ 1 & 1 & \dots & 1 & 2 \end{bmatrix}.$$

Jest jasne, że pierwsze $n - 1$ wierszy uzyskanej macierzy jest liniowo niezależnych, a ostatni nie jest kombinacją liniową wcześniejszych (patrz pierwsze $n - 1$ współrzędnych). Stąd mamy tezę.

Dowodzimy (c). Załóżmy przeciwnie, że dla pewnych układów wag a_0, \dots, a_k oraz b_{k+1}, \dots, b_n mamy

$$a_0 p_0 + a_1 p_1 + \dots + a_k p_k = b_{k+1} p_{k+1} + \dots + b_n p_n.$$

Mamy $a_0 + a_1 + \dots + a_k - b_{k+1} - \dots - b_n = 1 - 1 = 0$ i wyrażenie wyżej można równoważnie przekształcić:

$$\begin{aligned} & a_0 p_0 + a_1 p_1 + \dots + a_k p_k - b_{k+1} p_{k+1} - \dots - b_n p_n + (a_0 + a_1 + \dots + a_k - b_{k+1} - \dots - b_n) p_0 = \\ & a_1 \overrightarrow{p_0 p_1} + a_2 \overrightarrow{p_0 p_2} + \dots + a_k \overrightarrow{p_0 p_k} - b_{k+1} \overrightarrow{p_0 p_{k+1}} - \dots - b_n \overrightarrow{p_0 p_n} = \\ & a_1 \alpha_1 + a_2 \alpha_2 + \dots + a_k \alpha_k - b_{k+1} \alpha_{k+1} - \dots - b_n \alpha_n = 0 \end{aligned}$$

Jednak jedna z liczb a_i, b_j jest niezerowa, a układ $\alpha_1, \dots, \alpha_n$ jest liniowo niezależny. Sprzeczność.

Przechodzimy do ostatniej części. Niech $K = \text{af}(p_0, p_1)$ oraz $L = \text{af}(p_2, p_3)$. Mamy

$$T(K) = \alpha_1, \quad T(L) = \overrightarrow{p_2 p_3} = \overrightarrow{p_0 p_3} - \overrightarrow{p_0 p_2} = \alpha_3 - \alpha_2.$$

Odległość d prostych K oraz L równa jest długości rzutu wektora łączącego dowolne dwa jej punkty na przestrzeń prostopadłą do $\text{lin}(T(K), T(L))$. Ten wektor łączący to może być np. $\overrightarrow{p_0 p_3} = \alpha_3$, zaś owa przestrzeń, na którą rzutujemy to $\text{lin}(\alpha_1, \alpha_3 - \alpha_2)^\perp$. Zgodnie z twierdzeniem z wykładu (typu „objętość = podstawa \times wysokość”) mamy:

$$d = \sqrt{\frac{W(\alpha_1, \alpha_3 - \alpha_2, \alpha_3)}{W(\alpha_1, \alpha_3 - \alpha_2)}}.$$

Bez trudu wyznaczamy

$$G(\alpha_1, \alpha_3 - \alpha_2, \alpha_3) = \begin{bmatrix} 1 & 0 & \frac{1}{2} \\ 0 & 1 & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & 1 \end{bmatrix},$$

skąd szukana odległość to $\frac{\sqrt{2}}{2}$.

Uwaga 1. Idea geometryczna: realizując wierzchołki czworościanu foremego jako wierzchołki sześciangu o krawędzi $\frac{\sqrt{2}}{2}$ (krawędzie czworościanu to przekątne ścian bocznych sześciangu) dostajemy uzyskaną odpowiedź, bo szukana odległość prostych równa jest odległości przeciwległych ścian sześciangu.

Uwaga 2. Zachęcam Czytelnika do pokazania, że $\rho(L_k, S_k)$ równa jest, w zależności od n :

$$\sqrt{\frac{W(\alpha_1, \dots, \alpha_k, \alpha_n - \alpha_{k+1}, \dots, \alpha_n - \alpha_{n-1}, \alpha_n)}{W(\alpha_1, \dots, \alpha_k, \alpha_n - \alpha_{k+1}, \dots, \alpha_n - \alpha_{n-1})}} = \sqrt{\frac{n+1}{2(k+1)(n-k)}}.$$

Powyższe zadanie pochodzące z jednego z kolokwiów dotyczy przykładu zbioru, który nazywamy czasem równobocznym. Oto definicja pochodząca ze znanych 33 Miniatur J. Matouska.

Definicja 15.7: Zbiór równoboczny

Podzbiór równoboczny w przestrzeni afinicznej \mathbb{R}^n to zbiór punktów p_1, \dots, p_k takich, że wszystkie pary punktów p_i, p_j są równoodległe.

Na podstawie naszych rozważań nietrudno zobaczyć, że zbiór równoodległy w \mathbb{R}^n ma nie więcej niż $n+1$ punktów — tak jak sympleks d -wymiarowy oraz zbiór rozważany w zadaniu wyżej.

Problem znajdowania zbiorów równoodległych komplikuje się, gdy przejdziemy do innej metryki⁴, na przykład do metryki rzeka, zwanej w matematyce metryką l_1 : dla punktów $x = (x_1, \dots, x_n)$ oraz $y = (y_1, \dots, y_n)$ w przestrzeni \mathbb{R}^n określamy:

$$d(x, y) = |x_1 - y_1| + |x_2 - y_2| + \dots + |x_n - y_n|.$$

Przypomnijmy, że w metryce tej poruszamy się tylko wzdłuż prostych równoległych do osi. Dla tej metryki możemy łatwo wskazać zbiór równoodległy złożony z $2n$ elementów $\{e_1, -e_1, e_2, -e_2, \dots, e_n, -e_n\}$ gdzie e_i jest wektorem standardowym. Co ciekawe istnieje problem otwarty Kusnera z 1983 roku mówiący, że zbiór równoodległy nie może mieć więcej elementów. Aż do 2001 nie było jasno, że ograniczenie górne ma nie więcej niż $2^n - 1$ elementów. W następnych latach pojawiło się wiele ulepszeń tego wyniku, ale ostatecznego rozstrzygnięcia hipotezy wciąż nie ma.

Na koniec warto wspomnieć, że z macierzy Grama można odczytywać interesujące fakty dotyczące układów odległości w przestrzeni euklidesowej. Oto przykład.

Obserwacja 15.10

Nie istnieją cztery punkty na płaszczyźnie, których odległości są wszystkie liczbami nieparzystymi.

Dowód. Gdyby taki układ punktów istniał, to bez straty ogólności moglibyśmy założyć, że jeden z nich jest 0, a pozostałe to a, b, c (zakładamy, że jesteśmy w przestrzeni liniowej \mathbb{R}^2). Zgodnie z założeniami obserwacji liczby $\|a\|, \|b\|, \|c\|, \|a-b\|, \|b-c\|, \|c-a\|$ są nieparzyste.

Kluczowe jest, że gdy m jest liczbą nieparzystą, wtedy m^2 daje resztę 1 z dzielenia przez 8. Z twierdzenia kosinusów mamy zatem

$$2\langle a, b \rangle = \|a\|^2 + \|b\|^2 - \|a-b\|^2$$

co oznacza, że liczby $2\langle a, b \rangle, 2\langle a, c \rangle$ oraz $2\langle b, c \rangle$ też dają resztę 1 z dzielenia przez 8. W szczególności macierz Grama $G(a, b, c)$ ma tę własność, że oglądana modulo 8 ma postać:

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

Wyznacznik tej macierzy wynosi 4, a więc rząd macierzy $G(a, b, c)$ wynosi 3 (nie przystaje 0 modulo 8). Z drugiej strony mówimy o macierzy Grama układu 3 wektorów na płaszczyźnie — układu liniowo zależnego. A więc jej wyznacznik wynosi 0, zgodnie z faktem z wykładu. Uzyskaliśmy sprzeczność. \square

⁴Znowu odsyłam do 33 Miniatur J. Matouska: <https://kam.mff.cuni.cz/~matousek/stml-53-matousek-1.pdf>

Zadanie 3. W zorientowanej przestrzeni euklidesowej afinicznej $(\mathbb{R}^3, \langle \cdot, \cdot \rangle_{st})$ dany jest układ ośmiu punktów p_1, \dots, p_8 stanowiących zbiór wierzchołków równoległościanu $R = R(p_1; \overrightarrow{p_1p_2}, \overrightarrow{p_1p_3}, \overrightarrow{p_1p_5})$, przy czym spełnione są warunki $\overrightarrow{p_1p_2} + \overrightarrow{p_1p_3} = \overrightarrow{p_1p_4}$ oraz $\overrightarrow{p_5p_6} + \overrightarrow{p_5p_7} = \overrightarrow{p_5p_8}$.

Założmy, że R jest sześcianem, oraz że dla pewnej płaszczyzny $P \subset \mathbb{R}^3$ odległość punktu p_i od P równa jest i , dla $1 \leq i \leq 8$. Wyznacz długość krawędzi sześcianu R .

Uwaga. Wierzchołki $R = R(p_1; \alpha_1, \alpha_2, \alpha_3)$ to punkty postaci $p_1 + \epsilon_1\alpha_1 + \epsilon_2\alpha_2 + \epsilon_3\alpha_3$, gdzie $\epsilon_i \in \{0, 1\}$.

ROZWIĄZANIE. Odpowiedź to $\sqrt{21}$. Niech $T(P)^\perp = \text{lin}(\delta)$. Załóżmy też bez straty ogólności, że $\|\delta\| = 1$. Zauważmy, że zgodnie z założeniem rzuty α, β, γ na $\text{lin}(\delta)$ to wektory mające długości odpowiednio 1, 2, 4. Rzuty te mają jednocześnie postać (odpowiednio):

$$\frac{\langle \alpha, \delta \rangle}{\|\delta\|^2} \delta, \quad \frac{\langle \beta, \delta \rangle}{\|\delta\|^2} \delta, \quad \frac{\langle \gamma, \delta \rangle}{\|\delta\|^2} \delta$$

Liczby $\langle \alpha, \delta \rangle, \langle \beta, \delta \rangle, \langle \gamma, \delta \rangle$ są zatem równe co do modułu odpowiednio 1, 2, 4.

Skoro R jest sześcianem, to $\|\alpha\| = \|\beta\| = \|\gamma\|$ oraz układ α, β, γ jest prostopadły. To oznacza, że:

$$G(\alpha, \beta, \gamma, \delta) = \begin{bmatrix} \langle \alpha, \alpha \rangle & \langle \alpha, \beta \rangle & \langle \alpha, \gamma \rangle & \langle \alpha, \delta \rangle \\ \langle \beta, \alpha \rangle & \langle \beta, \beta \rangle & \langle \beta, \gamma \rangle & \langle \beta, \delta \rangle \\ \langle \gamma, \alpha \rangle & \langle \gamma, \beta \rangle & \langle \gamma, \gamma \rangle & \langle \gamma, \delta \rangle \\ \langle \delta, \alpha \rangle & \langle \delta, \beta \rangle & \langle \delta, \gamma \rangle & \langle \delta, \delta \rangle \end{bmatrix} = \begin{bmatrix} \|\alpha\|^2 & 0 & 0 & \pm 1 \\ 0 & \|\alpha\|^2 & 0 & \pm 2 \\ 0 & 0 & \|\alpha\|^2 & \pm 4 \\ \pm 1 & \pm 2 & \pm 4 & 1 \end{bmatrix},$$

przy czym macierz wyżej jest symetryczna. Układ $\alpha, \beta, \gamma, \delta$ jest liniowo zależny, czyli $W(\alpha, \beta, \gamma, \delta) = 0$. Wyznacznik ten jest natomiast równy $\|\alpha\|^6 - 21\|\alpha\|^4$, niezależnie od wyboru znaków $\langle \alpha, \delta \rangle, \langle \beta, \delta \rangle, \langle \gamma, \delta \rangle$. Wynika to z faktu, że przy operacji zamiany jednego z wektorów α, β, γ na przeciwny (co zmieniłoby tylko znak iloczynu skalarnego z δ) wyznacznik Grama się nie zmienia. Skoro $\|\alpha\| > 0$, to $\|\alpha\| = \sqrt{21}$.

Autorem zadania jest Łukasz Bożyk, patrz: <https://www.deltami.edu.pl/delta/archiwum/2018/12/2018/12/04/0-DELTA-2018-12.pdf>, str 3. Elementarne rozwiązanie (jedno z wielu) — na str. 5.

Rozdział 16

Orientacja i iloczyn wektorowy

Kolejny wykład geometryczny poświęcamy dwóm fundamentalnym pojęciom związanych ze znakiem wyznacznika. Pierwsze z nich – orientacja, pozwala na rozważanie „ n -wymiarowej miary ze znakiem”. Drugie – iloczyn wektorowy, jest podstawowym narzędziem geometrii przestrzennej, nie tylko w matematyce.

Definicja 16.1: Bazy zgodnie i przeciwnie zorientowane

Niech V będzie n -wymiarową przestrzenią nad ciałem \mathbb{R} . Mówimy, że bazy $\mathcal{A} = \{\alpha_1, \dots, \alpha_n\}$, $\mathcal{B} = \{\beta_1, \dots, \beta_n\}$ przestrzeni V są:

- ZGODNIE ZORIENTOWANE, jeśli $\det M(\text{id})_{\mathcal{A}}^{\mathcal{B}} > 0$,
- PRZECIWNIE ZORIENTOWANE, jeśli $\det M(\text{id})_{\mathcal{A}}^{\mathcal{B}} < 0$.

Przykład. Bazy $\mathcal{A} = \{(3, 2), (7, 4)\}$ oraz $\mathcal{B} = \{(1, 2), (1, 0)\}$ przestrzeni \mathbb{R}^2 są zgodnie zorientowane, bo:

$$\det M(\text{id})_{\mathcal{A}}^{\mathcal{B}} = \begin{vmatrix} 1 & 2 \\ 2 & 5 \end{vmatrix} > 0.$$

Relacja zgodnego zorientowania jest relacją równoważności w zbiorze wszystkich baz w przestrzeni liniowej V wymiaru n . Aby się o tym przekonać sprawdzamy trzy własności relacji równoważności.

- **Zwrotność.** Jeśli \mathcal{A} jest bazą V to $M(\text{id})_{\mathcal{A}}^{\mathcal{A}} = I$, czyli bazy \mathcal{A} oraz \mathcal{A} są zgodnie zorientowane.
- **Symetryczność.** Jeśli \mathcal{A}, \mathcal{B} są bazami V to $M(\text{id})_{\mathcal{A}}^{\mathcal{B}} = (M(\text{id})_{\mathcal{B}}^{\mathcal{A}})^{-1}$, czyli

$$\det M(\text{id})_{\mathcal{A}}^{\mathcal{B}} > 0 \Rightarrow \det M(\text{id})_{\mathcal{B}}^{\mathcal{A}} > 0.$$

- **Przechodność.** Jeśli $\mathcal{A}, \mathcal{B}, \mathcal{C}$ są bazami V to $M(\text{id})_{\mathcal{A}}^{\mathcal{C}} = M(\text{id})_{\mathcal{B}}^{\mathcal{C}} \cdot M(\text{id})_{\mathcal{A}}^{\mathcal{B}}$, czyli

$$\det M(\text{id})_{\mathcal{A}}^{\mathcal{B}} > 0, \det M(\text{id})_{\mathcal{B}}^{\mathcal{C}} > 0 \Rightarrow \det M(\text{id})_{\mathcal{A}}^{\mathcal{C}} > 0.$$

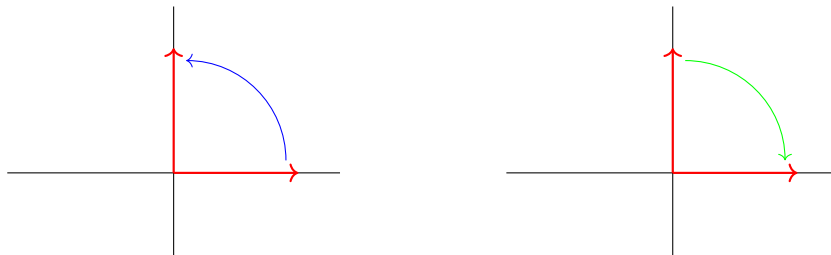
Uwaga: dla każdej bazy $\mathcal{A} = (\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n)$ przestrzeni V nad ciałem \mathbb{R} oraz bazy $\mathcal{A}' = (\alpha_2, \alpha_1, \alpha_3, \dots, \alpha_n)$ powstałej przez zamianę kolejności (pierwszych) dwóch wektorów, wówczas:

- bazy \mathcal{A} oraz \mathcal{A}' są przeciwnie zorientowane,
- każda baza przestrzeni liniowej V jest zgodnie zorientowana z \mathcal{A} lub \mathcal{A}' .

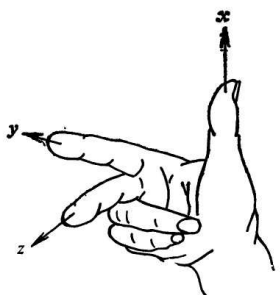
Definicja 16.2: Orientacja

Rodzinę wszystkich baz zgodnie zorientowanych z pewną bazą przestrzeni V nad ciałem \mathbb{R} nazywamy ORIENTACJĄ przestrzeni V . Mówimy, że przestrzeń V jest ZORIENTOWANA, jeśli wybrana jest jedna z jej (dwóch) orientacji. W przestrzeni zorientowanej baza \mathcal{A} jest DODATNIO (UJEMNIE) ZORIENTOWANA, jeśli jest zorientowana zgodnie (przeciwnie) z wybraną orientacją przestrzeni V .

Zauważmy, że dokonanie wyboru jednej z dwóch dostępnych orientacji przestrzeni liniowej (czy afinicznej) nie jest w żaden sposób uzasadnione matematycznie. Innymi słowy — wybór orientacji prowadzi do dwóch dualnych „geometrii”. Mimo wszystko wyborów tych często dokonujemy w oparciu o czynniki pozamatematyczne (np. biorąc pod uwagę ruch Ziemi czy ludzką anatomie). Ustalając orientację na płaszczyźnie mówimy o kierunku zgodnym lub przeciwnym ze wskazówkami zegara ustalamy tak naprawdę kolejność wektorów obranej bazy (np. standardowej). Jeśli płaszczyzna zorientowana jest zgodnie z bazą standardową, wówczas mówimy o orientacji przeciwnej do wskazówek zegara.



Szereg innych pojęć matematycznych można określać w oparciu o orientację, na przykład „leżenie po stronie” prostej (na płaszczyźnie) czy płaszczyzny (w przestrzeni) czy też „leżenie wewnątrz” krzywej zamkniętej. Są to pojęcia delikatne, w zależności od rozważanego obiektu, ale ważne choćby w analizie czy topologii.



Sz szczególnie ważna jest znana z fizyki interpretacja wyboru orientacji w oparciu o układ palców prawej ręki, gdzie mówimy o orientacji prawoskrętnej w oparciu o bazę utworzoną przez kierunki kciuka, palca wskazującego oraz środkowego. Również w przestrzeni czterowymiarowej można w sposób naiwny mówić o orientacji, choćby powołując się na interpretację czwartego wymiaru jako czasu. W ten sposób możemy mówić, że jakieś wydarzenia były wcześniej lub później niż inne. Sprawa jest oczywiście skomplikowana.

Po ustaleniu orientacji w przestrzeni euklidesowej możemy mówić o zorientowanej mierze n -wymiarowej. Po prostu mówimy, że objętość równoległoscianu rozpiętego na bazie $\alpha_1, \dots, \alpha_n$ wynosi $\pm \sqrt{W(\alpha_1, \dots, \alpha_n)}$, przy czym wybór znaku zależy od tego, czy baza $\alpha_1, \dots, \alpha_n$ jest dodatnio, czy ujemnie zorientowana. Czytelnika zainteresowanego tymi zagadnieniami w kontekście elementarnym zachęcam do lektury pracy „Zorientowane pole wielokątów” Agnieszki Burskiej¹.

Definicja 16.3

Załóżmy, że V jest zorientowaną przestrzenią liniową skończonego wymiaru nad \mathbb{R} . Izomorfizm $\phi : V \rightarrow V$ nazwiemy AUTOMORFIZMEM V . Powiemy, że automorfizm ϕ przestrzeni V :

- ZACHOWUJE ORIENTACJĘ V , jeśli dla każdej jej (równow. pewnej) bazy dodatnio zorientowanej przestrzeni $(\alpha_1, \dots, \alpha_n)$ baza $(\phi(\alpha_1), \dots, \phi(\alpha_n))$ jest dodatnio zorientowana,
- ZMIENIA ORIENTACJĘ V , jeśli nie zachowuje orientacji.

Łatwo sprawdzić, że automorfizm ϕ zachowuje orientację wtedy i tylko wtedy, gdy $\det \phi > 0$, a zmienia ją tylko wtedy, gdy $\det \phi < 0$. Przykładem automorfizmu zachowującego orientację jest obrót, a zmieniającą

¹http://www.math.uni.wroc.pl/~swiatkow/Repozytorium/pole/prace/skan_burska_zorient_pole.pdf.

ją – symetria prostopadła n -wymiarowej przestrzeni względem podprzestrzeni wymiaru $n - 1$.

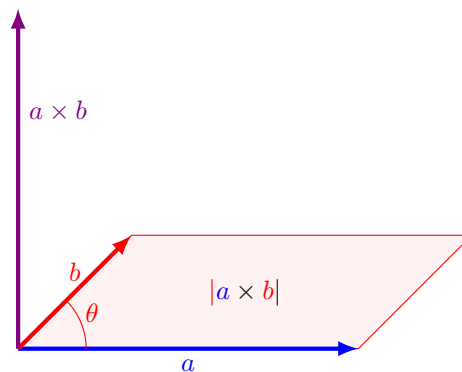
Wprowadźmy jeszcze jedno pojęcie, istotne z punktu widzenia rachunkowego i dla wielu zastosowań. Mówi ono o tym, że wybór iloczynu skalarnego i orientacji w n -wymiarowej przestrzeni liniowej V nad \mathbb{R} pozwala podać geometryczną metodę dopełniania liniowo niezależnego układu $n - 1$ wektorów z V do dodatnio zorientowanej bazy V .²

Definicja 16.4: Iloczyn wektorowy

Niech $(V, \langle \cdot, \cdot \rangle)$ będzie n -wymiarową przestrzenią euklidesową liniową, zorientowaną (przez pewną bazę). Niech $\alpha_1, \dots, \alpha_{n-1}$ będzie układem wektorów przestrzeni V . ILOCZYNEM WEKTOROWYM układu $\alpha_1, \dots, \alpha_{n-1}$ nazywamy wektor β , oznaczany dalej: $\alpha_1 \times \dots \times \alpha_{n-1}$, taki, że:

- (i) jeśli układ $\alpha_1, \dots, \alpha_{n-1}$ jest liniowo zależny, to $\beta = 0$,
- (ii) jeśli układ $\alpha_1, \dots, \alpha_{n-1}$ jest liniowo niezależny, to:
 - $\beta \in \text{lin}(\alpha_1, \dots, \alpha_{n-1})^\perp$,
 - $\|\beta\| = \sqrt{W(\alpha_1, \dots, \alpha_{n-1})}$,
 - baza $\alpha_1, \dots, \alpha_{n-1}, \beta$ jest dodatnio zorientowana.

Zobaczmy ilustrację iloczynu wektorowego w przestrzeni trójwymiarowej.



Warto odnotować następującą intuicję dotyczącą równoległociąnu 2-wymiarowego rozpiętego przez układ dwóch wektorów u, v w przestrzeni trójwymiarowej. W tym przypadku długość wektora $u \times v$ to po prostu pierwiastek z wyznacznika macierzy

$$\begin{bmatrix} \langle u, u \rangle & \langle u, v \rangle \\ \langle v, u \rangle & \langle v, v \rangle \end{bmatrix},$$

czyli $\|u\|^2 \cdot \|v\|^2 - \langle u, v \rangle^2$. A zatem dostaliśmy następującą równość:

$$\|u\|^2 \|v\|^2 = \langle u, v \rangle^2 + \|u \times v\|^2.$$

Wzór ten można interpretować jako znaną nam ze szkoły jedynkę trygonometryczną? Warto przy tej okazji odpowiedzieć sobie samodzielnie na pytanie: kiedy iloczyn wektorowy równy jest zero?

Przytoczmy dwa przykłady związane z rachunkami na iloczynie wektorowym.

Przykład. W przestrzeni liniowej $(\mathbb{R}^3, \langle \cdot, \cdot \rangle)$ mamy orientację wyznaczoną przez (przeciwnie zorientowaną do standardowej) bazę $((0, 1, 0), (1, 0, 0), (0, 0, 1))$. Niech $\alpha_1 = (1, 0, 2)$ oraz $\alpha_2 = (3, 2, 1)$. Wówczas:

- $\text{lin}((1, 0, 2), (3, 2, 1))^\perp = \text{lin}((4, -5, -2))$.
- $\sqrt{W(\alpha_1, \alpha_2)} = \sqrt{45}$.

²Definicja ta ma również ważne motywacje fizyczne; wiele momentów fizycznych za pomocą iloczynu wektorowego definiuje się moment siły lub moment pędu. Jest ono szczególnie przydatne w geometrii rzeczywistej przestrzeni trójwymiarowej, stanowiąc swego rodzaju namiastkę „operacji mnożenia wektorów”.

Wektor $(4, -5, -2)$ jest prostopadły do α_1, α_2 , ma długość $\sqrt{45}$ i baza

$$\alpha_1, \alpha_2, (4, -5, -2)$$

jest przeciwnie zorientowana z bazą standardową, a więc zgodna z wybraną orientacją. Mamy więc:

$$\alpha_1 \times \alpha_2 = (4, -5, -2).$$

Przykład. W przestrzeni liniowej \mathbb{R}^3 ze standardowym iloczynem skalarnym zorientowanej zgodnie z bazą standardową znaleźć równanie płaszczyzny L zawierającej punkt $(0, 0, 1)$, która przechodzi przez punkty $a = (1, 1, 3), b = (4, 1, 1), c = (5, 2, 0)$.

Zauważmy, że $T(L)$ jest płaszczyzną opisaną przez równanie

$$a_1x_1 + a_2x_2 + a_3x_3 = 0$$

i niezerowy wektor (a_1, a_2, a_3) wyznacza ją z dokładnością do stałej. Jest to wektor prostopadły do $T(L)$. Możemy więc przyjąć $(a_1, a_2, a_3) = \vec{ab} \times \vec{ac}$. Gdy wyznaczymy ten wektor pozostanie wyznaczyć równanie

$$a_1x_1 + a_2x_2 + a_3x_3 = d$$

płaszczyzny L przez wstawienie do otrzymanego równania punktu $(0, 0, 1)$.

Wyznaczanie iloczynu wektorowego jest szczególnie proste w przypadku wektorów przestrzeni trójwymiarowej danych za pomocą współrzędnych w bazie ortonormalnej.

Obserwacja 16.1

Niech $(V, \langle \cdot, \cdot \rangle)$ będzie trójwymiarową zorientowaną przestrzenią euklidesową liniową oraz niech $\mathcal{B} = (\beta_1, \beta_2, \beta_3)$ będzie jej bazą ortonormalną, dodatnio zorientowaną. Dla dowolnych wektorów $\alpha = a_1\beta_1 + a_2\beta_2 + a_3\beta_3$ oraz $\beta = b_1\beta_1 + b_2\beta_2 + b_3\beta_3$ zachodzi

$$\alpha \times \beta = \begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix} \beta_1 - \begin{vmatrix} a_1 & a_3 \\ b_1 & b_3 \end{vmatrix} \beta_2 + \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} \beta_3.$$

Dowód. Niech γ będzie wektorem zdefiniowanym w tezie naszej obserwacji (po prawej stronie ostatniej równości). Mamy

$$\langle \alpha, \gamma \rangle = a_1 \begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix} - a_2 \begin{vmatrix} a_1 & a_3 \\ b_1 & b_3 \end{vmatrix} + a_3 \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} = \begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ a_1 & a_2 & a_3 \end{vmatrix} = 0.$$

Analogicznie $\langle \beta, \gamma \rangle = 0$. Stąd $\gamma \in \text{lin}(\alpha, \beta)^\perp$. Mamy dalej:

$$\begin{aligned} \|\gamma\|^2 &= \begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix}^2 + \begin{vmatrix} a_1 & a_3 \\ b_1 & b_3 \end{vmatrix}^2 + \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}^2 = \\ &= (a_2b_3 - a_3b_2)^2 + (a_1b_3 - a_3b_1)^2 + (a_1b_2 - a_2b_1)^2 = \\ &= (a_1^2 + a_2^2 + a_3^2)(b_1^2 + b_2^2 + b_3^2) - (a_1b_1 + a_2b_2 + a_3b_3)^2 = \\ &= \langle \alpha, \alpha \rangle \cdot \langle \beta, \beta \rangle - \langle \alpha, \beta \rangle^2 = W(\alpha, \beta). \end{aligned}$$

Gdy α, β są liniowo niezależne, to dla $\mathcal{A} = (\alpha, \beta, \gamma)$ oraz $\mathcal{B} = (\beta_1, \beta_2, \beta_3)$:

$$\det M(\text{id})_{\mathcal{A}}^{\mathcal{B}} = \begin{vmatrix} a_1 & b_1 & \begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix} \\ a_2 & b_2 & -\begin{vmatrix} a_1 & a_3 \\ b_1 & b_3 \end{vmatrix} \\ a_3 & b_3 & \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} \end{vmatrix} = \begin{vmatrix} a_1 & b_1 & \begin{vmatrix} a_2 & b_2 \\ a_3 & b_3 \end{vmatrix} \\ a_2 & b_2 & -\begin{vmatrix} a_1 & b_1 \\ a_3 & b_3 \end{vmatrix} \\ a_3 & b_3 & \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} \end{vmatrix},$$

co po rozwinięciu względem trzeciej kolumny daje:

$$\begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix}^2 + \begin{vmatrix} a_1 & a_3 \\ b_1 & b_3 \end{vmatrix}^2 + \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}^2 > 0,$$

bo inaczej $(a_1, a_2, a_3), (b_1, b_2, b_3)$ będą liniowo zależne. Zatem układ α, β, γ tworzy bazę dodatnio zorientowaną (zorientowaną zgodnie z bazą $\beta_1, \beta_2, \beta_3$). Stąd $\alpha \times \beta$ jest równy γ . \square

16.1 Zadania do samodzielnej pracy

Zadania ilustrujące umiejętności niezbędne do zaliczenia przedmiotu oznaczone są symbolem ♠.

Przy tych zadaniach dodany jest opis umiejętności, które sprawdzają.

1. (♠ Wyznaczanie iloczynu wektorowego). W poniższym zadaniu rozważamy przestrzeń liniową \mathbb{R}^3 ze standardowym iloczynem skalarnym.

- Oblicz $(1, -1, 0) \times (1, 1, 0)$.
- Niech $u_1 = (1, 2, -1)$, $u_2 = (-1, 2, 0)$, $u_3 = (-2, 3, 1)$. Wyznacz wszystkie $v \in \mathbb{R}^3$ spełniające $u_1 \times v = u_2$ oraz $\langle u_3, v \rangle = 3$.
- Podaj przykład wektora $\alpha \in \mathbb{R}^3$, takiego że $(1, -1, 0) \times \alpha = (1, 1, 0)$.
- Wykaż, że dla dowolnych wektorów $\alpha, \beta, \gamma, \delta$ układ $\alpha \times \beta, \alpha \times \gamma, \alpha \times \delta$ jest liniowo zależny.
- Niech $u = (1, 2, 2)$ oraz $v = (1, 3, 3)$. Uzasadnij, że wektory $u, u \times v$ oraz $u \times (v \times u)$ tworzą bazę ortogonalną. Wyznacz współrzędne wektora v w tej bazie.
- Niech $u = (1, 2, 0) \in \mathbb{R}^3$. Opisz wszystkie wektory $v \in \mathbb{R}^3$ spełniające $u \times (u \times v) = v$. Udowodnij, że gdy $v \in \mathbb{R}^3$, to $u = v \times (u \times v) \iff u \perp v$ oraz $\|v\| = 1$.

2. Niech u, v, w będą wektorami w przestrzeni euklidesowej \mathbb{R}^3 . Wykaż, że

- $u \times v = -v \times u$,
- $\langle v_1 \times v_2, v_3 \rangle = \langle v_3 \times v_1, v_2 \rangle$.
- $\|v_1 \times v_2\|^2 + \langle v_1, v_2 \rangle^2 = \|v_1\|^2 \|v_2\|^2$.
- $v_1 \times (v_2 \times v_3) = \langle v_1, v_3 \rangle v_2 - \langle v_1, v_2 \rangle v_3$.
- $v_1 \times (v_2 \times v_3) + v_2 \times (v_3 \times v_1) + v_3 \times (v_1 \times v_2) = 0$.
- $(v_1 \times v_2) \times (v_3 \times v_4) = \langle v_1 \times v_3, v_4 \rangle v_2 - \langle v_2 \times v_3, v_4 \rangle v_1$.

3. (♠ Zgodne zorientowane bazy)

- Które z podanych baz przestrzeni \mathbb{R}^3 wyznaczają tę samą orientację?

$$\mathcal{A} = ((1, 0, 3), (1, 1, 1), (2, -1, 0)),$$

$$\mathcal{B} = ((2, 1, 1), (2, -1, 1), (2, 1, -1)),$$

$$\mathcal{C} = ((-1, 0, -1), (3, 2, -1), (0, 1, 0))$$

- Niech α, β będą wektorami w zorientowanej trójwymiarowej przestrzeni euklidesowej liniowej $(V, \langle \cdot, \cdot \rangle)$. Czy baza $(\alpha, \beta \times \alpha, \beta)$ przestrzeni V jest dodatnio, czy ujemnie zorientowana?
- Niech $A \in M_n(\mathbb{R})$ będzie macierzą o kolumnach k_1, \dots, k_n i niech $B \in M_n(\mathbb{R})$ będzie macierzą o kolumnach t_1, \dots, t_n . Załóżmy, że $\det A = -3$ i $\det B = -7$. Czy bazy k_1, \dots, k_n oraz t_1, \dots, t_n są zgodnie zorientowane?
- Załóżmy, że wektory $v_1, v_2, v_3 \in \mathbb{R}^4$ uzyskane są przez zastosowanie algorytmu Grama-Schmidta do układu liniowo niezależnych wektorów $u_1, u_2, u_3 \in \mathbb{R}^4$. Wykaż, że $v_1 \times v_2 \times v_3 = u_1 \times u_2 \times u_3$.

4. (♠ Zachowywanie orientacji przez endomorfizm)

- Niech $(V, \langle \cdot, \cdot \rangle)$ będzie przestrzenią euklidesową liniową, $\phi : V \rightarrow V$ izomorfizmem liniowym zmieniającym orientację. Czy istnieje izomorfizm $\psi : V \rightarrow V$, taki że $\psi \circ \phi$ zachowuje orientację?
- Dana jest przestrzeń euklidesowa \mathbb{R}^3 ze standardowym iloczynem skalarnym. Dla jakich wartości parametru $t \in \mathbb{R}$ przekształcenie $\phi : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ zachowuje orientację, gdzie

$$\phi((x_1, x_2, x_3)) = (2x_1 + tx_2 + 2x_3, -x_1 + 2x_2 + 2x_3, 2x_1 + 2x_2 - x_3)?$$

- Niech $(V, \langle \cdot, \cdot \rangle)$ będzie przestrzenią euklidesową liniową. Dla jakich k złożenie k symetrii prostopadłych względem podprzestrzeni W_1, \dots, W_k wymiaru $\dim V - 1$ zmienia orientację V ?

5. Dany jest wektor v w przestrzeni euklidesowej liniowej $(V, \langle \cdot, \cdot \rangle)$ spełniający $\|v\| = 1$. Wykaż, że rzut prostopadły $\phi : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ na podprzestrzeń $V = \text{lin}(v)^\perp$ dany jest wzorem $\phi(\alpha) = v \times (\alpha \times v)$.

6. Wykaż, że jeśli wektory $\alpha = (a_1, a_2, a_3), \beta = (b_1, b_2, b_3), \gamma = (c_1, c_2, c_3)$ należą do $(\mathbb{R}^3, \langle \cdot, \cdot \rangle_{st})$, to miara 3-wymiarowa równoległoscianu $R(\alpha, \beta, \gamma)$ równa jest

$$|\langle \alpha \times \beta, \gamma \rangle| = \left| \det \begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{bmatrix} \right|.$$

16.2 Uzupełnienie. Orientowalność i transformacje ciągłe

Badanie macierzy nie ogranicza się jedynie do algebry liniowej. W dalszych etapach studiów poznać Państwo także ich „grupową” i „pierścieniową” naturę. Tak się składa, że podejście „grupowe” pojawiło się na naszym wykładzie. Warto więc dodać kilka komentarzy.

Definicja 16.5: Grupa macierzy odwracalnych

Niech K będzie ciałem oraz niech n będzie dodatnią liczbą całkowitą. Przez $GL(n, K)$ oznaczamy podzbiór $M_n(K)$ złożony z macierzy odwracalnych.

Oznaczenie wprowadzone wyżej nie pojawia się na kursie, bowiem macierze $GL(n, K)$ nie tworzą podprzestrzeni. Tworzą one jednak grupę ze względu na mnożenie, co oznacza, że

- złożenie macierzy odwracalnych jest macierzą odwracalną,
- każda macierz z $GL(n, K)$ ma macierz odwrotną,
- macierz $I \in GL(n, K)$ ma tę własność, że $AI = IA = A$, czyli jest to element neutralny mnożenia.

Zauważmy jeszcze, że zbiór $GL(n, K)$ utożsamiać można ze zbiorem izomorfizmów przestrzeni K^n .

W kontekście naszych geometrycznych rozważań, a więc w kontekście przestrzeni nad \mathbb{R} , warto wyróżnić macierze odwracalne o dodatnim wyznaczniku i macierze o ujemnym wyznaczniku. Pierwsze oznaczamy przez $GL_+(n, \mathbb{R})$, a drugie przez $GL_-(n, \mathbb{R})$. Mamy $GL(n, \mathbb{R}) = GL_+(n, \mathbb{R}) \cup GL_-(n, \mathbb{R})$.

Kluczowe obserwacje to algebraiczne sformułowania obserwacji poczynionych w trakcie wykładu:

- Iloczyn dowolnych macierzy o dodatnim wyznaczniku jest kolejną macierzą o dodatnim wyznaczniku. Również odwrotność macierzy z $GL_+(n, \mathbb{R})$ należy do tego zbioru. Jest w nim również I , co oznacza, że $GL_+(n, \mathbb{R})$ jest tak zwaną podgrupą $GL(n, \mathbb{R})$.
- Iloczyn macierzy z $GL_+(n, \mathbb{R})$ oraz $GL_-(n, \mathbb{R})$ należy do $GL_-(n, \mathbb{R})$.
- Iloczyn macierzy z $GL_-(n, \mathbb{R})$ to macierz z $GL_+(n, \mathbb{R})$.

Dostajemy następujący wniosek. Istnieje funkcja $f : GL(n, \mathbb{R}) \rightarrow \{-1, 1\}$, która spełnia warunek:³

$$f(AB) = f(A)f(B).$$

Dlaczego to jest takie ważne? Ta dwuelementowa grupa $\{-1, 1\}$ reprezentuje dwie różne orientacje, jakie mogą pojawić się w przestrzeni euklidesowej. Gdyby miał istnieć jakiś inny sposób definicji orientacji, to mimo wszystko oczekiwalibyśmy, że relacja baz wspólnie zorientowanych będzie relacją równoważności oraz, że będzie miała jakiś związek z mnożeniem macierzy. Nawet więcej – chcielibyśmy, aby klasy równoważności relacji wspólnego zorientowania tworzyły grupę.

To nie są argumenty bardzo precyzyjne, ale można powiedzieć jedno: nie da się wprowadzić nietrywialnej (nie jednoelementowej) orientacji w oparciu o homomorfizm z $GL(n, \mathbb{R})$ do pewnej skończonej grupy innej niż $\{-1, 1\}$. Dowiedzie się Państwo tego na Topologii, odwołując się do ważnego pojęcia *drogi*.

Definicja 16.6: Droga nieosobliwa

Niech $A, B \in GL(n, \mathbb{R})$ będą odwracalne. Przyporządkowanie: $f : [0, 1] \rightarrow M_n(K)$ nazwiemy DROGĄ NIEOSOBLIwą w $M_n(\mathbb{R})$ łączącą A, B , jeśli

- $f(0) = A, f(1) = B$,
- dla $t \in [0, 1]$ macierz $f(t)$ jest odwracalna,
- jeśli $f(t) = [a_{ij}(t)]$, to funkcje $t \mapsto a_{ij}(t)$ są ciągłe.

³Funkcje spełniające równość obok nazywamy homomorfizmami grup. Zbiór $\{-1, 1\}$ z definicją mnożenia jest grupą.

Przykład. Funkcja $[0, 1] \ni t \mapsto \begin{bmatrix} 1+t & t \\ 0 & 1 \end{bmatrix}$ jest drogą nieosobliwą łączącą $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ oraz $B = \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}$.

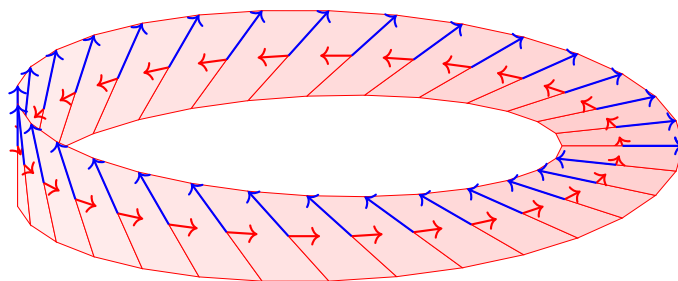
Zachodzi następujące twierdzenie.

Obserwacja 16.2

Baza (A_1, \dots, A_n) jest zorientowana zgodnie z bazą standardową (E_1, \dots, E_n) (w \mathbb{R}^n) wtedy i tylko wtedy, gdy istnieje nieosobliwa droga pomiędzy macierzami $[A_1, \dots, A_n]$ oraz $[E_1, \dots, E_n]$,

A zatem widzimy, że zgodność orientacji dwóch baz ma charakter wybitnie geometryczny. Dowód tego wyniku znaleźć można na przykład w skrypcie prof. Chabera i Pola w punkcie 14.3. Rozumowanie wymaga zastosowania macierzy ortogonalnych, o których dowiemy się za kilka wykładów. Warto odnotować, że w matematyce mówi się również o orientowalności rozmaitych obiektów, nie mających struktury przestrzeni liniowej. Jest to związane z pojęciem przestrzeni stycznej, które stosować można np. dla powierzchni lub różniczkowości gładkich.

W myśl takiego podejścia obiekt jest orientowalny jeśli można na zbiorze przestrzeni stycznych do wszystkich jego punktów wprowadzić orientację, które będzie można w sposób ciągle deformować. Rozróżnienie kiedy powierzchnia jest orientowalna, a kiedy nie, będzie jednym z tematów, który rozważać będziecie Państwo w dalszych studiach.



Przykład powierzchni nieorientowalnej – wstęgi Möbiusa. Czy Czytelnik widzi jaki jest związek z zacytowanym wynikiem?

Źródło: materiały prof. Jarosława Wiśniewskiego.

Z orientowalnością wiąże się wiele ważnych tematów. Oto prosty przykład: na płaszczyźnie litera L oraz jej symetryczne odwrócenie można traktować jako obiekty różne, bo nie można ich nałożyć na siebie (za pomocą izometrii) bez wyjścia poza płaszczyznę (dlaczego?).



Dla Płaszczaka – mieszkańca Flatlandii⁴ – niemogącego wyobrazić sobie ruchu w trzech wymiarach – powyższe obiekty mogą wydawać się być różnych kształtów. Jedną może nazwać lewą L, a drugą – prawą. Jeśli jednak znalazłyby przestrzeń trójwymiarową i mógł w niej umieścić obydwie te figury – byłby w stanie za pomocą obrotu zamienić jedną w drugą. Dla mieszkańca Flatlandii byłyby to szok – z jego punktu widzenia figura zmieniałaby kształt.

Podobnie jest z rozróżnianiem lewej ręki od prawej – status lewej i prawej ręki w przestrzeni trójwymiarowej jest identyczny, jak owych liter w przykładzie wyżej. Poprzez odpowiednie przekształcenie w przestrzeni czterowymiarowej możemy nałożyć rękę lewą na prawą. Może to budzić pewne zdziwienie. Jak sobie wyobrazić taki ruch?

We Flatlandii nie jest możliwe przesunięcie dwóch płaskich odwróconych plecami L tak, by dostać literę. Ale jest to możliwe na dwuwymiarowej, nieorientowalnej powierzchni – wstędze Möbiusa (patrz rysunek wyżej). Jest ona niezanurzalna w liniowej przestrzeni dwuwymiarowej (i dowód też Państwo poznacie).

⁴Serdecznie polecam wydaną w Polsce XIX-wieczną klasykę popularyzacji matematyki: *Flatlandia, czyli Kraina Płaszczaków* autorstwa Edwina Abbotta.

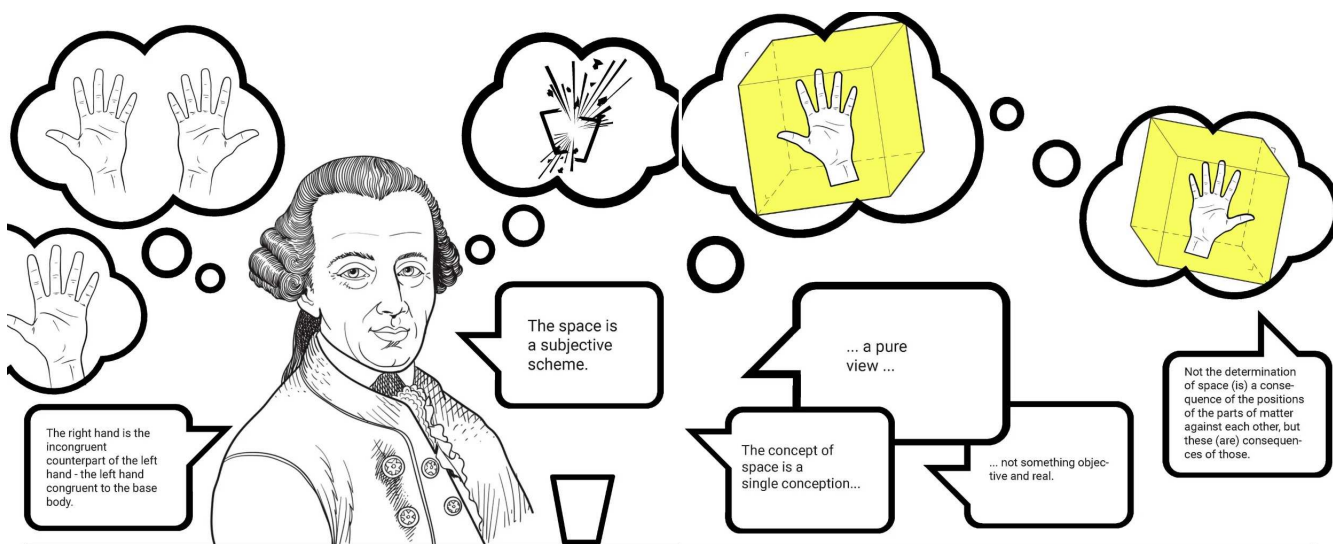
16.3 Trivia. Nieprzystające odpowiedniki

Problemy związane z orientacją rozważane są także w filozofii⁵. W pracy *O naczelnym podstawie różnicy kierunków w przestrzeni* z 1768 roku Immanuel Kant rozważa niezwykle ważny dla swojej filozofii argument dotyczący tzw. nieprzystających odpowiedników. Oto cytaty z tej pracy.

Lewoskrętnie nagwintowana śruba nigdy nie będzie pasowała do takiej nakrętki, której gwint biegnie odwrotnie, nawet wówczas, gdyby były one ze sobą w równym stopniu zgodne zarówno pod względem grubości trzpienia śruby, jak i skoku gwintu. Trójkąt sferyczny może być równy innemu oraz całkowicie do niego podobny, jednakże nie będzie z nim nigdy pokrywał. Lecz najpospolitszym, a zarazem najjaśniejszym przykładem są kończyny ludzkiego ciała, które ułożone są symetrycznie wokół pionowej płaszczyzny dzielącej nasze ciało na dwie równe części. Prawa ręka jest równa lewej i podobna do niej i jeśli patrzy się tylko na jedną z nich – [oceniając] proporcje i wzajemne ułożenie części oraz wielkość całości – to wyczerpujący opis jednej musi we wszystkich fragmentach dotyczyć także drugiej. Ciało równe innemu i całkowicie do niego podobne, jednakże nie dające się zamknąć dokładnie w tych samych granicach, nazywam jego nieprzystającym odpowiednikiem.

Dla Kanta wprowadzone pojęcie było potrzebne do rozważania problemu istnienia **absolutnej** przestrzeni, dzięki której możliwa by była relacja pomiędzy przedmiotami, także nieprzystającymi odpowiednikami.

„Jeśli wyobrazimy sobie, że pierwszą częścią stworzenia powinna być właśnie ludzka ręka, to z konieczności będzie to albo prawa, albo lewa, a w celu powołania do istnienia jednej z nich konieczne jest inne działanie przyczyny stwórczej, aniżeli to za pomocą którego mógł zostać stworzony jej odpowiednik. Jeżeli więc zgodzimy się z pojęciem wielu nowszych filozofów, zwłaszcza zaś niemieckich, [głoszących] iż przestrzeń polega jedynie na zewnętrznej relacji między istniejącymi obok siebie częściami materii, to wszelka rzeczywista przestrzeń we wprowadzonym [wyżej] przypadku byłaby jedynie tą, którą dłoń ta ogarnie. Ponieważ jednak [między dłońmi] nie istnieje absolutnie żadna różnica co do relacji części między sobą, to może to być dłoń prawa lub lewa, a zatem byłaby ona, ze względu na tę właściwość, zupełnie nieokreślona – tj. pasowałaby do każdej części ludzkiego ciała, co jest niemożliwe. Stąd jasnym jest, iż to nie określenia przestrzeni są następstwami wzajemnego ułożenia części materii, lecz odwrotnie, a także to, iż w budowie ciała napotkać można różnice i to najzupełniej prawdziwe, która odnoszą się jedynie do absolutnej oraz pierwotnej przestrzeni, ponieważ tylko dzięki niej możliwa jest relacja pomiędzy przedmiotami cielesnymi.



Grazyna Malcher

Illustration based on original source: Kant, Immanuel (1770): Von dem ersten Grunde des Unterschiedes der Gegenden im Raum [und] Von dem Raume. In: Jörg Düne, Stephan Günzel (2019): Raumtheorie. Grundtextente aus Philosophie und Kulturwissenschaften, Frankfurt: Suhrkamp, p. 74–84; further source: dreamstime.com

Źródło: <https://learn-in.eu/illustrated-spatial-theories/>

Kant wpisuje się tu w dyskusje Leibniza i Clarke'a na temat teorii substancjalistycznej – czymkolwiek są te teorie, możemy z nich wyczytać istotne zainteresowanie związkiem orientacji i rozróżniania obiektów oraz dostrzeganie ich uniwersalnego znaczenia w opisie rzeczywistości.

⁵Na artykułów: Kobiela F.: *Struktura i geneza świata w filozofii przedkrytycznej* I. Kanta, *Diametros*, no. 7, str. 2-36 (do znalezienia) oraz van Cleve J.: *Right, Left and the Fourth Dimension*, *The Philosophical Review* 96 (1987), str. 33-68.

Rozdział 17

Izometrie liniowe i afiniczne. Macierze ortogonalne

Celem tego wykładu jest powiedzieć o przekształceniach liniowych przestrzeni euklidesowych mających równoważne sobie własności: zachowywania iloczynu skalarnego oraz zachowywania długości wektorów. Podobnie jak prostopadłość (czy ogólniej mówiąc – struktura euklidesowa) wywiera wpływ na własności układów wektorów, np. gwarantując ich liniową niezależność, tak i w przypadku przekształceń liniowych zachowywanie struktury euklidesowej ma konsekwencje dla struktury samego przekształcenia.

Definicja 17.1

Niech $(V_1, \langle \cdot, \cdot \rangle_1), (V_2, \langle \cdot, \cdot \rangle_2)$ będą przestrzeniami euklidesowymi liniowymi oraz niech $\phi : V_1 \rightarrow V_2$ będzie przekształceniem liniowym.

(a) Mówimy, że ϕ ZACHOWUJE ILOCZYN SKALARNY, jeśli dla każdych $\alpha, \beta \in V_1$ zachodzi:

$$\langle \alpha, \beta \rangle_1 = \langle \phi(\alpha), \phi(\beta) \rangle_2.$$

(b) Mówimy, że ϕ ZACHOWUJE DŁUGOŚĆ WEKTORÓW jeśli dla każdego $\alpha \in V_1$ zachodzi

$$\|\alpha\|_1 = \|\phi(\alpha)\|_2,$$

gdzie $\|\alpha\|_1 = \sqrt{\langle \alpha, \alpha \rangle_1}$, $\|\gamma\|_2 = \sqrt{\langle \gamma, \gamma \rangle_2}$, dla każdych $\alpha \in V_1, \gamma \in V_2$.

Obserwacja 17.1

Niech $(V_1, \langle \cdot, \cdot \rangle_1), (V_2, \langle \cdot, \cdot \rangle_2)$ będą przestrzeniami euklidesowymi liniowymi oraz niech $\phi \in L(V_1, V_2)$. Wówczas ϕ zachowuje iloczyn skalarny wtedy i tylko wtedy, gdy ϕ zachowuje długość wektorów.

Dowód. Jeśli ϕ zachowuje iloczyn skalarny, to dla $\alpha \in V_1$ mamy:

$$\|\phi(\alpha)\|_2 = \sqrt{\langle \phi(\alpha), \phi(\alpha) \rangle_2} = \sqrt{\langle \alpha, \alpha \rangle_1} = \|\alpha\|_1.$$

Na odwrót: załóżmy, że ϕ zachowuje długość wektorów. Wówczas $\|\alpha + \beta\|^2 = \|\alpha\|^2 + \|\beta\|^2 + 2\langle \alpha, \beta \rangle$, a więc

$$2\langle \alpha, \beta \rangle = \|\alpha + \beta\|^2 - \|\alpha\|^2 - \|\beta\|^2,$$

dla dowolnych wektorów α, β . Zatem dla każdych $\alpha, \beta \in V_1$ mamy:

$$\begin{aligned} 2\langle \phi(\alpha), \phi(\beta) \rangle_2 &= \|\phi(\alpha) + \phi(\beta)\|_2^2 - \|\phi(\alpha)\|_2^2 - \|\phi(\beta)\|_2^2 = \\ &= \|\alpha + \beta\|_1^2 - \|\alpha\|_1^2 - \|\beta\|_1^2 = 2\langle \alpha, \beta \rangle_1. \end{aligned}$$

□

Obserwacja 17.2

Jeśli przekształcenie liniowe ϕ zachowuje iloczyn skalarny, to ϕ jest monomorfizmem.

Dowód. Dla $\alpha \in \ker(\phi)$ mamy $\phi(\alpha) = 0$, czyli $\|\phi(\alpha)\|_2 = 0$, skąd $\|\alpha\|_1 = 0$, więc $\alpha = 0$. \square

Definicja 17.2: Izometria przestrzeni euklidesowej (liniowej)

Niech $(V_1, \langle \cdot, \cdot \rangle_1), (V_2, \langle \cdot, \cdot \rangle_2)$ będą przestrzeniami euklidesowymi liniowymi. Mówimy, że przekształcenie liniowe $\phi : V_1 \rightarrow V_2$ jest **IZOMETRIĄ** przestrzeni $(V_1, \langle \cdot, \cdot \rangle_1)$ na przestrzeń $(V_2, \langle \cdot, \cdot \rangle_2)$ jeśli:

- ϕ jest izomorfizmem przestrzeni liniowej V_1 na przestrzeń liniową V_2 ,
- ϕ zachowuje iloczyn skalarny.

Izometrię przestrzeni $(V, \langle \cdot, \cdot \rangle)$ na $(V, \langle \cdot, \cdot \rangle)$ nazywamy **IZOMETRIĄ PRZESTRZENI EUKLIDESOWEJ** $(V, \langle \cdot, \cdot \rangle)$.

Oto dwa podstawowe przykłady izometrii przestrzeni euklidesowych.

- Symetrie prostopadłe.** Niech W będzie podprzestrzenią przestrzeni euklidesowej liniowej $(V, \langle \cdot, \cdot \rangle)$ i niech $\psi : V \rightarrow V$ będzie symetrią prostopadłą względem W . Wówczas ψ jest izomorfizmem oraz dla dowolnego $v = v_1 + v_2$, gdzie $v_1 \in W, v_2 \in W^\perp$, mamy $\psi(v) = v_1 - v_2$, czyli skoro $v_1 \perp v_2$, to:

$$\|\psi(v)\|^2 = \langle v_1 - v_2, v_1 - v_2 \rangle = \|v_1\|^2 + \|v_2\|^2 - 2\langle v_1, v_2 \rangle = \|v_1\|^2 + \|v_2\|^2 = \|v_1 + v_2\|^2 = \|v\|^2.$$

Zauważmy, że zgodnie z przyjętą definicją rzut prostopadły nie jest (zwykle) izometrią.

- Obroty.** Niech $(V, \langle \cdot, \cdot \rangle)$ będzie dwuwymiarową przestrzenią euklidesową liniową. Załóżmy, że V jest zorientowana i niech \mathcal{A} będzie bazą ortonormalną tej przestrzeni, zorientowaną zgodnie z zadaną orientacją. Wówczas przekształcenie $\phi : V \rightarrow V$ zadane warunkiem

$$M(\phi)_{\mathcal{A}}^{\mathcal{A}} = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}$$

nazywamy **OBROTEM O KĄT θ** .

Oczywiście obrót jest izomorfizmem. Jeśli $\mathcal{A} = \{\alpha_1, \alpha_2\}$ jest bazą ortonormalną V , to dla dowolnego $\alpha \in V$ biorąc $\alpha = a_1\alpha_1 + a_2\alpha_2$, z twierdzenia Pitagorasa mamy

$$\begin{aligned} \|\phi(\alpha)\|^2 &= \|\phi(a_1\alpha_1 + a_2\alpha_2)\|^2 = \|a_1\phi(\alpha_1) + a_2\phi(\alpha_2)\|^2 = \\ &= \|a_1(\cos(\theta)\alpha_1 + \sin(\theta)\alpha_2) + a_2(-\sin(\theta)\alpha_1 + \cos(\theta)\alpha_2)\|^2 = \\ &= \|(a_1 \cos(\theta) - a_2 \sin(\theta))\alpha_1 + (a_1 \sin(\theta) + a_2 \cos(\theta))\alpha_2\|^2 = \\ &= (a_1 \cos(\theta) - a_2 \sin(\theta))^2 + (a_1 \sin(\theta) + a_2 \cos(\theta))^2 = a_1^2 + a_2^2 = \\ &= \|a_1\alpha_1 + a_2\alpha_2\|^2 = \|\alpha\|^2. \end{aligned}$$

Definicja 17.3

Niech $(V, \langle \cdot, \cdot \rangle)$ będzie przestrzenią euklidesową liniową i niech $W \subseteq V$ będzie jej 2-wymiarową podprzestrzenią zorientowaną. Przekształcenie liniowe $\phi : V \rightarrow V$ takie, że $\phi|_W$ jest obrotem o kat θ w przestrzeni W , a $\phi|_{W^\perp}$ jest identycznością na przestrzeni W^\perp nazywamy **OBROTEM O KĄT θ WOKÓŁ PODPRZESTRZENI W^\perp** . Jeśli $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$ jest taką bazą przestrzeni V , że $\mathcal{A}' = (\alpha_1, \alpha_2)$ jest bazą ortonormalną przestrzeni W zorientowaną zgodnie z orientacją W , natomiast $(\alpha_3, \dots, \alpha_n)$ jest dowolną bazą przestrzeni W^\perp , to $M(\phi)_{\mathcal{A}}^{\mathcal{A}}$ jest w postaci blokowej

$$\begin{bmatrix} O_\theta & 0 \\ 0 & I_{n-2} \end{bmatrix}, \quad \text{gdzie} \quad O_\theta = M(\phi|_W)_{\mathcal{A}'}^{\mathcal{A}'} = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}.$$

Pojęcie obrotu wymaga dobrego zrozumienia pojęcia orientacji przestrzeni euklidesowej, ponieważ wyznaczenie właściwego kąta obrotu i podprzestrzeni wokół której obracamy możliwe jest jedynie wówczas, gdy blok O_θ macierzy endomorfizmu ϕ przestrzeni euklidesowych uzyskany jest w dodatnio zorientowanej bazie podprzestrzeni W . Inaczej macierz endomorfizmu ϕ ma właściwą postać blokową, ale możemy ją źle zinterpretować. Oto przykłady, które powinny dać jakąś intuicję.

- Niech $(V, \langle \cdot, \cdot \rangle)$ będzie przestrzenią \mathbb{R}^2 ze standardowym iloczynem skalarnym i orientacją wyznaczoną przez bazę standardową. Bierzymy $\phi : V \rightarrow V$ zadane macierzą

$$M(\phi)_{st}^{st} = \begin{bmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix}.$$

Wówczas ϕ jest obrotem o kąt $-\frac{\pi}{3}$.

- $V = \mathbb{R}^2$ ze standardowym iloczynem skalarnym i orientacją wyznaczoną przez bazę $\mathcal{A} = ((0, 1), (1, 0))$ (to nie jest baza standardowa!). Bierzymy ϕ zadane tym samym wzorem, co wyżej. Wówczas ϕ jest obrotem o kąt $\frac{\pi}{3}$. Dlaczego? Wprawdzie dalej w bazie standardowej przekształcenie ϕ ma macierz, jak wyżej, ale teraz baza standardowa nie jest zorientowana zgodnie z bazą \mathcal{A} wyznaczającą orientację. Mamy jednak

$$M(\phi)_{\mathcal{A}}^{\mathcal{A}} = \begin{bmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix}.$$

- $V = \mathbb{R}^3$ ze standardowym iloczynem skalarnym zawiera podprzestrzeń W o bazie \mathcal{A}' równej $((0, 1, 1), (0, 1, 0))$ i orientacja W jest zgodna z tą bazą. Określamy $\phi : V \rightarrow V$ wzorem:

$$M(\phi)_{st}^{st} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos \theta & -\sin \theta \\ 0 & \sin \theta & \cos \theta \end{bmatrix}.$$

Wówczas $\phi|_W$ jest obrotem o kąt $-\theta$. Dlaczego nie o kąt θ ? Niech $\mathcal{B}' = ((0, 1, 0), (0, 0, 1))$. Bazy \mathcal{A}' oraz \mathcal{B}' przestrzeni W są przeciwnie zorientowane. A zatem bazy \mathcal{A}' oraz $((0, 0, 1), (0, 1, 0))$ są zgodnie zorientowane. Baza \mathbb{R}^3 postaci $\mathcal{B} = ((0, 0, 1), (0, 1, 0), (1, 0, 0))$ również jest ortonormalna, a $M(\phi)_{\mathcal{B}}^{\mathcal{B}}$ ma postać:

$$M(\phi)_{\mathcal{B}}^{\mathcal{B}} = \begin{bmatrix} \cos \theta & \sin \theta & 0 \\ -\sin \theta & \cos \theta & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} \cos(-\theta) & -\sin(-\theta) & 0 \\ \sin(-\theta) & \cos(-\theta) & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Przekształcenie ϕ jest zatem obrotem podprzestrzeni W o kąt $-\theta$ wokół $\text{lin}((1, 0, 0))$.

- Kolejne dwie macierze: pierwsza jest macierzą obrotu (w bazie standardowej) w \mathbb{R}^4 ze standardowym iloczynem skalarnym:

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

a druga nie jest, bowiem ma dwa bloki odpowiadające obrotowi

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

Ostatni przykład dać nam może do myślenia, ponieważ wprawdzie wskazana w nim macierz nie jest macierzą obrotu, ale jest to jednak macierz izometrii przestrzeni \mathbb{R}^4 ze standardowym iloczynem skalarnym. Aby to pokazać Czytelnik mógłby zapewne inteligentnie skorzystać z dotychczasowych argumentów. Czas jednak powiedzieć kilka słów o macierzach izometrii. Jak się okazuje, szczególnie istotne jest rozważanie macierzy w bazach ortonormalnych.

Twierdzenie 17.1

Niech $(V_1, \langle \cdot, \cdot \rangle_1), (V_2, \langle \cdot, \cdot \rangle_2)$ będą przestrzeniami euklidesowymi liniowymi. Następujące warunki są równoważne dla $\phi \in L(V_1, V_2)$:

- (1) ϕ jest izometrią przestrzeni euklidesowej $(V_1, \langle \cdot, \cdot \rangle_1)$ na $(V_2, \langle \cdot, \cdot \rangle_2)$,
- (2) ϕ przeprowadza każdą bazę ortonormalną przestrzeni $(V_1, \langle \cdot, \cdot \rangle_1)$ na bazę ortonormalną $(V_2, \langle \cdot, \cdot \rangle_2)$,
- (3) ϕ przeprowadza pewną bazę ortonormalną przestrzeni $(V_1, \langle \cdot, \cdot \rangle_1)$ na bazę ortonormalną $(V_2, \langle \cdot, \cdot \rangle_2)$.

Co więcej, jeśli $A = M(\phi)_{\mathcal{A}}^{\mathcal{B}} \in M_n(\mathbb{R})$ jest macierzą izometrii przestrzeni euklidesowych w bazach ortonormalnych, wówczas kolumny A są prostopadłe w $(\mathbb{R}^n, \langle \cdot, \cdot \rangle_{st})$. Innymi słowy $A^T A = I$.

Dowód. W pierwszej części dowodu pokażemy tylko implikację (3) \Rightarrow (1), bo (2) \Rightarrow (3) jest trywialna, a implikacja (1) \Rightarrow (2) wynika stąd, że ϕ jako izometria zachowuje długość i prostopadłość.

Przypuśćmy zatem, że dla pewnej bazy ortonormalnej $\alpha_1, \dots, \alpha_n$ przestrzeni euklidesowej $(V_1, \langle \cdot, \cdot \rangle_1)$ układ wektorów $\phi(\alpha_1), \dots, \phi(\alpha_n)$ jest bazą ortonormalną przestrzeni $(V_2, \langle \cdot, \cdot \rangle_2)$. Wykażemy, że ϕ zachowuje iloczyn skalarny. Dla dowolnych $\alpha = x_1\alpha_1 + \dots + x_n\alpha_n$ oraz $\beta = y_1\alpha_1 + \dots + y_n\alpha_n$ w przestrzeni V_1 mamy

$$\phi(\alpha) = x_1\phi(\alpha_1) + \dots + x_n\phi(\alpha_n) \quad \text{oraz} \quad \phi(\beta) = y_1\phi(\alpha_1) + \dots + y_n\phi(\alpha_n),$$

a zatem z ortonormalności obydwu wyróżnionych baz mamy warunek $\langle \alpha_i, \alpha_i \rangle_1 = \langle \phi(\alpha_i), \phi(\alpha_i) \rangle_2 = 1$, dla każdych i, j , czyli¹:

$$\begin{aligned} \langle \alpha, \beta \rangle_1 &= \langle x_1\alpha_1 + \dots + x_n\alpha_n, y_1\alpha_1 + \dots + y_n\alpha_n \rangle_1 = \\ &= x_1y_1 \langle \alpha_1, \alpha_1 \rangle_1 + \dots + x_ny_n \langle \alpha_n, \alpha_n \rangle_1 = \\ &= x_1y_1 \langle \phi(\alpha_1), \phi(\alpha_1) \rangle_2 + \dots + x_ny_n \langle \phi(\alpha_n), \phi(\alpha_n) \rangle_2 = \\ &= \langle x_1\phi(\alpha_1) + \dots + x_n\phi(\alpha_n), y_1\phi(\alpha_1) + \dots + y_n\phi(\alpha_n) \rangle_2 = \\ &= \langle \phi(\alpha), \phi(\beta) \rangle_2. \end{aligned}$$

Przechodzimy do drugiej części dowodu. Niech $\phi : (V_1, \langle \cdot, \cdot \rangle_1) \rightarrow (V_2, \langle \cdot, \cdot \rangle_2)$ będzie dowolną izometrią. Niech $\mathcal{A} = (\alpha_1, \dots, \alpha_n), \mathcal{B} = (\beta_1, \dots, \beta_n)$ będą bazami ortonormalnymi odpowiednio $(V_1, \langle \cdot, \cdot \rangle_1), (V_2, \langle \cdot, \cdot \rangle_2)$. Rozważamy macierz $A = M(\phi)_{\mathcal{A}}^{\mathcal{B}} \in M_n(\mathbb{R})$ i chcemy pokazać, że $A^T A = I$.

Niech $i \neq j$ oraz niech $\phi(\alpha_i) = x_1\beta_1 + \dots + x_n\beta_n$ i $\phi(\alpha_j) = y_1\beta_1 + \dots + y_n\beta_n$. Aby pokazać tezę wystarczy pokazać, że:

$$\begin{aligned} x_1y_1 + \dots + x_ny_n &= 0, \\ x_1^2 + \dots + x_n^2 &= y_1^2 + \dots + y_n^2 = 1. \end{aligned}$$

Skoro jednak ϕ jest izometrią, to z ortonormalności układu α_i wynika ortonormalność układu $\phi(\alpha_i)$, to znaczy:

$$\langle \alpha_i, \alpha_j \rangle_1 = \begin{cases} 1, & i = j \\ 0, & i \neq j. \end{cases} \Rightarrow \langle \phi(\alpha_i), \phi(\alpha_j) \rangle_2 = \begin{cases} 1, & i = j \\ 0, & i \neq j. \end{cases}$$

Z drugiej strony $\langle \beta_i, \beta_j \rangle = 0$, dla $i \neq j$ oraz $\langle \beta_i, \beta_i \rangle = 1$, czyli:

$$\begin{aligned} \langle \phi(\alpha_i), \phi(\alpha_j) \rangle_2 &= \langle x_1\beta_1 + \dots + x_n\beta_n, y_1\beta_1 + \dots + y_n\beta_n \rangle_2 = \\ &= x_1y_1 \langle \beta_1, \beta_1 \rangle_2 + \dots + x_ny_n \langle \beta_n, \beta_n \rangle_2 = \\ &= x_1y_1 + \dots + x_ny_n. \end{aligned}$$

co natychmiast daje (\spadesuit) i tezę twierdzenia. □

Macierze opisane w twierdzeniu wyżej mają fundamentalne znaczenie.

¹W przejściu między trzecią a czwartą linią dodajemy elementy typu $x_iy_j \langle \phi(\alpha_i), \phi(\alpha_j) \rangle_2 = 0$, dla $i \neq j$, co można zrobić korzystając z ortonormalności układu $\phi(\alpha_i)$.

Definicja 17.4: Macierz ortogonalna

Macierz $A \in M_n(\mathbb{R})$ nazywamy ORTOGONALNĄ, jeśli $A^T A = I$. Inaczej mówiąc, kolumny macierzy ortogonalnej są bazą ortonormalną \mathbb{R}^n ze standardowym iloczynem skalarnym.

Macierze ortogonalne są to więc odwracalne macierze kwadratowe, których odwrotność równa jest ich transpozycji. Wśród wielu ważnych przykładów tych macierzy wyróżnić można macierze permutacyjne (w tym I), a także macierze obrotu i symetrii prostopadłej (w bazach ortonormalnych). Powyższe rozważania pozwalają sformułować następujący wniosek.

Obserwacja 17.3

Niech $(V_1, \langle \cdot, \cdot \rangle_1), (V_2, \langle \cdot, \cdot \rangle_2)$ będą przestrzeniami euklidesowymi. Przekształcenie liniowe $\phi : V_1 \rightarrow V_2$ jest izometrią przestrzeni euklidesowej $(V_1, \langle \cdot, \cdot \rangle_1)$ na przestrzeń euklidesową $(V_2, \langle \cdot, \cdot \rangle_2)$ wtedy i tylko wtedy, gdy dla pewnych (równoważnie: dla każdego) baz ortonormalnych \mathcal{A}_1 przestrzeni $(V_1, \langle \cdot, \cdot \rangle_1)$ oraz \mathcal{A}_2 przestrzeni $(V_2, \langle \cdot, \cdot \rangle_2)$ macierz $M(\phi)_{\mathcal{A}_2}^{\mathcal{A}_1}$ jest ortogonalna.

Wniosek ten daje wygodnie kryterium sprawdzania czy przekształcenie liniowe przestrzeni euklidesowych zadane wzorem jest izometrią, czy nie. Dla przykładu, weźmy endomorfizm przestrzeni \mathbb{R}^2 ze standardowym iloczynem skalarnym dany wzorem $\phi((x_1, x_2)) = (x_1, -x_1 + x_2)$. Baza standardowa jest bazą ortonormalną tej przestrzeni euklidesowej, a zatem do sprawdzenia czy ϕ jest izometrią wystarczy przekonać się czy $M(\phi)_{st}^{st}$ jest ortogonalna (wtedy będzie też pewność, że w dowolnych innych bazach ortonormalnych przestrzeni \mathbb{R}^2 przekształcenie to ma macierz ortogonalną). Mamy natomiast:

$$\begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}^T \cdot \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

W rezultacie ϕ nie jest izometrią.

Warto sformułować kolejny wniosek dotyczący zmiany baz.

Obserwacja 17.4

Jeśli \mathcal{A} oraz \mathcal{B} są bazami ortonormalnymi $(\mathbb{R}^n, \langle \cdot, \cdot \rangle)$, to

$$(M(\text{id})_{\mathcal{A}}^{\mathcal{B}})^{-1} = (M(\text{id})_{\mathcal{A}}^{\mathcal{B}})^T.$$

Zatem dla izometrii ϕ przestrzeni $(\mathbb{R}^n, \langle \cdot, \cdot \rangle)$:

$$M(\phi)_{\mathcal{A}}^{\mathcal{A}} = (M(\text{id})_{\mathcal{A}}^{\mathcal{B}})^T \cdot M(\phi)_{\mathcal{B}}^{\mathcal{B}} \cdot M(\text{id})_{\mathcal{A}}^{\mathcal{B}}.$$

Na koniec pozostawiam Państwu do wykazania dwa istotne fakty. Pierwszy jest bardzo prosty, bo wymaga jedynie analizy tego jak może wyglądać macierz ortogonalna rozmiaru 2, drugi wymaga nieco więcej wysiłku, w tym analizy możliwych wartości własnych izometrii.

Obserwacja 17.5

Każda izometria przestrzeni euklidesowej liniowej wymiaru 2 jest albo obrotem o kąt θ albo symetrią prostopadłą względem $\text{lin}((\sin \theta, 1 - \cos \theta))$, więc w pewnej bazie ortonormalnej ma jedną z poniższych macierzy:

$$\begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}, \quad \begin{bmatrix} \cos \theta & \sin \theta \\ \sin \theta & -\cos \theta \end{bmatrix}$$

Obserwacja 17.6

Każda izometria przestrzeni euklidesowej liniowej wymiaru 3 jest albo obrotem, albo obrotem złożonym z symetrią prostopadłą, albo symetrią płaszczyznową. Przekształcenia te mają w pewnej bazie ortonormalnej macierze postaci, odpowiednio:

$$\begin{bmatrix} \cos \theta & -\sin \theta & 0 \\ \sin \theta & \cos \theta & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} \cos \theta & -\sin \theta & 0 \\ \sin \theta & \cos \theta & 0 \\ 0 & 0 & -1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}.$$

Ostatnie twierdzenie można pokazać także korzystając z twierdzenia Cartana o rozkładzie izometrii przestrzeni trójwymiarowej na nie więcej niż trzy symetrie (kolejny wykład). Odnajmy proste uwagi dotyczące wyznacznika izometrii.

Obserwacja 17.7

Jeśli ϕ jest izometrią przestrzeni euklidesowej liniowej $(V, \langle \cdot, \cdot \rangle)$, wówczas $\det \phi = \pm 1$.
Jeśli izometria ϕ ma rzeczywiste wartości własne, to są one równe ± 1 .

Dowód. Niech \mathcal{A} będzie bazą ortonormalną V . Wtedy $M(\phi)_{\mathcal{A}}^{\mathcal{A}}$ jest macierzą ortogonalną, więc

$$(M(\phi)_{\mathcal{A}}^{\mathcal{A}})^T \cdot M(\phi)_{\mathcal{A}}^{\mathcal{A}} = I.$$

Wyznacznik macierzy równy jest wyznacznikowi jej transpozycji, a zatem:

$$\det((M(\phi)_{\mathcal{A}}^{\mathcal{A}})^T \cdot M(\phi)_{\mathcal{A}}^{\mathcal{A}}) = (\det M(\phi)_{\mathcal{A}}^{\mathcal{A}})^2 = (\det \phi)^2 = 1.$$

Skoro $\det \phi \in \mathbb{R}$, to $\det \phi = \pm 1$. Jeśli natomiast dla $\alpha \neq 0$ mamy $\phi(\alpha) = \lambda \cdot \alpha$, to skoro ϕ jest izometrią, mamy $\|\alpha\| = \|\phi(\alpha)\| = \|\lambda \cdot \alpha\| = |\lambda| \cdot \|\alpha\|$. Stąd $|\lambda| = 1$. \square

Zauważmy, że z wyżej wypisanych twierdzeń wynika, że w \mathbb{R}^2 oraz \mathbb{R}^3 jedynie obroty zachowują orientację. Jak się okaże, zbiory obrotów w \mathbb{R}^2 oraz \mathbb{R}^3 tworzą ważne obiekty, zwane specjalnymi grupami ortogonalnymi. O tym więcej w dodatku do wykładu.

Na sam koniec warto odnotować: czasem dzięki wyznacznikowi jesteśmy w stanie szybko stwierdzić czy dane przekształcenie liniowe jest danym typem izometrii, czy nie. Na przykład izometria o wyznaczniku równym -1 nie może być obrotem, ani złożeniem dwóch odbić. Jeszcze inna uwaga: jeśli np. wiemy, że izometria ϕ jest symetrią, to jak znaleźć podprzestrzeń, względem której jest ta symetria? Oczywiście jest to podprzestrzeń własna ϕ odpowiadająca wartości własnej 1. Schodzą się więc w tym miejscu różne poznane przez nas metody, pozwalając na rozpoznawanie izometrii w języku algebry.

Omówiwszy izometrie przestrzeni liniowej i związane z nimi macierze ortogonalne, przechodzimy do wątków geometrycznych i pojęcia izometrii przestrzeni afinicznej. Zagadnienie to omawiamy bardzo pobieżnie, odsyłając jednak w dodatkach do niezliczonych wątków geometrycznych, zarówno elementarnych, jak i bardzo klasycznych i nieoczywistych, choćby dotyczących „ruchu sztywnego” w \mathbb{R}^3 .

Definicja 17.5: Izometria przestrzeni euklidesowej afinicznej

Mówimy, że przekształcenie afiniczne $f : H_1 \rightarrow H_2$ jest **IZOMETRIĄ** przestrzeni euklidesowej afinicznej $(H_1, \langle \cdot, \cdot \rangle_1)$ na przestrzeń euklidesową afiniczną $(H_2, \langle \cdot, \cdot \rangle_2)$ jeśli:

- f jest izomorfizmem przestrzeni afinicznej H_1 na przestrzeń afiniczną H_2 ,
- $f' : T(H_1) \rightarrow T(H_2)$ jest izometrią $(T(H_1), \langle \cdot, \cdot \rangle_1)$ na $(T(H_2), \langle \cdot, \cdot \rangle_2)$.

Dla każdej przestrzeni euklidesowej afinicznej $(H, \langle \cdot, \cdot \rangle)$ izometrią przestrzeni $(H, \langle \cdot, \cdot \rangle)$ na $(H, \langle \cdot, \cdot \rangle)$ nazywamy **IZOMETRIĄ PRZESTRZENI EUKLIDESOWEJ AFINICZNEJ** $(H, \langle \cdot, \cdot \rangle)$.

Przykłady.

- PRZESUNIĘCIE. Niech $(H, \langle \cdot, \cdot \rangle)$ będzie przestrzenią euklidesową afiniczną oraz niech $\alpha \in T(H)$. Przekształcenie afiniczne $f_\alpha : H \rightarrow H$, zadane wzorem $f_\alpha(p) = p + \alpha$, czyli PRZESUNIĘCIE O WEKTOR α , jest izometrią przestrzeni afinicznej $(H, \langle \cdot, \cdot \rangle)$. Pochodną przesunięcia jest identyczność.
- SYMETRIA PROSTOPADŁA. Dla podprzestrzeni M przestrzeni euklidesowej afinicznej $(H, \langle \cdot, \cdot \rangle)$ symetria prostopadła względem M jest izometrią H .
- OBRÓT WOKÓŁ PUNKTU. Niech $(H, \langle \cdot, \cdot \rangle)$ będzie 2-wymiarową przestrzenią euklidesową afiniczną i załóżmy, że w $T(H)$ wybrana jest orientacja. Dla dowolnego punktu $p \in H$ przekształcenie afiniczne $f : H \rightarrow H$ nazywamy OBROTEM WOKÓŁ PUNKTU p o kąt θ ., gdy:

- $f(p) = p$,
- $f' : T(H) \rightarrow T(H)$ jest obrotem o kąt θ

Dla $\dim M \geq 2$ przekształcenie afiniczne $f : M \rightarrow M$ jest obrotem o kąt θ wokół podprzestrzeni W wymiaru $\dim(M) - 2$, jeśli:

- dla każdego $p \in W$ mamy $f(p) = p$,
- $f'|_{T(W)^\perp}$ jest obrotem o kąt θ (na $T(W)^\perp$ musi być zadana orientacja).

Warto wspomnieć też dwa przykłady przekształceń, które nie są izometriami:

- homotetia o skali różnej od ± 1 nie jest izometrią,
- rzut prostopadły różny od id nie jest izometrią.

Z własności przestrzeni euklidesowych liniowych dostajemy następującą charakteryzację izometrii przestrzeni euklidesowych afinicznych.

Obserwacja 17.8

Jeśli $(H_1, \langle \cdot, \cdot \rangle_1)$, $(H_2, \langle \cdot, \cdot \rangle_2)$ są przestrzeniami euklidesowymi afinicznymi oraz \mathcal{A}_i jest bazą ortonormalną przestrzeni $(H_i, \langle \cdot, \cdot \rangle_i)$, dla $i = 1, 2$, to przekształcenie afiniczne $f : H_1 \rightarrow H_2$ jest izometrią wtedy i tylko wtedy, gdy macierz $M(f')_{\mathcal{A}_1}^{\mathcal{A}_2}$ jest ortogonalna.

Z punktu widzenia geometrii afinicznej kluczową własnością izometrii jest jej odniesienie do pojęcia odległości, wyrażone w poniższej definicji.

Definicja 17.6

Niech $(H_1, \langle \cdot, \cdot \rangle_1)$, $(H_2, \langle \cdot, \cdot \rangle_2)$ będą przestrzeniami euklidesowymi afinicznymi i niech ρ_i oznacza odległość w przestrzeni $(H_i, \langle \cdot, \cdot \rangle_i)$, dla $i = 1, 2$. Powiemy, że funkcja^a $f : H_1 \rightarrow H_2$ ZACHOWUJE ODLEGŁOŚĆ PUNKTÓW, jeśli dla każdego $p, q \in H_1$ zachodzi:

$$\rho_1(p, q) = \rho_2(f(p), f(q)).$$

^aNiekoniecznie przekształcenie afiniczne, ale po prostu dowolna funkcja.

Obserwacja 17.9

Niech $(H, \langle \cdot, \cdot \rangle)$ będzie przestrzenią euklidesową afiniczną i niech ρ będzie odległością w tej przestrzeni. Dla dowolnego przekształcenia afinicznego $f : H \rightarrow H$ następujące warunki są równoważne:

- f jest izometrią przestrzeni H ,
- f zachowuje odległość punktów.

Dowód. Zaczniemy od (i) \Rightarrow (ii). Zgodnie z (i) przekształcenie $f' : T(H) \rightarrow T(H)$ zachowuje iloczyn skalarny, więc f' zachowuje normę wektorów. Stąd dla każdego punktu $p, q \in H$ mamy:

$$\rho(f(p), f(q)) = \|\overrightarrow{f(p)f(q)}\| = \|f'(\overrightarrow{pq})\| = \|\overrightarrow{pq}\| = \rho(p, q),$$

czyli f zachowuje odległość punktów. Również dowód (ii) \Rightarrow (i) jest natychmiastowy. Przypuścimy, że f jest przekształceniem afinicznym. Wówczas dla każdego punktu $p \in H$ oraz każdego wektora $\alpha \in T(H)$ mamy $f'(\alpha) = \overrightarrow{f(p)f(p+\alpha)}$, więc:

$$\|f'(\alpha)\| = \|\overrightarrow{f(p)f(p+\alpha)}\| = \rho(f(p), f(p+\alpha)) \stackrel{(ii)}{=} \rho(p, p+\alpha) = \|\overrightarrow{p(p+\alpha)}\| = \|\alpha\|.$$

Zatem f' zachowuje długość wektorów, czyli f jest izometrią przestrzeni $(H, \langle \cdot, \cdot \rangle)$. \square

Naszym celem jest pokazanie, że dowolna funkcja z przestrzeni afinicznej $(H, \langle \cdot, \cdot \rangle)$ w $(H, \langle \cdot, \cdot \rangle)$ – nie tylko przekształcenie afiniczne, zachowuje odległość na H wtedy i tylko wtedy, gdy jest jej izometrią. Jak jednak badać dowolne funkcje zachowujące odległość? Trzeba pokazać, że funkcje takie muszą być przekształceniami afinicznymi. Jest to zaskakujący i stosunkowo techniczny wynik, ale jak widzimy wyżej – sprowadzi on zagadnienie do przypadku omówionego w Obserwacji 17.9. Dowód jest bardzo pouczający.

Twierdzenie 17.2: Twierdzenie Mazura-Ułama

Niech $(H, \langle \cdot, \cdot \rangle)$ będzie przestrzenią euklidesową afiniczną i niech ρ będzie odległością w $(H, \langle \cdot, \cdot \rangle)$. Jeśli funkcja $f : H \rightarrow H$ zachowuje odległość ρ , to f jest przekształceniem afinicznym.

Dowód jest długi, ale idea jest następująca. Weźmiemy dowolną funkcję f zachowującą odległość punktów i zobaczymy jak zachowuje się ona na pewnym układzie ortonormalnym w H . Potem weźmiemy izometrię g , która na tym samym układzie ortonormalnym w H zachowuje się jak f i pokażemy, że f i g muszą być tym samym przekształceniem. Ten sposób dowodzenia jest bardzo charakterystyczny.

Dowód. Krok 1. Wykażemy, że dla każdej bazy punktowej p_0, \dots, p_n przestrzeni H położenie punktu w przestrzeni H jest jednoznacznie wyznaczone przez odległości od punktów p_0, \dots, p_n . Innymi słowy, jeśli dla pewnych $x, y \in H$ mamy $\rho(x, p_i) = \rho(y, p_i)$, dla $i = 0, \dots, n$, to koniecznie $x = y$.

Oznaczmy $\overrightarrow{p_0x} = \beta$, $\overrightarrow{p_0y} = \gamma$ oraz $\overrightarrow{p_0p_i} = \alpha_i$, dla $i = 1, \dots, n$. Wówczas:

$$\begin{aligned} \overrightarrow{xp_i} &= \overrightarrow{xp_0} + \overrightarrow{p_0p_i} = -\beta + \alpha_i = \alpha_i - \beta \\ \overrightarrow{yp_i} &= \overrightarrow{yp_0} + \overrightarrow{p_0p_i} = -\gamma + \alpha_i = \alpha_i - \gamma \\ \overrightarrow{xy} &= \overrightarrow{xp_0} + \overrightarrow{p_0y} = -\beta + \gamma = \gamma - \beta. \end{aligned}$$

Stąd dla każdego $i = 1, \dots, n$ mamy ciąg równoważności:

$$\begin{aligned} \rho(x, p_i) = \rho(y, p_i) &\Leftrightarrow \|\overrightarrow{xp_i}\|^2 = \|\overrightarrow{yp_i}\|^2 \Leftrightarrow \\ &\Leftrightarrow \|\alpha_i - \beta\|^2 = \|\alpha_i - \gamma\|^2 \Leftrightarrow \\ &\Leftrightarrow \|\alpha_i\|^2 - 2\langle \alpha_i, \beta \rangle + \|\beta\|^2 \\ &= \|\alpha_i\|^2 - 2\langle \alpha_i, \gamma \rangle + \|\gamma\|^2 \Leftrightarrow \\ &\Leftrightarrow \|\alpha_i\|^2 - 2\langle \alpha_i, \beta \rangle + \rho(x, p_0)^2 \\ &= \|\alpha_i\|^2 - 2\langle \alpha_i, \gamma \rangle + \rho(y, p_0)^2 \Leftrightarrow \\ &\Leftrightarrow 2\langle \alpha_i, \beta \rangle = 2\langle \alpha_i, \gamma \rangle \Leftrightarrow \\ &\Leftrightarrow \langle \alpha_i, \beta - \gamma \rangle = 0 \end{aligned}$$

Układ $\alpha_1, \dots, \alpha_n$ jest bazą przestrzeni $T(H)$, więc równości $\langle \alpha_i, \beta - \gamma \rangle = 0$, dla $i = 1, \dots, n$, oznaczają, że $\beta - \gamma$ jest prostopadły do $T(H)$, czyli $\beta = \gamma$. Stąd $x = y$.

Krok 2. Niech $f : H \rightarrow H$ będzie funkcją zachowującą odległość punktów. Niech $p_0; \alpha_1, \dots, \alpha_n$ będzie ortonormalnym układem bazowym przestrzeni H i niech $p_i = p_0 + \alpha_i$, dla $i = 1, \dots, n$. Niech $q_i = f(p_i)$, dla $i = 0, \dots, n$ oraz $\beta_i = \overrightarrow{q_0q_i}$, dla $i = 1, \dots, n$. Wykażemy, że $q_0; \beta_1, \dots, \beta_n$ też jest ortonormalnym układem bazowym w H .

Po pierwsze zauważmy, że funkcja f przeprowadza wektory o normie 1 na wektory o normie 1. W szczególności dla każdego $i = 1, \dots, n$:

$$\|\beta_i\| = \|\overrightarrow{q_0 q_i}\| = \rho(q_0, q_i) = \rho(f(p_0), f(p_i)) = \|\overrightarrow{p_0 p_i}\| = \|\alpha_i\| = 1.$$

Pozostaje pokazać, że f przeprowadza prostopadłe wektory na prostopadłe. Skorzystamy w tym celu z następującej obserwacji prawdziwej w każdej przestrzeni euklidesowej afinicznej: wśród wszystkich trójkątów równoramiennych o ramionach długości 1 tylko trójkąt prostokątny ma trzeci bok długości $\sqrt{2}$. Formalnie: dla dowolnych $p \in H$ oraz $\gamma, \delta \in T(H)$ spełniających $\|\gamma\| = \|\delta\| = 1$:

$$\gamma \perp \delta \Leftrightarrow \rho(p + \gamma, p + \delta) = \sqrt{2}.$$

Dowód $\rho(p + \gamma, p + \delta)^2 = \|\gamma - \delta\|^2 = \|\gamma\|^2 - 2\langle \gamma, \delta \rangle + \|\delta\|^2 = 2 - 2\langle \gamma, \delta \rangle$, więc $\langle \gamma, \delta \rangle = 0$ wtedy i tylko wtedy, gdy $\rho(p + \gamma, p + \delta)^2 = 2$.

Zauważmy, że dla każdego $i \neq j$ mamy $\rho(q_0 + \beta_i, q_0 + \beta_j) = \rho(q_i, q_j) = \rho(p_i, p_j) = \rho(p_0 + \alpha_i, p_0 + \alpha_j) = \sqrt{2}$, więc $\beta_i \perp \beta_j$, co kończy dowód ortonormalności układu β_1, \dots, β_n .

Krok 3. Niech p_0, \dots, p_n oraz q_0, \dots, q_n będą bazami punktowymi z Kroku 2. Niech $g : H \rightarrow H$ będzie przekształceniem afinicznym zadany warunkiem $g(p_i) = q_i$, dla $i = 0, \dots, n$. Wykażemy, że $f = g$, czyli dla każdego $x \in H$ mamy $f(x) = g(x)$.

Przekształcenie g jest izometrią przestrzeni $(H, \langle \cdot, \cdot \rangle)$, bo g' przeprowadza bazę ortonormalną $\alpha_1, \dots, \alpha_n$ na bazę ortonormalną β_1, \dots, β_n . Dla każdego punktu $x \in H$ zachodzi

$$\rho(f(x), q_i) = \rho(f(x), f(p_i)) = \rho(x, p_i) = \rho(g(x), q_i),$$

dla $i = 0, \dots, n$. Pokazaliśmy, że $q_0; \beta_1, \dots, \beta_n$ jest układem bazowym przestrzeni H , więc q_0, \dots, q_n jest bazą punktową przestrzeni H . Zatem z powyższego ciągu równości i tezy Kroku 1 wynika, że $f(x) = g(x)$, dla każdego $x \in H$. Stąd f jest przekształceniem afinicznym, co kończy dowód. \square

Wniosek 17.1

Niech $(H, \langle \cdot, \cdot \rangle)$ będzie przestrzenią euklidesową afiniczną i niech ρ będzie odległością w tej przestrzeni. Dla dowolnej funkcji $f : H \rightarrow H$ następujące warunki są równoważne:

- (1) f jest izometrią przestrzeni $(H, \langle \cdot, \cdot \rangle)$,
- (2) f zachowuje odległość punktów.

17.1 Uzupełnienie. Rozpoznawanie i zliczanie izometrii

W zadaniach dotyczących izometrii istotne znaczenie mają dwa aspekty: pierwszym jest samo rozpoznawanie izometrii, a drugim — ich opis. Zobaczmy pewne przykłady, zaczynając od przykładu ze skryptu.

Zadanie 17.1. Rozważmy przestrzenie liniowe $V_1 = V_2 = \mathbb{R}^2$, na których rozważamy iloczynny skalarny:

$$\langle (x_1, x_2), (y_1, y_2) \rangle_1 = 10x_1y_1 + 14x_1y_2 + 14x_2y_1 + 20x_2y_2, \quad \langle (x_1, x_2), (y_1, y_2) \rangle_2 = x_1y_1 + x_2y_2$$

Pokaż, że $\phi : (V_1, \langle \cdot, \cdot \rangle_1) \rightarrow (V_1, \langle \cdot, \cdot \rangle_2)$ dane wzorem $\phi((x_1, x_2)) = (x_1 + 2x_2, 3x_1 + 4x_2)$ jest izometrią.

Możemy podejść do rozwiązania na kilka sposobów:

- sprawdzić, czy ϕ zachowuje normę,
- sprawdzić, czy ϕ przeprowadza bazę ortonormalną na ortonormalną,
- sprawdzić, czy macierz ϕ w bazach ortonormalnych jest ortonormalna.

Z uwagi na to, że każda z metod stanowi zarazem przypomnienie wiadomości, wykonajmy wszystkie trzy. Być może docenimy, że w tym przypadku pierwsza działa dość szybko.

- **Sposób 1.** (skrypt) — bierzemy wektor $\alpha = (x_1, x_2)$ oraz jego obraz $\phi(\alpha) = (x_1 + 2x_2, 3x_1 + 4x_2)$ i porównujemy ich normy w odpowiedniej przestrzeni euklidesowej:

$$\begin{aligned} \|\alpha\|_1^2 &= 10x_1^2 + 28x_1x_2 + 20x_2^2, \\ \|\phi(\alpha)\|_2^2 &= (x_1 + 2x_2)^2 + (3x_1 + 4x_2)^2. \end{aligned}$$

Po uproszczeniu widzimy, że wyrażenia te są równe. Ten sposób uderza nas jako krótki i naturalny.

- **Sposób 2.** Aby wyznaczyć jakąś bazę ortonormalną $(V_1, \langle \cdot, \cdot \rangle_1)$ weźmy wektor $(1, 0) \in V_1$. Nie ma on normy 1, ale wektor $\alpha_1 = \frac{1}{\sqrt{10}}(1, 0)$ ma. Zbiór wektorów prostopadłych do α_1 wyznaczamy z warunku:

$$\begin{bmatrix} 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 10 & 14 \\ 14 & 20 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = 10x_1 + 14x_2 = 0.$$

A zatem $\text{lin}(\alpha_1)^\perp = \text{lin}((14, -10))$. Mamy $\|(14, -10)\|_1 = \sqrt{40} = 2\sqrt{10}$, a zatem biorąc wektor $\alpha_2 = \frac{1}{\sqrt{10}}(7, -5)$ dostajemy bazę ortonormalną α_1, α_2 przestrzeni $(V_1, \langle \cdot, \cdot \rangle_1)$. Mamy też:

$$\phi(\alpha_1) = \frac{1}{\sqrt{10}}(1, 3), \quad \phi(\alpha_2) = \frac{1}{\sqrt{10}}(-3, 1).$$

Z łatwością widzimy, że w standardowym iloczynie skalarnym $\langle \cdot, \cdot \rangle_2$ normy tych obrazów wynoszą 1 i są to wektory prostopadłe. A zatem rzeczywiście pewna baza ortonormalna $(V_1, \langle \cdot, \cdot \rangle_1)$ przechodzi na bazę ortonormalną $(V_2, \langle \cdot, \cdot \rangle_2)$.

- **Sposób 3.** Skoro już w poprzednim sposobie wyznaczyliśmy bazy ortonormalne, to oznaczając bazy $\mathcal{A} = (\alpha_1, \alpha_2)$ oraz $\mathcal{B} = ((1, 0), (0, 1))$ mamy

$$M(\phi)_{\mathcal{A}}^{\mathcal{B}} = \frac{1}{\sqrt{10}} \begin{bmatrix} 1 & -3 \\ 3 & 1 \end{bmatrix}.$$

Oczywiście macierz ta jest ortogonalna. A można jeszcze prościej: wziąć $\mathcal{C} = (\phi(\alpha_1), \phi(\alpha_2))$ i mamy:

$$M(\phi)_{\mathcal{A}}^{\mathcal{C}} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Niech ten ostatni przykład nie zdziwi Czytelnika — nie oznacza on oczywiście, że każda izometria ma wyznacznik 1. Dlaczego?

Zobaczyliśmy zatem jak fakty dowiedzione na wykładzie działają na opisanym przykładzie. Oczywiście wiedząc, że przekształcenie jest izometrią — a zwłaszcza wiedząc jaka to izometria (np. obrót wokół danej podprzestrzeni, symetria prostopadła względem podprzestrzeni) możemy wyznaczać macierze, wzory tych przekształceń wykorzystując choćby wzór z Obserwacji 17.4. Zobaczmy teraz nieco trudniejszy przykład, związany z izometriami afinicznymi.

Zadanie 17.2. W przestrzeni euklidesowej afinicznej \mathbb{R}^3 ze standardowym iloczynem skalarnym dana jest prosta $L = (0, 1, 0) + \text{lin}((1, 2, 1))$ oraz punkt $p_0 = (-3, -1, 1)$.

(a) Dla jakich $s \in \mathbb{R}$ istnieje izometria $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ spełniająca $f(L) = L$ oraz $f(p_0) = (s, 1, -s)$?

(b) Ile jest izometrii $g : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ takich, że $g((0, 0, 1)) = (0, 0, 1)$ oraz dla każdego punktu $p \in L$ mamy $g(p) = p$? Dla każdej takiej izometrii obliczyć $g((0, 0, 0))$.

ROZWIĄZANIE. Zaczniemy od (a). Izometria to przekształcenie zachowujące odległość. Zauważmy, że skoro prosta L przechodzi przy f na siebie, to odległość punktów $p_0 = (-3, -1, 1)$ oraz $(s, 1, -s)$ od prostej L musi być jednakowa. Odległość punktu od prostej L to norma rzutu ortogonalnego wektora łączącego ten punkt z dowolnym punktem L na $T(L)^\perp$. Wektor łączący $(-3, -1, 1)$ oraz punkt $(0, 1, 0) \in L$ to $(3, 2, -1)$. Przestrzeń $T(L)^\perp$ opisana jest równaniem $x_1 + 2x_2 + x_3 = 0$. Baza ortogonalna tej przestrzeni to $(1, 0, -1)$ oraz $(1, -1, 1)$. A zatem rzut ortogonalny $(3, 2, -1)$ na $T(L)^\perp$ to :

$$\frac{\langle (3, 2, -1), (1, 0, -1) \rangle}{\langle (1, 0, -1), (1, 0, -1) \rangle} \cdot (1, 0, -1) + \frac{\langle (3, 2, -1), (1, -1, 1) \rangle}{\langle (1, -1, 1), (1, -1, 1) \rangle} \cdot (1, -1, 1) = (2, 0, -2).$$

Wektor łączący $(s, 1, -s)$ z $(0, 1, 0)$ to $(s, 0, -s) \in T(L)^\perp$. A zatem aby f było izometrią potrzeba, aby $\|(2, 0, -2)\| = \|(s, 0, -s)\|$, czyli $s = \pm 2$.

Pokażmy, że dla $s = \pm 2$ rozważane izometrie istnieją. Rozważmy wektor łączący punkt $(0, 1, 0)$ z punktem $f(p_0) = (s, 1, -s)$. Jest to wektor $(s, 0, -s) \in T(L)^\perp$, bo przestrzeń $T(L)^\perp$ opisana jest równaniem $x_1 + 2x_2 + x_3 = 0$. Skoro $f(L) = L$, to $(0, 1, 0) = f(q_0)$, dla pewnego $q_0 = (0, 1, 0) + t(1, 2, 1) \in L$. Skoro wektor łączący $f(q_0)$ oraz $f(p_0)$ jest prostopadły do $T(L)$, to wobec faktu, że f' jest izometrią (zachowującą iloczyn skalarny), również wektor łączący q_0 oraz $p_0 = (-3, -1, 1)$ musi być prostopadły do L . Mamy $\overrightarrow{q_0 p_0} = (t, 2t + 1, t) - (-3, -1, 1) = (t + 3, 2t + 2, t - 1)$. Ten wektor należy do $T(L)^\perp$, jeśli spełnia równanie $x_1 + 2x_2 + x_3 = 0$, czyli $t + 3 + 4t + 4 + t - 1 = 0$, co daje $t = -1$. Stąd

$$q_0 = (-1, -1, -1), \quad f((-1, -1, -1)) = (0, 1, 0).$$

A zatem na prostej L przekształcenie f jest przesunięciem o wektor $(1, 2, 1)$. Dla parametru $s = -2$ mamy $f((-3, -1, 1)) = (-2, 1, 2)$, więc za szukaną izometrię f na \mathbb{R}^3 można wziąć przesunięcie o wektor $(1, 2, 1)$. Dla $s = 2$ niech f będzie przesunięciem o wektor $(1, 2, 1)$ złożonym z odbiciem względem prostej L wzdłuż $T(L)^\perp \ni \text{lin}(1, 0, -1)$. Wtedy f to izometria, $f(L) = L$ oraz $f((-3, -1, 1)) = (2, 0, -2)$, bo przy tym odbiciu punkt $(-2, 1, 2) = (0, 1, 0) + (-2, 0, 2)$ przechodzi na $(0, 1, 0) - (-2, 0, 2) = (2, 1, -2)$.

Przechodzimy do punktu (b). Skoro dla każdego $p \in L$ mamy mieć $g(p) = p$, to w szczególności $g((0, 1, 0)) = (0, 1, 0)$ oraz $g(-1, -1, -1) = (-1, -1, -1)$. Mamy też oczywiście $g((0, 0, 1)) = (0, 0, 1)$. W rezultacie $g'((0, 1, -1)) = (0, 1, -1)$ oraz $g'((1, 2, 1)) = (1, 2, 1)$, czyli g' jest identycznością na podprzestrzeni $\text{lin}((0, 1, -1), (1, 2, 1))$. Przestrzeń prostopadła do tej dwuwymiarowej przestrzeni stałej (dla g') jest jednowymiarowa i złożona z wektorów (x_1, x_2, x_3) spełniających:

$$\begin{bmatrix} 0 & 1 & -1 \\ 1 & 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix},$$

czyli jest to przestrzeń $\text{lin}((-3, 1, 1))$. Ta przestrzeń jest niezmiennicza przy izometrii g' , bo izometria zachowuje prostopadłość. Zatem wektor $(-3, 1, 1)$ przechodzi na $t(-3, 1, 1)$, dla pewnego t . Jednak jego norma nie zmienia się przy izometrii, więc $t = \pm 1$. Obrazem $(-3, 1, 1)$ przy g' musi być więc $(-3, 1, 1)$ lub $(3, -1, -1)$. Mamy zatem dwie izometrie g spełniające warunki zadania. Rozważmy je osobno.

- Jeśli $g'((-3, 1, 1)) = (-3, 1, 1)$, to $g' = \text{id}$ i skoro $g((0, 0, 1)) = (0, 0, 1)$, to dostajemy $g = \text{id}$. Stąd $g((0, 0, 0)) = (0, 0, 0)$.
- Jeśli $g'((-3, 1, 1)) = (3, -1, -1)$, to g' jest symetrią prostopadłą względem płaszczyzny T postaci $(0, 0, 1) + \text{lin}((0, 1, -1), (1, 2, 1))$. Płaszczyzna ta jest opisana równaniem $-3x_1 + x_2 + x_3 = 1$. Rzut prostopadły $(0, 0, 0)$ na tą płaszczyznę to pewien punkt $(0, 0, 0) + t(-3, 1, 1)$, który spełnia równanie wyżej. Stąd $t = \frac{1}{11}$. A zatem obraz $(0, 0, 0)$ w symetrii prostopadłej względem płaszczyzny T to

$$(0, 0, 0) + \frac{2}{11}(-3, 1, 1) = \left(-\frac{6}{11}, \frac{2}{11}, \frac{2}{11}\right) = g((0, 0, 0)).$$

■

Zadanie 17.3. Dla jakich $s, t \in \mathbb{R}$ istnieje izometria ϕ przestrzeni \mathbb{R}^3 ze standardowym iloczynem skalarnym taka, że $\phi(0, 4, s) = (4, t, 0)$ oraz $\phi(1, -4, 1) = (4, 1, 1)$?

ROZWIĄZANIE. Skoro ϕ jest izometrią to musi zachowywać standardowy iloczyn skalarny i normę wyznaczoną przez ten iloczyn. A zatem

$$\|(0, 4, s)\| = \|(4, t, 0)\| \quad \text{oraz} \quad \|(1, -4, 1)\| = \|(4, 1, 1)\|,$$

a także

$$\langle (0, 4, s), (1, -4, 1) \rangle = \langle (4, t, 0), (4, 1, 1) \rangle.$$

Pierwszy warunek oznacza, że $s^2 = t^2$, drugi zaś, że $-16 + s = 16 + t$. A zatem $s \neq t$ i dostajemy $s = -t = 16$. Oczywiście istnieje izometria $(\mathbb{R}^3, \langle \cdot, \cdot \rangle_{st})$ spełniająca powyższe warunki. Aby wypisać jej wzór wystarczy na przykład zażądać, by wektor $(0, 4, 16) \times (1, -4, 1)$ przechodził przy ϕ na $(4, -16, 0) \times (4, 1, 1)$.

■

* * *

Zobaczmy wreszcie przykład ze zliczaniem izometrii związanej z pojęciem orientacji.

Zadanie 17.4. Niech układ (v_1, \dots, v_n) będzie bazą zorientowanej przestrzeni euklidesowej $(V, \langle \cdot, \cdot \rangle)$. Ile jest zachowujących orientację izometrii $\phi : V \rightarrow V$ takich, że

$$\phi(\text{lin}(v_1, \dots, v_i)) = \text{lin}(v_1, \dots, v_i)$$

dla wszystkich $i = 1, \dots, n$?

ROZWIĄZANIE. Niech (v'_1, \dots, v'_n) będzie bazą ortonormalną $(V, \langle \cdot, \cdot \rangle)$ uzyskaną poprzez ortogonalizację Grama-Schmidta. Wówczas

$$\text{lin}(v_1, \dots, v_i) = \text{lin}(v'_1, \dots, v'_i),$$

dla każdego $i = 1, \dots, n$. Stąd $\phi(\text{lin}(v_1, \dots, v_i)) = \text{lin}(v_1, \dots, v_i)$ jest równoważny z następującym warunkiem $\phi(\text{lin}(v'_1, \dots, v'_i)) = \text{lin}(v'_1, \dots, v'_i)$ i możemy od początku założyć, że baza (v'_1, \dots, v'_n) jest ortonormalna.

Policzymy najpierw wszystkie izometrie takie, że $\phi(\text{lin}(v_1, \dots, v_i)) = \text{lin}(v_1, \dots, v_i)$, dla każdego $i = 1, 2, \dots, n$, przy czym (v_1, \dots, v_n) jest bazą ortonormalną. Wykażemy przez indukcję po n , że izometrii tych jest 2^n .

Dla $n = 1$ mamy $\phi(v_1) = v_1$ lub $\phi(v_1) = -v_1$, bo ϕ zachowuje normę wektora. Przechodzimy do kroku indukcyjnego. Weźmy dowolną izometrię $(V, \langle \cdot, \cdot \rangle)$ spełniającą warunki $\phi(\text{lin}(v_1, \dots, v_i)) = \text{lin}(v_1, \dots, v_i)$, dla każdego $i = 1, 2, \dots, n$, i obetnijmy ją do podprzestrzeni $W = \text{lin}(v_1, \dots, v_{n-1})$. Zgodnie z założeniem $\phi(\text{lin}(v_1, \dots, v_{n-1})) = \text{lin}(v_1, \dots, v_{n-1})$ obcięcie $\phi|_W$ jest „na”. Jego jądro jest zerowe, bo jądro ϕ jest zerowe. Oczywiście $\phi|_W$ zachowuje długość, więc to izometria. Co więcej, $\phi|_W(v_1, \dots, v_i) = (v_1, \dots, v_i)$, dla $i = 1, \dots, n-1$. A zatem z założenia indukcyjnego wiemy, że $\phi|_W$ można wybrać na 2^{n-1} sposobów. Zauważmy teraz, że $\phi(v_n) \notin W$, bo $v_n \in W^\perp$, skoro baza (v_1, \dots, v_n) jest ortonormalna. A zatem $\phi(v_n) = v_n$ lub $\phi(v_n) = -v_n$. A zatem mamy 2^n izometrii $(V, \langle \cdot, \cdot \rangle)$ spełniających warunek $\phi(\text{lin}(v_1, \dots, v_i)) = \text{lin}(v_1, \dots, v_i)$, dla $i = 1, \dots, n$. Krok indukcyjny jest zakończony.

Każda izometria przestrzeni zorientowanej $(V, \langle \cdot, \cdot \rangle)$ zachowuje orientację lub jej nie zachowuje. Co więcej, każdej izometrii ϕ_1 spełniającej warunek $\phi_1(\text{lin}(v_1, \dots, v_i)) = \text{lin}(v_1, \dots, v_i)$, dla $i = 1, \dots, n$ zachowującej orientację $(V, \langle \cdot, \cdot \rangle)$ odpowiada dokładnie jedna izometria ϕ_2 , która spełnia warunek $\phi_2(\text{lin}(v_1, \dots, v_i)) = \text{lin}(v_1, \dots, v_i)$, dla $i = 1, \dots, n$ i nie zachowuje orientacji. Wystarczy żądać, by $\phi_1(v_i) = \phi_2(v_i)$, dla $i = 1, \dots, n-1$ oraz $\phi_2(v_n) = -\phi_1(v_n)$. A zatem liczba izometrii $(V, \langle \cdot, \cdot \rangle)$ spełniających warunek $\phi(\text{lin}(v_1, \dots, v_i)) = \text{lin}(v_1, \dots, v_i)$, dla $i = 1, \dots, n$ wynosi 2^{n-1} .

■

17.2 Dodatek. Macierze ortogonalne i rozkłady

Macierze ortogonalne są jednymi z najważniejszych obiektów w zastosowaniach algebry liniowej. Ich znaczenie stanie się dla nas bardziej jasne, gdy będziemy mówili o diagonalizacji macierzy symetrycznych (rzeczywistych), ale warto wspomnieć o kilku wynikach mających niezwykle istotne znaczenie dla zastosowań. Cytujemy te twierdzenia wraz ze źródłami dowodów.

Twierdzenie 17.3: Rozkład QR

Każdą macierz $A \in M_n(\mathbb{R})$ można przedstawić jako iloczyn QR , gdzie Q jest macierzą ortogonalną oraz R jest górnotrójkątna. Jeśli A jest odwracalna, to rozkład ten jest jednoznaczny.

Twierdzenie 17.4: Rozkład Cholesky'ego

Niech $A \in M_n(\mathbb{R})$. Pokaż, że następujące warunki są równoważne:

- istnieje macierz dolnotrójkątna L taka, że $A = L \cdot L^T$,
- A jest symetryczna i dla każdego $\alpha \in \mathbb{R}^n$ mamy $\alpha^T A \alpha \geq 0$.

Dowód wymaga wykorzystania twierdzenia o ortogonalizacji Grama-Schmidta i umiejętnego zastosowania algorytmu Gaussa. Szczegóły znaleźć można w skrypcie dr. Andrzeja Strojnowskiego:

<https://www.mimuw.edu.pl/~stroa/GAL2wyk14.pdf>.

Rezultaty te są istotne, bowiem równania liniowe o macierzach ortogonalnych można (za pomocą algorytmów) rozwiązywać znacznie szybciej niż dowolne układy równań liniowych. Po prostu jeśli mamy równanie liniowe $Ax = b$, gdzie $A \in M_n(\mathbb{R})$ oraz $x, b \in \mathbb{R}^n$, to jeśli A jest odwracalna, mamy $x = A^{-1}b$. Rozkład QR daje nam:

$$x = (QR)^{-1}b = R^{-1}Q^{-1}b = R^{-1}Q^T b,$$

bo Q jest ortogonalna. Odwracanie macierzy górnotrójkątnej nie jest tak skomplikowane jak odwracanie dowolnej macierzy, a transpozycja jest niemal bezkosztowa. Co więcej, niedługo poznamy twierdzenie Cartana o rozkładzie izomerii na symetrie. W języku macierzowym będzie ono mówiło, że każda macierz ortogonalna jest iloczynem macierzy $S_1 \dots, S_n$ takich, że $H_1^{-1} = H_i$ (tzw. macierze Householdera). Więcej o tych zagadnieniach można przeczytać w artykule *LZNK. Rozkład QR. Metoda Householdera* na portalu <https://dydmat.mimuw.edu.pl/>.

Na koniec warto wspomnieć o postaci dowolnej macierzy ortogonalnej. Wynik ten jest częścią większej teorii dotyczącej macierzy normalnych. Wspomniemy o nich podczas rozważania zagadnień dotyczących iloczynów hermitowskich na przestrzeniach zespolonych.

Twierdzenie 17.5: Klasyfikacja izometrii w \mathbb{R}^n

Niech $(V, \langle \cdot, \cdot \rangle)$ będzie przestrzenią euklidesową i niech $\phi \in \text{End}(V)$ będzie izometrią. Wówczas

- jeśli $W \subseteq V$ jest ϕ -niezmiennicza, to W^\perp też jest ϕ -niezmiennicza,
- ϕ ma podprzestrzeń niezmienniczą wymiaru ≤ 2 ,
- istnieje baza ortonormalna \mathcal{A} przestrzeni $(V, \langle \cdot, \cdot \rangle)$, w której macierz ϕ ma postać:

$$M(\phi)_{\mathcal{A}}^{\mathcal{A}} = \text{diag}(\underbrace{1, \dots, 1}_k, \underbrace{-1, \dots, -1}_s, O_{\theta_1}, \dots, O_{\theta_t}),$$

gdzie $k + s + 2t = n$, $0 \leq k \leq s \leq n$, $0 \leq t \leq \lfloor n/2 \rfloor$ oraz

$$O_{\theta_i} = \begin{bmatrix} \cos \theta_i & -\sin \theta_i \\ \sin \theta_i & \cos \theta_i \end{bmatrix}.$$

Warto wspomnieć w tym kontekście o jeszcze jednym niezwykle istotnym rezultacie, czyli tzw. twierdzeniu o rozkładzie biegunowym.

Twierdzenie 17.6: Twierdzenie o rozkładzie biegunowym, wersja rzeczywista

Dla dowolnej macierzy $A \in M_n(\mathbb{R})$ istnieje macierz ortogonalna S taka, że $A = S \cdot \sqrt{A^T \cdot A}$.

Macierz $\sqrt{A^T \cdot A}$ to taka, że jej kwadrat wynosi $A^T A$. Nie dowodzimy w tym miejscu, że macierz $A^T A$ ma dokładnie jeden pierwiastek, ale za jakiś czas dowiemy się czym są macierze nieujemnie określone i być może także tego, że mają one jednoznaczne pierwiastki. Rozkład ten ma znaczenie, chociażby ze względu na związek z fundamentalnym dla zastosowań twierdzeniem o rozkładzie według wartości osobliwych.

Definicja 17.7: Wartości osobliwe endomorfizmu

Niech ϕ będzie endomorfizmem przestrzeni euklidesowej $(V, \langle \cdot, \cdot \rangle)$. WARTOŚCIAMI OSOBLIWYMI ϕ nazywamy wartości własne endomorfizmu $\sqrt{\phi^* \phi}$. Wartość osobliwa λ występuje z krotnością

$$\dim \ker(\sqrt{\phi^* \phi} - \lambda \text{id}).$$

Są to liczby nieujemne (bo operator $\sqrt{\phi^* \phi}$ jest dodatnio półokreślony).

Uwaga: wartości osobliwe można wyznaczać także dla przekształceń liniowych (czy ich macierzy) pomiędzy przestrzeniami różnych wymiarów. Np. biorąc:

$$A = \begin{bmatrix} 4 & 11 & 14 \\ 8 & 7 & -2 \end{bmatrix}, \quad A^T A = \begin{bmatrix} 80 & 100 & 40 \\ 100 & 170 & 140 \\ 40 & 140 & 200 \end{bmatrix},$$

wyznaczamy wartości własne $A^T A$ (macierz przekształcenia sprzężonego ϕ^* to A^T , jeśli macierz przekształcenia ϕ to A) postaci: zaś wartości osobliwe A to ich pierwiastki: $\sigma_1 = 6\sqrt{10}$, $\sigma_2 = 3\sqrt{10}$, $\sigma_3 = 0$.

Twierdzenie 17.7: Twierdzenie o rozkładzie według wartości osobliwych (SVD decomposition)

Niech $\phi : (V, \langle \cdot, \cdot \rangle_1) \rightarrow (W, \langle \cdot, \cdot \rangle_2)$ będzie przekształceniem liniowym o **niezerowych** wartościach osobliwych s_1, \dots, s_n . Istnieją wówczas bazy ortonormalne \mathcal{A}, \mathcal{B} przestrzeni V takie, że

$$M(\phi)_{\mathcal{A}}^{\mathcal{B}} = \text{diag}(s_1, \dots, s_n).$$

Innymi słowy, jeśli $A \in M_n(\mathbb{C})$, to istnieją macierze unitarne P, Q takie, że $A = P\Sigma Q$, gdzie $\Sigma = \text{diag}(s_1, \dots, s_n)$ ma na przekątnej^a niezerowe wartości osobliwe A .

^aOznaczenie diag stosujemy tu też dla macierzy niekwadratowej opisując jedyne jej niezerowe wyrazy stojące na przecięciu i -tego wiersza i i -tej kolumny macierzy $M(\phi)_{\mathcal{A}}^{\mathcal{B}}$ oraz Σ .

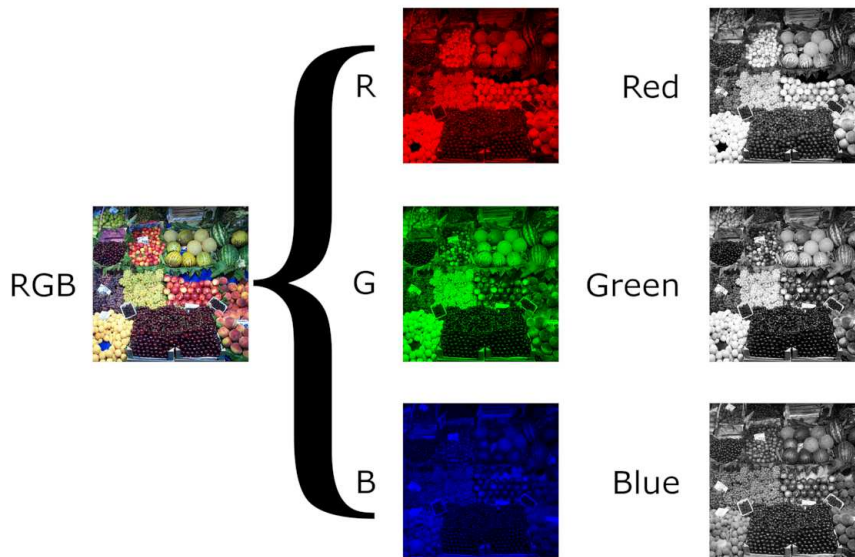
Przykład:

$$\begin{bmatrix} 4 & 11 & 14 \\ 8 & 7 & -2 \end{bmatrix} = \begin{bmatrix} \frac{3}{\sqrt{10}} & \frac{1}{\sqrt{10}} \\ \frac{1}{\sqrt{10}} & -\frac{3}{\sqrt{10}} \end{bmatrix} \cdot \begin{bmatrix} 6\sqrt{10} & 0 & 0 \\ 0 & 3\sqrt{10} & 0 \end{bmatrix} \cdot \begin{bmatrix} \frac{1}{3} & -\frac{2}{3} & \frac{2}{3} \\ \frac{2}{3} & -\frac{1}{3} & -\frac{1}{3} \end{bmatrix}^T.$$

Twierdzenie o rozkładzie według wartości osobliwych ma niezliczone zastosowania, poniżej kilka ciekawych odnośników. Dowód można znaleźć w moim wykładzie: https://mimuw.edu.pl/~amecel/20211/gal21/GAL2+_AM_w13.pdf.

- SVD wytłumaczony wizualnie i kompresja obrazów (świetny film!): <https://youtu.be/DG7YT1GnCEo>
- metody numeryczne (rozwiązywanie układów, pseudoodwrotność, metoda najmn. kwadratów): <http://th-www.if.uj.edu.pl/zfs/gora/metnum19/wyklad05.pdf>
- przeszukiwanie tekstów (ukryte indeksowanie) <http://osilek.mimuw.edu.pl/images/e/ea/ED-4.2-m13-1.01.pdf>
- rozpoznawanie twarzy, data-mining w polityce, kryształy itd. <https://people.maths.ox.ac.uk/porterm/papers/s4.pdf>

Powiedzmy o jednym zastosowaniu, związanym z kompresją. Załóżmy, że wykonaliśmy zdjęcie złożone z 600×400 pikseli ułożonych w prostokątną tablicę rozmiaru 600×400 .



Jeden ze sposobów reprezentacji barw w postaci cyfrowej mówi, że każdy obraz można rozłożyć na trzy kanały barwowe: czerwony, zielony i niebieski. Nасыcenie barwy reprezentowane jest przez jedną z liczb od 0 do 255. A zatem każdy obraz reprezentowany jest przez 3 macierze rozmiarów 600×400 , z których każda zawiera wyrazy całkowite, od 0 do 255. Z tych trzech macierzy możemy (program graficzny) odtworzyć nasz obraz.

Niestety z jakiegoś powodu nie podoba nam się myśl o przechowywaniu tylu liczb w tablicach. Co możemy zrobić? Przecież nie zaczniemy usuwać kolorów! A jednak okazuje się, że można je usuwać tak umiejętnie, by oko ludzkie miało trudność z dostrzeżeniem różnicy, a nasz plik będzie (nawet 3 razy) lżejszy. Jak to zrobić? Weźmy jedną z takich tablic, nazwijmy ją $A \in M_{600 \times 400}(\mathbb{R})$ i zastosujmy do niej rozkład SVD. Wówczas

$$A = U\Sigma V^T,$$

gdzie $\Sigma = (\sigma_{ij})$ ma tylko w wyrazach σ_{ii} niezerowe elementy, i to ułożone tak, że

$$\sigma_{11} \geq \sigma_{22} \geq \dots \geq \sigma_{400}.$$

Oczywiście sam rozkład SVD nie prowadzi do żadnej kompresji. Zamiast macierzy rozmiaru $m \times n$ mamy teraz trzy macierze. Idea jest taka, żeby popatrzeć na macierz Σ i „wyzerować” najmniejsze z elementów typu σ_{ii} , a zostawić tylko k pierwszych, mając nadzieję, że to nie zaburzy za bardzo całego iloczynu.

Oto obrazek, który pokazuje tę ideę (macierze po prawej mają dużo więcej zer):



Bez sensu? Obraz bez związku z oryginałem? Proszę poeksperymentować z liczbą k w poniższym apłecie i sprawdzić na „własne oczy”:

<http://timbaumann.info/svd-image-compression-demo/>.

Rozdział 18

Składanie izometrii

Złożenie izometrii jest izometrią. Ta oczywista obserwacja prowadzi do pięknych wniosków geometrycznych. Na tym wykładzie powiemy o rozkładaniu izometrii liniowych na symetrie prostopadłe, a dokładniej – na tak zwane odbicia. Na koniec (i w dodatku) przyjrzymy się podstawowym przykładom i faktom dotyczącym składania izometrii w przestrzeniach afinicznych. Zaczniemy od kilku przykładów.

W przestrzeni euklidesowej liniowej \mathbb{R}^3 ze standardowym iloczynem skalarnym, zorientowanej zgodnie z bazą standardową, rozważmy endomorfizm ϕ dany w bazie standardowej macierzą:

$$M(\phi)_{st}^{st} = \begin{bmatrix} \cos \theta & -\sin \theta & 0 \\ \sin \theta & \cos \theta & 0 \\ 0 & 0 & -1 \end{bmatrix}.$$

Czytelnik bez trudu widzi, że jest to macierz izometrii. W istocie: jest to macierz przekształcenia liniowego przestrzeni euklidesowej w bazach ortonormalnych — i jest ona ortogonalna. Co więcej, mamy:

$$M(\phi)_{st}^{st} = \begin{bmatrix} \cos \theta & -\sin \theta & 0 \\ \sin \theta & \cos \theta & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} \cos \theta & -\sin \theta & 0 \\ \sin \theta & \cos \theta & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

co oznacza, że ϕ jest w istocie złożeniem **przemiennych ze sobą** izometrii:

- symetrii prostopadłej względem $\text{lin}((1, 0, 0), (0, 1, 0))$,
- obrotu wokół $\text{lin}((0, 0, 1))$ o kąt θ .

Rozważmy izometrię $\phi \in \text{End}(\mathbb{R}^3, \langle \cdot, \cdot \rangle_{st})$ daną macierzą:

$$M(\phi)_{st}^{st} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & -1 & 0 \end{bmatrix}.$$

Znowu bez trudu widzimy, że macierz jest ortogonalna. Rozważmy analogiczny do powyższego rozkład:

$$M(\phi)_{st}^{st} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & -1 & 0 \end{bmatrix} = \underbrace{\begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}}_A \cdot \underbrace{\begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & -1 & 0 \end{bmatrix}}_B.$$

O ile widzimy, że macierz A po lewej to macierz symetrii prostopadłej względem $\text{lin}((0, 1, 0), (0, 0, 1))$, to może nie być jasne, że macierz B po prawej jest w istocie macierzą obrotu (chyba, że znamy Obserwację 17.6, wtedy widzimy to po dodatnim wyznaczniku). Aby to stwierdzić, trzeba sprawdzić, że jedną z wartości własnych macierzy B jest 1, a odpowiadający tej wartości własnej wektor własny to $(1, 1, -1)$. Innych rzeczywistych wartości własnych ta macierz nie ma. Okazuje się, że biorąc $\text{lin}((1, 1, -1))^\perp$ i ograniczając do tej podprzestrzeni izometrię zadaną przez macierz B dostajemy... obrót o kąt $\pm \frac{4\pi}{3}$, w zależności od przyjętej orientacji. Podsumowując: ϕ jest w istocie złożeniem (od prawej, zgodnie z kolejnością składania):

- obrotu wokół $\text{lin}((1, 1, -1))$ o kąt $\pm \frac{4\pi}{3}$,

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

Aby dać Czytelnikowi jaśniejszy pogląd na to co my tu tak naprawdę robimy, i w jaki sposób formułujemy wnioski o powyższej macierzy, odnotujmy następującą prostą obserwację.

Obserwacja 18.1

Niech $\phi : V \rightarrow V$ będzie izometrią przestrzeni euklidesowej liniowej $(V, \langle \cdot, \cdot \rangle)$. Jeśli $W \subseteq V$ jest podprzestrzenią ϕ -niezmienniczą, tzn. $\phi(W) \subseteq W$, to W^\perp jest również podprzestrzenią ϕ -niezmienniczą. W szczególności $\phi|_W$ oraz $\phi|_{W^\perp}$ są izometriami i istnieje baza ortonormalna V taka, że macierz ϕ ma w niej postać blokowo-diagonalną:

$$\begin{bmatrix} M(\phi|_W) & 0 \\ 0 & M(\phi|_{W^\perp}) \end{bmatrix} = \begin{bmatrix} M(\phi|_W) & 0 \\ 0 & I \end{bmatrix} \cdot \begin{bmatrix} I & 0 \\ 0 & M(\phi|_{W^\perp}) \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & M(\phi|_{W^\perp}) \end{bmatrix} \cdot \begin{bmatrix} M(\phi|_W) & 0 \\ 0 & I \end{bmatrix}.$$

Dowód. Niech $\beta \in W^\perp$. Chcemy pokazać, że $\phi(\beta) \in W^\perp$. Wystarczy pokazać, że dla każdego $\alpha \in W$ mamy $\langle \phi(\beta), \alpha \rangle = 0$. Skoro ϕ jest izomorfizmem, to $\phi|_W : W \rightarrow W$ jest mono, czyli jest izomorfizmem (z uwagi na skończony wymiar). Czyli $\phi^{-1}(W) = W$. Skoro jednak ϕ jest izometrią, to

$$\langle \phi(\beta), \alpha \rangle = \langle \beta, \phi^{-1}(\alpha) \rangle = 0.$$

Druga część jest teraz jasna: biorąc bazę ortonormalną $\mathcal{A} = (\alpha_1, \dots, \alpha_k)$ przestrzeni W oraz bazę ortonormalną $\mathcal{B} = (\alpha_{k+1}, \dots, \alpha_n)$ widzimy, że macierz ϕ ma w bazie $\alpha_1, \dots, \alpha_n$ żądaną postać. \square

Gdy teraz Czytelnik spojrzy na przykład macierzy

$$M(\psi)_{st}^{st} = \begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & -1 & 0 \end{bmatrix}$$

rozważanej wyżej, to wiedząc, że ma ona jedynie jedną wartość własną 1 o jednowymiarowej podprzestrzeni własnej $W = \text{lin}((1, 1, -1))$, będzie jasne, że W^\perp jest dwuwymiarową podprzestrzenią ψ -niezmienniczą. A to znaczy, że $\psi|_{W^\perp}$ jest izometrią przestrzeni dwuwymiarowej, która nie ma wartości własnych. To musi być zatem obrót. Kąt ujawni się po wypisaniu macierzy $\psi|_{W^\perp}$ w bazie ortonormalnej W^\perp .

Korzystając z powyższego faktu Czytelnik udowodni bez trudu Obserwację 17.6 i będzie miał narzędzie rozpoznawania izometrii przestrzeni wymiaru 3. Co więcej, fakt ten stanowi jedną z możliwych dróg dowodzenia twierdzenia klasyfikującego dowolne izometrie w \mathbb{R}^n : Rezultat ten był już przywoływany w jednym z dodatków, a tu cytujemy go bez dowodu (który najwygodniej robić metodami wykładu 20). Nie jest on obowiązkowy.

Twierdzenie 18.1: Klasyfikacja izometrii w \mathbb{R}^n

Niech $(V, \langle \cdot, \cdot \rangle)$ będzie przestrzenią euklidesową i niech $\phi \in \text{End}(V)$ będzie izometrią. Wówczas

- jeśli $W \subseteq V$ jest ϕ -niezmienniczą, to W^\perp też jest ϕ -niezmienniczą,
- ϕ ma podprzestrzeń niezmienniczą wymiaru ≤ 2 ,
- istnieje baza ortonormalna \mathcal{A} przestrzeni $(V, \langle \cdot, \cdot \rangle)$, w której macierz ϕ ma postać:

$$M(\phi)_{\mathcal{A}}^{\mathcal{A}} = \text{diag}(\underbrace{1, \dots, 1}_k, \underbrace{-1, \dots, -1}_s, O_{\theta_1}, \dots, O_{\theta_t}),$$

gdzie $k + s + 2t = n$, $0 \leq k \leq s \leq n$, $0 \leq t \leq \lfloor n/2 \rfloor$ oraz

$$O_{\theta_i} = \begin{bmatrix} \cos \theta_i & -\sin \theta_i \\ \sin \theta_i & \cos \theta_i \end{bmatrix}.$$

Zauważmy, że w powyższym twierdzeniu, podobnie jak w Obserwacji 18.1 mowa jest w istocie o rozkładzie V na sumę prostą pewnej liczby podprzestrzeni niezmienniczych. Na każdej z tych podprzestrzeni mamy izometrię i to taką, która rozszerzona do całego V (przez identyczność) jest przemienna z pozostałymi. Nie kontynuujemy tego wątku. Naszym celem będzie zwrócenie się w bardziej geometryczną stronę i opowiedzenie o rozkładzie dowolnej izometrii liniowej na odbicia. Czym one są?

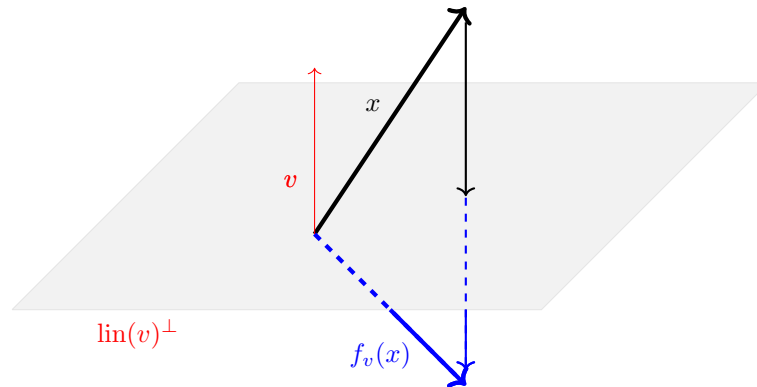
Definicja 18.1: Odbicie

Założmy, że $(V, \langle \cdot, \cdot \rangle)$ jest przestrzenią euklidesową liniową. Dla dowolnego wektora $0 \neq v \in V$ symetrię prostopadłą V względem podprzestrzeni $\text{lin}(v)^\perp$ określoną wzorem

$$f_v(x) = x - 2 \frac{\langle x, v \rangle}{\langle v, v \rangle} v$$

nazywamy ODBICIEM V względem $\text{lin}(v)^\perp$.

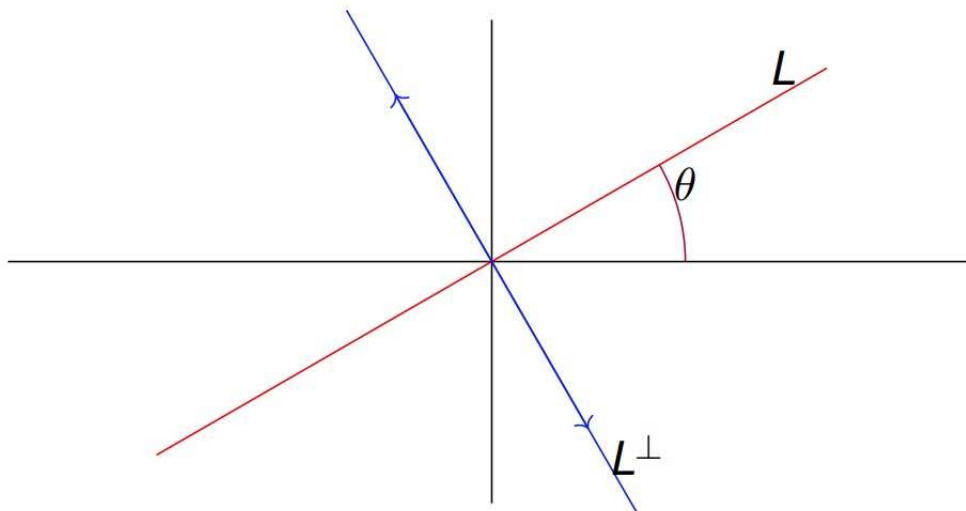
Oto ilustracja odbicia.



Warto przedstawić ilustrację odbicia na płaszczyźnie. Rozważmy kierunek nachylony do osi OX (kierunku $(1, 0)$) pod kątem θ , czyli wektor $(\cos \theta, \sin \theta)$. Zauważmy, że:

$$\begin{bmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{bmatrix} \cdot \begin{bmatrix} \cos \theta \\ \sin \theta \end{bmatrix} = \begin{bmatrix} \cos^2 \theta - \sin^2 \theta & 2 \cos \theta \sin \theta \\ 2 \cos \theta \sin \theta & \sin^2 \theta - \cos^2 \theta \end{bmatrix} \cdot \begin{bmatrix} \cos \theta \\ \sin \theta \end{bmatrix} = \begin{bmatrix} \cos \theta \\ \sin \theta \end{bmatrix}$$
$$\begin{bmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{bmatrix} \cdot \begin{bmatrix} -\sin \theta \\ \cos \theta \end{bmatrix} = \begin{bmatrix} \cos^2 \theta - \sin^2 \theta & 2 \cos \theta \sin \theta \\ 2 \cos \theta \sin \theta & \sin^2 \theta - \cos^2 \theta \end{bmatrix} \cdot \begin{bmatrix} -\sin \theta \\ \cos \theta \end{bmatrix} = - \begin{bmatrix} -\sin \theta \\ \cos \theta \end{bmatrix}$$

Widzimy zatem, że macierz kwadratowa po lewej definiuje odbicie prostopadłe do prostej L nachylonej pod kątem θ do osi OX (zdefiniowaliśmy je na bazie ortonormalnej).

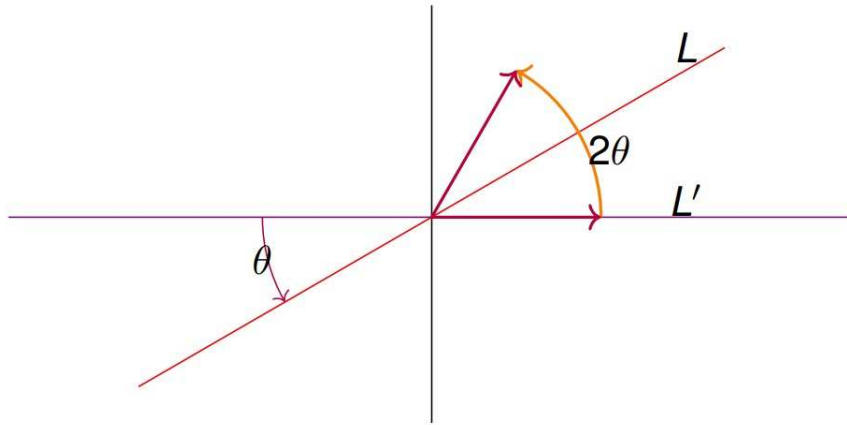


Źródło: materiały prof. Jarosława Wiśniewskiego

Po co nam teraz ta prosta pozioma $\text{lin}(1, 0)$? Otóż kluczowe jest to, że znamy macierz odbicia względem niej. Gdy wykonamy to odbicie, a potem odbicie względem $\text{lin}((\cos \theta, \sin \theta))$, dostaniemy macierz

$$\begin{bmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} \cos 2\theta & -\sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{bmatrix}.$$

A zatem złożenie dwóch odbić względem prostych pomiędzy którymi jest kąt θ , jest obrotem o 2θ w kierunku zależnym od kolejności złożenia odbić.



Źródło: materiały prof. Jarosława Wiśniewskiego

Widzimy, że na płaszczyźnie każdą izometrię można przedstawić jako złożenie nie więcej niż 2 odbić. Okazuje się, że twierdzenie to przenosi się na izometrie liniowe wyższych wymiarów.

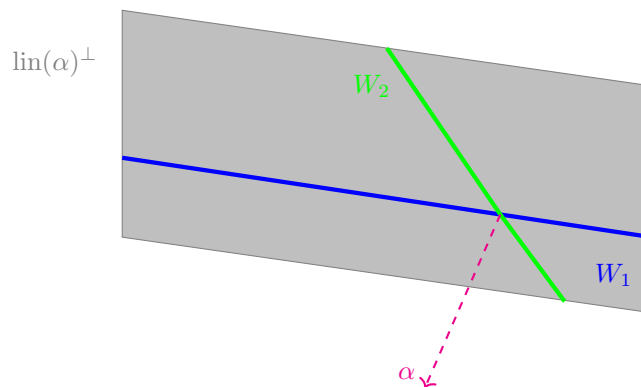
Twierdzenie 18.2: Cartan

Niech $(V, \langle \cdot, \cdot \rangle)$ będzie n wymiarową przestrzenią euklidesową liniową. Dla każdej izometrii ϕ przestrzeni $(V, \langle \cdot, \cdot \rangle)$ istnieje liczba $k \leq n$ taka, że ϕ jest złożeniem k (być może różnych) odbić przestrzeni V (tzn. symetrii prostopadłych wzgl. podprzestrzeni wymiaru $n - 1$).

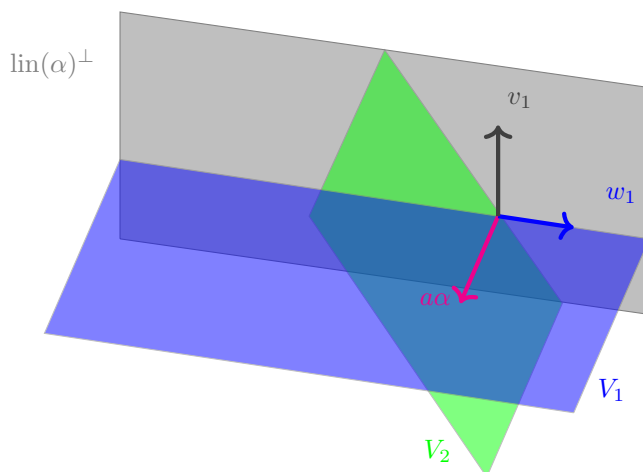
Dowód. Stosujemy indukcję po n . Dla $n = 0$ nie ma czego dowodzić. Dla $n = 1$ twierdzenie jest oczywiste, bo są tylko dwie izometrie 1-wymiarowej przestrzeni euklidesowej liniowej: id oraz $-\text{id}$. Dla pierwszej mamy $k = 0$, dla drugiej zaś $k = 1$. Wyżej ilustrowaliśmy tezę dla $n = 2$.

Założmy, że udowodniliśmy twierdzenie dla przestrzeni euklidesowych wymiaru mniejszego od $n > 1$. Niech $\phi : V \rightarrow V$ będzie izometrią n wymiarowej przestrzeni euklidesowej liniowej $(V, \langle \cdot, \cdot \rangle)$. Wybierzmy dowolny wektor $0 \neq \alpha \in V$ i rozpatrzmy $\text{lin}(\alpha)$. Możliwe są dwa przypadki: $\phi(\alpha) = \alpha$ oraz $\phi(\alpha) \neq \alpha$.

- Przypadek 1, gdy $\phi(\alpha) = \alpha$. Wówczas zgodnie z Obserwacją 18.1 $\text{lin}(\alpha)$ oraz $\text{lin}(\alpha)^\perp$ są ϕ -niezmiennicze, bo α to wektor własny. Przekształcenie $\phi|_{\text{lin}(\alpha)^\perp}$ jest zatem izometrią przestrzeni euklidesowej $\text{lin}(\alpha)^\perp$ wymiaru $n - 1$ z iloczynem skalarnym będącym obcięciem $\langle \cdot, \cdot \rangle$ do $\text{lin}(\alpha)^\perp$. Na mocy założenia indukcyjnego mamy dwa podprzypadki:
 - Gdy $\phi|_{\text{lin}(\alpha)^\perp} = \text{id}_{\text{lin}(\alpha)^\perp}$ (złożenie 0 symetrii), wtedy $\phi(\alpha) = \alpha \Rightarrow \phi = \text{id}_V$.
 - Gdy $\phi|_{\text{lin}(\alpha)^\perp} = \phi_k \circ \dots \circ \phi_1$, gdzie $k \leq n - 1$ oraz $\phi_i : \text{lin}(\alpha)^\perp \rightarrow \text{lin}(\alpha)^\perp$ jest odbiciem $\text{lin}(\alpha)^\perp$ względem podprzestrzeni $W_i \subseteq \text{lin}(\alpha)^\perp$. Zobaczmy poglądowy rysunek sytuacji w przypadku $V = \mathbb{R}^3$. Wówczas $\text{lin}(\alpha)^\perp$ to płaszczyzna i przyjmijmy, że nasza izometria obcięta do $\text{lin}(\alpha)^\perp$ to złożenie dwóch odbić:



Chcemy „podnieść ten rozkład” do rozkładu endomorfizmu ϕ na całej przestrzeni V . Inaczej, chcemy pokazać, że $\phi = \psi_k \circ \dots \circ \psi_1$, gdzie ψ_i są pewnymi odbiciami, które po obcięciu do $\text{lin}(\alpha)^\perp$ są przekształceniami ϕ_i . Określamy $V_i = \text{lin}(\alpha) + W_i$, dla $i = 1, \dots, k$. Skoro $W_i \subset \text{lin}(\alpha)^\perp$, to $V_i = \text{lin}(\alpha) \oplus W_i$.



Zauważmy, że jeśli ϕ_i jest symetrią prostokątną względem W_i w przestrzeni $\text{lin}(\alpha)^\perp$, to przekształcenie liniowe („podniesienie”) $\psi_i : V \rightarrow V$ określone, dla $w \in \text{lin}(\alpha)^\perp$, wzorem

$$\psi_i(a\alpha + w) = a\alpha + \phi_i(w)$$

jest symetrią V względem $n-1$ wymiarowej podprzestrzeni V_i . Rzeczywiście, możemy zapisać $w = a\alpha + w = a\alpha + w_i + v_i$, gdzie $w_i \in W_i, v_i \in (W_i^\perp \cap \text{lin}(\alpha)^\perp)$. W ten sposób:

$$\psi_i(a\alpha + w) = a\alpha + \phi_i(w) = a\alpha + \phi_i(w_i + v_i) = a\alpha + w_i - v_i,$$

czyli ψ jest odbiciem V względem V_i . Pozostaje pokazać, że mamy $\phi = \psi_k \circ \dots \circ \psi_1$. Rzeczywiście, dwa endomorfizmy V określone identycznie na dwóch składnikach sumy prostej $V = W \oplus W'$ muszą być identycznie, bo pokrywają się na pewnej bazie całej V (złożonej z baz każdego ze składników).

Obetnijmy więc złożenie $\psi_k \circ \dots \circ \psi_1$ do $\text{lin}(\alpha)$. Dostaniemy identyczność tak, jak dla ϕ , bo $\phi(\alpha) = \alpha$. Jeśli obetnijmy złożenie do $\text{lin}(\alpha)^\perp$ to mamy $\phi_k \circ \dots \circ \phi_1$, podobnie jak dla ϕ . Stąd $\phi = \psi_k \circ \dots \circ \psi_1$, bowiem przekształcenia te są identyczne na całym V .

- Przypadek 2, gdy $\phi(\alpha) \neq \alpha$. W rozumowaniu skorzystamy z następującego lematu.

Obserwacja 18.2

Założmy, że $(V, \langle \cdot, \cdot \rangle)$ jest przestrzenią euklidesową liniową. Jeżeli $u, v \in V$ spełniają $\|u\| = \|v\|$, to

$$u + v \perp u - v$$

oraz istnieje taka izometria f , będąca identycznością lub odbiciem, że $f(u) = v$ oraz $f(v) = u$.

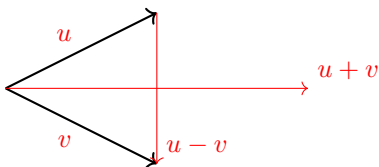
Pokażmy najpierw jak z lematu wynika teza. Mamy $\|\phi(\alpha)\| = \|\alpha\|$. Zgodnie z obserwacją wyżej istnieje odbicie f , które przeprowadza $\phi(\alpha)$ na α . Stąd przekształcenie $f \circ \phi : V \rightarrow V$ spełnia warunek

$$(f \circ \phi)(\alpha) = \alpha.$$

Na mocy Przypadku 1 mamy więc albo $f \circ \phi = \text{id}_V$, albo $f \circ \phi = \psi_k \circ \dots \circ \psi_1$, gdzie $k \leq n-1$ oraz $\psi_k : V \rightarrow V$ są odbiciami. Zatem (korzystając z $f^2 = \text{id}_V$) mamy albo $\phi = f$, albo $\phi = f \circ \psi_k \circ \dots \circ \psi_1$, co jest złożeniem nie więcej niż n odbić. Dowód jest zakończony.

□

Pokazujemy lemat.



Oczywiście jeśli $u = v$ teza jest oczywista, bo $u - u = 0$ jest prostopadły do każdego wektora i możemy wziąć $f = \text{id}$. Załóżmy więc, że $u \neq v$. Mamy: $\langle u + v, u - v \rangle = \|u\|^2 - \|v\|^2 = 0$. Skoro:

$$u = \underbrace{\frac{1}{2}(u + v)}_{\in \text{lin}(u-v)^\perp} + \underbrace{\frac{1}{2}(u - v)}_{\in \text{lin}(u-v)}.$$

to odbicie f_{u-v} względem $\text{lin}(u - v)^\perp$ spełnia warunki zadania:

$$u = \frac{1}{2}(u - v) + \frac{1}{2}(u + v) \xrightarrow{f_{u-v}} \frac{1}{2}(u + v) - \frac{1}{2}(u - v) = \frac{1}{2}v + \frac{1}{2}v = v.$$

Twierdzenie jest udowodnione. Warto odnotować ważną obserwację dotyczącą izomerii i orientacji, wynikającą z twierdzenia Cartana.

Obserwacja 18.3

Każdą izometrię ϕ zorientowanej przestrzeni euklidesowej liniowej można przedstawić w postaci złożenia parzystej albo nieparzystej liczby odbić. Jeśli $\det \phi = 1$, to izometria ϕ jest złożeniem parzystej liczby odbić. Gdy $\det \phi = -1$, to izometria ϕ jest złożeniem nieparzystej liczby odbić.

Powyższy wniosek motywuje następującą definicję.

Definicja 18.2: Izometria parzysta/nieparzysta

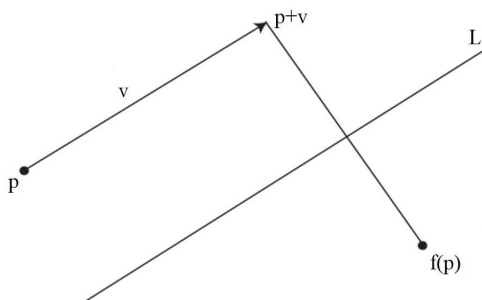
Izometrie przestrzeni euklidesowej liniowej o wyznaczniku równym 1 nazywamy **IZOMETRIAMI PARZYSTYMI**, a izometrie o wyznaczniku -1 nazywamy **IZOMETRIAMI NIEPARZYSTYMI**.

Oczywiście izometrie parzyste zachowują orientację i są złożeniem parzystej liczby odbić, a nieparzyste – nie zachowują orientacji, będąc złożeniem nieparzystej liczby odbić.

* * *

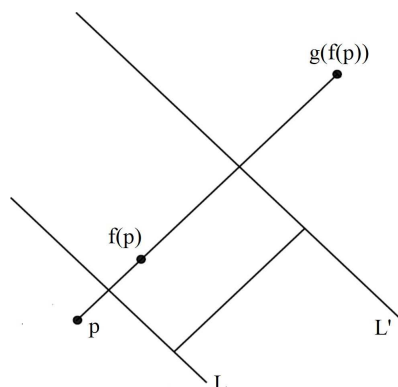
Na sam koniec powiedzmy o kilku przykładach złożenia przekształceń afinicznych. Szczególnie przydatne może być omówienie kilku przykładów, gdzie składamy znane nam obroty i symetrie z przesunięciami. Jest chyba jasne, że **każda izometria afiniczna \mathbb{R}^n jest złożeniem przesunięcia i izometrii liniowej**. Oczywiście jest tak dlatego, że \mathbb{R}^n zawiera wektor zerowy.

- **SYMETRIA Z POŚLIZGIEM.** Rozważmy dwuwymiarową przestrzeń afiniczną H i złożenie przekształcenia $f_v : H \rightarrow H$ będącego przesunięciem o wektor v oraz $s : H \rightarrow H$ będącego symetrią względem prostej L (nie musi być ona nawet prostopadła). Nietrudno widzieć, że $f = f_v \circ s = s \circ f_v$ działa jak na rysunku poniżej. Przekształcenie to nazywamy symetrią z poślizgiem.



- ZŁOŻENIE DWÓCH ODBIĆ AFINICZNYCH. Powiedzieliśmy, że złożenie odbić (liniowych) względem prostych przecinających się pod kątem α jest obrotem o kąt 2α . Jeśli proste te są podprzestrzeniami afinicznymi przecinającymi się w punkcie p , to złożenie odbić afinicznych względem nich będzie obrotem wokół punktu p . Zachęcam Czytelnika do formalnego dowodu tego faktu.

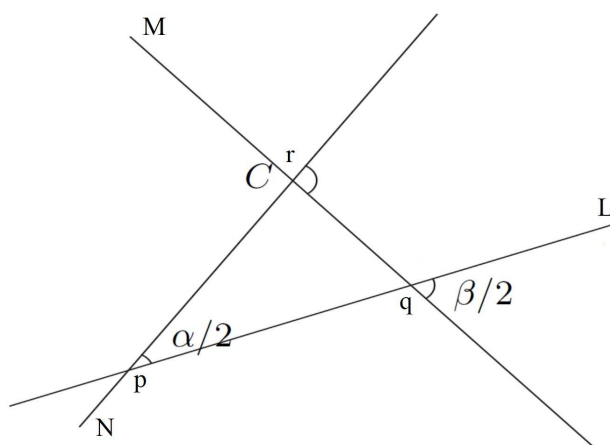
A jeśli proste, względem których odbijamy się nie przecinają? Wówczas w wyniku złożenia otrzymujemy przesunięcie. O jaki wektor? Co się stanie, gdy zamienimy kolejność przestrzeni, względem których odbijamy? Zachęcam zarówno do geometrycznego, jak i algebraicznego dowodu.



- ZŁOŻENIE OBROTÓW. Na zorientowanej płaszczyźnie niech f będzie obrotem o kąt α wokół p oraz g niech będzie obrotem o kąt β wokół q . Wiemy z wcześniejszych rozważań, że obrot o kąt 2θ można dostać poprzez złożenie dwóch odbić względem prostych przecinających się pod kątem θ . W szczególności weźmy prostą L przechodzącą przez punkty p oraz q . Niech prosta N przechodzi przez p i tworzy z L kąt $-\alpha/2$ (zorientowany), zaś prosta M niech przechodzi przez q i tworzy z L kąt zorientowany $\beta/2$. Niech s_X będzie odbiciem względem dowolnej prostej X . Wówczas

$$f = s_N \circ s_L, \quad g = s_L \circ s_M, \quad \implies f \circ g = s_N \circ s_L \circ s_L \circ s_M = s_N \circ s_M,$$

bowiem złożenie tej samej symetrii ze sobą to identyczność. Zachodzą dwie możliwości. Albo proste M oraz N są równoległe, co oznacza, że $\alpha + \beta = 180^\circ$, skąd prosty wniosek, że złożenie obrotów $f \circ g$ jest przesunięciem. Jeśli natomiast $\alpha + \beta \neq 180^\circ$, to niech $r = N \cap M$. Stąd nasze złożenie $f \circ g$ to złożenie odbić względem prostych M oraz N . Proste te przecinają się w punkcie r , więc złożenie jest obrotem o kąt dwa razy większy niż kąt pomiędzy prostymi M oraz N , czyli jest to obrót o kąt $\alpha + \beta$.



Fakt ten ma liczne zastosowania w geometrii elementarnej. Niektóre można znaleźć w następującym artykule prof. Piotra Grzeszczuka, w Delcie: http://www.deltami.edu.pl/temat/matematyka/geometria/planimetria/2011/02/16/Obroty_w_zadaniach_geometrycznych/. a także innych źródłach, choćby w książeczce „Wokół obrotów” dra Waldemara Pompe czy też w klasycznym zbiorze z geometrii Wiktora Prasolowa. Zastosowania te mają urok głównie w języku elementarnym.

18.1 Uzupełnienie. Grupy izometrii i obrotów

Możliwość przedstawienia dowolnej izometrii przestrzeni euklidesowej liniowej jako złożenia pewnej liczby symetrii to jedynie wierzchołek góry lodowej olbrzymiej teorii związanej z tak zwanymi liniowymi i afinicznymi grupami odbić, badanymi już w XIX wieku, w latach 20. XX wieku zastosowanymi w teorii grup Liego przez Weyla i Cartana, później zaś usamodzielnionymi przez prace Coxetera. Tamte wyniki mają wciąż wielkie znaczenie. Elementarnie formułowane geometryczne wyniki algebry liniowej, choćby klasyfikacja izometrii przestrzeni trójwymiarowej, nie są tylko ubieraniem matematyki „szkolnej” w język algebraiczny. Zaczniemy od definicji, którą zajmować się będziecie Państwo na Algebrze I.

Definicja 18.3: Grupa

GRUPĄ nazywamy trójkę (G, \circ, e) , gdzie G jest zbiorem niepustym, $\circ : G \times G \rightarrow G$ jest działaniem 2-argumentowym, $e \in G$, i w której spełnione są aksjomaty:

- łączność \circ ; dla każdych $a, b, c \in G$ mamy $(a \circ b) \circ c = a \circ (b \circ c)$,
- element e spełnia $a \circ e = a = e \circ a$, dla każdego $a \in G$,
- każdy element ma odwrotność, tzn. dla każdego $a \in G$ istnieje $b \in G$, że $a \circ b = b \circ a = e$.

Znamy już kilka grup, choć nie używaliśmy dotąd tego języka.

- Jeśli $(K, 0, 1, +, \cdot)$ jest ciałem, to trójki $(K, 0, +)$ oraz $(K \setminus \{0\}, 1, \cdot)$ są grupami, zwanymi odpowiednio: GRUPĄ ADDYTYWĄ oraz GRUPĄ MULTIPLIKATYWĄ ciała K .
- Jeśli V jest przestrzenią liniową to zbiór izomorfizmów liniowych przestrzeni V w siebie, ozn. $Aut(V)$ jest grupą (ze względu na składanie przekształceń oraz id_V).
- Podzbiór $GL_n(K)$ złożony z macierzy odwracalnych rozmiaru n nad ciałem K z działaniem mnożenia macierzy i elementem neutralnym I_n jest grupą, zwaną PEŁNĄ GRUPĄ LINIOWĄ nad K .
- Zbiór S_n macierzy permutacyjnych rozmiaru n , więc w istocie: zbiór permutacji zbioru n -elementowego wraz z operacją składania permutacji, jest grupą.

Grupy mają olbrzymie znaczenie w matematyce. Z punktu widzenia algebry liniowej również grają one poważną rolę, ale prowadzą do wielu skomplikowanych zagadnień, na które nie ma czasu w toku wykładu. Są im poświęcone nierzadko osobne przedmioty. Być może nie będzie zbyt dużym uproszczeniem, jeśli przyjmiemy, że bardzo ważną ideą teorii grup jest to, że można próbować wyróżnić pewien „reprezentatywny” podzbiór elementów grupy i próbować przedstawiać wszystkie inne za pomocą ciągów napisów złożonych z tych elementów oraz łączących je działań grupowych¹. Dla przykładu:

- w grupie $(\mathbb{Z}, +, 0)$ każdy element jest sumą jedynek lub elementów przeciwnych do jedynki,
- w grupie liczb całkowitych podzielnych przez 3 (z działaniem dodawania) każdy element jest sumą pewnej liczby elementów 3 lub -3 ,
- w grupie S_n każdy element jest złożeniem permutacji zamieniających sąsiednie wyrazy,
- w grupie $GL_n(K)$ każdy element jest iloczynem macierzy operacji elementarnych.

Obserwacja 18.4

Niech (V, \langle, \rangle) będzie przestrzenią euklidesową. Zbiór $O(V) \subseteq End(V)$ izometrii przestrzeni V na siebie jest grupą z działaniem składania przekształceń oraz elementem neutralnym równym id_V .

Dowód. Zaczniemy od zobaczenia, że złożenie dwóch izometrii H jest izometrią. Jeśli $f, g : H \rightarrow H$ są izometriami, to dla każdego $v \in V$ mamy $\|(g \circ f)(v)\| = \|g(f(v))\| = \|f(v)\| = \|v\|$, czyli $g \circ f$ zachowuje normę na H i jest izometrią. Przekształcenie id_V jest izometrią, bo nie zmienia normy. Jest to element neutralny działania składania izometrii w $O(V)$. Wreszcie, każda izometria f ma odwrotną. Rzeczywiście, f jest izomorfizmem, więc istnieje przekształcenie odwrotne f^{-1} . Skoro f zachowuje normę, to f^{-1} oczywiście też to robi. Jest więc izometrią. \square

¹Takie zbiory elementów nazywamy zbiorami generatorów. Grupa G może mieć różne zbiory generatorów, np. całe G .

Definicja 18.4

W zbiorze $Gl_n(K)$ wyróżniamy podzbiory:

$$O_n(K) = \{A \in Gl_n(K) \mid A^T A = I_n\},$$
$$SO_n(K) = \{A \in O_n(K) \mid \det(A) = 1\}.$$

Zbiory $O_n(K)$ oraz $SO_n(K)$ wraz z działaniami mnożenia macierzy oraz elementem neutralnym I_n tworzą (odpowiednio) tzw. GRUPĘ ORTOGONALNĄ oraz SPECJALNĄ GRUPĘ ORTOGONALNĄ.

Grupy $SO_2(\mathbb{R})$ oraz $SO_3(\mathbb{R})$ złożone są z macierzy ortogonalnych o wyznaczniku 1. Muszą to być macierze obrotów, a więc w istocie te grupy to grupy obrotów. Grupa $SO_4(\mathbb{R})$ nie jest już złożona z samych obrotów, ale je zawiera. Dlaczego? Naszym celem będzie zrozumienie, że grupa $O_n(\mathbb{R})$ jest „w istocie” (kiedyś poznamy termin: izomorfizmu grup) grupą izometrii przestrzeni \mathbb{R}^n , niezależnie od przyjętego na niej iloczynu skalarnego.

Dowiedliśmy, że każda symetria przestrzeni euklidesowej jest złożeniem odbić. W szczególności oznacza to, że każda macierz ortogonalna jest iloczynem macierzy odbić. Co to za macierze, nie ma w tym momencie aż tak wielkiego znaczenia (ale będzie miało znaczenie np., gdy poznamy Państwo odbicie jako transformację Householdera na matematyce obliczeniowej), ale nawet sama świadomość, że każda macierz z $O(V)$ jest iloczynem macierzy, które w kwadracie są identycznościami daje do myślenia. Interesujące pytanie jest następujące: bierzemy grupę $O_n(\mathbb{R})$ i rozważamy następujący problem, postawiony w 1934 przez wielkiego geometrę Coxetera².

Rozważmy skończoną liczbę ODBIĆ s_1, \dots, s_r przestrzeni euklidesowej liniowej $(\mathbb{R}^n, \langle, \rangle)$ i zacznijmy je ze sobą składać, a dalej składać złożenia itd. Innymi słowy rozważmy GRUPĘ GENEROWANĄ przez symetrie s_1, \dots, s_r , ozn. $W(s_1, \dots, s_r)$, nazywaną GRUPĄ SYMETRII. Uwaga: grupa symetrii nie składa się z samych symetrii, ale ze złożenia symetrii. $W(s_1, \dots, s_r)$ to „najmniejsza” grupa zawierająca wszystkie symetrie s_1, \dots, s_r . Kiedy ta grupa jest skończona?

Pytamy tu w istocie o tzw. skończone podgrupy $O_n(\mathbb{R})$. To, że takie podgrupy istnieją jest oczywiste, nawet jeśli ograniczymy się do badania izometrii płaszczyzny. Okazuje się bowiem, że skończone podgrupy $O_2(\mathbb{R})$ to grupy symetrii wielokątów foremnych. Kilka przykładów.

- Niech $\theta = 2\pi/m$ oraz niech:

$$R_\theta = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}, \quad T = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Wówczas elementy grupy H_m (tzw. grupa dihedralna) generowanej przez symetrie T oraz $R_\theta \cdot T$ to izometrie zachowujące m -kąąt foremny na płaszczyźnie (o środku w środku układu współrzędnych).

- Niech $\Delta^3 = S(e_1, e_2, e_3, e_4)$ będzie sympleksem trójwymiarowym w przestrzeni \mathbb{R}^4 , rozpiętym przez punkty $e_1 = (1, 0, 0, 0)$, $e_2 = (0, 1, 0, 0)$, $e_3 = (0, 0, 1, 0)$, $e_4 = (0, 0, 0, 1)$. Każdej parze wierzchołków odpowiada symetria s_{ij} , która przeprowadza i -ty wierzchołek na j -ty, a pozostałych nie rusza. Każda izometria zachowująca czworościan Δ^3 jest złożeniem elementarnych symetrii. **Grupa symetrii** czworościanu, to po prostu okazuje się być grupa permutacji S_4 zbioru 4-elementowego.
- **Twierdzenie:** każda skończona grupa **generowana przez obroty**³ w przestrzeni euklidesowej \mathbb{R}^3 (w języku macierzy: skończona podgrupa w $SO(3)$) *jest* albo grupą obrotów lub **grupą symetrii** wielokąta foremnego, albo jedną z trzech **grup symetrii** zachowujących wielościany platońskie (!).

Oczywiście Coxeter nie postawił tylko pytań, ale w serii artykułów w latach 1934-1935 dał początek powstaniu wielkiej geometrycznej teorii, dziś obejmującej swoim zakresem algebrę, geometrię algebraiczną, teorię reprezentacji i wiele innych dziedzin. Rozwiązanie problemu Coxetera wymagało wprowadzenia nowych obiektów i zrozumienia na nowo wielu obiektów uważanych za znane. Była to piękna realizacja XIX-wiecznego programu Felixa Kleina.

²Harold Scott MacDonald Coxeter (1907-2003), „Król geometrii” — jeden z najbardziej znanych geometrów XX wieku.

³Prosty tekst, gdzie (z obrazkami) opowiedziane jest jakie są te grupy odbić: *Symmetry Groups of Platonic Solids*, David Newcomb: <https://dnewcomb.com/pdfs/Platonic%20Solids.pdf>

18.2 Dodatek. Punkty stałe i klasyfikowanie izometrii

Badanie wielu klas przekształceń związane jest z poszukiwaniem punktu stałego. Mówi się nawet o teorii punktu stałego. Jest to jeden z bardzo często powracających motywów w matematyce.

Definicja 18.5: Punkt stały izometrii

Niech $(H, \langle \cdot, \cdot \rangle)$ będzie przestrzenią afiniczną oraz $f : H \rightarrow H$. Powiemy, że $x \in H$ jest PUNKTEM STAŁYM funkcji f jeśli $f(x) = x$.

Obserwacja 18.5

Niech $(H, \langle \cdot, \cdot \rangle)$ będzie przestrzenią euklidesową afiniczną. Dla dowolnego przekształcenia afinicznego $f : H \rightarrow H$ następujące warunki są równoważne:

- (1) istnieje baza punktowa H złożona z punktów stałych H ,
- (2) f jest przekształceniem identycznościowym.

Polecam każdemu próbę policzenia permutacji zbioru n -elementowego, które nie ruszają dokładnie jednego elementu⁴. Szereg twierdzeń o punkcie stałym pochodzących z rozmaitych działów matematyki nosi nazwiska znamienitych uczonych: Poincarego, Borela, Atiyaha, Lefschetza, Kakutaniego, Brouwera, Kleene, choć wydaje się, że jednym najważniejszych rezultatów tego typu jest twierdzenie Stefana Banacha. Wielu zresztą polskich matematyków, zwłaszcza związanych z topologią lub analizą funkcjonalną, dowodziło znakomite rezultaty dotyczące punktów stałych, jak choćby Schauder, Ryll-Nardzewski, Knaster, Kuratowski, Mazurkiewicz, Tarski, Borsuk, Sieklucki, a także prof. A. Białynicki-Birula.

Klasyfikacje różnych typów przekształceń prowadzi się niekiedy w oparciu o analizę punktów stałych⁵. Nie starczy nam na tym wykładzie miejsca na przeprowadzenie klasyfikacji izometrii przestrzeni afinicznych niskich wymiarów, a opiera się ona właśnie o rozgraniczenie izometrii, które nie mają punktów stałych (np. przesunięcia), które mają dokładnie jeden punkt stały (np. obrót na płaszczyźnie) lub więcej punktów stałych (np. symetria).

Ograniczę się do kilku uwag wraz z podaniem źródeł, gdzie można doczytać szczegóły i niektóre dowody. Rozważania te można prowadzić zarówno algebraicznie (w języku wektorów i wartości własnych), jak i czysto geometrycznie (zwłaszcza w \mathbb{R}^2).

Twierdzenie 18.3

Każda izometria skończonego wymiarowej przestrzeni afinicznej $(H, \langle \cdot, \cdot \rangle)$ może być przedstawiona jednoznacznie w postaci złożenia $t \circ k$, gdzie t jest przesunięciem, zaś k jest izometrią mającą punkt stały. Innymi słowy każda izometria f przestrzeni afinicznej ma punkt stały albo prostą niezmienniczą, na której f jest przesunięciem.^a

^aWykład dr. Strojnowskiego, tw. 19.4: <https://www.mimuw.edu.pl/~stroa/GAL2wyk14.pdf>.

W szczególności jeśli $H = \mathbb{R}^n$, to powyższa uwaga mówi, że każda izometria jest złożeniem przesunięcia i izometrii zachowującej wektor zerowy. Możemy zatem alternatywnie do tw. Cartana odwołać się do Twierdzenia 17.5. Przedstawię teraz rezultaty klasyfikujące⁶ wszystkie izometrie przestrzeni afinicznych \mathbb{R} , \mathbb{R}^2 oraz \mathbb{R}^3 (nie są to fakty obowiązkowe, ale na ćwiczeniach będą przykłady).

⁴Trivia: liczba permutacji zbioru n elementowego bez punktu stałego „ma taką samą asymptotykę” jak funkcja $n!/e$.

⁵Kto by chciał dowiedzieć się więcej o punktach stałych, izometriach i ich zastosowaniach w ładnych zadaniach, polecam tekst dra Krzysztofa Żyjewskiego (UAM) *O składaniu symetrii i obrotów. Punkty stałe izometrii*, pod adresem: http://wmii.uwm.edu.pl/f/images/PTM/SZM-2016/o_skladaniu_symetrii_i_obrotow._punkty_stale_izometrii_-_krzysztof_zyjewski.pdf. Tekst zawiera również ładne zastosowania elementarne.

⁶Opis ten odwołuje się do stron 42-43 w <https://www.mimuw.edu.pl/~stroa/GAL2wyk14.pdf>.

Obserwacja 18.6

Każda izometria prostej rzeczywistej \mathbb{R} jest postaci $f(x) = x + c$ lub $f(x) = -x + c$, dla pewnego $c \in \mathbb{R}$. Są to zatem: przesunięcie lub symetria środkowa.

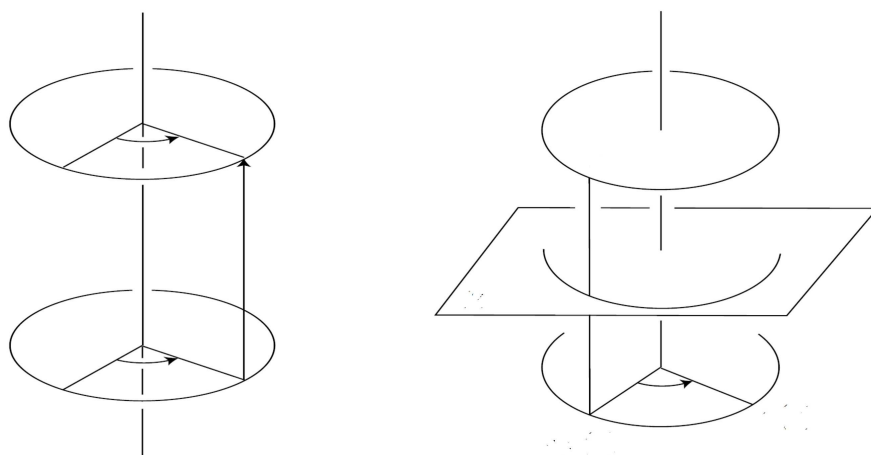
Obserwacja 18.7

Każda izometria płaszczyzny afinicznej \mathbb{R}^2 jest jednym z czterech przekształceń: przesunięciem, obrotem, symetrią lub tzw. symetrią z poślizgiem, czyli złożeniem niezerowego przesunięcia o wektor α oraz symetrii względem przestrzeni $\text{lin}(\alpha)$.

Dowód algebraiczny tego faktu wynika łatwo z twierdzenia klasyfikującego izometrie liniowe płaszczyzny jako obroty lub symetrie prostopadłe. Na mocy wcześniejszej uwagi każda izometria afiniczna jest złożeniem przesunięcia i jednego z tych przekształceń. Identyczność ma trzy afinicznie niezależne punkty stałe, symetria osiowa – dwa. Obrót ma jeden punkt stały, a przesunięcie i symetria z poślizgiem ich nie mają.

Twierdzenie 18.4

Każda izometria trójwymiarowej przestrzeni afinicznej jest identycznością, obrotem, symetrią płaszczyznową, obrotem z odbiciem (te izometrie mają punkty stałe) lub przesunięciem, obrotem z poślizgiem (ruch śrubowy) bądź symetrią płaszczyznową z poślizgiem (brak punktów stałych).



Obrót z poślizgiem w kierunku prostopadłym (ruch śrubowy), symetria płaszczyznowa z poślizgiem. Źródło: M. Audin. *Geometry*.

Fakt ten wywodzi się z twierdzenia Cartana o izometriach. Kto by chciał zobaczyć elementarny dowód, zachęcam do lektury pięknego tekstu prof. Kordosa: Rzut butem, czyli twierdzenie Chaslesa: <http://www.deltami.edu.pl/temat/matematyka/geometria/stereometria/2015/10/27/1511delta-chasles.pdf>. Opowiada on o wyjaśnieniu następującego fenomenu.

Zdjąłem z nogi but i cisnąłem nim byle jak, po czym on upadł byle gdzie i jakoś tam leży. Istnieje ruch po linii śrubowej, za pomocą którego można kulturalnie przenieść ten but z obecnego położenia na moją nogę.

Sens tego twierdzenia jest następujący: obrót z poślizgiem jest jedyną izometrią przestrzeni trójwymiarowej, której pochodna ma dodatni wyznacznik. Takie izometrie nazywa się RUCHAMI SZTYWNYMI. Istotnie, rzut butem nie zmienia przecież jego orientacji — trajektoria lotu w jedną stronę może nie być przekształceniem afinicznym, ale można ten but przywrócić na właściwe miejsce za pomocą ruchu po linii śrubowej (oczywiście może się zdarzyć, że obrót lub przesunięcie są trywialne).

18.3 Trivia. Twierdzenia o przedłużaniu

W trakcie wykładu pokazaliśmy Obserwację 18.2 mówiącą w istocie, że izometrię przestrzeni jednowymiarowych można rozszerzyć do izometrii przestrzeni, w których te jednowymiarowe izometryczne przestrzenie się znajdują. Rezultat ten jest szczególnym przypadkiem ważnego rezultatu zwanego twierdzeniem Witta o przedłużaniu. Sformułujmy ten rezultat

Twierdzenie 18.5: Twierdzenie Witta o przedłużaniu izometrii, sformułowanie pierwsze

Niech V, W będą izometrycznymi przestrzeniami euklidesowymi tzn. istnieje izometria V na W . Niech $V = X_1 \oplus V_1$ oraz $W = X_2 \oplus V_2$ oraz niech $f : X_1 \rightarrow X_2$ będzie izometrią. Wówczas istnieje izometria $F : V \rightarrow W$ taka, że

$$F|_{X_1} = f.$$

Twierdzenie 18.6: Twierdzenie Witta o przedłużaniu izometrii, sformułowanie drugie

Niech V będzie przestrzenią euklidesową^a. Jeśli $0 \neq U, W \subseteq V$ są podprzestrzeniami przestrzeni V oraz jeśli $i_0 : U \rightarrow W$ jest izometrią, to istnieje przedłużenie izometrii i_0 do izometrii i na V , tzn.

$$i|_U = i_0.$$

^aGdy poznamy formy dwuliniowe wtedy można będzie powiedzieć, że to twierdzenie działa dla nieosobliwych podprzestrzeni przestrzeni dwuliniowej nad ciałem charakterystyki różnej od 2. Wynik ten pochodzi z 1937 roku z przełomowej pracy o formach kwadratowych, która dała początek nowoczesnej algebrze liniowej i dziedzinom, które z niej wyrosły.

Rezultat Witta ma decydujące znaczenie w dowodzie jednoznaczności niezwykle ważnego twierdzenia o tzw. rozkładzie Witta. Opowiem o nim w dodatku do twierdzenia o formach kwadratowych.

Twierdzenia o przedłużaniu rozmaitych przekształceń mają bardzo ważne miejsce w matematyce. Przykłady (niektóre już znamy, a niektóre będą na dalszych latach).

- (algebra liniowa) każde przekształcenie liniowe przedłuża się jednoznacznie z bazy na całą dziedzinę,
- (geometria afiniczna) każde przekształcenie afiniczne przedłuża się jednoznacznie z bazy punktowej na całą dziedzinę,
- (topologia) lemat Tietzego o przedłużaniu przekształcenia ciągłego z podzbioru domkniętego przestrzeni metrycznej,
- (analiza funkcjonalna) twierdzenie Hahna-Banacha o przedłużaniu funkcjonalów ograniczonych na przestrzeni unormowanej,
- (analiza wielowymiarowa) twierdzenie Whitneya (mniej więcej) o przedłużaniu funkcji na zbiorze domkniętym tak, by miała ona z góry zadane pochodne,
- (teoria miary) twierdzenie Carathéodory'ego o konstrukcji miary itd.
- (algebra) twierdzenie o rozszerzaniu ciał oraz o istnieniu algebraicznego domknięcia.

Twierdzenia o przedłużaniu są często delikatne i wymagają użycia aksjomatu wyboru. Twierdzenie Hahna-Banacha, które poznał Państwo na analizie funkcjonalnej (dotyczy ono funkcjonalów i w materiałach dra T. Koźniewskiego jest jego skończone wymiarowa wersja) prowadzi do paradoksalnego rozkładu kuli autorstwa Banacha i Tarskiego (wynik wrocławskiego matematyka prof. Janusza Pawlikowskiego z 1991 roku).

A skoro o paradoksalnym rozkładzie mowa, to polecam tekst Joanny Jaszuskiej *O kul rozmnażaniu*, z Delti: http://www.deltami.edu.pl/temat/matematyka/analiza/teoria_miary/2017/03/25/0_kul_rozmnażaniu/

Rozdział 19

Przekształcenia samosprężone Twierdzenie spektralne (rzeczywiste)

Wśród przekształceń liniowych przestrzeni euklidesowych szczególnie interesujące są te, które zachowują pewien element struktury euklidesowej. Obok warunku zachowywania iloczynu skalarnego jest wiele innych możliwych warunków, które nakładać można na endomorfizmy przestrzeni (nie tylko) euklidesowych, aby uzyskiwać inne ważne wyniki strukturalne¹. Dziś² powiemy o warunku, który wysłowić można z jednej strony w języku funkcjonałów liniowych, a z drugiej — w języku macierzy symetrycznych. Rezultat, który dziś udowodnimy, mówiący o diagonalizowalności dowolnej rzeczywistej macierzy symetrycznej i o posiadaniu przez tę macierz ortonormalnej bazy z wektorów własnych jest jednym z najważniejszych rezultatów algebry liniowej, zwłaszcza z punktu widzenia zastosowań. Zaczniemy jednak od funkcjonałów.

Obserwacja 19.1

Niech $(V, \langle \cdot, \cdot \rangle)$ będzie liniową przestrzenią euklidesową wymiaru n . Każdemu wektorowi $v \in V$ przyporządkujemy funkcjonał $f_v \in V^*$ określony wzorem:

$$f_v(u) = \langle u, v \rangle, \text{ gdzie } u \in V.$$

Przyporządkowanie $\Phi : V \rightarrow V^*$ zadane wzorem $\Phi(v) = f_v$ jest izomorfizmem przestrzeni liniowych. Jeśli $\mathcal{V} = (v_1, \dots, v_n)$ jest bazą ortonormalną w V , to $(f_{v_1}, \dots, f_{v_n})$ jest dualną do \mathcal{V} bazą V^* .

Dowód. Przekształcenie f_v jest liniowe dla każdego $v \in V$, bo

$$\begin{aligned} f_v(au) &= \langle au, v \rangle = a \langle u, v \rangle = a \cdot f_v(u) \\ f_v(u_1 + u_2) &= \langle u_1 + u_2, v \rangle = \langle u_1, v \rangle + \langle u_2, v \rangle = f_v(u_1) + f_v(u_2) \end{aligned}$$

Stąd $f_v \in V^*$. Także przyporządkowanie Φ jest liniowe, ponieważ:

- $f_{av}(u) = \langle u, av \rangle = a \langle u, v \rangle = a \cdot f_v(u)$, czyli funkcjonały $\Phi(av)$ oraz $a \cdot \Phi(v)$ są identyczne na V ,
- $f_{v_1+v_2}(u) = \langle u, v_1 + v_2 \rangle = \langle u, v_1 \rangle + \langle u, v_2 \rangle = f_{v_1}(u) + f_{v_2}(u)$, czyli funkcjonały $\Phi(v_1 + v_2)$ oraz $\Phi(v_1) + \Phi(v_2)$ są identyczne na V .

Skoro V oraz V^* są tego samego wymiaru to do wykazania, że Φ jest izomorfizmem wystarczy pokazać, że Φ to monomorfizm. Jeśli $\Phi(v) = 0$, to $f_v \equiv 0$. W szczególności $f_v(v) = \langle v, v \rangle = 0$. Zatem $v = 0$. Czyli Φ jest izomorfizmem. Ostatnie stwierdzenie dotyczące baz dualnych wynika wprost z ich definicji. Rzeczywiście, jeśli (v_1^*, \dots, v_n^*) jest bazą dualną do bazy (v_1, \dots, v_n) , to z definicji:

$$v_i^*(v_j) = \begin{cases} 1, & \text{dla } j = i, \\ 0, & \text{dla } j \neq i. \end{cases} \quad \text{oraz} \quad f_{v_i}(v_j) = \langle v_j, v_i \rangle = \begin{cases} 1, & \text{dla } j = i, \\ 0, & \text{dla } j \neq i. \end{cases}$$

bowiem baza v_1, \dots, v_n jest ortonormalna. Stąd funkcjonały v_i^* oraz f_{v_i} są równe na bazie V , czyli są identyczne na V , dla każdego i . Stąd $v_i^* = f_{v_i}$. □

¹Zainteresowanych odsyłam do: <http://www.math.us.edu.pl/zat1/szymiczek/referaty/AlgebraLiniowa4.pdf>.

²Ostatnia aktualizacja: 15.05.2023 r.

Jaka jest zaleta tego rezultatu? Po pierwsze — praktyczna. W przestrzeni euklidesowej wyznaczanie bazy dualnej do bazy ortonormalnej jest niemal natychmiastowe. Biorąc w \mathbb{R}^3 , $\langle \cdot, \cdot \rangle_{st}$ bazę ortonormalną:

$$v_1 = (a_1, a_2, a_3), \quad v_2 = (b_1, b_2, b_3), \quad v_3 = (c_1, c_2, c_3),$$

widzimy, że bazę dualną do bazy v_1, v_2, v_3 tworzą funkcjonały:

$$\begin{aligned} f_1((x_1, x_2, x_3)) &= \langle (x_1, x_2, x_3), (a_1, a_2, a_3) \rangle = a_1x_1 + a_2x_2 + a_3x_3 \\ f_2((x_1, x_2, x_3)) &= \langle (x_1, x_2, x_3), (b_1, b_2, b_3) \rangle = b_1x_1 + b_2x_2 + b_3x_3, \\ f_3((x_1, x_2, x_3)) &= \langle (x_1, x_2, x_3), (c_1, c_2, c_3) \rangle = c_1x_1 + c_2x_2 + c_3x_3. \end{aligned}$$

Jeszcze inna interpretacja: rozwiązanie dowolnego jednorodnego układu równań liniowych postaci:

$$\begin{cases} a_{11}x_1 + \dots + a_{1n}x_n &= 0 \\ a_{21}x_1 + \dots + a_{2n}x_n &= 0 \\ &\vdots \\ a_{m1}x_1 + \dots + a_{mn}x_n &= 0 \end{cases},$$

w istocie polega na znalezieniu części wspólnej jąder przekształceń $f_{\alpha_1}, \dots, f_{\alpha_m}$, gdzie $\alpha_i = (a_{i1}, \dots, a_{in})$ jest i -tym wierszem macierzy układu wyżej. Co więcej, $\ker f_{\alpha_i} = \text{lin}(\alpha_i)^\perp$.

Wreszcie, kluczowa interpretacja pozwala na utożsamianie endomorfizmów przestrzeni V oraz V^* . Dokładniej: dla dowolnego endomorfizmu $\phi : V \rightarrow V$ oraz dla dowolnego $v \in V$, obraz funkcyjonału $f_v = \Phi(v)$ przy przekształceniu sprzężonym ϕ^* to funkcyjonał z V , czyli pewien funkcyjonał $f_{v'} = \Psi(v')$. Co mają ze sobą wspólnego v oraz v' ? Musimy mieć

$$\phi^*(f_v) = f_{v'},$$

czyli z definicji przekształcenia sprzężonego mamy

$$\phi^*(f_v) = f_v \circ \phi = f_{v'}.$$

A zatem z definicji f_v oraz $f_{v'}$ mamy, dla każdego $u \in V$:

$$\langle \phi(u), v \rangle = \langle u, v' \rangle.$$

Endomorfizm przestrzeni euklidesowej V przypisujący wektorowi v wektor v' tak, że spełniona jest powyższa równość nazywamy ENDOMORFIZMEM SPRZEŻONYM do ϕ ze względu na iloczyn skalarny $\langle \cdot, \cdot \rangle$. Zwyczajowo ten endomorfizm również oznacza się przez ϕ^* , mimo, że jest to (teraz) endomorfizm V . Mamy więc:

$$\langle \phi(u), v \rangle = \langle u, \phi^*(v) \rangle.$$

Czy rozważania te mają jakiś praktyczny skutek? Chodzi tu o to, że spojrzenie na endomorfizmy V jako na pochodzące od endomorfizmów V^* pozwala na wyróżnienie dodatkowych klas endomorfizmów. Chodzi o to, że możemy zapostulować pewne związki ϕ^* z ϕ . Jeden z nich już znamy.

Proszę zauważyć, że przyjmując w powyższej równości ϕ^* jako ϕ^{-1} dostajemy dokładnie definicję izometrii. Istotnie, skoro $\langle \phi(u), v \rangle = \langle u, \phi^{-1}(v) \rangle$, to dla $v = \phi(u)$ mamy:

$$\langle \phi(u), \phi(u) \rangle = \langle u, \phi^{-1}(\phi(u)) \rangle = \langle u, u \rangle.$$

A zatem ϕ zachowuje normę i jest izomorfizmem (bo istnieje ϕ^{-1}), czyli to izometria. Krótko mówiąc, izometrie to takie przekształcenia, że sprzężone do nich to ich odwrotności. Nie powinno nas to dziwić. Pamięamy przecież, że macierz przekształcenia sprzężonego w bazach sprzężonych to macierz transponowana. Z drugiej strony macierz M izometrii w bazach ortonormalnych jest ortogonalna, czyli spełnia $M^{-1} = M^T$. Widzimy więc głęboki związek tych pojęć.

Oczywiście jest mnóstwo endomorfizmów ϕ przestrzeni euklidesowych, które nie muszą spełniać $\phi^{-1} = \phi^*$, czyli nie są izometriami. Dziś rozważać będziemy jedną z najważniejszych takich klas, czyli endomorfizmy samosprzężone. Spełniają one warunek postaci $\phi^* = \phi$. Proszę zauważyć, że w języku macierzowym oznacza to, że macierz takiego przekształcenia spełnia $M^T = M$, czyli jest symetryczna (pokażemy to). Macierze izometrii symetryczne być nie muszą. W linkowanym wyżej skrypcie prof. Szyciczka znajdują Państwo również ogólną teorię tzw. operatorów normalnych, czyli takich ϕ , że $\phi \circ \phi^* = \phi^* \circ \phi$. Teoria ta unifikuje teorię izometrii i endomorfizmów samosprzężonych, a także rozszerza ją na inne endomorfizmy.

Definicja 19.1: Endomorfizm samosprężony

Niech $(V, \langle \cdot, \cdot \rangle)$ będzie przestrzenią euklidesową liniową. Przekształcenie liniowe $\phi : V \rightarrow V$ nazywamy SAMOSPRĘŻONYM, jeśli dla każdego $\alpha, \beta \in V$ zachodzi równość:

$$\langle \alpha, \phi(\beta) \rangle = \langle \phi(\alpha), \beta \rangle.$$

Definicja nie sugeruje, które endomorfizmy są samosprężone. Widzimy to jednak analizując, podobnie jak dla izometrii, macierze tych endomorfizmów w bazie ortonormalnej.

Obserwacja 19.2

Niech ϕ będzie endomorfizmem przestrzeni euklidesowej liniowej $(V, \langle \cdot, \cdot \rangle)$. Wówczas dla dowolnej bazy $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$ przestrzeni V następujące warunki są równoważne:

- ϕ jest samosprężone,
- dla każdego $1 \leq i, j \leq n$ mamy $\langle \alpha_i, \phi(\alpha_j) \rangle = \langle \phi(\alpha_i), \alpha_j \rangle$.

Dowód. Jeśli ϕ jest samosprężone, to oczywiście $\langle \alpha_i, \phi(\alpha_j) \rangle = \langle \phi(\alpha_i), \alpha_j \rangle$, dla każdego i, j . Odwrotnie, jeśli $\langle \alpha_i, \phi(\alpha_j) \rangle = \langle \phi(\alpha_i), \alpha_j \rangle$, dla każdego i, j , to dla każdego wektora $\alpha = x_1\alpha_1 + \dots + x_n\alpha_n$ oraz $\beta = y_1\alpha_1 + \dots + y_n\alpha_n$ mamy:

$$\begin{aligned} \langle \alpha, \phi(\beta) \rangle &= \langle x_1\alpha_1 + \dots + x_n\alpha_n, \phi(y_1\alpha_1 + \dots + y_n\alpha_n) \rangle = \langle x_1\alpha_1 + \dots + x_n\alpha_n, y_1\phi(\alpha_1) + \dots + y_n\phi(\alpha_n) \rangle = \\ &= \sum_{i,j=1}^n x_i y_j \langle \alpha_i, \phi(\alpha_j) \rangle = \sum_{i,j=1}^n x_i y_j \langle \phi(\alpha_i), \alpha_j \rangle = \langle x_1\phi(\alpha_1) + \dots + x_n\phi(\alpha_n), y_1\alpha_1 + \dots + y_n\alpha_n \rangle = \\ &= \langle \phi(x_1\alpha_1 + \dots + x_n\alpha_n), y_1\alpha_1 + \dots + y_n\alpha_n \rangle = \langle \phi(\alpha), \beta \rangle. \end{aligned}$$

□

Wniosek 19.1

Niech ϕ będzie endomorfizmem przestrzeni euklidesowej liniowej $(V, \langle \cdot, \cdot \rangle)$. Jeśli \mathcal{A} jest bazą ortonormalną przestrzeni V , to następujące warunki są równoważne:

- $\phi : V \rightarrow V$ jest samosprężone,
- $M(\phi)_{\mathcal{A}}^{\mathcal{A}}$ jest macierzą symetryczną.

Dowód. Niech $M(\phi)_{\mathcal{A}}^{\mathcal{A}} = [a_{ij}]$. Dla każdego $i, j = 1, \dots, n$ element a_{ij} jest i -tą współrzędną wektora $\phi(\alpha_j)$ w bazie ortonormalnej \mathcal{A} , czyli ma postać $a_{ij} = \langle \alpha_i, \phi(\alpha_j) \rangle$. Korzystając z samosprężoności ϕ oraz z symetryczności iloczynu skalarnego mamy $a_{ji} = \langle \alpha_j, \phi(\alpha_i) \rangle = \langle \phi(\alpha_j), \alpha_i \rangle = \langle \alpha_i, \phi(\alpha_j) \rangle = a_{ij}$. □

Naszym celem będzie pokazanie, że endomorfizmy samosprężone są diagonalizowane i to w pewnej bazie ortogonalnej. Oczywiście dla izometrii to nie jest prawda, ponieważ obroty diagonalizowalne nie są. Przygotujemy teraz szereg obserwacji zmierzających do wykazania tego bardzo ważnego rezultatu.

Obserwacja 19.3

Niech ϕ będzie endomorfizmem samosprężonym przestrzeni $(V, \langle \cdot, \cdot \rangle)$ i niech $W \subseteq V$ będzie podprzestrzenią ϕ -niezmienniczą, czyli $\phi(W) \subseteq W$. Wówczas W^\perp również jest ϕ -niezmienniczą, czyli $\phi(W^\perp) \subseteq W^\perp$. W szczególności, jeśli $\alpha \in V$ jest wektorem własnym ϕ , to $\phi(\text{lin}(\alpha)^\perp) \subseteq \text{lin}(\alpha)^\perp$.

Dowód. Niech W będzie ϕ -niezmienniczą i niech $v \in W^\perp$. Wówczas dla dowolnego $w \in W$ mamy

$$0 = \langle v, \phi(w) \rangle = \langle \phi(v), w \rangle,$$

czyli także $\phi(v) \in W^\perp$. □

Obserwacja 19.4

Jeśli α, β są wektorami własnymi przekształcenia samosprzężonego ϕ o różnych wartościach własnych, to $\alpha \perp \beta$.

Dowód. Niech $\phi(\alpha) = a\alpha$ oraz $\phi(\beta) = b\beta$, dla pewnych $a \neq b$. Wówczas:

$$a \langle \alpha, \beta \rangle = \langle a\alpha, \beta \rangle = \langle \phi(\alpha), \beta \rangle = \langle \alpha, \phi(\beta) \rangle = \langle \alpha, b\beta \rangle = b \langle \alpha, \beta \rangle.$$

Stąd $(a - b) \langle \alpha, \beta \rangle = 0$, czyli $\langle \alpha, \beta \rangle = 0$. □

Podstawową przeszkodą na drodze do ewentualnej diagonalizowalności endomorfizmu przestrzeni rzeczywistej może być brak rzeczywistych wartości własnych (są i inne potencjalne problemy, jak pamiętamy). W przypadku izometrii nietrudno wskazać przykłady obrotów, które nie mają wartości własnych. Wielomian charakterystyczny endomorfizmu nad \mathbb{R} może nie mieć rzeczywistych pierwiastków. Co więcej, do diagonalizowalności nad ciałem \mathbb{R} potrzeba, by wszystkie wartości własne były rzeczywiste (bo suma wymiarów podprzestrzeni własnych \leq suma krotności algebraicznych wartości własnych \leq wymiar, a diagonalizowalność wymaga równości tych wielkości). Okazuje się, że tak właśnie jest w przypadku endomorfizmów samosprzężonych. Zajmijmy się wartościami własnymi macierzy symetrycznej nad \mathbb{R} .

Twierdzenie 19.1

Niech $A \in M_n(\mathbb{R})$ będzie macierzą symetryczną. Wówczas wielomian charakterystyczny macierzy A rozkłada się nad ciałem \mathbb{R} na iloczyn czynników stopnia 1. Innymi słowy, wielomian ten ma n rzeczywistych pierwiastków.

Dowód. Traktujemy macierz A jako macierz z przestrzeni $M_n(\mathbb{C})$. Jak to rozumieć? Każdy wyraz a_{ij} tej macierzy jest postaci $x_{ij} + i \cdot y_{ij}$, przy czym wszystkie y_{ij} równe są 0 (bo wyrazy macierzy są w istocie rzeczywiste). Niech $z \in \mathbb{C}^n$ będzie wektorem własnym macierzy A o wartości własnej $c \in \mathbb{C}$ (korzystamy z zasadniczego twierdzenia algebry). Zatem:

$$A \cdot \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} = \begin{bmatrix} a_{11}z_1 + \dots + a_{1n}z_n \\ \vdots \\ a_{n1}z_1 + \dots + a_{nn}z_n \end{bmatrix} = c \cdot \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix},$$

czyli dla $i = 1, 2, \dots, n$ mamy:

$$a_{i1}z_1 + \dots + a_{in}z_n = cz_i.$$

Mnożymy i -tą równość (wypisaną wyżej) przez \bar{z}_i i otrzymujemy równość:

$$a_{i1}z_1\bar{z}_i + \dots + a_{in}z_n\bar{z}_i = cz_i\bar{z}_i = c|z_i|^2.$$

Dodajemy teraz do siebie wszystkie te równości, dla $i = 1, \dots, n$. Mamy wówczas:

$$\sum_{i,j=1}^n a_{ij}z_j\bar{z}_i = c(|z_1|^2 + \dots + |z_n|^2).$$

Lewą stronę uzyskanej równości przepisać możemy korzystając z założenia $a_{ij} = a_{ji}$ do sumy postaci:

$$a_{11}|z_1|^2 + \dots + a_{nn}|z_n|^2 + \sum_{i < j} a_{ij}(z_j\bar{z}_i + z_i\bar{z}_j).$$

Występujące w tej sumie wyrażenia $z_j\bar{z}_i + z_i\bar{z}_j$ są liczbami rzeczywistymi, bo są sumami liczb zespolonych i ich sprzężeń. Pozostałe składniki wypisanej sumy też są rzeczywiste, a zatem cała suma jest liczbą rzeczywistą. W szczególności także prawa strona równości, czyli $c(|z_1|^2 + \dots + |z_n|^2)$ jest liczbą rzeczywistą. Co więcej, $|z_1|^2 + \dots + |z_n|^2 \neq 0$, bo (z_1, \dots, z_n) jest wektorem własnym. A więc także $c \in \mathbb{R}$, jako iloraz liczby rzeczywistej przez niezerową liczbę rzeczywistą. □

Nawet fakt, że endomorfizm ma wielomian charakterystyczny rozkładający się na czynniki liniowe nie gwarantuje jeszcze diagonalizowalności, w przypadku gdy wartości własne są wielokrotnymi jego pierwiastkami. W przypadku endomorfizmów samosprzężonych problem ten nie występuje, jak pokazuje poniższe oczekiwane przez nas twierdzenie.

Twierdzenie 19.2: Twierdzenie spektralne, wersja rzeczywista

Niech $(V, \langle \cdot, \cdot \rangle)$ będzie przestrzenią euklidesową liniową i niech $\phi : V \rightarrow V$ będzie przekształceniem samosprzężonym. Wówczas istnieje baza ortonormalna przestrzeni $(V, \langle \cdot, \cdot \rangle)$ złożona z wektorów własnych endomorfizmu ϕ .

Zobaczmy przykład. Rozważmy przekształcenie samosprzężone $\phi \in \text{End}(\mathbb{R}^3)$, którego macierz w bazach standardowych ma postać:

$$M(\phi)_{st}^{st} = \begin{bmatrix} 14 & -13 & 8 \\ -13 & 14 & 8 \\ 8 & 8 & -7 \end{bmatrix}.$$

Wówczas poniższa baza \mathcal{A} przestrzeni \mathbb{R}^3 jest ortonormalna

$$\frac{1}{\sqrt{2}}(1, -1, 0), \quad \frac{1}{\sqrt{3}}(1, 1, 1), \quad \frac{1}{\sqrt{6}}(1, 1, -2)$$

i

$$M(\phi)_{\mathcal{A}}^{\mathcal{A}} = \begin{bmatrix} 27 & 0 & 0 \\ 0 & 9 & 0 \\ 0 & 0 & -15 \end{bmatrix}.$$

Dowód. Dowód jest indukcją po $n = \dim V$. Dla $n = 1$ twierdzenie jest oczywiste. Załóżmy jego prawdziwość dla $n - 1$. Niech $\dim V = n$. Niech \mathcal{B} będzie bazą ortonormalną $(V, \langle \cdot, \cdot \rangle)$. Wiemy, że $M(\phi)_{\mathcal{B}}^{\mathcal{B}}$ jest macierzą symetryczną o wyrazach rzeczywistych, więc na mocy ostatniej uwagi ma ona rzeczywistą wartość własną c . Niech $\alpha \in V$ będzie wektorem własnym ϕ o wartości własnej c . Pokazaliśmy wcześniej, że $\phi(\text{lin}(\alpha)^\perp) \subseteq \text{lin}(\alpha)^\perp$ (czyli, że $\text{lin}(\alpha)^\perp$ jest podprzestrzenią ϕ -niezmienniczą).

Rozpatrzmy obcięcie ϕ do podprzestrzeni $n - 1$ -wymiarowej $\text{lin}(\alpha)^\perp$. Wiemy, że obcięcie endomorfizmu do podprzestrzeni niezmienniczej jest endomorfizmem tej podprzestrzeni. Rozważane obcięcie to przekształcenie samosprzężone $n - 1$ -wymiarowej przestrzeni euklidesowej $(\text{lin}(\alpha)^\perp, \langle \cdot, \cdot \rangle|_{\text{lin}(\alpha)^\perp})$. Z założenia indukcyjnego istnieje zatem baza ortonormalna $\alpha_2, \dots, \alpha_n$ przestrzeni $\text{lin}(\alpha)^\perp$ złożona z wektorów własnych przekształcenia $\phi|_{\text{lin}(\alpha)^\perp}$. Oczywiście są to zatem także wektory własne przekształcenia ϕ stanowiące układ ortonormalny. Dopełniamy ten układ prostopadły do bazy ortonormalnej $(V, \langle \cdot, \cdot \rangle)$ znormalizowanym wektorem $\alpha_1 = \frac{1}{\|\alpha\|}\alpha$. Układ $\alpha_1, \dots, \alpha_n$ jest bazą ortonormalną $(V, \langle \cdot, \cdot \rangle)$ złożoną z wektorów własnych ϕ . \square

Wniosek 19.2

Każda macierz symetryczna $A \in M_n(\mathbb{R})$ jest diagonalizowalna nad \mathbb{R} . Co więcej istnieje macierz ortogonalna C taka, że macierz $C^T A C = C^{-1} A C$ jest diagonalna.

Dowód. Niech $\phi : \mathbb{R}^n \rightarrow \mathbb{R}^n$ będzie przekształceniem liniowym zadany warunkiem $M(\phi)_{st}^{st} = A$. Wówczas ϕ jest przekształceniem samosprzężonym przestrzeni \mathbb{R}^n ze standardowym iloczynem skalarnym, istnieje więc baza ortonormalna tej przestrzeni złożona z wektorów własnych ϕ . Niech $\mathcal{C} = (\gamma_1, \dots, \gamma_n)$ będzie taką bazą. Zatem macierz $C = M(id)_{\mathcal{C}}^{st}$ jest ortogonalna i spełnia tezę. \square

Twierdzenie o diagonalizowalności rzeczywistej macierzy symetrycznej przy pomocy bazy ortonormalnej, samo w sobie niezwykle istotne w rozmaitych zastosowaniach matematycznych, jest jedynie niby wrota do jaskini pełnej skarbów i rezultatów stanowiących punkt wyjścia do bardzo rozbudowanych teorii o niezliczonych zastosowaniach pozamatematycznych. Odnotujmy kolejny prosty wniosek.

Wniosek 19.3

Macierz $A \in M_n(\mathbb{R})$ jest diagonalizowalna nad \mathbb{R} wtedy i tylko wtedy, gdy jest podobna do macierzy symetrycznej.

Uwaga. Twierdzenie spektralne w podanej przez nas wersji nie działa dla macierzy zespolonych. Poniższa symetryczna macierz zespolona nie jest diagonalizowalna:

$$\begin{bmatrix} 1 & i \\ i & -1 \end{bmatrix}$$

(ale następnym razem naprawimy ten problem).

Na koniec zobaczmy dwa przykłady stosowania twierdzenia spektralnego w języku macierzowym.

Zadanie 19.1. Znajdź rzeczywistą macierz ortogonalną P taką, że macierz $P^T A P$ jest diagonalna, gdzie

$$A = \begin{bmatrix} 0 & 3 & 0 \\ 3 & 0 & 4 \\ 0 & 4 & 0 \end{bmatrix}.$$

ROZWIĄZANIE. Rozważmy przestrzeń euklidesową \mathbb{R}^3 ze standardowym iloczynem skalarnym i niech $\phi : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ będzie przekształceniem samosprzężonym zadanym w bazie standardowej macierzą A . Wyznamy bazę ortonormalną \mathbb{R}^3 złożoną z wektorów własnych ϕ . Te właśnie wektory stanowią kolumny macierzy P , która w ten sposób (jako macierz w bazach ortonormalnych) będzie ortogonalna, a więc $P^T = P^{-1}$. Wielomian charakterystyczny endomorfizmu ϕ to:

$$\det(A - \lambda I) = \begin{vmatrix} -\lambda & 3 & 0 \\ 3 & -\lambda & 4 \\ 0 & 4 & -\lambda \end{vmatrix} = -\lambda^3 + 25\lambda = -\lambda(\lambda - 5)(\lambda + 5).$$

Nietrudno widzieć, że $V_{(0)} = \text{lin}((4, 0, -3))$, $V_{(5)} = \text{lin}((3, 5, 4))$ oraz $V_{(-5)} = \text{lin}((3, -5, 4))$. Wektory rozpinające te podprzestrzenie są oczywiście prostopadłe w standardowym iloczynie skalarnym. Normalizując te wektory dostajemy szukane kolumny macierzy P , złożone z wektorów:

$$\frac{(4, 0, -3)}{\|(4, 0, -3)\|} = \left(\frac{4}{5}, 0, -\frac{3}{5}\right), \quad \frac{(3, 5, 4)}{\|(3, 5, 4)\|} = \left(\frac{3}{5\sqrt{2}}, \frac{1}{\sqrt{2}}, \frac{4}{5\sqrt{2}}\right), \quad \frac{(3, -5, 4)}{\|(3, -5, 4)\|} = \left(\frac{3}{5\sqrt{2}}, -\frac{1}{\sqrt{2}}, \frac{4}{5\sqrt{2}}\right).$$

Mamy zatem:

$$P^T A P = \begin{bmatrix} \frac{4}{5} & 0 & -\frac{3}{5} \\ \frac{3}{5\sqrt{2}} & \frac{1}{\sqrt{2}} & \frac{4}{5\sqrt{2}} \\ \frac{3}{5\sqrt{2}} & -\frac{1}{\sqrt{2}} & \frac{4}{5\sqrt{2}} \end{bmatrix} \cdot \begin{bmatrix} 0 & 3 & 0 \\ 3 & 0 & 4 \\ 0 & 4 & 0 \end{bmatrix} \cdot \begin{bmatrix} \frac{4}{5} & \frac{3}{5\sqrt{2}} & \frac{3}{5\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ -\frac{3}{5} & \frac{4}{5\sqrt{2}} & \frac{4}{5\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & -5 \end{bmatrix}.$$

■

Nieco trudniejsze zadanie, o zaskakująco prostej treści.

Zadanie 19.2. Niech $(V, \langle \cdot, \cdot \rangle)$ będzie liniową przestrzenią euklidesową. Czy jest możliwe, by dla pewnego układu \mathcal{A} wektorów w przestrzeni V wartość własna macierzy Grama $G(\mathcal{A})$ układu \mathcal{A} była ujemna?

ROZWIĄZANIE. NIE. Korzystamy z twierdzenia o diagonalizowalności endomorfizmów samosprzężonych. Macierz $G(\mathcal{A})$ jest symetryczną macierzą rzeczywistą, więc jest macierzą pewnego endomorfizmu samosprzężonego. Twierdzenie spektralne mówi, że istnieje macierz ortogonalna C taka, że macierz

$$C^T G(\mathcal{A}) C = C^{-1} G(\mathcal{A}) C = D$$

jest diagonalna. Na jej diagonalu stoją rzeczywiste wartości własne macierzy $G(\mathcal{A})$ (na mocy podobieństwa z D). Z drugiej strony D jest również macierzą Grama pewnego układu wektorów w V . Istotnie, wiemy, że $G(\mathcal{A}) = G^T G$, dla macierzy G zawierającej współrzędne wektorów z \mathcal{A} w pewnej bazie ortonormalnej \mathcal{X} przestrzeni V . Zatem

$$C^T G(\mathcal{A}) C = C^T G^T G C = (GC)^T (GC).$$

Niech \mathcal{B} będzie układem wektorów mających w bazie \mathcal{X} współrzędne stanowiące kolejne kolumny macierzy GC . Wówczas $D = G(\mathcal{B})$. A zatem D zawiera na diagonalu wartości $\langle \beta_i, \beta_i \rangle$, gdzie β_i to elementy układu \mathcal{B} . To muszą być liczby nieujemne. A zatem $G(\mathcal{A})$ nie ma ujemnych wartości własnych. ■

19.1 Uzupełnienie. Największa i najmniejsza wartość własna

Jednym z ważnych zastosowań teorii macierzy symetrycznych i twierdzenia o ich diagonalizowalności jest możliwość szacowania wartości własnych tych macierzy. Udowodnimy następujący rezultat.

Obserwacja 19.5

Niech $A \in M_n(\mathbb{R})$ będzie macierzą symetryczną. Dla $\alpha \in \mathbb{R}^n$ niech $\|\alpha\|$ oznacza normę wektora przy standardowym iloczynie skalarnym. Niech wartości własne A to $\lambda_1 \geq \dots \geq \lambda_n$. Wówczas

$$\lambda_1 = \max_{\|\alpha\|=1} \alpha^T A \alpha, \quad \lambda_n = \min_{\|\alpha\|=1} \alpha^T A \alpha.$$

Co więcej, jeśli dla pewnego wektora α mamy $\alpha^T A \alpha = \lambda_i \|\alpha\|^2$, to $A\alpha = \lambda_i \alpha$, gdzie $i = 1, \dots, n$.

Dowód. Dowodzimy tezę dla λ_1 , dla λ_n – całkowicie analogicznie. Niech $\alpha_1, \dots, \alpha_n$ będzie bazą ortonormalną $(\mathbb{R}^n, \langle \cdot, \cdot \rangle_{st})$ złożoną z wektorów własnych macierzy symetrycznej $A \in M_n(\mathbb{R})$ odpowiadających $\lambda_1 \geq \dots \geq \lambda_n$. Niech $\alpha = x_1 \alpha_1 + \dots + x_n \alpha_n$. Wówczas $\|\alpha\|^2 = x_1^2 + \dots + x_n^2$. Zatem

$$\alpha^T A \alpha = \lambda_1 x_1^2 + \dots + \lambda_n x_n^2 \leq \lambda_1 (x_1^2 + \dots + x_n^2) = \lambda_1 \|\alpha\|^2. \quad (*)$$

Z drugiej strony $\alpha_1^T A \alpha_1 = \lambda_1 \|\alpha_1\|^2$, co daje pierwszą część tezy.

Jeśli natomiast dla pewnego wektora α mamy $\alpha^T A \alpha = \lambda_1 \|\alpha\|^2$, to równość w nierówności (*) dostaniemy tylko, gdy $x_{k+1} = \dots = x_n = 0$, gdzie $\lambda_1 = \dots = \lambda_k > \lambda_{k+1} \geq \dots \geq \lambda_n$. Stąd $\alpha = x_1 \alpha_1 + \dots + x_k \alpha_k$ i dostajemy $A\alpha = \lambda_1 \alpha$. \square

Obserwacja 19.6

Niech $A \in M_n(\mathbb{R})$ będzie macierzą symetryczną o wyrazach nieujemnych i wartościach własnych $\lambda_1 \geq \dots \geq \lambda_n$. Istnieje wówczas niezerowy wektor $\alpha = (a_1, \dots, a_n)$ taki, że $A\alpha = \lambda_1 \alpha$ oraz $a_i \geq 0$, dla $1 \leq i \leq n$.

Dowód. Niech $\alpha_1 = (x_1, \dots, x_n)$ będzie wektorem własnym macierzy symetrycznej A o nieujemnych wyrazach o największej jej wartości własnej λ_1 , gdzie $\|\alpha_1\| = 1$. Niech $\alpha = (|x_1|, \dots, |x_n|)$. Wówczas $\|\alpha\| = \|\alpha_1\|$. Skoro A jest nieujemna, to $\alpha^T A \alpha \geq \alpha_1^T A \alpha_1 = \lambda_1$. Zatem z poprzedniego faktu mamy $\alpha^T A \alpha = \lambda_1$ oraz $A\alpha = \lambda_1 \alpha$. \square

Rezultaty te mają duże znaczenie na przykład w algebraicznej teorii grafów³. Uogólniają się one do tzw. twierdzenia min-max oraz twierdzenia Gershgorina.

Zadanie 19.3. Niech $A, B \in M_n(\mathbb{R})$ będą macierzami symetrycznymi, których wszystkie wartości własne są większe niż 1. Pokaż, że dla każdej rzeczywistej wartości własnej γ macierzy AB mamy $|\gamma| > 1$.

ROZWIĄZANIE. (IMC 2013) Rozważmy $(\mathbb{R}^n, \langle \cdot, \cdot \rangle_{st})$. Weźmy bazę ortonormalną $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$ złożoną z wektorów własnych macierzy B w \mathbb{R}^n oraz weźmy dowolny wektor $0 \neq \alpha \in \mathbb{R}^n$ mający w tej bazie współrzędne a_1, \dots, a_n . Mamy zatem (dzięki ortonormalności \mathcal{A}):

$$\begin{aligned} \|B\alpha\|^2 &= \|B(a_1 \alpha_1 + \dots + a_n \alpha_n)\|^2 = \\ &= \|\lambda_1 a_1 \alpha_1 + \dots + \lambda_n a_n \alpha_n\|^2 = \\ &= \langle \lambda_1 a_1 \alpha_1 + \dots + \lambda_n a_n \alpha_n, \lambda_1 a_1 \alpha_1 + \dots + \lambda_n a_n \alpha_n \rangle = \\ &= \lambda_1^2 a_1^2 + \dots + \lambda_n^2 a_n^2 > a_1^2 + \dots + a_n^2 = \|\alpha\|^2. \end{aligned}$$

Zatem przemnożenie przez B z lewej strony powiększa, normę dowolnego niezerowego wektora. Podobnie przemnożenie przez A powiększa normę wektora. A zatem dla każdego $0 \neq \alpha \in \mathbb{R}^n$ mamy $\|AB\alpha\| > \|\alpha\|$. Jeśli więc $\|AB\beta\| = \sqrt{\langle \lambda\beta, \lambda\beta \rangle} = |\lambda| \|\beta\|$, dla pewnego $\beta \neq 0$, to $|\lambda| > 1$. \blacksquare

³Przykładowe zastosowanie: jeśli macierz sąsiedztwa grafu G ma największą wartość własną mniejszą od 2, wówczas G musi być drzewem. Więcej: https://wazniak.mimuw.edu.pl/index.php?title=Matematyka_dyskretna_1/Wyk%C5%82ad_15:_Metody_algebraiczne_w_teorii_graf%C3%B3w

19.2 Trivia. Twierdzenie spektralne w teorii grafów

Obiecywałem, że twierdzenie spektralne prowadzi do wielu ciekawych wyników. Posiłkując się obserwacjami 19.5 i 19.6 z uzupełnienia można rozwiązać szereg przyjemnych zadań wymienionych niżej.

Zadanie 19.4. Załóżmy, że $G = (V, E)$ jest niezorientowanym grafem spójnym. Niech $v(G) = n$ oraz $\lambda_{\max}(G)$ (odp. $\lambda_{\min}(G)$) oznacza największą (odp. najmniejszą) wartość własną macierzy sąsiedztwa M_G grafu G . Uzasadnij, że:

1. krotność geometryczna wartości własnej $\lambda_{\max}(G)$ jest równa 1.
2. jeżeli $0 \neq v = (v_1, \dots, v_n) \in \mathbb{R}^n$ jest wektorem własnym macierzy sąsiedztwa M_G odpowiadającym wartości własnej $\lambda_{\max}(G)$, to $v_1, \dots, v_n > 0$ lub $v_1, \dots, v_n < 0$.
3. jeżeli $0 \neq v = (v_1, \dots, v_n) \in \mathbb{R}^n$ jest wektorem własnym macierzy sąsiedztwa M_G odpowiadającym wartości własnej $\lambda \in \sigma(M_G)$ oraz $v_1, \dots, v_n \geq 0$, to $\lambda = \lambda_{\max}(G)$.
4. gdy dla pewnego $k \geq 0$ graf G jest k -regularny, to $\lambda_{\max}(G) = k$.

Zadanie 19.5. Załóżmy, że G jest spójnym grafem niezorientowanym. Wykaż, że średnica G jest mniejsza niż liczba różnych wartości własnych M_G .

Zadanie 19.6. Niech G' będzie podgrafem indukowanym⁴ niezorientowanego grafu G . Wykaż, że

$$\lambda_{\min}(G) \leq \lambda_{\min}(G') \leq \lambda_{\max}(G') \leq \lambda_{\max}(G).$$

Zadanie 19.7. Niech $G = (V, E)$ będzie grafem, w którym najwyższy stopień wierzchołka wynosi k . Niech $\chi(G)$ oznacza liczbę chromatyczną grafu G . Wówczas

- $\chi(G) \leq k + 1$,
- $\frac{2|E|}{|V|} \leq \lambda_{\max}(G) \leq k$,
- $\chi(G) \leq 1 + \lambda_{\max}(G)$.

Zadanie 19.8. Niech $G = (V, E)$ będzie prostym grafem niezorientowanym. Przez $B(G) \in M_{|E| \times |V|}(\mathbb{R})$ oznaczamy macierz $0-1$ -kową, której wiersze indeksowane są krawędziami G , zaś kolumny indeksowane są wierzchołkami G , która na pozycji (i, j) ma 1 wtedy i tylko wtedy, gdy krawędź indeksująca i -ty wiersz $B(G)$ jest incydentna z wierzchołkiem indeksującym j -tą kolumnę $B(G)$.

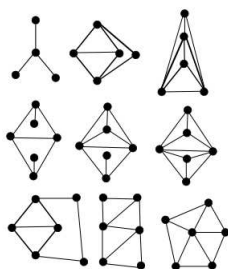
- Pokaż, że $B(G)^T B(G) = \Delta + M_G$, gdzie Δ to macierz diagonalna, której wyrazami są stopnie wierzchołków w G .
- Wywnioskuj stąd, że jeśli G_k jest grafem regularnym stopnia k , to $\lambda_{\min}(M_{G_k}) \geq -k$.

Zadanie 19.9. Niech $G = (V, E)$ będzie prostym grafem niezorientowanym. Grafem krawędziowym $L(G)$ grafu G nazywamy graf⁵, który ma $|E|$ wierzchołków i $|V|$ krawędzi, przy czym wierzchołkami (i, j) , (k, l) grafu $L(G)$ połączone są krawędzią wtedy i tylko wtedy, gdy $i \in \{k, l\}$ lub $j \in \{k, l\}$. Pokaż, że

$$\lambda_{\min}(L(G)) \geq -2.$$

⁴Czyli $V(G') \subseteq V(G)$ i zbiór krawędzi łączących wierzchołki G' jest taki sam, jak w G .

⁵Interesującym problemem jest pytanie czy każdy graf może być grafem krawędziowym. Okazuje się, że nie. W 1968 roku L. Beineke pokazał, że graf jest grafem krawędziowym wtedy i tylko wtedy, gdy nie zawiera żadnego z 9 grafów postaci:



Rozdział 20

Formy hermitowskie Przekształcenia unitarne

Na poprzednich wykładach rozważaliśmy strukturę przestrzeni euklidesowej na przestrzeni liniowej nad ciałem liczb rzeczywistych. Ograniczenie się do przestrzeni rzeczywistej V pozwalało na wprowadzenie warunku $\langle v, v \rangle > 0$, dla $v \neq 0$, co z kolei dało możliwość określenia w $(V, \langle \cdot, \cdot \rangle)$ długości wektora, kąta między wektorami, objętości itd. Podobne konstrukcje można rozważać nad ciałem liczb zespolonych \mathbb{C} .

Podstawowa intuicja pochodzi z geometrycznej interpretacji modułu liczby zespolonej $z = a + bi$ jako długości odcinka łączącego punkty 0 oraz $a+bi$ na płaszczyźnie zespolonej. Moduł ten równy jest $\sqrt{a^2 + b^2}$. Myśląc o przestrzeni \mathbb{C}^2 możemy uprawiać na niej geometrię euklidesową przez utożsamienie jej z \mathbb{R}^4 – każdej parze liczb zespolonych (z_1, z_2) przyporządkowujemy czwórkę (a_1, b_1, a_2, b_2) , przy czym mamy $z_1 = a_1 + b_1i$, $z_2 = a_2 + b_2i$. Załóżmy, że owa przestrzeń \mathbb{R}^4 wyposażona jest w standardowy iloczyn skalarny. Wówczas norma wektora (a_1, b_1, a_2, b_2) wynosi

$$\sqrt{a_1^2 + b_1^2 + a_2^2 + b_2^2}.$$

Powstaje pytanie: czy można przypisać parze $(z_1, z_2) \in \mathbb{C}^2$ jakiś rodzaj „zespolonego iloczynu skalarnego”, który dawałby identyczną normę? Pytamy więc: czy nie znając a_1, b_1, a_2, b_2 , a jedynie operując na samych liczbach zespolonych z_1, z_2 jesteśmy w stanie odtworzyć wzór na normę wektora (z_1, z_2) ?

Czy możemy zdefiniować „standardowy iloczyn skalarny” w \mathbb{C}^2 wzorem $\langle (z_1, z_2), (z'_1, z'_2) \rangle = z_1 z'_1 + z_2 z'_2$ i przyjąć jako normę wektora o współrzędnych zespolonych pierwiastek z „iloczynu skalarnego” tego wektora ze sobą? Otóż nie możemy, bowiem wówczas „norma” wektora (z_1, z_2) byłaby równa $\sqrt{z_1^2 + z_2^2}$, przy czym pod pierwiastkiem stoi liczba zespolona, a taki pierwiastek nie jest jednoznacznie określony. Co więcej, po rozpisaniu postaci ogólnych liczb z_1, z_2 norma ta (żadna z nich) nie byłaby równa $\sqrt{a_1^2 + b_1^2 + a_2^2 + b_2^2}$, poza szczególnymi (jakimi?) przypadkami. Szukany „iloczyn skalarny” w \mathbb{C}^2 uzyskamy natomiast wzorem:

$$\langle (z_1, z_2) | (z'_1, z'_2) \rangle = z_1 \overline{z'_1} + z_2 \overline{z'_2}.$$

Wprawdzie nadal możemy dostać w wyniku $\langle \cdot, \cdot \rangle$ liczbę zespoloną, ale teraz już

$$\langle (z_1, z_2) | (z_1, z_2) \rangle = z_1 \overline{z_1} + z_2 \overline{z_2} = |z_1|^2 + |z_2|^2 \geq 0.$$

A zatem „norma zespolona” wektora (z_1, z_2) według zmodyfikowanej definicji wynosi $\sqrt{a_1^2 + b_1^2 + a_2^2 + b_2^2}$, jak wcześniej.

Nowa definicja rodzi jednak pewne problemy. Otóż nowy „iloczyn skalarny” nie jest liniowy ze względu na drugą zmienną, np.

$$\begin{aligned} \langle (1, 1) | (1, i+1) \rangle &= 1 + (1-i) = 2-i, \text{ zaś} \\ \langle (1, 1), (1, i) \rangle + \langle (1, 1) | (1, 1) \rangle &= 1-i+2 = 3-i. \end{aligned}$$

Wyjaśnienie przynosi następująca definicja obejmująca wprowadzony wyżej „iloczyn półtoraliniowy”.

Definicja 20.1: Iloczyn hermitowski

Niech V będzie przestrzenią liniową nad ciałem \mathbb{C} . Funkcjonał $\langle \cdot | \cdot \rangle : V \times V \rightarrow \mathbb{C}$ nazywamy ILOCZYNEM HERMITOWSKIM (lub PÓŁTORALINIOWYM), jeśli dla każdych $\alpha, \beta, \gamma, \delta \in V$ i $a, b, c, d \in \mathbb{C}$ zachodzi:

$$\begin{aligned} \langle a\alpha + b\beta | \gamma \rangle &= a \langle \alpha | \gamma \rangle + b \langle \beta | \gamma \rangle && \text{liniowość wzgl. pierwszej zmiennej,} \\ \langle \alpha | c\gamma + d\delta \rangle &= \bar{c} \langle \alpha | \gamma \rangle + \bar{d} \langle \alpha | \delta \rangle && \text{antyliniowość wzgl. drugiej zmiennej,} \\ \langle \alpha | \beta \rangle &= \overline{\langle \beta | \alpha \rangle} && \text{hermitowska symetria,} \\ \alpha \neq 0 &\Rightarrow \langle \alpha | \alpha \rangle \in \mathbb{R}_+ && \text{dodatnia określoność.} \end{aligned}$$

Parę $(V, \langle \cdot | \cdot \rangle)$, gdzie V jest skończone wymiarową przestrzenią liniową nad \mathbb{C} oraz $\langle \cdot | \cdot \rangle$ jest iloczynem hermitowskim nazywamy PRZESTRZENIĄ UNITARNĄ.

Podstawowym przykładem iloczynu hermitowskiego jest odpowiednik standardowego iloczynu skalarnego na \mathbb{R}^n , czyli tzw. STANDARDOWY ILOCZYN HERMITOWSKI na \mathbb{C}^n dany wzorem:

$$\langle (z_1, z_2, \dots, z_n) | (z'_1, z'_2, \dots, z'_n) \rangle = z_1 \bar{z}'_1 + z_2 \bar{z}'_2 + \dots + z_n \bar{z}'_n.$$

Iloczyn hermitowski ma fundamentalne znaczenie dla mechaniki kwantowej, gdzie – mówiąc bardzo nieprecyzyjnie – opis stanu układu kwantowego dokonuje się w zespolonej przestrzeni wektorowej. Słynna zasada superpozycji mówi o tym, że stany układu w przestrzeni stanów mogą być kombinacjami liniowymi innych stanów. Klasycznym przykładem jest tu słynny eksperyment myślowy Schrödingera, mówiący o kocie znajdującym się w superpozycji dwóch stanów: „kot żywy” i „kot martwy”.

Obserwacja 20.1

Niech V będzie przestrzenią skończonego wymiaru nad \mathbb{C} oraz niech $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$ będzie bazą przestrzeni V . Wówczas wszystkie formy hermitowskie na V opisane są wzorami:

$$\langle (x_1\alpha_1 + \dots + x_n\alpha_n) | (y_1\alpha_1 + \dots + y_n\alpha_n) \rangle = \sum_{i,j} x_i \bar{y}_j \cdot \langle \alpha_i | \alpha_j \rangle.$$

Innymi słowy, jeśli $A = (a_{ij}) \in M_n(\mathbb{C})$, gdzie $a_{ij} = \langle \alpha_i | \alpha_j \rangle$, to dla każdych

$$\alpha = x_1\alpha_1 + \dots + x_n\alpha_n, \quad \beta = y_1\alpha_1 + \dots + y_n\alpha_n$$

zachodzi następująca równość: $\langle \alpha | \beta \rangle = [x_1 \quad \dots \quad x_n] \cdot A \cdot \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$.

Przykład. Rozważmy przestrzeń $(\mathbb{C}^3, \langle \cdot | \cdot \rangle)$ z formą hermitowską zadaną wzorem:

$$\langle (x_1, x_2, x_3) | (y_1, y_2, y_3) \rangle = -x_1 y_1 - 2i x_1 y_3 + 2x_2 y_2 + 2i x_3 y_1 - x_3.$$

Wówczas $\langle (1, 0, i) | (i, 0, 1) \rangle = 0$, bo:

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

Co więcej, układ

$$\left(\frac{1}{\sqrt{2}}, 0, \frac{i}{\sqrt{2}} \right), \quad (0, 1, 0), \quad \left(\frac{i}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}} \right)$$

stanowi bazę ortonormalną $(\mathbb{C}^3, \langle \cdot | \cdot \rangle)$ (za chwilę wyjaśnimy to pojęcie) i mamy:

$$\begin{bmatrix} -1 & 0 & -2i \\ 0 & 2 & 0 \\ 2i & 0 & -1 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{i}{\sqrt{2}} \\ 0 & 1 & 0 \\ \frac{i}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \end{bmatrix} \cdot \begin{bmatrix} 1 & & \\ & 2 & \\ & & -3 \end{bmatrix} \cdot \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & -\frac{i}{\sqrt{2}} \\ 0 & 1 & 0 \\ -\frac{i}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \end{bmatrix} \quad (\dagger).$$

Definicja 20.2

Niech V będzie przestrzenią nad \mathbb{C} oraz niech $\langle | \rangle$ będzie formą hermitowską na V . Wektory $v, w \in V$ nazywamy PROSTOPADŁYMI, jeśli $\langle v | w \rangle = 0$, ozn. $v \perp w$.

Co nas – matematyków interesuje w przestrzeniach unitarnych na obecnym etapie poznawania algebry liniowej? Przede wszystkim – problemy diagonalizowalności endomorfizmów. Mimo, że iloczyn hermitowski nie jest symetryczny, to prostopadłość wektorów taką własność zachowuje.

Obserwacja 20.2

Niech $(V, \langle | \rangle)$ będzie przestrzenią unitarną oraz niech $\alpha, \beta \in V$. Wówczas $\langle \alpha | \beta \rangle = 0$ wtedy i tylko wtedy, gdy $\langle \beta | \alpha \rangle = 0$.

Dowód. Warunek $\langle \alpha | \beta \rangle = 0$ jest równoważny warunkowi $\overline{\langle \beta | \alpha \rangle} = 0$, co jest równoważne warunkowi $\langle \beta | \alpha \rangle = 0$ (sprzężenie liczby zespolonej jest zerem wtedy i tylko wtedy, gdy ona sama jest zerem). \square

Definicja 20.3: Układ prostopadły

Układ wektorów $\alpha_1, \dots, \alpha_n$ przestrzeni V z formą hermitowską $\langle | \rangle$ nazywamy

- ORTOGONALNYM, jeśli $\langle \alpha_i | \alpha_j \rangle = 0$, dla $1 \leq i, j \leq n$, $i \neq j$,
- ORTONORMALNYM, jeśli jest ortogonalny i $\langle \alpha_i | \alpha_i \rangle = 1$, dla $i = 1, \dots, n$.

Dla podzbioru $S \subseteq V$ przez S^\perp rozumiemy podprzestrzeń liniową złożoną ze wszystkich wektorów z V prostopadłych do wszystkich wektorów ze zbioru S .

Szereg rezultatów dotyczących układów ortogonalnych w przestrzeniach euklidesowych przenosi się bez żadnych zmian na przypadek przestrzeni unitarnych. Czytelnik zechce, śledząc dowody z poprzednich wykładów, sprawdzić (co jest pouczające o tym jakie założenia są tu naprawdę ważne), że:

- układ wektorów ortogonalnych w przestrzeni unitarnej jest liniowo niezależny,
- każda przestrzeń unitarna ma bazę ortogonalną,
- dla podprzestrzeni $W \subseteq V$ mamy $V = W \oplus W^\perp$ oraz $(W^\perp)^\perp = W$,
- współrzędne wektora α w bazie ortogonalnej $(\gamma_1, \dots, \gamma_n)$ przestrzeni V wynoszą:

$$\frac{\langle \alpha | \gamma_1 \rangle}{\langle \gamma_1 | \gamma_1 \rangle}, \frac{\langle \alpha | \gamma_2 \rangle}{\langle \gamma_2 | \gamma_2 \rangle}, \dots, \frac{\langle \alpha | \gamma_n \rangle}{\langle \gamma_n | \gamma_n \rangle}.$$

Ostatni fakt zawiera w sobie pewną istotną delikatność. Liczniki ułamków opisujących współrzędne wektora w bazie ortogonalnej są iloczynami hermitowskimi, więc istotna jest kolejność. Innymi słowy mamy:

$$\langle \alpha | \gamma_i \rangle \neq \langle \gamma_i | \alpha \rangle.$$

To, że w ostatnim wyniku ustalona jest taka właśnie kolejność wynika z przyjętej przez nas definicji iloczynu hermitowskiego, w którym to zachodzi antyliniowość ze względu na drugą, a nie na pierwszą zmienną. Również twierdzenie o ortogonalizacji Grama-Schmidta układu liniowo niezależnego $\alpha_1, \dots, \alpha_n$ do układu ortogonalnego $\gamma_1, \dots, \gamma_n$ przenosi się bez zmian, o ile tylko pamiętamy o przyjęciu odpowiedniej kolejności. Wektory γ_i definiujemy w następujący sposób: $\gamma_1 = \alpha_1$ oraz dla $j > 1$:

$$\gamma_j = \alpha_j - \sum_{i=1}^{j-1} \frac{\langle \alpha_j | \gamma_i \rangle}{\langle \gamma_i | \gamma_i \rangle} \gamma_i.$$

Definicja 20.4: Norma

Niech $(V, \langle \cdot | \cdot \rangle)$ będzie przestrzenią unitarną. NORMĄ WEKTORA $v \in V$ nazywamy liczbę

$$\|v\| = \sqrt{\langle v | v \rangle}.$$

Odnotujmy, że $\|v\| = 0$ wtedy i tylko wtedy, gdy $v = 0$. Co więcej, nietrudno widzieć, że $\|av\| = |a| \cdot \|v\|$. Oto dowód:

$$\|av\|^2 = \langle av | av \rangle = a \langle v | av \rangle = a\bar{a} \langle v | v \rangle = |a|^2 \|v\|^2.$$

Pouczające jest również zobaczenie dowodów odpowiedników twierdzenia Pitagorasa, nierówności Schwarza i nierówności trójkąta (stosują się one także do przypadku euklidesowego).

Obserwacja 20.3

Niech $(V, \langle \cdot | \cdot \rangle)$ będzie przestrzenią unitarną.

- (twierdzenie Pitagorasa) Jeśli u, v są prostopadłe, to $\|u + v\|^2 = \|u\|^2 + \|v\|^2$.
- (nierówność Schwarza) Jeśli $u, v \in V$, to $|\langle u | v \rangle| \leq \|u\| \cdot \|v\|$.
- (nierówność trójkąta) Jeśli $u, v \in V$, to $\|u + v\| \leq \|u\| + \|v\|$.

Dowód. Dla dowodu twierdzenia Pitagorasa zauważmy, że:

$$\begin{aligned} \|u + v\|^2 &= \langle u + v | u + v \rangle = \\ &= \langle u | 1 \cdot u + 1 \cdot v \rangle + \langle v | 1 \cdot u + 1 \cdot v \rangle = \\ &= \bar{1} \langle u | u \rangle + \underbrace{\bar{1} \langle u | v \rangle + \bar{1} \langle v | u \rangle}_0 + \bar{1} \langle v | v \rangle = \\ &= \|u\|^2 + \|v\|^2. \end{aligned}$$

Nierówność Schwarza jest oczywista jeśli u lub v są wektorami zerowymi. Załóżmy przeciwnie. Posłużymy się rozkładem u na wektor będący jego rzutem na $\text{lin}(v)$ oraz pewien wektor z $\text{lin}(v)^\perp$. Dokładniej, określamy $w \in \text{lin}(v)^\perp$ przez:

$$w = u - \frac{\langle u | v \rangle}{\|v\|^2} v$$

Wówczas z twierdzenia Pitagorasa:

$$\begin{aligned} \|u\|^2 &= \left\| \frac{\langle u | v \rangle}{\|v\|^2} v \right\|^2 + \|w\|^2 = \left\langle \frac{\langle u | v \rangle}{\|v\|^2} v \middle| \frac{\langle u | v \rangle}{\|v\|^2} v \right\rangle + \|w\|^2 = \\ &= \frac{\langle u | v \rangle}{\|v\|^2} \langle v | \frac{\langle u | v \rangle}{\|v\|^2} v \rangle + \|w\|^2 = \frac{\langle u | v \rangle}{\|v\|^2} \frac{\langle u | v \rangle}{\|v\|^2} \langle v | v \rangle + \|w\|^2 = \\ &= \frac{|\langle u | v \rangle|^2}{\|v\|^4} \cdot \|v\|^2 + \|w\|^2 = \frac{|\langle u | v \rangle|^2}{\|v\|^2} + \|w\|^2 \geq \frac{|\langle u | v \rangle|^2}{\|v\|^2}. \end{aligned}$$

Mnożąc strony uzyskanej nierówności przez $\|v\|^2$ i pierwiastkując uzyskujemy nierówność Schwarza.

Wreszcie, nierówność trójkąta wymaga następującej dobrze znanej obserwacji zachodzącej dla każdej liczby zespolonej: $\text{Re}(z) \leq |z|$. Mamy podobnie jak wcześniej:

$$\begin{aligned} \|u + v\|^2 &= \langle u + v | u + v \rangle = \\ &= \langle u | u \rangle + \langle u | v \rangle + \langle v | u \rangle + \langle v | v \rangle = \\ &= \|u\|^2 + \|v\|^2 + \langle u | v \rangle + \overline{\langle u | v \rangle} = \\ &= \|u\|^2 + \|v\|^2 + 2\text{Re} \langle u | v \rangle \leq \\ &\leq \|u\|^2 + \|v\|^2 + 2|\langle u | v \rangle| \stackrel{\text{Schwarz}}{\leq} \\ &\leq \|u\|^2 + \|v\|^2 + 2\|u\|\|v\| = (\|u\| + \|v\|)^2. \end{aligned}$$

□

Podobnie jak dla przestrzeni euklidesowych wprowadzić można pojęcie układu i bazy ortonormalnej, a wraz z nim pojęcie macierzy i wyznacznika Grama układu wektorów $\alpha_1, \dots, \alpha_n$ przestrzeni unitarnej $(V, \langle | \rangle)$ o wyrazach postaci $\langle \alpha_i | \alpha_j \rangle$. Zauważmy jednak, że owa „macierz Grama” iloczynu hermitowskiego nie jest symetryczna. Jej wyrazy a_{ij} spełniają bowiem warunek hermitowskiej symetrii. Prowadzi to do fundamentalnej definicji, stanowiącej uogólnienie pojęć macierzy transponowanej i symetrycznej.

Definicja 20.5: Sprzężenie hermitowskie i macierz hermitowska

Niech $A \in (a_{ij}) \in M_n(\mathbb{C})$. Macierz $A^* \in M_n(\mathbb{C})$ mającą w i -tym wierszu i j -tej kolumnie wyraz $\overline{a_{ji}}$ nazywamy SPRZEŻENIEM HERMITOWSKIM macierzy A . Jeśli macierz $A \in M_n(\mathbb{C})$ spełnia warunek $A^* = A$, wówczas mówimy, że A jest macierzą HERMITOWSKĄ.

Oczywiście macierz hermitowska ma na przekątnej liczby rzeczywiste. Oto przykład takiej macierzy

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

Jak się (nietrudno) okazuje, pozostaje w mocy charakteryzacja układów liniowo niezależnych jako tych, których wyznacznik Grama jest niezerowy. Opis macierzy zespolonych stanowiących macierze Grama przypomina kryterium Sylwestera i dowodzi się w zasadzie analogicznie. Dla przykładu, przywołana wyżej macierz hermitowska w sposób oczywisty nie jest macierzą Grama żadnego iloczynu hermitowskiego.

Ma miejsce również niezwykle istotne twierdzenie o diagonalizowalności macierzy hermitowskich, stanowiące zespolony wariant twierdzenia spektralnego. Aby je sformułować (zrobimy to w dodatku — przykładem jest rozkład †), niezbędne jest określenie odpowiednika izometrii w kontekście przestrzeni unitarnych.

Definicja 20.6: Przekształcenie unitarne i macierz unitarna

Niech $(V_1, \langle | \rangle_1)$, $(V_2, \langle | \rangle_2)$ będą przestrzeniami unitarnymi.

- Izomorfizm $\phi : V_1 \rightarrow V_2$ nazywamy PRZEKSZTAŁCENIEM UNITARNYM, jeżeli zachowuje iloczyn hermitowski, tj. dla każdych $\alpha, \beta \in V_1$ mamy:

$$\langle \alpha | \beta \rangle_1 = \langle \phi(\alpha) | \phi(\beta) \rangle_2.$$

- Macierz $M \in M_n(\mathbb{C})$ nazywamy UNITARNĄ, jeśli $M \cdot M^* = M^* \cdot M = I_n$.

W przypadku przestrzeni euklidesowych dowodziliśmy, że ϕ jest izometrią wtedy i tylko wtedy, gdy jego macierz w pewnych (dowolnych) bazach ortonormalnych jest ortogonalna. Analogicznie pokazuje się, że przekształcenia unitarne przestrzeni unitarnych charakteryzują się posiadaniem w pewnych (dowolnych) bazach ortonormalnych macierzy unitarnej. Naszym celem jest pokazanie diagonalizowalności przekształceń unitarnych. Oznacza ona, że każda macierz unitarna jest podobna (nad \mathbb{C}) do macierzy diagonalnej.

Oto przykład macierzy unitarnej, której wartościami własnymi są i oraz 1 :

$$\frac{1}{2} \begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix}.$$

Przywołajmy tabelkę porównującą sytuację w przestrzeniach euklidesowych i unitarnych:

przestrzenie	euklidesowe	unitarne
forma dwuliniowa/półtoraliniowa	iloczyn skalarny	iloczyn hermitowski
macierz formy	symetryczna dod. okr.	hermitowska dod. okr.
macierz izometrii (w bazie ortonorm.)	ortogonalna	unitarna
macierz endom. samosprzężonego	symetryczna	hermitowska

Obserwacja 20.4

Endomorfizm ϕ przestrzeni unitarnej $(V, \langle \cdot | \cdot \rangle)$ jest przekształceniem unitarnym wtedy i tylko wtedy, gdy zachowuje on normę wektora, to znaczy dla każdego $v \in V$ mamy $\langle v | v \rangle = \langle \phi(v) | \phi(v) \rangle$.

Dowód. Konieczność tego warunku jest oczywista, bo przekształcenia unitarne zachowują iloczyn skalarny. Załóżmy, że warunek w tezie jest spełniony dla pewnego endomorfizmu ϕ przestrzeni unitarnej V . Pokażemy, że jest to przekształcenie unitarne. Na mocy założenia dla dowolnych wektorów $u, v \in V$ mamy $\langle u + v | u + v \rangle = \langle \phi(u + v) | \phi(u + v) \rangle$. A zatem po rozpisaniu:

$$\begin{aligned} \langle \phi(u + v) | \phi(u + v) \rangle &= \langle \phi(u) + \phi(v) | \phi(u) + \phi(v) \rangle = \\ &= \langle \phi(u) | \phi(u) \rangle + \langle \phi(v) | \phi(v) \rangle + \langle \phi(u) | \phi(v) \rangle + \langle \phi(v) | \phi(u) \rangle = \\ &= \langle u | u \rangle + \langle v | v \rangle + \langle \phi(u) | \phi(v) \rangle + \langle \phi(v) | \phi(u) \rangle, \end{aligned}$$

czyli $\langle \phi(u) | \phi(v) \rangle + \langle \phi(v) | \phi(u) \rangle = \langle u | v \rangle + \langle v | u \rangle$. Skoro równość ta jest prawdziwa dla dowolnych u, v , to wstawiając w miejsce v wektor iv i korzystając z \mathbb{C} -liniowości ϕ (czyli $\phi(iv) = i\phi(v)$) dostajemy:

$$\begin{aligned} \langle \phi(u) | \phi(iv) \rangle + \langle \phi(iv) | \phi(u) \rangle &= \langle \phi(u) | i\phi(v) \rangle + \langle i\phi(v) | \phi(u) \rangle = \\ &= -i \langle \phi(u) | \phi(v) \rangle + i \langle \phi(v) | \phi(u) \rangle = \\ &= -i \langle u | v \rangle + i \langle v | u \rangle, \end{aligned}$$

czyli po uproszczeniu i mamy

$$- \langle \phi(u) | \phi(v) \rangle + \langle \phi(v) | \phi(u) \rangle = - \langle u | v \rangle + \langle v | u \rangle.$$

Dodając stronami równości $=$ oraz $=$ dostajemy $\langle \phi(v) | \phi(u) \rangle = \langle v | u \rangle$, dla wszystkich $u, v \in V$. \square

Naszym celem jest pokazanie, że w przeciwieństwie do izometrii przestrzeni euklidesowych, przekształcenia unitarne przestrzeni unitarnych są zawsze diagonalizowalne.

Twierdzenie 20.1

Niech ϕ będzie endomorfizmem unitarnym przestrzeni $(V, \langle \cdot | \cdot \rangle)$. Wówczas każda wartość własna $\lambda \in \mathbb{C}$ endomorfizmu ϕ spełnia $|\lambda| = 1$. Wektory własne ϕ odpowiadające parami różnym wartościom własnym są ortogonalne. Istnieje też baza ortogonalna $(V, \langle \cdot | \cdot \rangle)$ złożona z wektorów własnych ϕ .

Dowód. Niech λ będzie wartością własną ϕ . Istnieje więc niezerowy wektor v taki, że $\phi(v) = \lambda v$. Wiemy, że przekształcenie unitarne zachowuje normę, więc mamy $\langle v | v \rangle = \langle \phi(v) | \phi(v) \rangle = \lambda \bar{\lambda} \langle v | v \rangle$. Skoro $\langle v | v \rangle \neq 0$, to $|\lambda|^2 = 1$, co dowodzi pierwszą część tezy.

Weźmy teraz $\lambda_1 \neq \lambda_2 \in \mathbb{C}$, dla których istnieją niezerowe wektory x, y , że $\phi(v_1) = \lambda_1 v_1$, $\phi(v_2) = \lambda_2 v_2$. Przekształcenie unitarne zachowuje iloczyn hermitowski, więc $\langle \phi(x) | \phi(y) \rangle = \langle x | y \rangle$. Skoro wiemy już z poprzedniego punktu tezy, że $|\lambda_2| = 1$, mamy $\bar{\lambda}_2 = \lambda_2^{-1}$. A zatem z założenia $\lambda_1 \neq \lambda_2$ widzimy, że $\lambda_1 \lambda_2^{-1} \neq 1$. Stąd warunek $\langle \phi(x) | \phi(y) \rangle = \langle x | y \rangle = \lambda_1 \bar{\lambda}_2 \langle x | y \rangle = \lambda_1 \lambda_2^{-1} \langle x | y \rangle$, pociąga za sobą $\langle x | y \rangle = 0$, co dowodzi prostopadłości wektorów własnych odpowiadających różnym wartościom własnym przekształcenia unitarnego.

Dowodzimy teraz istnienia bazy $(V, \langle \cdot | \cdot \rangle)$ złożonej z wektorów własnych ϕ . Dowód jest indukcją ze względu na wymiar n przestrzeni V . Dla $n = 1$ teza jest jasna. Przechodzimy do kroku indukcyjnego. Skoro ϕ jest endomorfizmem przestrzeni zespolonej, to oczywiście ma wartość własną (bo jego wielomian charakterystyczny musi mieć, jako wielomian o współczynnikach w \mathbb{C} , pierwiastek), którą oznaczamy λ . Niech x będzie odpowiadającym jej niezerowym wektorem własnym. Rozważmy $\text{lin}(x)^\perp$. Twierdzimy, że $(\text{lin}(x)^\perp, \langle \cdot | \cdot \rangle |_{\text{lin}(x)^\perp})$ jest przestrzenią unitarną (to jest w zasadzie oczywiste, tak jak dla iloczynów skalarnych, na mocy dodatniej określoności) oraz, że $\text{lin}(x)^\perp$ jest ϕ -niezmiennicza. Istotnie, weźmy $v \in \text{lin}(x)^\perp$. Z faktu, że ϕ zachowuje normę i jest izomorfizmem mamy

$$\langle \phi(v) | x \rangle = \langle v | \phi^{-1}(x) \rangle = \langle v | \lambda^{-1}x \rangle = \bar{\lambda}^{-1} \langle v | x \rangle = 0.$$

A zatem ϕ obcięte do $\text{lin}(x)^\perp$ jest endomorfizmem unitarnym przestrzeni wymiaru $n-1$ (już wspominałem, że w przestrzeni unitarnej mamy $V = \text{lin}(x) \oplus \text{lin}(x)^\perp$), a zatem na mocy założenia indukcyjnego jest diagonalizowalny w pewnej bazie $\alpha_1, \dots, \alpha_{n-1}$. Każdy z wektorów tej bazy jest prostopadły do x . A zatem układ $\alpha_1, \dots, \alpha_{n-1}, x$ jest bazą ortogonalną V złożoną z wektorów własnych ϕ . \square

20.1 Uzupełnienie. Twierdzenie spektralne (wersja zespolona)

Na poprzednich wykładach wspominaliśmy o klasie endomorfizmów przestrzeni euklidesowej, która stanowi wspólne przekształceń unitarnych i samosprężonych.

Definicja 20.7: Endomorfizm normalny

Niech $(V, \langle \cdot, \cdot \rangle)$ będzie przestrzenią euklidesową lub $(V, \langle \cdot | \cdot \rangle)$ będzie przestrzenią unitarną. Powiemy, że $\phi \in \text{End}(V)$ jest NORMALNY, jeśli zachodzi równość:

$$\phi \circ \phi^* = \phi^* \circ \phi.$$

Przykłady.

- Izometria przestrzeni euklidesowej spełnia $\phi^* = \phi^{-1}$, więc jest normalna, podobnie każde przekształcenie unitarne przestrzeni unitarnej.
- Endomorfizm samosprężony spełnia $\phi^* = \phi$, czyli jest normalny.

- Endomorfizm $\phi \in \mathbb{R}^3$ zadany macierzą $A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$ jest normalny, bo:

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

Naszym celem będzie pokazanie niełatwego twierdzenia spektralnego w wersji zespolonej.

Twierdzenie 20.2: Twierdzenie spektralne – wersja zespolona

Niech $(V, \langle \cdot | \cdot \rangle)$ będzie przestrzenią unitarną oraz $\phi \in \text{End}(V)$. Następujące warunki są równoważne:

- (1) V ma bazę ortonormalną złożoną z wektorów własnych ϕ ,
- (2) endomorfizm ϕ jest normalny.

Dowód implikacji (1) \Rightarrow (2) jest prosty. Niech V ma bazę ortonormalną \mathcal{A} wektorów własnych ϕ . Mamy zatem $M(\phi)_{\mathcal{A}}^{\mathcal{A}} = D$ oraz $M(\phi^*)_{\mathcal{A}}^{\mathcal{A}} = \overline{D}$, gdzie D jest diagonalna. Skoro dowolne dwie macierze diagonalne są przemieszczalne, to ϕ oraz ϕ^* są przemieszczalne, czyli ϕ jest endomorfizmem normalnym. Widać więc, że definicja endomorfizmu normalnego jest naturalna w kontekście twierdzenia spektralnego.

Do dowodu implikacji (2) \Rightarrow (1) będą potrzebne dwa (lub więcej) fakty.

Obserwacja 20.5: Zespolony rozkład QR

Każdą macierz $A \in M_n(\mathbb{C})$ można przedstawić w postaci $A = QR$, gdzie Q jest unitarna, zaś R jest górnotrójkątna.

Dowód wynika z ortogonalizacji Grama-Schmidta i przeprowadzany jest analogicznie jak dla przestrzeni euklidesowych. Zostawiamy go jako ćwiczenie.

Obserwacja 20.6: Lemat pomocniczy

Niech ϕ będzie endomorfizmem przestrzeni unitarnej $(V, \langle \cdot | \cdot \rangle)$. Wówczas ϕ jest normalny wtedy i tylko wtedy, gdy dla każdego $v \in V$ mamy:

$$\|\phi(v)\| = \|\phi^*(v)\|.$$

Pokażmy najpierw jak twierdzenie spektralne wynika z tych faktów. Dowód drugiego z nich nie jest wcale prosty, stąd poczekamy z jego ilustracją. Idea dowodu jest następująca: poprawić macierz operatora normalnego najpierw do górnotrójkątnej (rozkład QR), a potem do diagonalnej (lemat pomocniczy).

Dowód twierdzenia spektralnego. Załóżmy, że ϕ jest macierzą normalną. Wiadomo, że ϕ jest triangulizowalny jako endomorfizm przestrzeni zespolonej, czyli w pewnej bazie ma macierz górnotrójkątną A . Korzystając z rozkładu $A = QR$ znajdujemy ortonormalną bazę $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$ przestrzeni V taką, że:

$$M(\phi)_{\mathcal{A}}^{\mathcal{A}} = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ & \ddots & \vdots \\ 0 & & a_{nn} \end{bmatrix}, \quad M(\phi^*)_{\mathcal{A}}^{\mathcal{A}} = \begin{bmatrix} \overline{a_{11}} & & 0 \\ \vdots & \ddots & \\ \overline{a_{1n}} & \dots & \overline{a_{nn}} \end{bmatrix}$$

Pokażemy, że powyższe macierze są w istocie diagonalne. Mamy:

$$\|\phi(\alpha_1)\|^2 = |a_{11}|^2, \quad \|\phi^*(\alpha_1)\|^2 = |a_{11}|^2 + |a_{12}|^2 + \dots + |a_{1n}|^2.$$

Z lematu pomocniczego $\|\phi(\alpha_1)\| = \|\phi^*(\alpha_1)\|$. Zatem $a_{1j} = 0$, dla $j > 1$. Zatem:

$$\|\phi(\alpha_2)\|^2 = |a_{22}|^2 \quad \text{oraz} \quad \|\phi^*(\alpha_2)\|^2 = |a_{22}|^2 + \dots + |a_{2n}|^2.$$

Z Lematu pomocniczego mamy również

$$\|\phi(\alpha_2)\| = \|\phi^*(\alpha_2)\|, \quad \text{czyli} \quad a_{2j} = 0, \quad \text{dla } j > 2 \dots$$

Analogicznie zerujemy pozycje poza przekątną w kolejnych wierszach $M(\phi)_{\mathcal{A}}^{\mathcal{A}}$, co daje nam tezę twierdzenia spektralnego. \square

Naszkicujemy teraz dowód Lematu pomocniczego. Ma on kilka etapów i jest dość pouczający.

Obserwacja 20.7: Fakt 1 (na drodze do Lematu pomocniczego)

Jeśli $(V, \langle \cdot | \cdot \rangle)$ jest przestrzenią unitarną oraz $\phi \in \text{End}(V)$ spełnia równość

$$\langle \phi(v) | v \rangle = 0,$$

dla każdego $v \in V$, to $\phi = 0$.

Dowód. Nietrudno sprawdzić, że dla każdego $\phi \in \text{End}(V)$ oraz dla $u, w \in V$ mamy:

$$\langle \phi(u) | w \rangle = \frac{\langle \phi(u+w) | u+w \rangle - \langle \phi(u-w) | u-w \rangle}{4} + \frac{\langle \phi(u+iw) | u+iw \rangle - \langle \phi(u-iw) | u-iw \rangle}{4} i.$$

Jeśli dla każdego $v \in V$ mamy $\langle \phi(v) | v \rangle = 0$, to lewa strona równości wyżej wynosi 0, dla dowolnych $u, w \in V$. Dla $w = \phi(u)$ mamy zatem $\langle \phi(u) | \phi(u) \rangle = 0$, czyli $\phi(u) = 0$, dla każdego $u \in V$. Stąd oczywiście $\phi = 0$. \square

Wniosek 20.1: Endomorfizmy samosprężone *są jak* liczby rzeczywiste

Niech $(V, \langle \cdot | \cdot \rangle)$ będzie przestrzenią unitarną. Wówczas następujące warunki są równoważne dla przekształcenia $\phi \in \text{End}(V)$:

- ϕ jest samosprężony, tzn. $\phi = \phi^*$,
- $\langle \phi(v) | v \rangle \in \mathbb{R}$ dla każdego $v \in V$.

Dowód. Niech $v \in V$. Wówczas:

$$\langle \phi(v) | v \rangle - \overline{\langle \phi(v) | v \rangle} = \langle \phi(v) | v \rangle - \langle v | \phi(v) \rangle = \langle \phi(v) | v \rangle - \langle \phi^*(v) | v \rangle = \langle (\phi - \phi^*)(v) | v \rangle.$$

Jeśli $\langle \phi(v) | v \rangle \in \mathbb{R}$, dla każdego $v \in V$, to lewa strona równości wyżej wynosi 0, czyli dla każdego v mamy także $\langle (\phi - \phi^*)(v) | v \rangle = 0$. Z Faktu 1 mamy więc $\phi - \phi^* = 0$, czyli ϕ jest samosprężony. Jeśli ϕ jest z kolei samosprężony, to prawa strona powyższej równości wynosi 0, czyli $\langle \phi(v) | v \rangle \in \mathbb{R}$, dla każdego v . \square

Obserwacja 20.8: Fakt 2 (na drodze do Lematu pomocniczego)

Jeśli $(V, \langle \cdot, \cdot \rangle)$ jest przestrzenią euklidesową oraz przekształcenie samosprężone^a $\phi \in \text{End}(V)$ spełnia równość

$$\langle \phi(v) | v \rangle = 0,$$

dla każdego $v \in V$, to $\phi = 0$.

^aIstnieją endomorfizmy przestrzeni euklidesowych $\phi \neq 0$, że $\langle \phi(v) | v \rangle = 0$, dla $v \in V$.

Dowód. Dla każdych $u, w \in V$ mamy:

$$\langle \phi(u) | w \rangle = \frac{\langle \phi(u+w) | u+w \rangle - \langle \phi(u-w) | u-w \rangle}{4},$$

co wynika z równości:

$$\langle \phi(w) | u \rangle = \langle w | \phi(u) \rangle = \langle \phi(u) | w \rangle.$$

Jeśli $\langle \phi(v) | v \rangle = 0$, dla każdego $v \in V$, to równość wyżej daje $\langle \phi(u) | w \rangle = 0$, dla wszystkich $u, w \in V$. Czyli $\phi = 0$ (po wzięciu $w = \phi(u)$). \square

Dowodzimy teraz lemat pomocniczy, czyli pokazujemy, że endomorfizm ϕ przestrzeni unitarnej $(V, \langle \cdot | \cdot \rangle)$ jest normalny wtedy i tylko wtedy, gdy dla każdego $v \in V$ mamy:

$$\|\phi(v)\| = \|\phi^*(v)\|.$$

Niech $\phi \in \text{End}(V)$. Zauważmy, że $\phi^*\phi - \phi\phi^*$ jest samosprężony. Mamy zatem (pomijam symbol \circ):

$$\begin{aligned} \phi^*\phi - \phi\phi^* = 0 &\Leftrightarrow \langle (\phi^*\phi - \phi\phi^*)(v) | v \rangle = 0, \quad \forall v \in V \\ &\Leftrightarrow \langle (\phi^*\phi)(v) | v \rangle = \langle (\phi\phi^*)(v) | v \rangle, \quad \forall v \in V. \end{aligned}$$

Z definicji przekształcenia sprzężonego mamy $\langle (\phi^*\phi)(v) | v \rangle = \langle \phi(v) | \phi(v) \rangle$ oraz $\langle (\phi\phi^*)(v) | v \rangle = \langle \phi^*(v) | \phi^*(v) \rangle$, czyli ostatecznie dla każdego $v \in V$:

$$\langle (\phi^*\phi)(v) | v \rangle = \langle (\phi\phi^*)(v) | v \rangle \Leftrightarrow \|\phi(v)\|^2 = \|\phi^*(v)\|^2.$$

* * *

Z twierdzenia spektralnego można wyciągnąć szereg wniosków. Jednym z nich jest klasyfikacja endomorfizmów normalnych, uogólniająca między innymi klasyfikację izometrii. Rezultat ten podajemy bez dowodu. Nie jest on jednak specjalnie trudniejszy od powyższych rozumowań.

Twierdzenie 20.3

Niech $(V, \langle \cdot, \cdot \rangle)$ będzie przestrzenią euklidesową, oraz niech $\phi \in \text{End}(V)$. Wówczas następujące warunki są równoważne^a:

- ϕ jest normalny,
- istnieje baza ortonormalna V , w której macierz ϕ jest blokowo-diagonalna o klatkach wielkości 1×1 lub o klatkach wielkości 2×2 mających postać $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$, dla $b > 0$, na przykład:

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

^aWarto to sprawdzić choćby dla $\dim V = 2$.

20.2 Dodatek. Operatory zespolone przypominają liczby

Hasło powyższego dodatku może wydawać się nieco tajemnicze, ale stoi za nim bardzo poważny aparat wykorzystywany w zastosowaniach. Będziemy tu mówić o dowodach twierdzeń o rozkładach, które sygnalizowaliśmy w dodatku do rozdziału o izometriach. Oto niezbyt formalnie wypowiedziane analogie między \mathbb{C} a $\text{End}(V)$, gdzie $(V, \langle \cdot | \cdot \rangle)$ – przestrzeń unitarna:

- jeśli $\phi \in \text{End}(V)$ *jest jak* $z \in \mathbb{C}$, to ϕ^* jest jak \bar{z} ,
- jeśli ϕ jest samosprzężony, to *jest jak* liczba rzeczywista,
- jeśli ϕ jest dodatnio półokreślony, to *jest jak* liczba nieujemna,
- jeśli ϕ jest izometrią, czyli $\phi^*\phi = \text{id}$, to *jest jak* element $|z| = 1$,

Aby uzasadnić te intuicje wprowadzimy najpierw definicję endomorfizmu dodatnio półokreślonego.

Definicja 20.8: Endomorfizm i macierz niedodatnio półokreślona

Niech ϕ będzie endomorfizmem samosprzężonym przestrzeni unitarnej V (odp. euklidesowej). Powiemy, że ϕ jest

- DODATNIO OKREŚLONY, jeśli: $\langle \phi(v) | v \rangle > 0$, dla $v \neq 0$ (odp. $\langle \phi(v), v \rangle > 0$),
- DODATNIO PÓŁOKREŚLONY, jeśli $\langle \phi(v) | v \rangle \geq 0$, dla $v \in V$ (odp. $\langle \phi(v), v \rangle \geq 0$).

Macierze tych endomorfizmów w dowolnej bazie nazywamy odpowiednio dodatnio określonymi oraz dodatnio półokreślonymi (lub nieujemnie określonymi).

Zacznijmy od dwóch prostych obserwacji.

- Jeśli ϕ jest nieujemnie określony i λ jest wartością własną ϕ , to $\lambda \geq 0$, bo:

$$0 \leq \langle \phi(v) | v \rangle = \langle \lambda v | v \rangle = \lambda \langle v | v \rangle.$$

- Jeśli $\alpha_1, \dots, \alpha_n$ stanowią ortonormalną bazę V złożoną z wektorów własnych przekształcenia dodatnio półokreślonego ϕ o wartościach własnych $\lambda_1, \dots, \lambda_n$, to definiując $\psi \in \text{End}(V)$ na bazie V warunkami $\psi(\alpha_i) = \sqrt{\lambda_i} \alpha_i$ widzimy, że ψ jest dodatnio półokreślony oraz $\psi^2 = \phi$.

Twierdzenie 20.4: Przekształcenie nieujemnie określone *jest jak* liczba nieujemna

Niech ϕ będzie endomorfizmem przestrzeni unitarnej $(V, \langle \cdot | \cdot \rangle)$. Następujące warunki są równoważne:

- ϕ jest dodatnio półokreślone,
- ϕ jest samosprzężone i ma nieujemne wartości własne,
- ϕ ma dodatnio półokreślony pierwiastek^a
- ϕ ma samosprzężony pierwiastek
- istnieje $\psi \in \text{End}(V)$, że $\phi = \psi^* \circ \psi$.

Co więcej każdy dodatnio półokreślony ϕ ma dokładnie jeden dodatnio półokreślony pierwiastek.

^aOczywiście dodatnio półokreślone przekształcenie może mieć nieskończenie wiele pierwiastków, np. identyczność na przestrzeni unitarnej wymiaru większego niż 1.

Nie będziemy pokazywać dowodu tego twierdzenia, chcemy natomiast zrozumieć na czym polega intuicja bycia „jak” liczba nieujemna. Dla każdej liczby zespolonej $z \neq 0$ mamy rozkład $z = \left(\frac{z}{|z|}\right) |z| = \left(\frac{z}{|z|}\right) \sqrt{\bar{z}z}$, gdzie $z/|z|$ należy do okręgu jednostkowego, a $\bar{z}z$ to liczba nieujemna. I właśnie o tym ostatnim czynniku myślimy jako o części nieujemnie określonej. „Części”, bowiem zachodzi następujące twierdzenie.

Twierdzenie 20.5: Twierdzenie o rozkładzie biegunowym endomorfizmu

Dla dowolnej macierzy $T \in M_n(\mathbb{C})$ (odp. $T \in M_n(\mathbb{R})$) istnieje macierz unitarna (odp. ortogonalna) S taka, że $T = S\sqrt{T^*T}$. Innymi słowy każdy endomorfizm ϕ przestrzeni unitarnej (odp. euklidesowej) to złożenie przekształcenia unitarnego ψ (odp. izometrii) i dodatnio półokreślonego $\sqrt{\phi^* \circ \phi}$.

Dowód. Przez całe rozumowanie pomijamy symbol \circ . Niech $\phi \in \text{End}(V)$. Korzystając z faktu, że $\phi^*\phi$ jest nieujemnie określony (oczywiste) i ma pierwiastek nieujemnie określony dostajemy, dla każdego $v \in V$:

$$\begin{aligned} \|\phi(v)\|^2 &= \langle \phi(v) | \phi(v) \rangle = \\ &= \langle (\phi^*\phi)(v) | v \rangle = \\ &= \langle (\sqrt{\phi^*\phi}\sqrt{\phi^*\phi})(v) | v \rangle = \\ &= \langle (\sqrt{\phi^*\phi})(v) | (\sqrt{\phi^*\phi})(v) \rangle = \\ &= \|(\sqrt{\phi^*\phi})(v)\|^2. \end{aligned}$$

Stąd $\|\phi(v)\| = \|(\sqrt{\phi^*\phi})(v)\|$, dla $v \in V$.

Idea dowodu: określamy $\psi_1 : \text{im}(\sqrt{\phi^*\phi}) \rightarrow \text{im}(\phi)$ wzorem:

$$\psi_1(\sqrt{\phi^*\phi}(v)) = \phi(v).$$

oraz pokazujemy, że ψ_1 da się rozszerzyć do przekształcenia unitarnego (odp. izometrii) ψ takiej, że: $\phi = \psi\sqrt{\phi^*\phi}$.

Niech ϕ – endomorfizm V . Mamy

$$\|\phi(v)\| = \|(\sqrt{\phi^*\phi})(v)\|, \text{ dla } v \in V.$$

Określamy $\psi_1 : \text{im}(\sqrt{\phi^*\phi}) \rightarrow \text{im}(\phi)$ wzorem

$$\psi_1(\sqrt{\phi^*\phi}(v)) = \phi(v).$$

Po pierwsze ψ_1 jest dobrze określone. Biorąc $v_1, v_2 \in V$ takie, że $\sqrt{\phi^*\phi}(v_1) = \sqrt{\phi^*\phi}(v_2)$ mamy:

$$\begin{aligned} \|\psi_1(v) - \psi_2(v)\| &= \|\phi(v_1) - \phi(v_2)\| = \|\phi(v_1 - v_2)\| = \\ &= \|\sqrt{\phi^*\phi}(v_1 - v_2)\| = \|\sqrt{\phi^*\phi}(v_1) - \sqrt{\phi^*\phi}(v_2)\| = 0 \end{aligned}$$

Oczywiście ψ_1 jest liniowe. Mamy też $\|\psi_1(u)\| = \|u\|$, dla $u \in \text{im}(\sqrt{\phi^*\phi})$. Stąd ψ_1 to monomorfizm. Zatem z twierdzenia o sumie wymiarów jądra i obrazu mamy: $\dim \text{im}(\sqrt{\phi^*\phi}) = \dim \text{im} \phi$, co implikuje

$$\dim(\text{im}(\sqrt{\phi^*\phi}))^\perp = \dim(\text{im} \phi)^\perp.$$

Niech e_1, \dots, e_m oraz f_1, \dots, f_m to bazy ortonormalne odpowiednio $(\text{im}(\sqrt{\phi^*\phi}))^\perp$ oraz $(\text{im} \phi)^\perp$. Definiujemy $\psi_2 : (\text{im}(\sqrt{\phi^*\phi}))^\perp \rightarrow (\text{im} \phi)^\perp$ wzorem:

$$\psi_2(a_1e_1 + \dots + a_me_m) = a_1f_1 + \dots + a_mf_m.$$

Określamy ψ nad V tak, by równało się ψ_1 na $\text{im}(\sqrt{\phi^*\phi})$ oraz ψ_2 na $(\text{im}(\sqrt{\phi^*\phi}))^\perp$. Dla każdego $v \in V$ mamy:

$$\psi((\sqrt{\phi^*\phi})v) = \psi_1((\sqrt{\phi^*\phi})(v)) = \phi(v) \Rightarrow \phi = \psi\sqrt{\phi^*\phi}.$$

Pozostaje pokazać, że ψ to izometria. Jeśli $v = u + w$, gdzie $u \in \text{im}(\sqrt{\phi^*\phi})$ oraz $w \in (\text{im}(\sqrt{\phi^*\phi}))^\perp$, to $\psi_1(u) \perp \psi_2(w)$. Zatem z twierdzenia Pitagorasa:

$$\|\psi(v)\|^2 = \|\psi_1u + \psi_2(w)\|^2 = \|\psi_1(u)\|^2 + \|\psi_2(w)\|^2 = \|u\|^2 + \|w\|^2 = \|v\|^2$$

co kończy dowód twierdzenia o rozkładzie biegunowym. □

20.3 Trivia. Zasadnicze twierdzenie algebry — zrób to sam!

Teoria macierzy hermitowskich pozwala udowodnić zasadnicze twierdzenie algebry, o ile można używać faktu, że wielomiany rzeczywiste nieparzystego stopnia mają pierwiastek rzeczywisty oraz o ile wolno rozwiązywać równania kwadratowe. Nie jest to oczywiste, ale dowód jest niezwykle elegancki.

W trakcie studiów poznają Państwo zarówno czysto analityczny dowód zasadniczego twierdzenia algebry (Analiza 1.2), jak i topologiczny (Topologia 2), dowód w teorii funkcji zespolonych (Funkcje analityczne) i oczywiście dowód w teorii Galois (Algebra 2), a także (potencjalnie) inne.

Dowód prezentowany niżej pochodzi z lat 90-tych od H. Derksena, z artykułu *The Fundamental Theorem of Algebra and Linear Algebra*, Amer. Math. Monthly 110 (2003), 620–623. Jego opracowanie wraz z komentarzami i odnośnikami do innych materiałów przeglądowych o ZTA można znaleźć u Keitha Conrada <https://kconrad.math.uconn.edu/blurbs/fundthmalg/fundthmalglinear.pdf>, ale nie chcę zabierać Państwu przyjemności samodzielnego przeprowadzenia tego rozumowania.

* * *

Nasz cel: wykazać, że każda macierz $M \in M_n(\mathbb{C})$ ma wektor własny.

Zadanie 20.1. Niech $m > 1$ będzie ustaloną liczbą całkowitą, zaś K niech będzie takim ciałem, że dla każdej przestrzeni liniowej V nad ciałem K takiej, że $m \nmid \dim V$, każdy $\sigma \in \text{End}(V)$ ma wektor własny¹. Rozważmy dowolną parę przemiennych endomorfizmów ϕ, ψ przestrzeni V nad ciałem K spełniających warunek $m \nmid \dim V$. Niech $\lambda \in K$ będzie wartością własną endomorfizmu ϕ i niech

$$U = \text{im}(\phi - \lambda \text{id}), \quad V = \ker(\phi - \lambda \text{id}).$$

- Wykaż, że podprzestrzenie U, V są ψ -niezmiennicze.
- Wykaż, przez indukcję po (dozwolonych) $\dim V$, że ϕ, ψ mają wspólny wektor własny, tzn. istnieje $0 \neq u \in V$ oraz $a, b \in K$ takie, że $\phi(u) = au, \psi(u) = bu$.

Zadanie 20.2. Rozważamy $M_n(\mathbb{C})$ jako przestrzeń wymiaru $2n^2$ nad \mathbb{R} . Wykaż, że podprzestrzeń $M_n(\mathbb{C})$ złożona z macierzy hermitowskich (tzn. $M \in H_n \Leftrightarrow M = M^* := \overline{M^T}$), ozn H_n , ma wymiar n^2 (nad \mathbb{R}).

Zadanie 20.3. Niech $A \in M_n(\mathbb{C})$. Pokaż, że następujące odwzorowania są przemiennymi endomorfizmami przestrzeni macierzy hermitowskich H_n (uzasadnij w szczególności, że obrazy są w H_n):

$$L_1(B) = \frac{AB + BA^*}{2}, \quad L_2(B) = \frac{AB - BA^*}{2i}, \quad \text{gdzie } B \in H_n.$$

Wynioskuj stąd, że dla $2 \nmid n$ każda macierz $A \in M_n(\mathbb{C})$ ma wektor własny w \mathbb{C}^n (wsk.: $AB = \dots$).

Zadanie 20.4. Niech S_n będzie \mathbb{C} -podprzestrzenią macierzy symetrycznych w $M_n(\mathbb{C})$ (tzn. $M \in S_n \Leftrightarrow M = M^T$). Wykaż, że

$$\dim S_n = \frac{n(n+1)}{2}.$$

Niech $A \in M_n(\mathbb{C})$.

- Wykaż, że poniższe odwzorowania są przemiennymi endomorfizmami S_n (jako przestrzeni nad \mathbb{C}):

$$M_1(B) = AB + BA^T, \quad M_2(B) = ABA^T, \quad \text{gdzie } B \in S_n.$$

- Wykaż, że jeśli dla pewnej $B \in S_n$ mamy $M_1(B) = \lambda B$ oraz $M_2(B) = \mu B$, gdzie $\lambda, \mu \in \mathbb{C}$, to

$$(A^2 - \lambda A + \mu)B = 0.$$

Zadanie 20.5. Udowodnij, poprzez indukcję ze względu na wykładnik 2-adyczny liczby n , że każda macierz $A \in M_n(\mathbb{C})$ ma wektor własny. Jeśli nie rozwiązałeś któregoś z poprzednich zadań, po prostu pokaż jak postawione w nich tezy implikują poprawność tezy. W jaki sposób dostajemy stąd prawdziwość ZTA?

¹Założenie nie działa przy żadnym $m > 1$ dla $K = \mathbb{Q}$, ale działa dla $m = 2$ przy $K = \mathbb{R}$.

Rozdział 21

Przestrzenie dwuliniowe i ich bazy prostopadłe

Od kilku wykładów zajmujemy się badaniem przestrzeni liniowych V wyposażonych w dodatkową strukturę pochodzącą od pewnych funkcji na przestrzeni $V \times V$ (dotychczas nad \mathbb{R} i \mathbb{C}). Celem geometrycznym jest zrozumienie naturalnych obiektów związanych z prostopadłością. Z algebraicznego punktu widzenia interesujące było rozważanie przekształceń liniowych zachowujących dodatkową strukturę i sposobów ich klasyfikowania m.in. za pomocą macierzy ortogonalnych. Celem obecnych rozważań jest omówienie tych zagadnień w ogólnym kontekście, nie ograniczając się do ciał liczb rzeczywistych i zespolonych. Przypomnijmy kilka definicji i faktów, przedstawionych na wcześniejszych wykładach.

Definicja 21.1

Niech V będzie przestrzenią liniową nad ciałem K . Funkcję: $h : V \times V \rightarrow K$ nazywamy FORMĄ DWULINIOWĄ (albo FUNKCJONALEM DWULINIOWYM) na przestrzeni V , jeśli dla każdego $\alpha, \beta, \gamma, \delta \in V$ i $a, b, c, d \in K$ zachodzi:

- (1) $h(a\alpha + b\beta, \gamma) = a \cdot h(\alpha, \gamma) + b \cdot h(\beta, \gamma)$ liniowość względem pierwszej zmiennej,
- (2) $h(\alpha, c\gamma + d\delta) = c \cdot h(\alpha, \gamma) + d \cdot h(\alpha, \delta)$ liniowość względem drugiej zmiennej,

Jeśli h jest formą dwuliniową na V oraz $W \subseteq V$ jest podprzestrzenią, to formę $h' : W \times W \rightarrow K$ określoną dla każdego $u, w \in W$ wzorem $h'(u, w) = h(u, w)$ nazywamy OGRANICZENIEM FORMY h do W i oznaczamy $h|_W$.

Każda forma dwuliniowa $h : K^n \times K^n \rightarrow K$ na przestrzeni K^n zadana jest wzorem:

$$h((x_1, \dots, x_n), (y_1, \dots, y_n)) = h(x_1\epsilon_1 + \dots + x_n\epsilon_n, y_1\epsilon_1 + \dots + y_n\epsilon_n) = \sum_{i,j} x_i y_j h(\epsilon_i, \epsilon_j),$$

gdzie $(\epsilon_1, \dots, \epsilon_n)$ jest bazą standardową K^n . Podobnie można wykazać, że jeśli $(\alpha_1, \dots, \alpha_n)$ jest bazą przestrzeni V , to wszystkie formy dwuliniowe na V opisane są wzorami:

$$h((x_1\alpha_1 + \dots + x_n\alpha_n), (y_1\alpha_1 + \dots + y_n\alpha_n)) = \sum_{i,j} x_i y_j h(\alpha_i, \alpha_j).$$

Niech $h : V \times V \rightarrow K$ będzie formą dwuliniową na przestrzeni V i niech $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$ będzie bazą przestrzeni V . MACIERZĄ FORMY h W BAZIE \mathcal{A} nazywamy macierz $G(h; \mathcal{A}) = [h(\alpha_i, \alpha_j)] \in M_n(K)$.

Przypominamy, że jeśli $h : V \times V \rightarrow K$ jest formą dwuliniową, $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$ jest bazą przestrzeni V oraz $A = G(h; \mathcal{A})$, to dla dowolnych wektorów $\alpha = x_1\alpha_1 + \dots + x_n\alpha_n, \beta = y_1\alpha_1 + \dots + y_n\alpha_n$ przestrzeni V zachodzi:

$$h(\alpha, \beta) = \begin{bmatrix} x_1 & \dots & x_n \end{bmatrix} \cdot A \cdot \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}.$$

Ważnym wątkiem naszych rozważań będzie badanie macierzy form dwuliniowych w różnych bazach.

Definicja 21.2

Mówimy, że macierze $A, B \in M_n(K)$ są KONGRUENTNE NAD K jeśli istnieje macierz odwracalna $C \in M_n(K)$ taka, że

$$B = C^T A C.$$

Kluczowa motywacja, pokazana już wcześniej jest następująca: macierze $A, B \in M_n(K)$ są **kongruentne wtedy i tylko wtedy, gdy są macierzami tej samej formy dwuliniowej** (w pewnych bazach).

Podstawową metodą sprawdzania czy macierze są kongruentne jest próba znalezienia kongruentnej do nich macierzy diagonalnej. Kiedy macierz formy dwuliniowej jest diagonalna? Czy zawsze musi być diagonalna? Na te pytania odpowiada teoria przestrzeni dwuliniowych, stanowiących uogólnienie przestrzeni euklidesowych, pozostając jednak w obrębie teorii form symetrycznych.

Definicja 21.3: Symetryczna forma dwuliniowa

Mówimy, że forma dwuliniowa h na przestrzeni V jest SYMETRYCZNA, jeśli dla każdego wektorów $\alpha, \beta \in V$ mamy $h(\alpha, \beta) = h(\beta, \alpha)$.

Obserwacja 21.1

Relacja kongruencji nad ciałem K jest relacją równoważności w zbiorze macierzy symetrycznych rozmiaru n . W szczególności macierz symetryczna nie może być kongruentna do macierzy niesymetrycznej.

Dowód. Jeśli $A = A^T$ oraz $B = C^T A C$, dla pewnej macierzy A , to oczywiście

$$B^T = (C^T A C)^T = C^T A^T C = C^T A C = B.$$

□

Definicja 21.4: Przestrzeń dwuliniowa

Parę (V, h) , gdzie V jest skończenie wymiarową przestrzenią liniową nad ciałem K , zaś odwzorowanie $h : V \times V \rightarrow K$ jest formą dwuliniową symetryczną nazywamy PRZESTRZENIĄ DWULINIOWĄ.

Każda przestrzeń euklidesowa jest przestrzenią dwuliniową. Jeśli weźmiemy podprzestrzeń W przestrzeni dwuliniowej (V, h) nad K , wówczas obcięcie $h|_W : W \times W \rightarrow K$ formy h do W zadaje na W strukturę przestrzeni dwuliniowej $(W, h|_W)$. W przeciwieństwie jednak do przypadku euklidesowego, podprzestrzenie przestrzeni dwuliniowej mogą – jako przestrzenie dwuliniowe z „odziedziczoną formą” – mieć zupełnie inne własności niż wyjściowa przestrzeń. Problemowi temu przyjrzymy się w dalszej części wykładu.

Definicja 21.5: Wektory prostopadłe

Niech (V, h) będzie przestrzenią dwuliniową.

- Mówimy, że wektory α, β są PROSTOPADŁE, jeśli $h(\alpha, \beta) = 0$, ozn. $\alpha \perp \beta$. Jeśli X, Y są podzbiorami V i $\alpha \perp \beta$, dla każdego $\alpha \in X, \beta \in Y$, to piszemy $X \perp Y$. Zbiór wszystkich wektorów prostopadłych do zbioru $X \subseteq V$ oznaczamy X^\perp .
- Układ $\alpha_1, \dots, \alpha_k$ wektorów (V, h) nazywamy PROSTOPADŁYM (ORTOGONALNYM), jeśli $\alpha_i \perp \alpha_j$ (czyli $h(\alpha_i, \alpha_j) = 0$), dla każdego $i \neq j$.
- Bazę przestrzeni dwuliniowej (V, h) nazywamy PROSTOPADŁĄ (ORTOGONALNĄ), jeśli jest ona układem prostopadłym.

Problem znajdowania diagonalnej macierzy formy dwuliniowej jest zatem w istocie problemem istnienia i znajdowania bazy prostopadłej przestrzeni dwuliniowej. Owa macierz diagonalna nie zawsze będzie miała jedynki na przekątnej. Nie będzie też koniecznie odwracalna, jak dowolna macierz Grama układu liniowo niezależnego w przestrzeni euklidesowej.

Definicja 21.6

Niech (V, h) będzie przestrzenią dwuliniową. Mówimy, że wektory α, β są PROSTOPADŁE, jeśli $h(\alpha, \beta) = 0$, ozn. $\alpha \perp \beta$. Wektor $\alpha \in V$ nazywamy IZOTROPOWYM, jeśli $h(\alpha, \alpha) = 0$, tzn. $\alpha \perp \alpha$.

Przykład. Dla formy $h : \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}$ zadanej wzorem

$$h((x_1, x_2), (y_1, y_2)) = x_1 y_2 + x_2 y_1$$

mamy $\text{lin}(1, 0)^\perp = \text{lin}(1, 0)$ oraz $\text{lin}(0, 1)^\perp = \text{lin}(0, 1)$, a zatem wektory $(1, 0), (0, 1)$ nie tylko nie są prostopadłe, ale nie uda nam się, korzystając z żadnej „dwuliniowej ortogonalizacji” typu Grama-Schmidta¹, otrzymać bazy prostopadłej z tego układu. To rodzi następujące pytanie: czy w przestrzeni (\mathbb{R}^2, h) istnieje baza ortogonalna? Okazuje się, że tak, wystarczy obrócić układ $((1, 1), (1, -1))$. Pierwszy układ zawierał wektory izotropowe, drugi ich nie zawiera. Czy zawsze można wybrać bazę z wektorów nieizotropowych?

Przykład. W $(\mathbb{Z}_2)^2$ z formą $h : \mathbb{Z}_2 \times \mathbb{Z}_2 \rightarrow \mathbb{Z}_2$ daną wzorem:

$$h((x_1, x_2), (y_1, y_2)) = x_1 y_2 + x_2 y_1$$

nie ma bazy prostopadłej. Istotnie, gdyby α_1, α_2 było taką bazą, to $h(\alpha_1, \alpha_2) = h(\alpha_2, \alpha_1) = 0$. Co więcej, mielibyśmy także

$$h(\alpha_1, \alpha_1) = h(\alpha_2, \alpha_2) = 0,$$

bo każdy wektor w $((\mathbb{Z}_2)^2, h)$ jest izotropowy. To oznacza, że gdyby $\mathcal{A} = (\alpha_1, \alpha_2)$ było bazą, to macierz $G(h; \mathcal{A})$ byłaby zerowa. To by z kolei oznaczało, że h wykonane na dowolnej parze wektorów (v, w) jest zerowe (bo wykonanie h to przemnożenie $G(h; \mathcal{A})$ z obydwu stron przez wektory współrzędnych v, w w bazie \mathcal{A}). Mamy natomiast

$$h((1, 0), (0, 1)) = 1 \neq 0.$$

Sprzeczność.

Definicja 21.7: Przestrzeń i forma nieosobliwa

Niech (V, h) będzie przestrzenią dwuliniową.

- Mówimy, że przestrzeń dwuliniowa (V, h) jest NIEOSOBLIWA, jeśli dla każdej bazy \mathcal{A} przestrzeni V macierz $G(h, \mathcal{A})$ jest odwracalna. Będziemy wtedy mówić krótko, że h jest FORMĄ NIEOSOBLIwą oraz, że V jest nieosobliwa. Jeśli macierz $G(h, \mathcal{A})$ nie jest odwracalna, to mówimy, że przestrzeń dwuliniowa (V, h) (krócej: forma h /przestrzeń V) jest OSOBLIWA.
- Jeśli $h(v, w) = 0$, dla każdych $v, w \in V$, to mówimy, że forma h (przestrzeń V) jest CAŁKOWICIE ZDEGENEROWANA.

Przykłady:

- Weźmy formę dwuliniową na \mathbb{R}^4 zadaną macierzą:

$$G(h; st) = \begin{bmatrix} 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}.$$

Wówczas przestrzeń dwuliniowa (V, h) jest nieosobliwa, ale na podprzestrzeni $W = \text{lin}(\epsilon_1, \epsilon_2, \epsilon_3)$ forma $h|_W$ jest osobliwa. Podprzestrzeń $Z = \text{lin}(\epsilon_1, \epsilon_2)$ jest natomiast całkowicie zdegenerowana względem h .

¹Same wzory mają sens, bo w każdym ciele K dopuszczalny jest iloraz typu $h(\beta, \alpha)/h(\alpha, \alpha)$, gdzie α – nieizotropowy.

- Niech h będzie formą dwuliniową na przestrzeni liniowej $M_{2 \times 2}(\mathbb{R})$ zadaną wzorem $h(A, B) = 2 \cdot \text{tr}(AB) - \text{tr}(A) \cdot \text{tr}(B)$, dla każdych $A, B \in M_{2 \times 2}(\mathbb{R})$. Wówczas forma h jest osobliwa. Istnieje też podprzestrzeń $W \subset M_{2 \times 2}(\mathbb{R})$ wymiaru 3 taka, że forma $h|_{W \times W}$ jest nieosobliwa.

Rzeczywiście, biorąc macierz identycznościową $I \in M_{2 \times 2}(K)$ i dowolną macierz $X \in M_{2 \times 2}(K)$ mamy

$$h(I, X) = 2 \cdot \text{tr}(I \cdot X) - \text{tr}(I) \cdot \text{tr}(X) = 2 \cdot \text{tr}(X) - 2 \cdot \text{tr}(X) = 0.$$

A zatem na mocy uwagi z wykładu forma h jest osobliwa. Można to również zobaczyć wyznaczając macierz formy h w bazie $\mathcal{E} = (e_{11}, e_{12}, e_{21}, e_{22})$ przestrzeni $M_{2 \times 2}(K)$, przy czym:

$$e_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad e_{12} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad e_{21} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \quad e_{22} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

Nietrudno sprawdzić, że macierz ta ma postać

$$G(h; \mathcal{E}) = \begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 2 & 0 \\ 0 & 2 & 0 & 0 \\ -1 & 0 & 0 & 1 \end{bmatrix}.$$

Nie jest ona odwracalna (czyli h jest osobliwa), bo pierwszy wiersz jest przeciwny czwartemu. Widać też, że **macierz formy h ograniczonej do podprzestrzeni $W = \text{lin}((e_{11}, e_{12}, e_{21}))$** jest nieosobliwa.

Obserwacja 21.2

Niech (V, h) będzie przestrzenią dwuliniową. Następujące warunki są równoważne:

- (V, h) jest nieosobliwa,
- dla każdego niezerowego wektora $\alpha \in V$ istnieje wektor $\beta \in V$ taki, że $h(\alpha, \beta) \neq 0$.

Dowód. Załóżmy, że (V, h) jest nieosobliwa oraz, że dla pewnego niezerowego $\alpha \in V$ mamy $h(\alpha, \beta) = 0$, dla wszystkich $\beta \in V$. Wektor α dopełniamy do bazy \mathcal{A} przestrzeni V postaci $(\alpha, \beta_1, \dots, \beta_s)$. Wówczas $G(h, \mathcal{A})$ ma zerowy pierwszy wiersz i kolumnę, bo $h(\alpha, \alpha) = 0$ oraz $h(\alpha, \beta_i) = h(\beta_i, \alpha) = 0$, dla $i = 1, \dots, s$. A zatem $G(h, \mathcal{A})$ jest osobliwa, sprzeczność.

Na odwrót: załóżmy, że zachodzi (ii), ale dla pewnej bazy $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$ macierz $G(h; \mathcal{A})$ jest osobliwa. Oznacza to, że rząd tej macierzy nie jest maksymalny. A zatem kolumny tej macierzy są liniowo zależne, czyli istnieje wektor niezerowy $(x_1, \dots, x_n) \in K^n$ taki, że:

$$x_1 \begin{bmatrix} h(\alpha_1, \alpha_1) \\ \vdots \\ h(\alpha_1, \alpha_n) \end{bmatrix} + x_2 \begin{bmatrix} h(\alpha_2, \alpha_1) \\ \vdots \\ h(\alpha_2, \alpha_n) \end{bmatrix} + \dots + x_n \begin{bmatrix} h(\alpha_n, \alpha_1) \\ \vdots \\ h(\alpha_n, \alpha_n) \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Korzystając z liniowości formy dwuliniowej względem pierwszej zmiennej mamy zatem:

$$\begin{bmatrix} h(x_1\alpha_1 + x_2\alpha_2 + \dots + x_n\alpha_n, \alpha_1) \\ \vdots \\ h(x_1\alpha_1 + x_2\alpha_2 + \dots + x_n\alpha_n, \alpha_n) \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Niech $\alpha = x_1\alpha_1 + x_2\alpha_2 + \dots + x_n\alpha_n$. Zauważmy, że skoro $h(\alpha, \alpha_i) = 0$, dla każdego $i = 1, \dots, n$, to $h(\alpha, \beta) = 0$, dla każdego $\beta \in V$ (bo każde β jest sumą α_i). Skoro w (V, h) zachodzi (ii), to $\alpha = 0$. Ale α to kombinacja wektorów bazowych przestrzeni (V, h) o współczynnikach x_1, \dots, x_n . A zatem $x_1 = \dots = x_n = 0$, co przeczy wyborowi elementów x_i jako współczynników liniowej zależności kolumn $G(h; \mathcal{A})$. \square

Definicja 21.8

Niech (V, h) będzie przestrzenią dwuliniową. RZĘDEM PRZESTRZENI (V, h) (albo formy dwuliniowej h) nazywamy rząd macierzy $G(h; \mathcal{A})$ dla dowolnej bazy \mathcal{A} , oznaczany $r(V, h)$ lub $r(h)$.

Kilka ważnych wniosków

- Każda przestrzeń euklidesowa jest nieosobliwa.
- Przestrzeń (V, h) jest osobliwa wtedy i tylko wtedy, gdy istnieje niezerowy wektor $\alpha \in V$ taki, że $h(\alpha, \beta) = 0$, dla każdego $\beta \in V$.
- Przestrzeń dwuliniowa (V, h) jest nieosobliwa wtedy i tylko wtedy, gdy $r(V, h) = \dim V$.

Twierdzenie 21.1

Niech (V, h) będzie przestrzenią dwuliniową nad ciałem K i niech W będzie podprzestrzenią przestrzeni V . Następujące warunki są równoważne:

- (1) $V = W \oplus W^\perp$,
- (2) W jest nieosobliwa.

Dowód. Załóżmy, że $V = W \oplus W^\perp$. Mamy zatem $W \cap W^\perp = \{0\}$. Gdyby W była osobliwa to, na mocy Obserwacji 21.2, istniałby wektor $\alpha \in W$ taki, że dla każdego $\beta \in W$ mielibyśmy $h(\alpha, \beta) = 0$. W szczególności $h(\alpha, \alpha) = 0$, czyli $\alpha \in W^\perp$. A zatem $\alpha \in W \cap W^\perp$, sprzeczność.

Na odwrót: przypuśćmy, że przestrzeń W jest nieosobliwa. Mamy wykazać, że $V = W \oplus W^\perp$, czyli że dla każdego $\alpha \in V$ istnieją jednoznacznie wyznaczone wektory $\alpha' \in W$ oraz $\alpha'' \in W^\perp$ takie, że $\alpha = \alpha' + \alpha''$. Niech $\mathcal{A} = (\alpha_1, \dots, \alpha_k)$ będzie bazą przestrzeni W . Istnienie i jednoznaczność wektora $\alpha' = x_1\alpha_1 + \dots + x_k\alpha_k$ spełniającego powyższe warunki jest równoważne istnieniu i jednoznaczności współczynników $x_1, \dots, x_k \in K$ takich, że

$$\alpha - (x_1\alpha_1 + \dots + x_k\alpha_k) \in W^\perp.$$

Sprawdzenie czy jakiś wektor leży w W^\perp jest równoważne sprawdzeniu, czy wektor ten jest prostopadły do każdego wektora z bazy W (na mocy dwuliniowości h). A zatem teza (czyli (1)) jest równoważna temu, że zachodzi układ warunków

$$h(\alpha_j, \alpha - (x_1\alpha_1 + \dots + x_k\alpha_k)) = 0, \text{ dla każdego } j = 1, \dots, k,$$

czyli (1) równoważne jest, z liniowości h , istnieniu jednoznacznego rozwiązania (x_1, \dots, x_k) układu równań

$$\begin{cases} x_1h(\alpha_1, \alpha_1) + x_2h(\alpha_1, \alpha_2) + \dots + x_kh(\alpha_1, \alpha_k) &= h(\alpha_1, \alpha) \\ x_1h(\alpha_2, \alpha_1) + x_2h(\alpha_2, \alpha_2) + \dots + x_kh(\alpha_2, \alpha_k) &= h(\alpha_2, \alpha) \\ &\vdots \\ x_1h(\alpha_k, \alpha_1) + x_2h(\alpha_k, \alpha_2) + \dots + x_kh(\alpha_k, \alpha_k) &= h(\alpha_k, \alpha) \end{cases}$$

Macierzą współczynników tego (być może niejednorodnego) układu jest macierz $G(h|_W, \mathcal{A})$. Skoro W jest nieosobliwa, to macierz ta jest odwracalna, a zatem jej rząd wynosi k . Także rząd macierzy całego układu (rozmiarów $k \times k + 1$) wynosi k , a zatem na mocy Twierdzenia Kroneckera-Capelliego układ ten ma dokładnie jedno rozwiązanie. To kończy dowód istnienia i jednoznaczności wektora α' , więc i α'' . \square

Układ ortogonalny złożony z dwóch egzemplarzy wektora izotropowego nie jest liniowo niezależny. Okazuje się, że jest to w zasadzie jedyna przeszkoda do tego, aby układy ortogonalne były liniowo niezależne.

Obserwacja 21.3

Każdy układ prostopadły złożony z wektorów nieizotropowych jest liniowo niezależny.

Dowód. Niech $\alpha_1, \dots, \alpha_k$ będzie układem prostopadłym złożonym z wektorów nieizotropowych. Przypuśćmy, że dla pewnych $a_1, \dots, a_k \in K$ mamy: $a_1\alpha_1 + a_2\alpha_2 + \dots + a_k\alpha_k = 0$. Oczywiście dla każdej formy dwuliniowej na V oraz wektora $v \in V$ mamy $h(0, v) = h(v, 0) = 0$, bo $h(0, v) = 0 \cdot h(v, v) = 0$. A zatem dla każdego $j = 1, \dots, k$ mamy:

$$\begin{aligned} 0 &= h(0, \alpha_j) = h(a_1\alpha_1 + a_2\alpha_2 + \dots + a_k\alpha_k, \alpha_j) \\ &= a_1h(\alpha_1, \alpha_j) + \dots + a_jh(\alpha_j, \alpha_j) + \dots + a_kh(\alpha_k, \alpha_j) \\ &= a_jh(\alpha_j, \alpha_j), \end{aligned}$$

bo $h(\alpha_i, \alpha_j) = 0$, dla $i \neq j$. Układ nasz składa się z wektorów nieizotropowych, czyli $h(\alpha_j, \alpha_j) \neq 0$, dla $j = 1, \dots, k$. Z równości $0 = a_jh(\alpha_j, \alpha_j)$ dostajemy zatem $a_j = 0$, dla $j = 1, \dots, k$, czyli liniową niezależność układu $\alpha_1, \dots, \alpha_k$. \square

Poprzednia uwaga mówi, że jeśli rozpinający przestrzeń dwuliniową (V, h) układ prostopadły złożony jest z wektorów nieizotropowych, to układ ten jest bazą V . Jest również jasne, że prostopadłość bazy przestrzeni dwuliniowej (V, h) można wyrazić przez macierz $G(h; \mathcal{A})$ formy h w tej bazie. Mianowicie: baza \mathcal{A} jest prostopadła wtedy i tylko wtedy, gdy macierz $G(h; \mathcal{A})$ jest diagonalna.

Twierdzenie 21.2

Niech (V, h) będzie przestrzenią dwuliniową nad ciałem charakterystyki różnej od 2, to znaczy takim, że $1 + 1 \neq 0$. Wówczas (V, h) ma bazę prostopadłą.

Dowód. Stosujemy indukcję po V . Dla $\dim V = 1$ twierdzenie jest oczywiste. Załóżmy, że twierdzenie jest prawdziwe dla $\dim V = n - 1$. Dowodzimy dla $\dim V = n$.

- Przypadek 1. W przestrzeni V istnieje wektor nieizotropowy.
Niech $\alpha \in V$ będzie wektorem nieizotropowym. Rozpatrzmy przestrzeń $W = \text{lin}(\alpha)$. Skoro α jest nieizotropowy, to W jest przestrzenią nieosobliwą. Stąd $V = W \oplus W^\perp$, na mocy wcześniejszego twierdzenia. Zatem $\dim W^\perp = n - 1$. Z założenia indukcyjnego zatem W^\perp ma bazę prostopadłą. Oznaczmy ją przez $(\alpha_2, \dots, \alpha_n)$. Wówczas $(\alpha, \alpha_2, \dots, \alpha_n)$ jest bazą prostopadłą przestrzeni V .
- Przypadek 2. Wszystkie wektory przestrzeni V są izotropowe.
Dla każdych $\alpha, \beta \in V$ wektory $\alpha, \beta, \alpha + \beta$ są izotropowe, więc:

$$0 = h(\alpha + \beta, \alpha + \beta) = h(\alpha, \alpha) + 2h(\alpha, \beta) + h(\beta, \beta) = 2h(\alpha, \beta),$$

a stąd $h(\alpha, \beta) = 0$, bo $2 \neq 0$ w K (założenie o charakterystyce). Zatem wszystkie pary wektorów w przestrzeni V są prostopadłe, co oznacza, że każda baza V jest bazą prostopadłą. \square

Wniosek 21.1

Nad ciałem charakterystyki różnej od 2 każda macierz symetryczna jest kongruentna do macierzy diagonalnej (będącej macierzą odpowiedniej formy w bazie diagonalnej).

Wniosek 21.2

Nad ciałem charakterystyki różnej od 2 forma dwuliniowa symetryczna h na V wyznaczona jest jednoznacznie przez swoje wartości na parach (v, v) , dla $v \in V$.

Dowód powyższego twierdzenia daje nam także przepis na konstruowanie bazy prostopadłej dowolnej przestrzeni dwuliniowej (V, h) nad ciałem charakterystyki różnej od 2, zgodnie z poniższą procedurą.

- Szukaj w (V, h) wektora nieizotropowego. Jeśli nie ma takiego wektora, to wybierz dowolną bazę V i będzie ona prostopadła (por. Przypadek 2). Jeśli istnieje taki wektor α , to przejdź dalej.
- Podprzestrzeń $\text{lin}(\alpha)$ jest nieosobliwa, więc $V = \text{lin}(\alpha) \oplus \text{lin}(\alpha)^\perp$ (por. Przypadek 1). A zatem dla znalezienia kolejnych wektorów bazy V powtórz wcześniejszy krok dla przestrzeni $\text{lin}(\alpha)^\perp$.

Przykład. Znajdziemy bazę prostopadłą przestrzeni dwuliniowej (\mathbb{R}^3, h) , gdzie h jest zadana wzorem:

$$h((x_1, x_2, x_3), (y_1, y_2, y_3)) = x_1y_1 + x_1y_2 + x_2y_1 + 2x_2y_3 + 2x_3y_2 - 4x_3y_3.$$

Szukamy wektora nieizotropowego $\alpha_1 \in \mathbb{R}^3$. Możemy taki wektor zgadnąć, albo zapisać macierz $G(h; st)$ oraz $\alpha_1 = (x_1, x_2, x_3)$. Wówczas bycie wektorem nieizotropowym równoważne jest warunkowi:

$$[x_1 \quad x_2 \quad x_3] \cdot \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 2 \\ 0 & 2 & -4 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \neq 0.$$

Warunek ten spełnia na przykład $\alpha_1 = (1, 0, 0)$, bo $h(\alpha_1, \alpha_1) = 1$. Przechodzimy do kolejnego kroku. Opisujemy przestrzeń $\text{lin}(\alpha_1)^\perp$ i sprawdzamy czy w niej jest jakiś wektor nieizotropowy. Przestrzeń $\text{lin}(\alpha_1)^\perp$ składa się z wektorów $\beta = (y_1, y_2, y_3)$ spełniających równanie $h(\beta, \alpha_1) = 0$, więc:

$$\text{lin}(\alpha_1)^\perp = \{(y_1, y_2, y_3) \in \mathbb{R}^3 : y_1 + y_2 = 0\}.$$

W przestrzeni tej również istnieje wektor nieizotropowy, na przykład $\alpha_2 = (1, -1, 0)$, bo $h(\alpha_2, \alpha_2) = -1$. A zatem przechodzimy do kolejnego kroku. Układ (α_1, α_2) chcemy dopełnić do bazy prostopadłej \mathbb{R}^3 . Przestrzeń $\text{lin}(\alpha_1, \alpha_2)^\perp$ opisujemy przez układ warunków (prostopadłość do α_1 oraz do α_2):

$$\text{lin}(\alpha_1, \alpha_2)^\perp = \{(z_1, z_2, z_3) : z_1 + z_2 = 0, z_2 - 2z_3 = 0\} = \text{lin}((2, -2, -1)).$$

Wektor $(2, -2, -1)$ jest izotropowy, więc każdy wektor w $\text{lin}(\alpha_1, \alpha_2)^\perp$ jest izotropowy. A zatem dowolny układ liniowo niezależny z tej przestrzeni dopełnia (α_1, α_2) do bazy \mathbb{R}^3 . Tutaj potrzebowaliśmy tylko jednego wektora, ale teoretycznie już w poprzednim kroku mogliśmy trafić na przestrzeń mającą jedynie wektory izotropowe. A zatem bazą prostopadłą w (\mathbb{R}^3, h) jest układ $((1, 0, 0), (1, -1, 0), (2, -2, -1))$.

Powyższa procedura oparta była na dobieraniu do pojedynczego wektora nieizotropowego pewnego układu ortogonalnego. Nietrudno pokazać, że dowolny układ wektorów nieizotropowych przestrzeni dwuliniowej (V, h) można dopełnić do bazy ortogonalnej, o ile charakterystyka ciała bazowego nie jest równa 2.

Wniosek 21.3

Niech (V, h) będzie przestrzenią dwuliniową nad ciałem charakterystyki różnej od 2 wymiaru n . Niech $(\alpha_1, \dots, \alpha_k)$ będzie układem prostopadłym złożonym z wektorów nieizotropowych, gdzie $k < n$. Wówczas istnieją w przestrzeni V wektory $\alpha_{k+1}, \dots, \alpha_n$ takie, że układ $(\alpha_1, \dots, \alpha_n)$ jest bazą ortogonalną przestrzeni V .

Dowód. Rozważmy przestrzeń $W = \text{lin}(\alpha_1, \dots, \alpha_k)$. Układ prostopadły $\mathcal{A} = (\alpha_1, \dots, \alpha_k)$ złożony jest z wektorów nieizotropowych, a zatem jest to baza W . Macierz $G(h|_W, \mathcal{A})$ jest zatem diagonalna i na jej przekątnej stoją elementy niezerowe $h(\alpha_i, \alpha_i)$, dla $i = 1, \dots, k$. Zatem macierz ta ma niezerowy wyznacznik. W szczególności W jest nieosobliwa i mamy rozkład $V = W \oplus W^\perp$. Na mocy poprzedniego twierdzenia, istnieje baza ortogonalna W^\perp złożona z pewnych wektorów $\alpha_{k+1}, \dots, \alpha_n$. Układ $(\alpha_1, \dots, \alpha_n)$ jest zatem bazą ortogonalną V . \square

Na kolejnym wykładzie rozstrzygniemy problem kongruencji macierzy diagonalnych nad \mathbb{R} i \mathbb{C} , co pozwoli na pełen opis macierzy symetrycznych (nad tymi ciałami) z dokładnością do kongruencji. Postawowym rezultatem będzie twierdzenie Sylwestera o bezwładności.

21.1 Uzupełnienie. Formy i macierze antysymetryczne

W tym dodatku opowiemy o drugiej obok form symetrycznych niezwykle ważnej klasie form dwuliniowych.

Definicja 21.9: Forma dwuliniowa antysymetryczna

Formę dwuliniową h na przestrzeni liniowej V nazywamy **ANTYSYMETRYCZNĄ** (albo skośnie symetryczną), jeśli dla każdego $\alpha, \beta \in V$ mamy $h(\alpha, \beta) = -h(\beta, \alpha)$. Powiemy, że macierz $A \in M_n(K)$ jest antysymetryczna, jeśli $A^T = -A$.

Formy antysymetryczne mają duże znaczenie chociażby w związku z pojęciem wyznacznika, bowiem forma

$$h((x_1, x_2), (y_1, y_2)) = x_1 y_2 - x_2 y_1$$

odpowiada wyznacznikowi jako formie antysymetrycznej na przestrzeni wierszy lub kolumn macierzy 2×2 . Oczywiście dla ciała charakterystyki 2 formy symetryczne i antysymetryczne są tożsame. Ważną obserwacją jest natomiast stwierdzenie, że zarówno zbiór form dwuliniowych symetrycznych na V , jak i zbiór form dwuliniowych antysymetrycznych są przestrzeniami liniowymi.

Jeśli $\dim V < \infty$ i (V, h) jest formą dwuliniową (anty)symetryczną, to macierz tej formy jest w każdej bazie (anty)symetryczna. Innymi słowy, każda macierz (anty)symetryczna kongruentna do macierzy formy h jest macierzą tej formy.

Relacja kongruencji macierzy jest relacją równoważności na zbiorze macierzy symetrycznych, a także na zbiorze macierzy antysymetrycznych. Problem badania kongruencji w zbiorze macierzy niesymetrycznych jest bardzo trudny, choć można znaleźć sporo wyników cząstkowych, w tym współczesnych. Jedną z możliwych prób badania klas kongruencji macierzy niesymetrycznej A nad ciałem charakterystyki różnej od 2 jest badanie rozkładu:

$$A = \underbrace{\frac{1}{2}(A + A^T)}_{A^{sym}} + \underbrace{\frac{1}{2}(A - A^T)}_{A^{antysym}}$$

i próba znalezienia wspólnej macierzy odwracalnej $P \in M_n(K)$ takiej, że macierze $P^T A^{sym} P$, $P^T A^{antysym} P$ będą diagonalne. To jest zwykle trudne.

Drugi aspekt, nie uciekając się do szczegółowych rozważań, dotyczy form i macierzy nad ciałem charakterystyki 2? Wychodząc z twierdzenia z ostatniego wykładu, można uzasadnić dwa rezultaty.

Twierdzenie 21.3

Jeśli (V, h) jest przestrzenią dwuliniową taką, że forma h nie jest alternująca (tzn. $h(v, v) = 0$, dla każdego $v \in V$), wówczas w V jest baza ortogonalna. W konsekwencji dla każdej macierzy symetrycznej $A = [a_{ij}] \in M_n(K)$ o elementach z ciała K charakterystyki 2 takiej, że $a_{ii} \neq 0$ dla co najmniej jednego i , istnieje taka macierz odwracalna $P \in M_n(K)$, że $P^T A P$ jest diagonalna.

Twierdzenie 21.4

Każda macierz antysymetryczna odwracalna i mająca zera na przekątnej jest kongruentna z macierzą blokowo-diagonalną o blokach postaci:

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

Zachęcam Czytelnika do wykazania dwóch własności macierzy antysymetrycznych rzeczywistych:

- wyznacznik rzeczywistej macierzy antysymetrycznej jest nieujemny,
- rząd rzeczywistej macierzy antysymetrycznej jest parzysty.

21.2 Dodatek. Podprzestrzenie całkowicie zdegenerowane

Zrozumienie w jaki sposób umieszczone są w przestrzeni dwuliniowej przestrzenie, na których forma ta się zeruje jest niezwykle istotnym elementem teorii przestrzeni dwuliniowych. Zaczniemy od przykładów pokazujących, że problemy dotyczące tych zagadnień nie są trywialne.

Zadanie 21.1. *Forma dwuliniowa h zadana jest na przestrzeni $V = \mathbb{R}^3$ przy pomocy macierzy*

$$G(h, st) = \begin{bmatrix} 0 & 2 & 1 \\ 2 & 4 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

- Wyznacz bazę prostopadłą przestrzeni (V, h) . Czy (V, h) ma bazę złożoną z wektorów izotropowych?
- Pokaż, że są dokładnie dwie podprzestrzenie całkowicie zdegenerowane wymiaru 2 w (V, h) .

ROZWIĄZANIE. Szukamy wektora nieizotropowego w V . Dostrzegamy go od razu widząc, że na przekątnej $G(h, st)$ jest wartość 4 = $h(\epsilon_2, \epsilon_2)$. Niech więc pierwszy wektor szukanej bazy prostopadłej to $v_1 = (0, 1, 0)$. Zbiór wektorów prostopadłych do v_1 postaci $x_1\epsilon_1 + x_2\epsilon_2 + x_3\epsilon_3$, gdzie $st = (\epsilon_1, \epsilon_2, \epsilon_3)$, opisany jest warunkiem:

$$\begin{bmatrix} 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 2 & 1 \\ 2 & 4 & 1 \\ 1 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \Leftrightarrow 2x_1 + 4x_2 + x_3 = 0.$$

Zatem $\text{lin}(v_1)^\perp = \text{lin}((1, 0, -2), (0, 1, -4))$. Biorąc $v_2 = (1, 0, -2)$ mamy $h(v_2, v_2) = -4$ oraz $\text{lin}(v_1, v_2)^\perp$ opisana jest równaniami: $2x_1 + 4x_2 + x_3 = 0, -2x_1 + x_3 = 0$, więc $\text{lin}(v_1, v_2)^\perp = \text{lin}(1, -1, 2)$. Biorąc $v_3 = (1, -1, 2)$ dostajemy szukaną bazę prostopadłą $\mathcal{A} = (v_1, v_2, v_3)$, w której h ma macierz:

$$G(h, \mathcal{A}) = \begin{bmatrix} 4 & 0 & 0 \\ 0 & -4 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Przestrzeń V ma oczywiście bazę złożoną z wektorów izotropowych. Patrząc na powyższą postać diagonalną widać natychmiast, że biorąc układ: $\mathcal{B} = (v_1 - v_2, v_1 + v_2, v_3)$ mamy:

$$G(h, \mathcal{B}) = \begin{bmatrix} 0 & 8 & 0 \\ 8 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Z postaci macierzy $G(h, \mathcal{B})$ natychmiast odczytujemy dwie podprzestrzenie całkowicie zdegenerowane wymiaru 2, czyli

$$\text{lin}(v_1 + v_2, v_3), \quad \text{lin}(v_1 - v_2, v_3).$$

Trzeba pokazać, że nie ma innych przestrzeni całkowicie zdegenerowanych wymiaru 2. Mając bazę prostopadłą $\mathcal{A} = (v_1, v_2, v_3)$ widzimy, że wektor izotropowy postaci $av_1 + bv_2 + cv_3$ spełnia $a^2 = b^2$, czyli $a = b$ lub $a = -b$.

Rozważmy dowolną podprzestrzeń całkowicie zdegenerowaną U wymiaru 2. Twierdzimy, że $v_3 \in U$. Baza prostopadła tej przestrzeni złożona jest z pewnych wektorów

$$a'v_1 \pm a'v_2 + c'v_3 \quad \text{oraz} \quad a''v_1 \pm a''v_2 + c''v_3,$$

dla pewnych $a', a'' \neq 0$ oraz c', c'' . Odpowiednio skalując można zatem przyjąć, że $a' = a'' = 1$. Dodając, lub odejmując te wektory i ponownie skalując widzimy, że w istocie nasza przestrzeń całkowicie zdegenerowana ma postać:

$$U = \text{lin}(v_1 + v_2 + c'v_3, v_1 - v_2 + c''v_3),$$

gdzie $c' \neq c''$ (inaczej v_1 lub v_2 trafiają do U , a one nie są izotropowe). Zatem $(c' - c'')v_3 \in U$, czyli U zawiera v_3 . Stąd jednak jest jasne, że $v_1 + v_2 \in U$ lub $v_1 - v_2 \in U$. A zatem, zgodnie z oczekiwaniami, możliwe są tylko dwie dwuwymiarowe całkowicie zdegenerowane (podane wyżej). ■

Zadanie 21.2. *Niech V będzie przestrzenią liniową wymiaru n nad K , zaś V^* przestrzenią sprzężoną do V . Na przestrzeni liniowej $W = \{(v, f), v \in V, f \in V^*\}$ rozważamy symetryczną formę dwuliniową $h : W \times W \rightarrow K$ postaci*

$$h((v, f), (w, g)) = f(w) + g(v).$$

Wykazać, że forma h jest nieosobliwa oraz, że W można przedstawić w postaci sumy prostej dwóch podprzestrzeni całkowicie zdegenerowanych.

ROZWIĄZANIE. Aby pokazać, że forma jest nieosobliwa wystarczy pokazać, że dla każdej niezerowej pary $(v, f) \in W$ istnieje element $(v', f') \in W$, że $h((v, f), (v', f')) \neq 0$. Rozważamy dwa przypadki:

- Jeśli $v \neq 0$, to v można dopełnić do bazy \mathcal{A} przestrzeni V i wziąć element v^* z bazy dualnej V^* , spełniający $v^*(v) = 1$. Weźmy więc $(0, v^*) \in W$. Mamy $h((v, f), (0, v^*)) = f(0) + v^*(v) = 0 + 1 = 1$.
- Jeśli $f \neq 0$, to istnieje niezerowy wektor $w \in V$ taki, że $f(w) \neq 0$. Weźmy $(w, 0) \in W$ (na drugiej współrzędnej jest przekształcenie zerowe). Wówczas $h((v, f), (w, 0)) = f(w) + 0(v) = f(w) \neq 0$.

A zatem forma h jest nieosobliwa. Można to również zobaczyć rozważając macierz tej formy w bazie W złożonej z elementów postaci $(\alpha_i, 0)$ oraz $(0, \alpha_i^*)$, dla $i = 1, \dots, n$, gdzie $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$ jest dowolną bazą V , zaś $\mathcal{A}^* = (\alpha_1^*, \dots, \alpha_n^*)$ jest bazą dualną do \mathcal{A} . Szukane podprzestrzenie całkowicie zdegenerowane to chociażby podprzestrzenie postaci $V_1 = \{(v, 0), v \in V\}$ oraz $V_2 = \{(0, f), f \in V^*\}$. ■

W naszych rozważaniach rozpoczniemy od następującego bardzo ważnego lematu.

Obserwacja 21.4: Lemat o wymiarze dopełnienia ortogonalnego

Jeśli przestrzeń dwuliniowa (V, h) jest nieosobliwa, $\dim V = n$, to dla każdej podprzestrzeni $U \subseteq V$

$$\dim U + \dim U^\perp = n.$$

W szczególności wymiar całkowicie zdegenerowanej podprzestrzeni w V jest nie większy niż $\lfloor n/2 \rfloor$.

Dowód. Niech $\dim U = k$ i niech $\alpha_1, \dots, \alpha_k$ będzie bazą przestrzeni U . Element $\alpha \in V$ należy do U^\perp wtedy i tylko wtedy, gdy jest prostopadły do każdego z wektorów α_i . Niech \mathcal{A} będzie bazą V zawierającą układ $\alpha_1, \dots, \alpha_k$. Wówczas jeśli $B = M(h; \mathcal{A})$ oraz wektor $\alpha \in U^\perp$ wtedy i tylko wtedy, gdy:

$$\alpha_1 \cdot B \cdot \alpha^T = 0, \quad \dots, \quad \alpha_k \cdot B \cdot \alpha^T = 0.$$

Oczywiście w powyższych iloczynach bierzemy współrzędne wektorów α_i oraz α w bazie \mathcal{A}). A zatem $\alpha \in U^\perp$ wtedy i tylko wtedy, gdy jest rozwiązaniem jednorodnego układu k równań, którego macierz ma rząd równy dokładnie k , ponieważ macierz U jest odwracalna (wektory $\alpha_i \cdot B$ muszą tworzyć układ liniowo niezależny). A zatem z twierdzenia Kroneckera-Capellego $\dim U^\perp = n - k$. □

Twierdzenie 21.5: Maksymalne podprzestrzenie całkowicie zdegenerowane

Wszystkie maksymalne (ze względu na częściowy porządek inkluzji) podprzestrzenie całkowicie zdegenerowane nieosobliwej przestrzeni dwuliniowej (V, h) nad ciałem K są tego samego wymiaru, nie większego niż $(\dim V)/2$.

Dowód. Niech U_1, U_2 będą maksymalnymi całkowicie zdegenerowanymi podprzestrzeniami przestrzeni V i niech $W = U_1 \cap U_2$ oraz niech $W_1 \subseteq U_1, W_2 \subseteq U_2$ spełniają $W \oplus W_1 = U_1, W \oplus W_2 = U_2$. Pokażemy, że

$$W_2 \cap W_1^\perp = 0 \quad (\dagger).$$

Niech $v \in W_2 \cap W_1^\perp$. Skoro $v \in W_2 \subseteq U_2$, to skoro każdy wektor z U_2 jest prostopadły do wszystkiego w U_2 , to $v \in U_2^\perp \subseteq W^\perp$. Ale w W^\perp wszystkie wektory są prostopadłe do całego U_1 , więc $v \in U_1^\perp$. Skoro U_1 jest maksymalną podprzestrzenią całkowicie zdegenerowaną, to $U_1^\perp \setminus U_1$ nie może zawierać wektorów izotropowych. Stąd $v \in U_1$. Skoro $W_2 \subseteq U_2$, to $v \in U_1 \cap U_2 = W$, a skoro $W \cap W_2 = \{0\}$, to $v = 0$.

Skoro więc $W_2 \cap W_1^\perp = \{0\}$, to $\dim W_2 + \dim W_1^\perp \leq \dim V$. Zakładamy, że V jest nieosobliwa, więc z lematu wyżej mamy

$$\dim W_1 = \dim V - \dim W_1^\perp,$$

więc $\dim W_2 \leq \dim W_1$. Z symetrycznych powodów $\dim W_1 \leq \dim W_2$. Stąd $\dim W_1 = \dim W_2$, czyli $\dim U_1 = \dim U_2$. Oczywiście $\dim U_1 = \dim U_2 \leq (\dim V)/2$, bo V jest nieosobliwa i stosujemy ponownie lemat, pamiętając, że $U_1 \subseteq U_1^\perp, U_2 \subseteq U_2^\perp$. □

Szacowanie wymiaru maksymalnej podprzestrzeni całkowicie zdegenerowanej przez $(\dim V)/2$ jest naturalne i ma ważne interpretacje, choćby kombinatoryczne. Opierając się na (nieosobliwej) formie dwuliniowej na \mathbb{Z}_2^n postaci:

$$h((x_1, \dots, x_n), (y_1, \dots, y_n)) = x_1 y_1 + \dots + x_n y_n,$$

można pokazać następujące fakty kombinatoryczne².

Zadanie 21.3. *Miasteczko Parzystów liczy sobie n mieszkańców. W mieście tym jest m klubów, przy czym każdy klub ma parzystą liczbę członków i każde dwa kluby muszą mieć parzystą liczbę wspólnych członków. Żadne dwa kluby nie mają identycznej listy członków. Pokaż, że $m \leq 2^{\lfloor n/2 \rfloor}$.*

Zadanie 21.4. *Pokaż, że jeśli w Parzystowie jest mniej niż $2^{\lfloor n/2 \rfloor}$ klubów (przy n mieszkańcach), to znajdzie się miejsce na co najmniej jeden dodatkowy klub.*

Podajmy również zastosowanie pokazanego twierdzenia w kontekście przestrzeni macierzy.

Zadanie 21.5. *Załóżmy, że W jest taką podprzestrzenią $M_n(K)$, że $\text{tr}(AB) = 0$, dla wszystkich $A, B \in W$. Znajdź maksymalny możliwy wymiar W .*

ROZWIĄZANIE. Funkcja $h : M_n(K) \times M_n(K) \rightarrow K$ zadana wzorem

$$h(A, B) = \text{tr}(AB)$$

jest formą dwuliniową symetryczną. Problem sprowadza się zatem do zagadnienia znalezienia maksymalnej podprzestrzeni całkowicie zdegenerowanej względem tej formy. Twierdzenie wyżej mówi, że wszystkie maksymalne (ze względu na częściowy porządek inkluzji) podprzestrzenie całkowicie zdegenerowane nieosobliwej przestrzeni dwuliniowej (V, h) nad ciałem K są tego samego wymiaru, nie większego niż $\dim V/2$.

Nietrudno widzieć, że forma $\text{tr}(AB)$ jest niezdegenerowana na K – wystarczy bowiem wypisać macierz tej formy w bazie standardowej złożonej z jedynek macierzowych E_{ij} , gdzie E_{ij} to macierz mająca jedyny niezerowy wyraz równy 1 w i -tym wierszu i j -tej kolumnie macierzy A . Dla takich macierzy iloczyn $E_{ij} \cdot E_{kl}$ ma niezerową przekątną tylko, gdy $j = k$ oraz $i = l$. W szczególności porządkując n^2 elementów tej bazy \mathcal{C} najpierw w $\frac{n(n-1)}{2}$ par E_{ij}, E_{ji} , a potem n elementów E_{ii} , czyli:

$$\mathcal{C} = \underbrace{(E_{12}, E_{21}, E_{13}, E_{31}, \dots, E_{n-1,n}, E_{n,n-1})}_{n(n-1)} \underbrace{(E_{11}, \dots, E_{nn})}_n$$

widzimy, że $\text{tr}(E_{ij}, E_{ji}) = 1$, $\text{tr}(E_{ii}, E_{ii}) = 1$, i macierz $G(h, \mathcal{C})$ jest blokowo diagonalna, a na jej przekątnej jest $\frac{n(n-1)}{2}$ bloków odwracalnych

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

oraz blok będący macierzą identyczościową rozmiaru n . Stąd forma $\text{tr}(AB)$ jest nieosobliwa.

Twierdzimy, że przykładem maksymalnej podprzestrzeni całkowicie zdegenerowanej $M_n(K)$ względem rozważanej formy jest podprzestrzeń W złożona z macierzy ściśle górnotrójkątnych rozmiaru n :

$$\begin{bmatrix} 0 & * & * & * & \dots & * \\ 0 & 0 & * & * & \dots & * \\ 0 & 0 & 0 & * & \dots & * \\ \vdots & \vdots & \vdots & \vdots & \ddots & * \\ 0 & 0 & 0 & 0 & \dots & 0 \end{bmatrix}$$

Podprzestrzeń ta ma oczywiście wymiar $n(n-1)/2$. Gdyby istniała podprzestrzeń całkowicie zdegenerowana $W' \neq W$ zawierająca W , to do W' należałaby jakaś macierz postaci E_{ij} , gdzie $i > j$ (dlaczego?). Jednak przemnożenie tej macierzy przez $E_{ji} \in W$ daje nam E_{ii} , czyli macierz o śladzie 1. A zatem W jest maksymalną podprzestrzenią całkowicie zdegenerowaną, czyli ma też maksymalny możliwy wymiar. ■

²Więcej zastosowań kombinatorycznych znaleźć można w: L. Babai, P. Frank.: *Linear algebra methods in combinatorics*, <https://people.cs.uchicago.edu/~laci/babai-frank1-book2022.pdf>.

Rozdział 22

Kongruentność macierzy rzeczywistych i zespolonych

Poprzedni wykład dotyczył znajdowania baz prostopadłych w przestrzeniach dwuliniowych. Kluczowy rezultat zapewnia istnienie takiej bazy dla każdej przestrzeni dwuliniowej nad ciałem charakterystyki różnej od 2. Wynik ten ma bardzo istotne skutki dla problemu znajdowania macierzy danej symetrycznej dwuliniowej formy h . Pamiętając, że macierze kwadratowe $A, B \in M_n(K)$ są kongruentne tylko wtedy, gdy są macierzami pewnej formy dwuliniowej, otrzymamy kluczowy wniosek: nad ciałem charakterystyki różnej od 2 każda macierz symetryczna jest kongruentna do macierzy diagonalnej.

Naszym celem jest klasyfikacja symetrycznych macierzy nad ciałem K (przy czym $\text{char}K \neq 2$), które znajdują się w tej samej klasie kongruencji (nad K). Wiemy już, że każda macierz symetryczna jest w tej relacji z pewną macierzą diagonalną. Nad ciałami \mathbb{R} oraz \mathbb{C} możemy doprecyzować ten wniosek.

Wniosek 22.1

Niech (V, h) będzie przestrzenią dwuliniową nad ciałem K .

- (a) Jeśli $K = \mathbb{C}$, to istnieje taka baza prostopadła $(\alpha_1, \dots, \alpha_n)$ przestrzeni V , taka że $h(\alpha_i, \alpha_i) \in \{0, 1\}$, dla $i = 1, \dots, n$. Zatem dla $i, j = 1, \dots, n$ mamy:

$$h(\alpha_i, \alpha_j) = \begin{cases} 0 \text{ lub } 1 & \text{gdy } i = j \\ 0 & \text{gdy } i \neq j. \end{cases}$$

- (b) Jeśli $K = \mathbb{R}$, to istnieje taka baza prostopadła $(\alpha_1, \dots, \alpha_n)$ przestrzeni V , taka że $h(\alpha_i, \alpha_i) \in \{0, 1, -1\}$, dla $i = 1, \dots, n$. Zatem dla $i, j = 1, \dots, n$ mamy:

$$h(\alpha_i, \alpha_j) = \begin{cases} 0, 1 \text{ lub } -1 & \text{gdy } i = j \\ 0 & \text{gdy } i \neq j. \end{cases}$$

Dowód. Zarówno w (a), jak i (b) mamy ciała charakterystyki różnej od 2, a zatem na mocy znanych nam już wyników istnieje baza prostopadła przestrzeni V , nazwijmy ją $(\beta_1, \dots, \beta_n)$. Definiujemy następnie bazę $(\alpha_1, \dots, \alpha_n)$ przestrzeni V przy pomocy warunków:

$$\alpha_i = \begin{cases} \beta_i, & \text{dla } h(\beta_i, \beta_i) = 0, \\ \frac{1}{a_i}\beta_i, & \text{dla } h(\beta_i, \beta_i) \neq 0. \end{cases}$$

przy czym dla $i = 1, \dots, n$ element $a_i \in K$ jest:

- dowolną liczbą spełniającą $a_i^2 = h(\beta_i, \beta_i)$, dla $K = \mathbb{C}$,
- taki, że $a_i^2 = |h(\beta_i, \beta_i)|$, gdy $K = \mathbb{R}$.

Wówczas w przypadku $h(\beta_i, \beta_i) \neq 0$ mamy $h(\alpha_i, \alpha_i) = h\left(\frac{1}{a_i}\beta_i, \frac{1}{a_i}\beta_i\right) = \frac{1}{a_i^2}h(\beta_i, \beta_i) = \begin{cases} 1, & \text{gdy } K = \mathbb{C}, \\ 1, -1 & \text{gdy } K = \mathbb{R}. \end{cases}$ □

Wniosek 22.2

Każda niezerowa macierz symetryczna $A \in M_n(\mathbb{C})$ jest kongruentna (nad \mathbb{C}) do macierzy diagonalnej D_A , która ma na przekątnej k jedynek, potem $n - k$ zer, gdzie $k = r(A)$ czyli

$$D_A = \begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{bmatrix}$$

Każda niezerowa macierz symetryczna $A \in M_n(\mathbb{R})$ jest kongruentna (nad \mathbb{R}) do takiej macierzy diagonalnej D_A , która ma na przekątnej k jedynek, potem s minus jedynek i wreszcie $n - k - s$ zer, gdzie $k + s = r(A)$, czyli

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

Wniosek 22.3

Symetryczne macierze $A, B \in M_n(\mathbb{C})$ są kongruentne wtedy i tylko wtedy, gdy mają ten sam rząd. Istnieje więc $n + 1$ klas kongruencji symetrycznych macierzy zespolonych $n \times n$.

Dowód. Wykazaliśmy, że każda symetryczna macierz zespolona A jest kongruentna nad \mathbb{C} do macierzy D_A mającej postać z Wniosku 1. Przy tym liczba jedynek występującej na przekątnej macierzy D_A równa jest $r(D_A)$, czyli też $r(A)$, bo macierze kongruentne muszą mieć identyczny rząd (jest to rząd odpowiadającej im formy). Zatem jeśli macierze symetryczne $A, B \in M_n(\mathbb{C})$ mają ten sam rząd k , to obie są kongruentne do tej samej macierzy 0-1-kowej z Wniosku 1. Stąd, z przechodniości relacji kongruencji, macierze A i B są kongruentne nad \mathbb{C} . Macierzy $n \times n$ postaci D_A opisanej we Wniosku 1 jest $n + 1$, przy czym parami różne nie są kongruentne, bo mają różny rząd. Wynika stąd, że jest $n + 1$ klas kongruencji symetrycznych macierzy zespolonych $n \times n$. \square

Czego zatem dowiedzieliśmy się o każdej zespolonej symetrycznej formie dwuliniowej h na przestrzeni V ? Otóż można do niej dobrać bazę prostopadłą V taką, że forma h obcięta do podprzestrzeni rozpiętej przez pierwszych $r(h)$ wektorów tej bazy jest dodatnio określona. Zachowuje się ona na tej podprzestrzeni „w zasadzie jak” iloczyn skalarny. Jesteśmy wprawdzie nad \mathbb{C} , ale dla tej podprzestrzeni te $r(h)$ wektorów rozpinających to jest właściwie „baza ortonormalna”, której nie da się w przestrzeniach dwuliniowych często wyznaczyć (co innego z bazą ortogonalną). Na prostopadłej podprzestrzeni rozpiętej przez pozostałe $\dim V - r(h)$ wektorów (izotropowych) forma jest całkowicie zdegenerowana – zabija wszystko.

Zatem symetryczne formy dwuliniowe nad \mathbb{C} można oglądać „lokalnie” obcinając je do dwóch podprzestrzeni. Patrząc na każde obcięcie z osobna całkowicie rozumiemy co się w podprzestrzeni dzieje (z formą) i w łatwy sposób umiemy „skleić” obciążenia do pełnego opisu. Ta sama idea, tylko dotycząca „sklejania” endomorfizmu z jego obciążeniem do podprzestrzeni niezmienniczych leży u podstaw twierdzenia Jordana.

Twierdzenie 22.1: Sylwestera o bezwładności (inercji)

Niech $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$ oraz $\mathcal{B} = (\beta_1, \dots, \beta_n)$ będą bazami prostopadłymi przestrzeni dwuliniowej (V, h) nad ciałem \mathbb{R} . Oznaczmy:

- $r_+(\mathcal{A}) =$ liczba takich $1 \leq i \leq n$, że $h(\alpha_i, \alpha_i) > 0$,
- $r_-(\mathcal{A}) =$ liczba takich $1 \leq i \leq n$, że $h(\alpha_i, \alpha_i) < 0$,
- $r_+(\mathcal{B}) =$ liczba takich $1 \leq i \leq n$, że $h(\beta_i, \beta_i) > 0$,
- $r_-(\mathcal{B}) =$ liczba takich $1 \leq i \leq n$, że $h(\beta_i, \beta_i) < 0$.

Wówczas

$$r_+(\mathcal{A}) = r_+(\mathcal{B}) \quad \text{oraz} \quad r_-(\mathcal{A}) = r_-(\mathcal{B}).$$

Ponadto $r_+(\mathcal{A}) + r_-(\mathcal{A}) = r(h) = r_+(\mathcal{B}) + r_-(\mathcal{B})$.

Dowód. Definiujemy następujące trójki podprzestrzeni V rozpiętych przez elementy bazowe z \mathcal{A}, \mathcal{B} :

$$\begin{aligned} V_+ &= \text{lin}(\alpha_i \mid h(\alpha_i, \alpha_i) > 0), & W_+ &= \text{lin}(\beta_i \mid h(\beta_i, \beta_i) > 0), \\ V_- &= \text{lin}(\alpha_i \mid h(\alpha_i, \alpha_i) < 0), & W_- &= \text{lin}(\beta_i \mid h(\beta_i, \beta_i) < 0), \\ V_0 &= \text{lin}(\alpha_i \mid h(\alpha_i, \alpha_i) = 0), & W_0 &= \text{lin}(\beta_i \mid h(\beta_i, \beta_i) = 0). \end{aligned}$$

Jest jasne, że

$$r_+(\mathcal{A}) = \dim V_+, \quad r_-(\mathcal{A}) = \dim V_-, \quad r_+(\mathcal{B}) = \dim W_+, \quad r_-(\mathcal{B}) = \dim W_-.$$

Co więcej

$$V_+ \oplus V_- \oplus V_0 = V = W_+ \oplus W_- \oplus W_0,$$

skąd¹

$$\dim V_+ + \dim V_- + \dim V_0 = \dim V = \dim W_+ + \dim W_- + \dim W_0.$$

Przy tym

$$\dim V_+ + \dim V_- = r(h) = \dim W_+ + \dim W_-,$$

co daje

$$r_+(\mathcal{A}) + r_-(\mathcal{A}) = r(h) = r_+(\mathcal{B}) + r_-(\mathcal{B}),$$

co stanowi drugą część tezy.

Dowodzimy, że $r_+(\mathcal{A}) = r_+(\mathcal{B})$. Zaczniemy od pokazania tego, że $V_+ \cap (W_- + W_0) = \{0\}$. Otóż

- dla każdego niezerowego wektora $\alpha \in V_+$ mamy $h(\alpha, \alpha) = h(\sum a_i \alpha_i, \sum a_i \alpha_i) = \sum a_i^2 h(\alpha_i, \alpha_i) > 0$,
- dla każdego wektora $\beta \in W_-$ mamy $h(\beta, \beta) = h(\sum b_i \beta_i, \sum b_i \beta_i) = \sum b_i^2 h(\beta_i, \beta_i) \leq 0$.

A zatem dla każdego $\delta = \beta + \gamma$, gdzie $\beta \in W_-, \gamma \in W_0$ zachodzi:

$$h(\delta, \delta) = h(\beta + \gamma, \beta + \gamma) = h(\beta, \beta) + 2h(\beta, \gamma) + h(\gamma, \gamma) = h(\beta, \beta) + 0 + 0 \leq 0.$$

A zatem $V_+ \cap (W_- + W_0) = \{0\}$, a stąd

$$\dim V_+ + \dim(W_- + W_0) = \dim(V_+ + W_- + W_0) \leq \dim V.$$

Korzystając z $\dim(W_- + W_0) = \dim W_- + \dim W_0 = \dim V - \dim W_+$, możemy powyższą nierówność przepisać w postaci

$$\dim V_+ + \dim V - \dim W_+ \leq \dim V.$$

W rezultacie dostajemy $\dim V_+ \leq \dim W_+$. Tak samo dowodzimy, że $\dim W_+ \leq \dim V_+$, co daje łącznie $\dim V_+ = \dim W_+$. Korzystając z tej równości i równości udowodnionej w pierwszej części tezy mamy też $\dim V_- = \dim W_-$. Dowód jest zakończony. \square

¹Po prostu wektor przestrzeni V jest kombinacją liniową wektorów z V_+, V_-, V_0 , a przestrzenie te nie tylko mają zerowe przecięcie, ale każda z nich przecina się jedynie na zerze z sumą dwóch pozostałych. Stąd też wynika natychmiast, że wymiar sumy prostej trzech podprzestrzeni równy jest sumie wymiarów poszczególnych składników. Analogicznie dla rozkładu $V = W_+ \oplus W_- \oplus W_0$.

Definicja 22.1: Sygnatura rzeczywistej formy dwuliniowej

Niech (V, h) będzie przestrzenią dwuliniową nad ciałem \mathbb{R} . SYGNATURĄ PRZESTRZENI (V, h) (albo formy dwuliniowej h) nazywamy liczbę $r_+(\mathcal{A}) - r_-(\mathcal{A})$ z poprzedniego twierdzenia. Sygnaturę oznaczamy $s(V, h)$ lub $s(h)$. Twierdzenie pokazuje, że jest ona dobrze określona (nie zależy od wyboru bazy prostopadłej \mathcal{A}).

SYGNATURĄ MACIERZY SYMETRYCZNEJ $A \in M_n(\mathbb{R})$ nazywamy sygnaturę formy dwuliniowej $h : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$ zadanej macierzą $G(h; st) = A$. Sygnaturę macierzy A oznaczamy $s(A)$. Więc $s(A)$ równa jest różnicy liczby dodatnich oraz liczby ujemnych wyrazów na przekątnej w macierzy diagonalnej kongruentnej (nad \mathbb{R}) do macierzy A .

Przed nami kluczowy wniosek określający postaci kanoniczne kongruencji (nad \mathbb{R}) w zbiorze $M_n(\mathbb{R})$.

Wniosek 22.4

Symetryczne macierze $A, B \in M_n(\mathbb{R})$ są kongruentne (nad \mathbb{R}) wtedy i tylko wtedy, gdy mają równe rzędy i sygnatury, tzn. $r(A) = r(B)$ oraz $s(A) = s(B)$. Istnieje $(n+1)(n+2)/2$ klas kongruencji symetrycznych macierzy rzeczywistych $n \times n$.

Dowód. Rozumowanie jest takie samo jak w przypadku analogicznej charakteryzacji kongruencji symetrycznych macierzy zespolonych. Każda rzeczywista macierz symetryczna A jest kongruentna nad \mathbb{R} do macierzy diagonalnej D_A opisanej we Wniosku 2. Macierzy takich jest $(n+1)(n+2)/2$ przy czym parami różne z nich nie są kongruentne nad \mathbb{R} , bo mają różne rzędy lub sygnatury. \square

Dokonałiśmy klasyfikacji macierzy kongruentnych dla macierzy nad ciałami \mathbb{C} i \mathbb{R} . Dla jakich ciał istnieją analogiczne klasyfikacje? Nietrudno zobaczyć, że można zamienić \mathbb{C} na dowolne ciało algebraicznie domknięte. Ciało \mathbb{R} można zamienić na tzw. ciało kwadratowo domknięte (musimy umieć wyciągać pierwiastki kwadratowe z każdego elementu), w którym każda liczba jest, modulo pewien kwadrat, elementem 1 lub -1 . w dodatku pokażemy analog kryterium Sylwestera, które pozwala w wielu sytuacjach określać macierz diagonalną kongruentną do danej za pomocą głównych minorów wiodących.

Twierdzenie Sylwestera o bezwładności jest punktem wyjścia do mówienia o określoności form kwadratowych. Temat ten, niezwykle istotny dla zastosowań, omówimy następnym razem, zamykając tym samym teorię przestrzeni liniowych na tym wykładzie. Teoria wymiernych form dwuliniowych jest znacznie bardziej skomplikowana i przekracza ramy tego wykładu.

Zobaczmy kilka przykładów zadań wykorzystujących pokazane wyżej twierdzenia.

Zadanie 22.1. Pokazać, że macierze

$$A_1 = \begin{bmatrix} -2 & 0 & 2 \\ 0 & 1 & 0 \\ 2 & 0 & 1 \end{bmatrix} \quad \text{oraz} \quad A_2 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

są kongruentne nad \mathbb{R} i znaleźć macierz odwracalną $C \in M_{3 \times 3}(\mathbb{R})$ taką, że $A_2 = C^T A_1 C$.

ROZWIĄZANIE. Niech $h_1, h_2 : \mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R}$ będą formami dwuliniowymi o tej własności, że $A_1 = G(h_1, st)$ oraz $A_2 = G(h_2, st)$. Znajdziemy bazy prostopadłe przestrzeni (\mathbb{R}^3, h_1) oraz (\mathbb{R}^3, h_2) .

- Niech $\alpha_1 = (1, 0, 0)$. Mamy $h_1((1, 0, 0), (1, 0, 0)) = -2$ oraz $\text{lin}((1, 0, 0))^\perp : -2x_1 + 2x_3 = 0$. Weźmy $\alpha_2 = (0, 1, 0) \in \text{lin}((1, 0, 0))^\perp$. Wówczas $h_2((0, 1, 0), (0, 1, 0)) = 1$. $\text{lin}((1, 0, 1))^\perp : x_2 = 0$. A zatem biorąc $\alpha_3 = (1, 0, 1)$ dostajemy $h(\alpha_1, \alpha_2) = h(\alpha_1, \alpha_3) = 0$ oraz $h(\alpha_3, \alpha_3) = 3$. W szczególności forma h_1 ma rząd 3 i sygnaturę 1 oraz biorąc za C_1 macierz mającą w kolumnach wektory $\frac{1}{\sqrt{2}}\alpha_1, \alpha_2, \frac{1}{\sqrt{3}}\alpha_3$ mamy $C_1^T A_1 C_1 = D = \text{diag}(-1, 1, 1)$, czyli:

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 1 & 0 \\ \frac{1}{\sqrt{3}} & 0 & \frac{1}{\sqrt{3}} \end{bmatrix} \begin{bmatrix} -2 & 0 & 2 \\ 0 & 1 & 0 \\ 2 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{3}} \\ 0 & 1 & 0 \\ 0 & 0 & \frac{1}{\sqrt{3}} \end{bmatrix} = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

- Niech $\beta_1 = (1, 0, 0)$. Mamy: $h_2((1, 0, 0), (1, 0, 0)) = 1$ oraz $\text{lin}(\beta_1)^\perp : x_1 + x_3 = 0$. Przyjmijmy $\beta_2 = (0, 1, 0) \in \text{lin}(\beta_1)^\perp$. Wówczas $h_2((0, 1, 0), (0, 1, 0)) = 1$. Mamy też $\text{lin}(\beta_2)^\perp : x_2 = 0$. A zatem biorąc $\beta_3 = (1, 0, -1)$ mamy $h_2(\beta_1, \beta_3) = h_2(\beta_2, \beta_3) = 0$ oraz $h(\beta_3, \beta_3) = -1$. W szczególności forma h_2 ma rząd 3 i sygnaturę 1, podobnie jak h_1 . Co więcej biorąc za C_2 macierz mającą w kolumnach wektory $\beta_3, \beta_2, \beta_1$ dostajemy $C_2^T A_2 C_2 = D = \text{diag}(-1, 1, 1)$, czyli:

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

Na podstawie powyższych rachunków widzimy, że macierze A_1 oraz A_2 są kongruentne do identycznej macierzy kongruentnej, czyli są kongruentne. Używając powyższych oznaczeń widzimy, że szukana macierz odwracalna C taka, że $C^T A_1 C = A_2$ równa jest $C_1 C_2^{-1}$, bo $C_1^T A_1 C_1 = D$ oraz $(C_2^{-1})^T D C_2^{-1} = A_2$. ■

Zadanie 22.2. Dla każdego $t \in \mathbb{R}$ rozważmy formę dwuliniową symetryczną $h_t : \mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R}$

$$G(h_t; st) = \begin{bmatrix} 1 & 1 & 1 \\ 1 & t & 1 \\ 1 & 1 & 2 \end{bmatrix}.$$

W zależności od parametru t znaleźć rząd i sygnaturę formy h_t . Niech $t = 1$. Znaleźć bazę \mathcal{A} przestrzeni \mathbb{R}^3 taką, że macierz $G(h_1, \mathcal{A})$ jest diagonalna.

ROZWIĄZANIE. Wyznamy bazę prostopadłą przestrzeni (\mathbb{R}^3, h_t) . Weźmy dowolny niezerowy wektor, np. $\alpha_1 = (1, 0, 0)$. Mamy $h_t(\alpha_1, \alpha_1) = 1$, zatem $\mathbb{R}^3 = \text{lin}(\alpha_1) \oplus \text{lin}(\alpha_1)^\perp$. Wektor $v = (x_1, x_2, x_3)$ należy do $\text{lin}(\alpha_1)^\perp$ wtedy i tylko wtedy, gdy:

$$h_t(\alpha_1, v) = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ 1 & t & 1 \\ 1 & 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = x_1 + x_2 + x_3 = 0.$$

Weźmy $\alpha_2 = (1, 0, -1) \in \text{lin}(\alpha_1)^\perp$. Mamy $h_t(\alpha_2, \alpha_2) = 1$, a zatem $\mathbb{R}^3 = \text{lin}(\alpha_1, \alpha_2) \oplus \text{lin}(\alpha_1, \alpha_2)^\perp$. Wyznamy teraz wszystkie wektory $w = (x_1, x_2, x_3) \in \text{lin}(\alpha_1, \alpha_2)^\perp$. Współrzędne tych wektorów muszą spełniać równanie $x_1 + x_2 + x_3 = 0$ oraz równanie:

$$h_t(\alpha_2, w) = \begin{bmatrix} 1 & 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ 1 & t & 1 \\ 1 & 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 & 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = -x_3 = 0.$$

Przestrzeń $\text{lin}(\alpha_1, \alpha_2)^\perp$ jest zatem opisana układem równań liniowych postaci $x_1 + x_2 + x_3 = 0$, $x_3 = 0$. Niech $\alpha_3 = (1, -1, 0) \in \text{lin}(\alpha_1, \alpha_2)^\perp$. Układ $(\alpha_1, \alpha_2, \alpha_3)$ jest bazą prostopadłą przestrzeni dwuliniowej (\mathbb{R}^3, h_t) . Mamy też $h_t(\alpha_3, \alpha_3) = t - 1$. A zatem forma h_t w bazie $\mathcal{A} = (\alpha_1, \alpha_2, \alpha_3)$ ma postać:

$$G(h_t; \mathcal{A}) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & t - 1 \end{bmatrix}.$$

Stąd:

$$r(h_t) = \begin{cases} 2, & \text{dla } t = 1 \\ 3, & \text{dla } t \neq 1. \end{cases}, \quad s(h_t) = \begin{cases} 1, & \text{dla } t < 1 \\ 2, & \text{dla } t = 1 \\ 3, & \text{dla } t > 1. \end{cases}$$

Bazą (\mathbb{R}^3, h_1) , w której forma h_1 jest diagonalna jest zatem $((1, 0, 0), (1, 0, -1), (1, -1, 0))$. ■

Uwaga. Można zastosować także inną metodę poznaną na wykładzie, i na ćwiczeniach. Można przyjąć, że $M(G, h_t)$ jest macierzą pewnego endomorfizmu samosprzężonego ϕ przestrzeni $(\mathbb{R}^3, \langle \cdot, \cdot \rangle_{st})$ w bazie standardowej. Wówczas istnieje baza złożona z wektorów ortonormalnych w $(\mathbb{R}^3, \langle \cdot, \cdot \rangle_{st})$, będących wektorami własnymi ϕ .

22.1 Uzupełnienie. Twierdzenie Jacobiego

W niektórych sytuacjach możliwe jest określenie (nad dowolnym ciałem) macierzy diagonalnej, do której kongruentna jest dana macierz.

Twierdzenie 22.2: Jacobi

Niech (V, h) będzie taką przestrzenią dwuliniową taką, że wiodące minory główne $\Delta_i = \det A^{(i)}$ macierzy symetrycznej $A = G(h, \mathcal{A})$ są niezerowe, dla pewnej bazy \mathcal{A} przestrzeni V . Wówczas istnieje baza \mathcal{B} przestrzeni V taka, że

$$G(h, \mathcal{B}) = \text{diag} \left(\frac{\Delta_1}{\Delta_0}, \dots, \frac{\Delta_n}{\Delta_{n-1}} \right), \quad \text{gdzie } \Delta_0 = 1.$$

Przykład: dla poniższej macierzy $A \in M_n(\mathbb{Q})$ mamy $\Delta_0 = 1, \Delta_1 = 3, \Delta_2 = 2, \Delta_3 = -7$.

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

Macierz ta jest zatem kongruentna do macierzy diagonalnej (wymiernej) o wyrazach $3, \frac{2}{3}, -\frac{7}{2}$.

Dowód. Rozumowanie jest indukcją ze względu na wymiar n przestrzeni V . Teza jest oczywista dla $n = 1$. Niech $n = \dim V > 1$. Niech $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$. Niech $W = \text{lin}(\alpha_1, \dots, \alpha_{n-1})$. Zauważmy, że macierz $A^{(n-1)}$ jest macierzą formy h obciętej do podprzestrzeni: W i jej wiodące minory główne to wyznaczniki macierzy $A^{(1)}, A^{(2)}, \dots, A^{(n-1)}$. Wyznaczniki te są niezerowe, więc zgodnie z założeniem indukcyjnym istnieje taka baza $\beta_1, \dots, \beta_{n-1}$ przestrzeni W oraz dopełniający ją do bazy \mathcal{B}' wektor $\gamma_n \in W^\perp$ (wiemy, że W jest nieosobliwa, bo $\det A^{(n-1)} \neq 0$, czyli $V = W \oplus W^\perp$), że w bazie $\mathcal{C} = (\beta_1, \dots, \beta_{n-1}, \gamma_n)$ przestrzeni V mamy:

$$G(h, \mathcal{C}) = \begin{bmatrix} \Delta_1/\Delta_0 & 0 & \dots & 0 & 0 \\ 0 & \Delta_2/\Delta_1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & \Delta_{n-1}/\Delta_{n-2} & 0 \\ 0 & 0 & \dots & 0 & h(\gamma_n, \gamma_n) \end{bmatrix}.$$

Niech $C = M(\text{id})_{\mathcal{C}}^{\mathcal{A}}$ i $\det C = d$. Mamy $C^T \cdot A \cdot C = G(h, \mathcal{C})$ oraz $\det A = \Delta_n$. Zatem

$$d^2 \cdot \Delta_n = \Delta_{n-1} \cdot h(\gamma_n, \gamma_n).$$

Możemy podmienić wektor γ_n przez $\beta_n = d^{-1} \cdot \gamma_n$ dostając, że istnieje baza $\mathcal{B} = (\beta_1, \dots, \beta_n)$ przestrzeni V , że:

$$G(h, \mathcal{B}) = \begin{bmatrix} \Delta_1/\Delta_0 & 0 & \dots & 0 & 0 \\ 0 & \Delta_2/\Delta_1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & \Delta_{n-1}/\Delta_{n-2} & 0 \\ 0 & 0 & \dots & 0 & h(\gamma_n, \gamma_n)/d^2 \end{bmatrix}.$$

Stąd $\det M(\text{id})_{\mathcal{B}}^{\mathcal{A}} = 1$. Zatem

$$\Delta_n = \Delta_{n-1} \cdot \frac{h(\gamma_n, \gamma_n)}{d^2},$$

co kończy dowód. □

22.2 Dodatek. Izometrie przestrzeni dwuliniowych. Kongruencja macierzy diagonalnych

Dowodząc twierdzenie Sylwestera o inercji orzekamy w istocie które dwie macierze diagonalne są kongruentne. Problem ten jest, nad dowolnym ciałem, raczej skomplikowany. Warto jednak poczynić kilka uwag i udowodnić kilka rezultatów. Złożą się one na alternatywny dowód twierdzenia Sylwestera i pozwolą wyjaśnić kwestie izometryczności przestrzeni dwuliniowych, poruszoną już krótko w poprzednim dodatku. W trakcie całego tego tekstu przez $\text{diag}(a_1, \dots, a_n)$ rozumiemy macierz diagonalną rozmiaru n o wyrazach na diagonalu równych kolejno a_1, \dots, a_n . Macierze kongruentne A, B oznaczamy jako $A \simeq B$ (o ile wiemy nad jakim jesteśmy ciałem). Przypomnijmy najpierw oczywiste kwestie.

Trywialna uwaga 1 Jeśli $A = \text{diag}(a_1, \dots, a_n)$ oraz $B = \text{diag}(a_{\sigma(1)}, \dots, a_{\sigma(n)})$, dla pewnej permutacji $\sigma \in S_n$, to jeśli P jest macierzą permutacji σ , to $B = P^T A P$, czyli:

$$\text{diag}(a_1, \dots, a_n) \cong \text{diag}(a_{\sigma(1)}, \dots, a_{\sigma(n)}).$$

Innymi słowy, jeśli $A = G(h, \mathcal{A})$, gdzie $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$, to dla bazy $\mathcal{B} = (\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)})$ mamy $B = G(h, \mathcal{B})$.

Trywialna uwaga 2 Dla dowolnych $a_1, \dots, a_n, b_1 \neq 0, \dots, b_n \neq 0 \in K$ mamy:

$$\text{diag}(a_1, \dots, a_n) \cong \text{diag}(b_1^2 a_1, \dots, b_n^2 a_n).$$

Definicja 22.2: Ciało kwadratowo domknięte

Ciało K nazywamy KWADRATOWO DOMKNIĘTYM, jeśli każdy element K jest kwadratem pewnego elementu z K .

Przykłady ciał kwadratowo domkniętych:

- ciała algebraicznie domknięte,
- ciało \mathbb{Z}_2 (trudniejszy fakt: dowolne skończone ciało charakterystyki 2).

Obserwacja 22.1

Jeśli K jest ciałem kwadratowo domkniętym oraz jeśli $A = \text{diag}(a_1, \dots, a_r, 0, \dots, 0) \in M_n(K)$, gdzie $a_i \neq 0$, to

$$\text{diag}(a_1, \dots, a_r, 0, \dots, 0) \simeq \text{diag}(\underbrace{1, \dots, 1}_r, 0, \dots, 0).$$

Dowód. Jeśli $A = \text{diag}(a_1, \dots, a_r, 0, \dots, 0) \in M_n(\mathbb{C})$, gdzie $a_i \neq 0$, jest macierzą formy h na V w bazie $(\alpha_1, \dots, \alpha_n)$, to biorąc bazę $\mathcal{B} = (\beta_1, \dots, \beta_n)$ postaci:

$$\beta_j = \begin{cases} \frac{1}{\sqrt{a_i}} \alpha_i, & \text{dla } i \leq r, \\ \alpha_i, & \text{dla } i > r \end{cases}$$

dostajemy: $G(h, \mathcal{B}) = \text{diag}(1, \dots, 1, 0, \dots, 0)$, czyli $\text{diag}(a_1, \dots, a_r, 0, \dots, 0) \simeq \text{diag}(\underbrace{1, \dots, 1}_r, 0, \dots, 0)$. \square

Wniosek 22.5

Jeśli $A, B \in M_n(K)$, gdzie K jest ciałem kwadratowo domkniętym charakterystyki różnej od 2, to $A \cong B \Leftrightarrow r(A) = r(B)$.

Mała dygresja. Na zbiorze \dot{K} niezerowych elementów ciała K definiujemy relację równoważności: $a \sim b$ wtedy i tylko wtedy, gdy ab^{-1} jest kwadratem w K . Zbiór klas abstrakcji \dot{K}/\dot{K}^2 ma strukturę grupy z działaniem $[a] \cdot [b] = [ab]$ nazywanej GRUPĄ KLAS KWADRATÓW CIAŁA K .

Przykłady i uwagi (informacyjnie)

- Dla ciał kwadratowo domkniętych mamy $|\dot{K}/\dot{K}^2| = 1$.
- Jeśli $0 \neq a \in \mathbb{R}$, to $a \sim 1$ lub $a \sim -1$, czyli $|\dot{\mathbb{R}}/\dot{\mathbb{R}}^2| = 2$.
- Jeśli $p, q \in \mathbb{Q}$ są liczbami pierwszymi, to $p \sim q \Leftrightarrow p = q$, czyli $|\dot{\mathbb{Q}}/\dot{\mathbb{Q}}^2| = \infty$.
- Jeśli $|\dot{K}/\dot{K}^2|$ jest skończona, to ma 2^k elementów, dla pewnego k .
- Dla każdego ciała skończonego K charakterystyki $\neq 2$ mamy $|\dot{K}/\dot{K}^2| = 2$.
- Rozważa się tzw. CIAŁA SZEREGÓW FORMALNYCH (ilorazy szeregów formalnych) o współczynnikach w ciele K , ozn. $K((x))$. Okazuje się, że $|K((x))/K((x))^2| = 2 \cdot |\dot{K}/\dot{K}^2|$.

Naszym celem będzie pokazanie uogólnienia twierdzenie o inercji na macierze symetryczne nad ciałem K , dla $|\dot{K}/\dot{K}^2| = 2$. W tym celu wprowadzimy pojęcie izometrii przestrzeni dwuliniowych.

Definicja 22.3: Izometria przestrzeni dwuliniowych

Niech h będzie formą dwuliniową na przestrzeni V oraz niech h' będzie formą dwuliniową na izomorficznej z V przestrzeni W . Izomorfizm $i : V \rightarrow W$ nazwiemy IZOMETRIĄ przestrzeni (V, h) i (W, h') , jeśli dla każdych $x, y \in U$ mamy:

$$h(x, y) = h'(i(x), i(y)).$$

Jeśli istnieje izometria (V, h) i (W, h') , wówczas przestrzenie/formy te nazywamy IZOMETRYCZNYMI lub RÓWNOWAŻNYMI, ozn. $(V, h) \cong (W, h')$.

Przykłady:

- id oraz $-\text{id}$,
- obrót w $(\mathbb{R}^2, \langle \cdot, \cdot \rangle_{st})$,
- symetria prostopadła (V, h) względem podprzestrzeni nieosobliwej W ,
- złożenie dowolnej liczby izometrii.

Idea jest taka sama, jak w przestrzeniach euklidesowych czy unitarnych: izometria dokonuje „transportu” struktury dwuliniowej z V do W . Poniższy fakt pozostawiam jako ćwiczenie.

Obserwacja 22.2

Niech (V, h) oraz (W, h') będą skończenie wymiarowe i niech $A = G(h, \mathcal{A})$, $B = G(h', \mathcal{B})$, gdzie \mathcal{A}, \mathcal{B} są jakimikolwiek bazami V, W . Wówczas $(V, h) \cong (W, h') \iff A \cong B$.

Kluczowy będzie dowód poniższego twierdzenia, sprowadzającego problem badania kongruencji macierzy symetrycznych do problemu analizy macierzy, które na przekątnej mają rozłączne układy skalarów.

Twierdzenie 22.3: Twierdzenie Witta o skracaniu

Niech $\text{char } K \neq 2$ oraz niech $a_1, \dots, a_n, b_1, \dots, b_n, c_1 \neq 0, \dots, c_k \neq 0$ będą elementami K . Wtedy

$$\text{diag}(c_1, \dots, c_k, a_1, \dots, a_n) \cong \text{diag}(c_1, \dots, c_k, b_1, \dots, b_n) \implies \text{diag}(a_1, \dots, a_n) \cong \text{diag}(b_1, \dots, b_n).$$

Zauważmy, dla pewnego utrzymania motywacji, że z wyniku tego wyniku natychmiast alternatywny dowód twierdzenia Sylwestera o bezwładności (wersja rzeczywista).

Niech $A = \text{diag}(a_1, \dots, a_n)$, $B = \text{diag}(b_1, \dots, b_n)$ będą kongruentnymi macierzami diagonalnymi nad \mathbb{R} . Możemy założyć, że $a_i, b_j \in \{-1, 1\}$. Zgodnie z Trywialną Uwagą 1 możemy zakładać, że jeśli $a_i = 1$ oraz $a_j = -1$, to $i < j$, podobnie dla macierzy B .

Jeśli $|\{i : a_i = 1\}| \neq 0$, to również $|\{i : b_i = 1\}| \neq 0$. W przeciwnym razie z postaci macierzy B wynika, że $h(u, u) < 0$, dla dowolnego $u \in \mathbb{R}^n$, gdzie $A = G(h, st)$, co prowadzi do sprzeczności.

Jeśli $|\{i : a_i = 1\}| > |\{i : b_i = 1\}| > 0$, to na mocy twierdzenia Witt'a o skracaniu istnieją s, r takie, że:

$$\text{diag}(\underbrace{1, \dots, 1}_s, \underbrace{-1, \dots, -1}_r) \cong \text{diag}(\underbrace{-1, \dots, -1}_{s+r}),$$

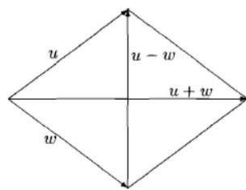
co prowadzi do sprzeczności, jak wyżej. Stąd

$$|\{i : a_i = 1\}| = |\{i : b_i = 1\}| \quad \text{oraz} \quad |\{i : a_i = -1\}| = |\{i : b_i = -1\}|.$$

Aby przeprowadzić dowód twierdzenia Witt'a o skracaniu potrzebujemy najpierw poniższego lematu.

Twierdzenie 22.4: Pierwsza wersja twierdzenia Witt'a o przedłużaniu izometrii

Niech (V, h) będzie przestrzenią dwuliniową nad ciałem charakterystyki $\neq 2$. Jeśli $u, w \in V$ są wektorami nieizotropowymi i $h(u, u) = h(w, w)$, to istnieje taka izometria przestrzeni $i : (V, h) \rightarrow (V, h)$, że $i(u) = w$.



Dowód. Gdy $u = w$ teza jest jasna. Niech $u \neq w$. Mamy $h(u, u) = h(w, w)$, więc $h(u - w, u + w) = 0$. Mamy więc (było na wykładzie)

$$u = \frac{1}{2}(u - w) + \frac{1}{2}(u + w).$$

Jeśli $u + w$ jest nieizotropowy, to symetria prostopadła V względem podprzestrzeni nieosobliwej $\text{lin}(u + w)$ przeprowadza $u \mapsto w$. Jeśli $u - w$ jest nieizotropowy, to symetria prostopadła V względem podprzestrzeni nieosobliwej $\text{lin}(u - w)$ przeprowadza $u \mapsto -w$, a zatem złożenie tej symetrii z $-\text{id}$ to izometria V przeprowadzająca $u \mapsto w$. Skoro u, w są nieizotropowe, to jeden z wektorów $u - w$ lub $u + w$ też, bo:

$$h(u - w, u - w) + h(u + w, u + w) = 2h(u, u) + 2h(w, w) = 4h(u, u) \neq 0.$$

□

Przejdźmy do dowodu twierdzenia o skracaniu. Zaczniemy od dowodu poniższej implikacji (dla $c \neq 0$):

$$\text{diag}(c, a_1, \dots, a_n) \cong \text{diag}(c, b_1, \dots, b_n) \Rightarrow \text{diag}(a_1, \dots, a_n) \cong \text{diag}(b_1, \dots, b_n).$$

Lewa strona powyższej implikacji oznacza, że na K^{n+1} istnieje forma dwuliniowa h oraz bazy ortogonalne $\mathcal{A} = \{\alpha, \alpha_1, \dots, \alpha_n\}$, $\mathcal{B} = \{\beta, \beta_1, \dots, \beta_n\}$ takie, że $G(h, \mathcal{A}) = \text{diag}(c, a_1, \dots, a_n)$, $G(h, \mathcal{B}) = \text{diag}(c, b_1, \dots, b_n)$. W szczególności $h(\alpha, \alpha) = h(\beta, \beta) = c \neq 0$, czyli z twierdzenie o przedłużaniu izometrii istnieje izometria $i : (K^{n+1}, h) \rightarrow (K^{n+1}, h)$, że $i(\alpha) = \beta$. Ponieważ i zachowuje prostopadłość wektorów, mamy $i(\text{lin}(\alpha)^\perp) = \text{lin}(\beta)^\perp$. Zatem $i|_{\text{lin}(\alpha)^\perp}$ jest izometrią. Z drugiej strony $\text{lin}(\alpha)^\perp = \text{lin}(\alpha_1, \dots, \alpha_n)$, $\text{lin}(\beta)^\perp = \text{lin}(\beta_1, \dots, \beta_n)$. A zatem mamy bazy prostopadłe izometrycznych przestrzeni, w których odpowiednio obcięte h mają macierze $\text{diag}(a_1, \dots, a_n) \cong \text{diag}(b_1, \dots, b_n)$. Dalej, podobnie jak w innych dowodach tego typu, stosujemy indukcję.

22.3 Trivia. Sygnatura, a geometria elementarna

W 1866 roku G. Darboux zdefiniował potęgę pary okręgów C_1, C_2 , czyli:

$$C_1 * C_2 = d^2 - r_1^2 - r_2^2,$$

gdzie r_1, r_2 to promienie okręgów C_1, C_2 , a d to odległość pomiędzy ich środkami. Jeśli okręgi się przecinają, wówczas $C_1 * C_2 = r_1 r_2 \cos \theta$, gdzie θ jest kątem pomiędzy okręgami. Jeśli okręgi są rozłączne, wówczas $C_1 * C_2$ równy jest kwadratowi długości odcinka narysowanego niżej.



Źródło: J. Kocik, *A theorem on circle configurations*.

Zbiór punktów na okręgu o promieniu r i środku (f, g) ma postać:

$$x^2 + y^2 - 2fx - 2gy + k = 0 \quad (\spadesuit)$$

gdzie $k = f^2 + g^2 - r^2$. W roku 1883 H. Cox zapisał produkt Darboux dwóch okręgów o środkach (f_1, g_1) , (f_2, g_2) i promieniach r_1, r_2 , odpowiednio, w języku współczynników równań (\spadesuit) :

$$C_1 * C_2 = k_1 + k_2 - 2f_1 f_2 - 2g_1 g_2.$$

W 1970 roku D. Pedoe zorientował się, że powyższą równość można interpretować jako... formę dwuliniową \langle, \rangle w przestrzeni \mathbb{R}^4 . Pomysł jest *rzutowy* w naturze: równanie (\spadesuit) można przeskalować do równania postaci: $a(x^2 + y^2) - 2bx - 2cy + d = 0$ i określić (dla tak opisanych okręgów):

$$\langle C_1, C_2 \rangle = b_1 b_2 + c_1 c_2 - \frac{d_1 a_1 + d_2 a_2}{2}.$$

O co tu chodzi? Każdemu okręgowi opisanemu w \mathbb{R}^2 równaniem:

$$a(x^2 + y^2) - 2bx - 2cy + d = 0, \quad a \neq 0.$$

przypisujemy wektor $C(a, b, c, d) \in \mathbb{R}^4$. Każda niezerowa wielokrotność tego wektora reprezentuje ten sam okrąg, więc możemy ograniczyć się do znormalizowanego równania opisującego C :

$$x^2 + y^2 - 2fx - 2gy + k = 0$$

i związanego z nim wektora współrzędnych $C(1, f, g, k)$.

Na \mathbb{R}^4 wprowadzamy strukturę przestrzeni dwuliniowej Minkowskiego (o wielkim znaczeniu w fizyce) poprzez zadanie formy dwuliniowej \langle, \rangle danej macierzą:

$$G(\langle, \rangle, st) = \begin{bmatrix} 0 & 0 & 0 & -\frac{1}{2} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -\frac{1}{2} & 0 & 0 & 0 \end{bmatrix},$$

i widzimy, że teraz rzeczywiście dla okręgów opisanych równaniami

$$a(x^2 + y^2) - 2bx - 2cy + d = 0$$

określić można wektory $(a, b, c, d) \in \mathbb{R}^4$ i wtedy

$$\langle C_1, C_2 \rangle = b_1 b_2 + c_1 c_2 - \frac{d_1 a_2 + d_2 a_1}{2}$$

Zauważmy też, że sens geometryczny mają także wektory (a, b, c, d) , gdzie $a = 0$:

- jeśli $a = 0$ oraz $b^2 + c^2 > 0$, to równanie *okręgu* opisuje prostą na płaszczyźnie, której można przypisać wektor

$$L(0, b, c, d),$$

- dla $a = b = c = 0$ oraz $d \neq 0$ żadne punkty nie spełniają tego równania i można utożsamić je z prostą niewłaściwą o współrzędnych

$$E(0, 0, 0, d).$$

Następujące fakty są prostymi ćwiczeniami:

- $\langle C_1, C_1 \rangle = r_1^2$,
- $\langle C_1, C_2 \rangle = 0$ wtedy i tylko wtedy, gdy okręgi C_1, C_2 są ortogonalne.
- $\langle C_1, C_2 \rangle \pm r_1 r_2$ wtedy i tylko wtedy, gdy C_1, C_2 są styczne,
- Jeśli C_1 jest punktem, czyli $r_1^2 = 0$, to $\langle C_1, C_2 \rangle$ równe jest minus potędze punktu C_1 względem okręgu C_2 ,
- punkt C_1 leży na okręgu C_2 wtedy i tylko wtedy, gdy $\langle C_1, C_2 \rangle = 0$,
- jeśli C_1, C_2 są punktami, to $\langle C_1, C_2 \rangle = -d^2/2$, gdzie $d = \rho(C_1, C_2)$,
- $\langle C_1, L_2 \rangle = -D$ jest skierowaną odległością od środka C_1 do L_2 ,
- prosta L_2 przechodzi przez środek C_1 wtedy i tylko wtedy, gdy $\langle L_2, C_1 \rangle = 0$,
- jeśli E to prosta w nieskończoności, to $\langle C_1, E \rangle = -1/2$,
- wszystkie proste właściwe są prostopadłe do prostej w nieskończoności (zwanej też prostą niewłaściwą).

Wyprowadzimy z tych faktów szereg bardziej i mniej znanych rezultatów o ważnych konfiguracjach okręgów. Niech $C_1(1, f_1, g_1, k_1), C_2(1, f_2, g_2, k_2)$ będą dwoma okręgami. Dla dowolnych $a_1, a_2 \in \mathbb{R}, a_1 + a_2 \neq 0$, określamy:

$$C = \frac{a_1 C_1 + a_2 C_2}{a_1 + a_2},$$

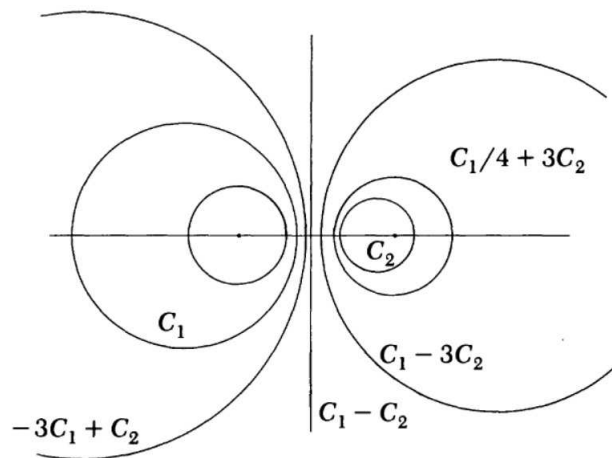
czyli okrąg o środku:

$$\left(\frac{a_1 f_1 + a_2 f_2}{a_1 + a_2}, \frac{a_1 g_1 + a_2 g_2}{a_1 + a_2} \right).$$

Jeśli $a_1 + a_2 = 0$, to zbiór $C = a_1 C_1 + a_2 C_2$ jest prostą, zwaną PROSTĄ POTĘGOWĄ okręgów C_1, C_2 , zaś zbiór okręgów

$$C = a_1 C_1 + a_2 C_2$$

(gdzie $a_1 \neq 0$ lub $a_2 \neq 0$) nazywamy **współosiowym pękiem okręgów**. Zbiór ten odpowiada $\text{lin}(C_1, C_2)$ w przestrzeni \mathbb{R}^4 .

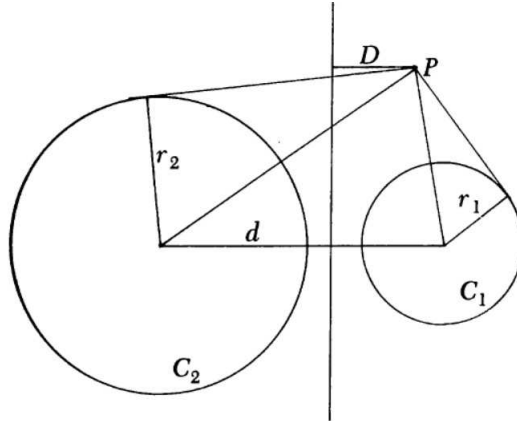


Obserwacja 22.3

Dla każdego punktu P oraz okręgów C_1, C_2 niech D będzie odległością od P do osi potęgowej $C_1 - C_2$ i niech d będzie odległością pomiędzy środkami C_1, C_2 . Wówczas:

$$2Dd = (d_1^2 - r_1^2) - (d_2^2 - r_2^2),$$

jest różnicą potęg punktu P względem C_1 i C_2 .



Dowód. Na mocy własności (vii) oraz (iv) mamy:

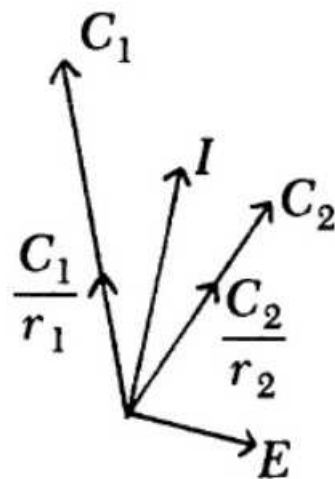
$$-D = \left\langle P, \frac{C_1 - C_2}{d} \right\rangle = (\langle P, C_1 \rangle - \langle P, C_2 \rangle) / d = (-(d_1^2 - r_1^2) + (d_2^2 - r_2^2)) / 2d.$$

□

Dwusieczne. Skoro $\langle C, C \rangle = r^2$, to dla okręgów C_1, C_2 o promieniach r_1, r_2 można określić wektory jednostkowe $C_1/r_1, C_2/r_2$. Przez analogię do zwykłych wektorów w przestrzeni euklidesowej można określić

$$I = C_1/r_1 + C_2/r_2, \quad E = C_1/r_1 - C_2/r_2.$$

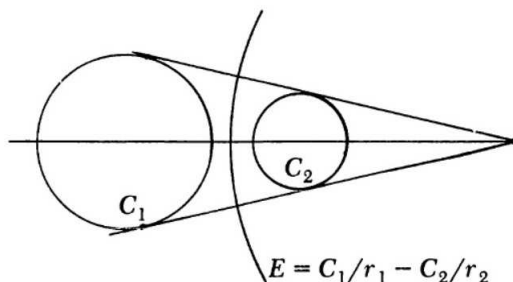
nazywane **wewnętrznym i zewnętrznym okręgiem antypodobieństwa** okręgów C_1, C_2 . Z punktów (viii), (ix) dowodzi się łatwo, że środki I oraz E leżą w punktach, w których przecinają się odpowiednio wewnętrzne i zewnętrzne wspólne styczne do C_1, C_2 (dla prostych są to: **dwusieczna wewnętrzna i zewnętrzna!**).



Inwersja. Odbicie u' wektora U względem V (lub równoległe do V) dane jest formułą:

$$U' = \pm \frac{2\langle U, V \rangle}{\langle V, V \rangle} V \mp U.$$

i jak się okazuje w języku rozważanego iloczynu skalarnego U' jest obrazem inwersyjnym okręgu U względem okręgu V . Dla przykładu, odbicie wektora C_1 względem wektorów I, E daje wektory $C_2, -C_2$ (z dokładnością do skalarnej wielokrotności), więc inwersja C_1 w okręgach I, E daje okrąg C_2 .



Liniowa niezależność. Okręgi C_i są liniowo niezależne jeśli $\sum x_i C_i = 0$ wtedy i tylko wtedy, gdy $x_i = 0$, dla wszystkich i . W szczególności trzy okręgi są liniowo niezależne jeśli żaden nie leży w pęku współosiowym pozostałych dwóch.

Obserwacja 22.4: Tw. Menelaosa

Dane są trzy liniowo niezależne okręgi C_1, C_2, C_3 . Jeśli

$$D_1 = a_1 C_2 + b_1 C_3, \quad D_2 = a_2 C_3 + b_2 C_1, \quad D_3 = a_3 C_1 + b_3 C_2,$$

wówczas D_1, D_2, D_3 są zależne (w tym samym pęku współosiowym) wtedy i tylko wtedy, gdy

$$a_1 a_2 a_3 = -b_1 b_2 b_3.$$

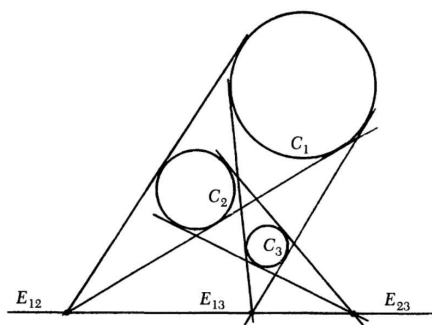
Dowód. Istnieją niezerowe x_i spełniające $\sum x_i D_i = 0$ wtedy i tylko wtedy, gdy poniższy układ ma niezerowe rozwiązanie:

$$\begin{bmatrix} 0 & b_2 & a_3 \\ a_1 & 0 & b_3 \\ b_1 & a_2 & 0 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

□

Obserwacja 22.5: Tw. Monge'a

Niech C_1, C_2, C_3 będą liniowo niezależnymi okręgami i niech I_{ij}, E_{ij} będą wewnętrznymi i zewnętrznymi okręgami antypodobieństwa dla C_i oraz C_j . Wówczas każdy z czterech układów okręgów jest liniowo zależny (czyli współpękowy): $\{E_{12}, E_{23}, E_{31}\}, \{E_{12}, I_{23}, I_{31}\}, \{I_{12}, E_{23}, I_{31}\}, \{I_{12}, I_{23}, E_{31}\}$. W szczególności środki okręgów w każdym układzie są współliniowe.



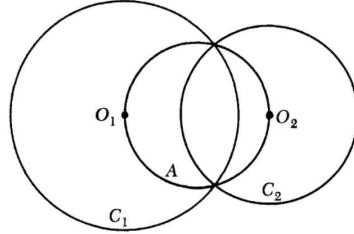
Obserwacja 22.6

Niech C_1 będzie ortogonalny do C_2 i niech okręgi te mają środki O_1, O_2 . Rozważmy **okrąg średni** postaci:

$$A = \frac{C_1 + C_2}{2}.$$

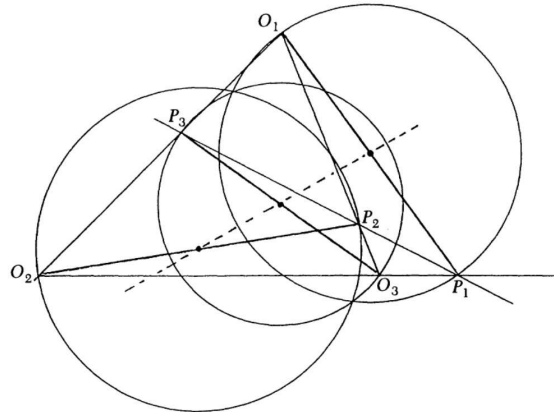
Wówczas O_1O_2 to średnica A , ponieważ (patrz (ix)):

$$\langle O_i, C_i \rangle = r_i^2/2, \quad \langle O_i, C_j \rangle = -r_i^2/2 \quad \Rightarrow \langle O_i, A \rangle = 0.$$



Obserwacja 22.7

Niech C_1, C_2, C_3 będą trzema wzajemnie prostymi okręgami o środkach O_1, O_2, O_3 . Załóżmy, że (znormalizowane) okręgi D_1, D_2, D_3 zdefiniowane jak w twierdzeniu Menelaosa, o środkach P_1, P_2, P_3 są zależne i niech A_i będą średnimi okręgami okręgów C_i oraz D_i . Wówczas okręgi A_1, A_2, A_3 są zależne (uzyskujemy m.in. tw. Gaussa-Bodenmüllera czy tw. Newtona).



Dysponując liniowo zależnym układem wektorów $\sum x_i V_i = 0$ i biorąc formę $\langle \cdot, \cdot \rangle$ z każdym z wektorów W_i widzimy, że istnieje niezerowe rozwiązanie układu:

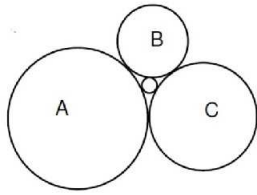
$$\begin{bmatrix} \langle W_1, V_1 \rangle & \dots & \langle W_1, V_n \rangle \\ \vdots & & \vdots \\ \langle W_n, V_1 \rangle & \dots & \langle W_n, V_n \rangle \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Dla $W_i = V_i$ widzimy, że wyznacznik Grama tego układu jest zerowy.

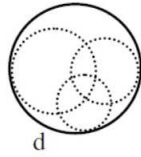
- **Wniosek 1.** Nie istnieją cztery parami prostopadłe okręgi — twierdzenie o bezwładności!
- **Wniosek 2.** Biorąc układ czterech parami stycznych zewnętrznie okręgów C_1, C_2, C_3, C_4 o promieniach r_1, r_2, r_3, r_4 oraz $C_5 = E$ warunek $W(C_i) = 0$ implikuje słynne twierdzenie Kartezjusza o okręgach:

$$\frac{1}{r_1^2} + \frac{1}{r_2^2} + \frac{1}{r_3^2} + \frac{1}{r_4^2} = \frac{1}{r_1 r_2} + \frac{1}{r_1 r_3} + \frac{1}{r_1 r_4} + \frac{1}{r_2 r_3} + \frac{1}{r_2 r_4} + \frac{1}{r_3 r_4}.$$

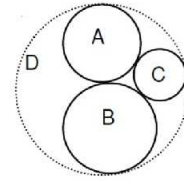
Macierze Grama² układów okręgów stycznych w różnych dopuszczalnych konfiguracjach.



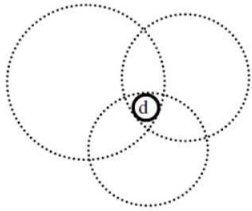
$$f = \begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix}$$



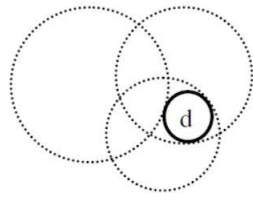
$$f = \begin{bmatrix} -1 & 0 & 0 & -1 \\ 0 & -1 & 0 & -1 \\ 0 & 0 & -1 & -1 \\ -1 & -1 & -1 & -1 \end{bmatrix}$$



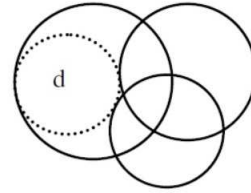
$$f = \begin{bmatrix} -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ -1 & -1 & -1 & -1 \end{bmatrix}$$



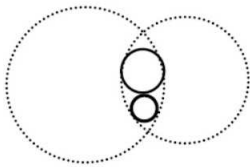
$$f = \begin{bmatrix} -1 & 0 & 0 & 1 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix}$$



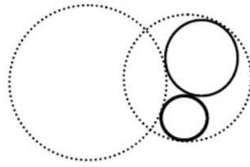
$$f = \begin{bmatrix} -1 & 0 & 0 & 1 \\ 0 & -1 & 0 & -1 \\ 0 & 0 & -1 & -1 \\ 1 & -1 & -1 & -1 \end{bmatrix}$$



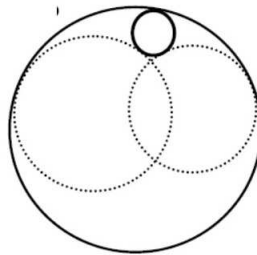
$$f = \begin{bmatrix} -1 & 0 & 0 & -1 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & -1 & 1 \\ -1 & 1 & 1 & -1 \end{bmatrix}$$



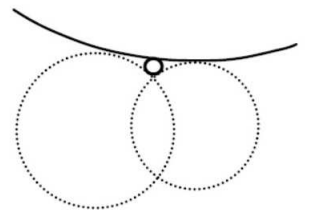
$$f = \begin{bmatrix} -1 & 0 & -1 & -1 \\ 0 & -1 & -1 & -1 \\ -1 & -1 & -1 & 1 \\ -1 & -1 & 1 & -1 \end{bmatrix}$$



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



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



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

²W cytowanej pracy iloczyn skalarny jest z przeciwnym znakiem niż u nas, czyli $\langle C_1, C_2 \rangle = (d_1 a_1 + d_2 a_2)/2 - b_1 b_2 - c_1 c_2$ i rozważa się go jedynie na czwórkach wektorów jednostkowych (można, po odpowiednim przeskalowaniu).

Rozdział 23

Formy kwadratowe

Dzisiejszy wykład stanowi kulminację rozważań dotyczących przestrzeni dwuliniowych. Formy kwadratowe badano na długo zanim powstała algebra liniowa, zwłaszcza w teorii liczb.

Definicja 23.1: Forma kwadratowa na przestrzeni liniowej

Niech V będzie przestrzenią liniową nad ciałem K . Funkcję $q : V \rightarrow K$ nazywamy FORMĄ KWADRATOWĄ NA PRZESTRZENI V , jeśli istnieje forma dwuliniowa $h : V \times V \rightarrow K$ taka, że dla każdego $\alpha \in V$ zachodzi

$$q(\alpha) = h(\alpha, \alpha).$$

Oto przykłady form kwadratowych na przestrzeni \mathbb{R}^2 oraz \mathbb{R}^3 :

$$\begin{aligned}q_1((x_1, x_2)) &= 2x_1^2 + 3x_1x_2 - 5x_2^2 \\q_2((x_1, x_2, x_3)) &= x_1^2 + 4x_1x_2 + 7x_2^2 - 6x_2x_3 + 3x_3^2.\end{aligned}$$

Obserwacja 23.1

Niech V będzie skończenie wymiarową przestrzenią liniową nad K i niech $(\alpha_1, \dots, \alpha_n)$ będzie bazą przestrzeni V . Następujące warunki są równoważne.

- funkcja $q : V \rightarrow K$ jest formą kwadratową na przestrzeni V ,
- istnieją elementy $a_{ij} \in K$, dla $i, j = 1, \dots, n$ takie, że dla każdych skalarów x_1, \dots, x_n z ciała K zachodzi równość:

$$q(x_1\alpha_1 + \dots + x_n\alpha_n) = \sum_{i,j=1}^n a_{ij}x_ix_j.$$

Dowód. Niech $q(\alpha) = h(\alpha, \alpha)$, dla pewnej formy dwuliniowej h na V . Niech $a_{ij} = h(\alpha_i, \alpha_j)$, dla $i, j = 1, \dots, n$. Dla $x_1, \dots, x_n, y_1, \dots, y_n \in K$ mamy:

$$h(x_1\alpha_1 + \dots + x_n\alpha_n, y_1\alpha_1 + \dots + y_n\alpha_n) = \sum_{i,j=1}^n a_{ij}x_iy_j,$$

więc w szczególności $q(x_1\alpha_1 + \dots + x_n\alpha_n) = \sum_{i,j=1}^n a_{ij}x_ix_j$.

Na odwrót: mając $q(x_1\alpha_1 + \dots + x_n\alpha_n) = \sum_{i,j=1}^n a_{ij}x_ix_j$ dla każdych $x_1, \dots, x_n \in K$ zadajemy formę dwuliniową h wzorem

$$h(x_1\alpha_1 + \dots + x_n\alpha_n, y_1\alpha_1 + \dots + y_n\alpha_n) = \sum_{i,j=1}^n a_{ij}x_iy_j.$$

Wówczas dla każdego $\alpha = x_1\alpha_1 + \dots + x_n\alpha_n$ mamy $h(\alpha, \alpha) = q(\alpha)$. □

Przyjmując $b_{ii} = a_{ii}$ dla $i = 1, \dots, n$ oraz $b_{ij} = a_{ij} + a_{ji}$ dla $1 \leq i, j \leq n$ w powyższej uwadze możemy ją przeformułować następująco.

Obserwacja 23.2

Niech V będzie skończenie wymiarową przestrzenią liniową nad K i niech $(\alpha_1, \dots, \alpha_n)$ będzie bazą przestrzeni V . Wówczas funkcja $q : V \rightarrow K$ jest formą kwadratową na przestrzeni V wtedy i tylko wtedy, gdy istnieją elementy $b_{ij} \in K$, dla $i, j = 1, \dots, n$ takie, że dla każdych $x_1, \dots, x_n \in K$:

$$q(x_1\alpha_1 + \dots + x_n\alpha_n) = \sum_{1 \leq i \leq j \leq n} b_{ij}x_i x_j.$$

Proste wnioski:

- Każda forma kwadratowa na przestrzeni K^n jest postaci:

$$q((x_1, \dots, x_n)) = \sum_{1 \leq i \leq j \leq n} b_{ij}x_i x_j,$$

- Jeśli $q : V \rightarrow K$ jest formą kwadratową na przestrzeni V , to dla każdej podprzestrzeni liniowej $W \subseteq V$ funkcja $q|_W : W \rightarrow K$, zadana jako $q|_W(\alpha) = q(w)$ dla każdego $\alpha \in W$, jest formą kwadratową na przestrzeni W .

Szczególnie interesujące jest szukanie baz, w której formę kwadratową można zapisać w postaci diagonalnej. Podstawową motywacją jest tu pytanie o to kiedy forma dwuliniowa jest iloczynem skalarnym, więc jest dodatnio określona. W istocie zagadnienie to sprowadza się do zbadania czy pewna forma kwadratowa może być zapisana w postaci sumy kwadratów. Na przykład forma na \mathbb{R}^3 dana wzorem

$$h((x_1, x_2, x_3), (y_1, y_2, y_3)) = x_1y_1 + x_1y_2 + x_2y_1 + 2x_2y_2 + 4x_3y_3,$$

jest iloczynem skalarnym, bowiem związana z nią forma kwadratowa ma postać:

$$h((x_1, x_2, x_3), (x_1, x_2, x_3)) = x_1^2 + 2x_1x_2 + 2x_2^2 + 4x_3^2 = (x_1 + x_2)^2 + x_2^2 + 4x_3^2$$

Definicja 23.2: Postać diagonalna formy kwadratowej

Niech $q : V \rightarrow K$ będzie formą kwadratową. POSTACIĄ DIAGONALNĄ FORMY KWADRATOWEJ q nazwiemy przedstawienie jej w formie:

$$q(x_1\alpha_1 + \dots + x_n\alpha_n) = a_1x_1^2 + a_2x_2^2 + \dots + a_nx_n^2,$$

gdzie $(\alpha_1, \dots, \alpha_n)$ jest pewną bazą przestrzeni V oraz $a_1, \dots, a_n \in K$.

Przykład. Niech

$$q((x_1, x_2, x_3, x_4)) = x_1^2 + 8x_1x_2 + 7x_2^2 + 2x_3x_4.$$

Forma q określona jest na \mathbb{R}^4 , a zapisany wzór oparty jest o współrzędne wektora w bazie standardowej. Rozważmy bazę

$$\alpha_1 = (1, 0, 0, 0), \quad \alpha_2 = (4, -1, 0, 0), \quad \alpha_3 = (0, 0, 1, 1), \quad \alpha_4 = (0, 0, 1, -1).$$

Jest to baza ortogonalna w (\mathbb{R}^4, h) , gdzie h jest symetryczna i $h(\alpha, \alpha) = q(\alpha)$, dla każdego α (to wyjaśnię niżej). Wówczas forma q zapisywać się będzie wzorem:

$$q((y_1\alpha_1 + y_2\alpha_2 + y_3\alpha_3 + y_4\alpha_4)) = y_1^2 - 9y_2^2 + 2y_3^2 - 2y_4^2.$$

Chcemy mieć narzędzia do rozróżniania określoności (zawsze diagonalizowalnych) form rzeczywistych, a dla dowolnego ciała – do diagonalizacji form kwadratowych i do stwierdzania kiedy ta ostatnia jest możliwa. Dla ciał charakterystyki różnej od 2 istnieje bardzo bliski związek pomiędzy formami kwadratowymi i symetrycznymi formami dwuliniowymi. Mówi o tym następujące stwierdzenie.

Obserwacja 23.3

Niech V będzie przestrzenią liniową nad ciałem K charakterystyki różnej od 2. Jeśli $q : V \rightarrow K$ jest formą kwadratową, to istnieje dokładnie jedna forma dwuliniowa symetryczna $h : V \times V \rightarrow K$ taka, że dla każdego $\alpha \in V$ zachodzi $q(\alpha) = h(\alpha, \alpha)$. Dokładniej, dla ciała charakterystyki różnej od 2 przyporządkowania:

- $h \mapsto q$, gdzie $q(\alpha) = h(\alpha, \alpha)$, dla każdego $\alpha \in V$,
- $q \mapsto h$, gdzie $h(\alpha, \beta) = \frac{1}{2}(q(\alpha + \beta) - q(\alpha) - q(\beta))$

zadają bijekcje pomiędzy formami dwuliniowymi symetrycznymi na przestrzeni V a formami kwadratowymi na przestrzeni V .

Zanim zobaczymy dowód zobaczymy krótki przykład. Weźmy formę kwadratową $q : \mathbb{R}^2 \rightarrow \mathbb{R}$ daną wzorem

$$q((x_1, x_2)) = 3x_1^2 - 4x_2^2 + 6x_1x_2.$$

Istnieje naturalnie wiele form dwuliniowych $h : \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}$ takich, że $q(\alpha) = h(\alpha, \alpha)$, dla każdego $\alpha \in V$, na przykład

$$h((x_1, x_2), (y_1, y_2)) = 3x_1y_1 + 2x_1y_2 + 4x_2y_1 - 4x_2y_2$$

lub

$$h((x_1, x_2), (y_1, y_2)) = 3x_1y_1 + 6x_1y_2 - 4x_2y_2.$$

ale istnieje wśród nich tylko jedna forma dwuliniowa symetryczna, mianowicie

$$h((x_1, x_2), (y_1, y_2)) = 3x_1y_1 + 3x_1y_2 + 3x_2y_1 - 4x_2y_2.$$

Dowód. Niech $h' : V \times V \rightarrow K$ będzie dowolną formą dwuliniową taką, że dla każdego $\alpha \in V$ zachodzi $q(\alpha) = h'(\alpha, \alpha)$. Wówczas funkcja $h : V \times V \rightarrow K$ zadana warunkami $h(\alpha, \beta) = \frac{1}{2}(h'(\alpha, \beta) + h'(\beta, \alpha))$ jest formą dwuliniową symetryczną na przestrzeni V i mamy równość $q(\alpha) = h'(\alpha, \alpha) = h(\alpha, \alpha)$, dla każdego $\alpha \in V$. To dowodzi istnienia żądanej formy dwuliniowej symetrycznej h . Aby wykazać jej jednoznaczność zauważmy, że jeśli h jest formą dwuliniową symetryczną spełniającą $q(\alpha) = h(\alpha, \alpha)$ dla każdego $\alpha \in V$, to dla każdych $\alpha, \beta \in V$ mamy

$$\frac{1}{2}(q(\alpha + \beta) - q(\alpha) - q(\beta)) = \frac{1}{2}(h(\alpha + \beta, \alpha + \beta) - h(\alpha, \alpha) - h(\beta, \beta)) = h(\alpha, \beta),$$

czyli h jest wyznaczona jednoznacznie przez q . □

* * *

Odtąd, aż do końca wykładu zakładamy, że ciało K jest charakterystyki różnej od 2.

* * *

Definicja 23.3: Macierz formy kwadratowej

Niech $q : V \rightarrow K$ będzie formą kwadratową na skończonej wymiarowej przestrzeni liniowej. MACIERZĄ FORMY KWADRATOWEJ q w bazie \mathcal{A} przestrzeni V nazywamy macierz formy dwuliniowej symetrycznej odpowiadającą formie q . Macierz formy kwadratowej q w bazie \mathcal{A} oznaczamy $G(q; \mathcal{A})$.

Zatem $G(q; \mathcal{A}) = G(h; \mathcal{A})$ gdzie $h : V \times V \rightarrow K$ jest formą dwuliniową symetryczną spełniającą $q(\alpha) = h(\alpha, \alpha)$, dla każdego $\alpha \in V$.

Przykład. Dla formy $q : K^n \rightarrow K$ zadanej wzorem $q((x_1, \dots, x_n)) = x_1^2 + \dots + x_n^2$ mamy $G(q; st) = I$. Dla formy $q : \mathbb{R}^2 \rightarrow \mathbb{R}$ zadanej wzorem $q((x_1, x_2)) = x_1^2 + 3x_1x_2 + 7x_2^2$ mamy

$$G(q; st) = \begin{bmatrix} 1 & \frac{3}{2} \\ \frac{3}{2} & 7 \end{bmatrix},$$

a w bazie $\mathcal{A} = ((1, 1), (1, -1))$ mamy $G(q; \mathcal{A}) = \begin{bmatrix} 11 & -6 \\ -6 & 5 \end{bmatrix}$.

Opis form kwadratowych w języku form dwuliniowych symetrycznych uruchamia całą maszynię i rezultaty uzyskane wcześniej. W szczególności mamy następujące własności macierzy form kwadratowych.

Obserwacja 23.4

Niech Q będzie formą kwadratową na skończonej wymiarowej przestrzeni liniowej V nad ciałem K .

- Jeśli $A = [a_{ij}]$ jest macierzą formy kwadratowej q w bazie $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$, to dla dowolnych elementów $x_1, \dots, x_n \in K$ zachodzi równość $q(x_1\alpha_1 + \dots + x_n\alpha_n) = \sum_{i,j=1}^n a_{ij}x_ix_j$.
- Jeśli A, B są macierzami formy kwadratowej q w bazach \mathcal{A}, \mathcal{B} odpowiednio, to $B = C^T A C$, gdzie $C = M(\text{id})_{\mathcal{B}}^{\mathcal{A}}$.
- Jeśli charakterystyka ciała K jest różna od 2 istnieje taka baza, w której macierz q ma macierz diagonalną, czyli taka baza $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$ przestrzeni V , że zachodzi równość $q(x_1\alpha_1 + \dots + x_n\alpha_n) = a_1x_1^2 + a_2x_2^2 + \dots + a_nx_n^2$.

Na ćwiczeniach będziecie Państwo stosować różne sposoby na diagonalizację formy q . Oto one:

- szukanie bazy prostopadłej przestrzeni dwuliniowej (V, h) , gdzie h jest formą symetryczną odpowiadającą formie kwadratowej q ,
- szukanie bazy ortonormalnej złożonej z wektorów własnych rzeczywistej macierzy symetrycznej $A = G(h; st)$ w przestrzeni euklidesowej ze standardowym iloczynem skalarnym (tutaj $K = \mathbb{R}$),
- intuicyjna metoda uzupełniania do kwadratów (jest ona opisana w skrypcie i na pewno będzie wspomniana na ćwiczeniach, choć powyższe dwie w zupełności wystarczają do diagonalizacji).

Definicja 23.4: Równoważność form kwadratowych

Mówimy, że formy kwadratowe $q_1 : V_1 \rightarrow K, q_2 : V_2 \rightarrow K$ są RÓWNOWAŻNE, jeśli istnieją bazy \mathcal{A}_1 przestrzeni V_1 oraz \mathcal{A}_2 przestrzeni V_2 takie, że $G(q_1; \mathcal{A}_1) = G(q_2; \mathcal{A}_2)$.

Istotną motywacją dla pojęcia równoważności jest możliwość stosowania podstawień liniowych.

Obserwacja 23.5

Niech $f = f(x_1, \dots, x_n)$ oraz $g = g(y_1, \dots, y_n)$ będą formami kwadratowymi na skończonej wymiarowej przestrzeni V nad ciałem K . Formy f, g są równoważne, jeśli istnieje macierz odwracalna $P \in M_n(K)$ o wyrazach p_{ij} taka, że

$$\begin{aligned} x_1 &= p_{11}y_1 + p_{12}y_2 + \dots + p_{1n}y_n \\ &\vdots \quad \quad \quad \vdots \quad \quad \quad \ddots \quad \quad \quad \vdots \\ x_n &= p_{n1}y_1 + p_{n2}y_2 + \dots + p_{nn}y_n, \end{aligned}$$

że $f(x_1, \dots, x_n) = g(y_1, \dots, y_n)$, dla dowolnych $y_j \in K$.

Przykład. Następujące formy są równoważne nad \mathbb{R}^4 :

$$q_1((x_1, x_2, x_3, x_4)) = x_1^2 + 8x_1x_2 + 7x_2^2 + 2x_3x_4, \quad q_2((y_1, y_2, y_3, y_4)) = y_1^2 - 9y_2^2 + 2y_3^2 - 2y_4^2.$$

bo $q_1(y_1 - 4y_2, y_2, y_3 + y_4, y_3 - y_4)$ równe jest

$$(y_1 - 4y_2)^2 + 8(y_1 - 4y_2)y_2 + 7(y_2)^2 + 2(y_3 + y_4)(y_3 - y_4) = y_1^2 - 9y_2^2 + 2y_3^2 - 2y_4^2.$$

Dowód. Jeśli przyjąć $X = [x_1 \ \dots \ x_n]^T, Y = [y_1 \ \dots \ y_n]^T$, to układ wyżej ma postać $X = PY$. W szczególności — jeśli $f(X) = X^T G(f; \mathcal{B}) X$, dla pewnej bazy \mathcal{B} przestrzeni K^n , to biorąc bazę \mathcal{A} przestrzeni K^n taką, że $M(\text{id})_{\mathcal{A}}^{\mathcal{B}} = P$ mamy:

$$g(Y) = f(X) = f(PY) = (PY)^T \cdot G(f; \mathcal{B}) \cdot PY = Y^T \cdot P^T \cdot G(f; \mathcal{B}) \cdot P \cdot Y = Y^T \cdot G(f, \mathcal{A}) \cdot Y.$$

□

Twierdzenie 23.1: Lagrange

Niech V będzie przestrzenią nad ciałem K charakterystyki różnej od 2 o bazie $\mathcal{B} = (\beta_1, \dots, \beta_n)$ oraz niech forma kwadratowa q zapisuje się w bazie \mathcal{B} macierzą $G(q, \mathcal{B}) = [b_{ij}]$, czyli

$$q(x_1\beta_1 + \dots + x_n\beta_n) = \sum_{i,j=1}^n b_{ij}x_ix_j.$$

Wówczas można wskazać taką zamianę zmiennych $X = PY$, że dla bazy $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$ przestrzeni V spełniającej $P = M(\text{id})_{\mathcal{A}}^{\mathcal{B}}$ mamy $q(y_1\alpha_1 + \dots + y_n\alpha_n) = a_1y_1^2 + \dots + a_ny_n^2$.

Dowód. Indukcja po wymiarze V . Dla $n = 1$ jest jasne. Załóżmy, że opisałiśmy metodę dla $\dim V \leq n - 1$. Niech $\dim V = n$. Rozważamy dwa przypadki:

- Przypadek 1. Istnieje i takie, że $b_{ii} \neq 0$.
- Przypadek 2. Dla każdego i mamy $b_{ii} = 0$.

W przypadku pierwszym można bez straty ogólności założyć, że $b_{11} \neq 0$. Mamy $b_{ij} = b_{ji}$, czyli:

$$\begin{aligned} q\left(\sum_{i=1}^n x_i\beta_i\right) &= \sum_{i,j=1}^n b_{ij}x_ix_j = b_{11}x_1^2 + 2b_{12}x_1x_2 + \dots + 2b_{1n}x_1x_n + \sum_{i,j=2}^n b_{ij}x_ix_j = \\ &= \frac{1}{b_{11}}(b_{11}x_1 + b_{12}x_2 + \dots + b_{1n}x_n)^2 + \sum_{i,j=2}^n b'_{ij}x_ix_j = \\ &= \frac{1}{b_{11}}y_1^2 + \sum_{i,j=2}^n b'_{ij}y_iy_j \end{aligned}$$

dla pewnych $b'_{ij} \in K$ oraz $y_1 = b_{11}x_1 + \dots + b_{1n}x_n$, $y_j = x_j$, dla $j > 1$ (czyli zmieniliśmy bazę β_1, \dots, β_n na bazę $\gamma_1, \dots, \gamma_n$ zadaną warunkami $\beta_1 = b_{11}\gamma_1$, $\beta_2 = b_{12}\gamma_1 + \gamma_2, \dots, \beta_n = b_{1n}\gamma_1 + \gamma_n$, co daje $\sum_{i=1}^n x_i\beta_i = \sum_{i=1}^n y_i\gamma_i$). Dalszy ciąg wynika z założenia indukcyjnego.

Przypadek 2. Dla każdego i mamy $b_{ii} = 0$. Jeśli $b_{ij} = 0$ to q jest zerowa i teza jest oczywista. Załóżmy (bsog), że $b_{12} \neq 0$. Wtedy podstawiając:

$$x_1 = y_1 + y_2, x_2 = y_1 - y_2, x_3 = y_3, \dots, x_n = y_n,$$

(czyli zmieniając bazę β_1, \dots, β_n na bazę $\gamma_1, \dots, \gamma_n$ zadaną warunkami $\gamma_1 = \beta_1 + \beta_2$, $\gamma_2 = \beta_1 - \beta_2$ oraz $\gamma_i = \beta_i$, dla $i > 2$), dostajemy $c_{ij} \in K$ takie, że:

$$q\left(\sum_{i=1}^n y_i\gamma_i\right) = \sum_{i,j=1}^n c_{ij}y_iy_j,$$

przy czym $c_{11} = b_{12} \neq 0$, co sprowadza tezę do Przypadku 1. □

Definicja 23.5: Określoność formy kwadratowej

Mówimy, że forma kwadratowa kwadratowej) $q : V \rightarrow \mathbb{R}$ jest

- DODATNIO OKREŚLONA, jeśli $q(\alpha) > 0$, dla każdego niezerowego $\alpha \in V$,
- UJEMNIE OKREŚLONA, jeśli $q(\alpha) < 0$, dla każdego niezerowego $\alpha \in V$,
- DODATNIO PÓŁOKREŚLONA, jeśli $q(\alpha) \geq 0$, dla każdego wektora $\alpha \in V$,
- UJEMNIE PÓŁOKREŚLONA, jeśli $q(\alpha) \leq 0$, dla każdego wektora $\alpha \in V$,
- NIEOKREŚLONA, jeśli istnieją $\alpha, \beta \in V$ takie, że $q(\alpha) > 0$ oraz $q(\beta) < 0$.

Powyższym pojęciom odpowiadają analogiczne dotyczące macierzy form.

Definicja 23.6

Mówimy, że symetryczna macierz kwadratowa $A \in M_n(\mathbb{R})$ jest

- DODATNIO OKREŚLONA, jeśli $v^T Av > 0$, dla każdego $v \in \mathbb{R}^n \setminus \{0\}$,
- UJEMNIE OKREŚLONA, jeśli $v^T Av < 0$, dla każdego $v \in \mathbb{R}^n \setminus \{0\}$,
- DODATNIO PÓŁOKREŚLONA, jeśli $v^T Av \geq 0$, dla każdego $v \in \mathbb{R}^n$,
- UJEMNIE PÓŁOKREŚLONA, jeśli $v^T Av \leq 0$, dla każdego $v \in \mathbb{R}^n$,
- NIEOKREŚLONA, jeśli istnieją $v, w \in \mathbb{R}^n$, takie, że $v^T Av > 0$ oraz $w^T Aw < 0$.

Określoność formy ma duży związek z jej postacią diagonalną.

Wniosek 23.1

Jeśli rzeczywista forma kwadratowa q ma w bazie $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$ postać diagonalną daną wzorem

$$q(x_1\alpha_1 + \dots + x_n\alpha_n) = a_1x_1^2 + a_2x_2^2 + \dots + a_nx_n^2,$$

dla pewnych $a_1, \dots, a_n \in \mathbb{R}$, to forma q jest:

- DODATNIO OKREŚLONA $\iff a_i > 0$, dla $i = 1, \dots, n$.
- UJEMNIE OKREŚLONA $\iff a_i < 0$, dla $i = 1, \dots, n$.
- DODATNIO PÓŁOKREŚLONA $\iff a_i \geq 0$, dla $i = 1, \dots, n$.
- UJEMNIE PÓŁOKREŚLONA $\iff a_i \leq 0$, dla $i = 1, \dots, n$.
- NIEOKREŚLONA \iff istnieją $1 \leq i, j \leq n$ takie, że $a_i > 0$ oraz $a_j < 0$.

Badanie określoności rzeczywistej formy kwadratowej opiera się na kryterium Sylwestera.

Twierdzenie 23.2

Niech $q : V \rightarrow \mathbb{R}$ będzie rzeczywistą formą kwadratową mającą w bazie \mathcal{A} przestrzeni V macierz $G(q; \mathcal{A}) = A \in M_{n \times n}(\mathbb{R})$. Wówczas forma q jest:

- DODATNIO OKREŚLONA $\iff \det A^{(i)} > 0$, dla $i = 1, \dots, n$.
- UJEMNIE OKREŚLONA $\iff (-1)^i \det A^{(i)} > 0$, dla $i = 1, \dots, n$.

Twierdzenia klasyfikacyjne dla form dwuliniowych i macierzy symetrycznych przenoszą się na formy kwadratowe.

Definicja 23.7

RZĘDEM FORMY KWADRATOWEJ (odpowiednio: SYGNATURĄ, w przypadku ciała \mathbb{R}) nazywamy rząd (sygnaturę) odpowiadającą jej formy dwuliniowej symetrycznej.

Obserwacja 23.6

Formy kwadratowe $q_1 : V_1 \rightarrow K$ oraz $q_2 : V_2 \rightarrow K$ są równoważne wtedy i tylko wtedy, gdy dla każdej bazy \mathcal{A}_1 przestrzeni V_1 oraz każdej bazy \mathcal{A}_2 przestrzeni V_2 macierze $G(q_1; \mathcal{A}_1)$, $G(q_2; \mathcal{A}_2)$ są kongruentne nad K .

Obserwacja 23.7

Każda forma kwadratowa na n wymiarowej przestrzeni liniowej nad \mathbb{C} jest równoważna formie $q : \mathbb{C}^n \rightarrow \mathbb{C}$ postaci

$$q((x_1, \dots, x_n)) = x_1^2 + \dots + x_r^2,$$

dla pewnego $0 \leq r \leq n$. Formy kwadratowe $q_1 : \mathbb{C}^n \rightarrow \mathbb{C}$, $q_2 : \mathbb{C}^n \rightarrow \mathbb{C}$ są równoważne wtedy i tylko wtedy, gdy mają równe rzędy.

Obserwacja 23.8

Każda forma kwadratowa na n wymiarowej przestrzeni liniowej nad \mathbb{R} jest równoważna formie $q : \mathbb{R}^n \rightarrow \mathbb{R}$ postaci

$$q((x_1, \dots, x_n)) = x_1^2 + \dots + x_r^2 - x_{r+1}^2 - \dots - x_{r+s}^2,$$

dla pewnych $r, s \geq 0$, $r + s \leq n$. Formy kwadratowe $q_1 : \mathbb{R}^n \rightarrow \mathbb{R}$, $q_2 : \mathbb{R}^n \rightarrow \mathbb{R}$ są równoważne wtedy i tylko wtedy, gdy mają równe rzędy i sygnatury.

Poniżej jeden bardziej zaawansowany przykład pokazujący, że wyznaczenie sygnatury może być łatwiejsze za pomocą wartości własnych.

Zadanie 23.1. Wykaż, że sygnatura macierzy $A_n = (a_{ij}) \in M_n(\mathbb{R})$ równa jest 0, gdzie:

$$a_{ij} = \begin{cases} 0, & |i - j| \neq 1, \\ \min(i, j), & |i - j| = 1. \end{cases}$$

ROZWIĄZANIE. Mamy:

$$A_n = \begin{bmatrix} 0 & 1 & & & \\ 1 & 0 & 2 & & \\ & 2 & 0 & \ddots & \\ & & \ddots & \ddots & n-1 \\ & & & n-1 & 0 \end{bmatrix},$$

więc nietrudno pokazać, że kładąc $f_n(\lambda) = \det(\lambda I_n - A_n)$ mamy

$$f_{n+1}(\lambda) = \lambda f_n(\lambda) - n^2 f_{n-1}(\lambda), \quad (\heartsuit)$$

przy czym $f_0 = 1$ oraz (formalnie weźmy) $f_{-1} = 0$. Twierdzimy, że stopień każdego jednomianu w f_n ma taką samą parzystość jak n oraz, że f_n ma niezerowy wyraz stopnia k dla wszystkich $1 \leq k \leq n$, że $k \equiv n \pmod{2}$, na przykład: $f_4(\lambda) = \lambda^4 - 14\lambda^2 - 9$. Dowód to łatwa indukcja korzystający z formuły (\heartsuit) .

Jeśli n jest parzyste, wówczas $f_n(0) \neq 0$ (bo wielomian ma niezerowy wyraz wolny). Co więcej mamy $f_n(\lambda) = 0 \iff f_n(-\lambda) = 0$, więc A_n nie ma wartości własnej 0 oraz ma po $n/2$ dodatnich i ujemnych wartości własnych. Jej sygnatura wynosi więc 0.

Jeśli n jest nieparzyste, wówczas $f_n(0) = 0$ oraz jeśli przyjmiemy

$$f_n(\lambda) = \lambda \cdot g_n(\lambda),$$

to g_n ma stopień parzysty i jedyne jego niezerowe wyrazy są parzystego stopnia. A zatem g_n ma dokładnie $(n-1)/2$ ujemnych i dodatnich wartości własnych (i nie ma zerowej). A zatem macierz A_n ma tyle samo dodatnich i ujemnych wartości własnych. ■

Na tym kończy się część wykładu dotycząca wprowadzania dodatkowej struktury na przestrzeni liniowej, pozwalającej przede wszystkim na rozważanie pojęcia ortogonalności wektorów, a w przypadku rzeczywistym także na mówienie o kątach, miarach, orientacji itd. Teoria ta pozwoliła nam na wyrobienie wstępnych intuicji geometrycznych niezbędnych do pracy w przestrzeniach afinicznych. Dała nam też posmak zjawiska, które będziecie Państwo często obserwować – zamiast rozważać czysto algebraiczne struktury typu przestrzenie liniowe czy przekształcenia między nimi uczyć się Państwo będziecie o ich szczególnych typach, wyposażonych w dodatkowe struktury algebraiczne (jak iloczyn skalarny), metryczne (jak choćby izometrie), i wiele innych. Konkluzją wykładu będzie badanie zbiorów opisanych (niekoniecznie liniowymi) równaniami algebraicznymi w przestrzeni afinicznej.

23.1 Uzupełnienie. Minima i maksima

Możliwość diagonalizacji formy kwadratowej ma olbrzymie znaczenie w teorii liczb i geometrii, a także w wielu innych działach matematyki. Przyjrzyjmy się teraz prostemu zastosowaniu, mającemu dalej istotne zastosowania analityczne.

Twierdzenie 23.3

Niech $q : \mathbb{R}^n \rightarrow \mathbb{R}$ będzie formą kwadratową na przestrzeni euklidesowej $(\mathbb{R}^n, \langle \cdot, \cdot \rangle)$. Załóżmy, że $A = G(h; st)$ jest macierzą tej formy oraz, że $(\alpha_1, \dots, \alpha_n)$ jest bazą prostopadłą $(\mathbb{R}^n, \langle \cdot, \cdot \rangle)$ oraz bazą ortonormalną $(\mathbb{R}^n, \langle \cdot, \cdot \rangle_{st})$ złożoną z wektorów własnych macierzy A o wartościach własnych $a_1 \geq a_2 \geq \dots \geq a_n$. Niech $I \subseteq (\mathbb{R}^n, \langle \cdot, \cdot \rangle)$ oznacza zbiór wektorów o normie 1. Wówczas na zbiorze I forma q ma największą wartość równą $q(\alpha_1/\|\alpha_1\|) = a_1$, a najmniejszą wartość równą $q(\alpha_n/\|\alpha_n\|) = a_n$.

Co to twierdzenie oznacza? Mówi ono, że przedstawienie formy kwadratowej w postaci diagonalnej, więc w „nowym układzie prostopadłym” pozwala odczytać kierunki „najszybszego” jej wzrostu i „najszybszego” jej spadku.

Przykład. Wyznamy największą i najmniejszą wartość funkcji dwóch zmiennych $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ postaci $f((x_1, x_2)) = x_1^2 + x_2^2 + 4x_1x_2$ na okręgu zadanym równaniem $x_1^2 + x_2^2 = 1$. Wykresem naszej funkcji jest pewna powierzchnia w \mathbb{R}^3 . Wkrótce dowiemy się więcej na temat tego jak ona w zasadzie wygląda.

Otóż w bazie $(\alpha_1, \alpha_2) = ((1, 1), (1, -1))$ (ortogonalnej w $(\mathbb{R}^2, \langle \cdot, \cdot \rangle_{st})$) funkcja f „traktowana jako” forma kwadratowa może być zapisana w postaci $f(y_1\alpha_1 + y_2\alpha_2) = 3y_1^2 - y_2^2$. Twierdzenie mówi, że po wzięciu kierunków powyższych wektorów o normie 1, czyli

$$\left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right) \quad \text{oraz} \quad \left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\right)$$

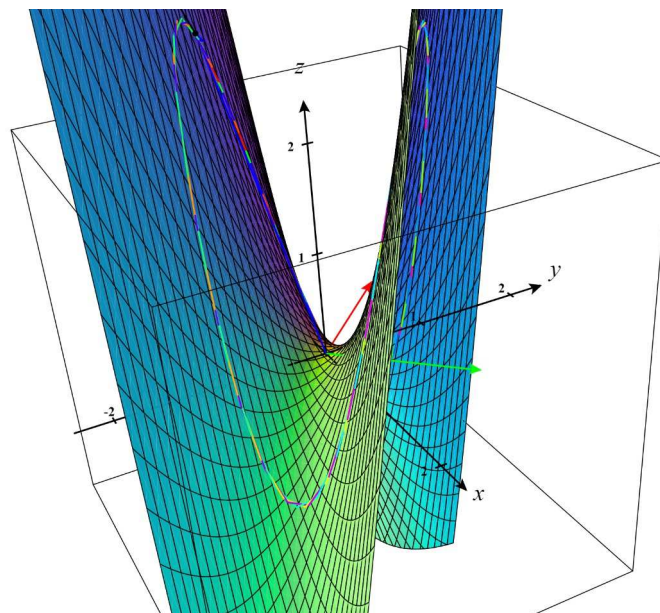
uzyskamy, że największa i najmniejsza wartość naszej funkcji na zbiorze I wynoszą odpowiednio

$$f\left(\left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right)\right) = 3 \quad \text{oraz} \quad f\left(\left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\right)\right) = -1.$$

Co ciekawe, moglibyśmy też wziąć wektory

$$\left(-\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\right) \quad \text{oraz} \quad \left(-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right)$$

i również dla nich dostaniemy odpowiednio największą w zbiorze I wartość f czyli 3 oraz najmniejszą wartość równą -1 . Poniżej poglądowy obrazek.



Obrazek wygenerowany online: <https://www.monroec.edu/faculty/paulseeburger/calcnst/CalcPlot3D/>

Pozostał nam dowód wyjściowego Twierdzenia 23.3. Zaczniemy od lematu ilustrującego istnienie bazy postulowanej w tym twierdzeniu.

Obserwacja 23.9

Niech $h : V \times V \rightarrow \mathbb{R}$ będzie formą dwuliniową symetryczną na skończonej wymiarowej przestrzeni liniowej V nad \mathbb{R} . Wówczas dla każdego iloczynu skalarnego $\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{R}$ istnieje taka baza ortonormalna przestrzeni euklidesowej $(V, \langle \cdot, \cdot \rangle)$, która jest też bazą prostopadłą przestrzeni (V, h) .

Dowód. Niech \mathcal{B} będzie bazą ortonormalną przestrzeni euklidesowej $(V, \langle \cdot, \cdot \rangle)$ i niech przekształcenie liniowe $\phi : V \rightarrow V$ będzie zadane warunkiem $M(\phi)_{\mathcal{B}}^{\mathcal{B}} = G(h; \mathcal{B})$. Macierz $G(h; \mathcal{B})$ jest symetryczna, więc ϕ jest samosprężone. Stąd istnieje baza ortonormalna \mathcal{A} przestrzeni $(V, \langle \cdot, \cdot \rangle)$ złożona z wektorów własnych endomorfizmu ϕ (twierdzenie spektralne). Wówczas macierz $C = M(\text{id})_{\mathcal{A}}^{\mathcal{B}}$ jest ortogonalna, czyli $C^T = C^{-1}$. Zatem

$$G(h; \mathcal{A}) = C^T \cdot G(h; \mathcal{B}) \cdot C = C^{-1} \cdot M(\phi)_{\mathcal{B}}^{\mathcal{B}} \cdot C = M(\phi)_{\mathcal{A}}^{\mathcal{A}},$$

przy czym macierz $M(\phi)_{\mathcal{A}}^{\mathcal{A}}$ jest diagonalna, bo baza \mathcal{A} jest złożona z wektorów własnych endomorfizmu ϕ . Wykazaliśmy więc, że macierz $G(h; \mathcal{A})$ jest diagonalna, więc \mathcal{A} jest bazą prostopadłą (V, h) . \square

Dowodzimy Twierdzenie 23.3. Niech h będzie formą dwuliniową symetryczną na \mathbb{R}^n odpowiadającą formie kwadratowej q . Niech $(\alpha_1, \dots, \alpha_n)$ będzie bazą ortogonalną (\mathbb{R}^n, h) oraz jednocześnie bazą ortonormalną złożoną z wektorów własnych macierzy A . Dla każdego $\alpha \in \mathbb{R}^n$ mamy rozkłady wektorów α oraz $A\alpha$ w bazie ortonormalnej postaci:

$$\alpha = \langle \alpha, \alpha_1 \rangle \alpha_1 + \dots + \langle \alpha, \alpha_n \rangle \alpha_n, \quad A\alpha = a_1 \langle \alpha, \alpha_1 \rangle \alpha_1 + \dots + a_n \langle \alpha, \alpha_n \rangle \alpha_n.$$

Jeśli założymy, że $\|\alpha\| = 1$, to mamy też $\langle \alpha, \alpha_1 \rangle^2 + \dots + \langle \alpha, \alpha_n \rangle^2 = 1$, a także

$$\langle \alpha, A\alpha \rangle = a_1 \langle \alpha, \alpha_1 \rangle^2 + \dots + a_n \langle \alpha, \alpha_n \rangle^2.$$

A zatem dla α o normie 1 mamy (proszę dokładnie przemyśleć zwłaszcza trzecią równość):

$$\begin{aligned} q(\alpha) = h(\alpha, \alpha) = \alpha^T A\alpha &= \langle \alpha, A\alpha \rangle = a_1 \langle \alpha, \alpha_1 \rangle^2 + \dots + a_n \langle \alpha, \alpha_n \rangle^2 \\ &\leq a_1 \langle \alpha, \alpha_1 \rangle^2 + \dots + a_1 \langle \alpha, \alpha_n \rangle^2 = a_1. \end{aligned}$$

Analogicznie pokazujemy, że $q(\alpha) \geq a_n$, dla $\|\alpha\| = 1$. Jeśli teraz α jest wektorem własnym A odpowiadającym a_1 oraz $\|\alpha\| = 1$, to

$$q(\alpha) = h(\alpha, \alpha) = \langle \alpha, A\alpha \rangle = \langle \alpha, a_1 \alpha \rangle = a_1 \|\alpha\|^2 = a_1.$$

Także $q(\beta) = a_n$, jeśli $\|\beta\| = 1$ oraz β jest wektorem własnym A odpowiadającym wartości własnej a_n . Dowód jest zatem zakończony.

Formy kwadratowe służą w analizie np. do określania kryteriów osiągnięcia lub nie ekstremów lokalnych. Są to wyniki analogiczne jak dla funkcji różniczkowalnej jednej zmiennej, gdzie np. minimum lokalne osiągnięte jest w punkcie zerowania się pochodnej, pod warunkiem, że druga pochodna jest dodatnia. Dla funkcji wielu zmiennych zamiast pochodnych odpowiednich stopni mamy różniczki, przy czym pierwsza różniczka jest przekształceniem liniowym, a druga – symetryczną formą dwuliniową. Jeśli np. różniczkowalna w pewnym punkcie funkcja dwóch zmiennych ma zerową różniczkę oraz jej druga różniczka jest dodatnio określona to w punkcie tym jest minimum lokalne. Zainteresowanych odsyłam do <http://smurf.mimuw.edu.pl/node/244> oraz notatki dr. M. Krycha: *Lokalne ekstrema, formy kwadratowe*: <https://www.mimuw.edu.pl/~krych/matematyka/AM2skrypt/am2cz06L.pdf>.

23.2 Dodatek. Twierdzenie Hasse-Minkowskiego

Załóżmy, że chcecie Państwo rozwiązać w liczbach całkowitych równanie $x^3 - 2x + 17 = 0$. Oczywiście znamy rezultat szkolny, który mówi jak to robić, ale on ukrywa meritum sprawy. To równanie nie ma rozwiązań w \mathbb{Z} (ani w \mathbb{Q}), bo jeśli „zajrzemy z nim” do małego świata ciała pięcioelementowego \mathbb{Z}_5 , to ma ono postać $x^3 + 3x + 2 = 0$ i nie ma w tym ciele rozwiązań. Stąd i wyjściowe równanie nad \mathbb{Z} ich nie ma. Pytanie: czy z każdym równaniem wielomianowym o współczynnikach całkowitych wystarczy „zajrzeć” do pewnych ciał skończonych, aby dowiedzieć się czy rozwiązanie w \mathbb{Z} istnieje? O tym mówi i owo twierdzenie szkolne, i wynik Hasse-Minkowskiego, o którym chcemy powiedzieć tu kilka zdań. Aby zrozumieć wysłownienie tego faktu odsyłam do jednego z wcześniejszych dodatków dotyczących ciał p -adycznych, a także do notatek z wykładu gwiazdkowego¹.

Na czym polega problem z rozwiązaniem równania wyżej? Niestety, gdybyśmy znaleźli rozwiązanie powyższego równania w \mathbb{Z}_5 , to nie mielibyśmy pewności, że istnieje ono nad \mathbb{Z} czy też \mathbb{Q} . Zacznijmy od zacytowania następującego rezultatu.

Twierdzenie 23.4: <https://arxiv.org/pdf/2102.08379.pdf>

Dana jest liczba całkowita $n \neq 1$ spełniająca warunki:

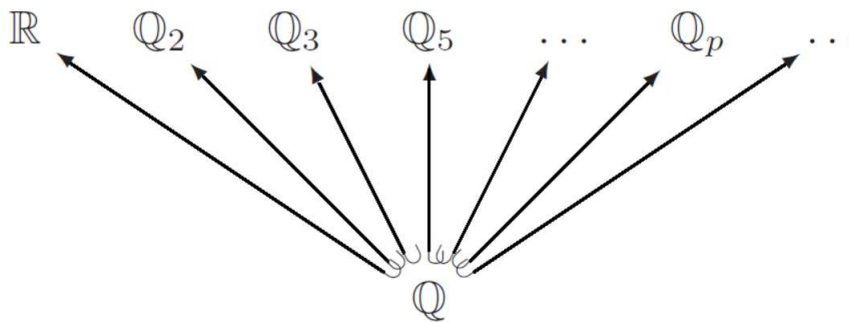
- n jest niepodzielna przez sześćian liczby pierwszej,
- $n \equiv 1 \pmod{9}$,
- jeśli liczba pierwsza q dzieli n , to $q \equiv 1 \pmod{3}$.

Wówczas wielomian:

$$(x^3 - n)(x^2 + 3) = 0$$

nie ma pierwiastków wymiernych, choć ma rozwiązania w ciele \mathbb{Z}_p .

Istnienie wielomianów o współczynnikach w \mathbb{Z} takich jak powyższe przeczy prawdziwości *zasady lokalno-globalnej* dla dowolnego równania $f = 0$, $f \in \mathbb{Q}[x]$. Pytanie: czy po ograniczeniu do pewnych klas równań zasada ta może działać (i jak ją dokładnie sformułować)? To jedno z centralnych zagadnień teorii liczb. Poniższy rezultat to jedno z ważniejszych twierdzeń teorii form kwadratowych początku XX stulecia, otwierające nowy rozdział jej rozwoju.



Oczywiście $\mathbb{Q}_p \subseteq \mathbb{Q}_p$, więc rozważanie formy q_p ma sens. Więcej o tym twierdzeniu można przeczytać w tekście <http://www.math.union.edu/~hatleyj/Capstone.pdf>.

Twierdzenie 23.5: Zasada lokalno-globalna (Hasse-Minkowski), 1921

Niech q będzie formą kwadratową na skończonej wymiarowej przestrzeni nad ciałem \mathbb{Q} oraz niech q_p oznacza formę q rozważaną nad ciałem liczb p -adycznych \mathbb{Q}_p , gdzie $p \in \mathbb{P}$ lub $p = \infty$ (konwencja: $\mathbb{Q}_\infty = \mathbb{R}$). Wówczas równanie $q(x) = 0$ ma rozwiązanie wtedy i tylko wtedy, gdy równania $q_p = 0$ mają rozwiązania dla każdego $p \in \mathbb{P} \cup \{\infty\}$.

¹Wykłady https://mimuw.edu.pl/~amecel/20211/gal21/GAL2+_AM_w16.pdf oraz https://mimuw.edu.pl/~amecel/20211/gal21/GAL2+_AM_w17.pdf.

23.3 Notka historyczna. Sumy kwadratów

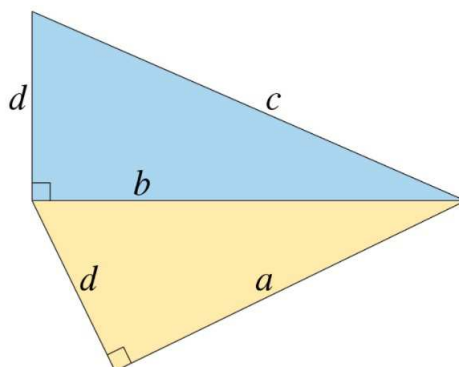
Wyrażeniami i równaniami typu kwadratowego zajmowano się już w starożytnym Babilonie. W starożytnej Grecji, a później w Afryce Północnej i Europie badano je także w kontekście geometrycznym (twierdzenie Pitagorasa, układ współrzędnych, stożkowe...) Najważniejszym czysto matematycznym źródłem była jednak teoria liczb. Punktem wyjścia był Problem 8 z Księgi II starożytnego traktatu *Arithmetica* Diofantosa z III wieku: daną liczbę wymierną przedstawić jako sumę kwadratów liczb wymiernych. Liczne przeformułowania były źródłami wielu słynnych problemów matematycznych stawianych najpierw przez uczonych arabskich w IX wieku, później przez czerpiącego z dorobku arabskiego Fibonacciego walczącego w XIII wieku z problemem CONGRUUM.

Fibonacci (1170-1250), a właściwie Leonardo (z Pizy) zasłynął przez upowszechnienie w początkach XIII wieku notacji arabskiej opartej na cyfrach 0 – 9 pochodzącej z tekstu al-Khwārizmiego z 825 roku (od którego nazwę bierze algebra). Nikogo by to nie interesowało gdyby nie fakt, że *Liber Abbaci* (Księga Liczydła), obok wprowadzenia słynnego dziś ciągu jako rozwiązania problemu rozmnażania się królików, zawierała istotne praktyczne wskazówki dotyczące używania ułamków i rozwiązywania rachunkowych problemów powstających przy... wymianie dóbr, zwłaszcza różnych walut. To było wtedy ważne.

W 1225 roku Pizę odwiedził cesarz Fryderyk II (syn Barbarossy). Znając reputację Leonardo cesarz uznał, że warto poddać ją próbie przez... zorganizowanie turnieju (typowe w tamtych czasach). Zawodnicy zadawali sobie nawzajem pytania. Drużynę cesarza stanowili Jan z Palermo i Mistrz Teodor, zaś drużynę Leonarda stanowił on sam. Pytanie mu postawione brzmiało: znaleźć kwadrat liczby wymiernej, który pozostaje kwadratem liczby wymiernej zarówno gdy dodamy do niego 5, jak i gdy odejmiemy od niego 5. Innymi (naszymi) słowy oczekiwano przykładowo, że 5 stanowi *congruum*, czyli różnicę w ciągu arytmetycznym trzech kwadratów liczb wymiernych. Najmniejszy przykład rozwiązania problemu turniejowego to $1681/144$ – co Leonardo wykrył (choć przed nim inni).

W swoim ważnym dziele *Liber quadratorum* Fibonacci atakował ogólny problem congruum próbując zastąpić liczbę 5 innymi, w tym kwadratami liczb całkowitych (np. 1), dla których nie umiał go rozwiązać.² Zrobił to dopiero Fermat, co wymagało prostego pomysłu zakładającego, że z istnienia „najmniejszej realizacji kwadratowego congruum” wywieść można istnienie jeszcze mniejszej realizacji (i dostać sprzeczność). Jest to *technika nieskończonego schodzenia*.

Fermat w 1670 roku rozwiązał problem Fibonacciego pokazując, że jeśli różnice pewnych dwóch par kwadratów liczb całkowitych (lub ogólniej: liczb wymiernych) są identyczne, to nie mogą być one kwadratami. Innymi słowy, w poniższej konfiguracji trójkątów prostokątnych jedna z długości a, b, c, d musi być liczbą niewymierną.



Jeśli $d^2 = b^2 - a^2 = c^2 - b^2$, to jedna z liczb a, b, c, d jest niewymierna. Źródło: Wikipedia. Fermat's right triangle theorem.

Fermat zajmował się między innymi badaniem możliwości rozkładania liczb na sumy kwadratów. Aby opowiedzieć nieco o historii tego znanego zagadnienia przejdźmy do języka form kwadratowych. W notce tej zajmiemy się niezwykle ważnym i ciekawym problemem reprezentowalności formy kwadratowej o współczynnikach całkowitych. Interesuje nas jakie wartości całkowite przyjmować może ta forma. Zaczniemy od ogólnej definicji.

²Do 1915 roku znano wszystkie congrua mniejsze niż 100. W 1986 roku – mniejsze niż 2000 (komputer). Ogólne rozwiązanie problemu congruum nie jest znane.

Definicja 23.8

Niech q będzie formą kwadratową na przestrzeni n wymiarowej V nad ciałem K . Element niezerowy $a \in K$ JEST REPREZENTOWANY PRZEZ q nad ciałem K , jeśli istnieją x_1, \dots, x_n takie, że $f(x_1, \dots, x_n) = a$.

- Zbiór niezerowych elementów ciała K reprezentowanych przez formę q nazywamy ZBIOREM WARTOŚCI tej formy, ozn. $D_K(q)$.
- Formę q nazywamy IZOTROPOWĄ, jeśli istnieje $x \neq 0$ należący do V , że $q(x) = 0$. Formę q nazywamy ANIZOTROPOWĄ, jeśli $q(x) = 0 \Rightarrow x = 0$.
- Formę q nazywamy UNIWERSALNĄ, jeśli $D_K(q) = K \setminus \{0\}$.

Interesuje nas odpowiedź na pytanie **jakie liczby całkowite mogą być reprezentowane przez formy kwadratowe o wyrazach całkowitych?** Kiedy formy te mają zbiór wartości \mathbb{Z}_+ , co określamy mianem **całkowitej formy uniwersalnej?**

Zobaczmy kilka przykładów.

- Równanie $x^2 - xy + y^2 = 2$ nie ma całkowitych rozwiązań. Można argumentować mod 3, ale można zauważyć, że:

$$x^2 - xy + y^2 = \left(x - \frac{1}{2}y\right)^2 + \frac{3}{4}y^2 = 2 \Rightarrow \frac{3}{4}y^2 \leq 3 \Rightarrow |y| < 2,$$

czyli $y \in \{-1, 0, 1\}$, a przez symetrię $x \in \{-1, 0, 1\}$.

- Ile jest całkowitoliczbowych rozwiązań równania $x^2 - 3xy + y^2 = 1$?

Rozwiązaniami są np. $(x, y) = \pm(1, 0), \pm(0, 1)$, ale też $(x, y) = (8, 3)$. Pomnożmy jednak strony wyjściowego równania przez 2 i zapiszmy:

$$\begin{aligned} 2x^2 - 6xy + 2y^2 &= [x \quad y] \begin{bmatrix} 2 & -3 \\ -3 & 2 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} \\ &= [x \quad y] \begin{bmatrix} -3 & -1 \\ 8 & 3 \end{bmatrix} \cdot \begin{bmatrix} 2 & -3 \\ -3 & 2 \end{bmatrix} \cdot \begin{bmatrix} -3 & 8 \\ -1 & 3 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} = 2. \end{aligned}$$

Więc jeśli $\begin{bmatrix} x \\ y \end{bmatrix}$ jest rozwiązaniem, to jest nim także $\begin{bmatrix} -3 & 8 \\ -1 & 3 \end{bmatrix}^n \cdot \begin{bmatrix} x \\ y \end{bmatrix}$, dla $n \geq 1$, czyli rozważane równanie ma nieskończenie wiele rozwiązań.

Problem reprezentowalności form kwadratowych znany jest (pod różnymi nazwami) od wieków. Oto kilka przykładów znanych rezultatów.

- **Euklides, -300.** Opis trójek liczb całkowitych, na których zeruje się forma całkowita (tzw. trójki pitagorejskie) $q(x_1, x_2, x_3) = x_1^2 + x_2^2 - x_3^2$.
- **Fermat, 1640.** Forma kwadratowa na \mathbb{Z}^2 postaci $q(x_1, x_2) = x_1^2 + x_2^2$ reprezentuje liczbę pierwszą p wtedy i tylko wtedy, gdy $p \equiv 1 \pmod{4}$.
- **Lagrange, 1772.** Forma kwadratowa na \mathbb{Z}^4 postaci $q(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 + x_3^2 + x_4^2$ reprezentuje każdą liczbę całkowitą nieujemną.
- **Legendre, 1798.** Forma kwadratowa na \mathbb{Z}^3 postaci $q(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2$ reprezentuje wszystkie liczby całkowite nieujemne, które nie mają postaci $4^a(8k+7)$, dla pewnych $a, k \in \mathbb{Z}$.
- **Liouville 1859-60.** Forma całkowita $x_1^2 + x_2^2 + 2x_3^2 + 2x_4^2$ jest uniwersalna, zaś forma całkowita $x_1^2 + x_2^2 + 5x_3^2 + 5x_4^2$ nie reprezentuje jedynie 3. Natomiast $x_1^2 + x_2^2 + 4x_3^2 + 4x_4^2$ nie reprezentuje tylko liczb dających resztę 3 modulo 4.
- **Ramanujan, 1917.** Jest dokładnie 55 uniwersalnych form całkowitych postaci $q(x_1, x_2, x_3, x_4) = ax_1^2 + bx_2^2 + cx_3^2 + dx_4^2$.

- **Dickson, 1926.** Ramanujan nie ma racji, są tylko 54 uniwersalne formy całkowite o czterech zmiennych. Jest nieskończenie wiele całkowitych form uniwersalnych, dla każdej liczby zmiennych większej niż 4 (co wynika z twierdzenia o czterech kwadratach Lagrange'a), ale też żadna forma postaci $ax_1^2 + bx_2^2 + cx_3^2$ nie jest uniwersalna (fajne ćwiczenie dla $a \leq b \leq c$).
- **Halmos, 1938.** Jeśli $a, b, c, d \in \mathbb{Z}_+$, to forma $ax_1^2 + bx_2^2 + cx_3^2 + dx_4^2$ jest uniwersalna wtedy i tylko wtedy, gdy reprezentuje pierwsze 15 dodatnich liczb całkowitych (tak naprawdę wystarczy 9 liczb: $\{1, 2, 3, 5, 6, 7, 10, 14, 15\}$).
- **Conway, Schneeberger, 1993 (15-theorem).** Wynik Halmosa jest prawdziwy dla dowolnej formy $q(x_1, \dots, x_n) = a_1x_1^2 + \dots + a_nx_n^2$ na \mathbb{Z}^n , gdzie $a_i \in \mathbb{Z}_+$. Hipoteza: jeśli nie założymy, że a_i są dodatnie, ale tylko, że q jest dodatnio określona (czyli $q(x) > 0$, dla $x \neq 0, x \in \mathbb{Z}^n$), to uniwersalność q zapewnia *już* reprezentowalność pierwszych 290 liczb całkowitych dodatnich.
- **Bhargava, 2000.** Wynik Halmosa działa dla dowolnej liczby zmiennych w mocniejszej wersji (9 liczb). Dowód jest elementarny, warto przeczytać pracę ze znakomitym wstępem Conwaya (który wywołał całe to *zamieszanie*): <http://www.fen.bilkent.edu.tr/~franz/mat/15.pdf>.
- **Bhargava, Hanke 2011.** Hipoteza Conwaya z 1993 roku jest prawdziwa. Do uniwersalności dodatnio określonej całkowitej formy kwadratowej potrzeba i wystarcza sprawdzenie reprezentowalności 27 liczb: 1, 2, 3, 5, 6, 7, 10, 13, 14, 15, 17, 19, 21, 22, 23, 26, 29, 30, 31, 34, 35, 37, 42, 58, 93, 110, 145, 203, 290. Takich form jest 6436 (to już policzono komputerowo).

Przykład problemu otwartego: forma ternarna Ramanujana³.

- **Ramanujan 1916.** Forma $x^2 + y^2 + 10z^2$ nie reprezentuje liczb parzystych postaci $4^a(16b+6)$, dla $a, b \in \mathbb{Z}_+$ oraz liczb nieparzystych: 3, 7, 31, 33, 33, 43, 67, 79, 87, 133, 217, 219, 223, 253, 307, 391.
- **Gupta, 1941** Forma $x^2 + y^2 + 10z^2$ nie reprezentuje też 2719.
- **Ono, Sonudrarajan 2011.** Hipoteza. Forma $x^2 + y^2 + 10z^2$ nie reprezentuje innych liczb nieparzystych, niż wypisane wyżej. Jeśli jednak zachodzi uogólniona Hipoteza Riemanna, to hipoteza jest prawdziwa!

Ważny problem: jakie liczby pierwsze reprezentowane są przez formy $x^2 + ay^2$? Zagadnienie to było motywem przewodnim rozwoju teorii liczb.

- Fermat (dowody dał Euler, dając początki prawu wzajemności)
 - forma $x^2 + y^2$ reprezentuje liczby pierwsze $p = 1 \pmod{4}$,
 - forma $x^2 + 2y^2$ reprezentuje liczby pierwsze $p = 1, 3 \pmod{8}$,
 - forma $x^2 + 3y^2$ reprezentuje $p = 3$ oraz $p = 1 \pmod{3}$.
- Hipotezy Eulera (nie umiał ich udowodnić, zrobił to Gauss)
 - forma $x^2 + 5y^2$ repr. liczby pierwsze $p = 3, 7 \pmod{20}$,
 - forma $x^2 + 14y^2$ repr. liczby pierwsze $p = 1, 9, 15, 23, 25, 39 \pmod{56}$,
 - forma $x^2 + 27y^2$ repr. $p = 1 \pmod{3}$ gdzie 2 jest resztą sześcienną mod p ,
 - forma $x^2 + 64y^2$ repr. $p = 1 \pmod{4}$ gdzie 2 jest resztą dwukwadratową mod p .
- Lagrange, Legendre, Gauss wnieśli do teorii zagadnienia takie, jak równoważność form, początki teorii genusu, użycie wyróżnika, teoria kompozycji form, wyższe prawa wzajemności.
- Dedekind, Kronecker, Minkowski, Dirichlet, Hilbert rozważali całkowite formy kwadratowe w kontekście algebraicznej teorii liczb i prapoczątków geometrii algebraicznej.

³Więcej: K. Williams: A "Four Integers" Theorem and a "Five Integers" Theorem, The American Mathematical Monthly, Vol. 122, No. 6 (June–July 2015), pp. 528–536, pod adresem (wymagane zalogowanie przez BUW): <https://www.jstor.org/stable/10.4169/amer.math.monthly.122.6.528>.

Rozdział 24

Wielomiany i funkcje wielomianowe Zbiory algebraiczne

Na poprzednim wykładzie zauważyliśmy, że formy kwadratowe mają „różne wzory w różnych bazach”. Dziś powiemy o tym w jaki sposób wpływa to na nasze rozumienie obiektów definiowanych przez równania wielomianowe. Tak, jak podzbiory przestrzeni K^n opisywane układami równań liniowych, można scharakteryzować jako podprzestrzenie afiniczne, tak można szukać klasyfikacji obiektów opisywanych równaniami wielomianowymi, przy czym mowa będzie o wielomianach wielu zmiennych.

Definicja 24.1: Wielomian od n (przemiennych) zmiennych

WIELOMIANEM ZMIENNYCH x_1, \dots, x_n O WSPÓŁCZYNNIKACH Z CIAŁA K nazywamy wyrażenie postaci:

$$\sum_{i_1, \dots, i_n} a_{i_1 \dots i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}, \quad (\dagger)$$

gdzie

- i_1, \dots, i_n są liczbami całkowitymi nieujemnymi (suma ta brana jest po wszystkich możliwych układach liczb całkowitych nieujemnych),
- elementy $a_{i_1 i_2 \dots i_n} \in K$, przy czym zakładamy, że suma ta jest skończona, czyli współczynniki $a_{i_1 i_2 \dots i_n}$ są różne od 0 tylko dla skończonej liczby indeksów i_1, \dots, i_n .

Zbiór wielomianów zmiennych x_1, \dots, x_n o współczynnikach w ciele K oznaczamy $K[x_1, \dots, x_n]$.

Rozważmy kilka przykładów dla przyswojenia sobie wprowadzonej notacji.

- W wielomianie $w \in \mathbb{R}[x_1, x_2]$ postaci $w = x_1^2 + 4x_1x_2 + 3x_2 + 5$ mamy $a_{20} = 1$, $a_{11} = 4$, $a_{01} = 3$, $a_{00} = 5$ oraz $a_{i_1 i_2} = 0$ dla pozostałych par i_1, i_2 .
- W wielomianie $g \in \mathbb{Q}[x_1, x_2, x_3]$ postaci $g = 7x_1x_2^2x_3^7 - 3x_1x_3^4 + 14x_2^5x_3$ mamy $a_{127} = 7$, $a_{104} = -3$, $a_{051} = 14$ oraz $a_{i_1 i_2 i_3} = 0$, dla pozostałych i_1, i_2, i_3 .
- Wielomian, dla którego w sumie (\dagger) jest jedynie jeden niezerowy składnik nazywamy JEDNOMIANEM. Gdy dokładnie dwa składniki są niezerowe — mówimy o dwumianie, a gdy trzy — o trójmianie (np. kwadratowym). Wreszcie, wielomian, dla którego wszystkie składniki w sumie (\dagger) są zerowe nazywamy WIELOMIANEM ZEROWYM.

Uwaga 1. W świetle powyższej definicji wyrażenie postaci x_2x_1 nie jest wielomianem zmiennych x_1, x_2 o współczynnikach w żadnym ciele K , czyli nie należy do $K[x_1, x_2]$. Jest to natomiast wielomian zmiennych x_2, x_1 , czyli element $K[x_2, x_1]$.

Uwaga 2. Z formalnego punktu widzenia zbiór $K[x_1, \dots, x_n]$ traktować należy jako zbiór takich funkcji $f : \mathbb{N}^n \rightarrow K$, które przyjmują niezerową wartość jedynie na skończonym zbiorze argumentów. Każda taka funkcja przypisuje ciągowi indeksów (i_1, i_2, \dots, i_n) współczynnik $a_{i_1 i_2 \dots i_n} \in K$.

Definicja 24.2: Stopień wielomianu

STOPNIEM WIELOMIANU $\sum_{i_1, \dots, i_n} a_{i_1, \dots, i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \in K[x_1, \dots, x_n]$ nazywamy największą z liczb $i_1 + i_2 + \dots + i_n$, dla których $a_{i_1, \dots, i_n} \neq 0$. Stopień wielomianu f oznaczamy $\deg f$. Jeśli f jest WIELOMIANEM ZEROWYM – to znaczy $a_{i_1, \dots, i_n} = 0$, dla wszystkich i_1, \dots, i_n , to piszemy $\deg f = -\infty$.

Wielomiany stopnia ≤ 0 nazywamy wielomianami stałymi. Wielomiany stopnia 1 postaci $a_1 x_1 + \dots + a_n x_n$ nazywamy często wielomianami liniowymi, a wielomiany stopnia 2: wielomianami kwadratowymi.

Definicja 24.3: Suma wielomianów

SUMĄ WIELOMIANÓW $\sum_{i_1, \dots, i_n} a_{i_1, \dots, i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ oraz $\sum_{i_1, \dots, i_n} b_{i_1, \dots, i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ nazywamy wielomian $\sum_{i_1, \dots, i_n} c_{i_1, \dots, i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ taki, że

$$c_{i_1, \dots, i_n} = a_{i_1, \dots, i_n} + b_{i_1, \dots, i_n},$$

dla każdych i_1, \dots, i_n .

Dla wielomianów w i g z wcześniejszych przykładów mamy $\deg w = 2$, $\deg g = 10$. Sumą wielomianów $2x_1^2 x_2 + 6x_1 x_2 - 5x_1$ oraz $7x_1^5 - 2x_1 x_2 + 5x_1$ jest wielomian $7x_1^5 + 2x_1^2 x_2 + 4x_1 x_2$.

Definicja 24.4: Iloczyn wielomianów

Niech $a_{i_1, \dots, i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ oraz $b_{j_1, \dots, j_n} x_1^{j_1} x_2^{j_2} \dots x_n^{j_n}$ będą jednomianami w $K[x_1, \dots, x_n]$. Iloczynem tych jednomianów nazywamy jednomian:

$$a_{i_1, \dots, i_n} \cdot b_{j_1, \dots, j_n} \cdot x_1^{i_1+j_1} x_2^{i_2+j_2} \dots x_n^{i_n+j_n}.$$

IŁOCZYNEM WIELOMIANÓW $f = \sum_{i_1, \dots, i_n} a_{i_1, \dots, i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ oraz $g = \sum_{j_1, \dots, j_n} b_{j_1, \dots, j_n} x_1^{j_1} x_2^{j_2} \dots x_n^{j_n}$ nazywamy wielomian, będący sumą iloczynów wszystkich par jednomianów, złożonych z jednomianu wielomianu f i jednomianu wielomianu g .

Dla przykładu iloczyn wielomianów $f = x_1 + 2x_2^3 - x_3$ oraz $g = x_2 - x_3$ należących do $k[x_1, \dots, x_n]$ równy jest: $fg = (x_1 + 2x_2^3 - x_3)(x_2 - x_3) = x_1 x_2 - x_1 x_3 + 2x_2^4 - 2x_2^3 x_3 - x_2 x_3 - x_3^3$. Odnotujmy, że dodawanie i mnożenie wielomianów jest operacją przemienną i łączną (łączność mnożenia sprawdzamy dla najpierw dla jednomianów, a później korzystamy z łączności dodawania). W szczególności wprowadzając operację mnożenia wielomianu przez wielomian stały (który utożsamiamy z elementem ciała K) sprawdzamy bez trudu, że zbiór $K[x_1, \dots, x_n]$ jest przestrzenią liniową nad ciałem K . W istocie zbiór ten ma strukturę tzw. przemiennego pierścienia łącznego, tzn. spełnia wszystkie aksjomaty ciała poza istnieniem elementu odwrotnego do dowolnego elementu niezerowego.

Definicja 24.5: Funkcja wielomianowa

FUNKCJĄ WIELOMIANOWĄ na przestrzeni K^n , zadaną wielomianem $\sum_{i_1, \dots, i_n} a_{i_1, \dots, i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ należącym do $K[x_1, \dots, x_n]$ nazywamy funkcję $f : K^n \rightarrow K$ taką, że dla każdych $s_1, \dots, s_n \in K$ zachodzi

$$f(s_1, \dots, s_n) = \sum_{i_1, \dots, i_n} a_{i_1, \dots, i_n} s_1^{i_1} s_2^{i_2} \dots s_n^{i_n}.$$

W szkole rozróżnienie pomiędzy wielomianami i funkcjami wielomianowymi było stosunkowo mgliste, ale gdy rozważamy współczynniki nad różnymi ciałami ma ono istotne znaczenie.

Twierdzenie 24.1

Dla każdego ciała nieskończonego K przyporządkowanie przypisujące każdemu wielomianowi zadaną przez niego funkcję wielomianową jest bijekcją.

Dowód. Z definicji funkcji wielomianowej odwzorowanie przypisujące każdemu wielomianowi zadaną przez niego funkcję jest „na” (nie ma funkcji wielomianowej, która nie była by zadaną przez wielomian). Jeżeli wielomiany $F_1, F_2 \in K[x_1, \dots, x_n]$ zadają tę samą funkcję wielomianową, to wielomian $F = F_1 - F_2$ zadaje funkcję zerową. Wykażemy, że jedynym wielomianem, który zadaje funkcję zerową jest wielomian zerowy.

Stosujemy indukcję po n . Zaczniemy od dowodu dla $n = 1$. Zgodnie z twierdzeniem o dzieleniu wielomianów z resztą (drugi wykład na pierwszym semestrze) element $b \in K$ jest pierwiastkiem wielomianu $F \in K[x]$ wtedy i tylko wtedy, gdy $F(x) = (x - b) \cdot G(x)$, dla pewnego $G \in K[x]$. Stąd jeśli parami różne $b_1, \dots, b_r \in K$ są pierwiastkami wielomianu F , to

$$F(x) = (x - b_1)(x - b_2) \dots (x - b_r) \cdot H(x),$$

dla pewnego $H \in K[x]$. Jeśli F (równoważnie H) nie jest wielomianem zerowym to ponownie na mocy twierdzenia o dzieleniu z resztą $\deg G = r + \deg H \geq r$. Zatem liczba parami różnych pierwiastków niezerowego wielomianu $F \in K[x]$ jest nie większa od stopnia tego wielomianu. W szczególności każdy niezerowy wielomian $F \in K[x]$ ma skończenie wiele pierwiastków. Jeśli więc K jest ciałem nieskończonym i wielomian F zadaje zerową funkcję wielomianową, to każdy element ciała K jest pierwiastkiem F , czyli F jest zerowy, co kończy dowód dla $n = 1$.

Założmy, że wykazaliśmy tezę indukcyjną dla wielomianów $< n$ zmiennych. Dowodzimy dla n . Przypuśćmy, że wielomian n zmiennych $F = \sum_{i_1, \dots, i_n} a_{i_1 \dots i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \in K[x_1, \dots, x_n]$ zadaje zerową funkcję wielomianową. Ustalmy s_2, \dots, s_n i rozpatrzmy wielomian $\bar{F} \in K[x]$ zadany wzorem

$$\begin{aligned} \bar{F} &= \sum_{i_1, \dots, i_n} a_{i_1 \dots i_n} x^{i_1} s_2^{i_2} \dots s_n^{i_n} \\ &= \sum_{i_2, \dots, i_n} a_{0i_2 \dots i_n} s_2^{i_2} \dots s_n^{i_n} x^0 + \sum_{i_2, \dots, i_n} a_{1i_2 \dots i_n} s_2^{i_2} \dots s_n^{i_n} x^1 + \dots \end{aligned}$$

Skoro funkcja wielomianowa zadana wielomianem F jest zerowa, to również funkcja wielomianowa zadana wielomianem \bar{F} jest zerowa. Teraz korzystamy dwukrotnie z założenia indukcyjnego.

Z przypadku $n = 1$ wnioskujemy, że \bar{F} jest wielomianem zerowym, czyli wszystkie jego współczynniki $a_{ji_2 \dots i_n} s_2^{i_2} \dots s_n^{i_n}$ są zerowe. Jest tak dla każdych s_2, \dots, s_n , więc funkcje wielomianowe $n - 1$ zmiennych zadane wielomianami

$$\sum_{i_2, \dots, i_n} a_{ji_2 \dots i_n} x_2^{i_2} \dots x_n^{i_n} \in K[x_2, \dots, x_n]$$

są zerowe. Ponownie więc korzystając z założenia indukcyjnego, tym razem dla tych wielomianów widzimy, że wszystkie te wielomiany zmiennych x_2, \dots, x_n są zerowe, czyli ich współczynniki $a_{ji_2 \dots i_n}$ są zerowe. Wykazaliśmy zatem, że F jest zerowy. \square

W ramach komentarza przypomnijmy przykłady znane z teorii wielomianów jednej zmiennej. Biorąc choćby wielomiany z $\mathbb{Z}_3[x]$ postaci: $x + 1, x^3 + 1, 2x^3 + 2x + 1$ widzimy, że zadają one tę samą funkcję wielomianową $f : \mathbb{Z}_3 \rightarrow \mathbb{Z}_3$, czyli funkcję „o tabelce” $f(0) = 1, f(1) = 2, f(2) = 0$.

Chcemy utożsamiać wielomiany z odpowiadającymi im funkcjami wielomianowymi, co wymaga wykluczenia ciał skończonych. Będziemy też dalej chcieli diagonalizować formy kwadratowe, co wymaga, aby charakterystyka ciała była różna od 2.

* * *

Od tej pory zakładamy, że rozpatrywane ciała są nieskończone i charakterystyki $\neq 2$.

Definicja 24.6: Funkcja wielomianowa na przestrzeni afinicznej

Niech H będzie skończenie wymiarową przestrzenią afiniczną nad ciałem K i niech p_0, \mathcal{A} będzie układem bazowym przestrzeni H , przy czym $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$. Funkcję $f : H \rightarrow K$ nazywamy FUNKCJĄ WIELOMIANOWĄ NA PRZESTRZENI H , jeśli istnieje wielomian $F = \sum_{i_1, \dots, i_n} a_{i_1 \dots i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ należący do zbioru $K[x_1, \dots, x_n]$ taki, że dla każdych $s_1, \dots, s_n \in K$ zachodzi:

$$f(p_0 + s_1\alpha_1 + s_2\alpha_2 + \dots + s_n\alpha_n) = \sum_{i_1, \dots, i_n} a_{i_1 \dots i_n} s_1^{i_1} s_2^{i_2} \dots s_n^{i_n}.$$

Czy może się zdarzyć, że dla danej funkcji f , dla układu bazowego $p_0; \mathcal{A}$ istnieje wielomian F spełniający warunek powyższej definicji, zaś dla innego układu bazowego $q_0; \mathcal{B}$ taki wielomian G nie istnieje?

Niech $F = \sum_{i_1, \dots, i_n} a_{i_1 \dots i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \in K[x_1, \dots, x_n]$. Przypuśćmy, że w układzie bazowym $p_0; \alpha_1, \dots, \alpha_n$ mamy $f(p_0 + s_1\alpha_1 + \dots + s_n\alpha_n) = \sum_{i_1, \dots, i_n} a_{i_1 \dots i_n} s_1^{i_1} s_2^{i_2} \dots s_n^{i_n}$, dla każdych $s_1, \dots, s_n \in K$. Dla układu bazowego $q_0; \beta_1, \dots, \beta_n$ niech $G = \sum_{i_1, \dots, i_n} b_{i_1 \dots i_n} y_1^{i_1} y_2^{i_2} \dots y_n^{i_n}$ będzie wielomianem powstałym z F przez podstawienie:

$$x_i = c_{i1}y_1 + c_{i2}y_2 + \dots + c_{in}y_n + w_i,$$

dla $i = 1, 2, \dots, n$, gdzie współczynniki c_{ij}, w_i są wyznaczone warunkami:

$$M(\text{id})_{\mathcal{B}}^{\mathcal{A}} = [c_{ij}] \in M_{n \times n}(K), \text{ dla } \mathcal{A} = (\alpha_1, \dots, \alpha_n), \mathcal{B} = (\beta_1, \dots, \beta_n) \text{ oraz } q_0 = p_0 + \sum_{i=1}^n w_i \alpha_i.$$

Wówczas $f(q_0 + t_1\beta_1 + \dots + t_n\beta_n) = \sum_{i_1, \dots, i_n} b_{i_1 \dots i_n} t_1^{i_1} t_2^{i_2} \dots t_n^{i_n}$, dla każdych $t_1, \dots, t_n \in K$.

Przykład. Jeśli $f : \mathbb{R}^3 \rightarrow \mathbb{R}$ dana jest wzorem $f(s_1, s_2, s_3) = s_1 + s_2$ oraz dane są układy bazowe przestrzeni \mathbb{R}^3 :

$$\begin{aligned} p_0; \mathcal{A} &= (0, 0, 0); (1, 0, 0), (0, 1, 0), (0, 0, 1), \\ q_0; \mathcal{B} &= (2, 1, 3); (1, -1, 0), (1, 0, 1), (0, 0, 1). \end{aligned}$$

To oczywiście w układzie bazowym $p_0; \mathcal{A}$ funkcji tej odpowiada wielomian $F(x_1, x_2, x_3) = x_1 + x_2$. A w układzie $q_0; \mathcal{B}$? Aby się dowiedzieć jaki wielomian $G(y_1, y_2, y_3)$ odpowiada tej funkcji zadajemy izomorfizm afiniczny, który przeprowadza współrzędne y_1, y_2, y_3 z $q_0; \mathcal{B}$ na współrzędne x_1, x_2, x_3 w $p_0; \mathcal{A}$:

$$M(\text{id})_{\mathcal{B}}^{\mathcal{A}} = \begin{bmatrix} 1 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix},$$

$$(2, 1, 3) = (0, 0, 0) + 2(1, 0, 0) + 1(0, 1, 0) + 3(0, 0, 1).$$

Wówczas po podstawieniu do $F(x_1, x_2, x_3) = x_1 + x_2$ obrazów y_1, y_2, y_3 przy tej zamianie zmiennych:

$$x_1 = y_1 + y_2 + 2, \quad x_2 = -y_1 + 1, \quad x_3 = y_3 + 3,$$

uzyskujemy wielomian $G(y_1, y_2, y_3) = y_2 + 3$, bowiem $F(y_1 + y_2 + 2, -y_1 + 1, y_3 + 3) = y_2 + 3$.

Definicja 24.7: Wielomian odpowiada funkcji wielomianowej w układzie bazowym

Niech $f : H \rightarrow K$ będzie funkcją wielomianową na n wymiarowej przestrzeni afinicznej H . Mówimy, że WIELOMIAN $F = \sum_{i_1, \dots, i_n} a_{i_1 \dots i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \in K[x_1, \dots, x_n]$ ODPOWIADA FUNKCJI f w układzie bazowym $p_0; \alpha_1, \dots, \alpha_n$, jeśli

$$f(p_0 + s_1\alpha_1 + \dots + s_n\alpha_n) = \sum_{i_1, \dots, i_n} a_{i_1 \dots i_n} s_1^{i_1} s_2^{i_2} \dots s_n^{i_n},$$

dla każdych $s_1, \dots, s_n \in K$. Liczbę $\deg F$ nazywamy STOPNIEM FUNKCJI WIELOMIANOWEJ f .

Co te wszystkie definicje mają wspólnego z rozważaniami z początku wykładu? Gdzie są narzędzia do opisu obiektów geometrycznych zadanych równaniami wielomianowymi? Oto jest kluczowa definicja.

Definicja 24.8: Zbiór algebraiczny, hiperpowierzchnia, stopień hiperpowierzchni

Niech H będzie skończenie wymiarową przestrzenią afiniczną nad K .

- Podzbiór $X \subset H$ nazywamy ALGEBRAICZNYM, jeśli istnieją funkcje wielomianowe f_1, \dots, f_k na przestrzeni H takie, że: $X = \{p \in H \mid f_1(p) = 0, \dots, f_k(p) = 0\}$.
- Jeżeli w układzie bazowym $p_0; \mathcal{A}$ funkcjom f_1, \dots, f_k odpowiadają wielomiany F_1, \dots, F_k , to mówimy, że w tym układzie bazowym X jest OPISYWANY WIELOMIANAMI F_1, \dots, F_k (albo OPISYWANY UKŁADEM RÓWNAŃ $F_1 = 0, \dots, F_k = 0$).
- Podzbiór $X \subset H$ nazywamy HIPERPOWIERZCHNIĄ, jeśli istnieje funkcja wielomianowa f na H taka, że $X = \{p \in H \mid f(p) = 0\}$. Mówimy wtedy, że HIPERPOWIERZCHNIA X JEST OPISYWANA PRZEZ FUNKCJĘ f .
- STOPNIEM HIPERPOWIERZCHNI X nazywamy najniższy ze stopni wielomianów opisujących X .

Przykłady.

- Rozważmy zbiór

$$O = \{(x_1, x_2) \in \mathbb{R}^2 \mid x_1^2 + x_2^2 = 1\}.$$

Co ten opis w ogóle znaczy? Mówi on, że biorę układ bazowy $(0, 0); (1, 0), (0, 1)$ w przestrzeni afinicznej \mathbb{R}^2 i rozpatruję wszystkie punkty postaci $p = (0, 0) + x_1(1, 0) + x_2(0, 1)$, których współrzędne x_1, x_2 spełniają równość $x_1^2 + x_2^2 = 1$. Jest to, jak się okazuje, hiperpowierzchnia stopnia 2. Biorąc bowiem wielomian $F \in K[x_1, x_2]$ postaci $x_1^2 + x_2^2 - 1$ oraz funkcję wielomianową na \mathbb{R}^2 odpowiadającą w układzie bazowym $(0, 0); (1, 0), (0, 1)$ wielomianowi F , dostaję $f(x_1, x_2) = x_1^2 + x_2^2 - 1$, czyli O jest zbiorem punktów $p \in \mathbb{R}^2$ spełniających warunek $f(p) = 0$. Jest to hiperpowierzchnia stopnia 2 w \mathbb{R}^2 .

Dlaczego podkreślam te detale? Kluczowa jest bowiem funkcja f , od której pochodzi równanie, które zapisaaliśmy (skrót myślowy) wyżej. Jeśli weźmiemy teraz układ bazowy $(2, 1); (1, 0), (1, 1)$, to jaki będzie wówczas wielomian odpowiadający funkcji f ? Zgodnie z uwagami wyżej trzeba wziąć $p_0 = (0, 0), \alpha_1 = (1, 0), \alpha_2 = (0, 1), q_0 = (2, 1), \beta_1 = (1, 0), \beta_2 = (1, -1)$. Wówczas stosując notację wyżej mamy $w_1 = 2, w_2 = 1, c_{11} = 1, c_{12} = 1, c_{21} = 0, c_{22} = -1$, czyli dokonując podstawienia $x_1 = 1 \cdot y_1 + 1 \cdot y_2 + 2, x_2 = 0 \cdot y_1 + -1 \cdot y_2 + 1$, dostajemy $x_1^2 + x_2^2 - 1 = y_1^2 + 2y_1y_2 + 2y_2^2 + 2y_1 + 4$. A zatem zbiór O opisywany jest w układzie bazowym $(0, 0), (1, 0), (0, 1)$ równaniem $x_1^2 + x_2^2 = 1$, zaś w układzie bazowym $(2, 1); (1, 0), (1, -1)$ opisany jest równaniem $y_1^2 + 2y_1y_2 + 2y_2^2 + 2y_1 + 4 = 0$.

- Zbiór $\{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1^2 + x_2^2 + x_3^2 = 1\}$ jest sferą. Jest to hiperpowierzchnia stopnia 2 w \mathbb{R}^3 .
- Zbiór $\{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1^2 + x_2^2 + x_3^2 = 1, x_3 = 0\}$ jest okręgiem. Jest to zbiór algebraiczny w \mathbb{R}^3 .
- Zbiór jednopunktowy $X = \{(a, b, c)\}$, gdzie a, b, c są ustalonymi liczbami rzeczywistymi jest hiperpowierzchnią stopnia 2 w \mathbb{R}^3 , opisaną w standardowym układzie bazowym równaniem stopnia 2 postaci: $(x_1 - a)^2 + (x_2 - b)^2 + (x_3 - c)^2 = 0$.

Ostatni przykład sugeruje utożsamienie zbiorów algebraicznych i hiperpowierzchni nad ciałem \mathbb{R} .

Obserwacja 24.1

Każdy zbiór algebraiczny w przestrzeni afinicznej nad ciałem \mathbb{R} jest hiperpowierzchnią.

Dowód. Rozpatrzmy zbiór $X = \{p \in H \mid f_1(p) = 0, \dots, f_k(p) = 0\}$, gdzie $f_i : H \rightarrow \mathbb{R}$ są funkcjami wielomianowymi na rzeczywistej przestrzeni afinicznej H , dla $i = 1, \dots, k$. Wówczas $f = f_1^2 + \dots + f_k^2$ jest funkcją wielomianową na H i $X = \{p \in H \mid f(p) = 0\}$. \square

Naszym celem jest przypatrywanie się hiperpowierzchniom stopnia ≤ 2 . Aparat algebraiczny, który mamy nie pozwoli na rozważania powierzchni wyższych stopni, do których potrzebne są przynajmniej metody przestrzeni rzutowych, a w bardziej zaawansowanym wydaniu – geometrii algebraicznej. W jaki sposób chcemy „klasyfikować” hiperpowierzchnie? Chodzi o opisywanie ich tymi samymi równaniami.

Definicja 24.9: Afiniczny izomorfizm hiperpowierzchni, typ afiniczny hiperpowierzchni

Mówimy, że hiperpowierzchnie H_1, H_2 w przestrzeni afinicznej H są AFINICZNIE IZOMORFICZNE (inaczej mówiąc: mają TEN SAM TYP AFINICZNY), jeśli istnieje izomorfizm afiniczny $h : H \rightarrow H$ taki, że $h(H_1) = H_2$.

Zauważmy, że izomorfizm afiniczny jest niczym innym jak „liniową zamianą współrzędnych”, którą wykonywaliśmy zarówno w przypadku form kwadratowych, jak i wielomianów w rozmaitych układach bazowych. Rzeczywiście, izomorfizm afiniczny jest jednoznacznie określony na układzie bazowym. Stąd natychmiast dostajemy podstawowe przykłady:

- W przestrzeni afinicznej H wymiaru n podprzestrzenie afiniczne H_1, H_2 są afinicznie równoważne wtedy i tylko wtedy, gdy $\dim H_1 = \dim H_2$.
- Niech $q_1, q_2 : K^n \rightarrow K$ będą formami kwadratowymi nad ciałem nieskończonym charakterystyki różnej od 2. Wówczas zbiory algebraiczne

$$H_1 = \{x \in K^n \mid q_1(x) = 0\}, \quad H_2 = \{x \in K^n \mid q_2(x) = 0\}$$

są afinicznie równoważne wtedy i tylko wtedy, gdy formy q_1, q_2 są równoważne. W szczególności odpowiadające tym formom kwadratowym symetryczne formy dwuliniowe $h_1, h_2 : K^n \times K^n \rightarrow K$ muszą mieć kongruentne macierze. Zauważmy zresztą, że H_1, H_2 są w istocie zbiorami wektorów izotropowych form h_1, h_2 .

- Zbiory algebraiczne w \mathbb{R}^2 zadane w standardowym układzie bazowym równaniami

$$x_1^2 + x_2^2 = 1, \quad x_1^2 + 4x_2^2 = 1,$$

są afinicznie równoważne, bowiem mamy izomorfizm $f((x_1, x_2)) = (x_1, \frac{1}{2}x_2)$ oraz $x_1^2 + x_2^2 = 1$ wtedy i tylko wtedy, gdy $x_1 + 4(\frac{1}{2}x_2)^2 = 1$. Drugi z powyższych zbiorów zidentyfikować można z elipsą. A zatem zobrazowaliśmy ogólną zależność: okrąg i elipsa są afinicznie równoważne.

- Jak się okaże, okrąg $x_1^2 + x_2^2 = 1$ nie jest afinicznie równoważny z parabolą $x_1^2 + x_2 = 0$. Na kolejnym wykładzie wprowadzimy ogólne narzędzia wykazywania takich faktów, ale na poziomie intuicji można wyjaśnić to w następujący sposób: zbiory te opisane są równaniami stopnia 2, których części kwadratowe $x_1^2 + x_2^2$ oraz x_1^2 mają różny rząd (jako formy kwadratowe). Jak się okaże, to już uniemożliwia izomorfizm afiniczny.

Obserwacja 24.2

Hiperpowierzchnie X_1, X_2 w H są afinicznie izomorficzne wtedy i tylko wtedy, gdy istnieją układy bazowe $p_0; \mathcal{A}$ oraz $q_0; \mathcal{B}$ takie, że X_1 jest w układzie $p_0; \mathcal{A}$ opisana takim samym równaniem, jak X_2 w układzie $q_0; \mathcal{B}$.

Dowód. Przypuśćmy, że X_1, X_2 są w H afinicznie izomorficzne. Jeśli X_1 jest w układzie $p_0; \alpha_1, \dots, \alpha_n$ opisywana równaniem $F = 0$ i $h(X_1) = X_2$, to X_2 jest w układzie bazowym $h(p_0); h'(\alpha_1), \dots, h'(\alpha_n)$ opisywana również równaniem $F = 0$. Na odwrót: przypuśćmy, że X_1 w układzie $p_0; \alpha_1, \dots, \alpha_n$ oraz X_2 w układzie $q_0; \beta_1, \dots, \beta_n$ są opisane równaniem $F = 0$. Wówczas izomorfizm afiniczny $h : H \rightarrow H$ zadany warunkami $h(p_0) = q_0$ oraz $h'(\alpha_i) = \beta_i$, dla $i = 1, \dots, n$, spełnia $h(X_1) = X_2$. \square

Powyższy fakt daje podstawową motywację naszych rozważań. Nawet z punktu widzenia przestrzeni afinicznych mówi on coś prostego, ale ważnego: podprzestrzeń afiniczna przestrzeni afinicznej wymiaru n jest wymiaru k wtedy i tylko wtedy, gdy w pewnym układzie bazowym można ją opisać (we współrzędnych w tym układzie) równaniami $x_1 = 0, x_2 = 0, \dots, x_{n-k} = 0$. Stąd podprzestrzenie równych wymiarów są afinicznie równoważne. Klasyfikacja hiperpowierzchni stopnia 1 jest więc bardzo czytelna (ale i nudna).

A zatem wiemy już co rozumieć można przez podzbiór przestrzeni afinicznej opisany równaniami typu wielomianowego. Mamy podstawowe narzędzia do badania równań opisujących owe zbiory w różnych układach bazowych. Na kolejnym wykładzie przekonamy się jak metody dotyczące form kwadratowych pomocne są w określaniu natury geometrycznej (typu afinicznego) hiperpowierzchni stopnia 1 i 2.

24.1 Uzupełnienie. Wielomiany jednorodne Przestrzenie i przekształcenia rzutowe

W tym dodatku powiemy kilka słów o przestrzeni rzutowej i związanymi z nią zbiorami rzutowymi.

Definicja 24.10: Przestrzeń rzutowa nad ciałem K

Niech V będzie $n + 1$ -wymiarową przestrzenią liniową nad ciałem K .

- PRZESTRZENIĄ RZUTOWĄ $\mathbb{P}(V)$ wyznaczoną przez V nazywamy zbiór wszystkich podprzestrzeni wymiaru 1 w V .
- Jeśli $V = K^{n+1}$, to piszemy $\mathbb{P}^n = K\mathbb{P}^n = \mathbb{P}(K^{n+1})$ i zbiór ten nazywamy n -WYMIAROWĄ PRZESTRZENIĄ RZUTOWĄ NAD CIAŁEM K .
- Jeśli $U \subseteq V$ jest podprzestrzenią liniową wymiaru $m + 1$, to zbiór $\mathbb{P}(U) \subseteq \mathbb{P}(V)$ nazywamy PODPRZESTRZENIĄ RZUTOWĄ wymiaru m w $\mathbb{P}(V)$. Dla $m = n - 1$ mówimy o hiperpłaszczyźnie rzutowej. Z definicji $\mathbb{P}(\{0\}) = \emptyset$.

Inaczej: $\mathbb{P}(V) = (V \setminus \{0\}) / \sim$, gdzie \sim jest relacją równoważności na $V \setminus \{0\}$ postaci:

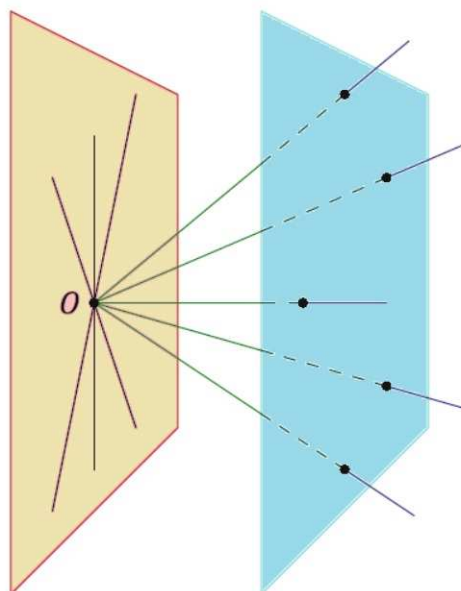
$$v \sim w \iff \exists \lambda \in K, \lambda \neq 0 : v = \lambda w.$$

Klasę $(x_0, \dots, x_n) \in K^{n+1}$ w relacji \sim nazywamy PUNKTEM w przestrzeni $K\mathbb{P}^n$ o (standardowych) WSPÓŁRZĘDNYCH JEDNORODNYCH x_0, \dots, x_n , ozn. $(x_0 : \dots : x_n)$.

Dwa intuicyjne modele. Model 1 w przestrzeni afinicznej K^{n+1} . Niech

$$E = \{(x_0, \dots, x_n) \in K^{n+1} \mid x_0 = 1\}$$

Każda prosta nie zawarta w $T(E)$ przecina E w dokładnie jednym punkcie. To daje utożsamienie $\mathbb{P}(K^{n+1}) \setminus \mathbb{P}(K^n)$ z E .



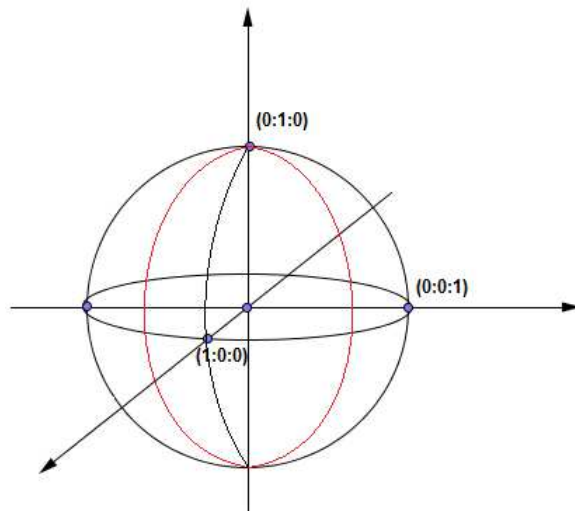
Rysunek zaadoptowany z *Algebra I, Textbook for Students of Mathematics*, A. L. Gorodentsev.

Rys. 1. Model płaszczyzny rzutowej $\mathbb{R}\mathbb{P}^2$, w którym każdy punkt płaszczyzny $x_0 = 1$ to jeden z PUNKTÓW WŁAŚCIWYCH odpowiadający pewnej prostej $\text{lin}(a, b, c)$, $a \neq 0$. Proste $\text{lin}(0, b, c)$ odpowiadają w tym modelu PUNKTOM NIEWŁAŚCIWYM. Model ten zinterpretujemy mapę afiniczną przestrzeni $\mathbb{R}\mathbb{P}^2$.

Dwa intuicyjne modele. Model 2 w przestrzeni afinicznej \mathbb{R}^{n+1} . Niech

$$\mathbb{S}^n = \{(x_0, \dots, x_n) \in \mathbb{R}^{n+1} \mid x_0^2 + x_1^2 + \dots + x_n^2 = 1\}$$

będzie n -wymiarową sferą. Na \mathbb{S}^n wprowadzamy relację równoważności $x \sim y \iff x = -y$. Jest jasne, że istnieje bijekcja między \mathbb{RP}^n oraz \mathbb{S}^n / \sim .



Rysunek zaadoptowany z *Imagining the projective Space*, <https://math.stackexchange.com/>.

Rys. 2. Model płaszczyzny rzutowej \mathbb{RP}^2 na \mathbb{S}^2 , w którym każdej parze punktów antypodycznych na sferze odpowiada jednoznacznie element \mathbb{RP}^2 . W modelu tym nie ma rozróżnienia punktów właściwych i niewłaściwych. Czym są *proste* w \mathbb{RP}^2 ?

Inne (ważne w dalszej edukacji) modele:

- M. Donten-Bury, *Czy widział ktoś płaszczyznę rzutową?*, Delta, 6.2011.
- M. Kordos, *Dziewięć twarzy płaszczyzny rzutowej*, Delta, 5.2013.

Intuicje cd. Każda podprzestrzeń rzutowa jest w (standardowych) współrzędnych jednorodnych opisana przez pewien układ równań liniowych jednorodnych:

$$\begin{cases} a_{10}x_0 + a_{11}x_1 + \dots + a_{1n}x_n = 0 \\ \vdots \\ a_{r0}x_0 + a_{r1}x_1 + \dots + a_{rn}x_n = 0 \end{cases}$$

Np. zbiór punktów $K\mathbb{P}^2$, których współrzędne jednorodne $(x_0 : x_1 : x_2)$ spełniają

$$a_0x_0 + a_1x_1 + a_2x_2 = 0,$$

dla pewnych $a_1, a_2, a_3 \in K$ nie wszystkich równych 0 nazywamy **prostą** w $K\mathbb{P}^2$.

Nietrudno pokazać, że:

- Dla każdych dwóch różnych punktów w płaszczyźnie rzutowej istnieje dokładnie jedna prosta, z którą punkty te są incydentne (należą do niej).
- Na płaszczyźnie rzutowej każde dwie różne proste przecinają się w 1 punkcie.

Intuicje cd. Rozpatrzmy w przestrzeni liniowej V z bazą $(\alpha_0, \alpha_1, \dots, \alpha_n)$ warstwę

$$A_0 = \alpha_0 + \text{lin}(\alpha_1, \dots, \alpha_n).$$

Dla każdego wektora $\alpha \in V$, jeśli prosta $l = \text{lin}(\alpha)$ nie jest zawarta w podprzestrzeni $\text{lin}(\alpha_1, \dots, \alpha_n)$, to $l \cap A_0$ jest zbiorem jednopunktowym.

Istotnie, jeśli $\alpha \notin \text{lin}(\alpha_1, \dots, \alpha_n)$ to $\alpha = x_0\alpha_0 + \dots + x_n\alpha_n$, gdzie $x_0 \neq 0$, stąd:

$$\lambda\alpha = \lambda x_0\alpha_0 + \dots + \lambda x_n\alpha_n = \alpha_0 + \beta,$$

gdzie $\beta \in \text{lin}(\alpha_1, \dots, \alpha_n)$ zachodzi wtedy i tylko wtedy, gdy $\lambda x_0 = 1$.

Każdy punkt wspólny prostej $\text{lin}(x_0\alpha_0 + \dots + x_n\alpha_n)$, $x_0 \neq 0$ przecina się z A_0 na:

$$\alpha_0 + \frac{x_1}{x_0}\alpha_1 + \dots + \frac{x_n}{x_0}\alpha_n,$$

Czyli w układzie bazowym $\alpha_0; \alpha_1, \dots, \alpha_n$ w A_0 punkt przecięcia ma współrzędne:

$$u_1 = \frac{x_1}{x_0}, \quad u_2 = \frac{x_2}{x_0}, \quad \dots, \quad u_n = \frac{x_n}{x_0}$$

Definicja 24.11

Niech (V, \langle, \rangle) będzie przestrzenią liniową wymiaru $n + 1$ i niech $0 \neq \zeta \in V^*$.

- Hiperpłaszczyznę afiniczną U_ζ złożoną z punktów $x \in V$ spełniających równanie $\zeta(x) = 1$ nazywamy MAPĄ AFINICZNĄ wyznaczoną przez ζ . Podzbiór $\ker(\zeta)$ nazywamy HIPERPLASZCZYZNĄ PUNKTÓW NIEWŁAŚCIWYCH mapy U_ζ .
- Niech $(\zeta, \zeta_1, \dots, \zeta_n)$ będzie bazą V^* dualną do pewnej bazy $(\alpha_0, \dots, \alpha_n)$ w V . Wówczas $\alpha_0; \alpha_1, \dots, \alpha_n$ tworzą układ bazowy w U_ζ . Współrzędne punktów w U_ζ nazywamy LOKALNYMI WSPÓLRZĘDNYMI AFINICZNYMI w U_ζ .
- Jeśli $(\zeta, \zeta_1, \dots, \zeta_n)$ jest bazą V^* to wektory

$$0 \neq v = (\zeta_0(v), \dots, \zeta_n(v)), \quad 0 \neq w = (\zeta_0(w), \dots, \zeta_n(w))$$

wyznaczają ten sam punkt w $p \in \mathbb{P}^n$ wtedy i tylko wtedy, gdy ich współrzędne są proporcjonalne. Układ $(x_0 : x_1 : \dots : x_n)$ nazywamy WSPÓLRZĘDNYMI JEDNORODNYMI punktu p w bazie ζ_0, \dots, ζ_n .

- Dla bazy $(\zeta_0, \zeta_1, \dots, \zeta_n)$ przestrzeni V^* zbiór $n + 1$ map afinicznych U_{ζ_i} , dla $0 \leq i \leq n$ nazywamy ATLASEM AFINICZNYM na \mathbb{P}^n . Oczywiście $\mathbb{P}^n = \bigcup_{i=0}^n U_{\zeta_i}$.

Uwagi i przykłady.

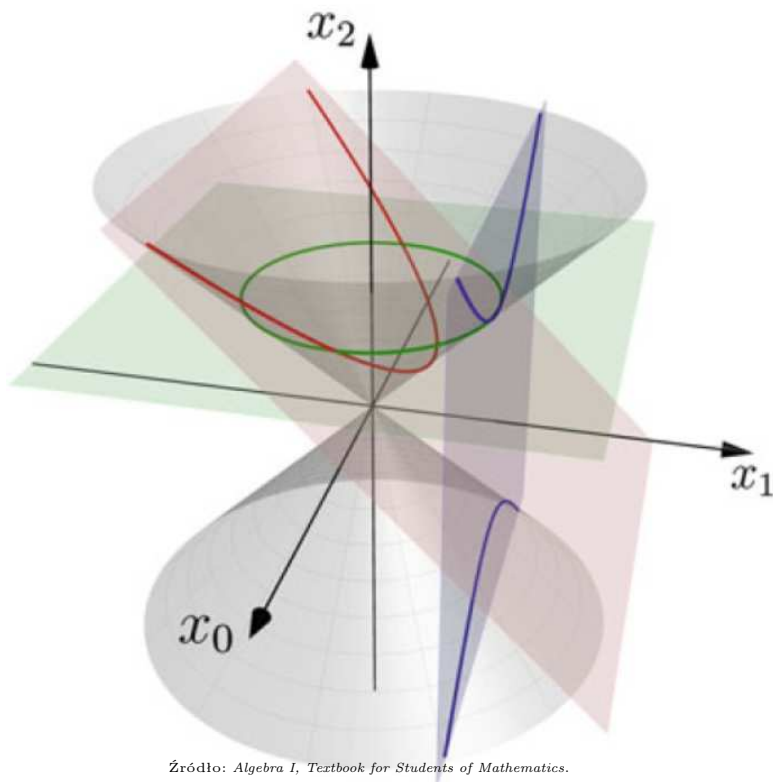
- Niech ζ_0, \dots, ζ_n będzie bazą V^* . Każdy punkt w \mathbb{P}^n ma przynajmniej jedną niezerową współrzędną jednorodną (w tej bazie), więc istnieje w atlasie afinicznym mapa U_{ζ_i} , w której jest on punktem właściwym.
- Mając punkt $p \in \mathbb{P}^n$ o współrzędnych jednorodnych $(x_0 : x_1 : \dots : x_n)$ w bazie ζ_0, \dots, ζ_n , wyznaczamy współrzędne afiniczne punktu p w U_{ζ_i} biorąc wektor $v = p/\zeta_i(p)$ taki, że $\zeta_i(v) = 1$. Wówczas $p \in U_{\zeta_i}$ (jeśli $\zeta_i(p) = 0$, to $p \notin U_{\zeta_i}$). Szukane współrzędne afiniczne to $\zeta_j(v)$, dla $j \neq i$.
- **Przykład.** Prosta afiniczna \mathbb{P}^1 . Weźmy dwie mapy afiniczne U_{ζ_0}, U_{ζ_1} w K^2 opisane odpowiednio równaniami

$$x_0 = 1, \quad x_1 = 1,$$

czyli $\zeta_i(x_0, x_1) = x_i$ dla $i = 0, 1$. Mamy $U_{\zeta_0} = \mathbb{P}^1 \setminus \{(0 : 1)\}$. Każdy punkt właściwy $(x_0 : x_1)$ dla $x_0 \neq 0$ jest w U_{ζ_0} reprezentowany przez punkt $(1 : x_1/x_0)$. Ma on lokalną współrzędną afiniczną równą $\zeta_1^*(1, x_1/x_0)$ czyli jest to $t = x_1/x_0$. Lokalną współrzędną punktów w U_{ζ_1} to $s = x_0/x_1 = 1/t$.

Kluczowy przykład. Rozważmy podzbiór \mathbb{RP}^2 złożony z punktów o współrzędnych jednorodnych $(x_0 : x_1 : x_2)$ spełniających:

$$x_0^2 + x_1^2 = x_2^2.$$



Na powyższym rysunku:

- w mapie standardowej U_{x_1} opisanej równaniem $x_1 = 1$ we współrzędnych $u_0 = \frac{x_0}{x_1}, u_2 = \frac{x_2}{x_1}$ ma równanie hiperboli:

$$u_2^2 - u_0^2 = 1.$$

- w mapie standardowej U_{x_2} opisanej równaniem $x_2 = 1$ we współrzędnych $u_0 = \frac{x_0}{x_2}, u_1 = \frac{x_1}{x_2}$ ma równanie okręgu:

$$u_0^2 + u_1^2 = 1.$$

- w mapie niestandardowej $U_{x_1+x_2}$ opisanej równaniem $x_1 + x_2 = 1$, we współrzędnych: $t = \frac{x_0}{x_1+x_2}, u = \frac{x_2-x_1}{x_2+x_1}$ ma równanie paraboli:

$$t^2 = u.$$

Zbiory w przestrzeniach rzutowych opisane są ważnymi typami równań.

Definicja 24.12

Wielomian $F \in K[x_1, \dots, x_n]$ nazwiemy JEDNORODNYM stopnia i , jeśli jest on sumą jednomianów stopnia i .

Przykłady.

- Wielomian $F[x, y] = x^2y + y^3$ jest jednorodny.
- Wielomian $F[x, y, z] = x^3 + y^3 + xy^2 - xyz$ jest jednorodny.

Oczywista uwaga. Jeśli funkcji wielomianowej $f : K^{n+1} \rightarrow K$ odpowiada w pewnym układzie bazowym p_0, \mathcal{A} wielomian jednorodny $F \in K[x_0, \dots, x_n]$, to jeśli dla pewnego $p_0 + t_0\alpha_0 + \dots + t_n\alpha_n$ mamy $f(t_0, \dots, t_n)$, to dla każdego niezerowego $\lambda \in K$ mamy:

$$f(\lambda x_0, \dots, \lambda x_n) = 0.$$

Definicja 24.13: Zbiór algebraiczny na przestrzeni rzutowej (rozmaitość rzutowa)

Powiemy, że funkcja wielomianowa $f(t_0, t_1, \dots, t_n)$ na K^{n+1} **zeruje się w punkcie** $\tilde{x} = (\zeta_0 : \zeta_1 : \dots : \zeta_n) \in \mathbb{P}^n$, jeśli $f(\zeta_0, \zeta_1, \dots, \zeta_n) = 0$ dla dowolnych współrzędnych jednorodnych punktu \tilde{x} . Innymi słowy, dla każdego niezerowego $\lambda \in K$ mamy:

$$f(\lambda\zeta_0, \dots, \lambda\zeta_n) = 0.$$

Niech g_i będą funkcjami wielomianowymi na K^{n+1} i niech G_i będą odpowiadającymi im (w standardowym ukl. bazowym) wielomianami jednorodnymi. Zbiór $S \subset \mathbb{P}^n$ punktów $(\zeta_0 : \zeta_1 : \dots : \zeta_n)$ spełniających warunki:

$$\begin{cases} g_1(\zeta_0, \dots, \zeta_n) = 0 \\ \vdots \\ g_k(\zeta_0, \dots, \zeta_n) = 0, \end{cases}$$

nazywamy ZBIOREM ALGEBRAICZNYM (RZUTOWYM).

Teoria rzutowych zbiorów algebraicznych (zwłaszcza nad ciałem algebraicznie domkniętym) jest punktem wyjścia klasycznej geometrii algebraicznej. Warto zapoznać się ze świetnymi materiałami prof. A. Nowickiego (UMK): <https://www-users.mat.umk.pl/~anow/ps-dvi/rzu-sd.pdf>.

Na koniec powiemy kilka słów o przekształceniach rzutowych.

Definicja 24.14: Przekształcenie rzutowe

Niech $f = (f_0, \dots, f_n) \in \text{End}(K^{n+1})$ będzie izomorfizmem (można myśleć, że $f_i \in (K^{n+1})^*$). Wówczas dla $x = (x_0, \dots, x_n)$ przyporządkowanie:

$$(x_0 : x_1 : \dots : x_n) \mapsto (f_0(x) : f_1(x) : \dots : f_n(x))$$

nazywamy PRZEKSZTAŁCENIEM RZUTOWYM.

Przykład 1. Przekształcenie

$$\phi(x_0 : x_1 : x_2) = (x_1 : x_0 : x_2)$$

jest rzutowe. Spróbujmy zobaczyć jak wygląda *ślad* tego przekształcenia w mapie U_{x_0} . Kładąc $x_0 = 1$ dostajemy przekształcenie afiniczne:

$$\phi(u_1, u_2) = (1/u_1, u_2/u_1).$$

Zauważmy, że kładąc $1/u_1 = u'_1$ oraz $u_2/u_1 = u'_2$ widzimy, że przeciwobraz okręgu $(u'_1)^2 + (u'_2)^2 = 1$ jest hiperbolą: $1 = u_2^2 - u_1^2$, bo:

$$(u'_1)^2 + (u'_2)^2 = 1 \iff \frac{x_0^2}{x_1^2} + \frac{x_2^2}{x_1^2} = 1 \iff x_1^2 - x_2^2 = x_0^2 \iff u_1^2 - u_2^2 = 1.$$

Przykład 2. Niech $\bar{f}_i : K^n \rightarrow K$ będzie funkcją afiniczną powstałą z funkcji liniowych $f_i : K^{n+1} \rightarrow K$ przez podstawienie $x_0 = 1$. Mamy (nie wszędzie określone):

$$(u_1, u_2, \dots, u_n) \mapsto \left(\frac{\bar{f}_1}{f_0}, \frac{\bar{f}_2}{f_0}, \dots, \frac{\bar{f}_n}{f_0} \right)$$

przekształcenie przestrzeni afinicznej K^n , utożsamianej z U_{x_0} (w sobie).

Przykład 3. Przekształcenie zadane we współrzędnych lokalnych w U_{x_0} wzorem

$$(u_1, u_2) \mapsto \left(\frac{2u_1}{1+u_2}, \frac{1-u_2}{1+u_2} \right)$$

przekształca parabolę $u_2 = u_1^2$ na okrąg.

24.2 Dodatek. Wstęp do algebry wieloliniowej. O iloczynie tensorowym, n-formach i n-wektorach

Iloczyn tensorowy jest jednym z kluczowych obiektów tak zwanej algebry wieloliniowej. Jest to dział algebry niezwykle przydatny z punktu widzenia wielowymiarowej analizy i geometrii różniczkowej. Poniższe rozważania mają charakter wstępny. Zainteresowanego Czytelnika odsyłam do bogatej literatury, zwłaszcza podręcznika *Algebra liniowa* autorstwa prof. Jacka Gancarzewicza lub do cytowanego w USOSie podręcznika Kostrikin *Wstęp do algebry 2 Algebra liniowa* (na podstawie tej książki przedstawiam poniższy materiał). W pierwszej części powiemy o formach wieloliniowych i tzw. tensorach, czyli formach zdefiniowanych na pewnych szczególnych typach przestrzeni liniowych. Rozpoznamy w nich wiele znanych obiektów. Potem zarysujemy kluczowe definicje iloczynu tensorowego, iloczynu zewnętrznego i symetrycznego. Z geometrycznego punktu widzenia opieram się na wyśmienitej książce D. Pedoe *Geometry, a comprehensive course* i przedstawiam na końcu tekstu pewne przykłady opisane w tej książce.

Jak klasyfikować poniższy materiał? Wychodzimy od algebry liniowej — od pojęć algebry wieloliniowej? Rozważane w pełnej ogólności prowadzą do bardzo dalekich uogólnień i konsolidacji dotychczasowego języka. O nich niewiele tu piszę, koncentrując się na definicji tensora, a zwłaszcza — tensora symetrycznego i antysymetrycznego. Analogicznie jak dla form dwuliniowych — te właśnie tensory mają zasadnicze znaczenie dla geometrii? Jaka to geometria? **Jest to geometria bez współrzędnych, formułująca w języku form wieloliniowych zagadnienia konfiguracyjne**, począwszy od elementarnego problemu współliniowości, po niezwykle złożone koncepcje, na które miejsce jest raczej na osobnym kursie (Grasmaniany, flagi, działania grup, orbity, rozmaitości, wiązki itd.).

Aby uzyskać pewne wstępne motywacje, rozważmy następujący problem. Czy jest jakaś relacja pomiędzy poniższymi przestrzeniami liniowymi wielomianów o współczynnikach w ciele K postaci $K[x, y]$, oraz $K[x]$ i $K[y]$? Oczywiście $K[x]$ oraz $K[y]$ są podprzestrzzeniami $K[x, y]$, ale nie jest to suma prosta, bowiem mamy $K \subseteq K[x] \cap K[y]$ oraz $xy \notin K[x] + K[y]$. Więc co to jest?

A może inaczej: weźmy zbiór par wielomianów $(f(x), g(y))$, czyli przestrzeń liniową $K[x] \times K[y]$. Chcemy przypisać każdej parze $(w(x), v(y))$ wielomian $\Phi(w(x), v(y))$ z $K[x, y]$. Jakie naturalne warunki spełnia Φ ?

Możemy spróbować przeprowadzić bazę $K[x] \times K[y]$ złożoną z $\{(x^i, y^j)\}$ na bazę $\{x^i y^j\}$ w $K[x, y]$. Możemy przypisać $(x^i, y^j) \mapsto x^i y^j$ ale jak rozwiązać $(w(x), v(y)) \mapsto 2xy$? Można to zrobić na wiele sposobów. Czy Φ może być liniowe? Wtedy $(x, y) + (1, 1) = (x+1, y+1) \mapsto xy+1$. To niedobrze, bo $(x+1, y+1) = (x, y) + (1, 0) + (0, 1)$, a przecież przypisujemy elementom bazowym elementy bazowe, czyli $(1, 0) \mapsto 0$ oraz $(0, 1) \mapsto 0$. Czyli $(x, y) \mapsto xy+1$? To jakiś absurd, bo teraz $(1, 1) \mapsto 0$.

A może inaczej: bierzemy zbiór par wielomianów $(f(x), g(y))$, czyli przestrzeń liniową $K[x] \times K[y]$ i chcemy przypisać każdej parze $(w(x), v(y))$ wielomian $\Phi(w(x), v(y))$ z $K[x, y]$. Jakie naturalne warunki spełnia Φ ? Możemy spróbować przeprowadzić bazę $K[x] \times K[y]$ złożoną z $\{(x^i, y^j)\}$ na bazę $\{x^i y^j\}$ w $K[x, y]$. Możemy przypisać $(x^i, y^j) \mapsto x^i y^j$ ale jak rozwiązać $(w(x), v(y)) \mapsto 2xy$? Można to zrobić na wiele sposobów.

Czy Φ może być **dwuliniowe**, czyli liniowe na każdej zmiennej? Teraz $\Phi(x+1, y+1) = \Phi(x, y) + \Phi(1, y) + \Phi(x, 1) + \Phi(1, 1) = xy + x + y + 1$. A jak dostać $xy+1$? Nie dostanie się! To jest $\Phi(x, y) + \Phi(1, 1)$. Czy to w ogóle ma jakiś sens? Owszem, zostaniemy przy naszym dwuliniowym funkcjonale Φ .

Okazuje się, że $\Phi : K[x] \times K[y] \rightarrow K[x, y]$ ma tzw. WŁASNOŚĆ UNIWERSALNĄ! Dla każdego przekształcenia **dwuliniowego** $\Psi : K[x] \times K[y] \rightarrow V$ istnieje przekształcenie **liniowe** $f : K[x, y] \rightarrow V$ zadane wzorem

$$K[x, y] \ni \sum_{i,j} a_{ij} \cdot \Phi(x^{k_i}, y^{s_j}) \xrightarrow{f} \sum_{i,j} a_{ij} \cdot \Psi(x^{k_i}, y^{s_j}) \in V.$$

i jest to **jedyne** przekształcenie liniowe takie, że przemienny jest diagram:

$$\begin{array}{ccc} K[x] \times K[y] & \xrightarrow{\Phi} & K[x, y] \\ & \searrow \Psi & \downarrow f \\ & & V \end{array}$$

W języku algebry wieloliniowej oznacza to, że $K[x, y]$ jest \simeq z **iloczynem tensorowym** przestrzeni $K[x]$ oraz $K[y]$ nad ciałem K , ozn. $K[x] \otimes_K K[y]$. Dowód pozostawiam Czytelnikowi.

Definicja 24.15: Produkt kartezjański przestrzeni liniowych

Niech V_1, V_2, \dots, V_n będą przestrzeniami liniowymi nad ciałem K . Na iloczynie kartezjańskim

$$V_1 \times V_2 \times \dots \times V_n$$

wprowadzamy strukturę przestrzeni liniowej definiując działania:

$$(v_1, v_2, \dots, v_n) + (v'_1, v'_2, \dots, v'_n) = (v_1 + v'_1, v_2 + v'_2, \dots, v_n + v'_n),$$
$$\lambda \cdot (v_1, v_2, \dots, v_n) = (\lambda \cdot v_1, \lambda \cdot v_2, \dots, \lambda \cdot v_n).$$

Klasyczne przykłady:

- $K^n \times K^m \simeq K^{n+m}$, w szczególności $\underbrace{K^n \times \dots \times K^n}_m \simeq M_{m \times n}(K)$.
- $V^p \times (V^*)^q = \underbrace{V \times V \times \dots \times V}_p \times \underbrace{V^* \times V^* \times \dots \times V^*}_q$.

Definicja 24.16: Odwzorowanie n -liniowe

Niech V_1, \dots, V_n oraz V będą przestrzeniami liniowymi nad ciałem K . Odwzorowanie

$$\varphi: V_1 \times \dots \times V_n \rightarrow V$$

nazywamy n -LINIOWYM, lub WIELOLINIOWYM, gdy dla dowolnych $v_1 \in V_1, \dots, v_n \in V_n$ następujące odwzorowania są liniowe $V_i \ni x \mapsto \varphi(v_1, \dots, v_{i-1}, x, v_{i+1}, \dots, v_n) \in V$ ($1 \leq i \leq n$).

Przykłady:

- wyznacznik (jako funkcja n -liniowa na kolumnach) $\det: \overbrace{K^n \times \dots \times K^n}^n \rightarrow K$,
- odwzorowanie: $f: K^n \rightarrow K$ postaci $f(a_1, \dots, a_n) = \prod a_i$ jest n -liniowe,
- $f: L(V, W) \times L(U, V) \rightarrow L(U, W)$ dane wzorem $(\theta, \mu) \mapsto \theta \circ \mu$ jest dwuliniowe.

Definicja 24.17: Odwzorowania symetryczne i antysymetryczne

Przestrzeń liniową odwzorowań n -liniowych $\phi: \underbrace{U \times \dots \times U}_n \rightarrow V$ oznaczamy przez $\text{Hom}^n(U, W)$.

Element tej przestrzeni nazywamy

- SYMETRYCZNYM, gdy dla dowolnych $u_1, \dots, u_n \in U$ oraz permutacji $\sigma \in S_n$ mamy:

$$\phi(u_{\sigma(1)}, \dots, u_{\sigma(n)}) = \phi(u_1, \dots, u_n).$$

- ANTYSYMETRYCZNYM (lub SKOŚNIE-SYMETRYCZNYM), gdy dla dowolnych $u_1, \dots, u_n \in U$ spełniających $u_i = u_j$, dla pewnych $1 \leq i < j \leq n$ mamy:

$$\phi(u_1, \dots, u_n) = 0.$$

Podprzestrzenie odwzorowań symetrycznych i antysymetrycznych w $\text{Hom}^n(U, W)$ oznaczamy przez $\text{Hom}_s^n(U, W)$ oraz $\text{Hom}_a^n(U, W)$.

Oczywiście \det jako forma n -liniowa należy do $\text{Hom}_a^n(K^n, K)$

Definicja 24.18: Tensor

Niech V będzie przestrzenią liniową nad K . Dowolny funkcjonal $(p+q)$ -liniowy:

$$\phi : V^p \times (V^*)^q \rightarrow K$$

nazywamy TENSOREM na V typu (p, q) , rzędu $p+q$. Mówimy też, że tensor ϕ jest p -krotnie KOWARIANTNY i q -krotnie KONTRAWARIANTNY. Ponadto z definicji przyjmujemy, że tensor typu $(0, 0)$ to skalar z ciała K .

Prawie wszystkie dobrze nam znane przykłady:

- tensory typu $(1,0)$ to funkcjonały liniowe,
- tensory typu $(0,1)$ można utożsamić z V (gdyż $V^{**} \simeq V$, gdy $\dim V < \infty$),
- tensory typu $(2,0)$ to formy dwuliniowe na V ,
- tensory typu $(0,2)$ to formy dwuliniowe na V^* ,
- $V \times V \times V^* \ni (v, w, f) \mapsto f(v \times w)$ jest tensorem typu $(2,1)$ na V ,
- wyznacznik jest tensorem typu $(n, 0)$ na $V = K^n$.

Obserwacja 24.3

Niech V będzie przestrzenią skończenie wymiarową. Istnieje wówczas bijekcja pomiędzy tensorami typu $(1,1)$ na V oraz $\text{End}(V)$.

Dowód. Idea dla $V = K^n$. Weź $\phi \in \text{End}(V)$ wyznaczone jednoznacznie przez ustalenie baz standardowych i wzięcie macierzy $M = M(\phi)_{st}^{st}$. Wówczas ϕ przypisać można funkcjonal $\Phi : V \times V^* \rightarrow K$ w następujący sposób $\Phi(w, f) = xMy$, gdzie

- $x \in M_{1 \times n}(K)$ – macierz $M(f)_{st}^{st}$,
- $y \in M_{n \times 1}(K)$ – współrzędne w w bazie standardowej.

□

Można zapytać: Czy twierdzenie jest prawdziwe dla $\dim V = \infty$? Jak wypisać ten izomorfizm bez użycia baz? Czy bycie przestrzenią euklidesową coś tu ułatwia?

Definicja 24.19: Tensor symetryczny i tensor antysymetryczny

Niech V będzie skończenie wymiarową przestrzenią liniową nad K .

- Zbiór tensorów symetrycznych typu $(p, 0)$ na V oznaczamy przez $\sum^p V^*$, zaś zbiór tensorów symetrycznych typu $(0, q)$ na V oznaczamy $\sum^q V$.
- Zbiór tensorów antysymetrycznych typu $(p, 0)$ na V oznaczamy $\bigwedge^p V^*$ nazywamy p -tymi FORMAMI ZEWNĘTRZNYMI lub p -KOWEKTORAMI na V . Zbiór tensorów antysymetrycznych typu $(0, p)$ oznaczamy przez $\bigwedge^p V$ i nazywamy p -WEKTORAMI.

Powyższa definicja pozwala na inne sformułowanie kluczowego w pierwszym semestrze faktu.

Twierdzenie 24.2: Wyznacznik jako tensor antysymetryczny

Wyznacznik jest, z dokładnością do skalaru w K , jedyną n -tą formą na K^n .

UWAGA. Nie każdy tensor jest sumą tensora symetrycznego i antysymetrycznego. Aby napisać odpowiedni przykład warto wprowadzić iloczyn tensorowy form (a dalej: iloczyn tensorowy przestrzeni, którego elementy zinterpretujemy jako tensory).

Definicja 24.20: Iloczyn tensorowy form

Niech $f : V_1 \times \dots \times V_r \rightarrow K$ oraz $g : W_1 \times \dots \times W_s \rightarrow K$ będą dwiema dowolnymi formami wieloliniowymi. ILOCZYNEM TENSOROWYM FORM f i g nazywamy odwzorowanie:

$$f \otimes g : V_1 \times \dots \times V_r \times W_1 \times \dots \times W_s \rightarrow K$$

określone wzorem: $(f \otimes g)(v_1, \dots, v_r; w_1, \dots, w_s) = f(v_1, \dots, v_r) \cdot g(w_1, \dots, w_s)$.

Uwagi:

- na ogół mamy $f \otimes g \neq g \otimes f$,
- ale zawsze mamy $(f \otimes g) \otimes h = f \otimes (g \otimes h)$,
- jeśli f jest tensorem typu (p, q) oraz g – tensorem typu (r, s) na V , to $f \otimes g$ jest formą wieloliniową na iloczynie:

$$V^p \times (V^*)^q \times V^r \times (V^*)^s \simeq V^{p+r} \times (V^*)^{q+s},$$

więc $f \otimes g$ uważać można za tensor typu $(p+r, q+s)$ nazywany ILOCZYNEM TENSOROWYM TENSORÓW f i g .

Przykład¹. Rozważmy tensor $T = \epsilon^1 \otimes \epsilon^2 \otimes \epsilon^3 \in \mathbb{T}_3^0(\mathbb{R}^3)$. Twierdzimy, że nie jest to suma tensora symetrycznego i antysymetrycznego. Rzeczywiście, dla $(v_1, v_2, v_3) \in (\mathbb{R}^3)^3$ mamy:

$$(\epsilon^1 \otimes \epsilon^2 \otimes \epsilon^3)(v_1, v_2, v_3) = \epsilon^1(v_1) \cdot \epsilon^2(v_2) \cdot \epsilon^3(v_3),$$

przy czym $\epsilon^i(v)$ zwraca i -tą współrzędną v w bazie standardowej. Mamy zatem:

$$T_{123} = 1, \quad T_{231} = 0.$$

Ale dla każdego tensora symetrycznego lub antysymetrycznego S typu $(3, 0)$ zachodzi $S_{123} = S_{231}$ (dla antysymetrycznych mamy: $S_{123} = -S_{213} = -(-S_{231})$).

Wniosek 24.1

Zbiór $\mathbb{T}_p^q(V)$ wszystkich tensorów typu (p, q) na przestrzeni V jest przestrzenią liniową. Wybierzmy w V oraz V^* bazy dualne^a: $(\epsilon_1, \dots, \epsilon_n), (\epsilon^1, \dots, \epsilon^n)$. Wartość tensora T typu (p, q) na układzie wektorów: $(\epsilon_{i_1}, \dots, \epsilon_{i_p}, \epsilon^{j_1}, \dots, \epsilon^{j_q})$ oznaczamy jako $T_{i_1 \dots i_p}^{j_1 \dots j_q}$ i nazywamy WSPÓLRZĘDNYMI TENSORA T w bazie (ϵ_i) .

^aW teorii tej stosujemy notację z indeksami dolnymi i górnymi: $\epsilon_i^* = \epsilon^i$

Uwaga. Gdy $\dim V < \infty$ to można traktować wektory z V jako funkcjonały na V^* oraz wektory z V^* jako funkcjonały na V . A zatem do $\mathbb{T}_p^q(V)$ należy tensor:

$$\epsilon^{i_1} \otimes \dots \otimes \epsilon^{i_p} \otimes \epsilon_{j_1} \otimes \dots \otimes \epsilon_{j_q}.$$

W istocie zbiór n^{p+q} tensorów jw. stanowi bazę $\mathbb{T}_p^q(V)$. Dokładniej, dla każdego $T \in \mathbb{T}_p^q(V)$ mamy:

$$T = \sum T_{i_1 \dots i_p}^{j_1 \dots j_q} \cdot \epsilon^{i_1} \otimes \dots \otimes \epsilon^{i_p} \otimes \epsilon_{j_1} \otimes \dots \otimes \epsilon_{j_q}.$$

Po tych wstępnych rozważaniach wiążących znane nam obiekty algebry liniowej z pojęciami algebry wieloliniowej nadszedł czas na definicję iloczynu tensorowego.

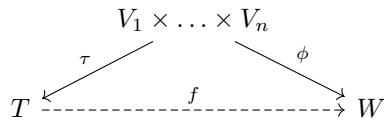
¹W języku tzw. liniowych reprezentacji grup (którego na tym kursie nie poznamy) oznacza to, że reprezentacja regularna grupy symetrycznej S_3 nie może być sumą reprezentacji trywialnych i reprezentacji permutacyjnych grupy S_3 . W istocie zawiera ona nieprzywiedlną 2-wymiarową reprezentację S_3 . Patrz np.: A. Śladek: Elementy teorii reprezentacji liniowych grup skończonych: <http://www.math.us.edu.pl/sladek/dydaktyka/SD/Etr1.pdf>.

Definicja 24.21: Iloczyn tensorowy

Niech V_1, \dots, V_n będą przestrzeniami liniowymi nad K . Wówczas istnieje para (T, τ) nazywana ILOCYZNEM TENSOROWYM przestrzeni V_1, \dots, V_n , gdzie:

- T , oznaczane przez $V_1 \otimes \dots \otimes V_n$, jest przestrzenią liniową nad K ,
- $\tau : V_1 \times \dots \times V_n \rightarrow T$ jest n -liniowe

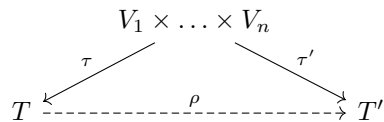
są wybrane tak, że dla dowolnego n -liniowego $\phi : V_1 \times \dots \times V_n \rightarrow W$ istnieje dokładnie jedno odwzorowanie liniowe $f : T \rightarrow W$ takie, że $\phi = f \circ \tau$:



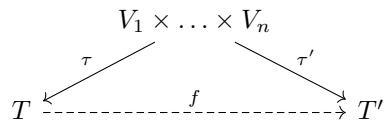
Intuicja: iloczyn tensorowy to konstrukcja sprowadzająca badanie odwzorowań wieloliniowych na zbiorze (potencjalnie nieskomplikowanych) przestrzeni do znanej nam algebry liniowej.

Twierdzenie 24.3: Jednoznaczność iloczynu tensorowego

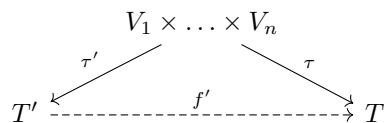
Iloczyn tensorowy (T, τ) **wyznaczony jest z dokładnością do izomorfizmu** (o ile w ogóle istnieje). Oznacza to, że jeśli para (T', τ') jest również iloczynem tensorowym przestrzeni V_1, \dots, V_n , to istnieje jedyny izomorfizm $\rho : T \rightarrow T'$ spełniający



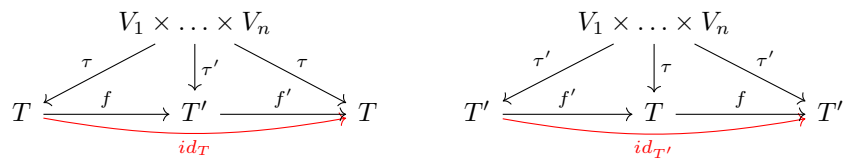
Dowód. Skoro (T, τ) jest iloczynem tensorowym V_1, \dots, V_n , więc dla $W = T'$ oraz $\phi = \tau'$ mamy dokładnie jedno przekształcenie liniowe $f : T \rightarrow T'$ takie, że:



Skoro (T', τ') jest iloczynem tensorowym V_1, \dots, V_n , więc dla $W = T$ oraz $\phi = \tau$ mamy dokładnie jedno przekształcenie liniowe $f' : T' \rightarrow T$ takie, że:



Przechodzimy do dowodu jednoznaczności (T, τ) . Załóżmy, że para (T', τ') jest również iloczynem tensorowym przestrzeni V_1, \dots, V_n . A zatem mamy przemiennosc następujących diagramów:



W rezultacie $f' \circ f = id_T$ oraz $f \circ f' = id_{T'}$, czyli f jest szukanym jedynym izomorfizmem. \square

Twierdzenie 24.4: Istnienie iloczynu tensorowego — konstrukcja

Niech F będzie **wolną przestrzenią liniową** nad K o bazie $V_1 \times \dots \times V_n$ (elementami przestrzeni F są formalne kombinacje liniowe postaci

$$\sum_{(v_1, \dots, v_n) \in V_1 \times \dots \times V_n} \lambda_{v_1, \dots, v_n} (v_1, \dots, v_n),$$

gdzie tylko skończenie wiele skalarów $\lambda_{v_1, \dots, v_n} \in K$ jest różnych od zera). Rozważmy podprzestrzeń N w F rozpiętą przez wszystkie wektory postaci

- $(v_1, \dots, v_i + v'_i, \dots, v_n) - (v_1, \dots, v_i, \dots, v_n) - (v_1, \dots, v'_i, \dots, v_n),$
- $(v_1, \dots, \lambda v_i, \dots, v_n) - \lambda(v_1, \dots, v_i, \dots, v_n)$

gdzie $v_i, v'_i \in V_i$ dla $1 \leq i \leq n$ oraz $\lambda \in K$. Wówczas para (T, τ) jest iloczynem tensorowym przestrzeni V_1, \dots, V_n , gdzie:

- $T = F/N$ jest przestrzenią ilorazową,
- τ to złożenie $V_1 \times \dots \times V_n \xrightarrow{\text{injekcja}} F \xrightarrow{\text{kanon.}} F/N = T$.

Dowód. Złożenie $\tau : V_1 \times \dots \times V_n \xrightarrow{i} F \xrightarrow{\pi} F/N$ przeprowadzające (v_1, \dots, v_n) na klasę $\pi(i(v_1, \dots, v_n)) = [(v_1, \dots, v_n)] \in T/N$ jest n -liniowe. Dla dowolnych $v_i, v'_i \in V_i$ oraz skalarów $\lambda, \mu \in K$ mamy:

$$\begin{aligned} & \tau(v_1, \dots, \lambda v_i + \mu v'_i, \dots, v_n) - \lambda \tau(v_1, \dots, v_i, \dots, v_n) - \mu \tau(v_1, \dots, v'_i, \dots, v_n) = \\ & [(v_1, \dots, \lambda v_i + \mu v'_i, \dots, v_n)] - \lambda [(v_1, \dots, v_i, \dots, v_n)] - \mu [(v_1, \dots, v'_i, \dots, v_n)] = \\ & [(v_1, \dots, \lambda v_i + \mu v'_i, \dots, v_n) - \lambda(v_1, \dots, v_i, \dots, v_n) - \mu(v_1, \dots, v'_i, \dots, v_n)] = 0. \end{aligned}$$

Rozważmy dowolne przekształcenie n -liniowe $\phi : V_1 \times \dots \times V_n \rightarrow W$. Interesuje nas określenie przekształcenia liniowego $f : F/N \rightarrow W$ tak, by:

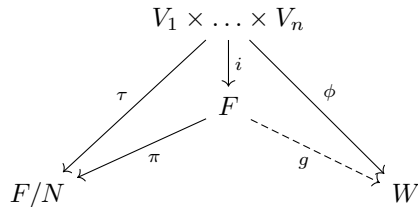
$$\begin{array}{ccc} & V_1 \times \dots \times V_n & \\ \tau \swarrow & & \searrow \phi \\ F/N & \xrightarrow{\quad f \quad} & W \end{array}$$

Dalej korzystamy z **Lematu (twierdzenie o izomorfizmie)**. Niech $W \subseteq V$ będzie podprzestrzenią. Wówczas dla każdego przekształcenia liniowego $\phi : V \rightarrow V'$ takiego, że $\ker(\phi) \supseteq W$, istnieje **dokładnie jedno** przekształcenie liniowe $\psi : V/W \rightarrow V'$ takie, że $\phi = \pi \circ \psi$. W szczególności dowolne przekształcenie liniowe $\phi : V \rightarrow W$ faktoryzuje się przez odpowiednie przekształcenie $\psi : V/\ker(\phi) \rightarrow W$ dane wzorem: $\psi(\alpha + \ker(\phi)) = \phi(\alpha)$. Dowód pozostawiam jak proste ćwiczenie (był on pokazany w dodatku do pierwszego semestru).

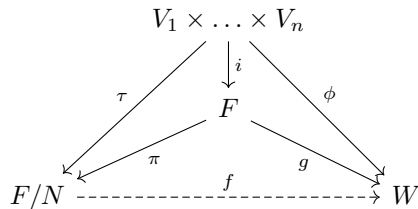
Wróćmy do dowodu. Przypomnijmy, że $\tau = \pi \circ i$.

$$\begin{array}{ccc} & V_1 \times \dots \times V_n & \\ & \downarrow i & \\ \tau \swarrow & F & \searrow \phi \\ \pi \swarrow & & \searrow \\ F/N & & W \end{array}$$

Skoro $V_1 \times \dots \times V_n$ jest bazą przestrzeni F , to istnieje jednoznacznie wyznaczone (na bazie!) przekształcenie liniowe $g : F \rightarrow W$ o własności $g \circ i = \phi$.



Ponieważ ϕ jest n -liniowe, to $N \subseteq \ker(g)$ (wprost z definicji N). Zatem na mocy lematu istnieje jednoznacznie wyznaczone odwzorowanie liniowe $f : F/N \rightarrow W$ spełniające $f \circ p = g$.



□

Dowód jest zatem zakończony. O co chodzi w tej konstrukcji? Zobaczmy kilka przykładów.

- Weźmy $V_1 = V_2 = V$, $K = \mathbb{R}$. Oto przykłady **różnych** elementów F :

$$2(v, 2v), \quad 2(v, v) + 2(v, v), \quad (2v, 2v), \quad 4(v, v), \quad 3(2v, v) - (v, 2v).$$

Wszystkie te elementy będą utożsamione w F/N z elementem: $4 \cdot v \otimes v$.

- Weźmy $V_1 = K[x], V_2 = K[y]$. Oto różne elementy F reprezentowane w iloczynie tensorowym $K[x] \otimes K[y]$ przez $4x \otimes y^2$, czyli: $(4x, y^2), (x, y^2) + 3(x, y^2), (2x, 2y^2)$, Elementy te utożsamiany z $4xy^2 \in K[x, y]$.
- Weźmy $V_1 = M_2(\mathbb{R})$ oraz $V_2 = \mathbb{C}$ jako przestrzeń nad \mathbb{R} . Wówczas elementy:

$$\left(\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, 1+i \right), \quad \left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, 2+2i \right),$$

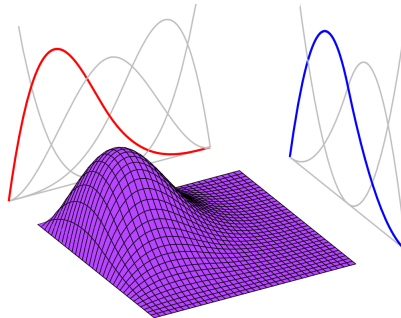
utożsamimy z macierzą z $M_2(\mathbb{C})$ postaci: $\begin{bmatrix} 2+2i & 0 \\ 0 & 2+2i \end{bmatrix}$.

- Niech K będzie ciałem oraz $n, m \geq 1$. Wówczas: $K^m \otimes K^n \simeq M_{m \times n}(K)$. Istotnie, traktując elementy K^n oraz K^m jako macierze jednokolumnowe mamy odwzorowanie:

$$K^m \times K^n \ni (x, y) \mapsto xy^T \in M_{m \times n}(K).$$

Jest to oczywiście odwzorowanie dwuliniowe i nietrudno pokazać, że odwzorowanie $\Psi(x \otimes y) = xy^T$ jest izomorfizmem liniowym. Dokładniej, można pokazać, że jeśli $\{u_1, \dots, u_m\}$ oraz $\{v_1, \dots, v_n\}$ są bazami standardowymi przestrzeni K^n oraz K^m , zaś $E_{ij} \in M_{m \times n}(K)$ są jedynkami macierzowymi, to $\Phi(u_i \otimes v_j) = E_{ij}$.

- $K[x] \otimes K[y] \simeq K[x, y]$. Istotnie, odwzorowanie $K[x] \times K[y] \ni (f, g) \mapsto f(x)g(y) \in K[x, y]$ jest dwuliniowe, więc istnieje odwzorowanie liniowe $\Phi : K[x] \otimes K[y] \rightarrow K[x, y]$ zadane wzorem $\Phi(f \otimes g) = f(x) \otimes g(y)$. Nietrudno widzieć, że jest to izomorfizm.



Ilustracja iloczynu tensorowego dwóch wielomianów Bernsteina. Źródło: Wikipedia.

Jak wyglądają elementy iloczynu tensorowego? Są to kombinacje liniowe tzw. tensorów prostych.

Definicja 24.22: Tensor prosty

Elementy przestrzeni $V_1 \otimes \dots \otimes V_n$ są kombinacjami liniowymi elementów postaci:

$$\pi(i(v_1, \dots, v_n)) = [(v_1, \dots, v_n)],$$

które nazywamy TENSORAMI PROSTYMI i oznaczamy

$$v_1 \otimes \dots \otimes v_n.$$

Oczywiście mamy np. w $V \otimes W$ nad \mathbb{R} : równości $2v \otimes w = v \otimes 2w = v \otimes w + v \otimes w = 4v \otimes \frac{1}{2}w + 0 \otimes 100w + 24v \otimes 0$. **Dobre ćwiczenie.** Załóżmy, że V jest przestrzenią liniową oraz $n \geq 1$. Przypuśćmy, że $v_1, \dots, v_n \in V$ są liniowo niezależne. Udowodnij, że jeśli dla pewnych $u_1, \dots, u_n \in V$ mamy:

$$v_1 \otimes u_1 + v_2 \otimes u_2 + \dots + v_n \otimes u_n = 0 \in V \otimes V,$$

to $u_1 = u_2 = \dots = u_n = 0$. W szczególności pozwala to na policzenie wymiaru $V \otimes V$.

Twierdzenie 24.5: Baza i wymiar iloczynu tensorowego

Niech $\{e_i\}_{i \in I}$ będzie bazą przestrzeni liniowej V oraz niech $\{f_j\}$ będzie bazą przestrzeni liniowej V — obydwu nad ciałem K . Wówczas zbiór tensorów prostych $\{e_i \otimes f_j\}_{(i,j) \in I \times J}$ jest bazą przestrzeni $V \otimes W$. W szczególności $\dim V \otimes W$ równy jest $\dim V \cdot \dim W$. Podobnie dla przestrzeni V_1, \dots, V_n nad ciałem K mamy $\dim V_1 \otimes \dots \otimes V_n = \dim V_1 \cdot \dim V_n$.

Przykład. Niech ϵ_1, ϵ_2 będzie bazą standardową przestrzeni \mathbb{R}^2 . Wówczas element $\epsilon_1 \otimes \epsilon_2 + \epsilon_2 \otimes \epsilon_1$ w $\mathbb{R}^2 \otimes \mathbb{R}^2$ nie jest tensorem prostym, czyli nie istnieją wektory $v, w \in \mathbb{R}^2$ takie, że $\epsilon_1 \otimes \epsilon_2 + \epsilon_2 \otimes \epsilon_1 = v \otimes w$.

Zajmijmy się teraz powiązaniem iloczynu tensorowego z tensorami zdefiniowanymi na początku. Kluczem jest następująca uwaga.

Obserwacja 24.4

Niech V będzie przestrzenią liniową nad K . Istnieje kanoniczny izomorfizm:

$$\underbrace{V^* \otimes \dots \otimes V^*}_p \otimes \underbrace{V \otimes \dots \otimes V}_q \mapsto \mathbb{T}_p^q(V)$$

przypisujący tensorowi:

$$f^1 \otimes \dots \otimes f^p \otimes v_1 \otimes \dots \otimes v_q, \quad f^i \in V^*, v_j \in V,$$

odwzorowanie wieloliniowe $T : V^p \times (V^*)^q \rightarrow K$ określone wzorem:

$$T(u_1, \dots, u_p, g^1, \dots, g^q) = f^1(u_1) \dots f^p(u_p) \cdot g^1(v_1) \dots g^q(v_q).$$

Możemy teraz zdefiniować potęgi tensorowe i przejść do tensorów symetrycznych i antysymetrycznych.

Definicja 24.23: Potęga tensorowa

Niech V będzie przestrzenią liniową. Wówczas p -krotny iloczyn tensorowy $V \otimes \dots \otimes V$ nazywa się p -krotną potęgą tensorową przestrzeni V i oznacza przez $V^{\otimes p}$. Innymi słowy:

$$\mathbb{T}_p^q(V) \simeq (V^*)^{\otimes p} \otimes V^{\otimes q}.$$

Za pomocą potęgi tensorowej uzyskamy przestrzenie tensorów, zdefiniowane na początku dodatku.

Definicja 24.24: Potęga symetryczna i potęga zewnętrzna

Niech $n \geq 1$ oraz V będzie przestrzenią liniową nad ciałem K . Rozważmy n -tą potęgę tensorową $T^n V = V^{\otimes n} = V \otimes \cdots \otimes V$ oraz jej podprzestrzenie

$$N_s = \text{lin}\{v_1 \otimes \cdots \otimes v_n - v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)} : v_1, \dots, v_n \in V \text{ oraz } \sigma \in S_n\},$$
$$N_a = \text{lin}\{v_1 \otimes \cdots \otimes v_n : v_1, \dots, v_n \in V \text{ oraz } v_i = v_j \text{ dla pewnych } 1 \leq i < j \leq n\}.$$

Zdefiniujmy $\sum^n V = T^n V / N_s$ oraz $\bigwedge^n V = T^n V / N_a$. Niech ponadto

$$\tau_s = p_s \circ \tau \quad \text{oraz} \quad \tau_a = p_a \circ \tau,$$

gdzie $\tau: V \times \cdots \times V \rightarrow T^n V$ to kanoniczne odwzorowanie n -liniowe, zaś $p_s: T^n V \rightarrow \sum^n V$ oraz $p_a: T^n V \rightarrow \bigwedge^n V$ to naturalne rzutowania.

Przestrzenie $\sum^n V$ oraz $\bigwedge^n V$ nazywamy, odpowiednio, n -TĄ POTĘGĄ SYMETRYCZNĄ oraz n -TĄ POTĘGĄ ZEWNĘTRZNĄ przestrzeni V . Elementy przestrzeni $\bigwedge^n V$ nazywamy czasami n -WEKTORAMI, zaś elementy $\bigwedge^n V^*$ nazywamy n -FORMAMI.

Obserwacja 24.5: Ćwiczenie

Niech $n \geq 1$ oraz V będzie przestrzenią liniową nad ciałem K . Niech

$$v_1 \odot \cdots \odot v_n = \tau_s(v_1, \dots, v_n) \quad \text{oraz} \quad v_1 \wedge \cdots \wedge v_n = \tau_a(v_1, \dots, v_n)$$

dla dowolnych $v_1, \dots, v_n \in V$. Udowodnij, że gdy $\dim V = m < \infty$ oraz zbiór $\{e_1, \dots, e_m\}$ jest bazą przestrzeni V , to zbiory

$$\{e_{i_1} \odot \cdots \odot e_{i_n} : 1 \leq i_1 \leq \cdots \leq i_n \leq m\} \quad \text{oraz} \quad \{e_{i_1} \wedge \cdots \wedge e_{i_n} : 1 \leq i_1 < \cdots < i_n \leq m\}$$

są bazami przestrzeni $\sum^n V$ oraz $\bigwedge^n V$, odpowiednio. W szczególności

$$\dim \sum^n V = \binom{n+m-1}{n} \quad \text{oraz} \quad \dim \bigwedge^n V = \binom{m}{n}.$$

Powoli musimy zatrzymać ten wstęp. Przywołałiśmy kluczowe pojęcia niezbędne do zrozumienia wybranych definicji na analizie matematycznej. Warto być może na koniec zilustrować ważne pojęcie 2-wektorów za pomocą geometrii. Przyjrzymy się więc przestrzeni 2-wektorów, czyli tensorów antysymetrycznych na przestrzeni rzeczywistej V . Składa się ona z sum postaci

$$\sum a_i(u_i \wedge v_i),$$

gdzie x_i są liczbami rzeczywistymi, zaś u_i, v_i są wektorami z V , które spełniają następujące zależności:

$$(a_1 u_1 + a_2 u_2) \wedge v = a_1(u_1 \wedge v) + a_2(u_2 \wedge v), \quad u \wedge (b_1 v_1 + b_2 v_2) = b_1(u \wedge v_1) + b_2(u \wedge v_2)$$
$$u \wedge u = 0, \quad u \wedge v + v \wedge u = 0.$$

Innymi słowy produkt zewnętrzny (tak nazywamy często operację \wedge) wektorów jest rozdzielny ze względu na dodawanie, ale nieprzemienne. Jak go interpretować geometrycznie? Jeżeli $u = (x_1, x_2)$ oraz $v = (y_1, y_2)$, wówczas dla bazy standardowej ϵ_1, ϵ_2 przestrzeni \mathbb{R}^2 , wówczas:

$$u \wedge v = (x_1 \epsilon_1 + x_2 \epsilon_2) \wedge (y_1 \epsilon_1 + y_2 \epsilon_2) = (x_1 y_2 - x_2 y_1) \epsilon_1 \wedge \epsilon_2.$$

Wyrażenie $x_1 y_2 - x_2 y_1$ jest dwukrotnością pola trójkąta uformowanego przez początek układu współrzędnych, punkty (x_1, x_2) , (y_1, y_2) oraz jest liczbą dodatnią, jeśli orientacja trójkąta jest przeciwna z kierunkiem ruchu wskazówek zegara (orientacja zgodna z bazą standardową).

Równanie na $u \wedge v$ pokazuje, że produkt zewnętrzny wektorów bazowych $\epsilon_1 \wedge \epsilon_2$ jest bazą przestrzeni 2-wektorów. Jest ona jednowymiarowa. Wynika stąd, że $u \wedge v = 0$ wtedy i tylko wtedy, gdy u, v są liniowo zależne. Licząc natomiast $u \wedge v \wedge w$, gdzie u, v, w leżą w \mathbb{R}^2 . Jest to wyrażenie postaci $\sum x_i y_j z_k (\epsilon_i \wedge \epsilon_j \wedge \epsilon_k)$, gdzie i, j, k to liczby 1 lub 2. Skoro $\epsilon_i \wedge \epsilon_i = 0$ oraz $\epsilon_j \wedge 0 = 0 \wedge \epsilon_k = 0$, to oznaczają, że $u \wedge v \wedge w = 0$.

Obserwacja 24.6

Niech \mathbb{R}^2 będzie przestrzenią afiniczną. Punkty a, b, c są współliniowe wtedy i tylko wtedy, gdy

$$a \wedge b + b \wedge c + c \wedge a = 0.$$

Dowód. Jeśli $a = x_1\epsilon_1 + x_2\epsilon_2$, $b = y_1\epsilon_1 + y_2\epsilon_2$, $c = z_1\epsilon_1 + z_2\epsilon_2$, wówczas wektor $a \wedge b + b \wedge c + c \wedge a$ to:

$$[(x_1y_1 - x_2y_1) + (y_1z_2 - y_2z_1) + (z_1x_2 - z_2x_1)](\epsilon_1 \wedge \epsilon_2) = 0.$$

A zatem wektor powyższy równy jest zero wtedy i tylko wtedy, gdy

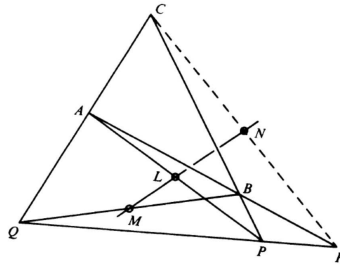
$$\begin{vmatrix} x_1 & x_2 & 1 \\ y_1 & y_2 & 1 \\ z_1 & z_2 & 1 \end{vmatrix} = 0.$$

□

Przykładowym zastosowaniem jest klasyczne twierdzenie Newtona (i wiele innych).

Obserwacja 24.7: Twierdzenie Newtona

Niech A, B, P, Q będą takimi punktami na płaszczyźnie rzeczywistej, że żadne trzy z prostych AB, BP, PQ, QA nie są współliniowe. Proste AQ oraz BP przecinają się w punkcie C , zaś proste AB, PQ przecinają się w punkcie R . Wówczas środki odcinków AP, BQ, CR są współliniowe.



Dowód. Niech L, M, N będą środkami odcinków AP, BQ, CR . Wówczas mamy:

$$2L = A + P, \quad 2M = B + Q, \quad 2N = C + R.$$

Wówczas:

$$4L \wedge M = (A + P) \wedge (B + Q) = A \wedge B + A \wedge Q + P \wedge B + P \wedge Q,$$

$$4M \wedge N = (B + Q) \wedge (C + R) = B \wedge C + B \wedge R + Q \wedge C + Q \wedge R$$

$$4N \wedge L = (C + R) \wedge (A + P) = C \wedge A + C \wedge P + R \wedge A + R \wedge P.$$

Dodając te równania stronami widzimy, że skoro punkty A, B, R są współliniowe, podobnie trójki A, Q, C , P, B, C oraz P, Q, R są odpowiednio współliniowe, czyli

$$A \wedge B + B \wedge R + R \wedge A = 0,$$

$$A \wedge Q + Q \wedge C + C \wedge A = 0,$$

$$P \wedge B + B \wedge C + C \wedge P = 0,$$

$$P \wedge Q + Q \wedge R + R \wedge P = 0.$$

Stąd po dodaniu równań po prawej stronie nic nie zostaje, a na lewej mamy po odpowiednim uproszczeniu równość $L \wedge M + M \wedge N + N \wedge L = 0$, co pokazuje, że L, M, N leżą na jednej prostej. □

Podobne zastosowania można znajdować pośród 3-wektorów na przestrzeni trójwymiarowej. W nieco starszych pozycjach zamiast 2- i 3-wektorów mówimy o biwektorach i triwektorach. Nie może nas dziwić, że najciekawsze zastosowania mają właśnie tensory symetryczne i antysymetryczne. Podobnie rozważania form dwuliniowych są najciekawsze dla form symetrycznych i antysymetrycznych. Niewątpliwie jednak także ogólna teoria ma istotne zastosowania, zwłaszcza przy uogólnieniu do tzw. modułów nad pierścieniami (przemiennymi i nieprzemiennymi).

24.3 To nie trivia. Wielomiany symetryczne

Poniższy krótki tekst piszę na podstawie skryptu dr. Michała Krycha², aby zaprezentować kilka ważnych faktów dotyczących wielomianów symetrycznych. Korzystam również z rozdziału 11 monografii³ Wacława Sierpińskiego *Zasady algebry wyższej*, cytując wybrane rezultaty. Zaczniemy od rozwiązania układu:

$$\begin{cases} x^2 + y^2 = 13 \\ xy = 6 \end{cases}.$$

Ciekawą metodą rozwiązania jest przyjęcie nowe zmienne $u = x + y$ oraz $v = yx$. Wówczas:

$$x^2 + y^2 = (x + y)^2 - 2xy = u^2 - 2v.$$

Zatem układ ma postać:

$$\begin{cases} u^2 - 2v = 13, \\ v = 6 \end{cases}.$$

Bez trudu odczytujemy rozwiązania (x, y) postaci $(2, 3), (3, 2), (-2, -3), (-3, -2)$. Podstawienie opisane wyżej można stosować w niektórych przypadkach. Aby je wskazać zaczniemy od definicji.

Definicja 24.25: Funkcja symetryczna

Wielomian $F = \sum_{i_1, \dots, i_n} a_{i_1 \dots i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \in K[x_1, \dots, x_n]$ nazywamy SYMETRYCZNYM, jeśli dla każdej permutacji σ zbioru n -elementowego $\{1, \dots, n\}$ mamy

$$a_{i_1 \dots i_n} = a_{i_{\sigma(1)} i_{\sigma(2)} \dots i_{\sigma(n)}}.$$

Funkcję $f : K^n \rightarrow K$ nazwiemy SYMETRYCZNA wtedy i tylko wtedy, gdy dla każdej permutacji σ zbioru n -elementowego $\{1, \dots, n\}$ i każdego $(x_1, \dots, x_n) \in K^n$ zachodzi równość:

$$f(x_1, x_2, \dots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}).$$

Wielomiany $x_1^2 + x_2^2, x_1 x_2, x_1^4 - x_1^2 x_2^2 - x_2^4 \in K[x_1, x_2]$ są symetryczne, a wielomiany $x_1^2 - x_2^2, x_1 + 3x_2, x_1^3 + x_1^2 x_2 + x_2^3$ nie są symetryczne.

Twierdzenie 24.6: O wielomianach symetrycznych, wersja prosta

Jeśli $f \in \mathbb{R}[x, y]$ jest wielomianem symetrycznym zmiennych x, y , to istnieje dokładnie jeden taki wielomian $g \in \mathbb{R}[x, y]$, że $g(x + y, xy) = f(x, y)$.

Dowód. Dowodzimy to twierdzenie przez indukcję względem $\deg f$. Jeśli $\deg f = 1$, to $f(x, y) = ax + by + c$. Ponieważ $a + c = f(1, 0) = f(0, 1) = b + c$, to $a = b$. Wobec tego $f(x, y) = a(x + y) + c$, więc możemy przyjąć w takim przypadku $g(u, v) = u + c$, by mieć zapewnioną tezę dla wielomianów stopnia 1.

Dowodzimy tylko istnienie g . Załóżmy, że twierdzenie zachodzi dla wszystkich wielomianów stopnia nie większego niż k oraz, że $\deg f = k + 1$. Wówczas w zapisie wielomianu f występuje składnik $ax^r y^s$, występuje składnik $ax^s y^r$. Tezę indukcyjną należy więc jedynie wykazać dla wielomianów postaci $ax^r y^s + ax^s y^r$. Jeśli $0 < r < s$, to

$$ax^r y^s + ax^s y^r = a(xy)^r (y^{s-r} + x^{s-r}),$$

skąd wynika, że w żądanej postaci należy przedstawić wielomian $y^{s-r} + x^{s-r}$, co wiemy dzięki założeniu indukcyjnemu. Rozpatrujemy zatem jedynie wielomian $x^{k+1} + y^{k+1}$. Ma on postać:

$$x^{k+1} + x^k y + y^{k+1} - xy(x^{k-1} + y^{k-1}) = (x + y)(x^k + y^k) - xy(x^{k-1} + y^{k-1}).$$

□

²https://www.mimuw.edu.pl/~krych/staszic/skrypt13-uklady-row_D.pdf

³<http://matwbn.icm.edu.pl/ksiazki/mon/mon11/mon1109.pdf>

Twierdzenie to pozostaje prawdziwe dla wielomianów symetrycznych dowolnej liczby zmiennych, ale wtedy trzeba zamiast $u = x + y$ oraz $v = xy$ mówić o zmiennych:

$$\begin{aligned} u_1 &= x_1 + x_2 + \dots + x_n \\ u_2 &= x_1x_2 + x_1x_3 + \dots + x_1x_k + x_2x_2 + x_2x_4 + \dots + x_{k-1}x_k \\ u_3 &= x_1x_2x_3 + x_1x_2x_4 + \dots + x_{k-2}x_{k-1}x_k \\ &\vdots \\ u_k &= x_1x_2 \dots x_k, \end{aligned}$$

zwanych ELEMENTARNYMI WIELOMIANAMI SYMETRYCZNYMI.

Dowód można przeczytać w książce W. Sierpińskiego, łącznie z pokazaniem, że elementarne wielomiany symetryczne są algebraicznie niezależne, to znaczy: nie istnieje wielomian W z $K[x_1, \dots, x_k]$ taki, że $W(u_1, \dots, u_k) = 0$. Odnotujmy, że wiele innych funkcji jest algebraicznie zależnych. Na przykład: dla funkcji $\sin x, \cos x$, wtedy wielomian $W(y_1, y_2) = y_1^2 + y_2^2 - 1$ nie jest zerowy, a jednak $W(\sin x, \cos x) = 0$. Zauważmy, że zgodnie ze wzorami Viete'a elementarne wielomiany symetryczne zmiennych x_1, \dots, x_k występują jako współczynniki wielomianu zmiennej t postaci:

$$(t - x_1)(t - x_2) \dots (t - x_k) = t^k - u_1t^{k-1} + u_2t^{k-2} - \dots + (-1)^k s_k.$$

Różne zastosowania wyniku wyżej, a także wyniki dotyczące jednoznaczności można znaleźć w tekście K. Conrada: <https://kconrad.math.uconn.edu/blurbs/galoistheory/symmfunction.pdf>. Jednym z kluczowych są wzory Newtona. Dotyczą one przedstawiania wielomianów będących sumami potęg jako wielomianów symetrycznych. Oto przykłady:

$$x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_2x_3 + x_3x_1).$$

W zbiorze $K[x_1, \dots, x_n]$ definiujemy wielomiany

$$s_k = x_1^k + x_2^k + \dots + x_n^k.$$

Zachęcam Czytelnika do pokazania następujących własności, przyjmując $s_k = 0$, dla $k < 0$.

- Dla $k > n$ mamy $s_k - u_1s_{k-1} + u_2s_{k-2} - \dots + (-1)^n u_n s_{k-n} = 0$.
- Pokaż, że dla $1 \leq k \leq n$ mamy

$$s_k - u_1s_{k-1} + u_2s_{k-2} - \dots + (-1)^{k-1} u_{k-1} s_1 + (-1)^k u_n = 0.$$

- O ile charakterystyka ciała K jest równa 0, to każdy wielomian symetryczny w $K[x_1, \dots, x_n]$ jest wielomianem od zmiennych s_1, \dots, s_k . Gdy poznacie Państwo pojęcie działania grupy na zbiorze, wówczas mówienie o wielomianach symetrycznych nabierze znacznie więcej sensu.

* * *

Rozważmy jeszcze jeden ciekawy przykład, czyli rozwiążmy w liczbach rzeczywistych układ

$$\begin{cases} x^3 + y^3 + z^3 = 1 \\ x + y + z = 1 \end{cases}$$

ROZWIĄZANIE. Zauważmy, że jeśli trójka x, y, z jest rozwiązaniem tego układu, to

$$(x + y + z)^3 - (x^3 + y^3 + z^3) = 0.$$

Zauważmy, że gdy $x + y = 0$, to równanie jest prawdziwe dla każdego z . W szczególności wielomian $(x + y + z)^3 - (x^3 + y^3 + z^3)$ można zapisać w postaci:

$$(x + y + z)^3 - (x^3 + y^3 + z^3) = \lambda(x + y)(y + z)(z + x).$$

Wstawiając do powyżej tożsamości np. $x = 1, y = 1, z = 0$ dostajemy $2\lambda = 6$, czyli $\lambda = 3$. Wobec tego równanie ma rozwiązanie, gdy $3(x + y)(y + z)(z + x) = 0$, co oznacza, że:

- gdy $x + y = 0$, to $z = 1$; wtedy rozwiązaniami są trójki $(x, -x, 1)$, gdzie $x \in \mathbb{R}$,
- gdy $y + z = 0$, to $x = 1$; wtedy rozwiązaniami są trójki $(1, y, -y)$, gdzie $y \in \mathbb{R}$,
- gdy $z + x = 0$, to $y = 1$; wtedy rozwiązaniami są trójki $(-z, 1, z)$, gdzie $x \in \mathbb{R}$.

■

Rozdział 25

Hiperpowierzchnie stopnia 2

Na ostatnim wykładzie wprowadziliśmy pojęcie wielomianu, funkcji wielomianowej oraz zbioru algebraicznego i hiperpowierzchni. Naszym celem jest znajdowanie możliwie prostych równań opisujących hiperpowierzchnie. Równanie opisujące zależy od wyboru układu bazowego w przestrzeni afinicznej zawierającej hiperpowierzchnię. Zaczniemy od bardzo prostego przypadku hiperpowierzchni stopnia 1. Intuicja mówi, że zbiory opisywalne przez równania liniowe to po prostu podprzestrzenie afiniczne. Tak jest w istocie.

Obserwacja 25.1

Hiperpowierzchnie stopnia 1 w n -wymiarowej przestrzeni afinicznej H to $n - 1$ -wymiarowe podprzestrzenie afiniczne przestrzeni H . Takie podprzestrzenie nazywamy HIPERPLASZCZYZNAMI.

Dowód. Jeśli $X \subset H$ jest hiperpowierzchnią stopnia 1, to dla pewnego układu bazowego $p_0; \alpha_1, \dots, \alpha_n$ mamy (z definicji) $X = \{p_0 + x_1\alpha_1 + \dots + x_n\alpha_n \in H \mid a_1x_1 + \dots + a_nx_n + b = 0\}$, dla pewnych $a_1, \dots, a_n \in K$. A zatem H jest hiperplaszczyną, bo zbiorem rozwiązań równania $a_1x_1 + \dots + a_nx_n + b = 0$ jest warstwa podprzestrzeni liniowej wymiaru $n - 1$. Na odwrót: niech $X \subset H$ będzie hiperplaszczyną, czyli podprzestrzenią afiniczną wymiaru $n - 1$ i niech $p_0; \alpha_1, \dots, \alpha_n$ będzie układem bazowym przestrzeni H . Wówczas zbiór $\{(x_1, \dots, x_n) \in K^n \mid p_0 + x_1\alpha_1 + \dots + x_n\alpha_n\}$ jest podprzestrzenią afiniczną wymiaru $n - 1$ w K^n , więc można go opisać równaniem liniowym $a_1x_1 + \dots + a_nx_n + b = 0$. \square

Głównym przedmiotem naszego zainteresowania będą hiperpowierzchnie stopnia 2, w opisie których wykorzystamy teorię form kwadratowych. Przypominam, że od poprzedniego wykładu **pracujemy wyłącznie nad ciałami nieskończonymi charakterystyki różnej od 2**.

Obserwacja 25.2

Każdy wielomian F stopnia 2, zmiennych x_1, \dots, x_n , o współczynnikach w ciele K , jest jednoznacznie wyznaczony przez macierz symetryczną $A \in M_{n \times n}(K)$, macierz $B \in M_{1 \times n}(K)$ oraz element $c \in K$ w następujący sposób: jeśli $x = [x_1 \ x_2 \ \dots \ x_n]^T$, to:

$$F = x^T Ax + Bx + c.$$

Dla przykładu mamy (ważne: zakładamy przemienność mnożenia zmiennych, np. $x_2x_1 = x_1x_2$):

$$2x_1^2 + 3x_2^2 + 10x_1x_2 - 3x_1 + 4x_2 + 6 = [x_1 \ x_2] \cdot \begin{bmatrix} 2 & 5 \\ 5 & 3 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + [-3 \ 4] \cdot \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + 6.$$

Dowód. Weźmy dowolny wielomian $F \in K[x_1, \dots, x_n]$ stopnia 2 i niech $F = F_2 + F_1 + F_0$, gdzie $F_i \in K[x_1, \dots, x_n]$ oraz F_i jest sumą jednomianów stopnia i , dla $i = 0, 1, 2$. Załóżmy też, że $f, f_0, f_1, f_2 : K^n \rightarrow K$ są funkcjami wielomianowymi odpowiadającymi (w sposób jednoznaczny) wielomianom F, F_0, F_1, F_2 w układzie bazowym $(0, 0, \dots, 0); st$. Wówczas istnieje forma kwadratowa $q : K^n \rightarrow K$, przekształcenie liniowe $g : K^n \rightarrow K$ oraz funkcja stała $c : K^n \rightarrow K$ takie, że $(q + g + c)(t_1, \dots, t_n)$ równe jest $f_2(t_1, \dots, t_n) + f_1(t_1, \dots, t_n) + f_0(t_1, \dots, t_n) = f(x_1, \dots, x_n)$. Zatem przyjmując za A macierz formy q w bazie standardowej, za B macierz przekształcenia g w bazie standardowej oraz $c = f(0, 0, \dots, 0)$ dostajemy żądany wynik. \square

W powyższym rozumowaniu przypisaliśmy wielomianowi F stopnia 2 formę kwadratową, przekształcenie liniowe i funkcję stałą poprzez uznanie, że wielomian ten zadaje pewną funkcję wielomianową w „standardowym” układzie bazowym. Wiedząc o istnieniu F wnioskujemy, że przy zmianie układu bazowego funkcja ta będzie zadawana przez inny wielomian. Wygodnie śledzić zależność tych wielomianów w oparciu o wprowadzone niezmienniki, zwłaszcza odpowiednią macierz formy kwadratowej.

Obserwacja 25.3

Założmy, że funkcji wielomianowej $f : H \rightarrow K$ stopnia 2 na n -wymiarowej przestrzeni afinicznej H odpowiada w układzie bazowym $p_0; \mathcal{A}$ wielomian $F \in K[x_1, \dots, x_n]$ postaci:

$$F = x^T A x + B x + c,$$

gdzie $x = [x_1 \dots x_n]^T$. Wówczas w układzie bazowym $q_0; \mathcal{B}$ funkcji f odpowiada wielomian

$$G = x^T A' x + B' x + c',$$

przy czym $A' = C^T A C$, gdzie $C = M(\text{id})_{\mathcal{B}}^{\mathcal{A}}$.

Dowód. Niech $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$, $\mathcal{B} = (\beta_1, \dots, \beta_n)$. Jeśli $q_0 + y_1 \beta_1 + \dots + y_n \beta_n = p_0 + x_1 \alpha_1 + \dots + x_n \alpha_n$, to dla $x = [x_1 \dots x_n]^T$ oraz $y = [y_1 \dots y_n]^T$ mamy $x = C y + w$, gdzie $C = M(\text{id})_{\mathcal{B}}^{\mathcal{A}}$ oraz gdzie $w = [w_1 \dots w_n]^T$ spełnia $q_0 = p_0 + w_1 \alpha_1 + \dots + w_n \alpha_n$. Wówczas:

$$\begin{aligned} x^T A x + B x + c &= (y^T C^T + w^T) A (C y + w) + B (C y + w) + c = \\ &= y^T (C^T A C) y + y^T C^T A w + w^T A C y + w^T A w + B C y + B w + c. \end{aligned}$$

Przy tym $y^T C^T A w = (y^T C^T A w)^T = w^T A C y$. Stąd teza zachodzi dla:

$$A' = C^T A C, \quad B' = 2w^T A C + B C, \quad c' = w^T A w + B w + c.$$

□

Przykład. Niech $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ zadana będzie w układzie bazowym $(0, 0); (1, 0), (0, 1)$ wielomianem $F = 2x_1^2 + 3x_2^2 + 10x_1x_2 - 3x_1 + 4x_2 + 6$, jak wyżej, dla którego

$$A = \begin{bmatrix} 2 & 5 \\ 5 & 3 \end{bmatrix}, \quad B = [3 \quad -4], \quad C = 6.$$

Weźmy układ bazowy $q_0 = (1, 2); \beta_1 = (-2, 5), \beta_2 = (1, 1)$. Wówczas kładąc $p_0 = (0, 0)$, $\alpha_1 = (1, 0), \alpha_2 = (0, 1)$ oraz $\mathcal{A} = ((1, 0), (0, 1)), \mathcal{B} = ((-2, 5), (1, 1))$ dostajemy:

$$C = M(\text{id})_{\mathcal{B}}^{\mathcal{A}} = \begin{bmatrix} -2 & 1 \\ 5 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 \\ 2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \quad \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} -2 & 1 \\ 5 & 1 \end{bmatrix} \cdot \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} + \begin{bmatrix} 1 \\ 2 \end{bmatrix}.$$

A zatem postać wielomianu G opisującego funkcję wielomianową f w układzie bazowym $q_0; \mathcal{B}$ uzyskujemy przez zamianę zmiennych $x_1 = -2y_1 + x_2 + 1, x_2 = 5y_1 + y_2 + 2$ w wielomianie F . Część kwadratowa wielomianu G opisana jest warunkiem $[y_1 \quad y_2] \cdot A' \cdot \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$, gdzie $C = M(\text{id})_{\mathcal{B}}^{\mathcal{A}}$ oraz

$$A' = C^T A C = \begin{bmatrix} -2 & 5 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 2 & 5 \\ 5 & 3 \end{bmatrix} \cdot \begin{bmatrix} -2 & 1 \\ 5 & 1 \end{bmatrix} = \begin{bmatrix} -17 & 26 \\ 26 & 15 \end{bmatrix}.$$

Więc część kwadratowa wielomianu G wynosi $-17y_1^2 + 52y_1y_2 + 15y_2^2$.

Wniosek 25.1

Macierze symetryczne części kwadratowych wielomianów stopnia 2 odpowiadających (w zadanych układach bazowych) tej samej funkcji wielomianowej $f : H \rightarrow K$ stopnia 2 są kongruentne. W szczególności macierze te mają ten sam rząd.

Definicja 25.1: Rząd funkcji wielomianowej

RZĘDEM FUNKCJI WIELOMIANOWEJ $f : H \rightarrow K$ stopnia 2 nazywamy rząd macierzy części kwadratowej wielomianu, który odpowiada f w pewnym układzie bazowym przestrzeni H . Rząd funkcji f oznaczamy $r(f)$.

Sformułuję teraz serię definicji i twierdzeń. Dowody zostaną odsunięte do dalszej części, dając nam najpierw pewien przegląd rezultatów. Zaczniemy od przestrzeni dowolnego wymiaru.

Twierdzenie 25.1

Niech $f : H \rightarrow K$ będzie funkcją wielomianową stopnia 2 określoną na n wymiarowej przestrzeni afinicznej H nad ciałem nieskończonym charakterystyki różnej od 2. Wówczas istnieje taki układ bazowy w H , w którym funkcji f odpowiada wielomian postaci:

$$\begin{aligned} & \text{(i)} \quad a_1x_1^2 + \dots + a_rx_r^2 + c \quad \text{gdzie} \quad r = r(f) \quad \text{oraz} \quad a_1, \dots, a_r \neq 0 \\ \text{lub} & \text{(ii)} \quad a_1x_1^2 + \dots + a_rx_r^2 + x_n \quad \text{gdzie} \quad r = r(f) < n \quad \text{oraz} \quad a_1, \dots, a_r \neq 0. \end{aligned}$$

Wniosek 25.2

Dla każdej hiperpowierzchni X stopnia 2 w n wymiarowej przestrzeni afinicznej istnieje układ bazowy, w którym X jest opisana równaniem postaci:

$$\begin{aligned} & \text{(a)} \quad a_1x_1^2 + \dots + a_rx_r^2 + c = 0 \quad \text{gdzie} \quad 1 \leq r \leq n \quad \text{oraz} \quad a_1, \dots, a_r \neq 0 \\ \text{lub} & \text{(b)} \quad a_1x_1^2 + \dots + a_rx_r^2 + x_n = 0 \quad \text{gdzie} \quad 1 \leq r \leq n - 1 \quad \text{oraz} \quad a_1, \dots, a_r \neq 0. \end{aligned}$$

Nieformalnie rzecz biorąc powyższe twierdzenie i wniosek odnoszą się do faktu, że nad ciałem charakterystyki różnej od 2 każda przestrzeń dwuliniowa ma bazę prostopadłą. Stąd w przypadkach (i)-(ii) postać wielomianów nie posiada jednomianów stopnia 2 innych niż kwadraty pojedynczych zmiennych. Pewnego wysiłku wymaga pokazanie, że postać części liniowej jest tylko jedną z dwóch możliwych. Dowód ten pokazę w drugiej części wykładu. Sformułujemy teraz, podobnie jak w przypadku przestrzeni dwuliniowych, wnioski związane z hiperpowierzchniami w rzeczywistych i zespolonych przestrzeniach afinicznych.

Wniosek 25.3

Dla każdej hiperpowierzchni X stopnia 2 w n wymiarowej przestrzeni afinicznej nad ciałem \mathbb{C} istnieje układ bazowy, w którym X opisana jest równaniem postaci:

$$\begin{aligned} & \text{(c1)} \quad x_1^2 + \dots + x_r^2 + 1 = 0 \quad \text{gdzie} \quad 1 \leq r \leq n \\ \text{lub} & \text{(c2)} \quad x_1^2 + \dots + x_r^2 = 0 \quad \text{gdzie} \quad 2 \leq r \leq n - 1 \\ \text{lub} & \text{(c3)} \quad x_1^2 + \dots + x_r^2 + x_n = 0 \quad \text{gdzie} \quad 1 \leq r \leq n - 1 \end{aligned}$$

Dowód. Niech w układzie bazowym $p_0; \alpha_1, \dots, \alpha_n$ hiperpowierzchnia X będzie opisana równaniem typu (a) lub (b) z Wniosku 1, w którym a_1, \dots, a_r są niezerowymi liczbami zespolonymi. Możemy przy tym zakładać, że w równaniu typu (a) współczynnik c wynosi 0 lub 1 (bo dla dowolnego $c \neq 0$ możemy równanie (a) przemnożyć przez c^{-1}). Rozpatrzmy liczby zespolone d_1, \dots, d_r takie, że $d_i^2 = a_i$, dla $i = 1, \dots, r$. Wówczas w układzie bazowym $p_0; \frac{1}{d_1}\alpha_1, \dots, \frac{1}{d_r}\alpha_r, \alpha_{r+1}, \dots, \alpha_n$ hiperpowierzchnia X jest opisana równaniem jednego z typów:

- (c1), gdy w $p_0; \alpha_1, \dots, \alpha_n$ była ona opisana równaniem typu (a) z $c = 1$,
- (c2), gdy w $p_0; \alpha_1, \dots, \alpha_n$ była ona opisana równaniem typu (a) z $c = 0$,
- (c3), gdy w $p_0; \alpha_1, \dots, \alpha_n$ była ona opisana równaniem typu (b).

Wniosek 25.4

Dla każdej hiperpowierzchni X stopnia 2 w n wymiarowej przestrzeni afinicznej nad ciałem liczb rzeczywistych \mathbb{R} istnieje układ bazowy, w którym X jest opisana równaniem postaci:

$$\begin{aligned} & (r1) \quad x_1^2 + \dots + x_s^2 - x_{s+1}^2 - \dots - x_r^2 + 1 = 0 \quad \text{gdzie} \quad 0 \leq s < r \leq n \\ \text{lub} & \\ & (r2) \quad x_1^2 + \dots + x_s^2 - x_{s+1}^2 - \dots - x_r^2 = 0 \quad \text{gdzie} \quad 1 \leq s < r \leq n \\ \text{lub} & \\ & (r3) \quad x_1^2 + \dots + x_s^2 - x_{s+1}^2 - \dots - x_r^2 + x_n = 0 \quad \text{gdzie} \quad 0 \leq s < r \leq n - 1 \end{aligned}$$

Dowód. Postępujemy jak w dowodzie poprzedniego wniosku. Współczynniki a_1, \dots, a_r są teraz niezerowymi liczbami rzeczywistymi. Po ich ewentualnym przenumerowaniu możemy zakładać, że $a_i > 0$ dla $i \leq s$ oraz $a_i < 0$ dla $i \geq s + 1$, dla pewnego $s \geq 0$. Rozpatrzmy liczby rzeczywiste d_1, \dots, d_r takie, że $d_i^2 = |a_i|$, dla $i = 1, \dots, r$. Wówczas w układzie bazowym $p_0; \frac{1}{d_1}\alpha_1, \dots, \frac{1}{d_r}\alpha_r, \alpha_{r+1}, \dots, \alpha_n$ hiperpowierzchnia X jest opisana równaniem typu (r1) lub (r2) lub (r3). □

Szczególnie eleganckie rezultaty dotyczące opisywalności hiperpowierzchni stopnia 2 uzyskuje się dla ważnej klasy hiperpowierzchni, które teraz definiuje.

Definicja 25.2: Hiperpowierzchnia właściwa

Mówimy, że hiperpowierzchnia X stopnia 2, w n wymiarowej przestrzeni afinicznej H jest WŁAŚCIWA, jeśli X nie jest zawarta w $n - 1$ wymiarowej podprzestrzeni afinicznej przestrzeni H .

Przykłady.

- Sfera $\{x_1, x_2, x_3 \in \mathbb{R}^3 \mid x_1^2 + x_2^2 + x_3^2 = 1\}$ jest właściwą hiperpowierzchnią stopnia 2 w przestrzeni \mathbb{R}^3 .
- Zbiór $X = \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1^2 + x_2^2 = 0\} = \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1 = x_2 = 0\}$ nie jest hiperpowierzchnią właściwą. X jest prostą $(0, 0, 0) + \text{lin}((0, 0, 1))$.

Zacznijmy od twierdzenia, którego dowód możecie Państwo znaleźć we „Wstępie do Algebry” Kostrikin, Jego wymowa powinna być jednak stosunkowo czytelna.

Twierdzenie 25.2

Niech X będzie hiperpowierzchnią stopnia 2 w przestrzeni afinicznej H nad ciałem K i niech $p_0; \alpha_1, \dots, \alpha_n$ będzie układem bazowym przestrzeni H .

- Jeśli X jest właściwa oraz $F, G \in K[x_1, \dots, x_n]$ są takimi wielomianami stopnia 2, że X jest opisana w układzie bazowym $p_0; \alpha_1, \dots, \alpha_n$ zarówno równaniem $F = 0$, jak i $G = 0$, to istnieje $c \in K$ takie, że $G = cF$.
- Jeśli X nie jest właściwa, to X jest podprzestrzenią afiniczną wymiaru mniejszego od $n - 1$.

Zauważmy, że twierdzenie to nie zachodzi, jeśli hiperpowierzchnia nie jest właściwa. Oto przykład. Mamy:

$$\{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1^2 + x_2^2 = 0\} = \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1^2 + 2x_2^2 = 0\},$$

ale dla wielomianów $F = x_1^2 + x_2^2$ oraz $G = x_1^2 + 2x_2^2$ nie istnieje $c \in K$, że $G = cF$.

Do odpowiedzi na pytanie o możliwość opisu hiperpowierzchni w afinicznej przestrzeni rzeczywistej różnymi typami równań (r1), (r2), (r3), w zależności od wyboru układu bazowego (teoretycznie jest to możliwe), wykorzystamy pojęcie środka symetrii. Wcześniej jednak sformułujemy twierdzenia, do których dążymy. Dotyczą one krzywych i hiperpowierzchni właściwych w \mathbb{R}^2 i \mathbb{R}^3 .

Twierdzenie 25.3: Klasyfikacja właściwych hiperpowierzchni (krzywych) stopnia 2 w \mathbb{R}^2

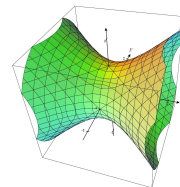
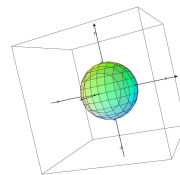
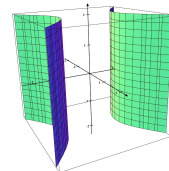
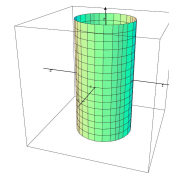
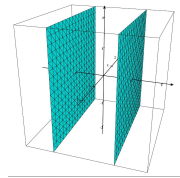
Każda właściwa hiperpowierzchnia stopnia 2 w \mathbb{R}^2 jest afinicznie izomorficzna z jedną z następujących krzywych opisanych (w standardowym układzie bazowym $(0, 0)$; $(1, 0)$, $(0, 1)$) równaniami:

- $-x_1^2 + 1 = 0$.
Jest to para prostych równoległych.
- $-x_1^2 - x_2^2 + 1 = 0$.
Krzywą tego typu afinicznego nazywamy ELIPSA.
- $x_1^2 - x_2^2 + 1 = 0$.
Krzywą tę nazywamy HIPERBOLA.
- $x_1^2 - x_2^2 = 0$.
Jest to para prostych przecinających się.
- $x_1^2 + x_2 = 0$.
Krzywą tę nazywamy PARABOLA.

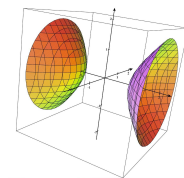
Twierdzenie 25.4: Klasyfikacja właściwych hiperpowierzchni stopnia 2 w \mathbb{R}^3

Każda właściwa hiperpowierzchnia stopnia 2 w \mathbb{R}^3 jest afinicznie izomorficzna z jedną z następujących krzywych opisanych w układzie bazowym $(0, 0, 0)$; $(1, 0, 0)$, $(0, 0, 1)$ równaniami:

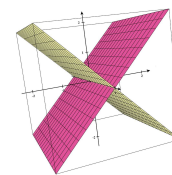
- $-x_1^2 + 1 = 0$
Jest to para płaszczyzn równoległych.
- $-x_1^2 - x_2^2 + 1 = 0$.
Jest to WALEC ELIPTYCZNY.
- $x_1^2 - x_2^2 + 1 = 0$.
Jest to WALCEC HIPERBOLICZNY.
- $-x_1^2 - x_2^2 - x_3^2 + 1 = 0$.
Jest to ELIPSOIDA.
- $x_1^2 - x_2^2 - x_3^2 + 1 = 0$.
Jest to HIPERBOLOIDA JEDNOPOWŁOKOWA.



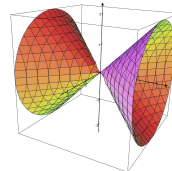
- $x_1^2 + x_2^2 - x_3^2 + 1 = 0$.
Jest to HIPERBOLOIDA DWUPOWŁOKOWA.



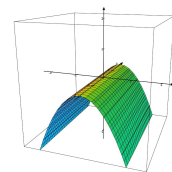
- $x_1^2 - x_2^2 = 0$.
Jest to para płaszczyzn przecinających się.



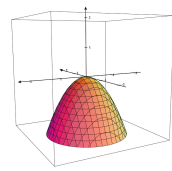
- $x_1^2 + x_2^2 - x_3^2 = 0$.
Jest to STOŻEK ELIPTYCZNY.



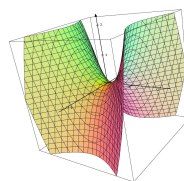
- $x_1^2 + x_3 = 0$.
Jest to WALEC PARABOLICZNY.



- $x_1^2 + x_2^2 + x_3 = 0$.
Jest to PARABOLOIDA ELIPTYCZNA.



- $x_1^2 - x_2^2 + x_3 = 0$.
Jest to PARABOLOIDA HIPERBOLICZNA.



Fakty te są wnioskami z zasadniczego rezultatu dotyczącego ogólnych hiperpowierzchni właściwych w \mathbb{R}^n .

Twierdzenie 25.5

Niech X będzie właściwą hiperpowierzchnią stopnia 2 w przestrzeni afinicznej H nad \mathbb{R} .

- (1) Jeśli X jest w układzie bazowym p_0 ; \mathcal{A} opisana równaniem postaci (r1), zaś w układzie bazowym q_0 ; \mathcal{B} – równaniem (rj), to $i = j$. Liczba r występująca w tych równaniach jest niezależna od wyboru układu bazowego.
- (2) Jeśli X jest opisywana równaniami typu (r1), to występująca w nich liczba s jest we wszystkich równaniach taka sama. Jeśli X jest opisywana równaniem (r2) lub (r3), tzn.

$$(r2) \quad x_1^2 + \dots + x_s^2 - x_{s+1}^2 - \dots - x_r^2 = 0 \quad \text{gdzie} \quad 1 \leq s < r \leq n$$

$$(r3) \quad x_1^2 + \dots + x_s^2 - x_{s+1}^2 - \dots - x_r^2 + x_n = 0 \quad \text{gdzie} \quad 0 \leq s < r \leq n - 1$$

to dla każdego dwóch różnych takich równań występujących w nich liczby s są albo jednakowe, albo ich suma wynosi r .

Zatem aby sprawdzić, czy hiperpowierzchnie X, Y są afinicznie izomorficzne wystarczy dla każdej z nich znaleźć opisujące ją równanie postaci (r1), (r2) lub (r3). Hiperpowierzchnie X, Y są afinicznie izomorficzne wtedy i tylko wtedy, gdy opisujące je równania postaci (r1) są identyczne, z dokładnością do rzędu i do znaku sygnatury, np. „utożsamiamy” równania $x_1^2 + x_2^2 - x_3^2 = 0$ oraz $-x_1^2 - x_2^2 + x_3^2 = 0$.

Definicja 25.3: Środek symetrii hiperpowierzchni

Mówimy, że punkt $p \in H$ jest ŚRODKIEM SYMETRII HIPERPOWIERZCHNI $X \subset H$, jeśli dla każdego punktu q należącego do X punkt $p - \vec{pq}$ też należy do X . Inaczej mówiąc: $p \in H$ jest środkiem symetrii hiperpowierzchni X , jeśli dla każdego wektora $\alpha \in T(H)$ zachodzi równoważność

$$p + \alpha \in X \Leftrightarrow p - \alpha \in X.$$

Zatem punkt p jest środkiem symetrii hiperpowierzchni X wtedy i tylko wtedy, gdy symetria względem punktu p (czyli jednokładność o środku p i skali -1) przeprowadza X na X .

Następujące twierdzenia określają jednoznacznie możliwość posiadania środka symetrii przez hiperpowierzchnię i jego (ewentualną) przynależność do niej. Dadzą one też (później) dowód Twierdzenia 25.5.

Twierdzenie 25.6

Niech X będzie właściwą hiperpowierzchnią stopnia 2 w przestrzeni afinicznej H opisaną w układzie bazowym $p_0; \alpha_1, \dots, \alpha_n$ równaniem

$$a_1x_1^2 + \dots + a_nx_r^2 + d = 0,$$

przy czym $a_1 \neq 0, \dots, a_r \neq 0$. Wówczas punkt p jest środkiem symetrii zbioru X wtedy i tylko wtedy, gdy p ma w tym układzie bazowym współrzędne $\underbrace{0, \dots, 0}_r, s_{r+1}, \dots, s_n$.

Zauważmy, że w przypadku hiperpowierzchni w rzeczywistych przestrzeniach afinicznych powyższe twierdzenie dotyczy hiperpowierzchni, które w pewnym układzie bazowym opisują się równaniem (r1) lub (r2). Zwróćmy jednak uwagę, że z twierdzenia tego wynika natychmiast, że środek symetrii hiperpowierzchni opisaną równaniem (r1) nie należy do tej hiperpowierzchni. W przypadku zaś hiperpowierzchni opisaną równaniem (r2) – środek symetrii należy do hiperpowierzchni.

Twierdzenie 25.7

Niech X będzie hiperpowierzchnią stopnia 2 w H opisaną w układzie bazowym $p_0; \mathcal{A}$ równaniem

$$a_1x_1^2 + \dots + a_rx_r^2 + x_n = 0,$$

przy czym $a_1 \neq 0, \dots, a_r \neq 0, r < n$. Wówczas X nie ma środka symetrii.

Widzimy ponownie, że w przypadku rzeczywistym sytuacja opisana przez powyższe twierdzenie dotyczy wyłącznie hiperpowierzchni opisywalnych w pewnym układzie bazowym równaniem (r3). Widzimy więc, że hiperpowierzchnia opisana jest równaniem tego samego typu, spośród typów (r1), (r2), (r3), niezależnie od układu bazowego. To daje pierwszą tezę z Twierdzenia 25.5. Liczby r oraz s występujące w równaniach typów (r1), (r2), (r3) opisane są, jak się okazuje, zależnościami (które wykażemy później...):

- Liczba r występująca w opisujących hiperpowierzchnię X równaniach (r1), (r2), (r3) jest we wszystkich tych równaniach (muszą być tego samego typu) taka sama.
- Jeśli X jest opisywana równaniami typu (r1), to występująca w nich liczba s jest we wszystkich równaniach taka sama. Jeśli X jest opisywana równaniem (r2) lub (r3), to dla każdych dwóch różnych takich równań występujące w nich liczby s są albo jednakowe, albo ich suma wynosi r .

W skrypcie dr. Strojnowskiego (<https://www.mimuw.edu.pl/~stroa/GAL2wyk14.pdf>, tw. 24.10) występuje ciekawe twierdzenie, bardzo użyteczne w kontekście praktycznym. Poprzedźmy je definicją.

Definicja 25.4: Pochodna cząstkowa wielomianu

Niech $A = x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ będzie jednomianem w $K[x_1, \dots, x_n]$. Przez pochodną cząstkową jednomianu względem zmiennej x_t oznaczać będziemy jednomian

$$\frac{\partial}{\partial x_t}(A) = i_t \cdot x_1^{i_1} \cdot x_{t-1}^{i_{t-1}} x_t^{i_t-1} x_{t+1}^{i_{t+1}} \dots x_n^{i_n}.$$

Wielomian ten nazywać będziemy POCHODNĄ CZĄSTKOWĄ JEDNOMIANU A WZGLĘDEM x_t , dla $t = 1, \dots, n$. Dla pary jednomianów $A, B \in K[x_1, \dots, x_n]$ oraz $a, b \in K$ definiujemy

$$\frac{\partial}{\partial x_t}(aA + bB) = a \frac{\partial}{\partial x_t}(A) + b \frac{\partial}{\partial x_t}(B).$$

W ten sposób definiujemy pochodną cząstkową $\frac{\partial}{\partial x_t}$ na całym $K[x_1, \dots, x_n]$.

Dla przykładu:

$$\begin{aligned}\frac{\partial}{\partial x_2}(x_1^2 x_2^5) &= 5x_1^2 x_2^4 \\ \frac{\partial}{\partial x_3}(x_1 x_2^2 x_3 x_4) &= x_1 x_2^2 x_4 \\ \frac{\partial}{\partial x_1}(x_1 x_3 + 2x_1 + x_2) &= x_3 + 2.\end{aligned}$$

Twierdzenie 25.8

Niech $H = \{p \in K^n \mid w(p) = 0\}$ będzie właściwą hiperpowierzchnią stopnia 2 opisaną w pewnym układzie bazowym wielomianem $W \in K[x_1, \dots, x_n]$. Wówczas punkt $q \in K^n$ jest środkiem symetrii H wtedy i tylko wtedy, gdy (formalnie – szukamy wartości pewnych funkcji wielomianowych):

$$\frac{\partial}{\partial x_1}(W)(q) = \frac{\partial}{\partial x_2}(W)(q) = \dots = \frac{\partial}{\partial x_n}(W)(q) = 0.$$

Dla przykładu: weźmy powierzchnię opisaną równaniem $x_1^2 + x_2^2 - x_3^2 = 0$ w \mathbb{R}^3 . Pochodne cząstkowe wielomianu $x_1^2 + x_2^2 - x_3^2$ to:

$$\begin{aligned}\frac{\partial}{\partial x_1}(x_1^2 + x_2^2 - x_3^2) &= 2x_1, \\ \frac{\partial}{\partial x_2}(x_1^2 + x_2^2 - x_3^2) &= 2x_2, \\ \frac{\partial}{\partial x_3}(x_1^2 + x_2^2 - x_3^2) &= -2x_3.\end{aligned}$$

zaś układ równań $2x_1 = 0, 2x_2 = 0$ oraz $-2x_3 = 0$ ma jedyne rozwiązanie $(0, 0, 0)$, które jest w istocie środkiem symetrii rozważanej hiperpowierzchni (przynależnym do niej).

Otrzymaliście Państwo zatem szereg narzędzi do badania hiperpowierzchni stopnia 2. W kolejnej części, obok dowodów wybranych twierdzeń przedstawione zostaną wnioski dotyczące klasyfikacji typów aficznych hiperpowierzchni właściwych stopnia 2 w \mathbb{R}^2 oraz \mathbb{R}^3 .

* * *

Zakończyliśmy część wykładu prezentującego twierdzenia klasyfikujące krzywe w \mathbb{R}^2 hiperpowierzchnie właściwe w \mathbb{R}^3 . Przejdziemy teraz do dowodu wybranych rezultatów. Dowody te nie są obowiązkowe, a w szczególności trudny rezultat jakim jest Twierdzenie 25.2.

Przypominam pierwsze twierdzenie, którego dowód teraz przedstawię.

Twierdzenie 25.9

Niech $f : H \rightarrow K$ będzie funkcją wielomianową stopnia 2 określoną na n -wymiarowej przestrzeni afinicznej H . Wówczas istnieje taki układ bazowy w H , w którym funkcji f odpowiada wielomian postaci:

$$\begin{aligned} & (i) \quad a_1x_1^2 + \dots + a_rx_r^2 + c \quad \text{gdzie } r = r(f) \quad \text{oraz } a_1, \dots, a_r \neq 0 \\ \text{lub} & \\ & (ii) \quad a_1x_1^2 + \dots + a_rx_r^2 + x_n \quad \text{gdzie } r = r(f) < n \quad \text{oraz } a_1, \dots, a_r \neq 0. \end{aligned}$$

Dowód. Niech $p_0; \mathcal{A}$ będzie dowolnym układem bazowym przestrzeni H . W układzie tym funkcji f odpowiada wielomian $F = x^T Ax + Bx + c$, gdzie $A \in M_{n \times n}(K)$ jest macierzą symetryczną, $B \in M_{1 \times n}(K)$ oraz $c \in K$. Niech $C \in M_{n \times n}(K)$ będzie taką macierzą odwracalną, że $C^T AC$ jest macierzą diagonalną, w której na przekątnej stoją kolejno: niezerowe wyrazy a_1, \dots, a_r , gdzie $r = r(f)$, a następnie zera. Rozpatrzmy układ bazowy $p_0; \mathcal{B}$, w którym baza \mathcal{B} zadana jest warunkiem $M(\text{id})_{\mathcal{B}}^{\mathcal{A}} = C$. W układzie tym funkcji f odpowiada wielomian

$$G = y^T C^T ACy + B'y + c' = a_1y_1^2 + \dots + a_ry_r^2 + b'_1y_1 + \dots + b'_ny_n + c'.$$

Inaczej mówiąc G jest otrzymany z F przez podstawienie $x = Cy$, gdzie $x = [x_1 \ \dots \ x_n]^T$ oraz $y = [y_1 \ \dots \ y_n]^T$. Otrzymany wielomian G możemy przedstawić w następujący sposób:

$$G = a_1 \left(y_1 + \frac{b'_1}{2a_1} \right)^2 + \dots + a_r \left(y_r + \frac{b'_r}{2a_r} \right)^2 + b'_{r+1}y_{r+1} + \dots + b'_ny_n - \frac{(b'_1)^2}{4a_1} - \dots - \frac{(b'_r)^2}{4a_r} + c'.$$

Interesuje nas pokazanie, że można zawsze tak dobrać układ bazowy $q_0; \mathcal{C}$, aby z powyższego wielomianu otrzymać przez pewną afiniczną zamianę zmiennych jeden z wielomianów występujących po prawych stronach równań (i) i (ii). Rozważmy dwa przypadki.

- Przypadek 1. $b'_{r+1} = \dots = b'_n = 0$. Wówczas wielomian $a_1z_1^2 + \dots + a_rz_r^2 + c$ typu (i) otrzymujemy z G przez podstawienie postaci:

$$z_i = \begin{cases} y_i + \frac{b'_i}{2a_i}, & \text{dla } i = 1, 2, \dots, r, \\ y_i, & \text{dla } i = r + 1, \dots, n. \end{cases}$$

- Przypadek 2. Pewna z liczb b'_{r+1}, \dots, b'_n jest niezerowa. Po ewentualnym przenumеровaniu zmiennych możemy przyjąć, że $b'_n \neq 0$. Wówczas wielomian $a_1z_1^2 + \dots + a_rz_r^2 + x_n$ typu (ii) otrzymujemy z G przez podstawienie postaci:

$$z_i = \begin{cases} y_i + \frac{b'_i}{2a_i}, & \text{dla } i = 1, 2, \dots, r, \\ y_i, & \text{dla } i = r + 1, \dots, n - 1, \\ b'_{r+1}y_{r+1} + \dots + b'_ny_n - \frac{(b'_1)^2}{4a_1} - \dots - \frac{(b'_r)^2}{4a_r} + c', & \text{dla } i = n. \end{cases}$$

□

Udowodnimy teraz twierdzenia dotyczące istnienia środka symetrii i jego ewentualnej przynależności do hiperpowierzchni stopnia 2. Przypominam definicję.

Definicja 25.5

Mówimy, że punkt $p \in H$ jest **ŚRODKIEM SYMETRII HIPERPOWIERZCHNI** $X \subset H$, jeśli dla każdego punktu q należącego do X punkt $p - \vec{pq}$ też należy do X . Inaczej mówiąc: $p \in H$ jest środkiem symetrii hiperpowierzchni X , jeśli dla każdego wektora $\alpha \in T(H)$ zachodzi równoważność $p + \alpha \in X \Leftrightarrow p - \alpha \in X$. Zatem punkt p jest środkiem symetrii hiperpowierzchni X wtedy i tylko wtedy, gdy symetria względem punktu p (tzn. jednokładność o środku p i skali -1) przeprowadza X na X .

Pierwsze z twierdzeń dotyczy sytuacji, gdy hiperpowierzchnię właściwą stopnia 2 można w pewnym układzie bazowym opisać równaniem typu (i). Mówi ono, że w przestrzeni afinicznej zawierającej taką hiperpowierzchnię właściwą X musi istnieć środek symetrii X . Podaje ono też położenie tego punktu.

Twierdzenie 25.10

Niech X będzie właściwą hiperpowierzchnią stopnia 2 w H opisaną w układzie bazowym $p_0; \alpha_1, \dots, \alpha_n$ równaniem

$$a_1x_1^2 + \dots + a_rx_r^2 + d = 0,$$

przy czym $a_1 \neq 0, \dots, a_r \neq 0$. Wówczas punkt p jest środkiem symetrii zbioru X wtedy i tylko wtedy, gdy p ma w tym układzie bazowym współrzędne $\underbrace{0, \dots, 0}_r, s_{r+1}, \dots, s_n$.

Dowód. Jeśli p ma w układzie bazowym $p_0; \alpha_1, \dots, \alpha_n$ współrzędne $\underbrace{0, \dots, 0}_r, s_{r+1}, \dots, s_n$, to dla każdego wektora $\alpha = y_1\alpha_1 + \dots + y_n\alpha_n$ mamy:

$$\begin{aligned} p + \alpha &= p_0 + s_{r+1}\alpha_1 + \dots + s_n\alpha_n + y_1\alpha_1 + \dots + y_n\alpha_n = \\ &= p_0 + y_1\alpha_1 + \dots + y_r\alpha_r + (s_{r+1} + y_{r+1})\alpha_{r+1} + \dots + (s_n + y_n)\alpha_n. \end{aligned}$$

Jest zatem jasne, że punkt $p - \alpha$ ma w rozważanym układzie bazowym współrzędne

$$-y_1, \dots, -y_r, s_{r+1} - y_{r+1}, \dots, s_n - y_n.$$

Mamy więc:

$$p + \alpha \in X \Leftrightarrow a_1y_1^2 + \dots + a_ry_r^2 + d = 0, \quad p - \alpha \in X \Leftrightarrow a_1^2(-y_1)^2 + \dots + a_r(-y_r)^2 + d = 0.$$

Jasne jest więc, że jeśli p ma w układzie bazowym $p_0; \alpha_1, \dots, \alpha_n$ współrzędne $\underbrace{0, \dots, 0}_r, s_{r+1}, \dots, s_n$, to jest środkiem symetrii hiperpowierzchni X .

Na odwrót: przypuśćmy, że punkt p o współrzędnych s_1, \dots, s_n jest środkiem symetrii hiperpowierzchni X . Wykażemy, że $s_1 = s_2 = \dots = s_r = 0$. Niech $z \in X$ ma współrzędne z_1, \dots, z_n . Zatem

$$a_1z_1^2 + \dots + a_ry_r^2 + d = 0 \tag{25.1}$$

Niech $\alpha = \vec{p}\vec{z}$, czyli $p + \alpha = z$. Skoro $z = p + \alpha \in X$, to z faktu, że p jest środkiem symetrii wynika, że $p - \alpha \in X$. Punkt $p - \alpha$ ma współrzędne $2s_1 - z_1, \dots, 2s_n - z_n$, więc:

$$a_1(2s_1 - z_1)^2 + \dots + a_r(2s_r - z_r)^2 + d = 0.$$

czyli

$$a_1(4s_1^2 - 4s_1z_1 + z_1^2) + \dots + a_r(4s_r^2 - 4s_ry_r + z_r^2) + d = 0. \tag{25.2}$$

Odejmując (25.1) od (25.2) i dzieląc przez 4 mamy: $a_1(s_1^2 - s_1z_1) + \dots + a_r(s_r^2 - s_ry_r) = 0$, czyli:

$$a_1s_1z_1 + \dots + a_ry_ry_r - a_1s_1^2 - \dots - a_ry_r^2 = 0. \tag{25.3}$$

Otrzymaliśmy: współrzędne z_1, \dots, z_n każdego punktu $z \in X$ spełniają (25.3). Więc X zawarty jest w zbiorze spełniającym (25.3). Gdyby $s_i \neq 0$, dla pewnego $i = 1, \dots, r$, to (25.3) opisywałoby $n - 1$ wymiarową podprzestrzeń afiniczną $M \subseteq H$ i mielibyśmy $X \subseteq M$, co przeczyłoby założeniu, że X jest właściwa. \square

Kolejne twierdzenie mówi o tym, że hiperpowierzchnia, którą w pewnym układzie bazowym można opisać równaniem typu (ii) nie może mieć środka symetrii.

Twierdzenie 25.11

Niech X będzie hiperpowierzchnią stopnia 2 w H opisaną w układzie bazowym $p_0; \mathcal{A}$ równaniem

$$a_1x_1^2 + \dots + a_ry_r^2 + x_n = 0,$$

przy czym $a_1 \neq 0, \dots, a_r \neq 0, r < n$. Wówczas X nie ma środka symetrii.

Dowód. Przypuśćmy, że punkt p o współrzędnych s_1, \dots, s_n jest środkiem symetrii X . Rozważamy dwa przypadki.

- Przypadek 1. Punkt p należy do X . Wówczas mamy

$$a_1 s_1^2 + \dots + a_r s_r^2 + s_n = 0. \quad (25.4)$$

Niech α będzie wektorem mającym w bazie \mathcal{A} przestrzeni $T(H)$ współrzędne $-2s_1, 0, 0, \dots, 0$. Wówczas punkt $p + \alpha$ ma współrzędne $-s_1, s_2, \dots, s_n$ więc $p + \alpha \in X$. Stąd $p - \alpha \in X$, bo p to środek symetrii. Punkt $p - \alpha$ ma jednak współrzędne $3s_1, s_2, \dots, s_n$, więc dostajemy

$$9a_1 s_1^2 + a_2 s_2^2 + \dots + a_r s_r^2 + s_n = 0. \quad (25.5)$$

Odejmując (25.4) od (25.5) dostajemy $8a_1 s_1^2 = 0$, a stąd $s_1 = 0$. Analogicznie dowodzimy jednak, że $s_2 = s_3 = \dots = s_r = 0$, a stąd z (25.4) $s_n = 0$. Zatem p ma współrzędne $0, 0, \dots, 0, s_{r+1}, \dots, s_{n-1}, 0$. Wówczas dla każdego wektora o współrzędnych z_1, \dots, z_n spełniających $a_1 z_1^2 + \dots + a_r z_r^2 + z_n = 0$ i $z_n \neq 0$ mamy $p + \beta \in X$ oraz $p - \beta \notin X$. A zatem otrzymujemy sprzeczność z założeniem, że p jest środkiem symetrii X .

- Przypadek 2. Punkt p nie należy do X . Wówczas mamy $a_1 s_1^2 + \dots + a_r s_r^2 + s_n \neq 0$. Niech α będzie wektorem o współrzędnych $0, 0, \dots, 0, a$, gdzie $a = -(a_1 s_1^2 + \dots + a_r s_r^2 + s_n)$. Wówczas $p + \alpha \in X$ zaś $p - \alpha \notin X$. Znowu sprzeczność z założeniem, że p jest środkiem symetrii X . □

Przypomnijmy wreszcie twierdzenie, którego dowód zajmie resztę wykładu.

Twierdzenie 25.12

Niech X będzie właściwą hiperpowierzchnią stopnia 2 w przestrzeni afinicznej H nad \mathbb{R} .

- (1) Jeżeli X jest w układzie bazowym p_0 ; \mathcal{A} opisana równaniem postaci (ri), zaś w układzie bazowym q_0 ; \mathcal{B} – równaniem (rj), to $i = j$.
- (2) Jeśli X jest pewnych układach bazowych opisywana równaniami postaci (ri), dla $i = 1, 2, 3$, to liczba r występująca w tych równaniach jest niezależna od wyboru układu bazowego.
- (3) Jeśli X jest opisywana równaniami typu (r1), to występująca w nich liczba s jest we wszystkich równaniach taka sama. Jeśli X jest opisywana równaniem (r2) lub (r3), to dla każdych dwóch różnych takich równań występujące w nich liczby s są albo jednakowe, albo ich suma wynosi r .

Przypomnijmy przy tym twierdzenie opisujące formy kanoniczne (r1), (r2), (r3), do których się odnosimy.

Twierdzenie 25.13

Dla każdej hiperpowierzchni X stopnia 2 w n wymiarowej przestrzeni afinicznej nad ciałem liczb rzeczywistych \mathbb{R} istnieje układ bazowy, w którym X jest opisana równaniem postaci:

$$\begin{aligned} (r1) \quad & x_1^2 + \dots + x_s^2 - x_{s+1}^2 - \dots - x_r^2 + 1 = 0 \quad \text{gdzie} \quad 0 \leq s < r \leq n, \\ \text{lub} \quad & \\ (r2) \quad & x_1^2 + \dots + x_s^2 - x_{s+1}^2 - \dots - x_r^2 = 0 \quad \text{gdzie} \quad 1 \leq s < r \leq n, \\ \text{lub} \quad & \\ (r3) \quad & x_1^2 + \dots + x_s^2 - x_{s+1}^2 - \dots - x_r^2 + x_n = 0 \quad \text{gdzie} \quad 0 \leq s < r \leq n - 1. \end{aligned}$$

Wniosek ten prowadzi, łącznie z innymi pokazanymi już rezultatami, do klasyfikacji hiperpowierzchni właściwych stopnia dwa w \mathbb{R}^2 oraz \mathbb{R}^3 . Klasyfikacja ta mówi między innymi o tym kiedy istnieje afiniczny izomorfizm, który przeprowadza jedną hiperpowierzchnię stopnia 2 w drugą. Prowadzi ona do wielu ciekawych obserwacji geometrycznych. Nie jest to zresztą jedyna klasyfikacja, o której warto wspomnieć. O tym wszystkim powiem nieco dalej. Wpierw jednak udowodnimy wreszcie powyższe twierdzenie.

Dowód. Jeśli X opisana jest równaniem postaci (r1), to X posiada środek symetrii, ale żaden jej środek symetrii nie należy do X . Istotnie, jeśli $p \in H$ jest środkiem symetrii powierzchni X opisanej w pewnym układzie bazowym równaniem $a_1x_1^2 + \dots + a_rx_r^2 + d = 0$, przy czym $a_1 \neq 0, \dots, a_r \neq 0$, wówczas punkt p jest środkiem symetrii zbioru X wtedy i tylko wtedy, gdy p ma w tym układzie bazowym współrzędne $\underbrace{0, \dots, 0}_{r}, s_{r+1}, \dots, s_n$. Nietrudno jednak widzieć, że jeśli X jest opisana równaniem

$$x_1^2 + \dots + x_s^2 - x_{s+1}^2 - \dots - x_r^2 + 1 = 0, \text{ wówczas punkt o współrzędnych } \underbrace{0, \dots, 0}_{r}, s_{r+1}, \dots, s_n \text{ nie spełnia}$$

tego równania. Z tych samych powodów powierzchnia X opisana równaniem (r2) zawiera wszystkie swoje środki symetrii. Jeśli X spełnia równanie (r3), to jak wiemy nie ma środka symetrii. Omówione przypadki wzajemnie się wykluczają, skąd wynika część (1) Wniosku.

Aby udowodnić pozostałą część Wniosku założmy, że hiperpowierzchnia X jest opisana:

- w układzie bazowym $p_0; \mathcal{A}$ równaniem postaci $F = 0$, gdzie $F \in \mathbb{R}[x_1, \dots, x_n]$,
- w układzie bazowym $q_0; \mathcal{B}$ równaniem $G = 0$, gdzie $G \in \mathbb{R}[y_1, \dots, y_n]$,

przy czym F, G są wielomianami stopnia 2.

Niech $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$, $\mathcal{B} = (\beta_1, \dots, \beta_n)$, $C = M(\text{id})_{\mathcal{B}}^{\mathcal{A}} \in M_n(\mathbb{R})$ oraz $q_0 = p_0 + w_1\alpha_1 + \dots + w_n\alpha_n$. Wówczas hiperpowierzchnia X jest opisana w układzie bazowym $q_0; \mathcal{B}$ równaniem $H = 0$, gdzie $H \in \mathbb{R}[y_1, \dots, y_n]$ powstaje z F przez podstawienie:

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = C \cdot \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} + \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix}. \quad (25.6)$$

Stąd macierze części kwadratowych wielomianów F, H są kongruentne nad \mathbb{R} , mają więc równe rzędy i sygnatury. Zauważmy też, że zarówno G , jak i H są wielomianami opisującymi hiperpowierzchnię właściwą X w tym samym układzie bazowym, a więc zgodnie z Twierdzeniem 25.2 istnieje $c \in \mathbb{R}$, że $H = cG$ (dowód tego twierdzenia będzie podany pod koniec wykładu).

To jest kluczowy moment. Można bowiem pytać — po co Twierdzenie 25.2, skoro zgodnie z Obserwacją 25.3 wiemy, że jeśli wielomian jest w jednym układzie bazowym opisany jednym równaniem kwadratowym, to w innym układzie bazowym jest opisany równaniem kwadratowym, którego część kwadratowa jest kongruentna do poprzedniej. Czy nie wiemy stąd, że H musi być opisana takim samym równaniem, jak G , z dokładnością do skali? Nie wiemy, bowiem istnienie jednego wielomianu odpowiadającego funkcji w danym układzie bazowym nie wyklucza istnienia zupełnie innego wielomianu, również odpowiadającego tej funkcji w tym układzie bazowym. Części kwadratowe mogą być zresztą kongruentne, podczas gdy żądany skalar nie istnieje, np. $x_1^2 + x_2^2$ oraz $x_1^2 + 2x_2^2$.

Macierze części kwadratowych wielomianów H oraz G (a zatem też wielomianów F i G) mają ten sam rząd, a ich sygnatury są równe z dokładnością do znaku (są równe gdy $c > 0$, są przeciwne, gdy $c < 0$). Jeśli równania $F = 0$ oraz $G = 0$ są w postaci (ri), to występująca w nich liczba r jest rzędem macierzy części kwadratowej. Zatem musi być ona taka sama w obydwu równaniach. To dowodzi (2). Ponadto różnica $s - (r - s) = 2s = r$ jest sygnaturą macierzy części kwadratowej równania postaci (ri), dla $i = 1, 2, 3$. Stąd jeśli rząd i sygnatura dla F wynoszą r, s , dla G wynoszą r', s' , to $2s - r = \pm(2s' - r')$, co uwzględniając $r = r'$ daje albo $2s - r = 2s' - r$, czyli $s = s'$, albo $2s - r = -(2s' - r)$, czyli $s' = r - s$, co dowodzi (3) odnośnie hiperpowierzchni typu afinicznego (r2) lub (r3).

Na koniec rozpatrzmy przypadek, gdy równania $F = 0, G = 0$ opisujące X są postaci (r1), to znaczy

$$F = x_1^2 + \dots + x_s^2 - x_{s+1}^2 - \dots - x_r^2 + 1 = 0, \quad G = y_1^2 + \dots + y_t^2 - x_{t+1}^2 - \dots - x_r^2 + 1 = 0.$$

Skoro H powstaje z F przez podstawienie (25.6) i równocześnie

$$H = cG = cy_1^2 + \dots + cy_t^2 - xy_{t+1}^2 - \dots - cy_t^2 + c,$$

to musi być $w_1 = w_2 = \dots = w_r = 0$ oraz $c = 1$. Stąd w przypadku (r1) dostajemy $s = t$, koniec. \square

Pozostał nam dowód Twierdzenia 25.2. Przypomnijmy treść.

Twierdzenie 25.14

Niech X będzie hiperpowierzchnią stopnia 2 w przestrzeni afinicznej H nad ciałem K i niech $p_0; \alpha_1, \dots, \alpha_n$ będzie układem bazowym przestrzeni H .

- (a) Jeśli X jest właściwa oraz $F, G \in K[x_1, \dots, x_n]$ są takimi wielomianami stopnia 2, że X jest opisana w układzie bazowym $p_0; \alpha_1, \dots, \alpha_n$ zarówno równaniem $F = 0$, jak i $G = 0$, to istnieje $c \in K$ takie, że $G = cF$.
- (b) Jeśli X nie jest właściwa, to X jest podprzestrzenią afiniczną wymiaru mniejszego od $n - 1$.

Plan dowodu tego twierdzenia jest następujący (za skryptem Profesorów Chabera i Pola).

- pokażemy, że dla każdej hiperpowierzchni właściwej stopnia 2 w \mathbb{R}^n istnieje w tejże \mathbb{R}^n prosta, która przecina się z nią w dokładnie dwóch punktach,
- pokażemy, że funkcja wielomianowa stopnia 2 (opisująca hiperpowierzchnię) ograniczona do punktów leżących na prostej opisanych w postaci parametrycznej $q_0 + tw$ zachowuje się jak funkcja kwadratowa od t ,
- zdefiniujemy λ i pokażemy, że $F_1 - \lambda F_2$ jest zerowy na całym \mathbb{R}^n .

Dowód. Zakładamy, że hiperpowierzchnia $H \subset \mathbb{R}^n$ jest właściwa, czyli w pewnym układzie bazowym $p_0; \mathcal{A}$ opisana jest jednym z równań:

$$\begin{aligned} (r1) \quad & x_1^2 + \dots + x_s^2 - x_{s+1}^2 - \dots - x_r^2 + 1 = 0, & \text{gdzie } 0 \leq s < r \leq n, \\ (r2) \quad & x_1^2 + \dots + x_s^2 - x_{s+1}^2 - \dots - x_r^2 = 0, & \text{gdzie } 0 \leq s < r < n, \\ (r3) \quad & x_1^2 + \dots + x_s^2 - x_{s+1}^2 - \dots - x_r^2 + x_n = 0, & \text{gdzie } 0 \leq s < r \leq n - 1. \end{aligned}$$

wówczas następująca prosta L przecina H dokładnie w dwóch punktach:

- w przypadku (r1): opisana w $p_0; \mathcal{A}$ równaniami: $x_j = 0$, dla $j \neq r$ co daje dokładnie dwa punkty należące do H : $(\underbrace{0, \dots, \pm 1}_r, 0, \dots, 0)$,
- w przypadku (r2): opisana w $p_0; \mathcal{A}$ równaniami $x_r = 1, x_j = 0$, dla $r \neq j > 1$ co daje dokładnie dwa punkty należące do H : $(\pm 1, 0, \dots, 0, \underbrace{1}_r, 0, \dots, 0)$,
- w przypadku (r3): opisana w $p_0; \mathcal{A}$ równaniami: $x_n = -1, x_j = 0$, dla $n > j > 1$ co daje dokładnie dwa punkty należące do H : $(\pm 1, 0, \dots, 0, -1)$.

A zatem hiperpowierzchnia właściwa stopnia 2 (patrz **zwłaszcza** równanie (r2)) przecina się z pewną prostą na dokładnie dwóch punktach.

Niech $f(p) = 0$ oraz $g(p) = 0$ będą równaniami pewnej hiperpowierzchni właściwej H stopnia 2 w \mathbb{R}^n . Załóżmy, że w układzie bazowym p_0, \mathcal{A} funkcjom tym odpowiadają wielomiany $F, G \in \mathbb{R}[x_1, \dots, x_n]$.

Niech $F(x) = x^T A x + B x + c$, gdzie $A = A^T$, $B \in M_{1 \times n}(\mathbb{R})$ oraz $c \in \mathbb{R}$. Niech $F_2(x) = x^T A x$ oraz niech funkcja f_2 będzie zadana przez F_2 na $p_0; \mathcal{A}$.

Jeśli $q + \text{lin}(w)$ jest prostą w \mathbb{R}^n oraz wektory x, z zawierają współrzędne q oraz w odpowiednio w układzie bazowym p_0, \mathcal{A} oraz bazie \mathcal{A} , to mamy:

$$\begin{aligned} F(x + tz) &= (x + tz)^T A(x + tz) + (x + tz)B + c = \\ &= t^2(z^T A z) + t(2x^T A + B)z + F(x). \end{aligned}$$

Zatem możemy zapisać:

$$f(q + tw) = at^2 + bt + c, \quad \text{gdzie } a = f_2(w), c = f(q) \quad (*)$$

Istnieje prosta $L = q_0 + \text{lin}(w_0)$ przecinająca H w dokładnie dwóch punktach (dwie wartości t , że $f(q_0 + tw_0) = 0$). Z (*) wynika zatem, że $a = f_2(w_0) \neq 0$. Bez straty ogólności załóżmy, że $a > 0$ (można zastąpić f przez $-f$) oraz możemy przyjąć $f(q_0) < 0$ (przesuwając w razie potrzeby q_0 po L).

Niech $\lambda = \frac{g(q_0)}{f(q_0)}$ i niech

$$E = \{q \in \mathbb{R}^n \mid g(q) = \lambda f(q)\}.$$

Pokażemy, że $\mathbb{R}^n = E$.

Z definicji $H \cup \{q_0\} \subseteq E$ (dla $p \in H$ mamy z definicji $f(p) = g(p) = 0$). Co więcej, stosując (*) do funkcji g oraz λf widzimy, że każda prosta w \mathbb{R}^n zawierająca trzy punkty zbioru E , w istocie zawiera się w E . Krótko mówiąc: $(g - \lambda f)(x + tz)$ jest co najwyżej funkcją kwadratową od r , a zeruje się na E .

Weźmy dowolną prostą $L_w = q_0 + \text{lin}(w)$ zawieszoną w q_0 taką, że $f_2(w) > 0$. Z (*) dla f na L_w wnioskujemy, że zbiór $L_w \cap H$ jest dwupunktowy (przecież f zeruje się na $L_w \cap H$, a $f(q_0) < 0$ oraz $a = f_2(w) > 0$). Co więcej $q_0 \in E \cap L_w$. Zatem $L_w \subseteq E$. A zatem dla wszystkich w takich, że $f_2(w) > 0$ mamy $L_w \subset E$.

Weźmy teraz dowolne $q = q_0 + u \in \mathbb{R}^n$. Punkty prostej $L_q = q + \text{lin}(w_0)$ możemy przedstawić w postaci $q_0 + (u + tw_0)$. A zatem powtarzając argumentację dla wzoru (*) możemy zapisać:

$$f_2(u + tw_0) = t^2 f_2(w_0) + tb + f_2(u) > 0,$$

dla dostatecznie dużych t (bo $f_2(w_0) > 0$). Dla takich t punkty $q_0 + (u + tw_0)$ prostej L_q są w E , więc cała L_q jest w E i stąd $q \in L_q \subseteq E$. A zatem $\mathbb{R}^n = E$. □

Powyższy dowód ma istotne znaczenie w bardzo elementarnych rozważaniach algebraiczno-geometrycznych. Wynika z niej bowiem stwierdzenie, że jeśli hiperpowierzchnia stopnia 2 zawiera trzy punkty prostej, to zawiera całą tę prostą.

Intuicja powinna być znowu zupełnie jasna. Każda hiperpowierzchnia stopnia 2 opisana jest równaniem $x^T Ax + Bx + C = 0$. Jeśli punkty x_1, x_2, x_3 leżą na pewnej prostej, to są one postaci $x_0 + t\alpha$, dla pewnych trzech wartości parametru t . A zatem równanie $(x_0 + t\alpha)^T A(x_0 + t\alpha) + B(x_0 + t\alpha) + C = 0$ traktowane jako równanie kwadratowe względem zmiennej t ma trzy pierwiastki. To oznacza, że jest ono tożsamościowo równe 0. Czy widać zatem dlaczego cała prosta zawiera się w hiperpowierzchni?

Zadanie. Dla każdych trzech nieprzecinających się prostych $l_1, l_2, l_3 \subseteq \mathbb{R}^3$ istnieje dokładnie jedna hiperpowierzchnia stopnia 2, która zawiera wszystkie te proste.

To, że dla prostych l_1, l_2, l_3 istnieje odpowiednia hiperpowierzchnia jest łatwe. Z każdej prostej wybieramy po trzy punkty p_i, p'_i, p''_i , dla $i = 1, 2, 3$. Każda hiperpowierzchnia stopnia 2 w \mathbb{R}^3 dana jest równaniem:

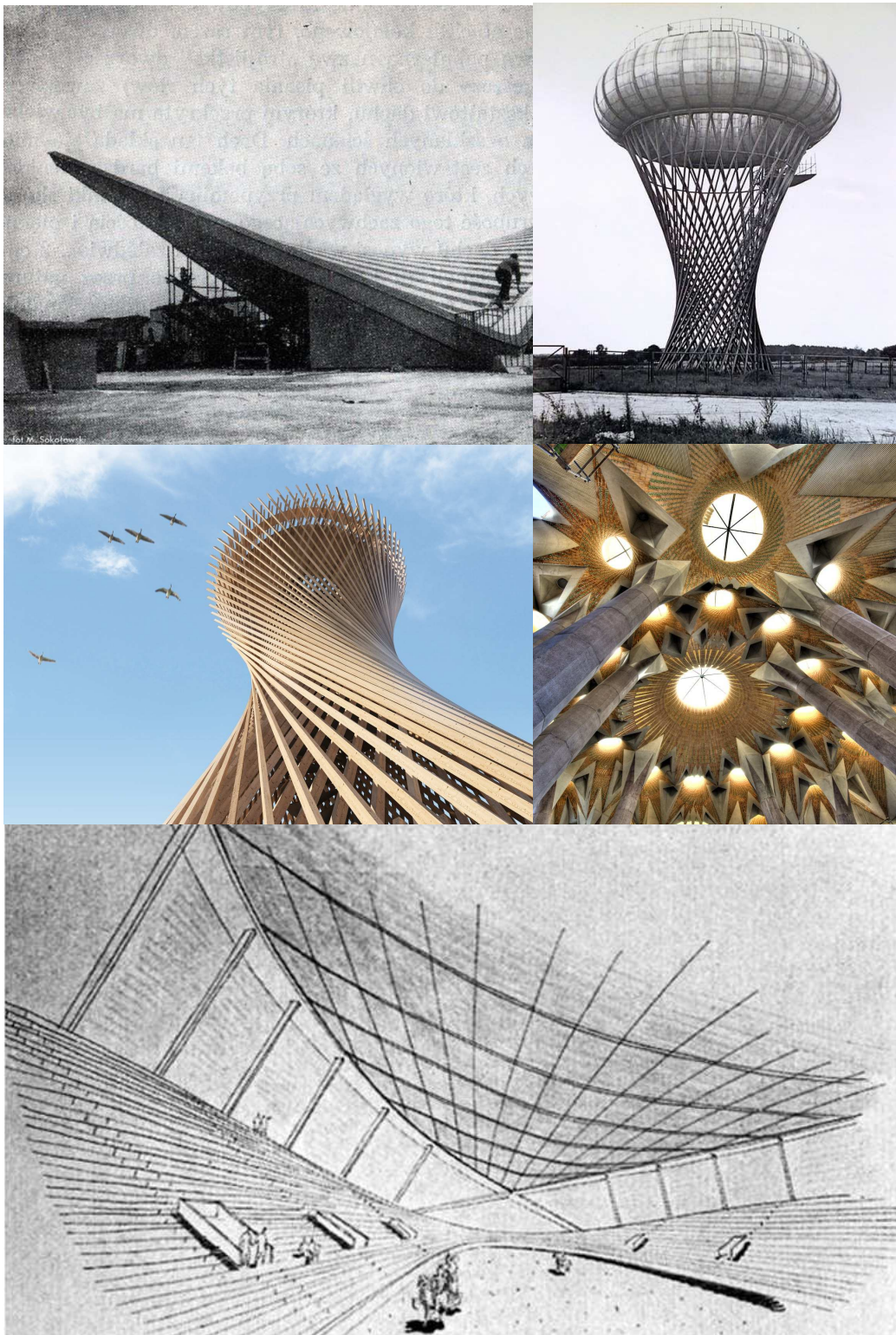
$$Ax_1^2 + Bx_2^2 + Cx_3^2 + Dx_1x_2 + Ex_1x_3 + Fx_2x_3 + Gx_1 + Hx_2 + Ix_3 + J = 0.$$

Musimy wyznaczyć A, B, C, \dots, J wstawiając do powyższej równości w miejsce x_1, x_2, x_3 współrzędne punktów p_i, p'_i, p''_i , dla $i = 1, 2, 3$. Dostajemy zatem układ 9 równań jednorodnych o 10 niewiadomych. A zatem ma on z pewnością **niezerowe rozwiązanie** dające współczynniki naszej hiperpowierzchni (może się zdarzyć oczywiście, że wyznaczona hiperpowierzchnia będzie w istocie płaszczyzną). Znaleziona hiperpowierzchnia stopnia 2 zawiera po 3 punkty każdej z prostych l_1, l_2, l_3 . Zawiera więc te proste w całości, na mocy poprzedniej uwagi. Pewnym problemem jest pokazanie jedności tej hiperpowierzchni. Tu potrzebne są (o ile mi wiadomo) argumenty z geometrii rzutowej.

Przytoczona argumentacja jest celowo napisana nieco nieporządnie. Komu wystarcza sama intuicja – niezbędne intuicje otrzymał. Kto potrzebuje dokładnego dowodu – będzie (mam nadzieję) w stanie uzupełnić szczegóły (patrz np. <http://math.uchicago.edu/~may/REU2014/REUPapers/Lazarus.pdf>). Różnych twierdzeń tego typu jest więcej. Można na przykład pokazać, że każda nierozkładalna niesingularna hiperpowierzchnia stopnia 3 zawiera 27 prostych (wyjaśnienie definicji i dowód w powyższym linku). Zagadnienia te należą do tzw. enumeratywnej geometrii algebraicznej. Przystępny tekst w tej dziedzinie to np. https://www.maa.org/sites/default/files/images/upload_library/22/Ford/Bachelor.pdf.

25.1 Uzupełnienie. Powierzchnie prostokreślne

Czy rozpoznajecie Państwo te budynki?



Dwa pierwsze budynki znajdują się w Polsce. Pierwszy od góry z lewej jest budynek dworca WKD Ochota, o parabolicznym dachu (ukończony w 1962 r.). Obok widzimy wieżę ciśnień w Ciechanowie (1972 r.) w kształcie torusa osadzonego na hiperbolicznym kominie. Poniżej z lewej podobnego kształtu budowla – wieża obserwacyjna w Varberg (Szwecja) z 2012 roku. Obok arcydzieło architektury – okna Gaudiego z Sagrada Familia (skoro światło porusza się w linii prostej, to tak je trzeba wpuszczać do pomieszczenia: przez hiperboloide). Wreszcie poniżej – szkic areny sportowej *Parableum* (Raleigh, USA) zaprojektowanej w 1949 roku przez jednego z największych polskich architektów XX wieku – Macieja Nowickiego.

Po II Wojnie Światowej, w czasie której opracowano szereg nowych materiałów budowlanych, wzrosło zainteresowanie innowacyjnymi metodami architektonicznymi. Zarówno w Stanach Zjednoczonych, jak i Związku Radzieckim czy Europie Zachodniej, modernistyczne projekty uwzględniały futurystyczne kształty – a za takie uważano właśnie wspomniane powierzchnie. Cóż wyróżnia geometrię tych obiektów?

Definicja 25.6

Zbiór X w przestrzeni afinicznej H nazwiemy **PROSTOKREŚLNYM**, jeśli każdy jego punkt leży na pewnej prostej, która jest zawarta w zbiorze X .

Przykłady.

- Zbiór rozwiązań równania $x_1^2 - x_2^2 = 0$ jest prostokreślny, ponieważ składa się on z dwóch prostych.
- Stożek oraz walec eliptyczny są prostokreślne w \mathbb{R}^3 , ale też *helikoida* i *konoida* (a cóż to takiego?).
- Przestrzeń afiniczna \mathbb{R}^n jest oczywiście zbiorem prostokreślnym.

Obserwacja 25.4

Gdy X jest paraboloidą hiperboliczną lub hiperboloidą jednopowłokową, to przez każdy punkt $p \in X$ przechodzą co najmniej dwie różne proste zawarte w X .

Dowód. (za skryptem prof. Toruńczyka). Badane tu własności zachowują się przy izomorfizmach afinicznych. Można więc założyć, że X jest podzbiorem przestrzeni \mathbb{R}^3 , zadany w standardowym układzie bazowym równaniem kanonicznym. Rozpatrzmy dwa przypadki.

- Przypadek 1. Zbiór X zadany jest równaniem $x_1^2 - x_2^2 + x_3 = 0$. Wtedy każda płaszczyzna postaci $P_c : \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1 - x_2 = c\}$ przecina paraboloidę X wzdłuż prostej K_c zadanej równaniami $c(x_1 + x_2) = -x_3, x_1 - x_2 = c$. Co więcej, każda płaszczyzna Q_c o równaniu $x_1 + x_2 = c$ przecina X wzdłuż prostej L_c , zadanej równaniami $c(x_1 - x_2) = -x_3, x_1 + x_2 = c$. Oczywiście każdy punkt przestrzeni leży na jednej z płaszczyzn P_c i na jednej z płaszczyzn Q_c , więc łatwo widzieć, że rodziny $\{K_c : c \in \mathbb{R}\}$ i $\{L_c : c \in \mathbb{R}\}$ spełniają żądane warunki.
- Przypadek 2. Zbiór X jest zadany równaniem $x_1^2 - x_2^2 - x_3^2 + 1 = 0$. Wtedy punkt $(0, 0, 1)$ leży w X i w płaszczyźnie $x_3 = -1$, a ta przecina X wzdłuż zbioru $K \cup L$, gdzie K jest prostą zadaną równaniami $x_1 = x_2, x_3 = -1$, zaś L – równaniami $x_1 = -x_2, x_3 = -1$. Oznaczmy przez \mathcal{K} (odpowiednio przez \mathcal{L}) rodzinę tych prostych w \mathbb{R}^3 , które są obrazem prostej K (odp. L) przy obrocie¹ wokół osi x_1 . Obie rodziny składają się z prostych, zawartych w X , a opisane obroty przeprowadzają X w X . Dowolny punktu $a = (a_1, a_2, a_3) \in X$ leży na pewnej prostej rodziny \mathcal{K} : przecięcie X z płaszczyzną $x_1 = a_1$ jest okręgiem, skąd pewien obrót wokół osi x_1 przeprowadza punkt a na punkt przecięcia tej płaszczyzny z prostą K . Dla rodziny \mathcal{L} rozumowanie jest analogiczne.

□

O hiperboloidzie jednopowłokowej i paraboloidzie hiperbolicznej można (łatwo) pokazać więcej niż to, że są prostokreślne. Są one w istocie **PODWÓJNIE PROSTOKREŚLNE** – to znaczy istnieją po dwie rodziny prostych zawartych w każdej z tych hiperpowierzchni takie, że każdy punkt tej hiperpowierzchni leży na dokładnie jednej prostej z każdej z rodzin, przy czym proste z danej rodziny są rozłączne i każda prosta z jednej rodziny przecina każdą prostą z drugiej rodziny. Niezwykle zaskakujący jest następujący fakt.

Twierdzenie 25.15

Każdy zbiór podwójnie prostokreślny w przestrzeni afinicznej \mathbb{R}^3 jest albo płaszczyzną, albo hiperboloidą jednopowłokową, albo paraboloidą hiperboliczną.

¹Warto pamiętać: prosta obracana w \mathbb{R}^3 wokół skośnej do niej prostej „zakreśla” (zwykle) hiperboloidę jednopowłokową.

25.2 Dodatek. Klasyfikacja izometryczna i rzutowa

Kilka słów o stożkowych

Jacek Komorowski w pięknej książce „*Od liczb zespolonych to tensorów, spinorów, algebr Liego i kwadryk*” (z której pochodzi niemała część niestandardowego materiału z tego wykładu) podsumowuje: *Można być przekonany, że dla każdego z czytelników naturalne jest odróżnienie okręgu małego od dużego, nie mówiąc już o okręgu i bardzo spłaszczonej elipsie, chociaż wszystkie te obiekty są afinicznie równoważne. Tym, co zmusza nas do takiego rozróżnienia, jest nasza „wrodzona” wrażliwość na związki metryczne, respektowane przez odwzorowania euklidesowe, a bezlitośnie gwałcone przez odwzorowania afiniczne.*

Czym by były owe rozróżnienia respektowane przez odwzorowania euklidesowe? Chodzi o sytuację, gdy rozpatrujemy hiperpowierzchnie w afinicznej przestrzeni euklidesowej i zamiast pytania o typ afiniczny pytamy o tzw. typ izometryczny. Znajdujemy się wówczas nad ciałem liczb rzeczywistych i naturalnie wydaje się pytanie: kiedy można przy pomocy izometrii przeprowadzić jedną hiperpłaszczyznę na drugą?

Definicja 25.7: Prostokątny układ współrzędnych

Niech V będzie przestrzenią liniową wymiaru n nad ciałem K .

- Dowolny izomorfizm $\phi : V \rightarrow K^n$ nazwiemy UKŁADEM WSPÓLRZĘDNYCH w V .
- Powiemy, że układ współrzędnych ϕ jest ZWIĄZANY Z BAZĄ $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$ przestrzeni V , jeśli ϕ przeprowadza α_i na i -ty wektor bazy standardowej.
- Układ współrzędnych w przestrzeni euklidesowej (V, \langle, \rangle) związany z bazą ortogonalną V , będziemy nazywać PROSTOKĄTNYM UKŁADEM WSPÓLRZĘDNYCH.
- AFINICZNYM UKŁADEM WSPÓLRZĘDNYCH w przestrzeni afinicznej E nad K (związanym z układem bazowym $p; \mathcal{A}$) nazywamy przekształcenie liniowe $\phi_p : E \rightarrow K^n$ dane wzorem:

$$\phi_p(p + v) = \phi(v),$$

gdzie $p \in E$, zaś ϕ jest układem współrzędnych w $T(E)$ związanym z bazą \mathcal{A} . Jeśli E jest przestrzenią euklidesową i \mathcal{A} jest bazą prostopadłą, to mówimy, że układ ϕ_p jest prostokątny.

Możemy teraz sformułować kluczową definicję.

Definicja 25.8: Izometryczna równoważność hiperpowierzchni

Niech $(H_1, \langle, \rangle_1)$, $(H_2, \langle, \rangle_2)$ – euklidesowe afiniczne oraz niech X_1, X_2 to hiperpowierzchnie odpowiednio w H_1 oraz H_2 . Powiemy, że X_1 ma ten sam **typ izometryczny** co X_2 , jeśli istnieje izometria $\phi : H_1 \rightarrow H_2$ taka, że $\phi(X_1) = X_2$.

Podstawowy rezultat jest następujący.

Definicja 25.9: Typ izometryczny hiperpowierzchni

Niech $(H_1, \langle, \rangle_1)$, $(H_2, \langle, \rangle_2)$ będą przestrzeniami euklidesowymi afinicznymi oraz niech X_1, X_2 będą hiperpowierzchniami odpowiednio w H_1 oraz H_2 . Powiemy, że X_1 ma ten sam **TYP IZOMETRYCZNY**, co X_2 , jeśli istnieje izometria $\phi : H_1 \rightarrow H_2$ taka, że $\phi(X_1) = X_2$.

Analogicznie do uwagi dotyczącej typu afinicznego można pokazać, że hiperpowierzchnie X_1, X_2 zawarte w tej samej przestrzeni euklidesowej afinicznej (H, \langle, \rangle) mają ten sam typ izometryczny wtedy i tylko wtedy, gdy istnieją ORTONORMALNE UKŁADY BAZOWE $p_0; \mathcal{A}, q_0; \mathcal{B}$, w których hiperpowierzchnie te są opisane tym samym równaniem. W wielu źródłach, między innymi w książkach Kostrikina, Komorowskiego lub skrypcie dr. Strojnowskiego (<https://www.mimuw.edu.pl/~stroa/GAL2wyk14.pdf>) znaleźć można następujące ważne twierdzenie, które podajemy wraz ze szkicem dowodu.

Twierdzenie 25.16: Klasyfikacja izometryczna hiperpowierzchni stopnia 2

Niech X będzie właściwą hiperpowierzchnią stopnia 2 w przestrzeni euklidesowej afinicznej H wymiaru n . Wówczas X ma w odpowiednim ortonormalnym układzie współrzędnych dokładnie jedno z poniższych równań:

$$\begin{aligned}
 & (i1) \quad \frac{x_1^2}{a_1^2} + \dots + \frac{x_s^2}{a_s^2} - \frac{x_{s+1}^2}{a_{s+1}^2} - \dots - \frac{x_r^2}{a_r^2} + 1 = 0 \quad \text{gdzie } a_1, \dots, a_r > 0, \text{ oraz } 0 \leq s < r \leq n, \\
 & \text{lub} \\
 & (i2) \quad \frac{x_1^2}{a_1^2} + \dots + \frac{x_s^2}{a_s^2} - \frac{x_{s+1}^2}{a_{s+1}^2} - \dots - \frac{x_r^2}{a_r^2} = 0 \quad \text{gdzie } a_1, \dots, a_r > 0, \text{ oraz } 1 \leq s < r \leq n, \\
 & \text{lub} \\
 & (i3) \quad \frac{x_1^2}{a_1^2} + \dots + \frac{x_s^2}{a_s^2} - \frac{x_{s+1}^2}{a_{s+1}^2} - \dots - \frac{x_r^2}{a_r^2} + x_n = 0 \quad \text{gdzie } a_1, \dots, a_r > 0, \text{ oraz } 0 \leq s < r \leq n-1.
 \end{aligned}$$

Umieszczenie wielkości a_i w mianownikach ma znaczenie symboliczne. Wielkości te nazywamy PÓŁOSIAMI HIPERPOWIERZCHNI. Nazwa ta może się Państwu kojarzyć geometrycznie zwłaszcza z pojęciem elipsy.

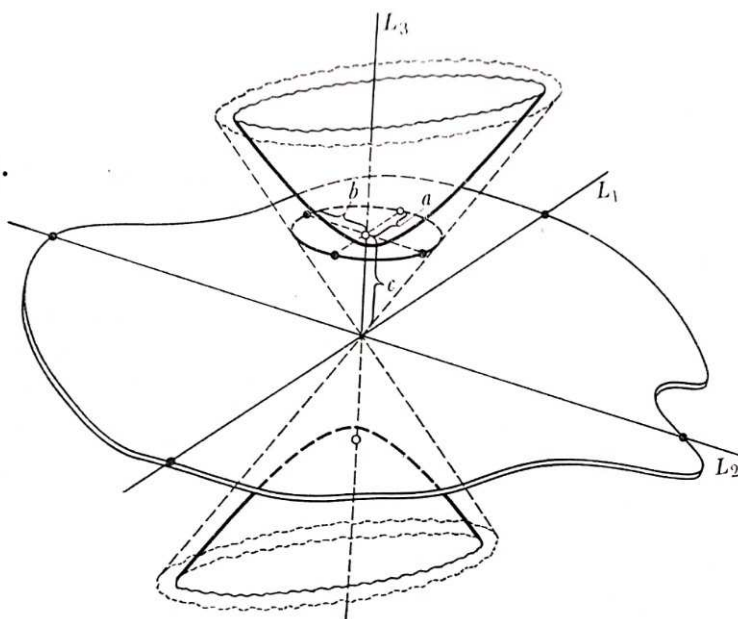
Trzy wyróżnione typy izometryczne (i1), (i2), (i3) korespondują bezpośrednio z typami (r1), (r2), (r3), występującymi w klasyfikacji afinicznej, i nikogo nie powinno to dziwić. Wszystkie powierzchnie typu (ij) mają typ afiniczny (rj), dla $j = 1, 2, 3$. Jeśli mógłbym podać Państwu jakąkolwiek intuicję, która rzuci tu nieco światła – proszę wrócić do dowodów z poprzednich wykładów i wypowiedzieć się – jaka była geometryczna natura dokonywanych przez nas zamian zmiennych. Czy niektóre nie były aby izometriami?

(d) *Hiperboloidea dwupowłokowa:*

$$f = \frac{x_1^2}{a^2} + \frac{x_2^2}{b^2} - \frac{x_3^2}{c^2} + 1,$$

$$f^{-1}(0) \in EH_{2,1},$$

$$N(f) = \left(\left\langle \frac{1}{a^2}, \frac{1}{b^2}, -\frac{1}{c^2} \right\rangle, 0, 1 \right).$$



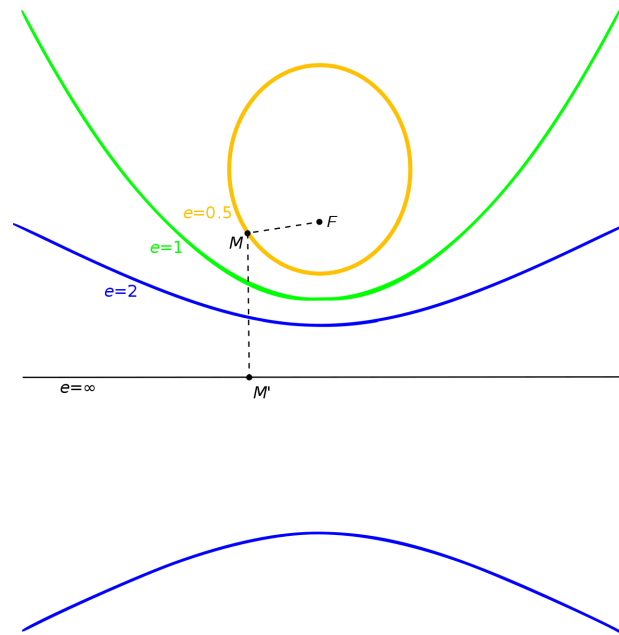
Rys. Jedna z wielu pięknych ilustracji z książki J. Komorowskiego „Od liczb zespolonych do tensorów, spinorów algebr Liego i kwadryk”, PWN 1978. (Każdemu gorąco polecam czytanie tej książki, a nawet jej zakup, jeśli to możliwe!)

Aby uprzedzić dowód ilustracją powyższego twierdzenia przy pomocy znanych obiektów, powiemy nieco o stożkowych, by na koniec wspomnieć też o rzutowej klasyfikacji powierzchni.

Definicja 25.10: Stożkowa na płaszczyźnie

Niech $F \in \mathbb{R}^2$, niech $K \subseteq \mathbb{R}^2$ będzie prostą i niech $e > 0$. Stożkową o **ognisku** F , **kierownicy** K i mimośrodku e w przestrzeni euklidesowej afinicznej \mathbb{R}^2 nazywamy zbiór:

$$S(F, K, e) = \{p \in \mathbb{R}^2 \mid \rho(p, F) = e \cdot \rho(p, K)\}.$$



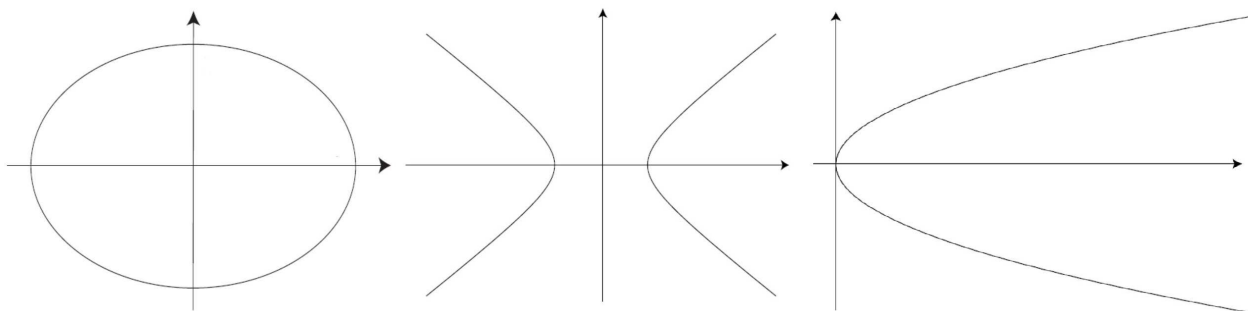
Nie wspominam w tym miejscu więcej o geometrycznych definicjach stożkowych, ale można je bez trudu znaleźć choćby w tekście Agaty Laskowskiej: <https://minut.polsl.pl/articles/A-21-001.pdf>. Twierdzenie, które nas interesuje wyraża się w teorii stożkowych w następujących sposób.

Twierdzenie 25.17: Fakt (<https://www.mimuw.edu.pl/~ziemians/gax2015w/galx15.pdf>)

Dla $F \not\subseteq K$ stożkowa jest zbiorem opisanym w pewnym prostopadłym układzie współrzędnych jednym z trzech równań:

- **elipsy**, dla $e < 1$, czyli $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$,
- **paraboli**, dla $e = 1$, czyli $x^2 = 2dy$,
- **hiperbolą**, dla $e > 1$, czyli: $\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$.

Istotne jest przede wszystkim widzenie prostopadłego układu bazowego w kategoriach geometrycznych. Oto odpowiednie ilustracje.



Dowód Twierdzenia 25.18. Zaczniemy od dowolnego prostokątnego układu współrzędnych p_0, \mathcal{A} w \mathbb{R}^n i niech X będzie w nim opisana równaniem: $0 = \sum_{i,j=1}^n a_{ij}x_i x_j + \sum_{i=1}^n b_i x_i + c = 0 = x^T A x + b^T x + c$, gdzie $A = A^T$. Istnieje baza ortonormalna \mathcal{B} , w której forma kwadratowa opisana w bazie \mathcal{A} macierzą A ma postać diagonalną. W prostokątnym układzie współrzędnych p_0, \mathcal{B} powierzchnia X ma równanie:

$$\sum_{i=1}^n \lambda_i y_i^2 + \sum_{i=1}^n b_i y_i + c = 0.$$

Założmy, że $\lambda_i \neq 0$, dla $i \leq r$ oraz $\lambda_i = 0$, dla $i > r$. Przepisujemy równanie wyżej:

$$\sum_{i=1}^r \lambda_i \left(y_i + \frac{b_i}{2\lambda_i} \right)^2 + \sum_{i=r+1}^n b_i y_i + c - \sum_{i=1}^n \frac{b_i^2}{4\lambda_i^2} = 0.$$

W prostokątnym układzie p_0, \mathcal{A} hiperpowierzchnia X jest opisana równaniem:

$$\sum_{i=1}^r \lambda_i \left(y_i + \frac{b_i}{2\lambda_i} \right)^2 + \sum_{i=r+1}^n b_i y_i + c - \sum_{i=1}^n \frac{b_i^2}{4\lambda_i^2} = 0.$$

Weźmy przesunięcie: $p_0 + (y_1, \dots, y_r, y_{r+1}, \dots, y_n) \xrightarrow{\text{izometria}} p_0 + (y_1 + \frac{b_1}{2\lambda_1}, \dots, y_r + \frac{b_r}{2\lambda_r}, y_{r+1}, \dots, y_n)$. Przeprowadza ona dotychczasowy układ na taki, w którym X opisana jest równaniem:

$$\sum_{i=1}^r \lambda_i z_i^2 + \sum_{i=r+1}^n b_i z_i + c' = 0, \quad \text{dla} \quad c' = c - \sum_{i=1}^n \frac{b_i^2}{4\lambda_i^2}.$$

Teraz rozważamy trzy przypadki (i) $b_i = 0, c' = 0$, (ii) $b_i \neq 0, c' = 0$, (iii) $b_i \neq 0$, dla pewnego i .

- **Przypadek 1.** $b_i = 0, c' = 0$. Założmy (ewentualnie zamieniając za pomocą izometrii kolejność zmiennych), że $\lambda_1 > 0, \dots, \lambda_s > 0, \lambda_{s+1} < 0, \dots, \lambda_r < 0$ (wszystkie λ_i nie mogą być jednego znaku). Wówczas biorąc $a_i = \frac{1}{\sqrt{|\lambda_i|}}$ dostajemy postać (i2), czyli

$$\frac{x_1^2}{a_1^2} + \dots + \frac{x_s^2}{a_s^2} - \frac{x_{s+1}^2}{a_{s+1}^2} - \dots - \frac{x_r^2}{a_r^2} = 0.$$

- **Przypadek 2.** $b_i = 0, c' \neq 0$. Możemy założyć (ewentualnie zamieniając za pomocą izometrii kolejność zmiennych), że $\lambda_1 > 0, \dots, \lambda_s > 0, \lambda_{s+1} < 0, \dots, \lambda_r < 0$. Wówczas mnożymy równanie przez $\frac{1}{c'}$ i przyjmujemy $a_i = \frac{\sqrt{|c_i|}}{\sqrt{|\lambda_i|}}$ uzyskując postać (i1), czyli:

$$\frac{x_1^2}{a_1^2} + \dots + \frac{x_s^2}{a_s^2} - \frac{x_{s+1}^2}{a_{s+1}^2} - \dots - \frac{x_r^2}{a_r^2} + 1 = 0.$$

- **Przypadek 3.** $b_i \neq 0$, dla pewnego i . Możemy założyć, że $\lambda_1 > 0, \dots, \lambda_s > 0, \lambda_{s+1} < 0, \dots, \lambda_r < 0$. Biorąc izometrię, która przeprowadza $p_0 + z_i \alpha_i \mapsto p_0 + z_i \alpha_i$, dla $i < n$ oraz

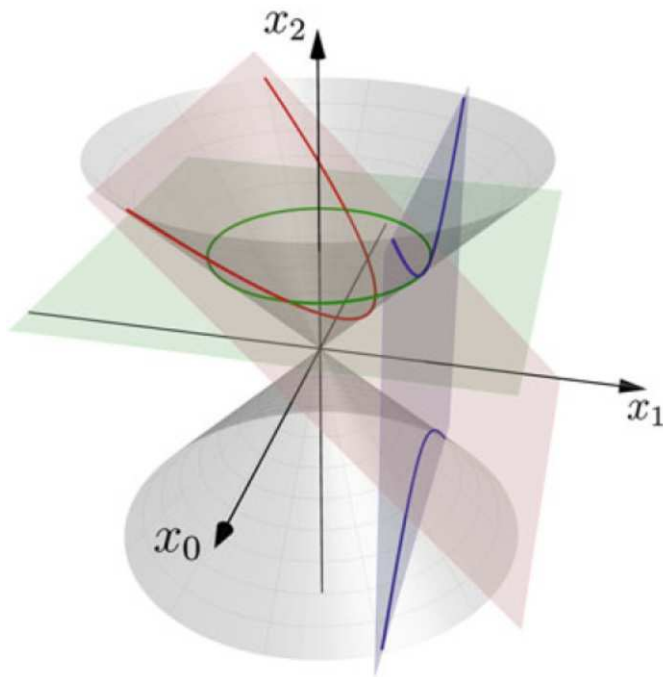
$$p_0 + \frac{\sum_{i=r+1}^n b_i z_i + c'}{\left\| \sum_{i=r+1}^n b_i z_i + c' \right\|} \alpha_n \mapsto p_0 + \frac{z_n}{\|z_n\|} \alpha_n,$$

dzieląc przez $d = \left\| \sum_{i=r+1}^n b_i z_i + c' \right\| / \|z_n\|$ i biorąc $a_i = \frac{\sqrt{|d|}}{\sqrt{|\lambda_i|}}$ dostajemy postać (i3):

$$\frac{x_1^2}{a_1^2} + \dots + \frac{x_s^2}{a_s^2} - \frac{x_{s+1}^2}{a_{s+1}^2} - \dots - \frac{x_r^2}{a_r^2} + x_n = 0.$$

A zatem pokazaliśmy, że każda hiperpowierzchnia właściwa stopnia 2 w przestrzeni euklidesowej afinicznej E wymiaru n jest opisana, w pewnym prostokątnym układzie współrzędnych, jednym z równań (i1)-(i3).

Na koniec powiedzmy nieco o przekształceniach rzutowych, powołując się na dodatek o przestrzeniach i przekształceniach rzutowych. Rozważmy podzbiór \mathbb{RP}^2 złożony z punktów o współrzędnych jednorodnych $(x_0 : x_1 : x_2)$ spełniających równanie: $x_0^2 + x_1^2 = x_2^2$.



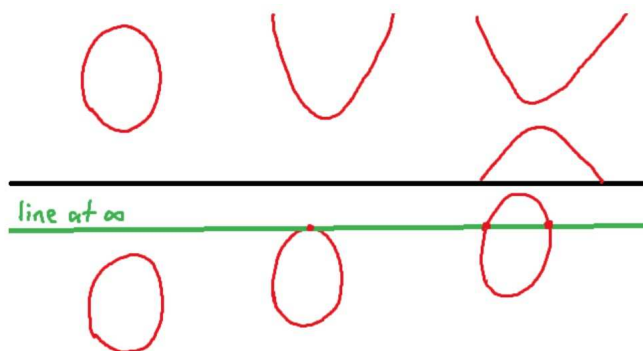
Źródło: *Algebra I, Textbook for Students of Mathematics.*

Wspominaliśmy, że w zależności od wyboru mapy standardowej stożkowa ta jest w istocie hiperbolą, okręgiem lub parabolą. Przejścia między tymi mapami są izomorfizmami rzutowymi, co jest świadectwem równoważności rzutowej tych krzywych.

Widzimy zatem, że mamy trzy rodzaje klasyfikacji: izometryczne, afiniczne i rzutowe. W tych klasyfikacjach szczególnie wyraźne jest rozróżnienie stożkowych:

- dwie elipsy mogą być izometrycznie nierównoważne, ale są zawsze afinicznie równoważne,
- żadna elipsa i parabola nie są afinicznie równoważne, mimo że są one zawsze rzutowo równoważne.

Gdyby Czytelnik był zaciekawiony znaczeniem geometrycznym tych faktów, zwłaszcza klasyfikacji rzutowej, warto pomyśleć o tym w następujący sposób: hiperbole i parabole są z rzutowego punktu widzenia elipsami, tylko przecinającymi w inny sposób prostą niewłaściwą. Hiperbola jest elipsą, która przecina prostą w nieskończoności w dwóch punktach. Parabola – w jednym, a elipsa — w żadnym.



Źródło: <https://blogs.adelaide.edu.au/maths-learning/2016/07/14/the-line-at-infinity-conics/>.

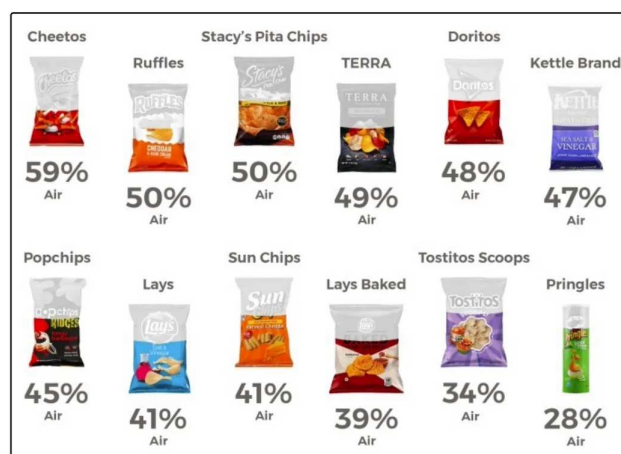
Tematyka ta rozważana była niegdyś jako element obowiązkowych kursu akademickiego geometrii analitycznej w n -wymiarach, choćby w podręczniku M. Starka: <http://matwbn.icm.edu.pl/ksiazki/mon/mon26/mon2622.pdf>. Czytelnik bez trudu znajdzie w Sieci pełny tekst tej książki. Biorąc pod uwagę, że współczesna algebra liniowa i geometria odeszły od badania obiektów algebraicznych „na współrzędnych”, dziś zaawansowane kursy geometrii dotyczą raczej związków z algebrą abstrakcyjną i topologią.

25.3 Trivia. Pringles

Na koniec naszych rozważań czas przyjrzeć się z pewnym przybliżeniem oka, pięknemu zastosowaniu teorii hiperpowierzchni w postaci popularnego produktu spożywczego — Pringles. Materiał przedstawiam na podstawie (przykładowe źródło): ZME Science <https://www.zmescience.com/feature-post/natural-sciences/mathematics/food-science-pringle/>. Oto nasi bohaterowie.

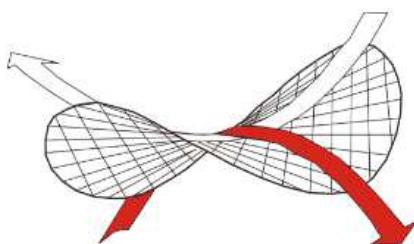


Powierzchnia tego produktu jest oczywiście modelowana na paraboloidzie hiperbolicznej. Dlaczego? Kluczowy powód to oczywiście kwestia układania tych produktów jeden na drugim tak, że łamliwość jest znacznie zredukowana, a procent powietrza w opakowaniu jest znacznie zmniejszony.



via Bakery and Snacks

Dzięki temu, że punkt przecięcia kierunków prostopadłych (osi głównych) na tej powierzchni jest tzw. punktem siodłowym, kształt Pringles zapewnia delikatną równowagę pomiędzy siłami działającymi na powierzchnię, pozwalając jej na zachowanie niewielkiej grubości (przy sporej powierzchni) i sporej wytrzymałości. Nie jest to tylko opinia, ale produkt pracy superkomputerów w latach 60-tych, zaprzęgniętych do rozwiązania problemu połamanych chipsów zgłaszanych przez konsumentów. Zainteresowanych odsyłam do krótkiego filmu: https://www.youtube.com/watch?v=9Z_Hb1RzgHQ&ab_channel=BingeDaily.



A jak ukształtowane są inne chipsy, na przykład Lays? Odsyłam do źródeł :)