1-INF-156/22 Algebra 2

Martin Sleziak, úpravy v 4.3 Jaroslav Guričan

29. mája 2023

Obsah

Úvod

Verzia: 29. mája 2023

Predhovor

V rámci tohoto textu sa budeme občas odkazovať aj na veci z predchádzajúceho semestra. Takéto odkazy budú označené napríklad ako veta I-3.2.6. (Keďže ste absolvovali predmet Algebra 1 dá sa predpokladať, že budete vedieť o akú vetu ide. Toto je viac-menej pomôcka - ak si nebudete istí, môžete si tam znenie príslušenej vety, lemy, či definície skontrolovať.) Verzia poznámok z predchádzajúceho semestra, na ktorú sa toto číslovanie vzťahuje, bude tiež na stránke predmetu.

Časti označené hviezdičkou sú nepovinné – doplnil som ich preto, že by Vás niektoré z nich mohli zaujímať. V cvičeniach hviezdička označuje náročnejšie cvičenia a + označuje nepovinné cvičenia (napríklad tie, ktoré sa týkajú nepovinných častí).

Sylaby a literatúra

Sylaby predmetu: Skalárny súčin, ortonormálna báza a ortogonálna projekcia na podpriestor. Kvadratické formy a ich kanonické tvary. Pozitívna (semi)definitnosť matice a kvadratickej formy a kritériá na overenie pozitívnej definitnosti.

Zmena bázy, podobné matice. Podobnosť matice s diagonálnou maticou. Vlastné čísla a vlastné vektory, charakteristický polynóm. Ortogonálne matice, ortogonálna podobnosť, Schurova veta a veta o hlavných osiach.

Okruhy a polynómy.

Literatúra: Základnou literatúrou pre tento kurz je [KGGS]; objavia sa však aj témy, ktoré v tejto knihe spracované nie sú, k nim sem časom doplním vhodnú literatúru.

Cvičenia v texte som vyberal z kníh [KGGS, BM, FS1, FS2, Kos, Pro1].

Označenia

Ako obvykle, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ označuje množinu celých, racionálnych, reálnych a komplexných čísel, $\mathbb{N} = \{1, 2, 3, \dots\}$ je množina prirodzených čísel a $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

Označenie A^B používame pre množinu zobrazení z B do A. Špeciálne v niektorých príkladoch sa vyskytuje množina $\mathbb{R}^{\mathbb{R}}$ a $\mathbb{R}^{\mathbb{N}}$, na oboch týchto množinách sa dajú prirodzeným spôsobom zaviesť sčitovanie a násobenie tak, že tieto množiny tvoria vektorové priestory.

Kapitola 1

Euklidovské vektorové priestory

Táto kapitola je spracovaná prevažne na základe [KGGS, 1.16,1.17].

1.1 Skalárny súčin

Skalárny súčin vektorov patriacich do $\mathbb{R}^2$ alebo $\mathbb{R}^3$ poznáte zo strednej školy. Tam ste skalárny súčin vektorov $\vec{\alpha} = (a_1, a_2)$ a $\vec{\beta} = (b_1, b_2)$ definovali ako

$$\langle \vec{\alpha}, \vec{\beta} \rangle = a_1 b_1 + a_2 b_2.$$

(Používali ste iné označenie pre skalárny súčin, ako budeme používať my.) Takisto ste sa na strednej škole naučili, ako súvisí skalárny súčin s veľkosťou vektora a uhlom, ktorý zvierajú 2 vektory:

$$\langle \vec{\alpha}, \vec{\beta} \rangle = |\vec{\alpha}||\vec{\beta}| \cos \varphi,$$
$$|\vec{\alpha}| = \sqrt{a_1^2 + a_2^2} = \sqrt{\langle \vec{\alpha}, \vec{\alpha} \rangle}.$$

My by sme teraz chceli zaviesť definíciu skalárneho súčinu o niečo všeobecnejšie – chceli by sme popísať, aké vlastnosti by mal mať skalárny súčin, aby sme pomocou neho mohli zmysluplne hovoriť o veľkosti alebo uhle vektorov z daného vektorového priestoru. Budeme opäť postupovať axiomaticky – zavedieme si niekoľko základných vlastností skalárneho súčinu, z ktorých sa budú dať odvodiť ostatné.

Definícia 1.1.1. Nech $(V, +, \cdot)$ je vektorový priestor nad poľom $\mathbb{R}$. Potom zobrazenie $g\colon V \times V \to \mathbb{R}$ sa nazýva *skalárny súčin* na V, ak pre ľubovoľné $\vec{\alpha}, \vec{\beta} \in V$ a $c \in \mathbb{R}$ platí

(i) $g(\vec{\alpha}, \vec{\beta}) = g(\vec{\beta}, \vec{\alpha})$,

(ii) $g(\vec{\alpha} + \vec{\beta}, \vec{\gamma}) = g(\vec{\alpha}, \vec{\gamma}) + g(\vec{\beta}, \vec{\gamma})$,

(iii) $g(c\vec{\alpha}, \vec{\beta}) = cg(\vec{\alpha}, \vec{\beta})$,

(iv) ak $\vec{\alpha} \neq \vec{0}$, tak $g(\vec{\alpha}, \vec{\alpha}) > 0$.

Vektorový priestor V spolu so skalárnym súčinom g nazývame *euklidovským vektorovým priestorom.*

Predchádzajúcu definíciu môžeme stručne preformulovať tak, že zobrazenie g je symetrické (i), kladne definitné (iv), a bilineárne (ii) a (iii). S pojmom kladnej definitnosti sa ešte stretneme, budeme sa ním zaoberať podrobnejšie v časti 2.3. Tento pojem by ste mohli poznať aj z matematickej analýzy, kde ste sa s ním mohli stretnúť v súvislosti s hľadaním extrémov viac premenných. Pod bilinearitou rozumieme to, že zobrazenie je lineárne v oboch premenných – ak zvolím pevne vektor $\vec{\alpha}$ a mením $\vec{\beta}$, môžeme ho chápať ako zobrazenie, ktoré vektoru $\vec{\beta}$ priradí reálne číslo. Z (ii) a (iii) vidíme, že toto zobrazenie je lineárne. Rovnako je to aj v prípade, že fixujeme $\vec{\beta}$.

Všimnite si, že skalárny súčin sme definovali iba pre vektorové priestory nad poľom $\mathbb{R}$.

Namiesto $g(\vec{\alpha}, \vec{\beta})$ budeme používať označenie $\langle \vec{\alpha}, \vec{\beta} \rangle$. Pri tomto označení uvedené vlastnosti môžeme prepísať nasledovne:

(i) $\langle \vec{\alpha}, \vec{\beta} \rangle = \langle \vec{\beta}, \vec{\alpha} \rangle$,

(ii) $\langle \vec{\alpha} + \vec{\beta}, \vec{\gamma} \rangle = \langle \vec{\alpha}, \vec{\gamma} \rangle + \langle \vec{\beta}, \vec{\gamma} \rangle$,

(iii) $\langle c\vec{\alpha}, \vec{\beta} \rangle = c\langle \vec{\alpha}, \vec{\beta} \rangle$,

(iv) ak $\vec{\alpha} \neq \vec{0}$, tak $\langle \vec{\alpha}, \vec{\alpha} \rangle > 0$.

Podmienku (iv) možno ekvivalentne vyjadriť aj tak, že pre každý vektor $\vec{\alpha}$ platí $\langle \vec{\alpha}, \vec{\alpha} \rangle) \geq 0$ a rovnosť nastáva jedine pre $\vec{\alpha} = \vec{0}$. (Skúste si rozmyslieť, ako z prvých troch podmienok v definícii vyplýva, že $\langle \vec{0}, \vec{\alpha} \rangle = 0$ pre ľubovoľné $\vec{\alpha}$.)

Ak V je euklidovský vektorový priestor, tak aj každý jeho podpriestor je euklidovský priestor (s rovnako definovaným skalárnym súčinom).

Poznámka 1.1.2. Niekedy sa skalárny súčin definuje aj pre vektorové priestory nad poľom $\mathbb{C}$. V tomto prípade sa podmienka (i) zmení na

$$\langle \vec{\alpha}, \vec{\beta} \rangle = \overline{\langle \vec{\beta}, \vec{\alpha} \rangle}.$$

Všimnime si, že táto podmienka implikuje, že $\langle \vec{\alpha}, \vec{\alpha} \rangle = \overline{\langle \vec{\alpha}, \vec{\alpha} \rangle}$, a teda $\langle \vec{\alpha}, \vec{\alpha} \rangle \in \mathbb{R}$. Vďaka tomu má zmysel aj podmienka (iv).

My sa však budeme zaoberať iba reálnymi euklidovskými priestormi.

Príklad 1.1.3. Zoberme si vektorový priestor $\mathbb{R}^n$ s obvyklým sčitovaním a skalárnym násobkom (po zložkách). Potom pre vektory $\vec{\alpha} = (a_1, \ldots, a_n)$ a $\vec{\beta} = (b_1, \ldots, b_n)$ definujeme

$$\langle \vec{\alpha}, \vec{\beta} \rangle = \sum_{k=1}^{n} a_k b_k.$$

V prípade $\mathbb{R}^2$ alebo $\mathbb{R}^3$ dostávame skalárny súčin ako ho poznáte zo strednej školy.

Vlastnosti z definície skalárneho súčinu sa overia pomerne jednoducho. Vlastnosť (i) je zrejmá. Vlastnosti (ii) a (iii) sa overia jednoduchou úpravou:

$$\sum_{k=1}^{n} (a_k + b_k)c_k = \sum_{k=1}^{n} (a_k c_k + b_k c_k) = \sum_{k=1}^{n} a_k c_k + \sum_{k=1}^{n} b_k c_k,$$

$$\sum_{k=1}^{n} c a_k = c \sum_{k=1}^{n} a_k.$$

Aby sme overili vlastnosť (iii), stačí si všimnúť, že

$$\langle \vec{\alpha}, \vec{\alpha} \rangle = \sum_{k=1}^{n} a_k^2.$$

Pretože $a_k^2 \geq 0$, aj skalárny súčin $\langle \vec{\alpha}, \vec{\alpha} \rangle \geq 0$ a rovný 0 bude iba v prípade, že všetky sčítance sú nulové, t.j. $a_k = 0$ pre každé k a $\vec{\alpha} = 0$.

Príklad 1.1.4. Definujme na $\mathbb{R}^2$ skalárny súčin nasledovne:

$$\langle \vec{\alpha}, \vec{\beta} \rangle = a_1 b_1 + a_1 b_2 + a_2 b_1 + 2 a_2 b_2,$$

pre $\vec{\alpha} = (a_1, a_2)$ a $\vec{\beta} = (b_1, b_2)$. Vlastnosti (i)–(iii) sa overia ľahko. Vlastnosť (iv) vyplýva z toho, že

$$\langle \vec{\alpha}, \vec{\alpha} \rangle = a_1^2 + 2 a_1 a_2 + 2 a_2^2 = (a_1 + a_2)^2 + a_2^2,$$

čiže $\langle \vec{\alpha}, \vec{\alpha} \rangle = 0$ platí práve vtedy, keď $a_1 = 0$ a súčasne $a_1 + a_2 = 0$, teda $a_1 = a_2 = 0$, čiže $\vec{\alpha} = \vec{0}$.

Príklad 1.1.5. Postup z predchádzajúceho príkladu sa dá zovšeobecniť. Všimnime si, že je to špeciálny prípad nasledujúceho zápisu:

$$g(\vec{\alpha}, \vec{\beta}) = (a_1 \dots a_n) C \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \vec{\alpha} C \vec{\beta}^T,$$

kde C je reálna matica typu $n \times n$. Takýto predpis priradí dvom vektorom $\vec{\alpha} = (a_1, \dots, a_n), \vec{\beta} = (b_1, \dots, b_n) \in \mathbb{R}^n$ nejaké reálne číslo. Nie vždy to však bude skalárny súčin.

Všimnime si, že tento predpis môžeme zapísať aj takto:

$$g(\vec{\alpha}, \vec{\beta}) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_i c_{ij} b_j.$$

V prípade, že ide o symetrickú maticu, čiže $c_{ij} = c_{ji}$, ľahko zistíme, že je splnená podmienka (i). Podmienky (ii) a (iii) sú splnené pre ľubovoľnú maticu.

S podmienkou (iv) je to o niečo komplikovanejšie. Budeme sa ňou zaoberať neskôr.

Príklad 1.1.6. Ako $C(a, b)$ označíme množinu všetkých spojitých funkcií $f \colon \langle a, b \rangle \to \mathbb{R}$. Tieto funkcie tvoria vektorový podpriestor priestoru všetkých funkcií z $\langle a, b \rangle$ do $\mathbb{R}$ a predpis

$$\langle f, g \rangle = \int_a^b f(x) g(x) dx$$

definuje skalárny súčin na tomto priestore. (Takto by sme vedeli definovať skalárny súčin aj na podstatne väčšom priestore funkcií – stačilo by zvoliť nejaké podmienky, ktoré zaručia, že súčin $f(x)g(x)$ bude mať konečný integrál. Keď však použijeme aj nespojité funkcie, budeme mať problémy pri overovaní podmienky (iv). Pravdepodobne v niektorom z vyšších ročníkov sa na analýze stretnete s Fourierovými radmi, kde sa objaví tento istý skalárny súčin a dozviete sa tam aj ako sa to dá definovať tak, aby to fungovalo aj pre iné funkcie, nielen spojité.)

Ak máme euklidovský vektorový priestor, tak môžeme prirodzeným spôsobom zadefinovať veľkosť vektora a uhol dvoch vektorov. Uvidíme, že takto zavedená veľkosť vektora spĺňa viaceré vlastnosti, ktoré platia pre veľkosť vektora v $\mathbb{R}^2$ a $\mathbb{R}^3$.

Definícia 1.1.7. Nech V je euklidovský vektorový priestor. Potom pre $\vec{\alpha} \in V$ definujeme veľkosť vektora $\vec{\alpha}$ ako

$$|\vec{\alpha}| = \sqrt{\langle \vec{\alpha}, \vec{\alpha} \rangle}.$$

Všimnite si, že podmienka (iv) z definície skalárneho súčinu zaručí, že veľkosť je definovaná pre ľubovoľný vektor (nikdy v predpise pre $|\vec{\alpha}|$ nedostaneme odmocninu zo záporného čísla.)

Niekedy sa používa aj označenie $\|\vec{\alpha}\|$ (napríklad v [KGGS]).

Tvrdenie 1.1.8. *Nech V je euklidovský vektorový priestor. Pre ľubovoľné $\vec{\alpha}, \vec{\beta} \in V$ a $c \in \mathbb{R}$ platí:*

(i) $|\vec{\alpha}| \geq 0$

(ii) $|\vec{\alpha}| = 0 \Leftrightarrow \vec{\alpha} = \vec{0}$

(iii) $|c\vec{\alpha}| = |c||\vec{\alpha}|$

(iv) $|\langle \vec{\alpha}, \vec{\beta} \rangle| \leq |\vec{\alpha}||\vec{\beta}|$ (*Schwarzova nerovnosť*)

(v) $|\vec{\alpha} + \vec{\beta}| \leq |\vec{\alpha}| + |\vec{\beta}|$ (*trojuholníková nerovnosť*)

V (iv) *nastáva rovnosť práve vtedy, keď vektor $\vec{\alpha}$ je násobkom vektora $\vec{\beta}$.*
V (v) *nastane rovnosť, ak $\vec{\alpha}$ je nezáporným násobkom $\vec{\beta}$.*

Nerovnosť z (iv) môžete stretnúť aj pod názvom *Cauchy-Schwarzova* alebo *Cauchy-Buňakovského nerovnosť.*

Dôkaz. Vlastnosti (i), (ii), (iii) sa overia ľahko priamo z definície.

(iv) Dokážeme použitím vlastnosti (i) pre vektor $\vec{\alpha} + c\vec{\beta}$, kde c je ľubovoľné reálne číslo. Na základe vlastností skalárneho súčinu môžeme urobiť tieto úpravy:

$$|\vec{\alpha} + c\vec{\beta}|^2 = \langle \vec{\alpha} + c\vec{\beta}, \vec{\alpha} + c\vec{\beta} \rangle = \langle \vec{\alpha}, \vec{\alpha} \rangle + 2c\langle \vec{\alpha}, \vec{\beta} \rangle + c^2 \langle \vec{\beta}, \vec{\beta} \rangle = |\vec{\alpha}|^2 + 2c\langle \vec{\alpha}, \vec{\beta} \rangle + c^2 |\vec{\beta}|^2 \geq 0.$$

Pretože uvedená nerovnosť má platiť pre každé reálne číslo c a môžeme ju chápať ako kvadratickú nerovnicu s neznámou c, diskriminant tejto nerovnice nesmie byť kladný (aby príslušná kvadratická rovnica nemala nenulové reálne korene)

$$D = 4\langle \vec{\alpha}, \vec{\beta} \rangle^2 - 4|\vec{\alpha}|^2 |\vec{\beta}|^2 \leq 0.$$

Z tejto nerovnosti dostaneme

$$\langle \vec{\alpha}, \vec{\beta} \rangle^2 \leq |\vec{\alpha}|^2 |\vec{\beta}|^2$$
$$|\langle \vec{\alpha}, \vec{\beta} \rangle| \leq |\vec{\alpha}||\vec{\beta}|$$

Tým je dokázaná platnosť nerovnosti (iv) pre ľubovoľné vektory $\vec{\alpha}$, $\vec{\beta}$. Ešte sa pozrime na otázku, kedy nastáva rovnosť. Z rovnosti $|\langle \vec{\alpha}, \vec{\beta} \rangle| = |\vec{\alpha}||\vec{\beta}|$ vyplýva $D = 0$. Potom existuje také $c \in \mathbb{R}$, že platí $|\vec{\alpha} + c\vec{\beta}| = 0$. To znamená, že $\vec{\alpha} + c\vec{\beta} = 0$, čiže $\alpha = -c\vec{\beta}$. Zistili sme teda, že ak nastane rovnosť, tak $\vec{\alpha}$ musí nutne byť násobkom $\vec{\beta}$. Ľahko sa overí, že ak vektor $\vec{\alpha}$ je násobkom vektora $\vec{\beta}$, tak rovnosť skutočne nastane.

(v) Pokúsme sa upraviť výraz $|\vec{\alpha}+\vec{\beta}|^2$. Platí

$$|\vec{\alpha}+\vec{\beta}|^2 = \langle \vec{\alpha}+\vec{\beta}, \vec{\alpha}+\vec{\beta}\rangle = \langle \vec{\alpha},\vec{\alpha}\rangle + 2\langle \vec{\alpha},\vec{\beta}\rangle + \langle \vec{\beta},\vec{\beta}\rangle = \\ |\vec{\alpha}|^2 + 2\langle \vec{\alpha},\vec{\beta}\rangle + |\vec{\beta}|^2 \overset{(1)}{\leq} |\vec{\alpha}|^2 + 2|\vec{\alpha}||\vec{\beta}| + |\vec{\beta}|^2 = (|\vec{\alpha}|+|\vec{\beta}|)^2$$

(v nerovnosti (1) sme použili Schwarzovu nerovnosť (iv)). Z poslednej nerovnosti už vyplýva (v).

Aby platila rovnosť, musí platiť rovnosť v Schwarzovej nerovnosti použitej v (1). Teda $\vec{\alpha} = k\vec{\beta}$ pre nejaké $k \in \mathbb{R}$. Ľahko sa overí, že k rovnosti dôjde iba v prípade, že $k \geq 0$. (Stačí si uvedomiť, že $|\vec{\alpha}+k\vec{\alpha}| = |1+k|\cdot|\vec{\alpha}|$ a $|\vec{\alpha}|+|k\vec{\alpha}| = (1+|k|)\cdot|\vec{\alpha}|$.) □

Schwarzova nerovnosť pre priestor $\mathbb{R}^n$ s obvyklým skalárnym súčinom sa často používa pri dôkaze rôznych nerovností.

$$\left|\sum_{k=1}^{n} x_k y_k\right| \leq \sqrt{\sum_{k=1}^{n} x_k^2 \sum_{k=1}^{n} y_k^2} \tag{1.1}$$

Definícia 1.1.9. Nech V je euklidovský vektorový priestor.

Uhol dvoch nenulových vektorov definujeme ako taký uhol, pre ktorý platí

$$\cos\varphi = \frac{\langle \vec{\alpha},\vec{\beta}\rangle}{|\vec{\alpha}||\vec{\beta}|}.$$

V prípade, že niektorý z vektorov je nulový, položíme $\varphi = 0$.

Všimnite si, že vďaka Schwarzovej nerovnosti je výraz vystupujúci v definícii uhla dvoch vektorov z intervalu $\langle -1, 1\rangle$, teda takýto uhol skutočne existuje.

Definícia 1.1.10. Vektory $\vec{\alpha}, \vec{\beta} \in V$ nazveme *kolmé* (*ortogonálne*), ak $\langle \vec{\alpha},\vec{\beta}\rangle = 0$.

O k-tici vektorov $\vec{\alpha}_1, \ldots, \vec{\alpha}_k$ hovoríme, že tieto vektory sú ortogonálne, ak ľubovoľné 2 z nich sú ortogonálne, t.j. $\langle \vec{\alpha}_i, \vec{\alpha}_j\rangle = 0$ pre každé $i \neq j$.

Tvrdenie 1.1.11. *Nech V je euklidovský vektorový priestor. Ak nenulové vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_k$ sú ortogonálne, tak sú lineárne nezávislé.*

Dôkaz. Nech $c_1, \ldots, c_k \in \mathbb{R}$ sú také, že $c_1\vec{\alpha}_1 + \cdots + c_k\vec{\alpha}_k = \vec{0}$. Zoberme ľubovoľné $i \in \{1, 2, \ldots, k\}$. Potom dostaneme

$$0 = \langle \vec{\alpha}_i, \vec{0}\rangle = \langle \vec{\alpha}_i, c_1\vec{\alpha}_1 + \cdots + c_k\vec{\alpha}_k\rangle = c_i|\vec{\alpha}_i|^2.$$

Táto rovnosť môže platiť jedine ak $\vec{\alpha}_i = \vec{0}$ alebo $c_i = 0$. Pretože $\vec{\alpha}_i \neq \vec{0}$, platí $c_i = 0$. Použitím rovnakej úvahy pre všetky $i = 1, 2, \ldots, k$ dostaneme $c_1 = c_2 = \ldots = c_k = 0$. Teda dané vektory sú lineárne nezávislé. □

Definícia 1.1.12. Nech V je euklidovský priestor a $M \subseteq V$. Potom

$$M^\perp = \{\vec{\alpha} \in V; \langle \vec{\alpha},\vec{\beta}\rangle = 0 \text{ pre všetky } \vec{\beta} \in M\}$$

sa nazýva *ortogonálny doplnok* množiny M.

Tvrdenie 1.1.13. *Nech V je euklidovský priestor a $M \subseteq V$. Potom $M^\perp$ je vektorový podpriestor priestoru V.*

Dôkaz. Zrejme $\vec{0} \in M^\perp$, preto $M^\perp$ je neprázdna množina.

Treba ešte overiť, že pre všetky $\vec{\alpha}_1, \vec{\alpha}_2 \in M^\perp$ a $c, d \in \mathbb{R}$ aj $c\vec{\alpha}_1 + d\vec{\alpha}_2 \in M^\perp$. Ak pre všetky $\vec{\beta} \in M$ platí $\langle \vec{\alpha}_1, \vec{\beta} \rangle = 0$ a $\langle \vec{\alpha}_2, \vec{\beta} \rangle = 0$, tak aj

$$\langle c\vec{\alpha}_1 + d\vec{\alpha}_2, \vec{\beta} \rangle = c\langle \vec{\alpha}_1, \vec{\beta} \rangle + d\langle \vec{\alpha}_2, \vec{\beta} \rangle = 0,$$

teda $c\vec{\alpha}_1 + d\vec{\alpha}_2 \in M^\perp$. □

Tvrdenie 1.1.14. *Ak V je euklidovský priestor a $M \subseteq N \subseteq V$, tak*

$$N^\perp \subseteq M^\perp.$$

Dôkaz. Ak $\alpha \in N^\perp$, tak $\langle \vec{\alpha}, \vec{\beta} \rangle = 0$ pre všetky vektory $\vec{\beta} \in N$. To ale znamená, že $\langle \vec{\alpha}, \vec{\beta} \rangle = 0$ platí aj pre všetky vektory $\vec{\beta} \in M$ (pretože $M \subseteq N$), a teda $N^\perp \subseteq M^\perp$. □

Lema 1.1.15. *Nech V je euklidovský priestor a $\vec{\alpha}_1, \ldots, \vec{\alpha}_k \in V$. Nech $S = [\vec{\alpha}_1, \ldots, \vec{\alpha}_k]$ je podpriestor vygenerovaný týmito vektormi. Potom $S^\perp = \{\vec{\alpha}_1, \ldots, \vec{\alpha}_k\}^\perp$.*

Dôkaz. Z toho, že $\{\vec{\alpha}_1, \ldots, \vec{\alpha}_k\} \subseteq S$ vyplýva inklúzia $S^\perp \subseteq \{\vec{\alpha}_1, \ldots, \vec{\alpha}_k\}^\perp$.

Naopak, nech $\vec{\beta} \in \{\vec{\alpha}_1, \ldots, \vec{\alpha}_k\}^\perp$. To znamená, že $\langle \vec{\beta}, \vec{\alpha}_i \rangle = 0$ pre $i = 1, 2, \ldots, k$. Potom $\langle \vec{\beta}, \vec{\alpha} \rangle = 0$ aj pre ľubovoľný vektor $\vec{\alpha} \in [\vec{\alpha}_1, \ldots, \vec{\alpha}_k]$, pretože každý vektor z tohoto podpriestoru má tvar $\alpha = c_1\vec{\alpha}_1 + \cdots + c_k\vec{\alpha}_k$ a

$$\langle \vec{\beta}, c_1\vec{\alpha}_1 + \cdots + c_k\vec{\alpha}_k \rangle = c_1\langle \vec{\beta}, \vec{\alpha}_1 \rangle + \ldots + c_k\langle \vec{\beta}, \vec{\alpha}_k \rangle = 0.$$

□

Tvrdenie 1.1.16. *Ak V je euklidovský priestor a S, T sú podpriestory V, tak*

$$(S + T)^\perp = S^\perp \cap T^\perp.$$

Dôkaz. Pretože $S \subseteq S + T$ aj $T \subseteq S + T$ máme $(S + T)^\perp \subseteq S^\perp$ a súčasne $(S + T)^\perp \subseteq T^\perp$, z čoho vyplýva

$$(S + T)^\perp \subseteq S^\perp \cap T^\perp.$$

Naopak, ak $\vec{\alpha} \in S^\perp \cap T^\perp$, tak vektor $\vec{\alpha}$ je kolmý na ľubovoľný vektor z S aj na ľubovoľný vektor z T. Každý vektor z $S + T$ sa dá zapísať v tvare $\vec{\beta} + \vec{\gamma}$, kde $\vec{\beta} \in S$ a $\vec{\gamma} \in T$, takže potom platí

$$\langle \vec{\alpha}, \vec{\beta} + \vec{\gamma} \rangle = \langle \vec{\alpha}, \vec{\beta} \rangle + \langle \vec{\alpha}, \vec{\gamma} \rangle = 0,$$

teda α je kolmý na každý vektor z $S + T$, čiže patrí do $(S + T)^\perp$. Ukázali sme, že platí aj opačná inklúzia

$$S^\perp \cap T^\perp \subseteq (S + T)^\perp.$$

□

1.2 Gram-Schmidtov ortogonalizačný proces

Definícia 1.2.1. Vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ sa nazývajú *ortonormálne,* ak pre všetky i platí $|\vec{\alpha}_i| = 1$ a pre $i \neq j$ platí

$$\langle \vec{\alpha}_i, \vec{\alpha}_j \rangle = 0.$$

Stručne povedané, sú to ortogonálne normované vektory (pod slovom „normované“ rozumieme, že ich veľkosť je 1).

Z tvrdenia 1.1.11 vyplýva, že ortonormálne vektory sú lineárne nezávislé. Ak ich teda bude dosť veľa (v prípade konečnorozmerného priestoru toľko, koľko je dimenzia priestoru), môžu tvoriť bázu.

Definícia 1.2.2. Ak vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ sú ortonormálne a tvoria bázu vektorového priestoru V, tak túto bázu nazývame *ortonormálna báza.*

Príklad 1.2.3. Najjednoduchší príklad je štandardná báza $\vec{e}_1, \ldots, \vec{e}_n$ v priestore $\mathbb{R}^n$ so štandardným skalárnym súčinom

$$\langle \vec{\alpha}, \vec{\beta} \rangle = \sum_{k=1}^{n} a_k b_k.$$

V takomto euklidovskom priestore majú všetky vektory $\vec{e}_1, \ldots, \vec{e}_n$ veľkosť 1 a každý z nich je kolmý na všetky ostatné.

Výhoda ortonormálnej bázy spočíva v tom, že ak máme 2 vektory vyjadrené pomocou ortonormálnej bázy veľmi ľahko vypočítame ich skalárny súčin – v podstate rovnako ako v predchádzajúcom príklade.

Majme $\vec{\alpha} = c_1\vec{\alpha}_1 + \cdots + c_n\vec{\alpha}_n$ a $\vec{\beta} = d_1\vec{\alpha}_1 + \cdots + d_n\vec{\alpha}_n$, kde vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ tvoria ortonormálnu bázu. Potom

$$\langle \vec{\alpha}, \vec{\beta} \rangle = \langle c_1\vec{\alpha}_1 + \cdots + c_n\vec{\alpha}_n, d_1\vec{\alpha}_1 + \cdots + d_n\vec{\alpha}_n \rangle = \sum_{i=1}^{n}\sum_{j=1}^{n} c_i d_j \langle \vec{\alpha}_i, \vec{\alpha}_j \rangle.$$

Jediné nenulové členy v predchádzajúcej sume sú tie, kde $i = j$. Navyše vieme, že $\langle \vec{\alpha}_i, \vec{\alpha}_i \rangle = 1$. Dostaneme teda

$$\langle \vec{\alpha}, \vec{\beta} \rangle = \sum_{i=1}^{n} c_i d_i.$$

Naším najbližším cieľom je ukázať ako z ľubovoľnej bázy v euklidovskom vektorovom priestore vieme dostať ortonormálnu bázu. Dôkaz nasledujúcej vety poskytuje jej konštrukciu, ktorá sa zvykne nazývať Gram-Schmidtov ortogonalizačný proces.

Veta 1.2.4. *Nech V je euklidovský vektorový priestor a $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ je báza priestoru V. Potom existuje ortonormálna báza $\vec{\beta}_1, \ldots, \vec{\beta}_n$ priestoru V.*

Dôkaz. Nech $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ je báza priestoru V. Najprv sa pokúsime nájsť takú bázu $\vec{\gamma}_1, \ldots, \vec{\gamma}_n$ priestoru V, ktorej vektory sú ortogonálne.

$$\begin{aligned}
\vec{\gamma}_1 &= \vec{\alpha}_1 \\
\vec{\gamma}_2 &= \vec{\alpha}_2 + c_{21}\vec{\gamma}_1 \\
\vec{\gamma}_3 &= \vec{\alpha}_3 + c_{31}\vec{\gamma}_1 + c_{32}\vec{\gamma}_2 \\
&\vdots \\
\vec{\gamma}_n &= \vec{\alpha}_n + c_{n1}\vec{\gamma}_1 + c_{n2}\vec{\gamma}_2 + \ldots + c_{n,n-1}\vec{\gamma}_{n-1}
\end{aligned}$$

Budeme postupovať indukciou. Prvý krok indukcie je jasný - stačí položiť $\vec{\gamma}_1 = \vec{\alpha}_1$.

Predpokladajme teraz, že už sme našli k ortogonálnych vektorov $\vec{\gamma}_1, \ldots, \vec{\gamma}_k$, ktoré majú uvedený tvar. Navyše platí

$$[\vec{\alpha}_1, \ldots, \vec{\alpha}_k] = [\vec{\gamma}_1, \ldots, \vec{\gamma}_k].$$

Chceli by sme nájsť vektor $\vec{\gamma}_{k+1}$ kolmý na všetky predchádzajúce, ktorý by mal navyše tvar

$$\vec{\gamma}_{k+1} = \vec{\alpha}_{k+1} + c_{k+1,1}\vec{\gamma}_1 + c_{k+1,2}\vec{\gamma}_2 + \ldots + c_{k+1,k}\vec{\gamma}_k$$

a súčasne taký, aby platilo

$$[\vec{\alpha}_1, \ldots, \vec{\alpha}_{k+1}] = [\vec{\gamma}_1, \ldots, \vec{\gamma}_{k+1}].$$

Ak má byť tento vektor kolmý na predchádzajúce, musia platiť rovnosti

$$\begin{aligned} 0 = \langle \vec{\gamma}_{k+1}, \vec{\gamma}_1 \rangle &= \langle \vec{\alpha}_{k+1}, \vec{\gamma}_1 \rangle + c_{k+1,1}\langle \vec{\gamma}_1, \vec{\gamma}_1 \rangle \\ 0 = \langle \vec{\gamma}_{k+1}, \vec{\gamma}_2 \rangle &= \langle \vec{\alpha}_{k+1}, \vec{\gamma}_2 \rangle + c_{k+1,2}\langle \vec{\gamma}_2, \vec{\gamma}_2 \rangle \\ 0 = \langle \vec{\gamma}_{k+1}, \vec{\gamma}_3 \rangle &= \langle \vec{\alpha}_{k+1}, \vec{\gamma}_3 \rangle + c_{k+1,3}\langle \vec{\gamma}_3, \vec{\gamma}_3 \rangle \\ &\vdots \\ 0 = \langle \vec{\gamma}_{k+1}, \vec{\gamma}_k \rangle &= \langle \vec{\alpha}_{k+1}, \vec{\gamma}_k \rangle + c_{k+1,k}\langle \vec{\gamma}_k, \vec{\gamma}_k \rangle \end{aligned} \tag{1.2}$$

(V každej rovnici sme vynechali všetky členy obsahujúce $\langle \vec{\gamma}_i, \vec{\gamma}_j \rangle$ pre $i \neq j$, $i, j \in \{1, 2, \ldots, k\}$, pretože podľa indukčného predpokladu sú tieto hodnoty nulové.) Z predchádzajúcich rovníc môžeme vyjadriť všetky koeficienty $c_{k+1,i}$:

$$c_{k+1,i} = -\frac{\langle \vec{\alpha}_{k+1}, \vec{\gamma}_i \rangle}{\langle \vec{\gamma}_i, \vec{\gamma}_i \rangle}$$

pre každé $i = 1, 2, \ldots, k$.

Z rovníc (1.2) vidno, že pre takéto hodnoty $c_{k+1,i}$ bude vektor $\vec{\gamma}_{k+1}$ skutočne kolmý na všetky predchádzajúce vektory.

Ďalej vieme, že $\vec{\alpha}_{k+1} \notin [\vec{\alpha}_1, \ldots, \vec{\alpha}_k] = [\vec{\gamma}_1, \ldots, \vec{\gamma}_k]$ (lebo vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ sú lineárne nezávislé). Teda aj $\vec{\alpha}_{k+1}, \vec{\gamma}_1, \ldots, \vec{\gamma}_k$ sú lineárne nezávislé, čiže ich lineárnou kombináciou nemôžeme dostať $\vec{0}$. Pretože $\vec{\gamma}_{k+1} = \vec{\alpha}_{k+1} + c_{k+1,1}\vec{\gamma}_1 + c_{k+1,2}\vec{\gamma}_2 + \ldots + c_{k+1,k}\vec{\gamma}_k$ je lineárna kombinácia týchto vektorov a koeficient pri $\vec{\alpha}_{k+1}$ je $1 \neq 0$. Z toho vyplýva, že $\vec{\gamma}_{k+1} \neq \vec{0}$.

Súčasne platí $\vec{\gamma}_{k+1} \in [\vec{\alpha}_{k+1}, \vec{\gamma}_1, \ldots, \vec{\gamma}_k] = [\vec{\alpha}_1, \ldots, \vec{\alpha}_{k+1}]$. Teda $[\vec{\gamma}_1, \ldots, \vec{\gamma}_{k+1}] \subseteq [\vec{\alpha}_1, \ldots, \vec{\alpha}_{k+1}]$.

Ďalej $\vec{\alpha}_{k+1} = \vec{\gamma}_{k+1} - (c_{k+1,1}\vec{\gamma}_1 + c_{k+1,2}\vec{\gamma}_2 + \ldots + c_{k+1,k}\vec{\gamma}_k)$ je lineárna kombinácia vektorov $\vec{\gamma}_1, \ldots, \vec{\gamma}_{k+1}$, čiže platí aj obrátená inklúzia $[\vec{\alpha}_1, \ldots, \vec{\alpha}_{k+1}] \subseteq [\vec{\gamma}_1, \ldots, \vec{\gamma}_{k+1}]$.

Takto sme dostali bázu priestoru V, ktorej vektory sú ortogonálne. Aby boli ortonormálne, potrebujeme, každý z nich vydeliť jeho veľkosťou, čiže ortonormálnu bázu dostaneme tak, že položíme

$$\vec{\beta}_i = \frac{\vec{\gamma}_i}{|\vec{\gamma}_i|}.$$

□

Príklad 1.2.5. Zoberme si priestor $V = [(1, 0, 1, 0), (0, 2, -1, 1), (0, 2, 1, 3)]$. Ľahko sa overí, že tieto vektory sú lineárne nezávislé, teda tvoria bázu priestoru V. Pomocou Gram-Schmidtovho procesu nájdeme ortogonálnu bázu pre V. Položíme

$$\vec{\gamma}_1 = \vec{\alpha}_1 = (1, 0, 1, 0).$$

Ďalej chceme nájsť vektor $\vec{\gamma}_2 = \vec{\alpha}_2 + c\vec{\gamma}_1 = (0, 2, -1, 1) + c(1, 0, 1, 0) = (c, 2, c-1, 1)$ tak, aby bol kolmý na $\vec{\gamma}_1 = (1, 0, 1, 0)$. Dostávame teda rovnosť

$$\langle (c, 2, c-1, c+1), (1, 0, 1, 0) \rangle = c + c - 1 = 2c - 1 = 0,$$

z ktorej vyplýva $c = \frac{1}{2}$ a $\vec{\gamma}_2 = (\frac{1}{2}, 2, -\frac{1}{2}, 1)$.

Tretí vektor $\vec{\gamma}_3$ hľadáme v tvare $\vec{\gamma}_3 = \vec{\alpha}_3 + d\vec{\gamma}_1 + e\vec{\gamma}_2$ tak, aby

$$\langle \vec{\gamma}_3, \vec{\gamma}_1 \rangle = \langle \vec{\alpha}_3, \vec{\gamma}_1 \rangle + d\langle \vec{\gamma}_1, \vec{\gamma}_1 \rangle = 0$$
$$\langle \vec{\gamma}_3, \vec{\gamma}_2 \rangle = \langle \vec{\alpha}_3, \vec{\gamma}_2 \rangle + e\langle \vec{\gamma}_2, \vec{\gamma}_2 \rangle = 0$$

z čoho

$$d = -\frac{\langle \vec{\alpha}_3, \vec{\gamma}_1 \rangle}{\langle \vec{\gamma}_1, \vec{\gamma}_1 \rangle}$$
$$e = -\frac{\langle \vec{\alpha}_3, \vec{\gamma}_2 \rangle}{\langle \vec{\gamma}_2, \vec{\gamma}_2 \rangle}$$

Keď vypočítame $\langle \vec{\alpha}_3, \vec{\gamma}_1 \rangle = 1$, $\langle \vec{\gamma}_1, \vec{\gamma}_1 \rangle = 2$, $\langle \vec{\alpha}_3, \vec{\gamma}_2 \rangle = \frac{13}{2}$ a $\langle \vec{\gamma}_2, \vec{\gamma}_2 \rangle = \frac{11}{2}$, dostaneme

$$d = -\frac{1}{2}$$
$$e = -\frac{13}{11}$$
$$\vec{\gamma}_3 = \vec{\alpha}_3 - \frac{1}{2}\vec{\gamma}_1 - \frac{13}{11}\vec{\gamma}_2$$
$$\vec{\gamma}_3 = \left(-\frac{12}{11}, -\frac{4}{11}, \frac{12}{11}, \frac{20}{11}\right)$$

Zatiaľ sme teda dostali ortogonálne vektory, ktoré generujú V. Aby sme z nich dostali ortonormálne, musíme ich predeliť veľkosťou. Platí

$$|\vec{\gamma}_1| = \sqrt{2}$$
$$|\vec{\gamma}_2| = \frac{\sqrt{11}}{\sqrt{2}}$$
$$|\vec{\gamma}_3| = \frac{\sqrt{704}}{11} = \frac{8\sqrt{11}}{11} = \frac{8}{\sqrt{11}}$$

a teda ortonormálna báza priestoru V je

$$\vec{\beta}_1 = \frac{1}{\sqrt{2}}(1, 0, 1, 0)$$
$$\vec{\beta}_2 = \frac{\sqrt{2}}{\sqrt{11}}(\frac{1}{2}, 2, -\frac{1}{2}, 1)$$
$$\vec{\beta}_3 = \frac{\sqrt{11}}{8}\left(-\frac{12}{11}, -\frac{4}{11}, \frac{12}{11}, \frac{20}{11}\right) = \frac{1}{8\sqrt{11}}(-12, -4, 12, 20) = \frac{2}{\sqrt{11}}(-3, -1, 3, 5).$$

Vidíme, že vektory, ktoré sme dostali vyzerajú pomerne zložito. Nevedeli by sme si nejako zjednodušiť tieto výpočty? Možnože keby sme mali bázové vektory pôvodnej bázy o niečo jednoduchšie, aj ortonormálna báza by vyšla jednoduchšia. Ale dostať „peknú“ bázu vieme – to sa dá urobiť pomocou elementárnych riadkových operácií. Takže skúsme ešte takýto postup – vypočítajme najprv jednoduchšiu bázu pre priestor V.

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

Vidíme teda, že $V = [(1, 0, 0, -1), (0, 1, 0, 1), (0, 0, 1, 1)]$, čiže tentokrát ako štartovací bod pre Gram-Schmidtovu ortogonalizáciu použijeme bázové vektory $\vec{\alpha}_1 = (1, 0, 0, -1)$, $\vec{\alpha}_2 =$

$(0,1,0,1)$, $\vec{\alpha}_3 = (0,0,1,1)$. (Dúfam, že Vás nebude príliš pliesť, že tentokrát sme ako $\vec{\alpha}_1$, $\vec{\alpha}_2$ a $\vec{\alpha}_3$ označili úplne iné vektory ako v prvej časti príkladu. Dôvod nie je ten, že by sme mali príliš málo gréckych písmeniek, ale ten, že som chcel aby sa označenie zhodovalo s označením použitým v predchádzajúcom dôkaze.)

Opäť dostaneme:

$$\vec{\gamma}_1 = \vec{\alpha}_1 = (1,0,0,-1).$$

Vektor $\vec{\gamma}_2$ hľadáme v tvare $\vec{\alpha}_2 + c\vec{\gamma}_1$ a z podmienky, že $\langle \vec{\gamma}_2, \vec{\gamma}_1 \rangle = 0$ nám vyjde, že

$$c = -\frac{\langle \vec{\gamma}_1, \vec{\alpha}_2 \rangle}{\langle \vec{\gamma}_1, \vec{\gamma}_1 \rangle} = -\frac{-1}{2} = \frac{1}{2}$$

$$\vec{\gamma}_2 = (0,1,0,1) + \frac{1}{2}(1,0,0,-1) = \left(\frac{1}{2}, 1, 0, \frac{1}{2}\right)$$

Ďalej hľadáme $\vec{\gamma}_3$ v tvare $\vec{\gamma}_3 = \vec{\alpha}_3 + d\vec{\gamma}_1 + e\vec{\gamma}_2$. Koeficienty e a f opäť určíme z podmienok ortogonality.

$$d = -\frac{\langle \vec{\alpha}_3, \vec{\gamma}_1 \rangle}{\langle \vec{\gamma}_1, \vec{\gamma}_1 \rangle} = \frac{1}{2}$$

$$e = -\frac{\langle \vec{\alpha}_3, \vec{\gamma}_2 \rangle}{\langle \vec{\gamma}_2, \vec{\gamma}_2 \rangle} = -\frac{1}{3}$$

$$\vec{\gamma}_3 = (0,0,1,1) + \frac{1}{2}(1,0,0,-1) - \frac{1}{3}\left(\frac{1}{2}, 1, 0, \frac{1}{2}\right) = \left(\frac{1}{3}, -\frac{1}{3}, 1, \frac{1}{3}\right)$$

Teraz už zostáva len každý vektor predeliť jeho veľkosťou.

$$\vec{\beta}_1 = \frac{\vec{\gamma}_1}{|\vec{\gamma}_1|} = \frac{1}{\sqrt{2}}(1,0,0,-1)$$

$$\vec{\beta}_2 = \frac{\vec{\gamma}_2}{|\vec{\gamma}_2|} = \sqrt{\frac{2}{3}}\left(\frac{1}{2}, 1, 0, \frac{1}{2}\right)$$

$$\vec{\beta}_3 = \frac{\vec{\gamma}_3}{|\vec{\gamma}_3|} = \frac{\sqrt{3}}{2}\left(\frac{1}{3}, -\frac{1}{3}, 1, \frac{1}{3}\right)$$

V predošlom príklad sme použili presne postup z dôkazu. Poďme si ešte ukázať inú možnosť ako by sme mohli nájsť ortogonálnu bázu podpriestoru V z predošlej úlohy.

Príklad 1.2.6. Chceme hľadať bázu podpriestoru $V = [(1,0,0,-1),(0,1,0,1),(0,0,1,1)]$. Začnime tým, že si uvedomíme, že tento podpriestor je presne množina vektorov kolmých na $(1,-1,-1,1)$. Inak povedané, našli sme $V^\perp = [(1,-1,-1,1)]$. (Ten vlastne vieme získať jednoducho riešením homogénnej sústavy, ktorej riadky sú bázové vektory podpriestoru V.)

Toto sa dá spraviť pre ľubovoľný podpriestor. Môžeme si tiež uvedomiť, že inak sa dá na to pozrieť tak, že sme vlastne vyjadrili tento podpriestor v tvare $V = \{(x_1,x_2,x_3,x_4) \in \mathbb{R}^4; x_1 - x_2 - x_3 + x_4 = 1\}$. Teda vlastne je to množina riešení homogénnej sústavy. V tomto prípade ide o veľmi jednoduchú sústavu pozostávajúcu iba z jednej rovnice. Ale z minulého semestra vieme, že každý podpriestor je množinou riešení nejakej sústavy (veta I-5.7.11).

Vyjadrili sme podpriestor V trochu iným spôsobom, ktorý by nám mal pomôcť pri hľadaní ortogonálnej bázy. Máme teda pôvodnú bázu $\vec{\alpha}_1$, $\vec{\alpha}_2$, $\vec{\alpha}_3$, ktorú by sme chceli trochu pomeniť.

Začnime tým, že $\vec{\gamma}_1 = \vec{\alpha}_1 = (1,0,0,-1)$. Teraz by sme chceli nájsť ďalší vektor. Od neho chceme aby bol kolmý na $\vec{\gamma}_1$. Navyše chceme aby patril do V, čo je ekvivalentné s tým, že je kolmý na $(1,-1,-1,1)$. Tieto dve podmienky nám dajú sústavu dvoch homogénnych rovníc:

$$\begin{pmatrix} 1 & 0 & 0 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & -1 & -1 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & -2 \end{pmatrix}$$

Za $\vec{\gamma}_2$ môžeme zobrať ľubovoľné nenulové riešenie tejto sústavy – priestor riešení je dvojrozmerný, máme teda veľa možností. Zoberme napríklad $\vec{\gamma}_2 = (1, 2, 0, 1)$.

Teraz by sme chceli nájsť vektor $\vec{\gamma}_3$, ktorý má spĺňať obe podmienky určené predošlou sústavou (má byť kolmý na $\vec{\gamma}_1$ a patriť) do V. Ale pribudne nám aj nová podmienka, že má byť kolmý na $\vec{\gamma}_2$, a tým aj nová rovnica.

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

Opäť za $\vec{\gamma}_3$ môžeme voliť ľubovoľné nenulové riešenie tejto sústavy. Teraz už je podpriestor riešení iba jednorozmerný, čiže máme o čosi menšiu voľnosť. (Vektor $\vec{\gamma}_3$ je určený jednoznačne až na násobok.) Zoberme $\vec{\gamma}_3 = (1, -1, 3, 1)$.

Ak by sme chceli dostať ortonormálnu bázu, tak tieto vektory ešte treba vydeliť ich veľkosťou. Všimnime si, že takto dostaneme presne rovnaké vektory ako pri predošlom postupe. (Samozrejme, $\vec{\gamma}_2$ sme mohli voliť aj inak, čo by potom ovplyvnilo aj to, ako by vyzeralo $\vec{\gamma}_3$. Tu sme ich naschvál volili tak, aby vyšiel rovnaký výsledok. Môžete si vyskúšať nejaký iný výber, ktorým dostanete inú ortogonálnu resp. ortonormálnu bázu.)

Existenciu ortogonálnej bázy môžeme použiť na dôkaz niektorých ďalších faktov o ortogonálnom doplnku.

Veta 1.2.7. *Nech S je podpriestor konečnorozmerného euklidovského priestoru V. Potom ľubovoľný vektor $\vec{\gamma} \in V$ sa dá jednoznačne vyjadriť ako*

$$\vec{\gamma} = \vec{\alpha} + \vec{\beta},$$

kde $\vec{\alpha} \in S$ a $\vec{\beta} \in S^\perp$.

Dôkaz. Existencia: Vieme, že S má ortonormálnu bázu a tú môžeme rozšíriť na ortonormálnu bázu celého V. (Presnejšie povedané: Vieme ju podľa Steinitzovej vety rozšíriť na bázu celého V, ak z tejto bázy postupom použitým v dôkaze vety 1.2.4 vytvoríme ortonormálnu bázu, tak bázové vektory patriace do S sa nezmenia, pretože boli ortonormálne už pred ortonormalizáciou.)

Nech teda vektory $\vec{\gamma}_1, \ldots, \vec{\gamma}_k$ tvoria ortonormálnu bázu S a vektory $\vec{\gamma}_{k+1}, \ldots, \vec{\gamma}_n$ sú ostatné vektory ortonormálnej bázy V. Ľubovoľný vektor $\vec{\gamma}$ sa dá jednoznačne zapísať ako

$$\vec{\gamma} = c_1\vec{\gamma}_1 + \cdots + c_k\vec{\gamma}_k + c_{k+1}\vec{\gamma}_{k+1} + \cdots + c_n\vec{\gamma}_n.$$

Ak zvolíme $\vec{\alpha} = c_1\vec{\gamma}_1 + \cdots + c_k\vec{\gamma}_k$ a $\vec{\beta} = c_{k+1}\vec{\gamma}_{k+1} + \cdots + c_n\vec{\gamma}_n$, tak $\vec{\alpha} \in S$ a $\vec{\beta} \in S^\perp$.

Jednoznačnosť: Majme dva rozklady uvedeným spôsobom, t.j.

$$\vec{\gamma} = \vec{\alpha}_1 + \vec{\beta}_1 = \vec{\alpha}_2 + \vec{\beta}_2,$$

pričom $\vec{\alpha}_1, \vec{\alpha}_2 \in S$ a $\vec{\beta}_1, \vec{\beta}_2 \in S^\perp$.

Z rovnosti

$$\vec{\alpha}_1 - \vec{\alpha}_2 = \vec{\beta}_2 - \vec{\beta}_1$$

vidíme, že vektor $\vec{\alpha}_1 - \vec{\alpha}_2$ patrí do $S \cap S^\perp$. Z toho ale potom vyplýva

$$\langle \vec{\alpha}_1 - \vec{\alpha}_2, \vec{\alpha}_1 - \vec{\alpha}_2 \rangle = 0$$

a $\vec{\alpha}_1 - \vec{\alpha}_2 = 0$, čiže $\vec{\alpha}_1 = \vec{\alpha}_2$. Samozrejme, potom musí platiť aj $\vec{\beta}_1 = \vec{\beta}_2$. □

Definícia 1.2.8. V situácii z predošlej vety sa vektor $\vec{\alpha}$ nazýva *ortogonálna projekcia* vektora $\vec{\gamma}$ na podpriestor S.

Termín *ortogonálna projekcia* sa často používa aj pre zobrazenie $P\colon V \to V$, ktoré danému vektoru priradí jeho ortogonálnu projekciu. Ľahko sa overí, že toto zobrazenie je lineárne (úloha 1.2.12).

Dôsledok 1.2.9. *Nech S, T sú podpriestory konečnorozmerného priestoru V. Potom:*

(i) $V = S \oplus S^\perp$

(ii) $(S^\perp)^\perp = S$

(iii) $(S \cap T)^\perp = S^\perp + T^\perp$.

Dôkaz. (i) Vyplýva z predchádzajúcej vety a z vety I-4.5.6.

(ii) Priamo z definície vidno, že $S \subseteq (S^\perp)^\perp$. (Každý vektor z S je kolmý na všetky vektory z $S^\perp$.) Súčasne máme

$$V = S \oplus S^\perp = (S^\perp)^\perp \oplus S^\perp,$$

z čoho pre dimenzie dostaneme

$$d(S) + d(S^\perp) = d((S^\perp)^\perp) + d(S^\perp),$$

a teda $d(S) = d((S^\perp)^\perp)$. Keďže S je podpriestor $(S^\perp)^\perp$ a majú rovnakú dimenziu, platí $S = S^\perp$ (tvrdenie I-4.4.18).

(iii) Použitím tvrdenia 1.1.16 a časti (ii) dostaneme

$$(S^\perp + T^\perp)^\perp = (S^\perp)^\perp \cap (T^\perp)^\perp = S \cap T.$$

Ak ešte raz aplikujeme operátor ortogonálneho doplnku a použijeme (ii), dostávame rovnosť

$$S^\perp + T^\perp = (S \cap T)^\perp.$$

□

Nasledujúci príklad ukazuje, že v nekonečnorozmerných priestoroch tvrdenia dokázané v predchádzajúcom dôsledku neplatia vo všeobecnosti v prípade, že euklidovský vektorový priestor a podpriestory vystupujúce v dôsledku sú nekonečnorozmerné. (Tento príklad je o čosi komplikovanejší, ale aspoň pre tých z vás, ktorých zaujíma analýza, by mohol byť zaujímavý.)

Príklad* 1.2.10. Priestor, v ktorom budeme pracovať je priestor postupností

$$V = \ell_2 = \{(x_n) \in \mathbb{R}^{\mathbb{N}}; \sum_{n=1}^{\infty} x_n^2 < +\infty\}.$$

Skalárny súčin, s ktorým budeme pracovať, je

$$\langle x, y\rangle = \sum_{n=1}^{\infty} x_n y_n.$$

Tento priestor hrá dôležitú úlohu v matematickej analýze.

Fakt, že tento predpis naozaj určuje zobrazenie $\ell_2 \times \ell_2 \to \mathbb{R}$ (teda, že pre každé 2 postupnosti z ℓ_2 je súčet $\sum_{n=1}^{\infty} x_n y_n$ konečný) vyplýva z nerovnosti (1.1). Stačí v nej zobrať limitu pre $n \to \infty$ a dostaneme nerovnosť

$$\left|\sum_{k=1}^{\infty} x_k y_k\right| \leq \sqrt{\sum_{k=1}^{\infty} x_k^2 \sum_{k=1}^{\infty} y_k^2},$$

čo je presne nerovnosť, ktorá sa nám hodí na tomto mieste.

Overenie jednotlivých vlastností skalárneho súčinu je len o niečo zložitejšie ako v príklade 1.1.3.

Stále sme však ešte neoverili, že ide o euklidovský vektorový priestor – chýba nám overenie podmienky, s ktorou obvykle začíname, t.j. to, že V je vektorový priestor. Keďže ide o podmnožinu vektorového priestoru $\mathbb{R}^{\mathbb{N}}$ (a operácie sú definované rovnako), stačí overiť uzavretosť na súčet a skalárny násobok. Netriviálna je iba uzavretosť na súčet. Ak $(x_n), (y_n) \in \ell_2$, znamená to, že rady $\sum_{n=1}^{\infty} x_n^2$ i $\sum_{n=1}^{\infty} y_n^2$ konvergujú. Potom máme

$$\sum_{n=1}^{\infty}(x_n + y_n)^2 = \sum_{n=1}^{\infty}(x_n^2 + 2x_n y_n + y_n^2) \overset{(*)}{=} \sum_{n=1}^{\infty} x_n^2 + 2\sum_{n=1}^{\infty} x_n y_n + \sum_{n=1}^{\infty} y_n^2. \tag{1.3}$$

Dôležité je uvedomiť si, či skutočne platí rovnosť (*), t.j. či môžeme takýmto spôsobom zmeniť poradie sumácie. Z matematickej analýzy vieme, že sa to dá urobiť, ak rady, ktoré sčitujeme sú absolútne konvergentné.[1] Keďže rady $\sum_{n=1}^{\infty} x_n^2$ a $\sum_{n=1}^{\infty} y_n^2$ sú rady s kladnými členmi, pre ne je absolútna konvergencia zrejmá. V prípade radu $\sum_{n=1}^{\infty} x_n y_n$ si stačí všimnúť, že platí nerovnosť

$$\sum_{n=1}^{\infty}|x_n y_n| \leq \sqrt{\sum_{n=1}^{\infty} x_n^2 . \sum_{n=1}^{\infty} y_n^2}.$$

Túto nerovnosť môžeme dostať napríklad limitným prechodom z (1.1) (z (1.1) vieme, že uvedená nerovnosť platí pre všetky čiastočné súčty radov, ktoré v nej vystupujú).

Vidíme teda, že rady vystupujúce na pravej strane rovnosti (1.3) sú absolútne konvergentné, čím mám dokázanú platnosť tejto rovnosti.

Navyše, keď si ešte uvedomíme, že platí

$$\sum_{n=1}^{\infty} x_n y_n \leq \sum_{n=1}^{\infty}|x_n y_n|,$$

tak vidíme, že všetky rady na pravej strane (1.3) majú konečný súčet, teda platí $\sum_{n=1}^{\infty}(x_n + y_n)^2 < +\infty$, čo znamená, že $(x_n + y_n) \in \ell_2$.

Zvoľme si teraz podpriestor

$$S = \{(x_n) \in \ell_2; x_n = 0 \text{ pre všetky } n \text{ okrem konečného počtu}\}$$

[1] Pripomeňme, že rad $\sum_{n=1}^{\infty} a_n$ je absolútne konvergentný, ak konverguje rad $\sum_{n=1}^{\infty}|a_n|$.

pozostávajúci z tých postupností, ktoré majú iba konečne veľa nenulových členov. Platí

$$S^\perp = \{0\}.$$

Stačí si uvedomiť, že ak ako e_n označíme postupnosť, ktorá má všetky členy okrem n-tého miesta nuly a jej n-tý člen 1, t.j. $e_n = (0, \dots, 0, 1, 0 \dots)$, tak všetky takéto postupnosti patria do S. Teda pre každú postupnosť z $S^\perp$ dostaneme

$$\langle x, e_n \rangle = x_n = 0.$$

Z toho dostaneme

$$S \oplus S^\perp = S \neq V,$$
$$(S^\perp)^\perp = \{0\}^\perp = V.$$

Cvičenia

Úloha 1.2.1. Nájdite bázu a dimenziu $S^\perp$ pre daný podpriestor S priestoru $\mathbb{R}^4$:
a) $S = [(1,1,0,1),(2,1,0,1)]$
b) $S = [(1,5,4,3),(2,-1,2,-1)]$
c) $S = [(1,2,1,1),(2,1,-1,-1)]$
d) $S = [(1,2,3,4),(1,1,1,1),(4,3,2,1)]$
e) $S = [(2,1,2,3),(0,1,-2,1),(1,0,2,1)]$
f) $S = [(1,1,1,2),(1,0,1,1),(0,1,2,1)]$

Úloha 1.2.2. Zistite, či daný predpis určuje skalárny súčin na $\mathbb{R}^3$. Nech $\vec{\alpha} = (a_1, a_2, a_3)$ a $\vec{\beta} = (b_1, b_2, b_3)$.
a) $\langle \vec{\alpha}, \vec{\beta} \rangle = a_1b_1 - a_1b_2 + a_1b_3 + a_2b_1 + 3a_2b_2 - a_3b_3$
b) $\langle \vec{\alpha}, \vec{\beta} \rangle = a_1b_1 + 2a_1b_2 + 2a_2b_1$
c) $\langle \vec{\alpha}, \vec{\beta} \rangle = 3a_1b_2 + 2a_2b_2 + a_3b_3$
d) $\langle \vec{\alpha}, \vec{\beta} \rangle = a_1b_1 + a_2b_2 + a_3b_3$
e) $\langle \vec{\alpha}, \vec{\beta} \rangle = a_1b_1 + a_1b_2 + a_2b_1 + 3a_2b_2 + a_3b_3$
f) $\langle \vec{\alpha}, \vec{\beta} \rangle = a_1b_1 + a_1b_2 + a_2b_1 + a_2b_2 + 2a_3b_3$
g) $\langle \vec{\alpha}, \vec{\beta} \rangle = a_1b_1 + 2a_1b_2 + 2a_2b_1 + a_2b_2 + 2a_3b_3$
h) $\langle \vec{\alpha}, \vec{\beta} \rangle = a_1b_2 + a_2b_1$
i) $\langle \vec{\alpha}, \vec{\beta} \rangle = 3a_1b_1 + 2a_1b_2 + a_2b_1 + 3a_3b_3$

Úloha 1.2.3. Zistite, či $\sin \pi x$ a $\cos \pi x$ sú kolmé v priestore $C(0,1)$ so skalárnym súčinom z príkladu 1.1.6. Akú majú tieto vektory veľkosť?

Úloha 1.2.4. Overte či predpis
a) $\langle f, g \rangle = f(0)g(0) + f(1)g(1)$
b) $\langle f, g \rangle = f(-1)g(-1) + f(0)g(0) + f(1)g(1)$
určuje skalárny súčin na priestore P_2 všetkých polynómov stupňa najviac 2 nad poľom $\mathbb{R}$.

Úloha 1.2.5. Ukáže, že pre ľubovoľné dva vektory $\vec{\alpha}$, $\vec{\beta}$ v euklidovskom vektorovom priestore platí $|\vec{\alpha}| = |\vec{\beta}|$ práve vtedy, keď vektory $\vec{\alpha} - \vec{\beta}$ a $\vec{\alpha} + \vec{\beta}$ sú na seba kolmé.

Úloha 1.2.6. Dokážte, že v ľubovoľnom euklidovskom priestore platí:
a) $\langle \vec{\alpha}, \vec{\beta} \rangle = 0 \Rightarrow |\vec{\alpha} + \vec{\beta}|^2 = |\alpha|^2 + |\beta|^2$ (Pytagorova veta)
b) $|\vec{\alpha} + \vec{\beta}|^2 = |\alpha|^2 + |\beta|^2 + 2\langle \vec{\alpha}, \vec{\beta} \rangle$ (kosínová veta)
c) $|\vec{\alpha} + \vec{\beta}|^2 + |\vec{\alpha} - \vec{\beta}|^2 = 2(|\vec{\alpha}|^2 + |\vec{\beta}|^2)$ (rovnobežníkové pravidlo)

Úloha 1.2.7*. Ukážte, že ak $|\cdot|\colon V \to \mathbb{R}$ je funkcia definovaná na vektorovom priestore V nad $\mathbb{R}$, ktorá spĺňa podmienky (i), (ii), (iii) a (v) z tvrdenia 1.1.8 i rovnobežníkové pravidlo, tak existuje skalárny súčin na V taký, že $|\alpha| = \sqrt{\langle\vec{\alpha},\vec{\alpha}\rangle}$ pre všetky $\vec{\alpha} \in V$.

Úloha 1.2.8. Ukážte, že funkcia $|\cdot|\colon \mathbb{R}^n \to \mathbb{R}$, $|(x_1,\ldots,x_n)| = \max\{|x_i|; i = 1,\ldots,n\}$ spĺňa podmienky (i), (ii), (iii) a (v) z tvrdenia 1.1.8, ale neexistuje skalárny súčin na $\mathbb{R}^n$ taký, že $|\alpha| = \sqrt{\langle\vec{\alpha},\vec{\alpha}\rangle}$ (pre všetky $\vec{\alpha} \in \mathbb{R}^n$).

Úloha 1.2.9. Pre štvorcovú maticu typu $n \times n$ definujeme stopu matice ako súčet jej diagonálnych prvkov, t.j. $\mathrm{Tr}(A) = \sum_{i=1}^{n} a_{ii}$. Overte, či na vektorovom priestore $M_{n,n}(\mathbb{R})$ určuje predpis

$$\langle A, B\rangle = \mathrm{Tr}(AB^T)$$

skalárny súčin. (Hint 1: Pokúste sa vyjadriť hodnotu $\langle A, B\rangle$ pomocou prvkov matíc A, B. Hint 2: Možno vám pri tom pomôžu rovnosti $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$ a $\mathrm{Tr}(A) = \mathrm{Tr}(A^T)$. Prvá z nich sa dá ľahko overiť pomocou definície súčinu, druhá je zrejmá.)

Úloha 1.2.10. Overte, že v priestore $C(0, 2\pi)$ všetkých spojitých funkcií z uzavretého intervalu $\langle 0, 2\pi\rangle$ do $\mathbb{R}$ so skalárnym súčinom $\langle f, g\rangle = \int_0^{2\pi} f(x)g(x)dx$ sú ľubovoľné dve rôzne funkcie z množiny $\{1, \sin nx, \cos nx; n \in \mathbb{N}\}$ na seba kolmé. (Po vynormovaní by sme dostali množinu funkcií, ktorá má v tomto priestore do istej miery podobné vlastnosti ako ortonormálna báza v konečnorozmerných priestorov. Tento systém funkcií je dôležitý v matematickej analýze v súvislosti s *Fourierovými radmi*.)

Úloha 1.2.11. Nájdite ortonormálnu bázu pre priestory z úlohy 1.2.1.

Úloha 1.2.12. Nech S je podpriestor konečnorozmerného euklidovského vektorového priestoru V. Nech $P\colon V \to V$ je ortogonálna projekcia na tento podpriestor. Overte, že:
a) P je lineárne zobrazenie;
b) $\mathrm{Im}\, P = S$ a $\mathrm{Ker}\, P = S^\perp$;
c) $P \circ P = P$.

Úloha 1.2.13. Nájdite maticu ortogonálnej projekcie pri obvyklom skalárnom súčine pre:
a) priestory z úlohy 1.2.1;
b) pre ľubovoľný podpriestor $S = [\vec{\alpha}]$, pričom vektor $\vec{\alpha}$ je normovaný (má jednotkovú dĺžku);
c) pre podpriestor $S = [\vec{\alpha}_1,\ldots,\vec{\alpha}_k]$, pričom vektory $\vec{\alpha}_1,\ldots,\vec{\alpha}_k$ sú ortonormálne.
[Odpovede: b) $\vec{\alpha}^T\vec{\alpha}$; c) A^TA, kde A je matica, ktorej riadky tvoria vektory $\vec{\alpha}_1,\ldots,\vec{\alpha}_k$; toto sa inak dá zapísať aj ako $\vec{\alpha}_1^T\vec{\alpha}_1 + \vec{\alpha}_2^T\vec{\alpha}_2 + \cdots + \vec{\alpha}_k^T\vec{\alpha}_k$.]

Úloha 1.2.14. Ukážte, že pre ľubovoľný podpriestor S euklidovského vektorového priestoru V platí $S^{\perp\perp\perp} = S^\perp$. (Hint: Skúste si uvedomiť, ktorú z inklúzií medzi S a $S^\perp$ sme v dôkaze dôsledku 1.2.9 dokázali bez použitia predpokladu o konečnorozmernosti. Túto inklúziu použite raz pre S a raz pre $S^\perp$.)

Kapitola 2

Kvadratické formy

Táto kapitola je spracovaná prevažne na základe [KGGS, Kapitola 9].

2.1 Definícia a základné vlastnosti

Definícia 2.1.1. Výraz (polynóm)

$$\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_i x_j,$$

kde $a_{ij} \in \mathbb{R}$ a $x_1, \ldots, x_n$ sú (komutujúce) premenné budeme nazývať *kvadratická forma* v premenných $x_1, \ldots, x_n$.

V súvislosti s touto definíciou je užitočné ozrejmiť si zopár faktov.

Poznámka 2.1.2.

1. Podobne by sme mohli definovať kvadratickú formu nad ľubovoľným poľom. Budeme sa však zaoberať iba reálnym prípadom.
2. Slovo polynóm je v definícii uvedené v zátvorke preto, že s polynómami viac premenných sme doteraz nepracovali. Intuitívne by však mohlo byť zrejmé, ako sa takéto polynómy sčitujú a násobia. Pri násobení polynómov viac premenných si treba uvedomiť, že platí $x_i x_j = x_j x_i$ – presne to je myslené tým, že v definícii sa hovorí, že premenné komutujú. Znamená to teda, že dva polynómy uvedeného tvaru sa rovnajú ak pre všetky i platí $a_{ii} = b_{ii}$ a súčasne pre $i \neq j$ platí $a_{ij} + a_{ji} = b_{ij} + b_{ji}$.
3. Vieme, že v prípade polynómov jednej premennej nad poľom $\mathbb{R}$ bola rovnosť polynómov ekvivalentná s rovnosťou polynomických funkcií, ktoré tieto polynómy určujú. Podobne je to aj v tomto prípade – čiže kvadratické formy môžeme chápať ako funkcie n premenných špeciálneho tvaru. (Takéto polynómy viacerých premenných, ktoré majú všetky členy rovnakého stupňa, sa nazývajú *homogénne polynómy.*)

Príklad 2.1.3. Príkladom kvadratickej formy je $x_1^2 + 2x_1x_2 + 2x_2^2 + 4x_1x_3 + 2x_2x_3 + x_3^2$.
Všimnime si, že ju môžeme zapísať aj pomocou maticového zápisu

$$(x_1, x_2, x_3)\begin{pmatrix}1 & 2 & 4\\ 0 & 2 & 2\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}x_1\\ x_2\\ x_3\end{pmatrix}$$

Všeobecne, ak označíme $\vec{\alpha} = (x_1, \ldots, x_n)$, tak pre ľubovoľnú maticu $A \in M_{n,n}(\mathbb{R})$ je $\vec{\alpha}A\vec{\alpha}^T$ kvadratická forma.

Tú istú kvadratickú formu by sme mohli zapísať aj pomocou iných matíc. Nám sa bude hodiť hlavne reprezentácia pomocou symetrickej matice

$$(x_1, x_2, x_3) \begin{pmatrix} 1 & 1 & 2 \\ 1 & 2 & 1 \\ 2 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}.$$

Výhoda reprezentácie pomocou symetrickej matice je v tom, že takáto reprezentácia je už jednoznačná.

Veta 2.1.4. *Každá kvadratická forma sa dá jednoznačne zapísať ako $\vec{\alpha}B\vec{\alpha}^T$, kde B je symetrická matica.*

Dôkaz. Uvažujme kvadratickú formu $\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_ix_j$. Podľa toho, čo sme si povedali o rovnosti kvadratických foriem, matica B vyjadruje tú istú kvadratickú formu práve vtedy, keď platí

$$a_{ij} + a_{ji} = b_{ij} + b_{ji}$$

pre ľubovoľné i a j. Vďaka tomu, že matica b je symetrická je táto rovnosť ekvivalentná s rovnosťami

$$2b_{ij} = a_{ij} + a_{ji}$$
$$b_{ij} = \frac{a_{ij} + a_{ji}}{2}$$

Ľahko vidíme, že matica určená takýmto predpisom je skutočne symetrická ($b_{ij} = b_{ji}$). Súčasne sme ukázali, že toto je jediná možnosť ako voliť koeficienty matice B. □

2.2 Kanonický tvar kvadratickej formy

Pokúsme sa upraviť kvadratickú formu z príkladu 2.1.3 na iný tvar, ktorý môže byť na niektoré účely vhodnejší. Upravíme ju pomocou doplnenia na štvorec.

Príklad 2.2.1.

$$x_1^2 + 2x_1x_2 + 2x_2^2 + 4x_1x_3 + 2x_2x_3 + x_3^2 = (x_1 + x_2 + 2x_3)^2 + x_2^2 - 2x_2x_3 - 3x_3^2 =$$
$$(x_1 + x_2 + 2x_3)^2 + (x_2 - x_3)^2 - 4x_3^2 = (x_1 + x_2 + 2x_3)^2 + (x_2 - x_3)^2 - (2x_3)^2$$

To znamená, že ak by sme zaviedli nové premenné

$$y_1 = x_1 + x_2 + 2x_3$$
$$y_2 = x_2 - x_3$$
$$y_3 = 2x_3$$

tak pomocou týchto premenných môžeme kvadratickú formu zapísať v jednoduchšom tvare $y_1^2 + y_2^2 - y_3^2$.

Skúsme si ešte rozmyslieť, ako tento fakt môžeme zapísať pomocou maticového zápisu. Ak označíme $\vec{\alpha} = (x_1, x_2, x_3)$ a $\vec{\beta} = (y_1, y_2, y_3)$, tak uvedenú transformáciu premenných môžeme zapísať ako

$$\vec{\beta} = \vec{\alpha}P,$$

kde

$$P = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 2 & -1 & 2 \end{pmatrix}.$$

Vieme, že túto kvadratickú formu môžeme zapísať pomocou symetrickej matice $A = \left(\begin{smallmatrix} 1 & 1 & 2 \\ 1 & 2 & 1 \\ 2 & 1 & 1 \end{smallmatrix}\right)$ ako $\vec{\alpha} A \vec{\alpha}^T$.

Ak vyjadríme vektor $\vec{\alpha}$ pomocou vektoru $\vec{\beta}$, t.j. $\vec{\alpha} = \vec{\beta} P^{-1}$, tak dostaneme

$$\vec{\alpha} A \vec{\alpha}^T = \vec{\beta} P^{-1} A (P^{-1})^T \vec{\beta}^T.$$

Zistili sme, že matica kvadratickej formy $y_1^2 + y_2^2 - y_3^2$ sa dá vyjadriť ako $B = P^{-1} A (P^{-1})^T$. Všimnime si, že táto matica je symetrická – platí totiž

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

Pretože podľa vety 2.1.4 je symetrická matica prislúchajúca danej kvadratickej formy jednoznačne určená, zistili sme vlastne, že pre maticu $D = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{smallmatrix}\right)$ platí

$$D = P^{-1} A {P^{-1}}^T$$
$$A = P D P^T$$

Môžeme to (pre tento konkrétny príklad) overiť aj priamym výpočtom:

$$PDP^T = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 2 & -1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & -1 \\ 0 & 0 & 2 \end{pmatrix} =$$
$$= \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 2 & -1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & -1 \\ 0 & 0 & -2 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 2 & 1 \\ 2 & 1 & 1 \end{pmatrix} = A$$

Definícia 2.2.2. Hovoríme, že matice A a B sú *kongruentné,* ak existuje regulárna matica P taká, že

$$A = P B P^T.$$

Ľahko sa dá overiť, že kongruencia matíc je relácia ekvivalencie (úloha 2.2.1).

Poznámka 2.2.3. Z postupu použitého v predchádzajúcom príklade by mohlo byť vidno, že dve matice sú kongruentné práve vtedy, keď predstavujú tú istú kvadratickú formu, len vyjadrenú v iných premenných. (Pričom vzťah medzi pôvodnými a novými premennými je lineárny.)

Teraz by sme chceli ukázať, že každú kvadratickú formu môžeme pomocou vhodnej transformácie premenných previesť na podobný tvar – taký, ktorý zodpovedá diagonálnej matici majúcej na diagonále iba prvky 0, ± 1. Inak povedané, chceme ukázať, že každá symetrická matica je kongruentná s diagonálnou maticou takéhoto tvaru. Dôkaz bude konštruktívny a bude sa podobať na postup z predchádzajúceho príkladu. Ešte skôr než sa pustíme do dôkazu, vyskúšame si na jednom príklade jediný krok tohoto dôkazu, kde používame iný postup než doplnenie na štvorce.

Príklad 2.2.4. Uvažujme kvadratickú formu x_1x_2. Všimnime si, že

$$x_1x_2 = \frac{(x_1+x_2)^2}{4} - \frac{(x_1-x_2)^2}{4} = \left(\frac{x_1}{2}+\frac{x_2}{2}\right)^2 - \left(\frac{x_1}{2}-\frac{x_2}{2}\right)^2.$$

To znamená, že túto kvadratickú formu vieme previesť na tvar $y_1^2 - y_2^2$ pomocou transformácie

$$y_1 = \frac{x_1+x_2}{2}$$
$$y_2 = \frac{x_1-x_2}{2}$$

Ekvivalentne to môžeme vyjadriť tak, že premenné x_1 a x_2 sme transformovali ako

$$x_1 = y_1 + y_2$$
$$x_2 = y_1 - y_2$$

Môžeme si všimnúť, že pre matice $A = \begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $P = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ opäť platí $A = PBP^T$. Alebo tiež obrátene, $B = QAQ^T$, kde $Q = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. (Tieto matice sme dostali z vyjadrenia transformácií premenných podobným spôsobom ako v predchádzajúcom príklade.)

Veta 2.2.5. *Pre ľubovoľnú kvadratickú formu $\sum_{i=1}^n \sum_{j=1}^n a_{ij}x_ix_j$ existuje regulárna transformácia premenných $(y_1,\dots,y_n) = (x_1,\dots,x_n)P$ taká, že táto kvadratická forma sa dá v premenných $y_1,\dots,y_n$ vyjadriť ako*

$$\sum_{i=1}^n \sum_{j=1}^n a_{ij}x_ix_j = \sum_{k=1}^n d_k y_k^2,$$

kde $d_k \in \{0, \pm 1\}$.

Zápis v tvare $\sum_{k=1}^n d_k y_k^2$ budeme nazývať kanonický tvar *kvadratickej formy $\sum_{i=1}^n \sum_{j=1}^n a_{ij}x_ix_j$.*

Pod pojmom *regulárna transformácia premenných* v predchádzajúcej vete rozumieme to, že matica P určujúca túto transformáciu je regulárna.

Dôkaz. Dôkaz je v podstate konštruktívny a budeme v ňom používať postupy, ktoré sme si ukázali v predchádzajúcich príkladoch.

Ukážeme len, že ľubovoľnú kvadratickú formu možno previesť na *diagonálny tvar*

$$c_1y_1^2 + c_2y_2^2 + \cdots + c_ny_n^2.$$

Z tohoto tvaru už kanonický tvar dostaneme ľahko – stačí zaviesť nové premenné $z_i = y_i$ pre tie i, pre ktoré $c_i = 0$ a $z_i = \sqrt{|c_i|}y_i$ pre ostatné i. Takáto transformácia premenných je očividne regulárna.

Budeme postupovať matematickou indukciou vzhľadom na počet premenných n.

1° Ak máme len 1 premennú, tak kvadratická forma $a_{11}x_1^2$ je už v diagonálnom tvare.

2° Predpokladajme, že uvedené tvrdenie platí pre ľubovoľnú kvadratickú formu $n-1$ premenných. Uvažujme kvadratickú formu $\sum_{i=1}^n \sum_{j=1}^n a_{ij}x_ix_j$. Bez ujmy na všeobecnosti môžeme predpokladať, že matica $A = \|a_{ij}\|$ je symetrická.

Predpokladajme najprv, že $a_{11} \neq 0$. Všimnime si všetky členy, ktoré obsahujú premennú x_1 a vhodne ich upravme.

$$\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_ix_j = a_{11}x_1^2 + 2a_{12}x_1x_2 + \cdots + 2a_{1n}x_1x_n + \sum_{i=2}^{n}\sum_{j=2}^{n} a_{ij}x_ix_j =$$

$$a_{11}\left(x_1^2 + 2\frac{a_{12}}{a_{11}}x_1x_2 + \cdots + 2\frac{a_{1n}}{a_{11}}x_1x_n\right) + \sum_{i=2}^{n}\sum_{j=2}^{n} a_{ij}x_ix_j =$$

$$a_{11}\left(x_1 + \frac{a_{12}}{a_{11}}x_2 + \cdots + \frac{a_{1n}}{a_{11}}x_n\right)^2 - \sum_{i=2}^{n}\frac{a_{1i}^2}{a_{11}}x_i^2 - \sum_{i=2}^{n}\sum_{j=i+1}^{n}\frac{a_{1i}a_{1j}}{a_{11}}x_ix_j + \sum_{i=2}^{n}\sum_{j=2}^{n} a_{ij}x_ix_j$$

Ak označíme $y_1 = x_1 + \frac{a_{12}}{a_{11}}x_2 + \cdots + \frac{a_{1n}}{a_{11}}x_n$, podarilo sa nám upraviť pôvodnú kvadratickú formu na tvar

$$a_{11}y_1^2 + B(x_2, \ldots, x_n),$$

kde $B(x_2, \ldots, x_n)$ je kvadratická forma v $n-1$ premenných $x_2, \ldots, x_n$.

Podľa indukčného predpokladu sa dá táto kvadratická forma previesť regulárnou transformáciou premenných na diagonálny tvar $c_2y_2^2 + \cdots + c_nx_n^2$. Kombináciou týchto 2 transformácií prevedieme pôvodnú kvadratickú formu na

$$a_{11}y_1^2 + c_2y_2^2 + \cdots + c_nx_n^2.$$

Ak ako P' označíme maticu transformácie pre kvadratickú formu $B(x_2, \ldots, x_n)$, tak matica transformácie pôvodnej kvadratickej formy je

$$\begin{pmatrix} 1 & 0 & \ldots & 0 \\ \frac{a_{21}}{a_{11}} & & & \\ \vdots & & P' & \\ \frac{a_{n1}}{a_{11}} & & & \end{pmatrix}$$

Ak urobíme Laplaceov rozvoj podľa prvého riadku, dostávame $|P| = |P'|$, čiže matica P je tiež regulárna.

Zostáva nám vyriešiť prípad, že $a_{11} = 0$. V prípade, že $a_{ii} \neq 0$ pre nejaké i stačí vymeniť premenné x_1 a x_i (čo je regulárna transformácia) a ďalej postupovať ako v predchádzajúcom prípade.

Ak sú všetky diagonálne prvky matice $\|a_{ij}\|$ nulové, ale existujú nejaké i a j také, že $a_{ij} \neq 0$, použijeme postup z príkladu 2.2.4. Ak totiž dosadíme $x_i = y_i + y_j$ a $x_j = y_i - y_j$, tak dostaneme novú kvadratickú formu, ktorá určite bude obsahovať y_i^2 s nenulový koeficientom. Ďalej môžeme opäť postupovať ako v predchádzajúcom prípade. Použitá transformácia je opäť regulárna.

Zostáva jediný prípad – že všetky čísla a_{ij} sú nulové. Vtedy je už kvadratická forma v kanonickom tvare $0x_1^2 + \cdots + 0x_n^2$. □

Z toho, čo sme si ukázali v príklade 2.2.1 vyplýva, že sme súčasne dokázali nasledujúce tvrdenie o symetrických reálnych maticiach.

Dôsledok 2.2.6. *Každá reálna symetrická matica typu $n \times n$ je kongruentná s nejakou diagonálnou maticou* $\operatorname{diag}(d_1, \ldots, d_n)$ *takou, že $d_i \in \{0, \pm 1\}$ pre $i = 1 \ldots n$.*

Vysvetlíme si ešte (aspoň na konkrétnom príklade) iný postup ako vieme z danej symetrickej matice dostať jej zodpovedajúcu diagonálnu maticu i príslušnú maticu prechodu. Predtým však pripomeňme niečo o tom, ako súvisia riadkové a stĺpcové operácie s násobením matíc (pozri podkapitolu I-5.6).

Vykonaním elementárnej riadkovej operácie na matici A dostaneme maticu EA, kde E je matica elementárnej riadkovej operácie – je to taká matica, ktorú dostaneme z jednotkovej matice použitím tejto riadkovej operácie. Napríklad pripočítanie c-násobku prvého riadku k druhému zodpovedá vynásobením maticou $\left(\begin{smallmatrix}1&0&0\\c&1&0\\0&0&1\end{smallmatrix}\right)$ zľava.

Podobne ako riadkové operácie zodpovedajú násobeniu vhodnou maticou zľava, pre stĺpcové operácie treba použiť násobenie sprava. Všimnime si tiež, že ak E je matica riadkovej operácie, pre tú istú stĺpcovú operáciu dostaneme maticu E^T. Vidno to z toho, že ak riadková operácia vytvorila z matice A maticu EA, stĺpcovú operáciu si môžeme predstaviť ako vykonanie riadkovej operácie na matici A^T (a potom opätovné transponovanie), takže dostaneme $(EA^T)^T = AE^T$. Napríklad pripočítanie c-násobku prvého stĺpca k druhému je to isté ako vynásobenie maticou $\left(\begin{smallmatrix}1&c&0\\0&1&0\\0&0&1\end{smallmatrix}\right)$ sprava.

Z toho vidno, že ak by sme začali s maticou A a robili na nej riadkové aj stĺpcové operácie (t.j. po použití riadkovej operácie by sme hneď urobili aj tú istú operáciu na stĺpcoch) dostali by sme maticu

$$E_n \dots E_1 A E_1^T \dots E_n^T = E_n \dots E_1 A (E_n \dots E_1)^T.$$

Ak by sa nám takto podarilo upraviť maticu A na diagonálnu maticu, dostali by sme rovnosť

$$PAP^T = D,$$

kde P označuje $E_n \dots E_1$. Teda použitím riadkových a stĺpcových operácií by sme mohli dostať diagonálnu maticu a aj maticu transformácie premenných.

Príklad 2.2.7. Postup, ktorý sme si práve vysvetlili, si ukážeme na matici kvadratickej formy z príkladu 2.2.1.

Budeme teda robiť striedavo elementárne riadkové a stĺpcové operácie. Súčasne budeme na matici I robiť tie isté riadkové operácie, aby sme dostali maticu, ktorá transformuje A na diagonálnu maticu

$A = \left(\begin{smallmatrix}1&1&2\\1&2&1\\2&1&1\end{smallmatrix}\right) \overset{(1)}{\sim} \left(\begin{smallmatrix}1&1&2\\0&1&-1\\2&1&1\end{smallmatrix}\right) \overset{(1')}{\sim} \left(\begin{smallmatrix}1&0&2\\0&1&-1\\2&-1&1\end{smallmatrix}\right) \overset{(2)}{\sim} \left(\begin{smallmatrix}1&0&2\\0&1&-1\\0&-1&-3\end{smallmatrix}\right) \overset{(2')}{\sim} \left(\begin{smallmatrix}1&0&0\\0&1&-1\\0&-1&-3\end{smallmatrix}\right) \overset{(3)}{\sim} \left(\begin{smallmatrix}1&0&0\\0&1&-1\\0&0&-4\end{smallmatrix}\right) \overset{(3')}{\sim}$
$\left(\begin{smallmatrix}1&0&0\\0&1&0\\0&0&-4\end{smallmatrix}\right) \overset{(4)}{\sim} \left(\begin{smallmatrix}1&0&0\\0&1&0\\0&0&-2\end{smallmatrix}\right) \overset{(4')}{\sim} \left(\begin{smallmatrix}1&0&0\\0&1&0\\0&0&-1\end{smallmatrix}\right) = D$

(1) `2r-=1r` (od druhého riadku odrátam prvý); (1') je rovnaká operácia pre stĺpce (všimnite si, že vždy po vykonaní riadkovej aj stĺpcovej operácie musím dostať symetrickú maticu)
(2) `3r-=2*1r`
(3) `3r+=2r`
(4) `3r*=1/2`

$I = \left(\begin{smallmatrix}1&0&0\\0&1&0\\0&0&1\end{smallmatrix}\right) \overset{(1)}{\sim} \left(\begin{smallmatrix}1&0&0\\-1&1&0\\0&0&1\end{smallmatrix}\right) \overset{(2)}{\sim} \left(\begin{smallmatrix}1&0&0\\-1&1&0\\-2&0&1\end{smallmatrix}\right) \overset{(3)}{\sim} \left(\begin{smallmatrix}1&0&0\\-1&1&0\\-3&1&1\end{smallmatrix}\right) \overset{(4)}{\sim} \left(\begin{smallmatrix}1&0&0\\-1&1&0\\-\frac{3}{2}&\frac{1}{2}&\frac{1}{2}\end{smallmatrix}\right) =: Q$

Priamym výpočtom môžeme overiť, že skutočne platí $D = QAQ^T$. Tiež si môžeme všimnúť, že pre maticu P, ktorú sme dostali v príklade 2.2.1 platí $P = Q^{-1}$.

Na tomto sme videli príklade, že pokiaľ sa v priebehu úprav v tom riadku, ktorý práve upravujeme, na diagonále nevyskytne 0, je postup veľmi podobný na úpravu matice na redukovaný trojuholníkový tvar. Jediný rozdiel bol v tom, že ak sme z prvku c na diagonále chceli dostať ± 1, nedelili sme riadok c-čkom ale iba $\sqrt{|c|}$. V prípade, že by sa vyskytla nula na diagonále, mohli by sme si pomôcť pripočítaním riadku (a stĺpca), ktorý obsahuje nenulový prvok mimo diagonály – ako v nasledujúcom príklade.

Príklad 2.2.8. Pokúsme sa upraviť na kanonický tvar nasledujúcu maticu. V jednotlivých krokoch je urobená vždy riadková aj stĺpcová úprava
$A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} =: D$

V poslednom kroku sme od druhého riadku/stĺpca odrátali tretí riadok/stĺpec. (Na to, aby sme na diagonále dostali nenulový prvok a mohli pokračovať ďalej, stačilo by nám pripočítať ľubovoľný nenulový násobok tretieho riadku/stĺpca. Zhodou okolností sa pri tejto voľbe vynulovali aj zvyšné nediagonálne prvky.)

Použitím rovnakých riadkových úprav na jednotkovú maticu dostaneme
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} := P$

Pre túto maticu platí $PAP^T = D$.

Cvičenia

Úloha 2.2.1. Overte, že relácia $A \sim B$, t.j. kongruencia symetrických matíc, je relácia ekvivalencie na množine reálnych symetrických matíc typu $n \times n$.

Úloha 2.2.2. Upravte na diagonálny (prípadne kanonický) tvar a nájdite príslušnú transformáciu premenných. Zapíšte aj maticové rovnosti, ktoré z nich vyplývajú:
a) $x_1^2 + 2x_1x_2 + 2x_2^2 + 4x_2x_3 + 5x_3^2$
b) $x_1^2 - 4x_1x_2 + 2x_1x_3 + 4x_2^2 + x_3^2$
c) $x_1x_2 + x_2x_3 + x_3x_1$
d) $x_1^2 - 2x_1x_2 + 2x_1x_3 - 2x_1x_4 + x_2^2 + 2x_2x_3 - 4x_2x_4 + x_3^2 - 2x_4^2$
e) $x_1^2 + x_1x_2 + x_3x_4$

Úloha 2.2.3*. Preveďte kvadratickú formu $\sum_{i=1}^{n} x_i^2 + \sum_{1 \le i < k \le n} x_i x_k$ na diagonálny tvar.

[Výsledok: $y_1^2 + \frac{3}{4}y_2^2 + \frac{4}{6}y_3^2 + \cdots + \frac{n+1}{2n}y_n^2$; $P = \begin{pmatrix} 1 & 0 & \dots & \dots & \dots & 0 \\ \frac{1}{2} & 1 & 0 & \dots & \dots & 0 \\ \frac{1}{2} & \frac{1}{3} & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \dots & \frac{1}{n} & 1 \end{pmatrix}$]

Úloha 2.2.4*. Preveďte kvadratickú formu $\sum_{1 \le i < k \le n} x_i x_k$ na diagonálny tvar.

2.3 Zákon zotrvačnosti

Keďže sme tvar kvadratickej formy z vety 2.2.5 nazvali kanonický, dá sa očakávať, že bude v nejakom zmysle jednoznačný. Cieľom tejto kapitoly je práve sformulovať a dokázať túto jednoznačnosť.

Veta 2.3.1. *Pre danú kvadratickú formu je počet výskytov $+1$ a počet výskytov -1 v jej kanonickom tvare jednoznačne určený (nezávisí od transformácie, ktorou sme túto kvadratickú formu previedli na kanonický tvar).*

Dôkaz. Uvažujme kvadratickú formu $\vec{\alpha}A\vec{\alpha}^T$. Predpokladajme, že sa dá regulárnou transformáciou previesť na tvar

$$y_1^2 + \cdots + y_k^2 - y_{k+1}^2 - \cdots - y_s^2 \tag{2.1}$$

a súčasne (inou regulárnou transformáciou) na tvar

$$z_1^2 + \cdots + z_r^2 - z_{r+1}^2 - \cdots - z_t^2. \tag{2.2}$$

Označme ako P_1 a P_2 regulárne matice, ktoré zodpovedajú tejto transformácii premenných, t.j. $(y_1, \dots, y_n) = (x_1, \dots, x_n)P_1$ a $(z_1, \dots, z_n) = (x_1, \dots, x_n)P_2$.

Chceme ukázať, že $s = t$ a $k = r$.

Všimnime si, že s je presne hodnosť diagonálnej matice zodpovedajúcej kvadratickej forme (2.1) a t je hodnosť matice pre kvadratickú formu (2.2). Tieto matice môžeme vyjadriť ako $D_1 = P_1^{-1}A(P_1^{-1})^T$ a $D_2 = P_2^{-1}A(P_2^{-1})^T$. Súčasne vieme, že násobenie regulárnou maticou zodpovedá lineárnemu izomorfizmu, takže nemení hodnosť matice. Teda s aj t sa musí rovnať hodnosti matice A.

Zostáva nám dokázať, že $k = r$. Máme rovnosť

$$z_1^2 + \cdots + z_r^2 - z_{r+1}^2 - \cdots - z_t^2 = y_1^2 + \cdots + y_k^2 - y_{k+1}^2 - \cdots - y_s^2,$$

ktorú môžeme upraviť na tvar

$$z_1^2 + \cdots + z_r^2 + y_{k+1}^2 + \cdots + y_s^2 = y_1^2 + \cdots + y_k^2 + z_{r+1}^2 + \cdots + z_t^2. \tag{2.3}$$

Predpokladajme najprv, že $r < k$. Ukážeme, že za tohoto predpokladu sa dá nájsť nenulový vektor $(x_1, \dots, x_n)$ tak, aby platilo

$$z_1 = \cdots = z_r = y_{k+1} = \cdots = y_n = 0. \tag{2.4}$$

Všimnime si, že $(z_1, \dots, z_r, y_{k+1} \dots y_n) = (x_1, \dots, x_n)P$, kde matica P pozostáva z prvých r stĺpcov matice P_2 a z $(k+1)$-vého až n-tého stĺpca matice P_1. Hľadanie vektora $(x_1, \dots, x_n)$, ktorý vyhovuje rovnici (2.4) teda zodpovedá riešeniu homogénnej sústavy

$$\vec{\alpha}P = \vec{0},$$
$$P^T\vec{\alpha}^T = \vec{0}^T.$$

Keďže táto sústava má menej rovníc než neznámych, existuje aspoň jedno nenulové riešenie.

Ak však nájdeme $x_1, \dots, x_n$ také, že platí (2.4), na základe (2.3) musia byť nulové aj všetky ostatné premenné $z_{r+1}, \dots, z_t$. Lenže potom máme

$$(x_1, \dots, x_n) = (z_1, \dots, z_n)P_2^{-1} = \vec{0},$$

čo je spor s tým, že vektor $(x_1, \dots, x_n)$ je nenulový.

Podobne aj predpoklad $r > k$ by viedol k sporu. Musí teda platiť $k = r$. □

Predchádzajúca veta nám teda vlastne hovorí, že kanonický tvar kvadratickej formy je až na výmenu premenných jednoznačne určený.

Niekedy nás zaujímajú kvadratické formy, ktorých kanonický tvar má na diagonále iba jednotky.

Definícia 2.3.2. Nech A je symetrická reálna matica. Hovoríme, že A je
a) *kladne semidefinitná*, ak pre každý vektor $\vec{\alpha}$ platí $\vec{\alpha}A\vec{\alpha}^T \geq 0$;
b) *kladne definitná*, ak pre každý nenulový vektor $\vec{\alpha} \neq \vec{0}$ platí $\vec{\alpha}A\vec{\alpha}^T > 0$;
c) *záporne semidefinitná*, ak pre každý vektor $\vec{\alpha}$ platí $\vec{\alpha}A\vec{\alpha}^T \leq 0$;
d) *záporne definitná*, ak pre každý nenulový vektor $\vec{\alpha} \neq \vec{0}$ platí $\vec{\alpha}A\vec{\alpha}^T < 0$.

Je ľahké si všimnúť, že A je kladne (semi)definitná práve vtedy, keď $-A$ je záporne (semi)definitná.

Nasledujúca veta charakterizuje kladne definitné matice. Tým súčasne charakterizuje symetrické matice, ktoré určujú skalárne súčiny na $\mathbb{R}^n$ (pozri príklad 1.1.5).

Veta 2.3.3. *Symetrická matica A je kladne definitná práve vtedy, keď existuje regulárna matica P taká, že $A = PP^T$.*

Chceli by sme dokázať kritérium, pomocou ktorého sa dá pomerne jednoducho určiť, či je daná matica kladne definitná. V dôkaze tohoto kritéria bude užitočné nasledujúce pomocné tvrdenie:

Tvrdenie 2.3.4. *Nech A je symetrická reálna matica typu $n \times n$ taká, že všetky rohové determinanty*

$$D_1 = |a_{11}|$$
$$D_2 = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}$$
$$\vdots$$
$$D_n = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}$$

sú nenulové.

Potom matica A je kongruentná s diagonálnou maticou $\operatorname{diag}(D_1, D_2/D_1, D_3/D_2, \dots, D_n/D_{n-1})$.

Determinanty podmatíc vystupujúce v predchádzajúcom tvrdení sa niekedy zvyknú nazývať aj *hlavné minory* matice A.

Dôkaz. Ukážeme, že danú maticu možno upraviť na diagonálnu maticu len použitím operácií typu „pripočítanie násobku riadka/stĺpca k inému“ (t.j. nepoužívame výmeny riadkov a ani násobenie riadkov konštantou) tak, že dostaneme práve diagonálnu maticu tvaru, ktorý je uvedený v tvrdení.

Tvrdenie dokážeme matematickou indukciou vzhľadom na rozmer matice n. Platnosť tvrdenia pre $n = 1$ je zrejmá.

Vieme, že $D_1 = a_{11}$. Vďaka tomu môžeme vynulovať všetky prvky v prvom riadku a prvom stĺpci. (Odčítaním vhodného násobku prvého stĺpca/riadku.) Dostaneme tak maticu A do tvaru

$$\begin{pmatrix} a_{11} & 0 & \dots & 0 \\ 0 & b_{22} & \dots & b_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & b_{n2} & \dots & b_{nn} \end{pmatrix}$$

Pritom vieme, že úpravy, ktoré sme použili, nemenia determinant matice A ani žiaden z jej hlavných minorov (veta I-6.3.9).

Označme $D'_2, \dots, D'_n$ minory podmatice, ktorá vznikne vynechaním prvého riadku a prvého stĺpca. Z tvaru matice vidíme, že pre $k = 2, \dots, n$ platí $a_{11} D'_k = D_k$ a teda

$$D'_k = \frac{D_k}{D_1}.$$

Podľa indukčného predpokladu vieme túto podmaticu upraviť na diagonálny tvar, kde ako prvý člen na diagonále bude $D'_2 = \frac{D_2}{D_1}$ a ďalšie členy budú tvaru $\frac{D'_{k+1}}{D'_k} = \frac{D_{k+1}}{D_k}$. Z toho dostávame diagonálny tvar

$$\operatorname{diag}(D_1, D_2/D_1, D_3/D_2, \dots, D_n/D_{n-1})$$

pre pôvodnú maticu. □

Veta 2.3.5. *Nech A je symetrická matica typu $n \times n$. Matica A je kladne definitná práve vtedy, keď všetky jej hlavné minory $D_1, \dots, D_n$ sú kladné.*

Dôkaz. $\boxed{\Rightarrow}$ Ak je matica kladne definitná, tak je kongruentná s jednotkovou maticou. Z toho máme $A = PP^T$ a

$$|A| = |PP^T| = |P||P^T| = |P|^2 > 0.$$

Podobné tvrdenie pre minory vyplynie z toho, že ak za premenné $x_{k+1}, \dots, x_n$ dosadíme 0, dostaneme tak kvadratickú formu v premenných $x_1, \dots, x_k$, ktorá je opäť kladne definitná a ktorej matica je presne podmatica určená prvými k riadkami a stĺpcami.

$\boxed{\Leftarrow}$ Ak všetky hlavné minory matice A sú kladné, tak podľa tvrdenia 2.3.4 možno príslušnú kvadratickú formu upraviť na diagonálny tvar, v ktorom sú všetky členy kladné. Preto je táto matica kladne definitná. □

Dôsledok 2.3.6. *Nech A je symetrická matica typu $n \times n$. Matica A je záporne definitná práve vtedy, keď hlavný minor D_k má rovnaké znamienko ako $(-1)^k$ pre všetky $k = 1, \dots, n$.* (*Teda znamienka hlavných minorov sú striedavo* $(-, +, -, +, \dots)$.)

Poznámka 2.3.7. Aby sme dostali kritérium pre kladne semidefinitné matice, nestačí v predchádzajúcej vete zmeniť slovo „kladné“ na „nezáporné“. (Ako jednoduchý kontrapríklad môžeme zobrať maticu $\left(\begin{smallmatrix} 0 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.) V podobnom kritériu pre kladne semidefinitné matice vystupujú všetky minory matice A (=všetky determinanty štvorcových podmatíc).

Možnosť overiť, či je nejaká matica kladne alebo záporne definitná, má význam v matematickej analýze pre hľadaní extrémov funkcií viacerých premenných. Nutná podmienka na to, aby v nejakom bode x_0 mala nejaká funkcia lokálny extrém je, aby všetky parciálne derivácie boli nulové. (Podobne ako v jednorozmere bola nutná podmienka $f'(x_0) = 0$.)

$$\frac{\partial f}{\partial x_1}(x_0) = \dots = \frac{\partial f}{\partial x_n}(x_0) = 0.$$

V prípade, že je v jednorozmere splnená táto podmienka, skúmame ďalej to, či je kladná alebo záporná v danom bode jej druhá derivácia. Vo viacrozmere funkciu druhej derivácie hrá matice

$$H = \begin{pmatrix} \frac{\partial^2 f}{\partial x_1^2}(x_0) & \frac{\partial^2 f}{\partial x_1 \partial x_2}(x_0) & \dots & \frac{\partial^2 f}{\partial x_1 \partial x_n}(x_0) \\ \frac{\partial^2 f}{\partial x_2 \partial x_1}(x_0) & \frac{\partial^2 f}{\partial x_2^2}(x_0) & \dots & \frac{\partial^2 f}{\partial x_2 \partial x_n}(x_0) \\ \dots & \dots & \dots & \dots \\ \frac{\partial^2 f}{\partial x_n \partial x_1}(x_0) & \frac{\partial^2 f}{\partial x_n \partial x_2}(x_0) & \dots & \frac{\partial^2 f}{\partial x_n^2}(x_0) \end{pmatrix}$$

Táto matica je symetrická pre každú funkciu, ktorá je dvakrát spojito diferencovateľná.

Z viacrozmernej verzie Taylorovej vety totiž vyplýva, že hodnotu funkcie v bode x_0 môžeme aproximovať ako

$$f(x) - f(x_0) = \frac{1}{2!}(x - x_0)H(x - x_0)^T$$

(kde $x - x_0$ sú body z $\mathbb{R}^n$, teda ich chápeme ako vektory.)

To znamená, že hodnota $f(x) - f(x_0)$ je aproximovaná (v nejakom okolí bodu x_0) kvadratickou formou s maticou H. Z toho vyplýva, že v bode $f(x_0)$ je lokálne minimum práve vtedy, keď táto matica je kladne definitná ($f(x) - f(x_0)$ je v nejakom okolí kladné), lokálne maximum ak je záporne definitná. (V prípade, že je kladne definitná, vieme dokonca povedať, že vo vhodných súradniciach sa táto funkcia lokálne podobná na funkciu $x_1^2 + \dots + x_n^2$, ktorú si vieme aspoň v dvojrozmere celkom dobre geometricky predstaviť. Inou podobnou funkciou vieme zasa aproximovať tie funkcie, ktoré majú maticu H záporne definitnú.)

Viac o tejto problematike sa môžete dozvedieť napríklad v [GĎ, Kapitola 9.4], [A], [Pro2] (a v podstate v každej učebnici, ktorá sa zaoberá analýzou viac premenných).

Príklad 2.3.8. V dôkaze tvrdenia 2.3.4 sme videli, ako sa (za predpokladu, že daná symetrická matica má nenulové hlavné minory) dajú nájsť koeficienty v diagonálnom tvare, do ktorého túto maticu vieme previesť iba pomocou operácie pripočítavania niektorého násobku riadku/stĺpca k inému. Kombinácia takýchto operácií znamená to, že matica transformácie bude mať na diagonále jednotky.

Vyskúšajme si to na kvadratickej forme z úlohy 2.2.3*. Zodpovedajúca symetrická matica je

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

Ak počítame jej hlavné minory dostávame $D_1 = 1$ a pre $k > 1$

$$D_k = \begin{vmatrix} 1 & \frac{1}{2} & \frac{1}{2} & \dots & \frac{1}{2} \\ \frac{1}{2} & 1 & \frac{1}{2} & \dots & \frac{1}{2} \\ \dots & \dots & \dots & \dots & \dots \\ \frac{1}{2} & \frac{1}{2} & \dots & 1 & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & \dots & \frac{1}{2} & 1 \end{vmatrix} = \begin{vmatrix} \frac{k+1}{2} & \frac{k+1}{2} & \frac{k+1}{2} & \dots & \frac{k+1}{2} \\ \frac{1}{2} & 1 & \frac{1}{2} & \dots & \frac{1}{2} \\ \dots & \dots & \dots & \dots & \dots \\ \frac{1}{2} & \frac{1}{2} & \dots & 1 & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & \dots & \frac{1}{2} & 1 \end{vmatrix} = (k+1) \begin{vmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \dots & \frac{1}{2} \\ \frac{1}{2} & 1 & \frac{1}{2} & \dots & \frac{1}{2} \\ \dots & \dots & \dots & \dots & \dots \\ \frac{1}{2} & \frac{1}{2} & \dots & 1 & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & \dots & \frac{1}{2} & 1 \end{vmatrix} = (k+1) \begin{vmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \dots & \frac{1}{2} \\ 0 & \frac{1}{2} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \frac{1}{2} & 0 \\ 0 & 0 & \dots & 0 & \frac{1}{2} \end{vmatrix} = \frac{k+1}{2^k}$$

(V prvom kroku sme k prvému riadku pripočítali všetky ostatné, v poslednom kroku sme odrátali prvý riadok od všetkých ostatných. Takéto operácie nemenia hodnotu determinantu.)

Pre koeficienty na diagonále potom dostávame

$$c_k = \frac{D_k}{D_{k-1}} = \frac{k+1}{2^k} \frac{2^{k-1}}{k} = \frac{k+1}{2k},$$

čiže rovnaký výsledok ako nám vyšiel v úlohe 2.2.3*.

Cvičenia

Úloha 2.3.1. Pre danú kvadratickú formu určte tie hodnoty parametra $t \in \mathbb{R}$, pre ktoré je kladne definitná.
a) $5x_1^2 + 3x_2^2 + tx_3^2 + 4x_1x_2 - 3x_1x_3 - 2x_2x_3$
b) $2x_1^2 + x_2^2 + 3x_3^2 + 2tx_1x_2 + 2x_1x_3$
c) $\frac{1}{2}x_1^2 + 2x_2^2 - 3tx_3^2 + 2x_1x_2 + 2tx_2x_3 + 2x_1x_3$
d) $(x_1^2 + x_2^2 + x_3^2 + 2x_1x_3 - 2x_2x_3) + t(6x_1x_2 - 2x_1x_3 - 2x_1^2) + t^2(x_1^2 + x_2^2)$
(Poznámka: Niekedy sa výpočet determinantov $D_1, D_2, \dots$ môže zjednodušiť, ak zmeníte poradie premenných. Takáto zmena neovplyvní to, či je matica kladne definitná.)

Úloha 2.3.2. Z údajov ktoré sú zadané o symetrickej matici A zistite, ako vyzerá kanonický tvar príslušnej kvadratickej formy.[1] (Dali by sa tieto úvahy použiť na zistenie kanonického tvaru pre niektoré kvadratické formy z predošlých príkladov?)
a) Matica A je *kladne definitná* symetrická matica rozmerov $n \times n$.
b) Matica A je *záporne definitná* symetrická matica rozmerov $n \times n$.
c*) A je nenulová symetrická matica rozmerov 3×3, ktorá má nulovú stopu aj determinant, t.j. $\det(A) = \mathrm{Tr}(A) = 0$.

Úloha 2.3.3. Nech A je symetrická reálna matica taká, že $D_1 > 0, D_2 > 0, \dots, D_n > 0$. (Determinanty D_k majú rovnaký význam ako v tvrdení 2.3.4.) Dokážte, že potom $a_{nn} > 0$.

[1] V časti c) treba použiť nejaké veci, ktoré budeme preberať v ďalších kapitolách – sem som úlohu zaradil iba preto, že sa podobá na ostatné časti a že súvisí s kanonickým tvarom kvadratickej formy.

Úloha 2.3.4. Nech V je euklidovský vektorový priestor a $\vec{\alpha}_1, \ldots, \vec{\alpha}_n \in V$. Definujme maticu $A = \|a_{ij}\|$ tak, že $a_{ij} = \langle \vec{\alpha_i}, \vec{\alpha_j} \rangle$. (Táto matica sa zvykne volať *Gramova matica.*) Dokážte, že $|A| \geq 0$ a že tieto vektory sú lineárne nezávislé práve vtedy, keď $|A| > 0$.

Úloha 2.3.5*. Pre kvadratické formy $f = \sum_{i,j} a_{ij} x_i x_j$ a $g = \sum_{i,j} b_{ij} x_i x_j$ definujeme kvadratickú formu $(f, g) = \sum_{i,j} a_{ij} b_{ij} x_i x_j$. Ukážte, že ak f a g sú kladne definitné, tak aj (f, g) je kladne definitná.

Kapitola 3

Podobnosť matíc

Úvodná časť tejto kapitoly je spracovaná na základe [KGGS, 9.4,9.5] a ..... Podkapitola 3.2 obsahuje poznámky spracované J. Guričanom k tejto téme.[1]

V minulej kapitole sme sa zaoberali kvadratickými formami a ukázali sme, že pri vhodnej zmene premenných vieme kvadratickú formu upraviť na veľmi jednoduchý a pekný tvar (diagonálny, prípadne kanonický). Súčasne nám vzťah medzi týmito kvadratickými formami povedal niečo o vzťahoch medzi ich maticami.

V tejto kapitole sa budeme zaoberať do istej miery podobným problémom. Tentokrát sa však budeme snažiť pomocou zmeny premenných nájsť čo najkrajší tvar matice lineárnej transformácie.

3.1 Matica prechodu, podobnosť matíc

Pripomeňme, že ak $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ je nejaká báza konečnorozmerného vektorového priestoru V, tak ľubovoľný vektor z V sa dá jednoznačne vyjadriť v tvare $\vec{\gamma} = c_1\vec{\alpha}_1 + \cdots + c_n\vec{\alpha}_n$. (Pozri vetu I-4.4.16.) Tento fakt nám vlastne hovorí, že báza nám poskytuje akúsi súradnicovú sústavu v priestore V – každý vektor má jednoznačne určené súradnice $c_1, \ldots, c_n$.

Definícia 3.1.1. Ak $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ je báza vektorového priestoru V nad poľom F a $\vec{\gamma} \in V$, tak n-ticu $(c_1, \ldots, c_n) \in F^n$ takú, že platí

$$\vec{\gamma} = c_1\vec{\alpha}_1 + \cdots + c_n\vec{\alpha}_n$$

nazývame *súradnicami vektora* $\vec{\gamma}$ *v báze* $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$.

Jednou z otázok, ktorými sa budeme v tejto podkapitole zaoberať, je to, ako sa zmenia súradnice vektora pri zmene bázy daného vektorového priestoru. Pri tom bude užitočná matica uvedená v nasledujúcej definícii, ktorá popisuje istým spôsobom vzťah medzi týmito dvoma bázami.

Definícia 3.1.2. Nech $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ a $\vec{\alpha}'_1, \ldots, \vec{\alpha}'_n$ sú dve bázy vektorového priestoru V nad

[1] `http://modx.gurican.sk/assets/files/algebra_i_3/podobnost.pdf`

poľom F. Nech $p_{ij} \in F$ sú také, že platí

$$\begin{aligned}\vec{\alpha}'_1 =& p_{11}\vec{\alpha}_1 + p_{12}\vec{\alpha}_2 + \cdots + p_{1n}\vec{\alpha}_n \\ \vec{\alpha}'_2 =& p_{21}\vec{\alpha}_1 + p_{22}\vec{\alpha}_2 + \cdots + p_{2n}\vec{\alpha}_n \\ &\vdots \\ \vec{\alpha}'_n =& p_{n1}\vec{\alpha}_1 + p_{n2}\vec{\alpha}_2 + \cdots + p_{nn}\vec{\alpha}_n\end{aligned} \tag{3.1}$$

Potom maticu $P = \|p_{ij}\|$ nazývame *matica prechodu* od bázy $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ k báze $\vec{\alpha}'_1, \ldots, \vec{\alpha}'_n$.

Inak povedané, matica prechodu je taká matica P, ktorej i-ty riadok je tvorený súradnicami vektoru $\vec{\alpha}'_i$ v báze $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$.

Poznámka 3.1.3. V literatúre nájdete často i presne opačnú definíciu, než sme uviedli my. Teda niektorí autori by túto maticu nazvali maticou prechodu od $\vec{\alpha}'_1, \ldots, \vec{\alpha}'_n$ k $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$.

Skúsme si rozmyslieť, čo vieme povedať o matici prechodu opačným smerom, t.j. od $\vec{\alpha}'_1, \ldots, \vec{\alpha}'_n$ k $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$. Označme túto maticu $P' = \|p_{ij}\|$. Platí:

$$\begin{aligned}\vec{\alpha}_i =& p'_{i1}\vec{\alpha}'_1 + p'_{i2}\vec{\alpha}'_2 + \cdots + p'_{in}\vec{\alpha}'_n = \\ =& p'_{i1}(p_{11}\vec{\alpha}_1 + p_{12}\vec{\alpha}_2 + \cdots + p_{1n}\vec{\alpha}_n) + \\ &+ p'_{i2}(p_{21}\vec{\alpha}_1 + p_{22}\vec{\alpha}_2 + \cdots + p_{2n}\vec{\alpha}_n) + \\ &\vdots \\ &+ p'_{in}(p_{n1}\vec{\alpha}_1 + p_{n2}\vec{\alpha}_2 + \cdots + p_{nn}\vec{\alpha}_n)\end{aligned}$$

(Vektory $\vec{\alpha}'_1, \ldots, \vec{\alpha}'_n$ sme upravili pomocou (3.1).) Túto rovnosť teraz upravíme tak, že dáme dokopy členy obsahujúci ten istý vektor $\vec{\alpha}_i$ – inak povedané tak, ako sme ju zapísali pred chvíľou to znamená, že sčítance teraz usporiadame po stĺpcoch.

$$\begin{aligned}\vec{\alpha}_i =& (p'_{i1}p_{11} + p'_{i2}p_{21} + \cdots + p'_{in}p_{n1})\vec{\alpha}_1 + \\ &+ (p'_{i1}p_{12} + p'_{i2}p_{22} + \cdots + p'_{in}p_{n2})\vec{\alpha}_2 + \\ &\vdots \\ &+ (p'_{i1}p_{1n} + p'_{i2}p_{2n} + \cdots + p'_{in}p_{nn})\vec{\alpha}_n\end{aligned}$$

Obe predchádzajúce úpravy sme mohli stručnejšie zapísať takto:[2]

$$\vec{\alpha}_i = \sum_{j=1}^{n} p'_{ij}\vec{\alpha}'_j = \sum_{j=1}^{n}\sum_{k=1}^{n} p'_{ij}p_{jk}\vec{\alpha}_k = \sum_{k=1}^{n}\left(\sum_{j=1}^{n} p'_{ij}p_{jk}\right)\vec{\alpha}_k.$$

Z jednoznačnosti vyjadrenia vektora v báze $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ vyplýva, že koeficienty na pravej strane rovnosti sa musia rovnať

$$\sum_{j=1}^{n} p'_{ij}p_{jk} = \delta_{ik} = \begin{cases}1, & \text{ak } i = k \\ 0, & \text{inak.}\end{cases}$$

[2] Aj v ďalšom budeme používať tento stručnejší zápis pomocou súm, chcel som však aspoň pri prvom použití celú úpravu rozpísať trochu podrobnejšie tak, aby súčasne bolo vidno, že sa tam skutočne násobil i-ty riadok matice P' s jednotlivými stĺpcami a aby sme si uvedomili, že na výmenu poradia sumácie sa dá v takýchto prípadoch pozerať tak, že namiesto toho, aby sme rovnosť prečítali po riadkoch, si ju prečítame po stĺpcoch. V prípade, že by výmena poradia sčitovania v niektorom z ďalších dôkazov robila problémy, môže pomôcť prepísať si ju tak ako tu.

Zistili sme teda, že platí $P'P = I$, čo znamená, že P' je inverzná matica k P (pozri poznámku I-5.5.8).

Ukážme si, ako sme celé predchádzajúce odvodenie mohli stručnejšie odvodiť pomocou maticového zápisu.

V prvom rade si uvedomme, že vzťah (3.1) sa dá ekvivalentne zapísať takto:

$$\begin{pmatrix} \vec{\alpha}'_1 \\ \vdots \\ \vec{\alpha}'_n \end{pmatrix} = P \begin{pmatrix} \vec{\alpha}_1 \\ \vdots \\ \vec{\alpha}_n \end{pmatrix}. \tag{3.2}$$

Keďže vektory $\vec{\alpha}'_1, \ldots, \vec{\alpha}'_n$ aj $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ tvoria bázu, matice $\begin{pmatrix} \vec{\alpha}'_1 \\ \vdots \\ \vec{\alpha}'_n \end{pmatrix}$ a $\begin{pmatrix} \vec{\alpha}_1 \\ \vdots \\ \vec{\alpha}_n \end{pmatrix}$ majú hodnosť n, čiže sú regulárne. Ak pomocou nich vyjadríme maticu P, zistíme, že aj táto matica je regulárna (súčin dvoch regulárnych), čiže k nej existuje inverzná.

Hneď vidíme, že ak platí rovnosť (3.2), tak platí i

$$P^{-1} \begin{pmatrix} \vec{\alpha}'_1 \\ \vdots \\ \vec{\alpha}'_n \end{pmatrix} = \begin{pmatrix} \vec{\alpha}_1 \\ \vdots \\ \vec{\alpha}_n \end{pmatrix}.$$

Posledná rovnosť znamená presne to, že P^{-1} je matica prechodu od $\vec{\alpha}'_1, \ldots, \vec{\alpha}'_n$ k $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$.

Mohli by sme použiť aj postup, ktorý by úplne presne kopíroval predchádzajúce odvodenie, pričom by sme dostali

$$\begin{pmatrix} \vec{\alpha}_1 \\ \vdots \\ \vec{\alpha}_n \end{pmatrix} = P'P \begin{pmatrix} \vec{\alpha}_1 \\ \vdots \\ \vec{\alpha}_n \end{pmatrix}$$

z čoho (na základe regularity matice $\begin{pmatrix} \vec{\alpha}_1 \\ \vdots \\ \vec{\alpha}_n \end{pmatrix}$) už vyplýva $P'P = I$.

Poznámka 3.1.4. Predchádzajúce odvodenie v skutočnosti nebolo úplne korektné. Z vektorov $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ môžeme vytvoriť maticu typu $n \times n$ len vtedy, ak ide o vektory vo vektorovom priestore $V = F^n$. Toto však môžeme pomerne ľahko opraviť – stačí si uvedomiť, že každý n-rozmerný priestor je izomorfný s F^n (veta I-5.5.14). Ak si pevne zvolíme nejaký izomorfizmus medzi V a F^n, môžeme potom už všetky úvahy robiť v F^n. Dôležité je uvedomiť si, že izomorfizmus neovplyvní veci ako dimenzia, lineárna kombinácia, lineárna nezávislosť, súradnice vektora v danej báze a pod. (Napríklad ak vektor $\vec{\gamma} \in V$ má v báze $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ súradnice $(c_1, \ldots, c_n)$ a $f\colon V \to F^n$ je ľubovoľný izomorfizmus, tak aj súradnice vektora $f(\vec{\gamma})$ v báze $f(\vec{\alpha}_1), \ldots, f(\vec{\alpha}_n)$ sú $(c_1, \ldots, c_n)$. Z tejto skutočnosti ďalej vyplýva, že sa zachová aj matica prechodu medzi dvoma bázami.)

V ďalších úvahách budeme niekedy používať podobné argumenty – bez toho, že by sme zdôraznili prechod do F^n. Čitateľ si môže na príslušných rozmyslieť, že to skutočne funguje. Budeme však vždy uvádzať aj odvodenie, ktoré sa neopiera o maticový zápis, a teda pri ňom takýto prechod nie je potrebný.

Dokázali sme nasledujúcu vetu:

Veta 3.1.5. *Ak P je matica prechodu od bázy $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ k báze $\vec{\alpha}'_1, \ldots, \vec{\alpha}'_n$, tak matica P je regulárna a matica P^{-1} je matica prechodu opačným smerom, teda od $\vec{\alpha}'_1, \ldots, \vec{\alpha}'_n$ k $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$.*

Ukážeme, že to funguje aj naopak – pre každú bázu a regulárnu maticu P použitím predpisu (3.1) dostaneme opäť bázu.

Tvrdenie 3.1.6. *Nech $P = \|p_{ij}\|$ je regulárna matica typu $n \times n$ a $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ je báza vektorového priestoru V. Potom aj vektory $\vec{\alpha}'_1, \ldots, \vec{\alpha}'_n$ určené vzťahmi*

$$\begin{aligned}\vec{\alpha}'_1 &= p_{11}\vec{\alpha}_1 + p_{12}\vec{\alpha}_2 + \cdots + p_{1n}\vec{\alpha}_n\\ \vec{\alpha}'_2 &= p_{21}\vec{\alpha}_1 + p_{22}\vec{\alpha}_2 + \cdots + p_{2n}\vec{\alpha}_n\\ &\vdots\\ \vec{\alpha}'_n &= p_{n1}\vec{\alpha}_1 + p_{n2}\vec{\alpha}_2 + \cdots + p_{nn}\vec{\alpha}_n\end{aligned}$$

tvoria bázu priestoru V.

Dôkaz. Podľa vety I-4.4.14 nám stačí ukázať, že tieto vektory sú lineárne nezávislé. Nech teda $c_1\vec{\alpha}_1 + \cdots + c_n\vec{\alpha}_n = \vec{0}$. Ak do tejto rovnosti dosadíme vyjadrenia vektorov $\vec{\alpha}'_1, \ldots, \vec{\alpha}'_n$ v báze $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ dostaneme

$$\vec{0} = \sum_{i=1}^{n} c_i \left(\sum_{j=1}^{n} p_{ij}\vec{\alpha}_j \right) = \sum_{j=1}^{n} \left(\sum_{i=1}^{n} c_i p_{ij} \right) \vec{\alpha}_j.$$

Všimnime si, že koeficienty pri vektoroch $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ na pravej strane predchádzajúcej rovnosti sú presne zložky vektora $(c_1, \ldots, c_n)P$. Pretože vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ sú lineárne nezávislé, aby platila táto rovnosť, musia sa všetky tieto koeficienty rovnať nule. Dostali sme teda rovnosti

$$\begin{aligned}(c_1, \ldots, c_n)P &= \vec{0}\\ (c_1, \ldots, c_n) &= \vec{0}P^{-1} = \vec{0}\\ c_1 &= \cdots = c_n = 0\end{aligned}$$

Tým sme ukázali, že $\vec{\alpha}'_1, \ldots, \vec{\alpha}'_n$ sú lineárne nezávislé. □

Opäť môžeme to isté tvrdenie dokázať aj s využitím (3.2).

Dôkaz. Keďže $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ tvoria bázu, tak hodnosť matice $\begin{pmatrix}\vec{\alpha}_1\\ \vdots\\ \vec{\alpha}_n\end{pmatrix}$ je n. Pretože násobenie regulárnou maticou nemení hodnosť, tak aj hodnosť matice

$$\begin{pmatrix}\vec{\alpha}'_1\\ \vdots\\ \vec{\alpha}'_n\end{pmatrix} = P \begin{pmatrix}\vec{\alpha}_1\\ \vdots\\ \vec{\alpha}_n\end{pmatrix}$$

je n, čo znamená, že riadky tejto matice tvoria bázu vektorového priestoru V (keďže jeho dimenzia je n; aj tu využívame vetu I-4.4.14). □

Zmena súradníc vektora pri zmene bázy

Ukážeme si ako pomocou matice prechodu môžeme dostať vzťah medzi vyjadrením súradníc daného vektora v dvoch rôznych bázach.

Veta 3.1.7. *Nech $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ a $\vec{\alpha}'_1, \ldots, \vec{\alpha}'_n$ sú bázy vektorového priestoru V. Nech P je matica prechodu od bázy $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ k báze $\vec{\alpha}'_1, \ldots, \vec{\alpha}'_n$. Nech $\vec{\gamma} \in V$ a $(x_1, \ldots, x_n)$ sú súradnice vektora $\vec{\gamma}$ v báze $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$, $(x'_1, \ldots, x'_n)$ sú jeho súradnice v báze $\vec{\alpha}'_1, \ldots, \vec{\alpha}'_n$. Potom platí*

$$(x_1, \ldots, x_n) = (x'_1, \ldots, x'_n)P.$$

Postup, ktorý použijeme v dôkaze je v podstate rovnaký, ako úpravy použité v dôkaze predchádzajúceho tvrdenia.

Dôkaz. To, že vektor $\vec{\gamma}$ má v báze $\vec{\alpha}'_1, \ldots, \vec{\alpha}'_n$ súradnice $(x'_1, \ldots, x'_n)$ znamená, že platí rovnosť

$$\vec{\gamma} = x'_1\vec{\alpha}'_1 + \cdots + x'_n\vec{\alpha}'_n.$$

Ak do tejto rovnosti dosadíme za $\vec{\alpha}'_1, \ldots, \vec{\alpha}'_n$ z (3.1), dostaneme

$$\vec{\gamma} = \sum_{i=1}^{n} x'_i \sum_{j=1}^{n} p_{ij}\vec{\alpha}_j.$$

Aby sme dostali koeficienty pri jednotlivých vektoroch z $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$, zmeníme poradie sčitovania.

$$\vec{\gamma} = \sum_{j=1}^{n} \vec{\alpha}_j \sum_{i=1}^{n} x'_i p_{ij}$$

Výraz $\sum_{i=1}^{n} x'_i p_{ij}$, ktorý sme dostali pri vektore $\vec{\alpha}_j$, je presne j-ty prvok z n-tice $(x'_1, \ldots, x'_n)P$. Tým je tvrdenie vety dokázané. □

Opäť môžeme predchádzajúci dôkaz zapísať stručnejšie maticovým zápisom.

Dôkaz. Uvedomme si najprv, že $\vec{\gamma}$ má súradnice $(x'_1, \ldots, x'_n)$ v báze $\vec{\alpha}'_1, \ldots, \vec{\alpha}'_n$ práve vtedy, keď platí rovnosť

$$\vec{\gamma} = (x'_1, \ldots, x'_n) \begin{pmatrix} \vec{\alpha}'_1 \\ \vdots \\ \vec{\alpha}'_n \end{pmatrix}.$$

Spolu s rovnosťou (3.2) potom dostaneme

$$(x'_1, \ldots, x'_n) \begin{pmatrix} \vec{\alpha}'_1 \\ \vdots \\ \vec{\alpha}'_n \end{pmatrix} = (x'_1, \ldots, x'_n)P \begin{pmatrix} \vec{\alpha}_1 \\ \vdots \\ \vec{\alpha}_n \end{pmatrix},$$

teda súradnice v báze $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ sú $(x'_1, \ldots, x'_n)P$. □

Matica zobrazenia v danej báze

Definícia 3.1.8. Nech V je vektorový priestor a $f\colon V \to V$ je lineárne zobrazenie. Nech $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ je báza V. *Matica zobrazenia f vzhľadom na bázu* $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ je matica $A = \|a_{ij}\|$ taká, že platí

$$f(\vec{\alpha}_i) = a_{i1}\vec{\alpha}_1 + \cdots + a_{in}\vec{\alpha}_n.$$

Predchádzajúca definícia teda hovorí, že matica zobrazenia f pri báze V je taká matica, ktorej i-ty riadok tvoria súradnice obrazu i-teho bázového vektora v tejto báze.

Táto definícia do istej miery pripomína definíciu matice zobrazenia, ktorú poznáme z prvého ročníka (definícia I-5.3.8). Tam sme používali štandardnú bázu. Na rozdiel od prípadu, ktorý sme uviedli tu, nepožadovali sme, aby zobrazenie išlo z daného vektorového priestoru do toho istého priestoru. Podobne aj tu by sme mohli definovať o čosi všeobecnejší pojem matice lineárneho zobrazenia $f\colon V \to W$ vzhľadom na nejakú dvojicu báz (jedna z nich je bázou priestoru V a druhá je bázou priestoru W), zatiaľ sa však uspokojíme s týmto jednoduchším prípadom.

Nasledujúce tvrdenie je do istej miery analogické s podobným výsledkom z prvého ročníka, ktorý hovoril o rovnosti medzi obrazom vektora a súčinom vektora s maticou zobrazenia (poznámka I-5.4.10).

Tvrdenie 3.1.9. *Nech V je vektorový priestor, $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ je báza V a $f\colon V \to V$ je lineárne zobrazenie. Ak A je matica zobrazenia f pri báze $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ a vektor $\vec{\gamma}$ má v tejto báze súradnice $(x_1, \ldots, x_n)$, tak jeho obraz $f(\vec{\gamma})$ má v tej istej báze súradnice*

$$(x_1, \ldots, x_n)A.$$

Dôkaz. Podľa predpokladov platí $\vec{\gamma} = x_1\vec{\alpha}_1 + \cdots + x_n\vec{\alpha}_n$. Ak použijeme na obe strany rovnosti zobrazenie f, tak (s využitím linearity f) dostaneme

$$f(\vec{\gamma}) = f\left(\sum_{i=1}^{n} x_i\vec{\alpha}_i\right) = \sum_{i=1}^{n} x_i f(\vec{\alpha}_i) = \sum_{i=1}^{n} x_i \sum_{j=1}^{n} a_{ij}\vec{\alpha}_j = \sum_{j=1}^{n} \vec{\alpha}_j \sum_{i=1}^{n} x_i a_{ij}.$$

Vidíme, že j-ta súradnica vektora $f(\vec{\gamma})$ v báze $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ je $\sum_{i=1}^{n} x_i a_{ij}$, čo je skutočne j-ta súradnica vektora $(x_1, \ldots, x_n)A$. □

Opäť nás bude zaujímať to, ako sa zmení matica zobrazenia, ak zmeníme bázu vektorového priestoru.

Veta 3.1.10. *Nech V je vektorové priestory, $f\colon V \to V$ je lineárne zobrazenie a $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$, $\vec{\alpha}'_1, \ldots, \vec{\alpha}'_n$ sú bázy priestoru V. Ak P je matica prechodu od $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ k $\vec{\alpha}'_1, \ldots, \vec{\alpha}'_n$, A je matica zobrazenia f pri báze $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ a B je matica tohoto zobrazenia pri báze $\vec{\alpha}'_1, \ldots, \vec{\alpha}'_n$, tak platí*

$$B = PAP^{-1}. \tag{3.3}$$

Dôkaz. Uvažujme vektor $\vec{\gamma}$, ktorý má v báze $\vec{\alpha}'_1, \ldots, \vec{\alpha}'_n$ súradnice $(x'_1, \ldots, x'_n)$. Podľa vety 3.1.7 má tento vektor v báze $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ súradnice $(x'_1, \ldots, x'_n)P$. Ďalej z tvrdenia 3.1.9 vieme, že tento vektor sa v zobrazení f zobrazí na taký vektor, ktorý má súradnice $(x'_1, \ldots, x'_n)PA$ (ide opäť o súradnice v báze $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$.)

Schematicky môžeme situáciu v súradniciach $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ znázorniť takto

$$(x'_1, \ldots, x'_n)P \mapsto (x'_1, \ldots, x'_n)PA.$$

Čo dostaneme, ak sa na situáciu pozrieme v súradniciach $\vec{\alpha}'_1, \ldots, \vec{\alpha}'_n$? Súradnice vektora $f(\vec{\gamma})$ vieme použitím vety 3.1.7 previesť do tejto bázy použitím matice prechodu od $\vec{\alpha}'_1, \ldots, \vec{\alpha}'_n$ k $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$. Podľa vety 3.1.5 je to matica P^{-1}.

Vektor $f(\vec{\gamma})$ má teda v báze $\vec{\alpha}'_1, \ldots, \vec{\alpha}'_n$ súradnice $(x'_1, \ldots, x'_n)PAP^{-1}$. V súradniciach $\vec{\alpha}'_1, \ldots, \vec{\alpha}'_n$ to teda vyzerá takto:

$$(x'_1, \ldots, x'_n) \mapsto (x'_1, \ldots, x'_n)PAP^{-1}$$

Podľa tvrdenia 3.1.9 však súčasne musí platiť, že $f(\vec{\gamma})$ má v báze $\vec{\alpha}'_1, \ldots, \vec{\alpha}'_n$ súradnice $(x'_1, \ldots, x'_n)B$.

$$(x'_1, \ldots, x'_n) \mapsto (x'_1, \ldots, x'_n)B$$

Z toho dostávame rovnosť

$$(x'_1, \ldots, x'_n)B = (x'_1, \ldots, x'_n)PAP^{-1}.$$

Pretože táto rovnosť platí pre ľubovoľnú n-ticu $(x'_1, \ldots, x'_n) \in F^n$, musí platiť maticová rovnosť

$$B = PAP^{-1}.$$

□

Definícia 3.1.11. Nech A, B sú štvorcové matice nad poľom F. Ak existuje matica P taká, že $B = PAP^{-1}$, hovoríme, že matice A a B sú *podobné.*

Z vety 3.1.10 vyplýva, že 2 matice sú podobné práve vtedy, keď existujú lineárne zobrazenie a dvojica báz také, že toto zobrazenie má v jednej báze maticu A a v druhej maticu B.

Je pomerne ľahké overiť, že podobnosť matíc je relácia ekvivalencie.

Cvičenia

Úloha 3.1.1. Ukážte, že podobnosť matíc (chápaná ako relácia na $M_{n,n}(F)$) je relácia ekvivalencie.

Úloha 3.1.2. Pre $\vec{\alpha}_1 = (2,1)$, $\vec{\alpha}_2 = (1,2)$, $\vec{\beta}_1 = (-1,1)$, $\vec{\beta}_2 = (2,3)$, $\vec{\gamma}_1 = (1,1)$, $\vec{\gamma}_2 = (3,1)$. Nájdite:
a) Maticu P_1 prechodu od bázy $\vec{\alpha}_1, \vec{\alpha}_2$ k báze $\vec{\beta}_1$, $\vec{\beta}_2$.
b) Maticu P_2 prechodu od bázy $\vec{\beta}_1, \vec{\beta}_2$ k báze $\vec{\gamma}_1$, $\vec{\gamma}_2$.
c) Maticu P_3 prechodu od bázy $\vec{\alpha}_1, \vec{\alpha}_2$ k báze $\vec{\gamma}_1$, $\vec{\gamma}_2$.
d) Aký je vzťah medzi maticami P_1, P_2 a P_3?

Úloha 3.1.3. Nájdite všetky matice, ktoré sú podobné s nulovou maticou.

Úloha 3.1.4. Ak aspoň jedna zo štvorcových matíc A, B stupňa n je regulárna, tak AB a BA sú podobné. Platí to aj za predpokladu, že nie sú regulárne?

Úloha 3.1.5. Nech $A = cI$. Aké matice sú podobné s maticou A?

Úloha 3.1.6. Pre vektory $\vec{\gamma}_i \in \mathbb{R}^3$, $i = 1,2,3$, označme ako $\vec{x}_i$ súradnice vektora v báze $\vec{\alpha}_1, \vec{\alpha}_2, \vec{\alpha}_3$ a $\vec{x}'_i$ súradnice toho istého v báze $\vec{\alpha}'_1, \vec{\alpha}'_2, \vec{\alpha}'_3$. Nájdite matice prechodu od $\vec{\alpha}_1, \vec{\alpha}_2, \vec{\alpha}_3$ k $\vec{\alpha}'_1, \vec{\alpha}'_2, \vec{\alpha}'_3$ ak viete, že $\vec{x}_1 = (1,2,1)$, $\vec{x}'_1 = (-1,1,1)$, $\vec{x}_2 = (-1,0,3)$, $\vec{x}'_2 = (1,-1,1)$, $\vec{x}_3 = (3,1,2)$ a $\vec{x}'_3 = (2,1,-2)$. (Návod: Bude to matica istého lineárneho zobrazenia.)

Úloha 3.1.7. Ukážte, že ak matica A je podobná matici B, tak aj matice A^{-1} a B^{-1} sú podobné.

Úloha 3.1.8. Ukážte, že ak A a B sú podobné, tak majú rovnakú hodnosť, determinant a stopu. (Stopu matice sme definovali v úlohe 1.2.9.)

Úloha 3.1.9. Nájdite všetky matice A také, že jediná matica, ktorá je podobná s A, je práve matica A. (Inak povedané, trieda ekvivalencie matice A je jednoprvková.)

3.2 Podobnosť s diagonálnou maticou

3.2.1 Nutné a postačujúce podmienky

Pre štvorcovú maticu A je zaujímavé zistiť, či je podobná s diagonálnou maticou, t.j. či existuje regulárna matica P taká, že PAP^{-1} je diagonálna (matica). Kvôli zjednodušeniu budeme diagonálnu maticu

$$D = \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & d_n \end{pmatrix}$$

skrátene zapisovať ako $\mathrm{diag}(d_1, d_2, \dots, d_n)$.

Ak teda A je podobná diagonálnej, je $PAP^{-1} = \mathrm{diag}(d_1, d_2, \ldots, d_n) = D$ pre vhodnú maticu P a vhodné čísla $d_1, \ldots, d_n$, potom vieme ľahko vypočítať napr. A^{100} ako

$$P^{-1}\mathrm{diag}(d_1^{100}, d_2^{100}, \ldots, d_n^{100})P,$$

alebo ak v danom poli existujú napr. $\sqrt{d}_1, \ldots, \sqrt{d}_n$, tak vieme vypočítať niečo ako $\sqrt{A}$ (t.j. maticu B takú, že $B^2 = A$) pomocou $P^{-1} \cdot \mathrm{diag}(\sqrt{d}_1, \sqrt{d}_2, \ldots, \sqrt{d}_n) \cdot P$ (matica B nie je vo všeobecnosti určená jednoznačne, toto je jedno možné riešenie). Alebo keby sme chceli vypočítať niečo typu e^A, mohli by sme použiť Taylorov rozvoj $e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots$ a potom počítať

$$e^A = P^{-1}(I + D + \frac{D^2}{2!} + \frac{D^3}{3!} + \ldots)P = P^{-1} \cdot \mathrm{diag}(e^{d_1}, \ldots, e^{d_n}) \cdot P$$

Tento výpočet je urobený formálne, bez toho, aby sme strážili konvergenciu potrebných radov, ale pri troche starostlivosti by sa dalo ukázať, že je to pomerne zmysluplný postup. Dá sa potom robiť pre napr. funkcie $f(x)$, ktoré majú Taylorov rozvoj, ktorý pri dosadení všetkých čísiel $d_1, \ldots, d_n$ konverguje - t.j. všetky sa nachádzajú vnútri polomeru konvergencie príslušného Taylorovho radu.

Dá sa potom definovať aj niečo ako $e^{At} = P^{-1} \cdot \mathrm{diag}(e^{d_1 t}, \ldots, e^{d_n t}) \cdot P$. (Ide o funkciu, ktorá každému reálnemu číslu t priradí maticu.) Pre funkciu $f(t) = e^{At}$, potom platí $f'(t) = Af(t)$, čo aspoň trochu naznačuje, že takáto funkcia by mohla súvisieť s riešením diferenciálnych rovníc. (Na overenie rovnosti $f'(t) = Af(t)$ sa stačí presvedčiť o tom, že $(e^{At})' = P(e^{Dt})'P^{-1} = PDe^{Dt}P^{-1} = PDP^{-1}Pe^{Dt}P^{-1} = Ae^{At}$.)

Jedna vec, ktorá v danom momente nie je zrejmá je, či čísla $d_1, \ldots, d_n$ závisia od P - matice prechodu - alebo nie. Z nasledujúceho postupu bude jasné, že nezávisia (okrem poradia).

Skúsme si uvedomiť, čo presne znamená, že matica A je podobná s diagonálnou maticou D. To nám hovorí, že zobrazenie, ktoré má pri štandardnej báze maticu A, má pri vhodnej báze $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ maticu $D = \mathrm{diag}(d_1, d_2, \ldots, d_n)$. Pre každý z vektorov bázy teda platí

$$\vec{\alpha}_i A = d_i \vec{\alpha}_i.$$

Skúsme sa na to ešte pozrieť trochu inak. To, že A a D sú podobné nám dáva rovnosti

$$PAP^{-1} = D$$
$$PA = DP$$

Označme teraz riadky matice P ako $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$. Potom z predchádzajúcej rovnosti dostaneme:

$$\begin{pmatrix} \vec{\alpha}_1 \\ \vdots \\ \vec{\alpha}_n \end{pmatrix} A = D \begin{pmatrix} \vec{\alpha}_1 \\ \vdots \\ \vec{\alpha}_n \end{pmatrix},$$
$$\begin{pmatrix} \vec{\alpha}_1 A \\ \vdots \\ \vec{\alpha}_n A \end{pmatrix} = \begin{pmatrix} d_1\vec{\alpha}_1 \\ \vdots \\ d_n\vec{\alpha}_n \end{pmatrix}. \tag{3.4}$$

Keď porovnáme jednotlivé riadky matíc v poslednej rovnosti, opäť dostávame presne rovnaký vzťah

$$\vec{\alpha}_i A = d_i \vec{\alpha}_i.$$

Zdá sa, že pri zisťovaní, či je daná matica podobná s diagonálnou, by mohli hrať zaujímavú úlohu dvojice $c \in F$ a $\vec{\alpha} \in F^n$ s vlastnosťou $\vec{\alpha}A = c\vec{\alpha}$. Budeme sa teda teraz chvíľu zaoberať tým, ako takéto dvojice nájsť.

Definícia 3.2.1. Nech A je štvorcová matica nad poľom F. Prvok $c \in F$ nazveme *vlastným číslom* matice A, ak existuje nenulový vektor $\vec{\alpha} \in F^n$ taký, že $\vec{\alpha}A = c\vec{\alpha}$.

Nenulový vektor $\vec{\alpha} \in F^n$ nazývame *vlastným vektorom* matice A, ak existuje $c \in F$ (c môže byť aj 0) také, že $\vec{\alpha}A = c\vec{\alpha}$.

Ak $\vec{\alpha}$ je nenulový vektor a pre $c \in F$ platí $\vec{\alpha}A = c\vec{\alpha}$, hovoríme, aj, že (vlastný) vektor $\vec{\alpha}$ prislúcha ku vlastnému číslu c, alebo že (vlastné) číslo c prislúcha ku vlastnému vektoru $\vec{\alpha}$.

Ako nájdeme vlastné čísla a vlastné vektory matice A?

Najprv vlastné čísla: Pozrime sa nasledujúce ekvivalentné tvrdenia:

1. c je vlastné číslo matice A
2. Existuje nenulový vektor $\vec{\alpha}$ taký, že $\vec{\alpha}A = c\vec{\alpha}$
3. Existuje nenulový vektor $\vec{\alpha}$ taký, že $\vec{\alpha}A = \vec{\alpha}(cI)$ (I je identická matica)
4. Existuje nenulový vektor $\vec{\alpha}$ taký, že $\vec{\alpha}(A - cI) = \vec{0}$
5. Jadro zobrazenia s maticou $A - cI$ je netriviálne (t.j. toto zobrazenie nie je injektívne, t.j. matica $A - cI$ je singulárna).
6. Determinant matice $A - cI$ je nulový.

Keďže v tomto momente hľadáme vhodné prvky c, môžeme sa na determinant matice $A - cI$ v poslednom tvrdení pozrieť ako na výraz v „neznámej“ c - skúsme radšej použiť premennú x. Je dobre si uvedomiť, že $|A - xI|$ je polynóm v premennej x, napríklad ak

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 4 \end{pmatrix}, \text{ tak } \quad |A - xI| = \begin{vmatrix} 1-x & 2 \\ 0 & 4-x \end{vmatrix} = (1-x)(4-x) - 0 \cdot 2 = 4 - 5x + x^2$$

Posledne menovaný determinant budeme nazývať *charakteristický polynóm* matice A a označovať ako $ch_A(x)$, t.j. $ch_A(x) = |A - xI|$. Zistiť vlastné čísla matice A teda znamená nájsť korene jej charakteristického polynómu $ch_A(x)$.

Pre uvedený príklad teda dostávame, že vlastné čísla sú 1 a 4.

Nájsť vlastné vektory znamená teraz pre dané vlastné číslo c nájsť netriviálne riešenia rovnice $\vec{\alpha}(A - cI) = \vec{0}$. Ak si napíšeme $\vec{\alpha} = (x_1, \ldots, x_n)$, rovnicu môžeme prepísať do tvaru

$$(A - cI)^T \vec{\alpha}^T = (A - cI)^T \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

čo je vlastne homogénny systém rovníc s neznámymi $x_1, \ldots, x_n$ a maticou systému $(A - cI)^T$.

Pre uvedenú maticu

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 4 \end{pmatrix}$$

teda vieme, že jej vlastné čísla sú 1 a 4. Nájdime vlastné vektory:

Pre vlastné číslo 1:

$$A - 1 \cdot I = \begin{pmatrix} 1-1 & 2 \\ 0 & 4-1 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 0 & 3 \end{pmatrix}, \text{ teda } \quad (A - 1 \cdot I)^T = \begin{pmatrix} 0 & 0 \\ 2 & 3 \end{pmatrix}$$

Hľadáme riešenia homogénneho systému rovníc s poslednou maticou, t.j.

$$(A - 1 \cdot I)^T = \begin{pmatrix} 0 & 0 \\ 2 & 3 \end{pmatrix} \sim \begin{pmatrix} 2 & 3 \\ 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & \frac{3}{2} \\ 0 & 0 \end{pmatrix}$$

odkiaľ je vidieť, že vlastné vektory prislúchajúce vlastnému číslu 1 sú nenulové vektory z podpriestoru $[(-\frac{3}{2}, 1)] = [(-3, 2)]$. (Overte si, že napríklad $(-3, 2)A = (-3, 2)$.)

Pre vlastné číslo 4:

$$A - 4 \cdot I = \begin{pmatrix} 1-4 & 2 \\ 0 & 4-4 \end{pmatrix} = \begin{pmatrix} -3 & 2 \\ 0 & 0 \end{pmatrix}, \text{ teda } \quad (A - 4 \cdot I)^T = \begin{pmatrix} -3 & 0 \\ 2 & 0 \end{pmatrix}$$

Hľadáme riešenia homogénneho systému rovníc s poslednou maticou, t.j.

$$(A - 4 \cdot I)^T = \begin{pmatrix} -3 & 0 \\ 2 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

odkiaľ je vidieť, že vlastné vektory prislúchajúce vlastnému číslu 4 sú nenulové vektory z podpriestoru $[(0, 1)]$. (Overte si, že $(0, 1)A = 4(0, 1)$.)

Teraz sa môžeme zamyslieť nad tým, akú maticu má lineárna transformácia určená v báze $(1, 0), (0, 1)$ maticou A v báze $(-3, 2), (0, 1)$, t.j. ak $\vec{\varepsilon}_1 = (1, 0), \vec{\varepsilon}_2 = (0, 1)$ a $\vec{\alpha}_1 = (-3, 2), \vec{\alpha}_2 = (0, 1)$, $A = A_\varphi^{\vec{\varepsilon}_1, \vec{\varepsilon}_2} (= A_\varphi^\varepsilon)$, čo bude $A_\varphi^{\vec{\alpha}_1, \vec{\alpha}_2} (= A_\varphi^\alpha)$. Podľa vzorca (3.3) je

$$A_\varphi^\alpha = P A_\varphi^\varepsilon P^{-1}, \text{ kde } \quad P = \begin{pmatrix} -3 & 2 \\ 0 & 1 \end{pmatrix},$$

t.j. riadky matice P sú vektory $\vec{\alpha}_1, \vec{\alpha}_2$, t.j. generátory podpriestorov $[(-3, 2)]$ (ktorého nenulové vektory sú vlastné vektory prislúchajúce ku vlastnému číslu 1) a $[(0, 1)]$ (ktorého nenulové vektory sú vlastné vektory prislúchajúce ku vlastnému číslu 4). P je samozrejme matica prechodu od epsilonovej ku alfovej báze. Ale A_φ^α v $i-$tom riadku obsahuje súradnice obrazu vektora $\vec{\alpha}_i$ vyjadrené v báze $\vec{\alpha}_1, \vec{\alpha}_2$, a keďže $\vec{\alpha}_1$ je vlastný vektor prislúchajúci ku vlastnému číslu 1, je

$$\vec{\alpha}_1 A = 1.\vec{\alpha}_1 + 0.\vec{\alpha}_2$$

a podobne, keďže $\vec{\alpha}_2$ je vlastný vektor prislúchajúci ku vlastnému číslu 4, je

$$\vec{\alpha}_2 A = 0.\vec{\alpha}_1 + 4.\vec{\alpha}_2$$

a preto je $A_\varphi^\alpha = \text{diag}(1, 4) = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} = PAP^{-1}$

Iný spôsob, ako môžeme zdôvodniť túto rovnosť je použiť rovnaký postup ako pri odvodení (3.4).

V predchádzajúcom príklade tvorili vlastné vektory bázu priestoru $\mathbb{R}^2$, v ktorom sme pracovali. Vďaka tomu sme z nich dostali regulárnu maticu P. Nasledujúci príklad ukazuje, že to tak nemusí byť vždy.

Príklad 3.2.2. Vypočítajme vlastné čísla a vlastné vektory pre maticu

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

Tu je $ch_A(x) = \begin{vmatrix} 1-x & -3 & 3 \\ 0 & 1-x & -2 \\ 0 & 0 & 1-x \end{vmatrix} = (1-x)^3$, t.j. máme jediné vlastné číslo, 1 - je trojnásobný koreň charakteristického polynómu - (to samo ešte nemusí byť na závadu). Ale keď hľadáme vlastné vektory, zistíme, že sú to riešenia homogénneho systému rovníc s maticou $(A-I)^T$, t.j. $\begin{pmatrix} 0 & -3 & 3 \\ 0 & 0 & -2 \\ 0 & 0 & 0 \end{pmatrix}^T = \begin{pmatrix} 0 & 0 & 0 \\ -3 & 0 & 0 \\ 3 & -2 & 0 \end{pmatrix}$. Táto matica má očividne hodnosť 2 a preto riešenia tohoto systému tvoria jednorozmerný podpriestor ($[(0,0,1)]$), ktorého nenulové prvky sú jediné vlastné vektory tejto matice. Ako ukážeme, toto je problém (málo lineárne nezávislých vlastných vektorov), ktorý spôsobuje, že uvedená matica nie je podobná so žiadnou diagonálnou maticou.

Veta 3.2.3. *Nech $A = ||a_{ij}||$ je štvorcová matica typu $n \times n$ nad poľom F. Potom A je podobná s diagonálnou maticou práve vtedy, keď spomedzi vlastných vektorov vieme vybrať bázu.*

Dôkaz. $\Rightarrow$: Nech A je podobná diagonálnej matici $\mathrm{diag}(d_1, d_2, \ldots, d_n)$, t.j. existuje regulárna matica P taká, že $PAP^{-1} = \mathrm{diag}(d_1, d_2, \ldots, d_n)$. Potom ak $\varphi\colon F^n \to F^n$ je zobrazenie s maticou A, t.j. $A = A_\varphi^\varepsilon = A_\varphi^{\vec{\varepsilon}_1,\ldots,\vec{\varepsilon}_n}$, tak maticu P môžeme považovať za maticu prechodu od bázy $\vec{\varepsilon}_1, \ldots, \vec{\varepsilon}_n$ ku báze $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$, kde $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ sú postupne riadky matice P. Podľa vzorca (3.3) platí

$$PA_\varphi^\epsilon P^{-1} = A_\varphi^{\vec{\alpha}_1,\ldots,\vec{\alpha}_n},$$

a teda $A_\varphi^{\vec{\alpha}_1,\ldots,\vec{\alpha}_n} = \mathrm{diag}(d_1, d_2, \ldots, d_n)$. Toto a význam matice $A_\varphi^{\vec{\alpha}_1,\ldots,\vec{\alpha}_n}$ hovorí, že $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ sú vektory s vlastnosťou $\vec{\alpha}_i A = 0 \cdot \vec{\alpha}_1 + \cdots + d_i\vec{\alpha}_i + \cdots + 0 \cdot \vec{\alpha}_n = d_i\vec{\alpha}_i$, t.j. $\vec{\alpha}_i, i = 1, \ldots, n$ sú vlastné vektory matice A prislúchajú po rade vlastným číslam $d_i, i = 1, \ldots, n$ (a tiež, že $d_i, i = 1, \ldots, n$ sú vlastné čísla). Ale keďže vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ sú riadky regulárnej matice P, tvoria bázu F^n, takže vieme, že existujú vlastné vektory tvoriace bázu.

Opäť i v tomto prípade by sme ako alternatívne zdôvodnenie mohli použiť rovnaký postup ako pri odvodení (3.4).

$\Leftarrow$: Nech sa z vlastných vektorov matice A dá vybrať báza $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$. Potom ak tieto vektory uložíme ako riadky do matice P, tak rovnako ako v prvej časti dôkazu vidíme, že $PAP^{-1} = PA_\varphi^\epsilon P^{-1} = A_\varphi^{\vec{\alpha}_1,\ldots,\vec{\alpha}_n}$. Ale matica $A_\varphi^{\vec{\alpha}_1,\ldots,\vec{\alpha}_n}$ je diagonálna, lebo $c_1, \ldots, c_n$ sú vlastné čísla. □

Táto veta umožňuje zistiť, či je matica podobná s diagonálnou alebo nie, ale jej použitie je numericky pomerne náročné, a preto je vhodné (ak nás naozaj zaujíma len táto skutočnosť a nie aj matica prechodu P) nájsť iné, aspoň postačujúce podmienky, ktoré zabezpečia to, že matica A je podobná diagonálnej. Jedna z dvoch, ktoré si uvedieme, je založená na leme

Lema 3.2.4. *Nech $A = ||a_{ij}||$ je štvorcová matica typu $n \times n$ nad poľom F a vlastné čísla $c_1, \ldots, c_k$ matice A sú navzájom rôzne prvky poľa F, $\vec{\alpha}_1, \ldots, \vec{\alpha}_k$ sú vlastné vektory po rade prislúchajúce $c_1, \ldots, c_k$. Potom sú vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_k$ lineárne nezávislé.*

(*Stručne: Rôznym vlastným číslam zodpovedajú lineárne nezávislé vlastné vektory.*)

Dôkaz. Sporom. Vektor $\vec{\alpha}_1$ je vlastný vektor a preto je nenulový. Preto je závislosť vektorov $\vec{\alpha}_1, \ldots, \vec{\alpha}_k$ ekvivalentná s tým, že jeden z nich (pre $i > 1$) lineárnou kombináciu predchádzajúcich, t.j. existujú $a_1, \ldots, a_{i-1}$ také, že

$$\vec{\alpha}_i = a_1\vec{\alpha}_1 + \cdots + a_{i-1}\vec{\alpha}_{i-1}$$

Predpokladajme, že sme vybrali najmenšie i s takouto vlastnosťou, t.j. že vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_{i-1}$ už sú lineárne nezávislé. Teraz využijeme, že $\vec{\alpha}_1, \ldots, \vec{\alpha}_k$ sú vlastné vektory, preto

$$\vec{\alpha}_i A = c_i \vec{\alpha}_i = c_i(a_1\vec{\alpha}_1 + \cdots + a_{i-1}\vec{\alpha}_{i-1}) = c_i a_1 \vec{\alpha}_1 + \cdots + c_i a_{i-i}\vec{\alpha}_{i-1},$$

kde aspoň jedno z čísiel $a_1, \ldots, a_{i-1}$ je nenulové (inak by bol vektor $\vec{\alpha}_i$ nulový, čo sa vlastnému vektoru nemôže stať) ale aj

$$(a_1\vec{\alpha}_1 + \cdots + a_{i-1}\vec{\alpha}_{i-1})A = a_1\vec{\alpha}_1 A + \cdots + a_{i-i}\vec{\alpha}_{i-1}A = c_1 a_1 \vec{\alpha}_1 + \cdots + c_{i-1}a_{i-i}\vec{\alpha}_{i-1}$$

odkiaľ porovnaním a prehodením všetkých členov na ľavú stranu získame rovnosť

$$(c_i - c_1)a_1\vec{\alpha}_1 + \cdots + (c_i - c_{i-1})a_i\vec{\alpha}_{i-1} = \vec{0}$$

Keďže všetky čísla $c_i - c_1, \ldots, c_i - c_{i-1}$ sú nenulové, tak aspoň jedno z čísiel $(c_i - c_1)a_1, \ldots, (c_i - c_{i-1})a_{i-1}$ je nenulové, čím dostávame spor s lineárnou nezávislosťou vektorov $\vec{\alpha}_1, \ldots, \vec{\alpha}_{i-1}$. □

Príslušná postačujúca podmienka (ešte stále numericky pomerne náročná) potom znie

Dôsledok 3.2.5. *Nech $A = ||a_{ij}||$ je štvorcová matica typu $n \times n$ nad poľom F a vlastné čísla $c_1, \ldots, c_n$ matice A sú navzájom rôzne prvky poľa F (t.j. A má n navzájom rôznych vlastných čísiel z poľa F). Potom A je podobná s diagonálnou maticou.*

Dôkaz. Treba spojiť výsledok lemy 3.2.4 a vety 3.2.3 a uvedomiť si, že n lineárne nezávislých vektorov v priestore F^n tvorí bázu. □

Ešte sformulujme niekoľko pomocných kritérií, ktoré pomôžu zistiť skutočnosť, že dve konkrétne matice A, B nie sú podobné (obe tieto kritériá naozaj fungujú len jedným smerom, t.j. žiadne z nich nevie potvrdiť, že matice A, B sú podobné, vedia len vylúčiť tento fakt - sú to nutné podmienky na podobnosť).

Lema 3.2.6. *Nech A, B sú štvorcové matice typu $n \times n$ nad poľom F. Ak A a B sú podobné, tak $ch_A(x) = ch_B(x)$.*

Dôkaz. Nech sú A, B podobné, t.j. existuje taká regulárna matica P, že $PAP^{-1} = B$. Počítajme

$$\begin{aligned} ch_B(x) &= |B - xI| = |PAP^{-1} - xI| = |PAP^{-1} - xPIP^{-1}| = |P(A - xI)P^{-1}| = \\ &= |P||A - xI||P^{-1}| = |PP^{-1}||A - xI| = |I||A - xI| = |A - xI| = ch_A(x) \end{aligned}$$

□

a ešte jednoduchšie kritérium

Dôsledok 3.2.7. *Pre maticu $A = ||a_{ij}||$ - štvorcová matica typu $n \times n$ nad poľom F položme $\mathrm{Tr}(A) = a_{11} + a_{22} + \cdots + a_{nn}$ - t.j. $\mathrm{Tr}(A)$ je súčet prvkov na diagonále matice A. Ak sú matice A, B podobné, tak $\mathrm{Tr}(A) = \mathrm{Tr}(B)$.*

Hodnota $\mathrm{Tr}(A)$ sa nazýva *stopa matice A*.

Dôkaz. Treba si uvedomiť, ako vyzerá charakteristický polynóm matice A, je to

$$A - xI = \begin{vmatrix} a_{11}-x & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22}-x & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{n,n-1} & a_{nn}-x \end{vmatrix}$$

Podľa definície determinant $|B| = ||b_{ij}||$ je súčet súčinov $(-1)^{i(\varphi)} b_{1\varphi(1)} \dots b_{n\varphi(n)}$, kde $\varphi \in S_n$. Špeciálne pre našu maticu $A - xI$ si treba všimnúť, že pre φ identickú permutáciu, t.j. výber diagonálnych prvkov tam máme člen $+(a_{11}-x)) \cdots (a_{nn}-x)$. Ak zoberieme akýkoľvek iný súčin, neobsahuje aspoň jeden diagonálny prvok, ale musí obsahovať z každého riadka a každého stĺpca práve jeden prvok, tak musí existovať ešte jeden diagonálny prvok, ktorý neobsahuje a preto ako polynóm v premennej x má stupeň najviac $n-2$. Keďže

$$\begin{aligned}(a_{11}-x)\cdots(a_{nn}-x) &= (-1)^n x^n + (-1)^{n-1}(a_{11}+\cdots+a_{nn})x^{n-1} + \dots \\ &= (-1)^n x + (-1)^{n-1}\operatorname{Tr}(A)x^{n-1} + \dots\end{aligned}$$

a ostatné súčiny neovplyvnia koeficienty pri x^n a x^{n-1} v $ch_A(x)$, a podľa predošlej lemy $ch_A(x) = ch_B(x)$. Preto ich koeficienty pri x^{n-1} sú rovnaké, ale tieto koeficienty sú (až na znamienko) $\operatorname{Tr}(A)$, respektíve $\operatorname{Tr}(B)$, dostávame rovnosť $\operatorname{Tr}(A) = \operatorname{Tr}(B)$. □

Iný dôkaz. Ľahko sa dá overiť, že platí $\operatorname{Tr}(AB) = \operatorname{Tr}(BA)$ (úloha I-5.4.4). Z toho máme $\operatorname{Tr}(PAP^{-1}) = \operatorname{Tr}(APP^{-1}) = \operatorname{Tr}(A)$. □

Podobným spôsobom sa dá dokázať, že podobné matice A, B majú rovnaké determinanty (až na znamienko sú to absolútne koeficienty - koeficienty pri x^0 - v charakteristických polynómoch). Opäť, ten istý fakt môžeme dokázať aj použitím rovnosti $|AB| = |A||B| = |BA|$.

Príklad 3.2.8. Ak si vezmeme matice $A = \left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)$ a $B = \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$, tak vidíme, že obe matice majú rovnaký charakteristický polynóm $ch_A(x) = ch_B(x) = (x-1)^2$. Ľahko sa overí, že matica B nie je podobná so žiadnou diagonálnou maticou

Tento príklad teda ukazuje, že implikácie v leme 3.2.6 platí iba jedným smerom. (Iný kontrapríklad môžete nájsť v úlohe 3.2.14.)

3.2.2 Symetrické matice – veta o hlavných osiach

Teraz prejdeme ku druhému sľubovanému kritériu, ktoré zabezpečí, že matica je podobná s diagonálnou. Je založené na úplne inom princípe ako kritérium z dôsledku 3.2.5. Nižšie je sformulované pod názvom „veta o hlavných osiach“ (veta 3.2.11). Numericky je veľmi jednoduché, ale má pomerne úzky „rozsah aplikovateľnosti“ – hovorí, že každá reálna symetrická matica je podobná s diagonálnou maticou a že dokonca v tomto prípade vieme podobnosť zabezpečiť pomocou ortogonálnej matice P, t.j. táto podobnosť je zároveň kongruencia matíc (lebo *ortogonálna matica* je definovaná ako matica P spĺňajúca podmienku $P^T = P^{-1}$, a teda $PAP^{-1} = PAP^T$). Takúto podobnosť budeme nazývať ortogonálna podobnosť.

Zastavme sa chvíľu pri definícii ortogonálnej matice. Podľa definície je to matica, ktorá spĺňa $PP^T = P^TP = I$. Rovnosť $PP^T = I$ vlastne znamená, že riadky matice P sú ortonormálne vektory. Rovnosť $P^TP = I$ hovorí to isté o stĺpcoch matice P.

Pred uvedením samotnej vety o hlavných osiach potrebujeme dve tvrdenia.

Veta 3.2.9 (Schurova veta)**.** *Nech $A = ||a_{ij}||$ je štvorcová matica typu $n \times n$ nad poľom $\mathbb{R}$. Nech všetky vlastné čísla matice A sú z poľa $\mathbb{R}$. Potom existuje horná trojuholníková matica T, ktorá je ortogonálne podobná s maticou A.*

Dôkaz. Nech $a_n \in \mathbb{R}$ je vlastné číslo matice A, nech $\vec{\alpha}_n \in \mathbb{R}^n$ je vlastný vektor matice A prislúchajúci ku a_n a ktorý má dĺžku 1. Nech $\vec{\alpha}_1, \ldots, \vec{\alpha}_{n-1}$ sú vektory v $\mathbb{R}^n$, ktoré dopĺňajú $\vec{\alpha}_n$ do ortonormálnej bázy priestoru $\mathbb{R}^n$. Transformácia s maticou A (t.j. A je matica tejto transformácie pri štandardnej báze) má v báze $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ maticu A', ktorej posledný riadok obsahuje len jeden zaujímavý prvok — posledný prvok je a_n a ostatné prvky v poslednom riadku sú nuly, t.j. ak sú riadky matice P po rade vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$, tak

$$\left(\begin{array}{c|c} & c_1 \\ \mathrm{B} & \vdots \\ & c_{n-1} \\ \hline 0 \ldots 0 & a_n \end{array}\right) = A' = PAP^T$$

Keďže riadky matice P sú ortonormálne vektory, platí $P^T = P^{-1}$ (matica P je ortogonálna).

Celý dôkaz teraz urobíme indukciou. Štart indukcie — matica A je 1×1, teda A je horná trojuholníková a nemáme čo dokazovať.

Nech to teraz platí pre všetky matice B typu $(n-1) \times (n-1)$. Urobme vyššie uvedenú úvahu. Keďže pre charakteristické polynómy matíc A a B platí vzťah $ch_A(x) = (x - a_n)ch_B(x)$ (lebo matice A, A' sú podobné), každá vlastná hodnota matice B je vlastná hodnota matice A a preto všetky vlastné hodnoty matice B ležia v poli $\mathbb{R}$. Matica B je podľa indukčného predpokladu ortogonálne podobná hornej trojuholníkovej matici, označme ju T'. Teda existuje ortogonálna matica Q typu $(n-1) \times (n-1)$ taká, že $QBQ^T = T'$. Potom

$$\left(\begin{array}{c|c} & 0 \\ Q & \vdots \\ & 0 \\ \hline 0 \ldots 0 & 1 \end{array}\right) \cdot \left(\begin{array}{c|c} & c_1 \\ B & \vdots \\ & c_{n-1} \\ \hline 0 \ldots 0 & a_n \end{array}\right) \cdot \left(\begin{array}{c|c} & 0 \\ Q^T & \vdots \\ & 0 \\ \hline 0 \ldots 0 & 1 \end{array}\right) =$$

$$= \left(\begin{array}{c|c} QBQ^T & Q\gamma^T \\ \hline 0 \ldots 0 & a_n \end{array}\right) = \left(\begin{array}{c|c} T' & Q\gamma^T \\ \hline 0 \ldots 0 & a_n \end{array}\right),$$

kde $\gamma = (c_1, \ldots, c_{n-1})$. Posledná matica je ale vďaka indukčnému predpokladu horná trojuholníková matica. Keďže je matica

$$Q' = \left(\begin{array}{c|c} & 0 \\ Q & \vdots \\ & 0 \\ \hline 0 \ldots 0 & 1 \end{array}\right)$$

ortogonálna (overte!), je tým je ukončený dôkaz indukčného kroku. □

Ortogonálna podobnosť zachováva pojmy ako symetričnosť, kososymetričnosť a ortogonálnosť, t.j. ak je A symetrická (kososymetrická, ortogonálna) a P je ortogonálna matica, potom PAP^T je tiež symetrická (kososymetrická, ortogonálna). Ak je A symetrická, a T je horná trojuholníková ortogonálne podobná s A, tak T je tiež symetrická, t.j. diagonálna. Ak by sme vedeli, že reálna symetrická matica A je ortogonálne podobná hornej trojuholníkovej - t.j. vďaka Schurovej vete sa stačí presvedčiť, že reálna symetrická matica má vždy všetky vlastné čísla reálne - vedeli by sme, že je (dokonca ortogonálne) podobná diagonálnej matici.

Veta 3.2.10. *Nech $A = ||a_{ij}||$ je štvorcová symetrická matica typu $n \times n$ nad poľom $\mathbb{R}$, potom všetky vlastné čísla matice A sú z poľa $\mathbb{R}$.*

Dôkaz. Podľa predpokladu je polynóm $ch_A(x)$ polynóm s reálnymi koeficientami, t.j. jeho korene sú buď reálne alebo komplexné čísla. Budeme predpokladať, že sú to komplexné čísla $a+bi$ $(a,b \in \mathbb{R})$ a dokážeme, že pre symetrickú maticu A je vždy $b=0$, t.j. je to reálne číslo.

Keďže $A = ||a_{ij}||$ je matica nad $\mathbb{R}$, určite je to aj matica nad poľom komplexných čísiel $\mathbb{C}$. Ak uvažujeme o jej (možno komplexnom) vlastnom čísle $z = a + bi$, musí k nemu prislúchať (možno komplexný) vlastný vektor $(z_1, \ldots, z_n) = (a_1 + b_1 i, \ldots, a_n + b_n i) = (a_1, \ldots, a_n) + (b_1, \ldots, b_n)i$ $(a_i, b_i \in R)$, t.j. platí $\vec{z}A = (a + bi)\vec{z}$. Ak položíme $\vec{\alpha} = (a_1, \ldots, a_n)$ a $\vec{\beta} = (b_1, \ldots, b_n)$, tak vďaka tomu, že A je reálna matica môžeme túto rovnosť napísať ako

$$(\vec{\alpha} + \vec{\beta}i)A = (a + bi)(\vec{\alpha} + \vec{\beta}i) = (a\vec{\alpha} - b\vec{\beta}) + (a\vec{\beta} + b\vec{\alpha})i$$

Ale platí aj $(\vec{\alpha} + \vec{\beta}i)A = (\vec{\alpha}A) + (\vec{\beta}A)i$, kde vektory $\vec{\alpha}A$, $\vec{\beta}A$ sú reálne vektory, aspoň jeden z nich nie je nulový. Porovnaním reálnych a imaginárnych častí dostaneme

$$\begin{aligned} \vec{\alpha}A &= a\vec{\alpha} - b\vec{\beta} \\ \vec{\beta}A &= a\vec{\beta} + b\vec{\alpha} \end{aligned}$$

Pozrime sa teraz na skalárny súčin $\langle \vec{\alpha}A, \vec{\beta} \rangle$. Jedna z možností, ako počítať tento skalárny súčin je použiť maticové násobenie, presnejšie pre štandardný skalárny súčin platí $\langle \vec{x}, \vec{y} \rangle = \vec{x}\vec{y}^T$. Použitím tohoto vzorca dostaneme

$$\langle \vec{\alpha}A, \vec{\beta} \rangle = \vec{\alpha}A\vec{\beta}^T = \vec{\alpha}A^T\vec{\beta}^T = \vec{\alpha}(\vec{\beta}A)^T = \langle \vec{\alpha}, \vec{\beta}A \rangle$$

Druhá rovnosť je dôsledok symetrie matice A. Ale použitím vzorcov pre $\vec{\alpha}A$ a $\vec{\beta}A$, ktoré sme získali vyššie dostaneme

$$\langle \vec{\alpha}A, \vec{\beta} \rangle = \langle a\vec{\alpha} - b\vec{\beta}, \vec{\beta} \rangle = a\langle \vec{\alpha}, \vec{\beta} \rangle - b\langle \vec{\beta}, \vec{\beta} \rangle$$

a

$$\langle \vec{\alpha}, \vec{\beta}A \rangle = \langle \vec{\alpha}, a\vec{\beta} + b\vec{\alpha} \rangle = a\langle \vec{\alpha}, \vec{\beta} \rangle + b\langle \vec{\alpha}, \vec{\alpha} \rangle$$

čiže $a\langle \vec{\alpha}, \vec{\beta} \rangle - b\langle \vec{\beta}, \vec{\beta} \rangle = a\langle \vec{\alpha}, \vec{\beta} \rangle + b\langle \vec{\alpha}, \vec{\alpha} \rangle$, a teda

$$\begin{aligned} -b\langle \vec{\beta}, \vec{\beta} \rangle &= b\langle \vec{\alpha}, \vec{\alpha} \rangle, \\ b(\langle \vec{\beta}, \vec{\beta} \rangle + \langle \vec{\alpha}, \vec{\alpha} \rangle) &= 0 \end{aligned}$$

Keďže aspoň jeden z vektorov $\vec{\alpha}$, $\vec{\beta}$ je nenulový, platí $\langle \vec{\beta}, \vec{\beta} \rangle + \langle \vec{\alpha}, \vec{\alpha} \rangle > 0$. Preto z poslednej rovnosti vyplýva $b = 0$, a teda vlastné číslo $z = a + 0i$ je reálne číslo. □

Na základe Schurovej vety teda dostávame tvrdenie, ktoré je známe ako „Veta o hlavných osiach“:

Veta 3.2.11 (o hlavných osiach)**.** *Nech $A = ||a_{ij}||$ je štvorcová symetrická matica typu $n \times n$ nad poľom $\mathbb{R}$, potom A je ortogonálne podobná s diagonálnou maticou.*

Pri hľadaní príslušnej ortogonálnej matice prechodu je užitočné vedieť nasledujúci fakt

Veta 3.2.12. *Nech $A = ||a_{ij}||$ je štvorcová symetrická matica typu $n \times n$ nad poľom $\mathbb{R}$, nech $a \neq b$ sú dve vlastné čísla matice A a nech $\vec{\alpha}$ je vlastný vektor prislúchajúci ku vlastnému číslu a, podobne $\vec{\beta}$ je vlastný vektor prislúchajúci ku vlastnému číslu b. Potom $\vec{\alpha} \perp \vec{\beta}$ (t.j. $\vec{\alpha}$ a $\vec{\beta}$ sú na seba kolmé v zmysle štandardného skalárneho súčinu).*

Dôkaz. Jedno z čísiel a, b je nenulové, nech je to a. Vypočítajme hodnotu $a\langle\vec{\alpha},\vec{\beta}\rangle$:

$$a\langle\vec{\alpha},\vec{\beta}\rangle = \langle a\vec{\alpha},\beta\rangle = \langle\vec{\alpha}A,\beta\rangle = \vec{\alpha}A\vec{\beta}^T = \vec{\alpha}A^T\vec{\beta}^T = \vec{\alpha}(\vec{\beta}A)^T = \langle\vec{\alpha},\vec{\beta}A\rangle = \langle\vec{\alpha},b\vec{\beta}\rangle = b\langle\vec{\alpha},\vec{\beta}\rangle$$

čiže $(a-b)\langle\vec{\alpha},\vec{\beta}\rangle = 0$ a pretože $a-b\neq 0$, je skalárny súčin $\langle\vec{\alpha},\vec{\beta}\rangle = 0$, t.j. $\vec{\alpha}\perp\vec{\beta}$. □

Ilustrujme si použitie tejto vety na konkrétnom príklade.

Príklad 3.2.13.

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

Ak existujú, nájdite ortogonálnu maticu P a diagonálnu maticu D tak, aby $D = PAP^T$.

Charakteristický polynóm je $-(x+3)^2(x-6)$, čiže vlastné hodnoty sú -3 a 6.

Riešením sústav s maticami $(A+3I)^T$, resp. $(A-6I)^T$ dostaneme vlastné vektory. Dôležité je vlastné vektory normalizovať, prípadne ak je niektorá vlastné hodnota viacnásobná, tak aj z nich urobiť ortonormálnu bázu. (Aby sme dostali ortogonálnu maticu.) Vďaka predchádzajúcej vete máme automaticky zabezpečené, že vlastné vektory pre rôzne vlastné hodnoty budú na seba kolmé.

Vlastné vektory prislúchajúce k -3 sú $(\frac{1}{\sqrt{2}},-\frac{1}{\sqrt{2}},0)$, $(\frac{1}{3\sqrt{2}},\frac{1}{3\sqrt{2}},\frac{4}{3\sqrt{2}})$. Vlastný vektor prislúchajúci k 6 je $(\frac{2}{3},\frac{2}{3},-\frac{1}{3})$. Keď tieto vektory dáme do stĺpcov dostaneme hľadanú maticu P.

$$\begin{pmatrix} 1 & 4 & -2 \\ 4 & 1 & -2 \\ -2 & -2 & -2 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{3\sqrt{2}} & \frac{2}{3} \\ -\frac{1}{\sqrt{2}} & \frac{1}{3\sqrt{2}} & \frac{2}{3} \\ 0 & \frac{4}{3\sqrt{2}} & -\frac{1}{3} \end{pmatrix} \begin{pmatrix} -3 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & 6 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ \frac{1}{3\sqrt{2}} & \frac{1}{3\sqrt{2}} & \frac{4}{3\sqrt{2}} \\ \frac{2}{3} & \frac{2}{3} & -\frac{1}{3} \end{pmatrix}$$

Veta o hlavných osiach nám poskytuje rozklad symetrickej matice na matice projekcie. Ortogonálna podobnosť matice A s diagonálnou maticou nám totiž hovorí, že existuje ortogonálna matica P taká, že

$$A = P^T DP,$$

pričom vieme, že na diagonále matice D sú vlastné čísla $d_1,\ldots,d_n$ matice A a riadky matice P sú vlastné vektory matice A. Predchádzajúcu rovnosť potom môžeme upraviť na tvar

$$A = \begin{pmatrix}\vec{\alpha}_1^T & \ldots & \vec{\alpha}_n^T\end{pmatrix} \begin{pmatrix} d_1 & 0 & \ldots & 0 \\ 0 & d_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & d_n \end{pmatrix} \begin{pmatrix}\vec{\alpha}_1 \\ \vdots \\ \vec{\alpha}_n\end{pmatrix} = \begin{pmatrix}\vec{\alpha}_1^T & \ldots & \vec{\alpha}_n^T\end{pmatrix} \begin{pmatrix} d_1\vec{\alpha}_1 \\ \vdots \\ d_n\vec{\alpha}_n\end{pmatrix}$$

$$A = d_1\vec{\alpha}_1^T\vec{\alpha}_1 + d_2\vec{\alpha}_2^T\vec{\alpha}_2 + \cdots + d_n\vec{\alpha}_n^T\vec{\alpha}_n \tag{3.5}$$

Predchádzajúci zápis sa niekedy zvykne nazývať *spektrálny rozklad* matice A.

Všimnime si, že maticu A sme rozložili na súčet násobkov ortogonálnych projekcií do smerov vlastných vektorov. (Matica $\vec{\alpha}_i^T\vec{\alpha}_i$ je presne matica ortogonálnej projekcie na podpriestor $[\vec{\alpha}_i]$ – pozri úlohu 1.2.13).

Môžeme si všimnúť, že matice tvaru $A = \vec{\alpha}^T\vec{\alpha}$ majú niektoré pekné vlastnosti. Očividne platí $A^T = A$, čiže takáto matica je symetrická. Vďaka tomu, že matica P je ortogonálna, sú vlastné vektory $\vec{\alpha}_1,\ldots,\vec{\alpha}_n$ ortonormálne. Špeciálne vďaka tomu, že majú veľkosť 1, dostaneme $AA = \vec{\alpha}^T(\vec{\alpha}\vec{\alpha}^T)\vec{\alpha} = \vec{\alpha}^T.1.\vec{\alpha} = \vec{\alpha}^T\vec{\alpha} = A$. Matice (a im zodpovedajúce lineárne zobrazenia), pre ktoré platí $A^2 = A$ sa zvyknú nazývať *projekcie*.

3.2.3 Cayley-Hamiltonova veta

Ak by sme chceli teóriu načatú v tomto texte chceli študovať serióznejšie, potrebovali by sme tzv. Caley-Hamiltonovu vetu, my ju teraz uvedieme len ako malé doplnenie problematiky a možno ako zaujímavosť.

Veta 3.2.14 (Cayley-Hamilton)**.** *Nech A je štvorcová matica nad poľom F. Potom A je koreňom svojho charakteristického polynómu, presnejšie ak je $ch_A(x) = (-1)^n x^n + c_{n-1}x^{n-1} + \cdots + c_0$ tak $(-1)^n A^n + c_{n-1}A^{n-1} + \cdots + c_0 I = \|0\|_{n\times n}$.*

Dôkaz. Vzhľadom na to, že charakteristický polynóm je determinant, je vhodné pripomenúť jednu zaujímavú vlastnosť - v prvom semestri sme ju používali pre výpočet inverznej matice ku regulárnej matici. Teraz ju uvedieme v trochu všeobecnejšej formulácii, ktorú využijeme v dôkaze: majme štvorcovú maticu A typu $n \times n$. Znakom A_{ij} $(1 \leq i, j \leq n)$ označme determinant matice, ktorá z A vznikne vynechaním i-teho riadku a j-teho stĺpca vynásobený číslom $(-1)^{i+j}$ (tzv. algebraický doplnok prvku a_{ij} matice A). Známy vzorec na výpočet inverznej matice ku regulárnej matici A (veta I-6.5.1) hovorí, že

$$A^{-1} = \begin{pmatrix} \frac{A_{11}}{|A|} & \frac{A_{21}}{|A|} & \cdots & \frac{A_{n1}}{|A|} \\ \frac{A_{12}}{|A|} & \frac{A_{22}}{|A|} & \cdots & \frac{A_{n2}}{|A|} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{A_{1n}}{|A|} & \frac{A_{2n}}{|A|} & \cdots & \frac{A_{nn}}{|A|} \end{pmatrix}$$

čo je špeciálny prípad nasledujúceho vzorca:

$$A \cdot \begin{pmatrix} A_{11} & A_{21} & \ldots & A_{n1} \\ A_{12} & A_{22} & \ldots & A_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ A_{1n} & A_{2n} & \ldots & A_{nn} \end{pmatrix} = |A| \cdot \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix} = |A| \cdot I,$$

ktorý platí aj v prípade, že je $|A| = 0$. (A dá sa dokázať podobne ako veta I-6.5.1.)

Matica

$$\begin{pmatrix} A_{11} & A_{21} & \ldots & A_{n1} \\ A_{12} & A_{22} & \ldots & A_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ A_{1n} & A_{2n} & \ldots & A_{nn} \end{pmatrix}$$

sa označuje znakom $\mathrm{adj}(A)$, t.j. platí $A \cdot \mathrm{adj}(A) = |A| \cdot I$.

Naviac je dôležité to, že pojem determinantu môžeme rovnako ako pre matice nad (nejakým) poľom F zaviesť pre matice nad ľubovoľným komutatívnym okruhom a v prípade, že je to okruh s 1, uvedený vzorec bude platiť (i keď možno napr. nemôžeme maticu upraviť na redukovaný trojuholníkový tvar a na základe známych viet o tom (tieto vety ostanú v platnosti aj pre matice nad komutatívnym okruhom), ako sa správa determinant pri elementárnych riadkových operáciách potom počítať determinant - to je vo všeobecnosti výsada matíc nad poliami).

Teraz môžeme pristúpiť ku samotnému dôkazu. Nech $B = A - xI$. Potom B_{ij} ako (až na znamienko) determinant „podmatice“ matice B, ktorá vznikla vynechaním jedného riadku a jedného stĺpca je polynóm stupňa menej ako n, t.j. nanajvýš stupňa $n-1$ v premennej x. T.j. matica $\mathrm{adj}(B)$ je matica s prvkami z $F[x]$, čo je komutatívny okruh s 1.

Vzhľadom na uvedené možné stupne polynómov existujú také matice $C_{n-1}, \dots C_1, C_0$ - všetko matice $n \times n$ nad poľom F (t.j. ich prvky už sú konštanty, nie polynómy), že

$$\mathrm{adj}(A - xI) = \mathrm{adj}(B) = C_{n-1}x^{n-1} + \cdots + C_1 x + C_0$$

Označme si $ch_A(x) = |B| = (-1)^n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$

$|B| \cdot I = (-1)^n I x^n + c_{n-1} \cdot I x^{n-1} + \cdots + c_1 \cdot I x + c_0 I = B \cdot \mathrm{adj}(B) = (A - xI) \cdot (C_{n-1}x^{n-1} + \cdots + C_1 x + C_0)$,

odkiaľ porovnaním „koeficientov“ pri rovnakých mocninách x dostaneme

$$\begin{aligned} c_0 I &= AC_0 \\ c_1 I &= AC_1 - C_0 \\ c_2 I &= AC_2 - C_1 \\ &\dots \\ c_{n-1} I &= AC_{n-1} - C_{n-2} \\ \text{a nakoniec} & \\ (-1)^n I &= -C_{n-1} \end{aligned}$$

Vynásobme zľava teraz postupne prvú rovnicu maticou I, druhú rovnicu maticou A, tretiu rovnicu maticou $A^2, \dots$, a poslednú, t.j. rovnicu s poradovým číslom $n+1$ maticou A^n, dostaneme

$$\begin{aligned} c_0 I &= AC_0 \\ c_1 A &= A^2 C_1 - AC_0 \\ c_2 A^2 &= A^3 C_2 - A^2 C_1 \\ &\dots \\ c_{n-1} A^{n-1} &= A^n C_{n-1} - A^{n-1} C_{n-2} \\ \text{a nakoniec} & \\ (-1)^n A^n &= -A^n C_{n-1} \end{aligned}$$

Po sčítaní ľavých a pravých strán týchto rovníc dostaneme

$$\begin{aligned} (-1)^n A^n + c_{n-1}A^{n-1} + \cdots + c_1 A + c_o I &= \\ -A^n C_{n-1} + (A^n C_{n-1} - A^{n-1} C_{n-2}) + \cdots + (A^3 C_2 - A^2 C_1) + (A^2 C_1 - AC_0) + AC_0 &= \|0\|_{n\times n} \end{aligned}$$

t.j. $ch_A(A) = \|0\|$. □

Cvičenia

Úloha 3.2.1. Nájdite vlastné hodnoty a vlastné vektory daných matíc nad poľom $\mathbb{C}$:
a) $\left(\begin{smallmatrix} 2 & 4 \\ 5 & 3 \end{smallmatrix}\right)$
b) $\left(\begin{smallmatrix} 3 & 1 \\ 1 & 3 \end{smallmatrix}\right)$
c) $\left(\begin{smallmatrix} 1 & 2 \\ 2 & -2 \end{smallmatrix}\right)$
d) $\left(\begin{smallmatrix} -1 & 2i \\ -2i & 2 \end{smallmatrix}\right)$
e) $\left(\begin{smallmatrix} 2 & 1 \\ -1 & 0 \end{smallmatrix}\right)$
f) $\left(\begin{smallmatrix} 4 & 1 \\ 3 & 2 \end{smallmatrix}\right)$
Ak taká matica existuje, nájdite regulárnu maticu P s vlastnosťou, že PAP^{-1} je diagonálna.

Úloha 3.2.2. Ukážte, že vlastné vektory matice A typu $n \times n$ prislúchajúce k danej vlastnej hodnote c spolu s nulovým vektorom tvoria podpriestor priestoru F^n.

Úloha 3.2.3. Ako vyzerá matica A zodpovedajúca otočeniu v rovine okolo počiatku súradnicovej sústavy o nenulový uhol φ? Nájdite jej vlastné hodnoty a vlastné vektory v $\mathbb{C}$? Ako možno geometricky interpretovať fakt, že táto matica nemá reálne vlastné vektory?

Úloha 3.2.4. Ukážte, že pre $c \in \mathbb{R} \setminus \{0\}$ matica $\left(\begin{smallmatrix} 1 & c \\ 0 & 1 \end{smallmatrix}\right)$ nie je podobná s diagonálnou maticou. Aká je geometrická interpretácia tohoto výsledku?

Úloha 3.2.5. Ukážte, že ak k je smernica vlastného vektora matice A typu 2×2, tak k spĺňa kvadratickú rovnicu $a_{21}k^2 + (a_{11} - a_{22})k - a_{12} = 0$.

Úloha 3.2.6. Ak A, B sú regulárne matice, tak AB a BA majú rovnaké vlastné hodnoty.

Úloha 3.2.7. Dokážte: Štvorcová matica A je regulárna práve vtedy, keď 0 nie je vlastné číslo matice A.

Ak A je regulárna, tak c je vlastné číslo matice A práve vtedy, keď c^{-1} je vlastné číslo matice A^{-1}.

Úloha 3.2.8. Ak A je idempotentná matica, čiže $A^2 = A$, tak jej vlastné hodnoty môžu byť jedine 0 alebo 1.

Úloha 3.2.9. Nech A je štvorcová matica. Ukážte, že λ je vlastné číslo matice A práve vtedy, keď $\lambda + a$ je vlastné číslo matice $A + aI$.

Úloha 3.2.10. Nájdite (ak taká matica existuje) maticu P takú, že $PAP^{-1} = D$ je diagonálna matica.

a) $\left(\begin{smallmatrix} -2 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$

b) $\left(\begin{smallmatrix} 1 & 2 & 1 \\ 6 & -1 & 0 \\ -1 & -2 & -1 \end{smallmatrix}\right)$

c) $\left(\begin{smallmatrix} -1 & -1 & 1 \\ 0 & -2 & 1 \\ 0 & 0 & -1 \end{smallmatrix}\right)$

d) $\left(\begin{smallmatrix} 1 & 1 & 0 \\ 0 & 2 & 0 \\ 1 & 0 & 1 \end{smallmatrix}\right)$

Úloha 3.2.11. Nájdite (ak taká matica existuje) ortogonálnu maticu P takú, že $PAP^T = D$ je diagonálna matica.

a) $\left(\begin{smallmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{smallmatrix}\right)$

b) $\left(\begin{smallmatrix} -1 & 0 & 0 \\ 0 & 1 & 5 \\ 0 & 5 & 1 \end{smallmatrix}\right)$

c) $\left(\begin{smallmatrix} -1 & 2 & 0 \\ 2 & -1 & 0 \\ 0 & 0 & 4 \end{smallmatrix}\right)$

d) $\left(\begin{smallmatrix} -2 & 3 & 0 \\ 3 & -2 & 0 \\ 0 & 0 & 7 \end{smallmatrix}\right)$

e) $\left(\begin{smallmatrix} -1 & 2 & 0 & 0 \\ 2 & -1 & 0 & 0 \\ 0 & 0 & -1 & 4 \\ 0 & 0 & 4 & -1 \end{smallmatrix}\right)$

f) $\left(\begin{smallmatrix} -1 & 2 & 0 & 0 \\ 2 & -1 & 0 & 0 \\ 0 & 0 & 2 & 3 \\ 0 & 0 & 3 & 2 \end{smallmatrix}\right)$

g) $\left(\begin{smallmatrix} 3 & 2 & 2 \\ 2 & 4 & 1 \\ 2 & 1 & 4 \end{smallmatrix}\right)$

h) $\left(\begin{smallmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \\ 2 & 2 & -1 \end{smallmatrix}\right)$

i) $\left(\begin{smallmatrix} 2 & 1 & -2 \\ 1 & 2 & -2 \\ -2 & -2 & 5 \end{smallmatrix}\right)$

j) $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & 1 \end{pmatrix}$
k) $\begin{pmatrix} 2 & 1 & 2 \\ 1 & 2 & 2 \\ 2 & 2 & 5 \end{pmatrix}$

Úloha 3.2.12. Sú matice $A = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 2 & \dots & 0 & 0 \\ 0 & 0 & \dots & n-1 & 0 \\ 0 & 0 & \dots & 0 & n \end{pmatrix}$ a $B = \begin{pmatrix} n & 0 & \dots & 0 & 0 \\ 0 & n-1 & \dots & 0 & 0 \\ 0 & 0 & \dots & 2 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}$ podobné? Ak áno, nájdite maticu P takú, že $B = PAP^{-1}$.

Úloha 3.2.13. Pre dané matice vyrátajte charakteristické polynómy $ch_A(x)$, $ch_B(x)$. Vyrátajte aj stopu a determinant týchto matíc a porovnajte ich s príslušnými koeficientami charakteristického polynómu. Sú tieto matice podobné?
$A = \begin{pmatrix} 1 & 4 & -2 \\ 4 & 1 & -2 \\ -2 & -2 & -2 \end{pmatrix}$; $B = \begin{pmatrix} 1 & 5 & -2 \\ 2 & 1 & -4 \\ -2 & -4 & -2 \end{pmatrix}$.

Úloha 3.2.14. Pre dané matice vyrátajte charakteristické polynómy $ch_A(x)$, $ch_B(x)$. Sú dané matice podobné?
$A = \begin{pmatrix} 1 & 4 & -2 \\ 4 & 1 & -2 \\ -2 & -2 & -2 \end{pmatrix}$; $B = \begin{pmatrix} 1 & 4 & -2 \\ 1 & 1 & -8 \\ -2 & -2 & -2 \end{pmatrix}$

Úloha 3.2.15*. Nájdite symetrickú a ortogonálnu maticu P takú, že PAP^{-1} je diagonálna matica ak

$$A = \begin{pmatrix} a^2 & ab & ab & b^2 \\ ab & a^2 & b^2 & ab \\ ab & b^2 & a^2 & ab \\ b^2 & ab & ab & a^2 \end{pmatrix}$$

Úloha 3.2.16*. Nech V je vektorový priestor všetkých matíc typu $n \times n$ nad $\mathbb{R}$, nech $A \in V$ nech $T\colon V \to V$ je definované ako $T(X) = AX$. Nájdite charakteristický polynóm matice zobrazenia T a ukážte, že ak matica A je podobná s diagonálnou maticou, tak aj T je podobná s diagonálnou maticou. (Poznámka: Matica zobrazenia T síce závisí od voľby bázy priestoru V, nie je však ťažké si uvedomiť, že charakteristický polynóm ani diagonalizovateľnosť matice sa nemenia prechodom k inej báze, čiže od voľby bázy nezávisia.)

3.3 Krivky druhého rádu

Ako aplikáciu vety o hlavných osiach si popíšeme ako vyzerajú množiny bodov v rovine popísané polynómom 2 premenných stupňa 2. Z toho, čo si o nich povieme, by snáď mohlo byť zrejmé, prečo sa táto veta nazýva „veta o hlavných osiach“.

3.3.1 Ortogonálne matice 2×2

Najprv sa na chvíľu zastavme pri ortogonálnych maticiach. Keďže chceme skúmať situáciu v $\mathbb{R}^2$, budú nás hlavne zaujímať reálne symetrické matice rozmeru 2×2.

Pripomeňme, že ortogonálna matica je štvorcová matica O, ktorá spĺňa podmienku $OO^T = I$. Táto podmienka znamená, že riadky tejto matice tvoria ortonormálnu bázu v F^n.

Ekvivalentne môžeme definovať ortogonálne matice podmienkou $O^TO = I$, čo znamená, že ortonormálnu bázu tvoria stĺpce. Iná ekvivalentná formulácia je, že transponovaná matica k O je súčasne k tejto matici inverzná, t.j. $O^T = O^{-1}$. Takisto priamo z definície vidno, že ortogonálna matica musí byť regulárna.

Ľahko sa dá ukázať, že ortogonálne matice daného rozmeru tvoria vzhľadom na násobenie matíc grupu (úloha 3.3.1). Všimnime si ešte jednu vlastnosť ortogonálnych matíc. Uvažujme

štandardný skalárny súčin na $\mathbb{R}^n$. Pre ľubovoľné 2 vektory $\vec{\alpha}, \vec{\beta} \in \mathbb{R}^n$ a ortogonálnu maticu O dostaneme

$$\langle \vec{\alpha}O, \vec{\beta}O \rangle = \vec{\alpha}O(\vec{\beta}O)^T = \vec{\alpha}OO^T\vec{\beta}^T = \vec{\alpha}\vec{\beta}^T = \langle \vec{\alpha}, \vec{\beta} \rangle.$$

Zistili sme, že lineárne zobrazenie zodpovedajúce matici O zachováva skalárny súčin. Z toho špeciálne vyplýva, že zachováva veľkosť a uhly vektorov.

Teraz sa pozrime len na matice rozmeru 2×2. Ak reálna matica $O = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ je ortogonálna, jej prvky musia spĺňať

$$\begin{aligned} a^2 + b^2 &= 1 \\ c^2 + d^2 &= 1 \\ ac + bd &= 0 \end{aligned}$$

Ak $a = 0$, dostaneme z prvej rovnice $b = \pm 1$ a z tretej rovnice $d = 0$. Z toho potom vyplýva $c = \pm 1$.

Ak $b = 0$, dostaneme $a = \pm 1$, $c = 0$ a $d = \pm 1$.

Ak $ab \neq 0$ môžeme poslednú rovnicu vydeliť číslom ab a dostaneme $\frac{c}{b} + \frac{d}{a} = 0$, čiže $\frac{c}{b} = -\frac{d}{a}$. Ak označíme $\frac{c}{b} = -\frac{d}{a} =: k$, máme $c = bk$ a $d = -ak$. Po dosadení do druhej rovnice máme

$$(a^2 + b^2)k^2 = 1.$$

Spolu s prvou rovnicou to znamená, že $k^2 = 1$, a teda $k = \pm 1$.

Ľubovoľné riešenie prvej rovnice je tvaru $a = \cos\varphi$, $b = \sin\varphi$. V závislosti od voľby k dostaneme buď $c = \sin\varphi$ a $d = -\cos\varphi$ alebo $c = -\sin\varphi$ a $d = \cos\varphi$. Všimnime si, že tieto riešenia zahŕňajú aj prípad $a = 0$ a $b = 0$, ktoré sme riešili zvlášť (pre $\varphi = 0, \frac{\pi}{2}, \pi, \frac{3}{2}\pi$).

Zistili sme teda, že všetky ortogonálne matice 2×2 sú tvaru

$$\begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix} \qquad \begin{pmatrix} \cos\varphi & \sin\varphi \\ \sin\varphi & -\cos\varphi \end{pmatrix}$$

pre $\varphi \in \langle 0, 2\pi)$.

(Tieto riešenia možno ľahko nájsť aj na základe geometrického významu rovníc, ktoré sme používali. Hľadali sme vlastne vektory (a, b) a (c, d), ktoré sú navzájom kolmé a majú veľkosť 1. Skúste si nakresliť obrázok.)

Prvá z uvedených matíc je presne matica otočenia okolo počiatku súradnicovej sústavy o uhol φ proti smeru pohybu hodinových ručičiek (stačí si všimnúť, že pri tomto lineárnom zobrazení sa vektor $(1, 0)$ zobrazí na $(\cos\varphi, \sin\varphi)$ a vektor $(0, 1)$ na $(-\sin\varphi, \cos\varphi)$).

Z rovnosti

$$\begin{pmatrix} \cos\varphi & \sin\varphi \\ \sin\varphi & -\cos\varphi \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix}$$

vidíme, že ostatné ortogonálne matice zodpovedajú zobrazeniam, ktoré sú zložením osovej súmernosti podľa osi x a otočenia o uhol φ.

Záver: Lineárne zobrazenia zodpovedajúce ortogonálnym maticiam sú práve zobrazenia, ktoré vzniknú zložením osových súmerností (podľa osi prechádzajúcej počiatkom) a otočení (okolo počiatku).

Niečo podobné platí aj vo všeobecnosti – každá reálna ortogonálna matica sa dá napísať ako súčin matice nejakej rotácie okolo počiatku a matice, ktorá zodpovedá lineárnemu zobrazeniu takému, že jednotkové vektory sa pri ňom nejakým spôsobom povymieňajú a niektoré z nich sa zmenia na opačné.

3.3.2 Popis kriviek druhého rádu

Teraz sa už skúsme dostať k otázke, ktorou sme sa chceli zaoberať pôvodne – preskúmať krivky v rovine popísané rovnicami druhého stupňa. Presnejšie, ak

$$f(x_1, x_2) = a_{11}x_1^2 + 2a_{12}x_1x_2 + a_{22}x_2^2 + 2a_1x_1 + 2a_2x_2 + d, \tag{3.6}$$

kde aspoň jedno z čísel a_{11}, a_{12}, a_{22} je nenulové (t.j. člen druhého stupňa v tejto funkcii je nenulový), tak nás zaujíma ako vyzerá množina bodov

$$K = \{(x_1, x_2) \in \mathbb{R}^2; f(x_1, x_2) = 0\}.$$

Ako sa dá uhádnuť z označenia použitého v (3.6), tento problém bude nejako súvisieť s kvadratickými formami.

Ako sa dá uhádnuť z označenia použitého v (3.6), tento problém bude nejako súvisieť s kvadratickými formami. Ak si všímame len kvadratickú časť predpisu $f(x_1, x_2)$, vidíme, že ide o kvadratickú formu

$$g(x_1, x_2) = a_{11}x_1^2 + 2a_{12}x_1x_2 + a_{22}x_2^2.$$

Matica tejto kvadratickej formy $A = \left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{smallmatrix}\right)$ je symetrická. Podľa vety o hlavných osiach 3.2.11 teda existuje ortogonálna matica P tak, že $PAP^T = \mathrm{diag}(\lambda_1, \lambda_2)$, kde $\lambda_{1,2}$ sú vlastné čísla matice A. Bez ujmy na všeobecnosti môžeme predpokladať, že P je maticou otočenia okolo počiatku súradnicovej sústavy. (Ak by to nebola matica otočenia, stačí výraz PAP^T zľava aj sprava vynásobiť maticou $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.)

Matica P zodpovedá zmene premenných, ktorá je lineárna, teda v nových súradniciach bude rovnica našej krivky vyzerať

$$f(y_1, y_2) = \lambda_1 y_1^2 + \lambda_2 y_2^2 + 2b_1y_1 + 2b_2y_2 + d' = 0.$$

Uvažujme najprv prípad, že $\lambda_1\lambda_2 \neq 0$. Potom môžeme túto rovnicu ďalej upraviť doplnením na štvorec. Zavedieme nové premenné $z_1 = y_1 + \frac{b_1}{\lambda_1}$, $z_2 = y_2 + \frac{b_2}{\lambda_2}$. Dostaneme

$$f(z_1, z_2) = \lambda_1 z_1^2 + \lambda_2 z_2^2 + d'' = 0.$$

Geometricky zmena premenných, ktorú sme urobili, zodpovedá posunutiu o vektor $(-\frac{b_1}{\lambda_1}, -\frac{b_2}{\lambda_2})$.

V závislosti od znamienka koeficientov vystupujúcich v tejto rovnici už z nej vieme vyčítať tvar krivky. V prípade, že $\lambda_1, \lambda_2 > 0$ a $d'' < 0$, ako aj v prípade $\lambda_1, \lambda_2 < 0$ a $d'' > 0$ ide o *elipsu.*

Ak $\lambda_1, \lambda_2 > 0$ a $d'' > 0$ alebo $\lambda_1, \lambda_2 < 0$ a $d'' < 0$, tak uvedené rovnica nemá riešenie.

V prípade, že λ_1 a λ_2 majú rôzne znamienka a $d'' \neq 0$, je to *hyperbola.*

Ak $d'' = 0$ tak ide buď o *jednobodovú množinu* (ak λ_1 a λ_2 majú rovnaké znamienko) alebo o *dvojicu pretínajúcich sa priamok* (ak majú rôzne znamienka).

Zostáva nám vyriešiť prípad, keď niektoré vlastné číslo je nulové. Nech napríklad $\lambda_1 = 0$. V tomto prípade môžeme doplnenie na štvorec použiť len v druhej premennej a dostaneme

$$\lambda_2 z_2^2 + 2b_1z_1 + d'' = 0.$$

Ak $b_1 \neq 0$, je to *parabola.* Ak $b_1 = 0$, tak v závislosti od znamienka d'' to môže byť prázdna množina (rovnaké znamienko ako λ_2), *priamka* (ak $d'' = 0$) alebo *dvojica rovnobežných priamok.*

Zistili sme teda, že – s výnimkou degenerovaných prípadov – každá krivka vyjadrená rovnicou druhého stupňa bude vhodne posunutá a otočená elipsa, hyperbola alebo parabola. Vlastné hodnoty matice A nám udávajú hlavnú a vedľajšiu poloos týchto kužeľosečiek.

3.3.3 Invarianty kriviek druhého rádu

V tejto časti si ukážeme, ako možno zistiť typ krivky druhého rádu bez toho, aby sme ju museli upravovať na kanonický tvar.

Definícia 3.3.1. *Invariantom* krivky druhého rádu

$$a_{11}x_1^2 + 2a_{12}x_1x_2 + a_{22}x_2^2 + 2a_1x_1 + 2a_2x_2 + d = 0$$

rozumieme taký algebraický výraz závisiaci od a_{11}, a_{12}, a_{22}, a_1, a_2 a d, ktorý sa nezmení, ak túto krivku vyjadríme v iných súradniciach, ktoré dostaneme posunutím a otočením.

Tvrdenie 3.3.2. *Výrazy* $s = \mathrm{Tr}(A) = a_{11} + a_{22}$, $\delta = |A| = \begin{vmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{vmatrix}$ *a* $\Delta = \begin{vmatrix} a_{11} & a_{12} & a_1 \\ a_{12} & a_{22} & a_2 \\ a_1 & a_2 & d \end{vmatrix}$

sú invariantmi krivky druhého rádu

$$a_{11}x_1^2 + 2a_{12}x_1x_2 + a_{22}x_2^2 + 2a_1x_1 + 2a_2x_2 + d = 0$$

Dôkaz. Overme najprv, že tieto výrazy sa nezmenia pri posunutí. Položme $x_1 = y_1 + d_1$ a $x_2 = y_2 + d_2$. Dostaneme

$$\begin{aligned} &a_{11}x_1^2 + 2a_{12}x_1x_2 + a_{22}x_2^2 + 2a_1x_1 + 2a_2x_2 + d = \\ &a_{11}y_1^2 + 2a_{12}y_1y_2 + a_{22}y_2^2 + 2(a_1 + a_{11}d_1 + a_{12}d_2)y_1 + 2(a_2 + a_{22}d_2 + a_{12}d_1)y_2 + a_{11}d_1^2 + \\ &\qquad 2a_{12}d_1d_2 + a_{22}d_2^2 + 2a_1d_1 + 2a_2d_2 + d. \end{aligned}$$

Pre vyjadrenie krivky v nových súradniciach máme $s = a_{11} + a_{22}$, $\delta = |A| = \begin{vmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{vmatrix}$ a

$$\Delta = \begin{vmatrix} a_{11} & a_{12} & a_1 + a_{11}d_1 + a_{12}d_2 \\ a_{12} & a_{22} & a_2 + a_{22}d_2 + a_{12}d_1 \\ a_1 + a_{11}d_1 + a_{12}d_2 & a_2 + a_{22}d_2 + a_{12}d_1 & a_{11}d_1^2 + 2a_{12}d_1d_2 + a_{22}d_2^2 + 2a_1d_1 + 2a_2d_2 + d \end{vmatrix}$$

Stačí si všimnúť, že maticu v determinante Δ môžeme dostať ako

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ d_1 & d_2 & 1 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & a_1 \\ a_{12} & a_{22} & a_2 \\ a_1 & a_2 & d \end{pmatrix} \begin{pmatrix} 1 & 0 & d_1 \\ 0 & 1 & d_2 \\ 0 & 0 & 1 \end{pmatrix}.$$

(Pri hľadaní matíc, ktorými musíme prenásobiť pôvodnú maticu, je môže pomôcť všimnúť si, aké riadkové a stĺpcové operácie sa dajú použiť.) Keďže sme pôvodnú maticu násobili maticami s determinantom 1, determinant sa tým nezmení.

Teraz skúsme to isté overiť pre otočenie o uhol φ, čiže $x_1 = y_1\cos\varphi + y_2\sin\varphi$ a $x_2 = -y_1\sin\varphi + y_2\cos\varphi$. Dostaneme

$$\begin{aligned} &a_{11}x_1^2 + 2a_{12}x_1x_2 + a_{22}x_2^2 + 2a_1x_1 + 2a_2x_2 + d = \\ &(a_{11}\cos^2\varphi - 2a_{12}\cos\varphi\sin\varphi + a_{22}\sin^2\varphi)y_1^2 + 2(a_{11}\cos\varphi\sin\varphi + a_{12}(\cos^2\varphi - \sin^2\varphi) - a_{22}\cos\varphi\sin\varphi)y_1y_2 + \\ &(a_{11}\sin^2\varphi - 2a_{12}\sin^2\varphi + a_{22}\cos^2\varphi)y_2^2 + 2(a_1\cos\varphi - a_2\sin\varphi)y_1 + 2(a_1\sin\varphi + a_2\cos\varphi) + d \end{aligned}$$

Potom dostaneme
$s = \mathrm{Tr}(A) = (a_{11}\cos^2\varphi - 2a_{12}\cos\varphi\sin\varphi + a_{22}\sin^2\varphi) + (a_{11}\sin^2\varphi - 2a_{12}\sin^2\varphi + a_{22}\cos^2\varphi) =$
$a_{11}(\cos^2\varphi + \sin^2\varphi) + a_{22}(\cos^2\varphi + \sin^2\varphi) = a_{11} + a_{22}$.

$$\delta = \begin{vmatrix} a_{11}\cos^2\varphi - 2a_{12}\cos\varphi\sin\varphi + a_{22}\sin^2\varphi & a_{11}\cos\varphi\sin\varphi + a_{12}(\cos^2\varphi - \sin^2\varphi) - a_{22}\cos\varphi\sin\varphi \\ a_{11}\cos\varphi\sin\varphi + a_{12}(\cos^2\varphi - \sin^2\varphi) - a_{22}\cos\varphi\sin\varphi & a_{11}\sin^2\varphi + 2a_{12}\cos\varphi\sin\varphi + a_{22}\cos^2\varphi \end{vmatrix}$$

a súčasne

$$\begin{pmatrix} a_{11}\cos^2\varphi - 2a_{12}\cos\varphi\sin\varphi + a_{22}\sin^2\varphi & a_{11}\cos\varphi\sin\varphi + a_{12}(\cos^2\varphi - \sin^2\varphi) - a_{22}\cos\varphi\sin\varphi \\ a_{11}\cos\varphi\sin\varphi + a_{12}(\cos^2\varphi - \sin^2\varphi) - a_{22}\cos\varphi\sin\varphi & a_{11}\sin^2\varphi + 2a_{12}\cos\varphi\sin\varphi + a_{22}\cos^2\varphi \end{pmatrix} =$$
$$\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{pmatrix} \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix}$$

Keďže sme pôvodnú maticu vynásobili ortogonálnou maticou (a tá má determinant rovný 1), determinant sa nezmení.

Podobne dostaneme

$$\begin{pmatrix} a'_{11} & a'_{12} & a_1\cos\varphi - a_2\sin\varphi \\ a'_{21} & a'_{22} & a_1\sin\varphi + a_2\cos\varphi \\ a_1\cos\varphi - a_2\sin\varphi & a_1\sin\varphi + a_2\cos\varphi & d \end{pmatrix} =$$
$$\begin{pmatrix} \cos\varphi & -\sin\varphi & 0 \\ \sin\varphi & \cos\varphi & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & a_1 \\ a_{12} & a_{22} & a_2 \\ a_1 & a_2 & d \end{pmatrix} \begin{pmatrix} \cos\varphi & \sin\varphi & 0 \\ -\sin\varphi & \cos\varphi & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Ani v tomto prípade sa determinant nezmení. □

V predchádzajúcej časti sme rozanalyzovali akú krivku dostaneme na základe znamienok $\lambda_{1,2}$ a d''. Na určenie týchto znamienok nám však budú stačiť aj spomínané invarianty.

Ukázali sme, že rovnicu krivky druhého rádu môžeme upraviť na tvar $\lambda_1 z_1^2 + \lambda_2 z_2^2 + d'' = 0$ (v prípade, že obe vlastné hodnoty sú nenulové). V tomto prípade platí $s = \lambda_1 + \lambda_2$, $\delta = \lambda_1\lambda_2$, $\Delta = \lambda_1\lambda_2 d''$.

V prípade, že $\lambda_1 = 0$ sa rovnica danej krivky dala upraviť na tvar $\lambda_2 z_2^2 + 2b_1 z_1 + d'' = 0$. Hodnoty invariantov sú $s = \lambda_2$, $\delta = 0$ a $\Delta = -b_1^2\lambda_2$.

Uvažujme najprv prípad $\delta \neq 0$, ktorý zodpovedá tomu, že obe vlastné hodnoty sú nenulové. Ak $\delta > 0$ znamená to, že vlastné hodnoty majú rovnaké znamienka, ak $\delta < 0$ tak majú opačné znamienka.

Ak majú vlastné hodnoty rovnaké znamienka, tak dostávame buď prázdnu množinu – ak aj d'' má rovnaké znamienko ako vlastné hodnoty – alebo elipsu, ak má opačné znamienko.

Ak $\Delta = 0$, znamená to, že $d'' = 0$, čiže ide o jednobodovú množinu.

Nech teraz $\delta < 0$, čiže vlastné hodnoty majú rôzne znamienka. Pre $d'' \neq 0$ (čiže $\Delta \neq 0$) dostaneme hyperbolu. Ak je d'' nulové, je to dvojica pretínajúcich sa priamok.

Zostáva nám prípad, že niektorá z vlastných hodnôt je nulová, podobne ako doteraz budeme predpokladať, že je to λ_1. Potom ak b_1 je nenulové, ide o parabolu. To zodpovedá tomu, že $\Delta \neq 0$. V opačnom prípade ide o dvojicu rovnobežných priamok, jedinú priamku alebo prázdnu množinu (v závislosti od toho, či λ_2 a d'' majú rovnaké znamienka).

$\delta > 0$	$\Delta \neq 0$	elipsa alebo prázdna množina
$\delta > 0$	$\Delta = 0$	jediný bod
$\delta < 0$	$\Delta \neq 0$	hyperbola
$\delta < 0$	$\Delta = 0$	pretínajúce sa priamky
$\delta = 0$	$\Delta \neq 0$	parabola
$\delta = 0$	$\Delta = 0$	rovnobežné priamky alebo $\emptyset$

3.3.4 Kužeľosečky

Krivky, ktoré takýmto spôsobom dostaneme sa zvyknú nazývať kužeľosečky. Vieme ich totiž dostať ako prienik kužeľa s vhodnou rovinou. (Dvojicu rovnobežných priamok vieme dostať

ako prienik valca s vhodnou rovinou.) Na prvý pohľad vidno, že ak vezmeme kužeľ $z^2 = x^2+y^2$ a rovinu $ax+by+cz = d$, a ak napríklad koeficient c je nenulový, tak môžeme z druhej rovnice vyjadriť $z = \frac{d-ax-by}{c}$ a dosadiť do prvej, očividne tak dostaneme rovnicu druhého stupňa.

Pokúsme sa vyjadriť kužeľosečku v súradniciach určených danou rovinou. Naša rovina nech je daná rovnicou

$$(x_1, x_2, x_3) = (b_1, b_2, b_3) + t(u_1, u_2, u_3) + s(v_1, v_2, v_3).$$

Vhodné bude predpokladať, že vektory $\vec{u} = (u_1, u_2, u_3)$ a $\vec{v} = (v_1, v_2, v_3)$ sú na seba kolmé. (Takto vyjadríme hľadanú krivku v pravouhlej súradnicovej sústave.) Vyrátajme jej priesečník s kužeľom $x_3^2 = x_1^2 + x_2^2$. Po dosadení za x_1, x_2 a x_3 do rovnice kužeľa dostaneme

$$(b_3 + tu_3 + sv_3)^2 - (b_1 + tu_1 + sv_1)^2 - (b_2 + tu_2 + sv_2)^2 = 0$$

a po úprave

$$\begin{aligned}(u_3^2 - u_1^2 - u_2^2)t^2 + 2(u_3v_3 - u_1v_1 - u_2v_2)st + (v_3^2 - v_1^2 - v_2^2)s^2 + \\ 2(b_3u_3 - b_1u_1 - b_2u_2)t + 2(b_3v_3 - b_1v_1 - b_2v_2)s + (b_3^2 - b_1^2 - b_1^2) = 0\end{aligned}$$

Ak s a t chápeme ako súradnice, vidíme, že ide skutočne o krivku druhého stupňa. Pokúsme sa vyrátať aspoň δ – tento invariant určuje typ krivky.

$$\begin{aligned}\begin{vmatrix} u_3^2-u_1^2-u_2^2 & u_3v_3-u_1v_1-u_2v_2 \\ u_3v_3-u_1v_1-u_2v_2 & v_3^2-v_1^2-v_2^2 \end{vmatrix} &= (u_3^2 - u_1^2 - u_2^2)(v_3^2 - v_1^2 - v_2^2) - (u_3v_3 - u_1v_1 - u_2v_2)^2 = \\ &= u_1^2v_1^2 + u_2^2v_2^2 + u_3^2v_3^2 + u_1^2v_2^2 + u_2^2v_1^2 - u_1^2v_3^2 - u_3^2v_1^2 - u_2^2v_3^2 - u_3^2v_2^2 \\ &\quad - u_1^2v_1^2 - u_2^2v_2^2 - u_3^2v_3^2 - 2u_1u_2v_1v_2 + 2u_1u_3v_1v_3 + 2u_2u_3v_2v_3 = \\ &= u_1^2v_2^2 + u_2^2v_1^2 - 2u_1u_2v_1v_2 - u_1^2v_3^2 - u_3^2v_1^2 + 2u_1u_3v_1v_3 - u_2^2v_3^2 - u_3^2v_2^2 + 2u_2u_3v_2v_3 = \\ &= (u_1v_2 - u_2v_1)^2 - (u_1v_3 - u_3v_1)^2 - (u_2v_3 - u_3v_2)^2\end{aligned}$$

Ak smerové vektory roviny sú (u_1, u_2, u_3) a (v_1, v_2, v_3), tak jej normálový vektor je

$$(n_1, n_2, n_3) = (u_1, u_2, u_3) \times (v_1, v_2, v_3) = (u_2v_3 - u_3v_2, u_3v_1 - u_1v_3, u_1v_2 - u_2v_1).$$

Dostali sme teda

$$\delta = n_3^2 - n_1^2 - n_2^2.$$

Elipsu dostaneme v prípade, že $\delta > 0$, čo zodpovedá tomu, že normálový vektor smeruje do vnútra uvažovaného kužeľa. Aby sme dostali parabolu, musí platiť $\delta = 0$, t.j. normálový vektor patrí uvažovanému kužeľu. Vzhľadom k tomu, že sme zobrali kužeľ s rovnicou $x_3^2 = x_1^2 + x_2^2$, je to ekvivalentné s tým, že rovina je rovnobežná s niektorou priamkou ležiacou na povrchu kužeľa. Zostávajúci prípad $\delta < 0$ zodpovedá tomu, že normálový vektor smeruje mimo daný kužeľ.

Pokúsme sa pozrieť na to, či by sme niečo podobné dostali aj keby sme rátali s ľubovoľným kužeľom. Kužeľ, ktorý má os orientovanú v smere vektora $(0, 0, 1)$ a vrchol v počiatku súradnicovej sústavy bude mať rovnicu $x_1^2 + x_2^2 - ax_3^2 = 0$, kde $a > 0$ je nejaká kladná konštanta. Túto rovnicu môžeme prepísať v tvare $\vec{x}K\vec{x}^T = 0$ pre

$$K = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -a \end{pmatrix}.$$

Táto matica je diagonálna, čo znamená, že je symetrická a tiež, že ľahko vieme vyrátať inverznú maticu $K^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -\frac{1}{a} \end{pmatrix}$.

Zapíšme rovnicu roviny ako $\vec{x} = \vec{x}_0 + \vec{u}s + \vec{v}t$, pričom predpokladáme, že $\vec{u}$, $\vec{v}$ majú jednotkovú veľkosť a sú na seba kolmé. Po dosadení do rovnice $\vec{x}K\vec{x}^T = 0$ dostaneme $\vec{u}K\vec{u}^T s^2 + (\vec{u}K\vec{v}^T + \vec{v}K\vec{u})^T st + \vec{v}K\vec{v}^T t^2 + \cdots = 0$. (Chceme vyrátať δ, čiže nás zaujímajú len členy, ktoré sú stupňa 2.) Máme teda

$$\delta = \begin{vmatrix} \vec{u}K\vec{u}^T & \vec{u}K\vec{v}^T \\ \vec{v}K\vec{u}^T & \vec{v}K\vec{v}^T \end{vmatrix}.$$

Všimnime si, že $\vec{u}K\vec{v}^T = u_1v_1 + u_2v_2 - au_3v_3 = \vec{v}K\vec{u}^T$ (alebo tiež $\vec{u}K\vec{v}^T = (\vec{u}K\vec{v}^T)^T = \vec{v}K^T\vec{u}^T = \vec{v}K\vec{u}^T$), teda uvedená matica je skutočne symetrická a môžeme použiť to, čo sme odvodili v predošlej časti. (Používame tu výsledky, ktoré platia pre symetrické matice.)

Na vyjadrenie tohoto determinantu nám pomôže, keď si všimneme

$$\begin{pmatrix} \vec{u} \\ \vec{v} \\ \vec{n}K^{-1} \end{pmatrix} K \begin{pmatrix} \vec{u}^T & \vec{v}^T & K^{-1}\vec{n}^T \end{pmatrix} = \begin{pmatrix} \vec{u}K\vec{u}^T & \vec{u}K\vec{v}^T & 0 \\ \vec{v}K\vec{u}^T & \vec{v}K\vec{v}^T & 0 \\ 0 & 0 & \vec{n}K^{-1}\vec{n}^T \end{pmatrix},$$

kde $\vec{n} = \vec{u} \times \vec{v}$ je vektorový súčin vektorov $\vec{u}$ a $\vec{v}$, čiže je to normálový vektor danej roviny.

Ak na obe strany rovnosti použijeme determinant, tak máme:

$$\begin{vmatrix} \vec{u} \\ \vec{v} \\ \vec{n}K^{-1} \end{vmatrix}^2 |K| = \delta \cdot \vec{n}K^{-1}\vec{n}^T$$

Súčasne si môžeme všimnúť, že $\vec{n}K^{-1}\vec{n}^T = n_1^2 + n_2^2 - \frac{1}{a}n_3^2$, $|K| = -a$ a

$$\begin{vmatrix} \vec{u} \\ \vec{v} \\ \vec{n}K^{-1} \end{vmatrix} = \begin{vmatrix} u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \\ n_1 & n_2 & -\frac{n_3}{a} \end{vmatrix} = n_1^2 + n_2^2 - \frac{1}{a}n_3^2,$$

z čoho už dostaneme

$$\delta = -a\left(n_1^2 + n_2^2 - \frac{1}{a}n_3^2\right),$$

čiže znamienko δ je rovnaké ako znamienko výrazu $n_1^2 + n_2^2 - \frac{1}{a}n_3^2$, ktorý určuje, akú polohu má daná rovina vzhľadom ku kužeľu.

3.3.5 Maximálna a minimálna vlastná hodnota

Ešte sa pozrime na geometrický význam, ktorý má najväčšia a najmenšia vlastná hodnota v prípade, že ide o elipsu. Uvažujme rovnicu už upravenú na diagonálny tvar

$$\lambda_1 x_1^2 + \lambda_2 x_2^2 = d.$$

Nech napríklad $\lambda_1 \geq \lambda_2$. Pre jednoduchosť predpokladajme, že obe vlastné hodnoty sú kladné. (V opačnom prípade by sme ich v predchádzajúcej rovnici nahradili ich absolútnymi hodnotami.)

Skúsme hľadať bod na elipse s najväčšou možnou vzdialenosťou od jej stredu. Máme

$$d = \lambda_1 x_1^2 + \lambda_2 x_2^2 \geq \lambda_2(x_1^2 + x_2^2)$$
$$x_1^2 + x_2^2 \leq \frac{d}{\lambda_2}$$

Vidíme teda, že najväčšia možná hodnota, akú môže výraz $x_1^2 + x_2^2$ nadobúdať, je $\frac{d}{\lambda_2}$. Táto hodnota sa skutočne aj nadobúda pre $x_1 = 0$. Keďže táto rovnica je už v nových súradniciach, znamená to, že bod z najväčšou vzdialenosťou od stredu leží v smere vlastného vektora prislúchajúceho k λ_2.

Všeobecne – vlastná hodnota s najmenšou absolútnou hodnotou a jej vlastný vektor nám určujú najvzdialenejší bod elipsy od stredu, podobne ak vezmeme v absolútnej hodnote najväčšiu vlastnú hodnotu a jej vlastný vektor, nádjeme tak najbližší bod. Vlastné vektory a vlastné čísla nám teda udávajú *hlavné osi* tejto elipsy.

Maximum z absolútnych hodnôt vlastných hodnôt matice A sa zvykne nazývať *spektrálny polomer* matice A. Je dôležitý napríklad z toho dôvodu, že – ako sme už spomínali – na zistenie či nejaký mocninový rad obsahujúci matice konverguje je potrebné zistiť, či všetky vlastné hodnoty sú menšie ako polomer konvergencie. Samozrejme, na to nám stačí skúmať najväčšiu vlastnú hodnotu.

Cvičenia

Úloha 3.3.1. Dokážte, že ortogonálne matice typu $n \times n$ tvoria s operáciou násobenia matíc grupu.

3.4 Jordanov normálny tvar

Keď sme sa zaoberali kvadratickými formami a kongruenciou matíc, podarilo sa nám ukázať, že každú maticu (kvadratickú formu) možno upraviť na diagonálny tvar. Tento diagonálny tvar bol teda spoločným reprezentantom celej triedy kongruentných matíc.

Podobne aj pri podobnosti matíc sa dá z každej triedy vybrať „pekný“ reprezentant. Ako sme však videli v predchádzajúcej kapitole, nie každá matica je podobná s diagonálnou. Preto v tomto prípade matice reprezentujúce jednotlivé triedy vyzerajú o čosi komplikovanejšie. Ukážeme si jednu z možností výberu takéhoto reprezentanta, ktorá sa nazýva Jordanov normálny tvar matice.

Vetu o Jordanovom normálnom tvare uvedieme bez dôkazu. Jeden možný dôkaz, ktorý využíva teóriu modulov (=isté zovšeobecnenie pojmu vektorového priestoru), sa môžete dozvedieť na predmete Vybrané kapitoly z algebry [G3]. Dôkaz toho tvrdenia môžete nájsť aj v [Z, Kapitola 20]. Iný dôkaz založený na teórii matíc (využíva okrem iného aj komplexnú verziu Schurrovej vety) možno nájsť v [HJ, Theorem 3.1.11].

Definícia 3.4.1. *Jordanov blok* veľkosti k prislúchajúci číslu λ je matica typu $k \times k$ tvaru

$$J_k(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \dots & \dots & 0 \\ 0 & \lambda & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & \lambda & 1 & 0 \\ 0 & \dots & \dots & 0 & \lambda & 1 \\ 0 & \dots & \dots & \dots & 0 & \lambda \end{pmatrix}$$

Veta 3.4.2 (Jordanov normálny tvar)**.** *Pre každú maticu A nad $\mathbb{C}$ existuje blokovo diagonálna matica J, ktorej diagonálne bloky sú Jordanove bloky taká, že A je podobná s maticou J.*

$$A \sim \begin{pmatrix} J_{k_1}(\lambda_1) & 0 & \dots & \dots & 0 \\ 0 & J_{k_2}(\lambda_2) & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & J_{k_j}(\lambda_{j-1}) & 0 \\ 0 & \dots & \dots & 0 & J_{k_j}(\lambda_j) \end{pmatrix}$$

Matica J sa nazýva Jordanov normálny tvar *matice A.*

Navyše platí, že matica J je jednoznačne určená až na poradie Jordanových blokov na diagonále.

Ďalej platí, že dve matice A a B sú podobné práve vtedy, keď majú rovnaký Jordanov tvar (až na poradie Jordanových blokov).

Hodnoty $\lambda_1, \ldots, \lambda_k$ vystupujúce v predchádzajúcej vete sú vlastné hodnoty matice A. V prípade, že je matica A diagonalizovateľná, všetky Jordanove bloky v jej Jordanovom normálnom tvare majú veľkosť 1.

Vieme, že podobné matice majú rovnakú stopu i determinant. Keďže stopu a determinant matice v Jordanovom normálnom tvare možno vypočítať veľmi jednoducho, vidíme, že stopa matice je presne súčet jej vlastných hodnôt (vrátane násobnosti[3]) a determinant matice dostaneme ako súčin jej vlastných hodnôt (vrátane násobnosti). To isté sme už vlastne odvodili v dôkaze dôsledku 3.2.7 a poznámke za ním.

Keď už poznáme kanonický tvar z vety 3.4.2, na spôsob, ako ho nájsť, môžeme prísť veľmi podobne ako pri hľadaní diagonálnej matice podobnej s danou maticou.

Pre jednoduchosť sa pozrime najprv na to, čo znamená, že daná matica je podobná s Jordanovým blokom, t.j. existuje taká regulárna matica P, že platí $PAP^{-1} = J_n(\lambda)$. Predchádzajúcu rovnosť môžeme prepísať ako

$$PA = J_n(\lambda)P$$

Označme riadky matice A ako $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ a prečítajme si tú istú maticovú rovnosť po riadkoch.

$$\begin{pmatrix} \vec{\alpha}_1 \\ \vec{\alpha}_2 \\ \vdots \\ \vec{\alpha}_{n-1} \\ \vec{\alpha}_n \end{pmatrix} A = \begin{pmatrix} \lambda & 1 & 0 & \ldots & 0 \\ 0 & \lambda & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & \lambda & 1 \\ 0 & \ldots & \ldots & 0 & \lambda \end{pmatrix} \begin{pmatrix} \vec{\alpha}_1 \\ \vec{\alpha}_2 \\ \vdots \\ \vec{\alpha}_{n-1} \\ \vec{\alpha}_n \end{pmatrix} \tag{3.7}$$

$$\begin{pmatrix} \vec{\alpha}_1 A \\ \vec{\alpha}_2 A \\ \vdots \\ \vec{\alpha}_{n-1} A \\ \vec{\alpha}_n A \end{pmatrix} = \begin{pmatrix} \lambda\vec{\alpha}_1 + \alpha_2 \\ \lambda\vec{\alpha}_2 + \alpha_3 \\ \vdots \\ \lambda\vec{\alpha}_{n-1} + \alpha_n \\ \lambda\vec{\alpha}_n \end{pmatrix} \tag{3.8}$$

Porovnaním týchto matíc vidíme, že musí platiť

$$\vec{\alpha}_n A = \lambda\vec{\alpha}_n.$$

To znamená, že λ je vlastná hodnota matice A a $\vec{\alpha}_n$ je vlastný vektor, ktorý k nej prislúcha. Vlastné hodnoty a vlastné vektory už vieme hľadať – nájdeme korene charakteristického polynómu $|A - xI|$ a pre ne potom riešime homogénnu sústavu určenú maticou $(A - \lambda I)^T$.

Predchádzajúci vektor má spĺňať rovnosť

$$\vec{\alpha}_{n-1} A = \lambda\vec{\alpha}_{n-1} + \alpha_n$$

alebo, ekvivalentne,

$$\vec{\alpha}_{n-1}(A - \lambda I) = \vec{\alpha}_n.$$

Vektor $\vec{\alpha}_{n-1}$ teda môžeme nájsť riešením nehomogénnej sústavy rovníc

$$(A - \lambda I)^T \vec{\alpha}_{n-1}^T = \vec{\alpha}_n^T.$$

[3]Rozumieme tým násobnosť vlastnej hodnoty ako koreňa charakteristického polynómu.

Podobne postupujeme ďalej – v každom kroku nájdeme nový vektor riešením sústavy

$$(A-\lambda I)^T\vec{\alpha}_{j-1}^T=\vec{\alpha}_j^T.$$

Ak nájdeme vektory spĺňajúce uvedené rovnosti, tak matica P skutočne spĺňa rovnosti (3.8) a $PAP^{-1}=J_n(\lambda)$. Navyše, ukázali sme, že aby pre maticu P tieto rovnosti platili, jej riadky musia spĺňať všetky uvedené podmienky.

Na ten istý problém sa môžeme pozrieť ešte aj iným spôsobom. Vieme, že podobnosť matíc znamená, že obe matice predstavujú pri rôznych bázach to isté zobrazenie. Čiže hľadáme bázu $\vec{\alpha}_1,\dots,\vec{\alpha}_n$, pri ktorej má zobrazenie určené (pri štandardnej báze) maticou A maticu $J_\lambda(n)$. To znamená špeciálne, že má platiť

$$\begin{aligned}\vec{\alpha}_nA&=\lambda\vec{\alpha}_n\\ \vec{\alpha}_{n-1}A&=\lambda\vec{\alpha}_{n-1}+\vec{\alpha}_n\\ &\vdots\\ \vec{\alpha}_1&=\lambda\vec{\alpha}_1+\vec{\alpha}_2\end{aligned}$$

Dostali sme teda presne tie isté rovnice pre $\vec{\alpha}_1,\dots,\vec{\alpha}_n$.

Vo všeobecnosti môžeme mať Jordanových blokov viac, nie iba jeden ako v predchádzajúcej úvahe. Ukážme si na konkrétnom príklade, ako môžeme potom nájsť Jordanov normálny tvar danej matice.

Príklad 3.4.3. Nájdime Jordanov normálny tvar pre maticu

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

Najprv chceme nájsť vlastné hodnoty. Vypočítajme charakteristický polynóm.

$$ch_A(x)=\begin{vmatrix}6-x&1&-3&2&5\\-1&2-x&1&-3&0\\1&0&1-x&3&0\\-1&0&1&3-x&-2\\-2&0&2&2&-2-x\end{vmatrix}\overset{(1)}{=}\begin{vmatrix}6-x&1&-3&2&5\\0&2-x&2-x&0&0\\1&0&1-x&3&0\\-1&0&1&3-x&-2\\-2&0&2&2&-2-x\end{vmatrix}=(2-x)\begin{vmatrix}6-x&1&-3&2&5\\0&1&1&0&0\\1&0&1-x&3&0\\-1&0&1&3-x&-2\\-2&0&2&2&-2-x\end{vmatrix}=$$

$$=(2-x)\begin{vmatrix}6-x&0&-4&2&5\\0&1&1&0&0\\1&0&1-x&3&0\\-1&0&1&3-x&-2\\-2&0&2&2&-2-x\end{vmatrix}\overset{(2)}{=}(2-x)\begin{vmatrix}6-x&-4&2&5\\1&1-x&3&0\\-1&1&3-x&-2\\-2&2&2&-2-x\end{vmatrix}\overset{(3)}{=}(2-x)\begin{vmatrix}6-x&-4&2&5\\1&1-x&3&0\\-1&1&3-x&-2\\0&0&2x-4&2-x\end{vmatrix}=$$

$$=(2-x)^2\begin{vmatrix}6-x&-4&2&5\\1&1-x&3&0\\-1&1&3-x&-2\\0&0&-2&1\end{vmatrix}=(2-x)^2\begin{vmatrix}6-x&-4&12&0\\1&1-x&3&0\\-1&1&-1-x&0\\0&0&-2&1\end{vmatrix}=(2-x)^2\begin{vmatrix}6-x&-4&12\\1&1-x&3\\-1&1&-1-x\end{vmatrix}\overset{4}{=}(2-x)^2\begin{vmatrix}6-x&-4&12\\1&1-x&3\\0&2-x&2-x\end{vmatrix}=$$

$$=(2-x)^3\begin{vmatrix}6-x&-4&12\\1&1-x&3\\0&1&1\end{vmatrix}=(2-x)^3\begin{vmatrix}6-x&-16&0\\1&-2-x&0\\0&1&1\end{vmatrix}=(2-x)^3\begin{vmatrix}6-x&-16\\1&-2-x\end{vmatrix}=$$

$$(2-x)^3[(x-6)(x+2)+16]=(2-x)^3(x^2-4x+4)=(2-x)^5$$

Použité úpravy:
(1) Pripočítanie tretieho riadku k druhému
(2) Laplaceov rozvoj podľa druhého stĺpca
(3) Odpočítanie dvojnásobku tretieho riadku od štvrtého.
(4) Pripočítanie druhého riadku k tretiemu

Našli sme charakteristický polynóm

$$ch_A(x) = -(x-2)^5.$$

Jediný koreň charakteristického polynómu (a jediná vlastná hodnota) je teda číslo 2.

Teraz nájdeme k tejto vlastnej hodnote vlastné vektory. Riešime sústavu danú maticou $(A-2I)^T$.

$$\begin{pmatrix} 4 & -1 & 1 & -1 & -2 \\ 1 & 0 & 0 & 0 & 0 \\ -3 & 1 & -1 & 1 & 2 \\ 2 & -3 & 3 & 1 & 2 \\ 5 & 0 & 0 & -2 & -4 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & -1 & -2 \\ 0 & 1 & -1 & 1 & 2 \\ 0 & -3 & 3 & 1 & 2 \\ 0 & 0 & 0 & -2 & -4 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & -1 & -2 \\ 0 & 1 & -1 & 1 & 2 \\ 0 & -3 & 3 & 1 & 2 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & -3 & 3 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Podpriestor riešení tejto sústavy je $[(0,1,1,0,0),(0,0,0,2,-1)]$. Ľahko overíme, že tieto vektory sú skutočne vlastné vektory prislúchajúce k vlastnej hodnote 2. Podobne je vlastným vektorom aj každá ich lineárna kombinácia $a(0,1,1,0,0)+b(0,0,0,2,-1)$.

Keďže množina vlastných vektorov je dvojrozmerná, pre maticu A sa dajú nájsť 2 lineárne nezávislé vlastné vektory. Znamená to, že jej Jordanov normálny tvar bude mať 2 Jordanove bloky.

Teraz budeme riešiť rovnicu zadanú maticou $(A-2I)^T$, v ktorej pravú stranu tvoria práve vypočítané vlastné vektory.

$$\left(\begin{array}{ccccc|c} 4 & -1 & 1 & -1 & -2 & 0 \\ 1 & 0 & 0 & 0 & 0 & a \\ -3 & 1 & -1 & 1 & 2 & a \\ 2 & -3 & 3 & 1 & 2 & 2b \\ 5 & 0 & 0 & -2 & -4 & -b \end{array}\right) \sim \left(\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 0 & a \\ 4 & -1 & 1 & -1 & -2 & 0 \\ -3 & 1 & -1 & 1 & 2 & a \\ 2 & -3 & 3 & 1 & 2 & 2b \\ 5 & 0 & 0 & -2 & -4 & -b \end{array}\right) \sim \left(\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 0 & a \\ 0 & -1 & 1 & -1 & -2 & -4a \\ 0 & 1 & -1 & 1 & 2 & 4a \\ 0 & -3 & 3 & 1 & 2 & -2a+2b \\ 0 & 0 & 0 & -2 & -4 & -5a-b \end{array}\right) \sim$$

$$\left(\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 0 & a \\ 0 & -1 & 1 & -1 & -2 & -4a \\ 0 & 1 & -1 & 1 & 2 & 4a \\ 0 & -3 & 3 & 1 & 2 & -2a+2b \\ 0 & 0 & 0 & 1 & 2 & \frac{5}{2}a+\frac{1}{2}b \end{array}\right) \sim \left(\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 0 & a \\ 0 & -1 & 1 & & & -\frac{3}{2}a+\frac{1}{2}b \\ 0 & 1 & -1 & 0 & 0 & \frac{3}{2}a-\frac{1}{2}b \\ 0 & -3 & 3 & 0 & 0 & -\frac{9}{2}a+\frac{3}{2}b \\ 0 & 0 & 0 & 1 & 2 & \frac{5}{2}a+\frac{1}{2}b \end{array}\right) \sim \left(\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 0 & a \\ 0 & 1 & -1 & 0 & 0 & \frac{3}{2}a-\frac{1}{2}b \\ 0 & 0 & 0 & 1 & 2 & \frac{5}{2}a+\frac{1}{2}b \end{array}\right)$$

Našli sme riešenie $a(1,\frac{3}{2},0,\frac{5}{2},0)+b(0,-\frac{1}{2},0,\frac{1}{2},0)$ pre vlastný vektor $a(0,1,1,0,0)+b(0,0,0,2,-1)$. Keďže sme našli riešenie pre každý vlastný vektor, oba Jordanove bloky musia mať veľkosť aspoň 2. Vzhľadom k tomu, že súčet ich veľkostí je 5, musia to byť bloky veľkosti 2 a 3. To znamená, že už vieme, ako vyzerá Jordanov normálny tvar našej matice, pokúsime sa však ešte dopočítať aj maticu prechodu.

Opäť riešime sústavu danú tou istou maticou, pričom za pravú stranu vezmeme ľubovoľný vektor tvaru $a(1,\frac{3}{2},0,\frac{5}{2},0)+b(0,-\frac{1}{2},0,\frac{1}{2},0)$.

$$\left(\begin{array}{ccccc|c} 4 & -1 & 1 & -1 & -2 & a \\ 1 & 0 & 0 & 0 & 0 & \frac{3}{2}a-\frac{1}{2}b \\ -3 & 1 & -1 & 1 & 2 & 0 \\ 2 & -3 & 3 & 1 & 2 & \frac{5}{2}a+\frac{1}{2}b \\ 5 & 0 & 0 & -2 & -4 & 0 \end{array}\right) \sim \left(\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 0 & \frac{3}{2}a-\frac{1}{2}b \\ 4 & -1 & 1 & -1 & -2 & a \\ -3 & 1 & -1 & 1 & 2 & 0 \\ 2 & -3 & 3 & 1 & 2 & \frac{5}{2}a+\frac{1}{2}b \\ 5 & 0 & 0 & -2 & -4 & 0 \end{array}\right) \sim \left(\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 0 & \frac{3}{2}a-\frac{1}{2}b \\ 0 & -1 & 1 & -1 & -2 & -5a+2b \\ 0 & 1 & -1 & 1 & 2 & \frac{9}{2}a-\frac{3}{2}b \\ 0 & -3 & 3 & 1 & 2 & -\frac{1}{2}a+\frac{3}{2}b \\ 0 & 0 & 0 & -2 & -4 & -\frac{15}{2}a+\frac{5}{2}b \end{array}\right) \sim$$

$$\left(\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 0 & \frac{3}{2}a-\frac{1}{2}b \\ 0 & -1 & 1 & -1 & -2 & -5a+2b \\ 0 & 1 & -1 & 1 & 2 & \frac{9}{2}a-\frac{3}{2}b \\ 0 & -3 & 3 & 1 & 2 & -\frac{1}{2}a+\frac{3}{2}b \\ 0 & 0 & 0 & 1 & 2 & \frac{15}{4}a-\frac{5}{4}b \end{array}\right) \sim \left(\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 0 & \frac{3}{2}a-\frac{1}{2}b \\ 0 & -1 & 1 & 0 & 0 & -\frac{5}{4}a+\frac{3}{4}b \\ 0 & 1 & -1 & 0 & 0 & \frac{3}{4}a-\frac{1}{4}b \\ 0 & -3 & 3 & 0 & 0 & -\frac{17}{4}a+\frac{11}{4}b \\ 0 & 0 & 0 & 1 & 2 & \frac{15}{4}a-\frac{5}{4}b \end{array}\right)$$

Aby predchádzajúca sústava mala riešenie, musí platiť $-\frac{5}{4}a+\frac{3}{4}b=-\frac{3}{4}a+\frac{1}{4}b$ (dostaneme to porovnaním druhého a tretieho riadku). Z toho dostaneme $a=b$. Tým prejde sústava na tvar

$$\left(\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 0 & a \\ 0 & -1 & 1 & 0 & 0 & -\frac{a}{2} \\ 0 & 1 & -1 & 0 & 0 & \frac{a}{2} \\ 0 & -3 & 3 & 0 & 0 & -\frac{3}{2}a \\ 0 & 0 & 0 & 1 & 2 & \frac{5}{2}a \end{array}\right) \sim \left(\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 0 & a \\ 0 & 1 & -1 & 0 & 0 & \frac{a}{2} \\ 0 & 0 & 0 & 1 & 2 & \frac{5}{2}a \end{array}\right)$$

Ako jedno z možných riešení dostaneme $a(1,\frac{1}{2},0,\frac{5}{2},0)$. Pri voľbe $a=1$ máme

$\vec{\alpha}_1 = (1,\frac{1}{2},0,\frac{5}{2},0)$

$\vec{\alpha}_2 = \vec{\alpha}_1(A-2I) = (1,1,0,3,0)$

$\vec{\alpha}_3 = \vec{\alpha}_2(A - 2I) = (0, 1, 1, 2, -1)$
Dostali sme presne vlastný vektor zodpovedajúci hodnotám $a = b = 1$. Tieto 3 vektory určujú jeden Jordanov blok. Aby sme dostali druhý, potrebujeme použiť nejaký vlastný vektor lineárne nezávislý od $(0, 1, 1, 2, -1)$. Môžeme zvoliť napríklad $a = 1$, $b = 0$:
$\vec{\alpha}_4 = (1, \frac{3}{2}, 0, \frac{5}{2}, 0)$
$\vec{\alpha}_5 = \vec{\alpha}_4(A - 2I) = (0, 1, 1, 0, 0)$

Dostali sme teda

$$P = \begin{pmatrix} 1 & \frac{1}{2} & 0 & \frac{5}{2} & 0 \\ 1 & 1 & 0 & 3 & 0 \\ 0 & 1 & 1 & 2 & -1 \\ 1 & \frac{3}{2} & 0 & \frac{5}{2} & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix} \qquad J = \begin{pmatrix} 2 & 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

Pre tieto matice skutočne platí

$$J = PAP^{-1}.$$

Vlastné vektory sú určené rovnosťou $\vec{\alpha}(A - 2I) = \vec{0}$ Všimnime si, že pre ostatné vektory, ktoré sme dostali v predošlom príklade platí $\vec{\alpha}_2(A-2I)^2 = \vec{\alpha}_4(A-2I)^2 = \vec{0}$ a $\vec{\alpha}_1(A-2I)^3 = \vec{0}$. Vektory, ktoré vyhovujú rovnici $\vec{\alpha}(A - \lambda I)^n$ pre nejaké $n \in \mathbb{N}$ a $\lambda \in \mathbb{C}$, sa nazývajú *zovšeobecnené vlastné vektory.*

Vďaka tomuto pozorovaniu môžeme hľadať vlastné vektory aj iným spôsobom. Konkrétne ide o to, že sa môžeme pozrieť na mocniny matice $A - \lambda I$, teda na matice tvaru $(A - \lambda I)^n$.

Ak je matica A podobná s blokovo-diagonálnou maticou J pozostávajúcich Jordanových blokov, tak $A - \lambda I$ je podobná s maticou $J - \lambda I$. Táto matica vyzerá tak, že v blokoch zodpovedajúcich vlastnej hodnote λ sa λ nahradila nulou a v blokoch zodpovedajúcich nejakej vlastnej hodnote $\mu \neq \lambda$ nahradíme na diagonále μ číslom $\mu - \lambda$.

Ak nás zaujíma hodnosť matice $(A - \lambda I)^n$, stačí sa pozrieť na maticu $(J - \lambda I)^n$, lebo podobné matice majú rovnakú hodnosť. Táto matica je výrazne jednoduchšia, takže ju budeme asi vedieť ľahšie umocniť. Skutočne, ak umocňujeme blokovo-diagonálnu maticu, tak výsledok je opäť blokovo-diagonálna matica, pričom jednotlivé bloky sú mocninami blokov vystupujúcich v pôvodnej matici. Takže sa nám stačí pozrieť na to, čo sa deje pri umocňovaní jednotlivých blokov.

Z blokov zodpovedajúcich vlastnej hodnote λ sme dostali bloky takéhoto tvaru:

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

Vidíme, že v každom taktomto bloku je jeden riadok nulový a ostatné sú lineárne nezávislé. Bloky zodpovedajúce ostatným vlastným hodnotám vyzerajú takto

$$\begin{pmatrix} \mu-\lambda & 1 & 0 & \cdots & \cdots & 0 \\ 0 & \mu-\lambda & 1 & 0 & & 0 \\ \vdots & & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & 0 \\ 0 & & & \mu-\lambda & 1 & 0 \\ 0 & & & & \mu-\lambda & 1 \\ 0 & \cdots & \cdots & \cdots & \cdots & \mu-\lambda \end{pmatrix}$$

Fakt, že $\mu - \lambda \neq 0$ zabezpečí, že takáto bloková matica bude regulárna.

Keď sa teraz pozrieme na celú maticu $A - \lambda I$, tak táto matica obsahuje toľko nulových riadkov, koľko je v nej Jordanových blokov prislúchajúcich k vlastnej hodnote λ a ostatné

riadky sú lineárne nezávislé. Teda počet Jordanových blokov pre túto vlastnú hodnotu je $n - h(A - \lambda I)$, ak pôvodná matica A má rozmery $n \times n$.

Ešte by sme si mali rozmyslieť, čo dostaneme umocňovaním takýchto matíc. Nie je ťažké uvedomiť si, že ak umocníme ľubovoľnú maticu tvaru

$$\begin{pmatrix} 0 & c_{1,2} & c_{1,3} & \dots & \dots & c_{1,n} \\ 0 & 0 & c_{2,3} & c_{2,4} & & c_{2,n} \\ \vdots & & \ddots & \ddots & \ddots & \vdots \\ 0 & & & 0 & c_{n-2,n-1} & c_{n-1,n} \\ 0 & & & & 0 & c_{n-1,n} \\ 0 & \dots & \dots & \dots & \dots & 0 \end{pmatrix}$$

t.j. ľubovoľnú maticu, ktorá má na hlavnej diagonále aj pod ňou samé nuly, tak v druhej mocnine nám pribudnú nuly tesne nad diagonálou. V tretej mocnine nám pribudne ďalšia vedľajšia diagonála pozostávajúca zo samých núl. (Do istej miery podobná úvaha ako robíme za rovnosťou (3.13).) Čiže keď porovnáme $(k-1)$-vú a k-tu mocninu, tak nám pre každý Jordanov blok veľkosti aspoň k pribudol jeden nulový riadok.

Bloky, ktoré mali na diagonále nenulové čísla $\mu - \lambda$ budú vo svojich mocninách na diagonále nenulové čísla $(\mu - \lambda)^n$ a zostanú regulárne. Podobná úvaha by fungovala aj pre ľubovoľnú maticu tvaru

$$\begin{pmatrix} d_1 & c_{1,2} & c_{1,3} & \dots & \dots & c_{1,n} \\ 0 & d_2 & c_{2,3} & c_{2,4} & & c_{2,n} \\ \vdots & & \ddots & \ddots & \ddots & \vdots \\ 0 & & & d_{n-2} & c_{n-2,n-1} & c_{n-1,n} \\ 0 & & & & d_{n-1} & c_{n-1,n} \\ 0 & \dots & \dots & \dots & \dots & d_n \end{pmatrix}.$$

Keď zhrnieme doterajšie úvahy, zistili sme, že v matici $(A - \lambda I)^k$ je počet nulových riadkov rovný $n_1 + \cdots + n_k$, kde n_k označuje počet Jordanových blokov veľkosti aspoň k prislúchajúcich vlastnej hodnote λ. Ostatné riadky sú lineárne nezávislé. Teda z hodností takýchto matíc vieme zistiť počty Jordanových blokov jednotlivých veľkostí.

Ukážme si tento postup na tej istej matici ako v predošlom príklade.

Príklad 3.4.4. Opäť teda budeme pracovať s maticou $A = \begin{pmatrix} 6 & 1 & -3 & 2 & 5 \\ -1 & 2 & 1 & -3 & 0 \\ 1 & 0 & 1 & 3 & 0 \\ -1 & 0 & 1 & 3 & -2 \\ -2 & 0 & 2 & 2 & -2 \end{pmatrix}$. Už sme vyrátali, že charakteristický polynóm je $ch_A(x) = -(x-2)^5$ a jediné vlastné číslo je 2.

Pozrime sa teraz na to, ako vyzerajú mocniny matice $(A - 2I)$. Z Cayley-Hamiltonovej vety vieme, že $(A-2I)^5 = 0$, teda budeme musieť ísť nanajvýš po piatu mocninu. (To vyzerá na prvý pohľad veľmi prácne – ideme násobiť maticu 5×5 – keď si však všimneme, že druhý a tretí riadok sa líšia až na skalárny násobok; podobne je to pre štvrtý a piaty riadok; tak keď máme druhý a štvrtý riadok v matici $(A - 2I)^2$, hneď poznáme aj tretí a piaty, ktoré dostaneme ako príslušné násobky.)

$$A - 2I = \begin{pmatrix} 4 & 1 & -3 & 2 & 5 \\ -1 & 0 & 1 & -3 & 0 \\ 1 & 0 & -1 & 3 & 0 \\ -1 & 0 & 1 & 1 & -2 \\ -2 & 0 & 2 & 2 & -4 \end{pmatrix}$$

$$(A - 2I)^2 = \begin{pmatrix} 0 & 4 & 4 & 8 & -4 \\ 0 & -1 & -1 & -2 & 1 \\ 0 & 1 & 1 & 2 & -1 \\ 0 & -1 & -1 & -2 & 1 \\ 0 & -2 & -2 & -4 & 2 \end{pmatrix}$$

$$(A - 2I)^3 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Vidíme, že $h(A-2I)=3$, $h((A-2I)^2)=1$ a $h((A-2I)^3)=0$.

Z hodností, ktoré sme vyrátali, vidíme, že počet Jordanových blokov je $2=5-3$. Počet blokov, ktoré majú veľkosť aspoň dva je $2=3-1$ a počet blokov veľkosti aspoň tri je $1=1-0$. Teda máme jeden blok veľkosti 2 a jeden blok veľkosti 3. (Môžeme si všimnúť aj to, že nám stačilo rátať prvé dve mocniny.)

Teraz už teda vieme, ako vyzerá Jordanov normálny tvar:

$$J=\begin{pmatrix}2&1&0&0&0\\0&2&1&0&0\\0&0&2&0&0\\0&0&0&2&1\\0&0&0&0&2\end{pmatrix}$$

Nevýhoda oproti predošlému postupu je tá, že sme nezostavili maticu P. (Čiže pri predošlom postupe sme mohli urobiť kontrolu vynásobením PAP^{-1}.)

Tak sa skúsme pozrieť na to, či by sme tu vedeli nájsť zovšeobecnené vlastné vektory. Vektor $\vec{\alpha}_3$ je tvaru $\vec{\alpha}_1(A-2I)^2$. Každý taký vektor je násobkom vektora $(0,1,1,2,-1)$. (Pozeráme sa na vektory, ktoré sú v podpriestore generovanom riadkami matice $(A-2I)^2$, v našom konkrétnom prípade je tento podpriestor jednorozmerný.) Môžeme teda zvoliť $\vec{\alpha}_3=(0,1,1,2,-1)$.

Mali by sme teraz nájsť vektor $\vec{\alpha}_2$ taký, že $\vec{\alpha}_2(A-2I)=\vec{\alpha}_3$ a vektor $\vec{\alpha}_1$ vyhovujúci rovnosti $\vec{\alpha}_1(A-2I)=\vec{\alpha}_2$. To sa dá urobiť riešením sústavy; v podstate rovnakú sústavu sme riešili pri počítaní predošlým postupom, vieme teda, že možné riešenia sú $\vec{\alpha}_1=(1,\frac{1}{2},0,\frac{5}{2},0)$, $\vec{\alpha}_2=\vec{\alpha}_1(A-2I)=(1,1,0,3,0)$.

Ďalej by nás zaujímal vektor $\vec{\alpha}_5$, ktorý je vlastným vektorom a súčasne sa dá dostať ako $\vec{\alpha}_5=\vec{\alpha}_4(A-2I)$ pre nejaký vektor $\vec{\alpha}_4$. (Týmto podmienkam vyhovuje aj vektor $\vec{\alpha}_3$, my chceme nejaký vektor, ktorý nie je jeho násobkom.)

Vektor $\vec{\alpha}_5$ teda patrí do podpriestoru $[(4,1,-3,2,5),(1,0,-1,3,0),(1,0,-1,-1,2)]$ generovaného riadkami matice $(A-2I)$. Súčasne by mal byť vlastným vektorom, teda by mal ležať v podpriestore $[(0,1,1,0,0),(0,0,0,2,-1)]$. (Tento podpriestor sme našli ako podpriestor riešení homogénneho systému s maticou $(A-2I)^T$ už v predošlom postupe.)

Prienik dvoch podpriestorov by sme vedeli vyrátať, v tomto konkrétnom prípade máme však situáciu výrazne zjednodušenú. Pretože celý podpriestor $[(0,1,1,0,0),(0,0,0,2,-1)]$ je dvojrozmerný a máme v ňom dva vektory lineárne nezávislé $\vec{\alpha}_3$ a $\vec{\alpha}_5$, tak vieme, že ten prienik musí byť dvojrozmerný, bude sa teda zhodovať s podpriestorom $[(0,1,1,0,0),(0,0,0,2,-1)]$. Preto je vhodným kandidátom pre $\vec{\alpha}_5$ ľubovoľný nenulový vektor z tohoto podpriestoru rôzny od $\vec{\alpha}_3$. Ak napríklad zvolíme $\vec{\alpha}_5=(0,1,1,0,0)$, tak riešením sústavy dostaneme $\vec{\alpha}_4=(1,\frac{3}{2},0,\frac{5}{2},0)$.

Poznámka 3.4.5. Na základe toho, že z hodností matíc $h((A-\lambda I)^k)$ sa dá vyčítať počet blokov jednotlivých veľkostí, by sme vedeli dokázať aspoň to, že Jordanov normálny tvar je jednoznačne určený až na poradie blokov.

Cvičenia

Úloha 3.4.1. Nájdite Jordanov normálny tvar J matice A a regulárnu maticu P takú, že platí $PAP^{-1}=J$.

a) $A=\begin{pmatrix}0&0&1\\1&3&-3\\0&1&0\end{pmatrix}$

b) $A=\begin{pmatrix}0&1&0\\0&3&1\\1&-3&0\end{pmatrix}$

c) $A = \begin{pmatrix} 1 & -1 & -1 & 1 \\ 0 & 0 & -1 & 1 \\ -2 & -2 & -1 & 4 \\ -1 & -2 & -2 & 4 \end{pmatrix}$

d) $A = \begin{pmatrix} 0 & 2 & 2 \\ -1 & 3 & 1 \\ -1 & 1 & 3 \end{pmatrix}$

e) $A = \begin{pmatrix} 2 & 0 & -1 \\ -1 & 2 & 1 \\ 2 & -1 & -1 \end{pmatrix}$

[a) $ch_A(x) = -(x-1)^3$, vlastný vektor $(1,1,-2)$, $J = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$; b) $ch_A(x) = -(x-1)^3$, jediný vlastný vektor $(1,1,1)$, $J = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$; c) $ch_A(x) = -(x-1)^4$, vlastné vektory $[(-1,1,0,0),(-2,0,-1,2)]$, $J = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$; d) $ch_A(x) = -(x-2)^3$, vlastné vektory $[(1,0,-2),(0,1,-1)]$, $J = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$; e) $ch_A(x) = -(x-1)^3$, vlastné vektory $[(1,-1,-1)]$, $J = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$]

Úloha 3.4.2. Nájdite Jordanov normálny tvar daných matíc.
$\begin{pmatrix} 0 & 1 & 0 \\ -4 & 4 & 0 \\ -2 & 1 & 2 \end{pmatrix}$ $\begin{pmatrix} 2 & 6 & -15 \\ 1 & 1 & -5 \\ 1 & 2 & -6 \end{pmatrix}$ $\begin{pmatrix} 9 & -6 & -2 \\ 18 & -12 & -3 \\ 18 & -9 & -6 \end{pmatrix}$ $\begin{pmatrix} 4 & -5 & 2 \\ 5 & -7 & 3 \\ 6 & -9 & 4 \end{pmatrix}$ $\begin{pmatrix} 1 & -3 & 3 \\ -2 & -6 & 13 \\ -1 & -4 & 8 \end{pmatrix}$ $\begin{pmatrix} 7 & -12 & 6 \\ 10 & -19 & 10 \\ 12 & -24 & 13 \end{pmatrix}$ $\begin{pmatrix} t & 0 & 0 \\ 0 & t & 0 \\ t & 0 & t \end{pmatrix}$ pre $t \neq 0$
Riešenia: $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}$ $\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{pmatrix}$ $\begin{pmatrix} -3 & 0 & 0 \\ 0 & -3 & 1 \\ 0 & 0 & -3 \end{pmatrix}$ $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ $\begin{pmatrix} 1 & 0 & 0 \\ 0 & t & 1 \\ 0 & 0 & t \end{pmatrix}$

Úloha 3.4.3. Nájdite Jordanov normálny tvar daných matíc.
$\begin{pmatrix} 1 & -3 & 0 & 3 \\ -2 & -6 & 0 & 13 \\ 0 & -3 & 1 & 3 \\ -1 & -4 & 0 & 8 \end{pmatrix}$ $\begin{pmatrix} 3 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 3 & 0 & 5 & -3 \\ 4 & -1 & 3 & -1 \end{pmatrix}$ $\begin{pmatrix} 3 & -4 & 0 & 2 \\ 4 & -5 & -2 & 4 \\ 0 & 0 & 3 & -2 \\ 0 & 0 & 2 & -1 \end{pmatrix}$ $\begin{pmatrix} 3 & -1 & 1 & -7 \\ 9 & -3 & -7 & -1 \\ 0 & 0 & 4 & -8 \\ 0 & 0 & 2 & -4 \end{pmatrix}$
Riešenia $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ $\begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}$ $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & -1 \end{pmatrix}$ $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$

Úloha 3.4.4. Nájdite Jordanov tvar danej matice:
a) $\begin{pmatrix} -2 & -5 & 3 \\ 1 & 0 & -1 \\ 0 & -4 & 1 \end{pmatrix}$
b) $\begin{pmatrix} 0 & 1 & -1 \\ 1 & 0 & 1 \\ 2 & -2 & 3 \end{pmatrix}$
Výsledky: a) $\begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ b) $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

Úloha 3.4.5. Nájdite charakteristický polynóm a Jordanov tvar matice Nájdite aj príslušnú maticu prechodu a zapíšte príslušnú maticovú rovnosť.
$\begin{pmatrix} -3 & 0 & 4 \\ 3 & -1 & -5 \\ -2 & 0 & 3 \end{pmatrix}$ $\begin{pmatrix} 1 & 4 & -3 \\ 0 & -3 & 1 \\ 0 & -4 & 1 \end{pmatrix}$ $\begin{pmatrix} -2 & -5 & 3 \\ 1 & 0 & -1 \\ 0 & -4 & 1 \end{pmatrix}$ $\begin{pmatrix} 2 & -1 & 0 \\ 1 & 0 & 0 \\ 2 & 2 & 1 \end{pmatrix}$ $\begin{pmatrix} 3 & -3 & 1 \\ 2 & -2 & 1 \\ 2 & -3 & 2 \end{pmatrix}$ $\begin{pmatrix} 3 & -3 & 1 \\ 2 & -2 & 1 \\ 2 & -3 & -2 \end{pmatrix}$
Výsledky: $\begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ $\begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ $\begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ $\begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

3.5 Aplikácie podobnosti a Jordanovho normálneho tvaru

3.5.1 Lineárne rekurencie

Pomocou Jordanovho normálneho tvaru sa dá odvodiť riešenie lineárnych rekurentných rovníc. My sa pre jednoduchosť obmedzíme na rekurencie druhého rádu.

Pod *lineárnou rekurenciou druhého rádu* rozumieme predpis

$$A_{n+1} = aA_n + bA_{n-1}, \tag{3.9}$$

kde $a, b \in \mathbb{C}$. Je zrejmé, že ak nejaká postupnosť $(A_n)_{n=1}^{\infty}$ vyhovuje rovnici (3.9) pre všetky $n \in \mathbb{N}$ a ak poznáme jej počiatočné hodnoty A_0 a A_1, tak tým je už postupnosť $(A_n)_{n=1}^{\infty}$ jednoznačne určená.

Základom pre to, aby sme mohli aplikovať naše poznatky o podobnosti matíc na lineárne rekurencie je uvedomiť si, že s rovnosťou (3.9) je ekvivalentný nasledovný maticový zápis

$$\begin{pmatrix} A_{n+1} \\ A_n \end{pmatrix} = \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix} \begin{pmatrix} A_n \\ A_{n-1} \end{pmatrix} \tag{3.10}$$

Charakteristický polynóm tejto matice je

$$ch_A(x) = \begin{vmatrix} a-x & b \\ 1 & -x \end{vmatrix} = x(x-a) - b = x^2 - ax - b.$$

Vlastné hodnoty sú riešenia rovnice $ch_A(x) = 0$. Táto rovnica sa zvykne nazývať *charakteristická rovnica* rekurencie (3.9).

Pre vlastné hodnoty $\lambda_{1,2}$ matice $A = \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix}$ teda platí

$$\begin{aligned} \lambda_1 + \lambda_2 &= a \\ \lambda_1 \cdot \lambda_2 &= -b \end{aligned} \tag{3.11}$$

Z rovnosti (3.10) dostaneme postupne

$$\begin{pmatrix} A_{n+1} \\ A_n \end{pmatrix} = A \begin{pmatrix} A_n \\ A_{n-1} \end{pmatrix} = A^2 \begin{pmatrix} A_{n-1} \\ A_{n-2} \end{pmatrix} = \cdots = A^n \begin{pmatrix} A_1 \\ A_0 \end{pmatrix} \tag{3.12}$$

Ak poznáme Jordanov tvar matice A, t.j. ak platí $A = P^{-1}JP$, tak túto rovnosť vieme prepísať ako

$$\begin{pmatrix} A_{n+1} \\ A_n \end{pmatrix} = A^n \begin{pmatrix} A_1 \\ A_0 \end{pmatrix} = P^{-1}J^nP \begin{pmatrix} A_1 \\ A_0 \end{pmatrix}.$$

Na ďalšie výpočty potrebujeme vedieť ako vyzerajú mocniny matice v Jordanovom normálnom tvare. V prípade, že J je diagonálna matica, jednoducho umocníme prvky na diagonále. Pre matice 2×2 máme.

$$J = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \qquad \Rightarrow \qquad J^n = \begin{pmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{pmatrix}$$

Vo všeobecnosti nám stačí umocňovať Jordanove bloky. V prípade matice 2×2 je situácia pomerne jednoduchá:

$$J = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \qquad J^2 = \begin{pmatrix} \lambda^2 & 2\lambda \\ 0 & \lambda^2 \end{pmatrix} \qquad \ldots \qquad J^n = \begin{pmatrix} \lambda^n & n\lambda^{n-1} \\ 0 & \lambda^n \end{pmatrix} \tag{3.13}$$

Keďže pracujeme iba s rekurenciami druhého stupňa, vystačíme s maticami 2×2. Môžete si ale skúsiť rozmyslieť, že podobne to bude fungovať aj pre Jordanove bloky väčších rozmerov, t.j. k-ta mocnina Jordanovho bloku obsahuje (počnúc od diagonály) prvky $\lambda^k, k\lambda^k, \binom{k}{2}\lambda^{k-1}, \ldots$

Pozrime sa teraz nato, čo z predchádzajúcich rovností dostaneme pre rekurentné postupnosti.

V prípade, že Jordanov tvar je diagonálny, máme

$$\begin{pmatrix} A_{n+1} \\ A_n \end{pmatrix} = \begin{pmatrix} p'_{11} & p'_{12} \\ p'_{21} & p'_{22} \end{pmatrix} \begin{pmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{pmatrix} \begin{pmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{pmatrix} \begin{pmatrix} A_1 \\ A_0 \end{pmatrix} = \begin{pmatrix} p'_{11} & p'_{12} \\ p'_{21} & p'_{22} \end{pmatrix} \begin{pmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{pmatrix} \begin{pmatrix} a'_1 \\ a'_0 \end{pmatrix} =$$
$$= \begin{pmatrix} p'_{11} & p'_{12} \\ p'_{21} & p'_{22} \end{pmatrix} \begin{pmatrix} a'_1\lambda_1^n \\ a'_0\lambda_2^n \end{pmatrix} = \begin{pmatrix} p'_{11}a'_1\lambda_1^n + p'_{12}a'_0\lambda_2^n \\ p'_{21}a'_1\lambda_1^n + p'_{22}a'_0\lambda_2^n \end{pmatrix}$$

Ak porovnáme druhý riadok matíc na ľavej a pravej strane v predošlej rovnosti, vyšlo nám, že

$$A_n = c_1\lambda_1^n + c_2\lambda_2^n.$$

Na vyrátanie konštánt $c_{1,2}$ môžeme použiť to, že poznáme iniciálne hodnoty $A_{0,1}$.

Pozrime sa na prípad, že matica A nie je diagonalizovateľná. Jej Jordanov tvar potom obsahuje jediný Jordanov blok veľkosti 2. Vlastné hodnoty sú rovnaké, ich spoločnú hodnotu označme λ. Potom máme

$$\begin{pmatrix} A_{n+1} \\ A_n \end{pmatrix} = \begin{pmatrix} p'_{11} & p'_{12} \\ p'_{21} & p'_{22} \end{pmatrix} \begin{pmatrix} \lambda^n & n\lambda^{n-1} \\ 0 & \lambda^n \end{pmatrix} \begin{pmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{pmatrix} \begin{pmatrix} A_1 \\ A_0 \end{pmatrix} = \begin{pmatrix} p'_{11} & p'_{12} \\ p'_{21} & p'_{22} \end{pmatrix} \begin{pmatrix} \lambda^n & n\lambda^{n-1} \\ 0 & \lambda^n \end{pmatrix} \begin{pmatrix} a'_1 \\ a'_0 \end{pmatrix} =$$
$$= \begin{pmatrix} p'_{11} & p'_{12} \\ p'_{21} & p'_{22} \end{pmatrix} \begin{pmatrix} a'_1\lambda^n + a'_0 n\lambda^{n-1} \\ a'_0\lambda^n \end{pmatrix} = \begin{pmatrix} (p'_{11}a'_1 + p'_{12}a'_0)\lambda^n + p'_{11}n\lambda^{n-1} \\ (p'_{21}a'_1 + p'_{22}a'_0)\lambda^n + p'_{21}n\lambda^{n-1} \end{pmatrix}$$

Zistili sme, že

$$A_n = c_1\lambda^n + c_2 n\lambda^{n-1}.$$

Opäť, konštanty $c_{1,2}$ môžeme vyrátať z počiatočných podmienok.

Podobným spôsobom sa dá odvodiť aj všeobecný vzťah pre lineárne rekurencie k-tého stupňa

$$A_{n+k} = c_{k-1}A_{n+k-1} + c_{k-2}A_{n+k-2} + \cdots + c_1A_{n+1} + c_0A_n.$$

Opäť, riešenie môžeme nájsť ako lineárnu kombináciu geometrických postupností určených koreňmi charakteristickej rovnice, v prípade, že je niektorý koreň viacnásobný, treba brať do úvahy okrem geometrickej postupnosti λ^n aj postupnosti $n\lambda^{n-1}, n^2\lambda^{n-2}, \ldots$ (toľko z nich, koľko je násobnosť príslušného koreňa).

Viac o lineárnych rekurenciách ako aj dôkaz vety o tvare riešení založený práve na použití Jordanovho normálneho tvaru môžete nájsť napríklad v [CFR, Section 2.2]. Iný dôkaz môžete nájsť v [W].

Príklad 3.5.1. Nájdime vyjadrenie n-tého člena Fibonacciho postupnosti určenej predpisom

$$F_{n+1} = F_n + F_{n-1} \tag{3.14}$$

a počiatočnými hodnotami

$$F_0 = 0, F_1 = 1.$$

Maticový zápis rovnice (3.14) je

$$\begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix} \tag{3.15}$$

Charakteristická rovnica je $x^2 - x - 1 = 0$ a jej korene sú

$$\lambda_{1,2} = \frac{1 \pm \sqrt{5}}{2}.$$

Na základe Viétových vzťahov pre ne platí

$$\lambda_1 + \lambda_2 = 1,$$
$$\lambda_1 \lambda_2 = -1.$$

Vlastné vektory pre vlastnú hodnotu λ_1 nájdeme riešením sústavy s maticou

$$\begin{pmatrix} 1-\lambda_1 & 1 \\ 1 & -\lambda_1 \end{pmatrix} = \begin{pmatrix} \lambda_2 & 1 \\ 1 & -\lambda_1 \end{pmatrix}$$

Vidíme, že obom rovniciam vyhovuje napríklad vektor $(1, -\lambda_2)$.

Podobne vlastným vektorom pre vlastnú hodnotu λ_2 je $(1, -\lambda_1)$. Teda pre maticu

$$P = \begin{pmatrix} 1 & -\lambda_2 \\ 1 & -\lambda_1 \end{pmatrix}$$

platí $PAP^{-1} = \operatorname{diag}(\lambda_1, \lambda_2)$.

Inverzná matica k matici P je

$$P^{-1} = \frac{1}{\lambda_2 - \lambda_1} \begin{pmatrix} -\lambda_1 & \lambda_2 \\ -1 & 1 \end{pmatrix}$$

Dosadením do (3.12) potom dostaneme

$$\begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = P^{-1} \begin{pmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{pmatrix} P \begin{pmatrix} F_1 \\ F_0 \end{pmatrix} = \frac{1}{\lambda_2 - \lambda_1} \begin{pmatrix} -\lambda_1^{n+1} & \lambda_2^{n+1} \\ -\lambda_1^n & \lambda_2^n \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\lambda_2 - \lambda_1} \begin{pmatrix} \lambda_2^{n+1} - \lambda_1^{n+1} \\ \lambda_2^n - \lambda_1^n \end{pmatrix}$$

Na základe porovnania spodného riadku na ľavej a pravej strane predchádzajúcej rovnosti vidno, že

$$F_n = \frac{\lambda_2^n - \lambda_1^n}{\lambda_2 - \lambda_1}, \tag{3.16}$$

Ak dosadíme $\lambda_2 = \frac{1+\sqrt{5}}{2}$ a $\lambda_1 = \frac{1-\sqrt{5}}{2}$, tak máme

$$F_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}. \tag{3.17}$$

Vzorec (3.17) (resp. (3.16)) sa volá *Cauchy-Binetova formula.*

Maticové rovnosti (3.10) a (3.15) nám môžu pomôcť nielen odvodiť vzorec pre n-tý člen postupnosti ale aj na odvodenie niektorých vzťahov platných pre rekurentné postupnosti. Ako jednoduchý príklad si môžeme ukázať odvodenie vzorca pre súčet prvých n členov Fibonacciho postupnosti.

Viac o využití matíc pri odvodzovaní rôznych identít platných pre členy Fibonacciho postupnosti (prípadne aj všeobecnejšie pre lineárne rekurencie druhého stupňa) sa môžete dočítať napríklad v [J, Š].

Príklad 3.5.2. Využijeme rovnosti

$$\begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = A^{n-1} \begin{pmatrix} F_2 \\ F_1 \end{pmatrix},$$
$$\begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix} = A^{n-2} \begin{pmatrix} F_2 \\ F_1 \end{pmatrix},$$
$$\vdots$$
$$\begin{pmatrix} F_2 \\ F_1 \end{pmatrix} = I \begin{pmatrix} F_2 \\ F_1 \end{pmatrix}.$$

Ich sčítaním dostaneme

$$\begin{pmatrix} F_2 + \cdots + F_{n+1} \\ F_1 + \cdots + F_n \end{pmatrix} = (I + A + \cdots + A^{n-1}) \begin{pmatrix} F_2 \\ F_1 \end{pmatrix}.$$

Všimnime si, že platí

$$(A - I)(I + A + \cdots + A^{n-1}) = A^n - I,$$

a teda

$$I + A + \cdots + A^{n-1} = (A - I)^{-1}(A^n - I).$$

Ľahko vypočítame, že

$$(A - I)^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = A.$$

(Tento fakt sme mohli spozorovať aj z charakteristickej rovnice. Podľa Cayley-Hamiltonovej vety 3.2.14 totiž musí platiť $ch_A(A) = A^2 - A - I = 0$, z čoho dostaneme $A(A - I) = I$ a $(A - I)^{-1} = A$.)

Máme teda

$$\begin{pmatrix} F_2 + \cdots + F_{n+1} \\ F_1 + \cdots + F_n \end{pmatrix} = (A - I)^{-1}(A^n - I) \begin{pmatrix} F_2 \\ F_1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} F_{n+2} - 1 \\ F_{n+1} - 2 \end{pmatrix} = \begin{pmatrix} F_{n+3} - 1 \\ F_{n+2} - 1 \end{pmatrix}.$$

Vypočítali sme teda, že

$$\sum_{k=1}^{n} F_k = F_{n+2} - 1.$$

Poznamenajme, že identitu odvodenú v predchádzajúcom príklade by sme mohli ľahko overiť indukciou. Za výhodu uvedeného prístupu možno považovať to, že takto sme boli schopní tento vzorec objaviť – pri dôkaze indukciou musíme najprv uhádnuť ako vzorec vyzerá. (Táto výhoda je možno zjavnejšia pri odvodzovaní niektorých komplikovanejších rovností; my sme sa uspokojili s týmto veľmi jednoduchým príkladom.)

Cvičenia

Úloha 3.5.1. Nájdite predpis pre n-tý člen danej rekurentnej postupnosti:
a) $a_n = 5a_{n-1} - 6a_{n-2}$, pričom $a_0 = 4$ a $a_1 = 7$;
b) $a_n = a_{n-1} + 2a_{n-2}$, pričom $a_0 = 4$ a $a_1 = 5$;
c) $a_n = 6a_{n-1} - 9a_{n-2}$, pričom $a_0 = 2$ a $a_1 = 3$;
d) $a_n = 2a_{n-1} - 2a_{n-2}$, pričom $a_0 = a_1 = 2$.
[Výsledky: a) $5.2^n - 3^n$; b) $3.2^n + (-1)^n$; c) $2.3^n - n.3^n$ d) $(1 + i)^n + (1 - i)^n$.]

Viaceré cvičenia v tejto časti sú zamerané na dôkaz niektorých identít týkajúcich sa Fibonacciho čísel pomocou matíc. Pre mnohé z nich sa dajú dokázať podobné výsledky aj pre ľubovoľné rekurentné postupnosti druhého rádu. Na porovnanie obtiažnosti si môžete niektoré z nich skúsiť dokázať aj matematickou indukciou, dosadením vzorca (3.17) pre n-tý člen alebo inými spôsobmi (generujúce funkcie, rôzne metódy na výpočet súm, ...).

Úloha 3.5.2. Ukážte, že pre maticu $A = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ a pre $n \in \mathbb{N}$ platí $A^n = \left(\begin{smallmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{smallmatrix}\right)$.

Na základe toho ukážte, že:
a) $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$ (Cassiniho identita)
b) $F_{m+n} = F_m F_{n+1} + F_{m-1}F_n$ (konvolučná vlastnosť)
c) $F_{2n} = F_n(F_{n+1} + F_{n-1})$ a $F_{2n+1} = F_{n+1}^2 + F_n^2$.

Vedeli by ste pomocou výsledkov z časti c) navrhnúť efektívny algoritmus na výpočet n-tého Fibonacciho čísla.

Úloha 3.5.3. Dokážte, že $\sum_{k=0}^{n} F_{2k+1} = F_{2(n+1)}$ a $\sum_{k=0}^{n} F_{2k} = F_{2n+1} - 1$.

Úloha 3.5.4. Ukážte, že $\sum_{k=0}^{n} F_k^2 = F_n F_{n+1}$. (Hint k maticovému odvodeniu: Čomu sa rovná $(A^k)^2$? Iná možnosť: Použiť nejako úlohu 3.5.2c).)

Úloha 3.5.5. Ukážte, že $F_{2n} = \sum_{k=0}^{n} \binom{n}{k} F_k$. (Hint k maticovému odvodeniu: Skúste využiť rovnosť $A^2 = I + A$.)

Úloha 3.5.6. Nájdite vzorec pre F_{j+k+l} a pre F_{3n}.

V zostávajúcich úlohách budeme používať aj iné postupy ako použitie matíc. Cieľom je ukázať niektoré zaujímavé vlastnosti Fibonacciho postupnosti.

Úloha 3.5.7. a) Vyjadrite F_{n+3} a F_n pomocou F_{n+1} a F_{n+2}.
b) Ukážte, že $F_{n+2}^2 - F_{n+1}^2 = F_n F_{n+3}$ platí pre ľubovoľné $n \in \mathbb{N}$.

Úloha 3.5.8. Lucasova postupnosť je postupnosť určená predpisom $L_{n+1} = L_n + L_{n-1}$ a podmienkami $L_0 = 2$, $L_1 = 1$.
a) Nájdite vyjadrenie n-tého člena Lucasovej postupnosti.
b) Ukážte, že $L_n = F_{n-1} + F_{n+1}$.

Úloha 3.5.9. Ukážte, že pre Fibonacciho postupnosť platí:
a) $F_n \mid F_{kn}$,
b) $(F_n, F_{n+1}) = 1$,
c) $(F_{kn+r}, F_n) = (F_r, F_n)$,
d) $(F_m, F_n) = F_{(m,n)}$.

Koľko delení so zvyškom je potrebné vykonať, ak hľadáme (F_n, F_{n-1}) pomocou Euklidovho algoritmu?

3.5.2 Sústavy lineárnych homogénnych diferenciálnych rovníc

V tejto časti sa budeme zaoberať sústavami lineárnych homogénnych diferenciálnych rovníc. Pre jednoduchosť sa opäť obmedzíme na sústavy 2 rovníc. Sú to teda sústavy tvaru

$$x'(t) = ax(t) + by(t)$$
$$y'(t) = cx(t) + dy(t)$$

pričom $a, b, c, d \in \mathbb{C}$ sú konštanty, $x(t), y(t)$ sú hľadané funkcie reálnej premennej a všetky derivácie vystupujúce v sústave chápeme ako derivácie podľa t.

Stručnejšie budeme predchádzajúcu sústavu zapisovať ako

$$\begin{aligned} x' &= ax + by \\ y' &= cx + dy \end{aligned} \tag{3.18}$$

Budeme využívať to, že vieme, že riešením diferenciálnej rovnice

$$u' = ku$$

pre dané $k \in \mathbb{R}$ je funkcia

$$u(t) = Ce^{kt},$$

pričom $C = u(0)$. (Ľahko overíme, že táto funkcia danej rovnici skutočne vyhovuje. Akonáhle je dané $u(0)$, je tým už funkcia u jednoznačne určená.)

Pozrime sa najprv na nasledujúci jednoduchý príklad, kde sa dá uhádnuť ako môžeme sústavu previesť na tvar, ktorý už vieme riešiť.

Príklad 3.5.3. Riešme sústavu

$$\begin{aligned} x' &= x + 2y \\ y' &= 2x + y \end{aligned}$$

Upravme túto sústavu tak, že jednotlivé rovnice sčítame a odčítame. Dostaneme tak rovnice

$$\begin{aligned} x' + y' &= 3x + 3y \\ x' - y' &= -x + y \end{aligned}$$

čiže

$$\begin{aligned} (x + y)' &= 3(x + y) \\ (x - y)' &= -(x - y) \end{aligned}$$

Z týchto 2 rovníc máme

$$\begin{aligned} x + y &= c_1 e^{3t} \\ x - y &= c_2 e^{-t} \end{aligned}$$

a po vyjadrení x a y dostaneme riešenie

$$\begin{aligned} x &= a_1 e^{3t} + a_2 e^{-t} \\ y &= a_1 e^{3t} - a_2 e^{-t} \end{aligned}$$

(Kvôli „krajšiemu“ zápisu sme zaviedli nové konštanty $a_{1,2}$ také, že $c_1 = 2a_1$, $c_2 = 2a_2$.)

Dosadením do pôvodnej rovnice sa ľahko presvedčíme, že je to skutočne riešenie pôvodnej sústavy.

Opäť, podobne ako v prípade rekurencií, vieme sústavu (3.18) zapísať maticovo ako

$$(x', y') = (x, y)A \tag{3.19}$$

pričom

$$A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

Všimnime si, čo sme vlastne v predchádzajúcom príklade urobili. Najprv sme zaviedli nové funkcie u a v (zmena súradníc), pre ktoré sme sústavu vedeli riešiť, a potom sme urobili opačnú zmenu súradníc, aby sme dostali riešenie pre pôvodné funkcie. To presne zodpovedá podobnosti matíc – pri nej tiež robíme zmenu súradníc P a zmenu súradníc opačným smerom P^{-1}. Na tento problém sa teda možno pozerať tak, že hľadáme maticu podobnú matici A, pričom chceme, aby táto matica (a tým pádom aj zodpovedajúca sústava) boli čo najjednoduchšie. Vhodným kandidátom by mohol byť Jordanov normálny tvar.

Čo dostaneme ak maticu P prevedieme na Jordanov normálny tvar? Máme potom

$$(x', y') = (x, y)P^{-1}JP$$

čiže

$$(x', y')P^{-1} = (x, y)P^{-1}J.$$

Uvažujme nové funkcie $u(t)$ a $v(t)$ určené ako

$$(u, v) = (x, y)P^{-1}.$$

Z nich vieme vyrátať hľadané funkcie x a y a získali sme pre ne o čosi jednoduchšiu sústavu

$$(u', v') = (u, v)J.$$

Rozmyslime si aspoň najjednoduchší prípad, matica J je diagonálna a obe vlastné hodnoty sú reálne čísla. Potom sústava, ktorej majú vyhovovať u a v je

$$u' = \lambda_1 u$$
$$v' = \lambda_2 v$$

a jej riešenie je

$$u = c_1 e^{\lambda_1 t}$$
$$v = c_2 e^{\lambda_2 t}$$

Riešenia pôvodnej sústavy dostaneme vynásobením sprava maticou P.

$$(x(t), y(t)) = (c_1 e^{\lambda_1 t}, c_2 e^{\lambda_2 t})P$$

Keď riadky matice P (čo sú súčasne vlastné vektory matice A) označíme ako $\vec{\alpha}_1$, $\vec{\alpha}_2$, tak predchádazjúca rovnosť znamená

$$(x(t), y(t)) = c_1 e^{\lambda_1 t}\vec{\alpha}_1 + c_2 e^{\lambda_2 t}\vec{\alpha}_2,$$

čiže riešenia pôvodnej sústavy sú lineárne kombinácie riešení $e^{\lambda_1 t}\vec{\alpha}_1$ a $e^{\lambda_2 t}\vec{\alpha}_2$.

Viac o riešení sústav lineárnych diferenciálnych rovníc a tiež spôsob, akým sa riešia prípady komplexných alebo viacnásobných vlastných hodnôt, možno nájsť napríklad v [GŠŠ].

3.6 PageRank algoritmus

V tejto časti chceme z hľadiska lineárnej algebry popísať PageRank algoritmus, ktorý sa dá použiť na ohodnotenie dôležitosti webových stránok. Je dôležitý pri vyhľadávaní na zoradenie výsledkov. Podrobnejšie o tejto téme sa môžete dozvedieť napríklad v článku [BL] alebo v knihe [LM] (táto podkapitola spracovaná z týchto dvoch zdrojov a z [Me]). Ďalším

dostupným zdrojom je bakalárska práca [Mi], v ktorej nájdete dokázaný i všeobecný prípad niektorých tvrdení, ktoré tu dokážeme iba v zjednodušenom prípade, že ide o matice podobné s diagonálnou maticou.

Autormi tohoto algoritmu sú zakladatelia firmy Google Sergey Brin a Larry Page, začali na ňom pracovať v druhej polovici 90-tych rokov. Oproti dovtedy používaným spôsobom hodnotenia dôležitosti nájdených výsledkov je významným rozdielom to, že dôležitosť sa tu neurčuje na základe obsahu stránky, ale podľa hypertextových odkazov na danú stránku z iných stránok. Približne v tom istom čase navrhol Jon Kleinberg algoritmus HITS, ktorý bol do značnej miery podobný, nesnažil sa ho však komerčne využiť. V súčasnosti niektoré vyhľadávače používajú tento algoritmus. Hlavný rozdiel medzi oboma algoritmami je v tom, že HITS okrem liniek smerujúcich na danú stránku zohľadňuje aj linky, ktoré smerujú z nej.

V tejto súvislosti treba spomenúť, že PageRank nie je jediné kritérium, na základe ktorého Google vytvára poradie nájdených výsledkov.

Základná idea PageRank algoritmu sa dá popísať veľmi jednoducho. Ak dôležitosť posudzujeme podľa toho, koľko stránok sa na ňu odkazuje, môžeme sa na to pozrieť ako na „hlasovanie“. Každá stránka dostane 1 hlas a ak na nej je n liniek, tak s váhou $1/n$ hlasuje za dôležitosť stránok, na ktoré sa odkazuje. Teda každá stránka má rovnocenné „hlasovacie právo“, a hlas stránky sa rozdelí medzi tie, na ktoré odkazuje.

Znamená to, že dôležitosť stránky bude úmerná tomu, koľko liniek na ňu odkazuje.

Práve popísaný výpočet môžeme popísať veľmi jednoducho ako

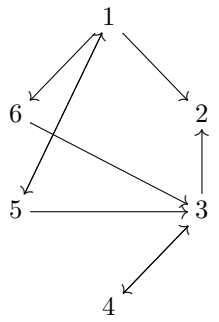
$$\vec{x} = \vec{e}A,$$

kde vektor $\vec{x} = (x_1, \ldots, x_n)$ obsahuje ohodnotenia stránok, $\vec{e} = (1, 1, \ldots, 1)$ a matica A je určená ako

$$a_{ij} = \begin{cases} \frac{1}{n_i} & \text{ak } i\text{-ta stránka obsahuje odkaz na } j\text{-tu,} \\ 0 & \text{inak.} \end{cases}$$

pričom n_i označuje počet liniek na i-tej stránke.

Napríklad pre web naznačený v nasledujúcom diagrame



vyzerá matica A ako

$$A = \begin{pmatrix} 0 & \frac{1}{3} & 0 & 0 & \frac{1}{3} & \frac{1}{3} \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

Poznamenajme, že aj v reálnych aplikáciach bude táto matica obsahovať veľa núl – ide o takzvanú *riedku maticu*. To prináša dve výhody – maticu možno uložiť (pomocou vhodnej

dátovej štruktúry) tak, aby nezaberala zbytočne veľa priestoru. Takisto niektoré výpočty, napríklad násobenie takouto maticou, možno implementovať tak, že budú oveľa rýchlejšie ako pre matice, ktoré majú skoro všetky hodnoty nenulové.

Nedostatok hodnotenia, ktoré získame doteraz popísaným spôsobom, je v tom, že sme rovnakú vážnosť prikladali linkám z menej dôležitých stránok ako linkám z významných stránok. Ako však odlíšiť významné a menej významné stránky a zabezpečiť, aby hlas dôležitých stránok zavážil viac? Môžeme jednoducho zobrať práve vypočítaný odhad pre dôležitosť ako váhy stránok a znovu urobiť to isté. To znamená, že budeme postupne počítať

$$\vec{x}_0 = \vec{e}$$
$$\vec{x}_1 = \vec{x}_0 A$$
$$\vec{x}_2 = \vec{x}_1 A = \vec{x}_0 A^2$$
$$\dots$$
$$\vec{x}_n = \vec{x}_{n-1} A = \vec{x}_0 A^n$$

V prípade, že váhový vektor $\vec{x}_n$ konverguje k nejakej limite, je pomerne prirodzené túto limitu považovať za ohodnotenie významnosti jednotlivých stránok.

Spomeňme ešte iný pohľad, ako možno interpretovať tieto výpočty. Dá sa na to hľadieť tak, že popisujeme browsovanie náhodného surfera, ktorý sa správa tak, že z niektorej stránky si náhodne vyberie ľubovoľnú linku a na tú stránku ide ďalej. Ak stránka neobsahuje žiadne linky, tak si náhodne vyberie ľubovoľnú stránku a zase browsuje ďalej. Takto možno považovať vektor, ku ktorému konverguje $\vec{x}_n$, chápať ako hodnotu pravdepodobnosti, že sa v danom okamihu surfer nachádza na danej stránke za predpokladu, že ho necháme surfovať neobmedzene dlho. (Aby sme boli presní, ak chceme použiť túto pravdepodobnostnú interpretáciu, použijeme $\vec{x}_0 = \frac{1}{n}\vec{e}$ alebo iný vektor, ktorý má kladné súradnice a ich súčet je 1 – pretože táto podmienka musí platiť pre pravdepodobnosť.) Práve tento pohľad dáva do súvisu PageRank algoritmus s markovovskými reťazcami. Tie sa študujú v teórii stochastických procesov, čo je matematická oblasť patriaca do teórie pravdepodobnosti.

Teraz sa budeme zaoberať tým, pre aké matice A si môžeme byť istý, že vektor $\vec{x}_n$ bude skutočne konvergovať k nejakej hodnote. Ako uvidíme, aby to fungovalo v praxi, bude potrebné maticu, ktorú sme práve popísali, ešte trochu upraviť.

Najprv si všimnime, že ak $\vec{x}_0 A^n$ konverguje k nejakému nenulovému vektoru, musí to byť vlastný vektor matice A prislúchajúci k vlastnej hodnote 1.

Ak totiž platí

$$\vec{x} = \lim_{n\to\infty} \vec{x}_0 A^n,$$

tak máme aj

$$\vec{x}A = \lim_{n\to\infty} \vec{x}_0 A^{n+1} = \vec{x}.$$

(Tu sme využili fakt, že v priestore $\mathbb{R}^n$ je každé lineárne zobrazenie spojité.[4] Lineárne zobrazenie je vlastne násobenie maticou A.)

Všimnime si, že súčet prvkov v každom nenulovom riadku matici A je rovný 1 (prvá iterácia bola demokratická – každá stránka mala rovnaké „hlasovacie právo“).

Definícia 3.6.1. Matica A sa nazýva *riadkovo stochastická,* ak súčet prvkov jej ľubovoľného riadku je 1.

[4]Stručné zdôvodnenie tohoto faktu: Ak označíme $\|A\|_{max} = \max_{i,j}|a_{ij}|$, tak očividne pre každý vektor $\vec{z}$ taký, že $\max|z_i| < \delta$ platí, že všetky súradnice vektora $\vec{z}A$ nepresahujú v absolútnej hodnote $\delta n\|A\|_{max}$. Takže ak máme dané $\varepsilon > 0$ a dvojicu vektorov takú, že pre všetky ich súradnice platí $|x_i - y_i| < \frac{\varepsilon}{n\|A\|_{max}}$, tak dostaneme $\vec{x}A - \vec{y}A = (\vec{x} - \vec{y})A < n\|A\|_{max}\frac{\varepsilon}{n\|A\|_{max}} = \varepsilon$.

Tvrdenie 3.6.2. *Ak matica A je riadkovo stochastická, tak číslo 1 je jej vlastnou hodnotou.*

Dôkaz. Stačí si všimnúť, že súčet stĺpcov matice $A - I$ je $\vec{0}$, čo znamená, že jej stĺpce sú lineárne závislé a táto matica je teda singulárna. □

Všimnime si ešte jednu vlastnosť riadkovo stochastických matíc – lineárne zobrazenie prislúchajúce takejto matici nemení súčet jednotlivých zložiek vektora.

Tvrdenie 3.6.3. *Nech A je riadkovo stochastická matica, $\vec{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$ a $\vec{y} = (y_1, \ldots, y_n) = \vec{x}A$. Potom platí $\sum_{i=1}^{n} y_i = \sum_{i=1}^{n} x_i$.*

Dôkaz. Máme

$$y_i = \sum_{j=1}^{n} a_{ji} x_j.$$

Sčítaním týchto rovníc dostaneme

$$\sum_{i=1}^{n} y_i = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ji} x_j = \sum_{j=1}^{n} x_j \sum_{i=1}^{n} a_{ji} = \sum_{j=1}^{n} x_j,$$

kde posledná rovnosť vyplýva z faktu, že súčet prvkov matice A v danom riadku je 1. □

Iný dôkaz. Fakt, že riadky majú súčet jedna, sa dá stručne jedným vzťahom vyjadriť ako

$$A\vec{e}^T = \vec{e}^T.$$

Všimnime si tiež, že súčet jednotlivých súradníc vektora je presne rovný skalárnemu súčinu $\vec{x}\vec{e}^T$. Potom dostaneme

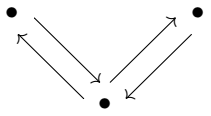
$$\vec{x}A\vec{e}^T = \vec{x}\vec{e}^T,$$

čo je presne dokazované tvrdenie. □

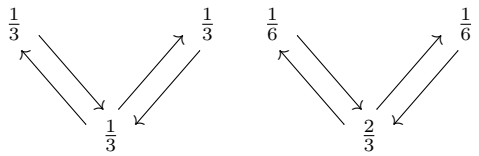
Z tvrdenia 3.6.2 teda vidíme, že keby sme v matici A nemali nulové riadky, mali by sme zaručenú existenciu aspoň jedného kadidáta na výsledné ohodnotenie. Aby sme dostali riadkovo stochastickú maticu, nahradíme každý nulový riadok vektorom $\frac{1}{n}\vec{e}$. (Na stránke bez liniek sa surfer rozhodne úplne náhodne pre ľubovoľnú stránku na internete.)

Zatiaľ však stále nemáme nijako zaručené, že vlastný vektor pre vlastné číslo 1 bude jediný a ani to, že k nemu budú naše vektory skutočne konvergovať.

Veľmi jednoduchý príklad ukazujúci, že tento proces nemusí konvergovať je takáto sieť



Pomerne ľahko vidíme, že ak na začiatku sú pravdepodobnosti výskytu v týchto troch vrcholoch $(\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$, tak v ďalšej iterácii dostaneme $(\frac{1}{6}, \frac{2}{3}, \frac{1}{6})$.



Zodpovedajúca matica je

$$\begin{pmatrix} 0 & 1 & 0 \\ \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 1 & 0 \end{pmatrix}.$$

Ak skontrolujeme, že vlastné hodnoty sú 0 a ± 1, tak pre zodpovedajúcu diagonálnu maticu máme $D^n = \mathrm{diag}(1, 0, (-1)^n)$; teda aj tu vidíme striedanie dvoch hodnôt.

Ukážeme, že vlastný podpriestor prislúchajúci k vlastnej hodnote 1 bude jednorozmerný, v prípade, že matica A mala všetky prvky kladné.

Lema 3.6.4. *Nech matica A je riadkovo stochastická a $a_{ij} > 0$ pre $i, j = 1, \ldots, n$. Potom každý jej vlastný vektor prislúchajúci k vlastnej hodnote 1 má všetky súradnice rovnakého znamienka (všetky nezáporné alebo všetky nekladné).*

Dôkaz. V dôkaze použijeme fakt, že nerovnosť $|\sum_{i=1}^n y_i| \leq \sum_{i=1}^n |y_i|$ je ostrá pre každý vektor obsahujúci prvky so zmiešanými znamienkami.

Budeme postupovať sporom. Nech by $\vec{x}A = \vec{x}$ a vektor $\vec{x}$ má na niektorých súradniciach rôzne znamienka. Potom máme ostré nerovnosti

$$|x_i| = \left| \sum_{j=1}^n a_{ji} x_j \right| < \sum_{j=1}^n a_{ji} |x_j|.$$

Sčítaním týchto nerovností dostaneme

$$\sum_{i=1}^n |x_i| < \sum_{i=1}^n \sum_{j=1}^n a_{ji} |x_j| = \sum_{j=1}^n |x_j| \sum_{i=1}^n a_{ji} = \sum_{j=1}^n |x_j|.$$

(V poslednej rovnosti sme využili, že súčet prvkov j-teho riadku matice a je 1.)

Dostali sme nerovnosť

$$\sum_{i=1}^n |x_i| < \sum_{j=1}^n |x_j|,$$

čo je samozrejme spor. □

Veľmi podobným spôsobom ako v predchádzajúcej leme môžeme odvodiť nasledujúci fakt, ktorý bude neskôr užitočný pri dôkaze konvergencie použitej metódy.

Lema 3.6.5. *Nech matica A je riadkovo stochastická a $a_{ij} \geq 0$ pre $i, j = 1, \ldots, n$. Ak λ je jej vlastná hodnota, tak $|\lambda| \leq 1$.*

Dôkaz. Pre vlastnú hodnotu λ a príslušný vlastný vektor máme.

$$\lambda x_i = \sum_{j=1}^n a_{ji} x_j$$

$$|\lambda| |x_i| = \left| \sum_{j=1}^n a_{ji} x_j \right| \leq \sum_{j=1}^n a_{ji} |x_j|$$

Sčítaním týchto nerovností dostaneme

$$|\lambda| \sum_{i=1}^n |x_i| \leq \sum_{i=1}^n \sum_{j=1}^n a_{ji} |x_j| = \sum_{j=1}^n |x_j| \sum_{i=1}^n a_{ji} = \sum_{j=1}^n |x_j|$$

$$|\lambda| \leq 1$$

(V poslednom kroku sme využili, že $\vec{x} \neq \vec{0}$, čiže aj $\sum_{j=1}^n |x_j| \neq 0$.) □

Lema 3.6.6. *Ak $\vec{\alpha}$, $\vec{\beta}$ sú lineárne nezávislé vektory, tak existujú koeficienty $c, d \in \mathbb{R}$ také, že $c\vec{\alpha} + d\vec{\beta}$ obsahuje prvky so zmiešanými znamienkami.*

Dôkaz. Ak pre vektor $\vec{\alpha} = (a_1, \ldots, a_n)$ platí $\sum_{i=1}^{n} a_i = 0$, tak tento vektor obsahuje zmiešané znamienka (keďže je nenulový) a stačí zvoliť $c = 1$ a $d = 0$. Podobne v prípade, že to platí pre vektor $\vec{\beta}$.

Ak žiadny z vektorov nedáva nulový súčet, stačí nám zvoliť c a d tak, aby $c\sum_{i=1}^{n} a_i + d\sum_{i=1}^{n} b_i = 0$. Lineárna nezávislosť zabezpečí to, že vektor $c\vec{\alpha} + d\vec{\beta}$ je nenulový, dostávame teda, že znamienka jeho súradníc nemôžu byť všetky rovnaké. □

Dôsledok 3.6.7. *Ak A je riadkovo stochastická matica, ktorej prvky sú kladné, tak podpriestor tvorený vlastnými vektormi k vlastnému číslu 1 je jednorozmerný.*

Aby matica A mala všetky členy kladné, zabezpečíme tak, že namiesto pôvodnej matice použijeme maticu

$$G = \alpha A + (1 - \alpha)\frac{1}{n}\vec{e}^T\vec{e},$$

kde $\alpha \in (0, 1)$. Všimnime si, že aj matica G je riadkovo stochastická.

V predchádzajúcej rovnosti sme skombinovali maticu A s maticou $\frac{1}{n}\vec{e}^T\vec{e}$, ktorá na každom svojom mieste obsahuje hodnotu $\frac{1}{n}$. Zodpovedá to tomu, že náhodne sa pohybujúci surfer sa v nejakom percente prípadov (určenom koeficientom $1 - \alpha$) rozhodne nepokračovať linkou zo stránky, na ktorej sa nachádza, ale vyberie si novú stránku úplne náhodne. (Z takejto interpretácie vidno aj to, že „náhodnému surferovi“ týmto zabránime zacykliť sa. Cykly, podobne ako stránky, z ktorých nevychádzajú linky, by spôsobili, že pravdepodobnosť výskytu stránky pri náhodnom surfovaní – a teda jej váha – sa nám pri iteráciách postupne naakumuluje vo vrcholoch cyklu.) Súčasne sme touto zmenou nezvýhodnili niektorú stránku oproti iným (všade sme pripočítali rovnakú hodnotu).

Neskôr ukážeme, že nastavenie parametra α ovplyvňuje rýchlosť konvergencie k hľadanému riešeniu a tým aj počet krokov potrebných na dosiahnutie dostatočnej presnosti. Okrem toho na tomto parametre závisí aj citlivosť metódy na zmenu matice A.

Vďaka tomu, že súčet použitých koeficientov je 1 a obe matice sú riadkovo stochastické, aj výsledná matica je riadkovo stochastická.

Na prvý pohľad by sa mohlo zdať, že sme touto zmenou matice stratili výhodu, ktorú nám prinášala riedkosť matice A. Keďže sme ale pripočítali maticu, ktorá má všetky prvky rovnaké, je jasné, že ju nemusíme mať v pamäti uloženú po jednotlivých prvkoch a aj to, že násobiť takouto maticou sa tiež dá dosť jednoducho.

Už teda vieme, že ak bude $\vec{x_0}A^n$ konvergovať, môže konvergovať jedine k hľadanej vlastnej hodnote. Pre jednoduchosť konvergenciu overíme len pre diagonalizovateľné matice. Na to najprv dokážeme vetu o spektrálnom rozklade diagonalizovateľnej matice.

Veta 3.6.8. *Ak je matica A typu $n \times n$ podobná s diagonálnou maticou* $\operatorname{diag}(\lambda_1, \ldots, \lambda_n)$*, tak existujú matice $G_1, \ldots, G_n$ také, že platí*

$$A = \lambda_1 G_1 + \lambda_2 G_2 + \cdots + \lambda_n G_n$$

a súčasne

$$G_1 + \cdots + G_n = I,$$

pre každé i platí $G_i^2 = G_i$ a pre $i \neq j$ platí $G_i G_j = 0$.

Všimnime si, že z podmienok uvedených v predchádzajúcej vete vyplýva

$$A^k = \lambda_1^k G_1 + \lambda_2^k G_2 + \cdots + \lambda_n^k G_n.$$

Dôkaz. Podľa predpokladu existuje regulárna matica P taká, že $PAP^{-1} = D$, čiže $P^{-1}DP = A$. Označme stĺpce matice P^{-1} ako $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ a riadky matice P ako $\vec{\beta}_1, \ldots, \vec{\beta}_n$.

$$P^{-1} = (\vec{\alpha}_1^T, \ldots, \vec{\alpha}_n^T) \qquad P = \begin{pmatrix} \vec{\beta}_1 \\ \vdots \\ \vec{\beta}_n \end{pmatrix}$$

Z rovnosti $P^{-1}DP = A$ potom dostaneme (podobným spôsobom ako v dôkaze (3.5))

$$A = (\vec{\alpha}_1^T, \ldots, \vec{\alpha}_n^T) \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} \begin{pmatrix} \vec{\beta}_1 \\ \vdots \\ \vec{\beta}_n \end{pmatrix} = \lambda_1 \vec{\alpha}_1^T \vec{\beta}_1 + \cdots + \lambda_n \vec{\alpha}_n^T \vec{\beta}_n.$$

Označme $G_i = \vec{\alpha}_i^T \vec{\beta}_i$. Takto definované G_i sú matice $n \times n$ a platí pre ne $A = \lambda_1 G_1 + \lambda_2 G_2 + \cdots + \lambda_n G_n$.

Overme, že platia aj ostatné rovnosti uvedené vo vete. Rovnosť $I = P^{-1}P$ môžeme prepísať ako

$$I = (\vec{\alpha}_1^T, \ldots, \vec{\alpha}_n^T) \begin{pmatrix} \vec{\beta}_1 \\ \vdots \\ \vec{\beta}_n \end{pmatrix} = \vec{\alpha}_1^T \vec{\beta}_1 + \cdots + \vec{\alpha}_n^T \vec{\beta}_n = G_1 + \cdots + G_n.$$

Ak násobíme PP^{-1}, tak dostaneme

$$I = \begin{pmatrix} \vec{\beta}_1 \\ \vdots \\ \vec{\beta}_n \end{pmatrix} (\vec{\alpha}_1^T, \ldots, \vec{\alpha}_n^T) = \begin{pmatrix} \vec{\beta}_1 \vec{\alpha}_1^T & \ldots & \vec{\beta}_1 \vec{\alpha}_n^T \\ \ldots & \ldots & \ldots \\ \vec{\beta}_n \vec{\alpha}_1^T & \ldots & \vec{\beta}_n \vec{\alpha}_n^T \end{pmatrix}$$

Porovnaním oboch matíc dostaneme $\vec{\beta}_i \vec{\alpha}_i^T = 1$ a $\vec{\beta}_i \vec{\alpha}_i^T = 0$ pre $i \neq j$. To znamená, že

$$G_i^2 = \vec{\alpha}_i^T (\vec{\beta}_i \vec{\alpha}_i^T) \vec{\beta}_i = \vec{\alpha}_i^T \vec{\beta}_i = G_i$$

a

$$G_i G_j = \vec{\alpha}_i^T (\vec{\beta}_i \vec{\alpha}_j^T) \vec{\beta}_j = \vec{\alpha}_i^T . 0 . \vec{\beta}_j = 0.$$

□

Z vety o spektrálnom rozklade dostaneme, v prípade, že naša matica je diagonalizovateľná,

$$A^k = G_1 + \lambda_2^k G_2 + \cdots + \lambda_n^k G_n$$

a

$$\vec{x_0} A^k = \vec{x_0} G_1 + \lambda_2^k \vec{x_0} G_2 + \cdots + \lambda_n^k \vec{x_0} G_n$$

Z nasledujúceho tvrdenia vyplynie, že vlastné hodnoty $\lambda_2, \ldots, \lambda_n$ sú v absolútnej hodnote ostro menšie ako 1, čiže pre ne platí $\lambda_i^k \longrightarrow 0$. To znamená, že uvedený výraz skutočne konverguje.

Z predchádzajúcej rovnice vidíme tiež, že rýchlosť konvergencie závisí od vlastnej hodnoty, ktorá je druhá najväčšia v absolútnej hodnote. Nasledujúce tvrdenie súčasne ukazuje, že veľkosť tejto vlastnej hodnoty (a teda aj rýchlosť konvergencie) závisí od parametra α.

Tvrdenie 3.6.9. *Nech A je riadkovo stochastická matica a jej vlastné čísla sú $1, \lambda_2, \ldots, \lambda_n$. Potom matica*

$$G = \alpha A + (1-\alpha)\frac{1}{n}\vec{e}^T\vec{e}$$

má vlastné hodnoty $1, \alpha\lambda_2, \ldots, \alpha\lambda_n$.

Dôkaz. Skutočnosť, že súčty v riadkoch matice A sú rovné 1, je ekvivalentná s rovnosťou

$$A\vec{e}^T = \vec{e}^T.$$

Nech Q je ľubovoľná regulárna matica, ktorej prvý stĺpec je $\vec{e}^T$.

$$Q = (\vec{e}^T, X)$$

Ak prvý riadok inverznej matice Q^{-1} označíme $\vec{y}$, tak máme

$$Q^{-1}Q = \begin{pmatrix}\vec{y}\\ Y\end{pmatrix}(\vec{e}^T, X) = \begin{pmatrix}\vec{y}\vec{e}^T & \vec{y}X\\ Y\vec{e}^T & YX\end{pmatrix} = \begin{pmatrix}1 & \vec{0}\\ \vec{0}^T & I\end{pmatrix}. \tag{3.20}$$

(Všimnime si, že X a Y nie sú štvorcové matice, takže rovnosť $YX = I$ vyplývajúca z predchádzajúcej rovnosti neznamená, že tieto matice sú navzájom inverzné.)

Ak vynásobíme týmito maticami maticu A, tak dostaneme

$$Q^{-1}AQ = \begin{pmatrix}\vec{y}\\ Y\end{pmatrix}A(\vec{e}^T, X) = \begin{pmatrix}\vec{y}A\\ YA\end{pmatrix}(\vec{e}^T, X) = \begin{pmatrix}\vec{y}A\vec{e}^T & \vec{y}AX\\ YA\vec{e}^T & YAX\end{pmatrix}$$

Súčasne použitím (3.20) dostaneme

$$\vec{y}A\vec{e}^T = \vec{y}\vec{e}^T = 1$$

a

$$YA\vec{e}^T = Y\vec{e}^T = \vec{0}^T.$$

Dostali sme teda

$$Q^{-1}AQ = \begin{pmatrix}1 & \vec{y}AX\\ \vec{0}^T & YAX\end{pmatrix}.$$

Z poslednej rovnosti a z toho, čo vieme o vlastných hodnotách matice A, vyplýva, že matica YAX je podobná s hornou trojuholníkovou maticou, ktorá má na diagonále hodnoty $\lambda_2, \ldots, \lambda_n$. (Stačí si všimnúť, že pre hornú trojuholníkovú maticu je charakteristický polynóm jednoznačne určený hodnotami na diagonále. Jordanov normálny tvar ľubovoľnej matice je horná trojuholníková matica.)

Vypočítajme teraz to isté pre maticu $\vec{e}^T\vec{e}$. Dostaneme

$$Q^{-1}\vec{e}^T\vec{e}Q = \begin{pmatrix}\vec{y}\\ Y\end{pmatrix}\vec{e}^T\vec{e}(\vec{e}^T, X) = \begin{pmatrix}\vec{y}\vec{e}^T\\ Y\vec{e}^T\end{pmatrix}(\vec{e}\vec{e}^T, \vec{e}X) = \begin{pmatrix}1\\ \vec{0}^T\end{pmatrix}(n, \vec{e}X) = \begin{pmatrix}n & \vec{e}X\\ \vec{0}^T & 0\end{pmatrix}$$

Pre maticu G potom dostaneme

$$Q^{-1}GQ = \alpha Q^{-1}AQ + (1-\alpha)\frac{1}{n}Q^{-1}\vec{e}^T\vec{e}Q =$$
$$\alpha\begin{pmatrix}1 & \vec{y}AX\\ \vec{0}^T & YAX\end{pmatrix} + (1-\alpha)\begin{pmatrix}1 & \frac{1}{n}\vec{e}X\\ \vec{0}^T & 0\end{pmatrix} = \begin{pmatrix}1 & \alpha\vec{y}AX + (1-\alpha)\frac{1}{n}\vec{e}X\\ \vec{0}^T & \alpha YAX\end{pmatrix}$$

Matica αYAX je podobná s hornou trojuholníkovou maticou, ktorá má na diagonále prvky $\alpha\lambda_1, \ldots, \alpha\lambda_n$, z čoho už vyplýva dokazované tvrdenie. □

Hodnota α, ktorú Google reálne používa, je $0,85$. Vďaka tomu veľkosť druhej najväčšej vlastnej hodnoty je nanajvýš $0,85$. Všímnime si, že čím menšiu hodnotu α zvolíme, tým rýchlejšie bude táto metóda konvergovať, spôsobíme tým však súčasne to, že nad maticou A popisujúcou vzhľad webu prevládne matica $\frac{1}{n}\vec{e}\vec{e}^T$, ktorú sme pridali umelo na zabezpečenie konvergencie.

Kapitola 4

Okruhy a polynómy

4.1 Okruhy (a súvisiace pojmy)

Definícia 4.1.1. Trojicu $(R, +, \cdot)$ nazývame *okruh* ak $+$ a $\cdot$ sú binárne operácie na množine R také, že

(i) $(R, +)$ je komutatívna grupa,

(ii) operácia $\cdot$ je asociatívna[1],

$$(\forall a, b, c \in R) \qquad a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

(iii) pre operácie $+$ a $\cdot$ platia *distributívne zákony*

$$(\forall a, b, c \in R) \qquad a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(\forall a, b, c \in R) \qquad (b + c) \cdot a = b \cdot a + c \cdot a$$

Neutrálny prvok operácie $+$ budeme označovať 0. Podobne ako sme to robili pre polia, inverzný prvok k prvku a vzhľadom na operáciu $+$ budeme označovať $-a$. Označenie $b - a$ bude znamenať $b + (-a)$.

Ak je navyše operácia $\cdot$ komutatívna, t.j.

$$(\forall a, b \in R) \qquad a \cdot b = b \cdot a,$$

tak $(R, +, \cdot)$ voláme *komutatívny okruh.*

Ak existuje neutrálny prvok e operácie $\cdot$ a súčasne $e \neq 0$ (ako sme sa dohodli, 0 označuje neutrálny prvok operácie $+$), tak tento neutrálny prvok označujeme 1 a hovoríme že, že $(R, +, \cdot)$ je (*komutatívny*) *okruh s jednotkou.*[2]

Poznámka 4.1.2. Označenie pre operáciu $\cdot$ obvykle vynechávame, čiže namiesto $a \cdot b$ častejšie budeme používať označenie ab.

[1] t.j. $(R, \cdot)$ je pologrupa

[2] Prípad, že neutrálny prvok oboch operácií je ten istý, ktorý sme z tejto definície vylúčili, nastane iba pre jednoprvkový okruh $\{0\}$.
Z minulého semestra vieme, že jednotka v okruhu musí byť jednoznačne určená – tvrdenie I-3.1.7.
V niektorých učebniciach sa v definícii okruhu s jednotkou nepožaduje podmienka $1 \neq 0$, potom sa však táto podmienka objaví ako jeden z predpokladov vo väčšine viet, ktoré o okruhoch s jednotkou dokazujeme, preto sme tu zvolili túto formu definície.

Takisto, keď budú uvažované binárne operácie jasné z kontextu, budeme písať stručne R namiesto $(R, +, \cdot)$.

Pri grupách sme spomínali aditívny a multiplikatívny zápis – v okruhu vždy pre operáciu $+$ používame aditívny a pre operáciu $\cdot$ multiplikatívny zápis. Teda použitie operácie viackrát na ten istý prvok označíme ako $n \times a$ pre operáciu $+$ a a^n pre operáciu $\cdot$ (kde $n \in \mathbb{N} \setminus \{0\}$).

Príklad 4.1.3. $(\mathbb{Z}, +, \cdot)$ – celé čísla s obvyklým sčitovaním a násobením tvoria komutatívny okruh s jednotkou.
$(\mathbb{Z}_n, \oplus, \odot)$ – množina $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ so sčitovaním modulo n tvorí komutatívny okruh s jednotkou.

Príklad 4.1.4. Príklad komutatívneho okruhu, ktorý nemá jednotku: $(2\mathbb{Z}, +, \cdot)$.

Dôkaz nasledujúcej lemy ponechávame ako cvičenie, keďže je veľmi podobný dôkazom, ktoré sme robili pre polia.

Lema 4.1.5. *Nech $(R, +, \cdot)$ je okruh, $a, b \in R$. Potom platí*

$$0a = a0 = 0$$
$$a(-b) = -ab = (-a)b$$
$$(-a)(-b) = ab$$

Príklad 4.1.6. Na množine $\mathbb{Z} \times \mathbb{Z}$ definujeme operácie $+$ a $\cdot$ ako sčitovanie a násobenie po zložkách, t.j.

$$(a, b) + (a', b') = (a + a', b + b'),$$
$$(a, b)(a', b') = (aa', bb').$$

Potom $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$ je komutatívny okruh s jednotkou. (Jednotka je dvojica $(1, 1)$, nula je dvojica $(0, 0) = 0$.)

Všimnime si, že $(1, 0) \cdot (0, 1) = (0, 0)$, teda v okruhu môže byť súčin nenulových prvkov rovný nule.

Predchádzajúci príklad možno jednoducho zovšeobecniť:

Príklad 4.1.7. Ak $(R_1, +, \cdot)$ a $(R_2, +, \cdot)$ sú okruhy, tak $R_1 \times R_2$ tvorí s operáciami definovanými po zložkách

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$$
$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 \cdot b_1, a_2 \cdot b_2)$$

tiež okruh.

Podobne, ak pre každé $i \in M$ je $(R_i, +, \cdot)$ okruh, tak aj množina[3] $\prod_{i \in M} R_i = \{f \colon M \to \bigcup_{i \in M} R_i \mid (\forall i \in M)(f(i) \in R_i)\}$ tvorí s operáciami definovanými po zložkách

$$(f + g)(i) = f(i) + g(i)$$
$$(f \cdot g)(i) = f(i) \cdot g(i)$$

okruh.

V prípade, že všetky použité okruhy sú rovnaké, t.j. $R_i = R$ pre každé $i \in M$, budeme používať označenie R^M. Okruh R^M pozostáva zo všetkých zobrazení z M do R.

[3]Takto sa definuje karteziánsky súčin pre ľubovoľný (teda nie len konečný) počet množín. V prípade, že ste to nemali na žiadnom inom predmete, bude asi jednoduchšie, keď túto definíciu budete čítať tak, ako keby $R_i = R$ pre všetky $i \in M$ – pozri poznámku na konci tohoto príkladu.

Príklad 4.1.8. Dôležitý príklad okruhu tvoria matice $M_{n,n}(F)$ typu $n \times n$ nad poľom F spolu s násobením matíc. To, že sčitovanie a násobenie matíc spĺňajú podmienky z definície okruhu, sme ukázali v minulom semestri. Tento okruh má jednotku, je ňou jednotková matica I. Tento okruh nie je komutatívny.

Definícia 4.1.9. Nech $(R, +, \cdot)$ je okruh a $S \subseteq R$ je neprázdna podmnožina množiny R. Hovoríme, že S je *podokruh* okruhu R, ak pre ľubovoľné $a, b \in S$ platí $a - b \in S$, $ab \in S$.

$$a, b \in S \qquad \Rightarrow \qquad a - b \in S, ab \in S$$

Inými slovami, podokruh je podgrupa grupy $(R, +)$, ktorá je navyše uzavretá vzhľadom na násobenie.

Pomerne jednoducho sa dá overiť, že platí

Tvrdenie 4.1.10. *Nech $(R, +, \cdot)$ je okruh a $S \subseteq R$, $S \neq \emptyset$. Množina S je podokruh okruhu $(R, +, \cdot)$ práve vtedy, keď S s operáciami $+$ a $\cdot$ zúženými na množinu S tvorí okruh.*

Príklad 4.1.11. $2\mathbb{Z}$ je podokruh $(\mathbb{Z}, +, \cdot)$.

$\mathbb{N}$ nie je podokruh $(\mathbb{Z}, +, \cdot)$ (je uzavretý na násobenie a súčet, nie však na rozdiel).

Príklad 4.1.12. Uvažujme zobrazenia z uzavretého intervalu $\langle 0, 1\rangle$ do $\mathbb{R}$. Z matematickej analýzy vieme, že rozdiel a súčin spojitých funkcií je opäť spojitá funkcia. Vďaka tomu spojité funkcie $f\colon \langle 0, 1\rangle \to \mathbb{R}$ tvoria, so sčitovaním a násobením funkcií po bodoch, podokruh okruhu $\mathbb{R}^{\langle 0,1\rangle}$. Tento okruh označujeme $C(0, 1)$.

Definícia 4.1.13. Ak v okruhu $(R, +, \cdot)$ neexistujú prvky a, b také, že $a, b \neq 0$ a

$$ab = 0,$$

tak hovoríme, že R je *okruh bez deliteľov nuly* (alebo tiež, že R nemá delitele nuly).

Ak $(R, +, \cdot)$ je komutatívny okruh s jednotkou bez deliteľov nuly, hovoríme, že $(R, +, \cdot)$ je *obor integrity.*

Fakt, že R je okruh bez deliteľov nuly môžeme vyjadriť pomocou nasledovnej implikácie[4]

$$(\forall a, b \in R) \qquad ab = 0 \Rightarrow a = 0 \vee b = 0.$$

Príklad okruhu, ktorý nie je oborom integrity, je okruh $\mathbb{Z} \times \mathbb{Z}$ z príkladu 4.1.6. Dokonca ľubovoľný okruh tvaru $R_1 \times R_2$ (pozri príklad 4.1.7), kde ani jeden z okruhov R_1, R_2 nie je nulový, nám dáva takýto príklad.

Ľahko sa overí, že v okruhu bez deliteľov nuly môžeme krátiť nenulovými prvkami:

Tvrdenie 4.1.14. *Nech R je okruh bez deliteľov nuly a $a, b, c \in R$. Ak $a \neq 0$ a platí $ab = ac$, tak $b = c$.*

Dôkaz. Z rovnosti $ab = ac$ dostaneme pomocou distributívnosti $a(b - c) = 0$. Keďže $a \neq 0$, máme $b - c = 0$, a teda $b = c$. □

Definícia 4.1.15. Okruh R s jednotkou nazývame *telesom,* ak ku každému nenulovému prvku $a \in R \setminus \{0\}$ existuje inverzný prvok vzhľadom na násobenie, t.j.

$$(\forall a \in R \setminus \{0\})(\exists b \in R) \qquad ab = ba = 1$$

Komutatívne teleso voláme *pole.*

[4] Je to negácia výroku $(\exists a, b \in \mathbb{R})\ \ ab = 0 \wedge (a \neq 0 \wedge b \neq 0)$.

Tvrdenie 4.1.16. *Každé teleso je okruh bez deliteľov nuly.*
Každé pole je oborom integrity.

Dôkaz. Nech R je teleso a pre $a, b \in R$ platí $ab = 0$. Predpokladajme, že $a \neq 0$. Potom existuje $c \in R$ taký, že $ca = 1$. Z toho dostaneme

$$b = 1b = cab = c0 = 0,$$

čiže $b = 0$. Podobne, z predpokladu $b \neq 0$ by sme dostali $a = 0$.
Druhá časť tvrdenia ľahko vyplýva z prvej časti. □

Definícia 4.1.15 vlastne hovorí, že ak $(R, +, \cdot)$ je okruh a navyše $(R \setminus \{0\}, \cdot)$ je grupa, ide o teleso. Ak je to komutatívna grupa, ide o pole. Táto definícia poľa je teda ekvivalentná s definíciou I-3.3.1, ktorú sme uviedli v minulom semestri. Z minulého semestra poznáme veľa príkladov polí – $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ s obvyklým sčitovaním a násobením, $(\mathbb{Z}_p, \oplus, \odot)$ pre ľubovoľné prvočíslo p.

Príkladom telesa, ktoré nie je poľom (t.j. nekomutatívneho telesa) sú kvaternióny. Viac sa o nich môžete dozvedieť v [KGGS, Kapitola 4.7].

Cvičenia

Úloha 4.1.1. Zistite (a svoje tvrdenie zdôvodnite) ktoré z uvedených vlastností sa z okruhu R prenesú na uvedené konštrukcie: [5]

	$R \times R$	R/I	R^M	podokruh
pole				
obor integrity				
nemá delitele nuly				
má delitele nuly				
komutatívny okruh				
okruh s jednotkou				

Úloha 4.1.2. Je každý podokruh poľa okruh bez deliteľov nuly? Je každý podokruh poľa obsahujúci 1 oborom integrity?

Úloha 4.1.3. Zistite, či nasledujúce množiny tvoria podokruhy poľa $(\mathbb{C}, +, \cdot)$. Zistite, ktoré z nich sú navyše poliami.
a) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}; a, b \in \mathbb{Z}\}$
b) $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$

Úloha 4.1.4. Zistite, či nasledujúce množiny tvoria podokruhy poľa $(\mathbb{Q}, +, \cdot)$. Sú niektoré z nich polia?
a) Všetky zlomky také, že v základnom tvare je menovateľ nepárne číslo.
b) Všetky zlomky také, že v základnom tvare je menovateľ párne číslo.
c) Všetky zlomky také, že v základnom tvare je čitateľ nepárne číslo.
d) Všetky zlomky také, že v základnom tvare je čitateľ párne číslo.
e) Všetky druhé mocniny racionálnych čísel.

Úloha 4.1.5. Dokážte: Ak R je obor integrity a $x^2 = 1$, tak $x = 1$ alebo $x = -1$.

[5] Označenie R/I označuje faktorový okruh okruhu R podľa ideálu I. O faktorových okruhoch sa dozviete v nasledujúcej podkapitole, čiže tento stĺpec zatiaľ nechajte nevyplnený a vráťte sa k nemu neskôr.

Úloha 4.1.6. Ak R je okruh bez deliteľov nuly a $ab = 1$, tak aj $ba = 1$.

Úloha 4.1.7. Nech $(R, +, \cdot)$ je okruh. Definujme binárnu operáciu $*$ ako $a*b = b\cdot a$. Dokážte, že aj $(R, +, *)$ je okruh.

Úloha 4.1.8. Dokážte, že $\{(r, r); r \in R\}$ je podokruh okruhu $R \times R$. Je tento podokruh izomorfný s okruhom R?

Úloha 4.1.9. Zistite, či S je podokruhom R, a tiež či v okruhoch S a R existuje jednotka (a ak áno, tak či je v oboch prípadoch rovnaká).
a) $R = \mathbb{Z}_6$, $S = 2\mathbb{Z}_3 = \{0, 2, 4\}$.
b) $R = A \times A$ a $S = A \times \{0\}$, kde A je ľubovoľný okruh s jednotkou.
c) $R = M_{2,2}(\mathbb{R})$, t.j. reálne matice rozmerov 2×2 a $S = \{\left(\begin{smallmatrix} a & 0 \\ 0 & 0 \end{smallmatrix}\right); a \in \mathbb{R}\}$.

Úloha 4.1.10. Nech R je okruh. Centrom okruhu R nazveme množinu $Z = \{z \in R; (\forall r \in R) zr = rz\}$. Ukážte, že:
a) Z je podokruh R.
b) Ak R má jednotku, tak $1 \in Z$.
c) Centrum telesa je pole.

Úloha 4.1.11*. Nech $(R, +, \cdot)$ je okruh s jednotkou. Ak existuje inverzný prvok vzhľadom na operáciu $\cdot$ k $1 - ab$, tak existuje aj inverzný prvok k $1 - ba$.

4.2 Okruhy polynómov – definícia a delenie so zvyškom

Na strednej škole ste strávili veľa času s kvadratickými rovnicami $ax^2+bx+c = 0$. Venovali ste sa aj všeobecnejším rovniciam vyššieho stupňa. Tieto rovnice súvisia s funkciami $f\colon \mathbb{R} \to \mathbb{R}$ tvaru

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0.$$

Takéto funkcie budeme volať polynomické funkcie.

V tejto časti by sme chceli zaviesť podobný pojem pre ľubovoľný komutatívny okruh s jednotkou. V minulom semestri sme pracovali s polynomickými funkciami nad $\mathbb{R}$ ako s prvkami vektorového priestoru $\mathbb{R}^{\mathbb{R}}$ všetkých zobrazení z $\mathbb{R}$ do $\mathbb{R}$. Vtedy sme často používali fakt, že polynomická funkcia $f(x) = a_n x^n+a_{n-1}x^{n-1}+\cdots+a_0$ sa rovná nulovej funkcii (t.j. v každom bode nadobúda hodnotu 0) práve vtedy, keď všetky koeficienty sú nulové, t.j.

$$a_n = a_{n-1} = \ldots = a_0 = 0.$$

(Ako uvidíme, táto vlastnosť neplatí pre všetky polia, v prípade poľa $\mathbb{R}$ však platí, ukážeme to v tvrdení 4.2.13.)

Práve toto je vlastnosť, ktorú budeme požadovať od pojmu polynómu, ktorý teraz ideme definovať.

4.2.1 Definícia okruhu polynómov

Definícia 4.2.1. Nech R je komutatívny okruh s jednotkou. Potom formálne zápisy tvaru

$$p = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0,$$

kde n je prirodzené číslo a $a_i \in R$ pre $i = 0, \ldots, n$ nazývame *polynómy* v premennej x nad okruhom R.

Namiesto zápisu $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ budeme často používať stručnejší zápis

$$p = \sum_{i=0}^{n} a_i x^i.$$

Prvky $a_n, a_{n-1}, \ldots, a_0 \in R$ voláme *koeficienty* polynómu p.

Ak navyše $a_n \neq 0$, tak n voláme *stupeň polynómu p,* označujeme $\operatorname{st} p = n$, alebo $\operatorname{st}(p) = n$. V prípade nulového polynómu (všetky koeficienty sú nulové) definujeme $\operatorname{st} p = -\infty$. (Všimnite si, že s výnimkou nulového polynómu je možné také n zvoliť, t.j. stupeň je definovaný pre každý polynóm.) Polynómy stupňa menšieho ako 1 voláme *konštantné polynómy.*

Koeficient $a_n \neq 0$ pre $n = \operatorname{st} p$ voláme *vedúci koeficient* polynómu p.

Dva polynómy považujeme za rovnaké, ak majú rovnaké koeficienty, t.j. ak $p = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, $q = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$ a $n \geq m$, tak $p = q$ práve vtedy, keď

$$a_i = b_i \qquad \text{pre } i = 0, 1, \ldots, m$$

a $a_i = 0$ pre $i = m+1, \ldots, n$.

V tejto definícii môže byť trochu nejasné, čo je x a prečo sa volá premenná. Ešte sa tohoto problému dotkneme na konci tejto časti, je to však možné jednoducho brať tak, že doplnenie symbolov x^i je len spôsob zápisu – polynóm je jednoznačne určený svojimi koeficientami.

Príklad 4.2.2. Napríklad $0x^3 + 1x^2 + 2x + 1 = 1x^2 + 2x + 1$ chápeme ako dva rôzne zápisy toho istého polynómu z $\mathbb{R}[x]$.

Vidíme teda, že pridanie alebo odobranie nulových koeficientov polynóm tento polynóm nemení.

Ďalej by sme radi rozumným spôsobom zadefinovali sčitovanie a násobenie polynómov. „Rozumný“ spôsob by mal spĺňať prinajmenšom to, že nejakým spôsobom bude rešpektovať násobenie v okruhu R a tiež by bolo vhodné, aby výsledný okruh bol komutatívny.

Pritom polynóm budeme chápať ako súčet výrazov $a_i x^i$. To vlastne jednoznačne určuje sčitovanie, napríklad pre $p = x^2 + 2x + 1$ a $q = 2x + 1$ máme

$$p + q = (x^2 + 2x + 1) + (2x + 1) = x^2 + 2x + 2x + 1 + 1 = x^2 + 4x + 2.$$

(Využili sme iba to, že polynóm vieme rozložiť na jednotlivé členy a distributívnosť.)

Tieto požiadavky (t.j. vlastnosti komutatívneho okruhu a to, že koeficienty sa násobia rovnako ako v R) už takmer určujú násobenie. Ak chceme napríklad vynásobiť polynómy $p = x^2 + 2x + 1$ a $q = 2x + 1$ v $\mathbb{Z}[x]$, tak z distributívnosti dostaneme

$$(x^2 + 2x + 1)(2x + 1) = x^2.2x + 2x.2x + 1.2x + x^2.1 + 2x.1 + 1.1.$$

Na základe komutatívnosti dostaneme

$$(x^2 + 2x + 1)(2x + 1) = 2x^2.x + 4x.x + 2.x + 1x^2 + 2x + 1.$$

Predpokladajme, že násobenie výrazov obsahujúcich iba x^k funguje takým spôsobom, že $x^m.x^n = x^{m+n}$. Potom predchádzajúci výraz môžeme upraviť na tvar

$$(x^2 + 2x + 1)(2x + 1) = 2x^3 + 4x^2 + 2x + 1x^2 + 2x + 1.$$

Opäť z distributívnosti dostaneme

$$(x^2 + 2x + 1)(2x + 1) = 2x^3 + 5x^2 + 4x + 1.$$

Možno sa tento jednoduchý výpočet zdá rozpísaný zbytočne priveľmi podrobne, cieľom však bolo ukázať, aké vlastnosti potrebujeme, keď chceme niečo podobné definovať nad ľubovoľným komutatívnym okruhom s jednotkou. Zopakovaním rovnakej úvahy pre všeobecný prípad dostaneme:

Definícia 4.2.3. Nech R je komutatívny okruh s jednotkou. Nech $p = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ a $q = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0$ sú ľubovoľné polynómy nad R. (Tým, že u oboch polynómov predpokladáme rovnaký počet koeficientov sme sa nijako neobmedzili – v prípade potreby je možné niektorý polynóm doplniť nulami.)

Potom *súčet polynómov* p a q je

$$p + q = \sum_{i=0}^{n} (a_i + b_i)x^i.$$

Súčin polynómov p a q je polynóm $r = \sum_{i=0}^{2n} c_i x^i$, kde

$$c_k = \sum_{j=0}^{k} a_j b_{k-j}.$$

Teda obe operácie sme definovali rovnako ako v predchádzajúcom príklade – pri sčitovaní sa jednoducho sčítajú koeficienty a pri násobení sú koeficienty výsledného polynómu práve tie výrazy, ktoré by sme dostali roznásobením (koeficient c_k je súčet všetkých možných $a_s b_l$ pre $s + l = k$, čo sú presne všetky možnosti, ako môžeme dostať $x^k = x^s.x^l$).

Definíciu súčinu by sme mohli ekvivalentne prepísať ako

$$c_k = \sum_{m+n=k} a_m b_n.$$

Z tejto ekvivalentnej definície vidno, že pre násobenie polynómov platí asociatívnosť: pre $p = \sum_{i=0}^{n} a_i x^i$, $q = \sum_{i=0}^{n} b_i x^i$, $r = \sum_{i=0}^{n} c_i x^i$ dostaneme $(pq)r = \sum_{i=0}^{3n} d_i x^i$, kde koeficienty d_k majú hodnoty

$$d_k = \sum_{m+n=k} a_m \sum_{s+t=n} b_s c_t = \sum_{m+s+t=k} a_m b_s c_t.$$

Vďaka tomu dostaneme, že

Tvrdenie 4.2.4. *Nech R je komutatívny okruh s jednotkou. Množina všetkých polynómov nad R s násobením a sčitovaním definovaným v predchádzajúcej definícii tvorí komutatívny okruh s jednotkou. Tento okruh označujeme $R[x]$ a voláme ho* okruh polynómov nad R.

Sčitovanie a násobenie polynómov sme vlastne definovali tak, aby akákoľvek rovnosť, ktorá platí pre polynómy platila aj keď namiesto x napíšeme akýkoľvek prvok okruhu R (alebo nejakého nadokruhu, ktorý obsahuje R). To zdôvodňuje použitie názvu premenná – namiesto x môžeme napísať (dosadiť) hocijaký prvok, čiže sa môže meniť. (Aj dosadzovaniu do polynómov sa budeme ešte venovať.)

Dohoda. V ďalšom budeme polynómy zapisovať ako $p(x)$, $q(x)$ atď., čím označíme o polynóm v akej premennej ide. (Ak budeme niekde hovoriť súčasne o polynómoch aj o funkciách, tak opäť použijeme radšej jednopísmenkové označenie p, q; aby nemohlo dôjsť k omylu, že máme na mysli nejakú funkciu resp. jej funkčnú hodnotu.)

Poznámka 4.2.5. Všimnime si, že sčitovanie a násobenie konštantných polynómov funguje rovnako ako násobenie v okruhu R. To znamená, že keď prvky okruhu R stotožníme s im

prislúchajúcimi konštantnými polynómami, môžeme R chápať ako podokruh okruhu $R[x]$. (Formálne by sme tento fakt sformulovali tak, že zobrazenie, ktoré prvku $a \in R$ priradí konštantný polynóm $a \in R[x]$ je okruhový homomorfizmus, ktorý je navyše injektívny.) V ďalšom budeme toto stotožnenie často používať (aj bez toho, že by sme na to výslovne upozornili.) To znamená, že R budeme chápať priamo ako podmnožinu $R[x]$.

Všimnime si ešte, že vlastnosť „byť oborom integrity“ sa prenesie z okruhu R na okruh $R[x]$ polynómov nad týmto okruhom.

Tvrdenie 4.2.6. *Ak R je obor integrity, tak pre ľubovoľné nenulové polynómy $f, g \in R[x]$ platí*

$$\mathrm{st}(fg) = \mathrm{st}(f) + \mathrm{st}(g)$$

a okruh $R[x]$ polynómov nad okruhom R je obor integrity.

Dôkaz. Ak f a g sú nenulové polynómy, môžeme ich zapísať ako

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0,$$
$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0,$$

pričom $n = \mathrm{st}\, f$, $m = \mathrm{st}\, g$. Vyrátajme, aký bude koeficient c_{n+m} polynómu $f.g$ pri x^{n+m}. Priamo z definície máme, že

$$c_{n+m} = a_n b_m,$$

a pretože R je obor integrity, dostávame $c_{n+m} \neq 0$. To znamená, že polynóm $f.g$ je nenulový (teda $R[x]$ je obor integrity) a tiež, že

$$\mathrm{st}(fg) = m + n = \mathrm{st}(f) + \mathrm{st}(g).$$

□

4.2.2 Delenie so zvyškom

Pre nás bude dôležitý hlavne prípad keď okruh R je pole. Ako sme už ukázali, v tomto prípade platí

$$\mathrm{st}(pq) = \mathrm{st}\, p + \mathrm{st}\, q.$$

Neskôr bude pre nás dôležitá nasledujúca veta:

Veta 4.2.7 (Veta o delení so zvyškom)**.** *Nech F je pole, $f(x), g(x) \in F[x]$ a $g(x) \neq 0$. Potom existujú $q(x), r(x) \in F[x]$ také, že*

$$f(x) = q(x).g(x) + r(x)$$

a $\mathrm{st}\, r(x) < \mathrm{st}\, g(x)$.

Navyše, $q(x)$ a $r(x)$ sú týmito podmienkami jednoznačne určené.

Definícia 4.2.8. Polynómy $q(x)$ a $r(x)$ jednoznačne určené podmienkami z vety 4.2.7 sa nazývajú *podiel* a *zvyšok po delení* polynómu $f(x)$ polynómom $g(x)$. Zvyšok po delení označujeme $f(x) \bmod g(x)$.

Dôkaz. Existencia. Matematickou indukciou vzhľadom na $n = \mathrm{st}(f)$.

1° Ak $\mathrm{st}\, f(x) < \mathrm{st}\, g(x)$, stačí položiť $q(x) = 0$ a $r(x) = f(x)$.

2° Nech $n = \mathrm{st}\, f(x) \geq \mathrm{st}\, g(x)$ a každý polynóm stupňa menej ako n sa dá vydeliť so zvyškom polynómom $g(x)$ (indukčný predpoklad).

Označme $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$ pričom $a_n, b_m \neq 0$. Položme $h(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$. Koeficient pri x^n v polynóme $h(x)$ je $a_n - a_n b_m^{-1} b_m = 0$. Teda $\mathrm{st}(h) < \mathrm{st}(f)$, čiže pre polynóm h (podľa indukčného predpokladu) existujú $s(x), r(x) \in F[x]$ také, že

$$h(x) = s(x)g(x) + r(x)$$

a $\mathrm{st}(r) < \mathrm{st}(g)$. Potom

$$f(x) = (s(x) + a_n b_m^{-1} x^{n-m})g(x) + r(x).$$

Jednoznačnosť. Nech platí

$$f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x),$$

pričom $\mathrm{st}(r_1) < \mathrm{st}(g)$, $\mathrm{st}(r_2) < \mathrm{st}(g)$. Potom máme

$$(q_1(x) - q_2(x))g(x) = r_2(x) - r_1(x).$$

Na pravej strane je polynóm stupňa menšieho ako $\mathrm{st}(g)$. Ak by platilo $q_1(x) - q_2(x) \neq 0$, tak na ľavej strane tejto rovnosti dostaneme polynóm stupňa aspoň $\mathrm{st}(g)$, čo je spor. Preto musí platiť $q_1(x) - q_2(x) = 0$ a $q_1(x) = q_2(x)$.

Z toho potom dostávame aj $r_1(x) - r_2(x) = 0$ a $r_1(x) = r_2(x)$. □

Všimnime si, že dôkaz predchádzajúcej vety nám súčasne dáva návod, ako rátať pre dané polynómy ich podiel a zvyšok.

Príklad 4.2.9. Vydeľme so zvyškom polynóm $f(x) = x^4 + 6x^3 + 12x^2 + 12x + 10$ polynómom $g(x) = x^2 + x + 1$. Podľa návodu z dôkazu by sme sa mali pozrieť najprv na vedúce členy – vidíme, že $x^4 = x^2 \cdot x^2$. Vypočítame teda

$$f(x) - x^2 g(x) = (x^4 + 6x^3 + 12x^2 + 12x + 10) - x^2(x^2 + x + 1) = 5x^3 + 11x^2 + 12x + 10.$$

Výsledok by sme opäť mali deliť polynómom $g(x)$ a postup opakovať, až kým nedostaneme polynóm stupňa menšieho ako $g(x)$.

$$5x^3 + 11x^2 + 12x + 10 - 5x(x^2 + x + 1) = 6x^2 + 7x + 10$$
$$6x^2 + 7x + 10 - 6(x^2 + x + 1) = x + 4$$

Celkovo sme dostali, že $f(x) - (x^2 + 5x + 6)g(x) = x + 4$, čiže

$$f(x) = (x^2 + 5x + 6)g(x) + (x + 4),$$

teda podiel je $x^2 + 5x + 6$ a zvyšok po delení je $x + 4$.

V prípade, že je polynóm $g(x)$ (=stupňa 1) môžeme podiel vyrátať jednoduchším spôsobom, ktorý sa naučíme v časti 4.4.1.

Neskôr bude pre nás užitočný fakt, že analogická veta platí aj v okruhu $(\mathbb{Z}, +, \cdot)$. Dala by sa dokazovať podobným spôsobom ako predchádzajúca veta , tu si ukážeme o trochu iný dôkaz.

Veta 4.2.10. *Nech a, b sú celé čísla, $b > 0$. Potom existujú celé čísla q a r také, že*

$$a = q \cdot b + r \qquad a \qquad 0 \leq r < b.$$

Navyše, q a r sú týmito podmienkami jednoznačne určené.

Definícia 4.2.11. Číslo r z predchádzajúcej vety sa nazýva *zvyšok a po delení b* a označuje sa $a \mod b$.

Dôkaz. Existencia: Množina $\{k; kb \leq pa\}$ je zhora ohraničená. Preto existuje $q := \max\{k; kb \leq a\}$. Položme $r = a - qb$. Očividne platí $a = qb + r$ a $r \geq 0$.

Tvrdíme, že $r < b$. Nech by to tak nebolo. Z nerovnosti $r \geq b$ dostaneme $a \geq (q+1)b$, čo je spor s definíciou čísla q.

Jednoznačnosť: Predpokladajme, že $a = qb + r = q'b + r'$, kde $0 \leq r, r' < b$. Potom

$$(q - q')b = r' - r.$$

Predpokladajme, že by $|q - q'| > 0$. Potom $|r - r'| \geq b$, čo je spor s tým, že $0 \leq r, r' < b$.

Preto platí

$$(q - q')b = r - r' = 0,$$

a $q = q'$, $r = r'$. □

4.2.3 Polynómy a polynomické funkcie

V tomto článku budeme polynómy vždy označovať ako $p, q, \ldots$ (t.j. jedným písmenom).

Definícia 4.2.12. Nech R je komutatívny okruh s jednotkou. *Polynomickou funkciou* nad R budeme rozumieť ľubovoľnú funkciu $f\colon R \to R$ určenú predpisom

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

pre nejaké $n \in \mathbb{N}$ a $a_1 \ldots a_n \in R$.

Množina všetkých polynomických funkcií s obvyklým násobením a sčitovaním funkcií opäť tvorí okruh (je to podokruh okruhu R^R – úloha 4.2.1), tento okruh budeme označovať $R\langle x\rangle$.

Pri zavedení polynómov sme spomínali polynomické funkcie nad poľom $\mathbb{R}$. Zaujíma nás, aký je vo všeobecnosti vzťah medzi okruhmi $F[x]$ a $F\langle x\rangle$, ak F je ľubovoľné pole.

Máme prirodzené priradenie medzi polynómami a polynomickými funkciami $\varphi\colon F[x] \to F\langle x\rangle$, ktoré polynómu $p = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ priradí funkciu danú predpisom $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$. Dá sa overiť, že toto zobrazenie je surjektívny homomorfizmus z okruhu $F[x]$ na okruh $F\langle x\rangle$.

V prípade, že homomorfizmus φ je injektívny, tak je to izomorfizmus. Čiže na to, aby sme zistili, či sú tieto dva okruhy izomorfné, stačí zistiť, ako vyzerá $\operatorname{Ker}\varphi$. Ukážeme, že pre nekonečné polia sú okruhy $F[x]$ a $F\langle x\rangle$ izomorfné, zatiaľčo pre konečné polia to platiť nemusí.

Tvrdenie 4.2.13. *Ak F je nekonečné pole tak polynomická funkcia $f\colon F \to F$*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

sa rovná nulovej funkcii práve vtedy, keď $a_0 = a_1 = \cdots = a_n = 0$, t.j. vtedy, keď sú všetky koeficienty nulové.

Náčrt dôkazu. Vyberme $n+1$ navzájom rôznych prvkov $x_0, \ldots, x_n$ poľa F. Potom koeficienty $a_0, \ldots, a_n$ spĺňajú sústavu $n+1$ lineárnych rovníc

$$\begin{aligned} a_n x_0^n + a_{n-1} x_0^{n-1} + \cdots + a_0 &= 0 \\ a_n x_1^n + a_{n-1} x_1^{n-1} + \cdots + a_0 &= 0 \\ &\cdots \\ a_n x_n^n + a_{n-1} x_n^{n-1} + \cdots + a_0 &= 0 \end{aligned}$$

Z úlohy I-6.5.8 (pozri tiež napríklad [Kor, Príklad 6.2.17(2)], [KGGS, s.114/7]) vieme, že determinant matice tejto sústavy je

$$\begin{vmatrix} 1 & x_0 & x_0^2 & \dots & x_0^n \\ 1 & x_1 & x_1^2 & \dots & x_1^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_x^n \end{vmatrix} = \prod_{0 \le i < j \le n} (x_j - x_i)$$

čiže ak prvky x_i sú navzájom rôzne, je nenulový. To znamená, že táto matica je regulárna a uvedenej sústave rovníc vyhovuje iba nulové riešenie.

Teda $\operatorname{Ker} f$ v tomto prípade pozostáva iba z nulového polynómu (všetky koeficienty sú nuly). □

Príklad 4.2.14. Homomorfizmus $\varphi\colon \mathbb{Z}_2[x] \to \mathbb{Z}_2\langle x\rangle$, ktorý polynómu priraďuje zodpovedajúcu polynomickú funkciu, nie je injektívny.

Stačí si všimnúť, že pre každé $x \in \mathbb{Z}_2$ platí $x^2 + x = 0$, teda polynomická funkcia $x^2 + x$ je nulová a

$$x^2 + x \in \operatorname{Ker} \varphi.$$

Homomorfizmus $\varphi\colon R[x] \to R\langle x\rangle$ nám súčasne dáva možnosť „dosadzovať“ do polynómov. Ak totiž máme daný prvok $b \in R$ a nejaký polynóm $f = a_n x^n + a_{n-1}x^{n-1} + \dots + a_0 \in R[x]$, tak mu vieme priradiť funkciu $\varphi(f)\colon R \to R$. Potom môžeme b dosadiť do tejto funkcie, čiže dostaneme

$$\varphi(f)(b) = a_n b^n + a_{n-1}b^{n-1} + \dots + a_0.$$

Navyše, zobrazenie $f_b\colon R[x] \to R$ určené predpisom

$$f_b\colon f \mapsto a_n b^n + a_{n-1}b^{n-1} + \dots + a_0$$

je okruhový homomorfizmus taký, že $f(x) = b$ (t.j. polynóm x sa zobrazí na prvok b.)

To, že f_b je skutočne homomorfizmus možno vidieť napríklad z toho, že $f_b = g_b \circ \varphi$, kde $g_b\colon R^R \to R$ je homomorfizmus daný predpisom $g_b(f) = f(b)$ (úloha 4.2.2).

Definícia 4.2.15. Ak R je komutatívny okruh a $b \in R$, tak homomorfizmus $f_b\colon R[x] \to R$ daný predpisom

$$f_b\colon f \mapsto a_n b^n + a_{n-1}b^{n-1} + \dots + a_0$$

voláme *dosadzovací homomorfizmus.*

4.2.4 Iné možnosti, ako definovať okruh polynómov

Keďže považujeme izomorfné okruhy za rovnaké (z toho dôvodu, že sú nerozlíšiteľné pomocou pojmov definovaných „v jazyku okruhov“, t.j. nemožno ich odlíšiť žiadnou vlastnosťou sformulovanou len s použitím sčitovania a násobenia v okruhu), je jasné, že akákoľvek iná definícia okruhov, ktorá by ako výsledok poskytla okruh izomorfný s okruhom $R[x]$, by bola rovnako dobrá.

Pomerne jednoduchá definícia, s ktorou by sa nám dobre pracovalo a ktorej by sme intuitívne celkom dobre rozumeli, by bola definícia okruhu $R[x]$ ako okruhu všetkých polynomických funkcií. Ako sme už videli, takto okruh $R[x]$ nemôžeme definovať, pretože pre konečné polia by sme takto zadefinovali niečo úplne iné než chceme.

Iná možná definícia okruhu polynómov nad okruhom R by bola nasledovná (takto sa definujú okruhy polynómov v [KGGS]):

Definícia 4.2.16. Nech R je komutatívny okruh s jednotkou. Predpokladajme, že R je podokruh nejakého komutatívneho okruhu R' a existuje prvok $x \in R'$ taký, že rovnosť

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

pre $a_1, \ldots, a_n \in R$ platí práve vtedy, keď $a_1 = \cdots = a_n = 0$. Potom prvok x voláme *transcendentný prvok* nad R.

Podokruh

$$R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0; n \in \mathbb{N}, a_1, \ldots, a_n \in R\}$$

okruhu R' potom voláme *okruhom polynómov* v premennej x nad R.

Overiť, že množina $R[x]$ zadefinovaná v predchádzajúcej definícii je skutočne podokruhom R' je jednoduché – dá sa dokonca ukázať, že je to najmenší podokruh obsahujúci $R \cup \{x\}$. Z toho vyplýva výhoda tejto definície – automaticky vidíme, že $R[x]$ je okruh, z toho, že ide o podokruh okruhu R'. (V našej definícii sme to museli dokazovať.)

Táto definícia si vyžaduje istú prácu navyše – aby sme mohli definovať $R[x]$ pre ľubovoľný komutatívny okruh R s jednotkou, treba dokázať, že pre každý takýto okruh R existuje vhodný nadokruh R', t.j. existuje nadokruh obsahujúci aspoň jeden transcendentný prvok. O chvíľu sa dozvieme, ako sa dá dokázať takéto niečo.

Ďalej pri použití takejto definície musíme ukázať aj to, že bez ohľadu na voľbu nadokruhu R' a transcendentného prvku $x \in R'$ dostaneme vždy (až na izomorfizmus) to isté.

Skúsme sa ešte na chvíľu pozrieť na našu definíciu 4.2.1. K nej by sme mohli mať jednu vážnu výhradu – kedysi v minulom semestri sme tvrdili, že pre nás bude pojem množiny základným pojmom, ktorý síce nedefinujeme (iba popíšeme niektoré jeho vlastnosti), pomocou množín a operácii s nimi už však budeme schopní vystavať celú potrebnú teóriu, teda všetky ďalšie pojmy budeme schopný preformulovať v jazyku množín.

V tejto definícii sme použili „symbol x“ a „formálne zápisy tvaru“ $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ – čo rozhodne nesedí s našou koncepciou definovať všetko pomocou množín. (Čo je symbol? Čo znamená *formálny zápis*?)

Ukážeme si, ako to môžeme zachrániť – t.j. zadefinujeme okruh polynómov tak, aby naša definícia bola „množinová“. Súčasne nám táto definícia poskytne aj riešenie jedného z problémov s definíciou 4.2.16 – existenciu nadokruhu, ktorý obsahuje transcendentný prvok.

Napriek tomu sa však menej formálna definícia 4.2.1 zdá byť lepšia – pretože pri nej s prvkami okruhu $R[x]$ pracujeme rovnako ako s výrazmi obsahujúcimi nejaké prvky okruhu R. Násobenie, ako sme ho definovali v tejto definícii je teda veľmi prirodzené. V nasledujúcej definícii bude o niečo komplikovanejšie a striktné používanie tejto definície by viedlo k zložitejším zápisom polynómov.

Definícia 4.2.17. Nech R je ľubovoľný komutatívny okruh s jednotkou. Ako $R[x]$ označíme množinu všetkých postupností prvkov z R takých, že iba konečne veľa členov tejto postupnosti je nenulových. Ďalej zadefinujeme sčitovanie dvoch postupností ako

$$(a_n)_{n=1}^{\infty} + (b_n)_{n=1}^{\infty} = (a_n + b_n)_{n=1}^{\infty}$$

a súčin postupností $(a_n)_{n=1}^{\infty}$, $(b_n)_{n=1}^{\infty}$ definujeme ako postupnosť $(c_n)_{n=1}^{\infty}$, ktorej členy sú určené predpisom

$$c_k = \sum_{j=0}^{k} a_j b_{k-j} = \sum_{m+n=k} a_m b_n.$$

Táto množina postupností s uvedeným sčitovaním a násobením tvorí okruh, ktorý voláme *okruh polynómov* nad R.

Táto definícia v istom zmysle presne zodpovedá definícii 4.2.1 – postupnosti sú tiež jednoznačne určené svojimi členmi, takisto ako dva polynómy sme v definícii 4.2.1 prehlásili za rovnaké, ak mali rovnaké koeficienty.

Dôkaz, že takýmto spôsobom dostaneme okruh je takmer totožný s dôkazom tvrdenia 4.2.4.

Polynóm $3x^2 - 1x + 0$ v tejto definícii zodpovedá postupnosti $(0, -1, 3, 0, 0, \ldots)$. Prvky z R môžeme stotožniť s postupnosťami tvaru $(a, 0, 0, 0, \ldots)$, kde $a \in R$. Všimnime si, že polynóm x zodpovedá postupnosti $(0, 1, 0, 0, \ldots)$ a dá sa ukázať, že v okruhu $R[x]$ (chápanom ako postupnosti, čiže ako v poslednej uvedenej definícii) je tento prvok transcendentným prvkom nad R.

Cvičenia

Úloha 4.2.1. Dokážte, že polynomické funkcie (definícia 4.2.12) tvoria podokruh okruhu F^F.

Úloha 4.2.2. Dokážte, že zobrazenie $f_1 \colon R_1 \times R_2 \to R_1$ určené predpisom $f_1(r_1, r_2) = r_1$ je homomorfizmus.

Dokážte, že pre každé $i \in I$ je zobrazenie $f_i \colon R^I \to R$ dané predpisom $f_i(g) = g(i)$ (pre ľubovoľné $g \colon I \to R$) je homomorfizmus.

4.3 Deliteľnosť v okruhoch

V tejto časti sa budeme zaoberať deliteľnosťou v okruhoch. Najdôležitejšími príkladmi budú pre nás okruh $(\mathbb{Z}, +, \cdot)$ celých čísel a okruh $(F[x], +, \cdot)$ polynómov nad poľom F.

V celej podkapitole budeme predpokladať, že okruh, s ktorým pracujeme, je obor integrity. Nasledujúcu vlastnosť oborov integrity budeme často používať, preto ju sformulujeme ako samostatnú lemu. (Vlastne to je špeciálny prípad krátenia nenulovým prvkom v obore integrity – tvrdenie 4.1.14.)

Lema 4.3.1. *Nech R je obor integrity, $a, b \in R$. Ak platí $ab = a$ pre $a \neq 0$, tak $b = 1$.*

Dôkaz. Z rovnosti $ab = a = a1$ vyplýva

$$ab - a1 = a(b - 1) = 0,$$

čiže v obore integrity pre $a \neq 0$ máme $b - 1 = 0$, čiže $b = 1$. □

Definícia 4.3.2. Nech R je obor integrity. Hovoríme, že a *delí* b, označujeme $a \mid b$, ak existuje $c \in R$ také, že $b = ca$.

Lema 4.3.3. *Nech R je obor integrity. Potom pre ľubovoľné $a, b, c, d \in R$, $a_i, r_i \in R$ platí*

(i) $a \mid a$

(ii) $a \mid b \wedge b \mid c \Rightarrow a \mid c$

(iii) $a \mid b \wedge c \mid d \Rightarrow ac \mid bd$

(iv) $a \mid 0$, $1 \mid a$

(v) $0 \mid a \Leftrightarrow a = 0$

(vi) $ac \mid bc \wedge c \neq 0 \Rightarrow a \mid b$

(vii) $a \mid a_i$ *pre* $i = 1, \dots n \Rightarrow a \mid a_1 r_1 + \cdots + a_n r_n$

Dôkaz. Jednoduchý – ponecháme ako cvičenie. □

Príklad 4.3.4. V prípade okruhu $\mathbb{Z}$ je relácia $\mid$ tá istá relácia deliteľnosti, ktorú poznáte zo strednej školy, t.j. napríklad $3 \mid 12$, lebo $12 = 3 \cdot 4$, zatiaľčo $3 \nmid 7$.

Všimnime si, že $a \mid b$ znamená to isté, ako že zvyšok čísla b po delení číslom a je 0.

Príklad 4.3.5. V okruhoch $\mathbb{Z}[x]$, $\mathbb{R}[x]$ platí $x - 1 \mid x^2 - 1$, pretože $x^2 - 1 = (x - 1)(x + 1)$.

Pritom si môžeme všimnúť, že v $\mathbb{R}[x]$ platí aj $2x - 2 \mid x^2 - 1$ (lebo $x^2 - 1 = (2x - 2)(\frac{1}{2}x + \frac{1}{2})$), ale v okruhu $\mathbb{Z}[x]$ už táto relácia neplatí. Deliteľnosť polynómov, ak ich chápeme ako polynómy nad $\mathbb{Z}$ a nad $\mathbb{R}$, sú rôzne pojmy, hoci $\mathbb{R}$ je nadpoľom $\mathbb{Z}$.

Všimnime si, že aj v okruhoch $F[x]$ platí $f(x) \mid g(x)$ práve vtedy, keď zvyšok polynómu $g(x)$ po delení $f(x)$ je 0. (Neskôr si to zdôvodníme podrobnejšie vo všeobecnejšom prípade)

Definícia 4.3.6. Ak $a, b \in R$, kde R je obor integrity, hovoríme, že prvky a a b sú *asociované,* označujeme $a \sim b$, ak $a \mid b$ a súčasne $b \mid a$

$$a \mid b \ \wedge \ b \mid a \Leftrightarrow a \sim b$$

Lema 4.3.7. *Nech R je obor integrity. Pre ľubovoľné $a, b, c, d \in R$ platí*

(i) $a \sim b \wedge b \sim c \Rightarrow a \sim c$

(ii) $a \sim a$

(iii) $a \sim b \Rightarrow b \sim a$

(iv) $a \sim b \wedge c \sim d \Rightarrow ac \sim bd$

Dôkaz lemy 4.3.7 pre jednoduchosť vynechávame. Môžeme si všimnúť, že prvé tri vlastnosti nám hovoria, že relácia „byť asociovaný“ je relácia ekvivalencie. (Podobným spôsobom môžeme dostať z ľubovoľného čiastočného usporiadania reláciu ekvivalencie – úloha 4.3.2.) Posledná podmienka hovorí, že relácia $\sim$ sa správa rozumne vzhľadom na násobenie.

Definícia 4.3.8. Ak okruh R má jednotku a $ab = 1$, hovoríme, že a je *deliteľ jednotky.* Množinu všetkých deliteľov jednotky budeme označovať $U(R)$.

Tvrdenie 4.3.9. *Nech R je obor integrity. Potom*

(i) *Delitele jednotky s operáciou násobenia tvoria grupu, t.j. $(U(R), \cdot)$ je grupa.*

(ii) *$a \sim b$ práve vtedy, keď existuje deliteľ jednotky u taký, že $a = bu$.*

Dôkaz. (i) Uzavretosť na násobenie: Ak $a, b \in U(R)$, znamená to existenciu $c, d \in R$ takých, že $ac = 1$, $bd = 1$. Potom $acbd = (ab)(cd) = 1$, čiže aj ab je deliteľ jednotky.

Asociatívnosť máme priamo z definície okruhu, neutrálny prvok je 1.

Existencia inverzného prvku: Ak a je deliteľ jednotky, znamená to, že existuje $b \in R$ také, že $ab = 1$. To znamená, že $b \in U(R)$ a tento prvok je inverzný k a vzhľadom na násobenie.

(ii) Ľahko vidno, že $a \sim 0$ platí práve vtedy, keď $a = 0$ (z lemy 4.3.3 vieme, že $0 \mid a$ iba pre $a = 0$). Samozrejme, $u0 = 0$ pre ľubovoľné $u \in U(R)$.

Zostáva nám teda dokázať tvrdenie pre prípade $a \neq 0$.

Ak $a \mid b$ a $b \mid a$, tak existujú $c, d \in R$ také, že $ac = b$ a $bd = a$. Potom máme

$$a = bd = (ac)d = a(cd)$$

a z lemy 4.3.1 dostaneme $cd = 1$, čiže c aj d sú delitele jednotky. □

Príklad 4.3.10. Ľahko sa dá overiť, že ± 1 sú delitele jednotky v $\mathbb{Z}$ a všetky nenulové konštantné polynómu sú delitele jednotky v $F[x]$.

Takisto nie je ťažké ukázať, že iné delitele jednotky tam už nie sú. Skutočne, ak $ab = 1$ v $\mathbb{Z}$, tak $a, b \neq 0$, z čoho máme $|a| \geq 1$, $|ab| = |a||b| \geq 1$. Aby v predchádzajúcej rovnosti nastala rovnosť, musí byť $|a| = 1$, čiže $a = \pm 1$.

Ak $f(x)$ je deliteľ jednotky v $F[x]$, tak máme $f(x)g(x) = 1$. Pritom $g(x) \neq 0$ (lebo potom by sme dostali $f(x)g(x) = 0$), preto $\operatorname{st} g \geq 0$. Potom (tvrdenie 4.2.6) $\operatorname{st}(fg) = \operatorname{st} f + \operatorname{st} g \geq \operatorname{st} f$. Súčasne vieme $\operatorname{st}(fg) = \operatorname{st} 1 = 0$, preto aj $\operatorname{st} f = 0$ a $f(x)$ je konštantný polynóm. (Nemôže platiť $f(x) = 0$; zdôvodniť to môžeme rovnako ako sme to spravili pre polynóm $g(x)$.)

4.3.1 Najväčší spoločný deliteľ, Euklidov algoritmus

Veta 4.2.7 o delení so zvyškom je dôležitou vlastnosťou okruhu $F[x]$ polynómov nad poľom F. Veta 4.2.10 nám hovorí, že analogickú vlastnosť má aj okruh celých čísel $(\mathbb{Z}, +, \cdot)$.

Na základe tejto vety môžeme odvodiť mnohé vlastnosti, ktoré sú spoločné pre oba spomínané okruhy – najjednoduchšie bude odvodiť ich všeobecne pre oba spomínané okruhy.

Podobne ako pre celé čísla, aj v oboroch integrity vieme definovať pojem najväčší spoločný deliteľ.

Definícia 4.3.11. *Najväčší spoločný deliteľ* prvkov $a, b \in R$ je taký prvok $c \in R$, že

(i) $c \mid a$, $c \mid b$,

(ii) pre ľubovoľný prvok $d \in R$ taký, že $d \mid a$ a $d \mid b$ platí aj $d \mid c$.

Označujeme ho $\gcd(a, b)$.

Inak povedané, $\gcd(a, b)$ je najväčší (vzhľadom na usporiadanie $|$) prvok z množiny čísel, ktoré súčasne delia a aj b (=spoločné delitele čísel a, b).

Priamo z definície vidno, že najväčší spoločný deliteľ (ak existuje) je určený jednoznačne až na asociovanosť.[6]

Pre okruhy $\mathbb{Z}$ a $F[x]$ sa vďake vete o delení so zvyškom dá na dôkaz existencie a výpočet najväčšieho spoločného deliteľa použiť tzv. Euklidov algoritmus, ktorý je založený na nasledujúcom tvrdení

Lema 4.3.12. *Ak R je obor integrity a $a, b \in R$, tak*

$$\gcd(a, b) = \gcd(a + bx, b)$$

pre ľubovoľné $x \in R$. Uvedenú rovnosť treba chápať tak, že ak existuje jedna strana (ľavá alebo pravá), potom existuje aj druhá a platí uvedená rovnosť.

Dôkaz. Nech $c = \gcd(a, b)$ (t.j. okrem iného existuje $\gcd(a, b)$), t.j. $c \mid a$, $c \mid b$. Vďaka tvrdeniu 4.3.3(vii) potom $c \mid a + bx$ a samozrejme aj $c \mid b$. Takže $\gcd(a, b)$ má vlastnosť 1 z definície najväčšieho spoločného deliteľa pre prvky $a + bx, b$. Nech teraz $d \mid a + bx$, $d \mid b$. Potom opäť z 4.3.3(vii) dostávame, že $d \mid (a + bx) + b(-x) = a$, $d \mid b$, čiže $d \mid c = \gcd(a, b)$. Preto $\gcd(a + bx, b)$ existuje a $\gcd(a, b) = \gcd(a + bx, b)$.

[6] Pretože najväčší spoločný deliteľ nie je jednoznačne určený, nemal by som používať označenie $c = \gcd(a, b)$; znamienko rovnosti typicky používame keď na oboch stranách máme jednoznačne určený objekt. Na druhej strane napríklad pri okruhoch $\mathbb{Z}$ a $F[x]$ sme z viacerých možností schopný vybrať „pekného“ reprezentanta. V $\mathbb{Z}$ vyberieme nezáporné číslo, v $F[x]$ vyberieme polynóm kde vedúci koeficient je jednotka. Čiže v týchto prípadoch ste asi zvyknutí na takýto výber najväčšieho spoločného deliteľa. Používam v tomto texte zápis s rovnosťou – ale upozornil som na to, že nie je úplne korektný.

Dokázali sme, že ak pre $a, b \in R$ existuje $\gcd(a, b)$, tak pre každé $x \in R$ existuje aj $\gcd(a + bx, b)$ a platí uvedená rovnosť. Teda vidíme, že ak existuje $\gcd(a + bx, b)$, tak existuje aj $\gcd((a + bx) + b(-x), b)$, t.j. $\gcd(a, b)$ a platí uvedená rovnosť. □

Ak postupne počítame zvyšky po delení, vieme ich vyjadriť ako kombináciu polynómov $a = a(x)$, $b = b(x)$. Rovnaký postup môžeme použiť pre celé čísla, v postupe stačí stupeň polynómu nahradiť absolútnou hodnotou čísla.

$$\begin{aligned}
a &= q_1 \cdot b + r_1 && \mathrm{st}(r_1) < \mathrm{st}(b) && r_1 = a - q_1.b \\
b &= q_2 \cdot r_1 + r_2 && \mathrm{st}(r_2) < \mathrm{st}(r_1) && r_2 = b - q_2.r_1 = (1 + q_1q_2)b - q_2a \\
r_1 &= q_3 \cdot r_2 + r_3 && \mathrm{st}(r_3) < \mathrm{st}(r_2) && r_3 = r_2 - q_3.r_2 = \cdots = x_3a + y_3b \\
&\vdots && && \vdots \\
r_{l-2} &= q_l \cdot r_{l-1} + r_l && \mathrm{st}(r_l) < \mathrm{st}(r_{l-1}) && r_l = r_{l-2} - q_l.r_{l-1} = \cdots = x_la + y_lb \\
r_{l-1} &= q_{l+1} \cdot r_l && \text{zvyšok } 0
\end{aligned}$$

Pretože v každom kroku stupeň (absolútna hodnota) zvyšku klesá, po istom čase sa algoritmus musí zastaviť a dostaneme nulový zvyšok. Navyše, z predchádzajúcej lemy vidíme, že v každom kroku platí $\gcd(r_k, r_{k-1}) = \gcd(a, b)$ (ak uvedené najväčšie spoločné delitele existujú), preto na konci platí $\gcd(a, b) = \gcd(r_{l-1}, r_l) = \gcd(q_{l+1}r_l, r_l) = r_l$. Ale je jasné, že $\gcd(q_{l+1}r_l, r_l)$ existuje a platí $\gcd(q_{l+1}r_l, r_l) = r_l$, preto existujú všetky uvedené najväčšie spoločné delitele, špeciálne existuje $\gcd(a, b)$.

Ďalej, každý zvyšok sme vedeli vyjadriť v tvare $r_k = x_ka + y_kb$, kde $x_k, y_k \in R$, čiže týmto algoritmom vieme získať takéto vyjadrenie pre $\gcd(a, b)$.

Takže máme vetu

Tvrdenie 4.3.13. *Ak R je okruh $\mathbb{Z}$ alebo $F[x]$, tak pre ľubovoľné $a, b \in R$ existuje v R najväčší spoločný deliteľ $c = \gcd(a, b)$.*

Navyše, existujú také $x, y \in R$, že

$$c = xa + yb.$$

Uvedený postup na výpočet $\gcd(a, b)$ sa nazýva Euklidov algoritmus - jeho výstup je teda $\gcd(a, b)$. Postup naviac umožnuje aj výpočet/určenie prvkov (polynómov, čísiel) $x, y \in R$ takých, že $\gcd()a, b) = xa + yb$, ak aj tieto výpočty zahrnieme do nášho algoritmu, nazývame ho rozšírený Euklidov algotitmus (jeho výstup sú teda hodnoty $\gcd(a, b)$ a x, y také, že $\gcd()a, b) = xa + yb$ — tieto hodnoty nie sú určené jednoznačne, ale uvedný výpočet vždy poskytne rovnaký výsledok).

Naviac, je vidieť, že Euklidov algoritmus môžeme použiť v každom obore integrity, v ktorom nejakým rozumným spôsobom platí veta o delení so zvyškom (t.j. analógia viet 4.2.7 a 4.2.10, akurát budeme musieť nahradiť stupeň, resp. absolútnu hodnotu nejakou inou funkciou, ktorá bude "kontrolovať veľkosť"zvyšku, také okruhy sa nazývajú *Euklidovské okruhy.*)

Z predchádzajúceho tvrdenia dostávame nasledujúci dôsledok, ktorý je často užitočný.

Dôsledok 4.3.14. *Nech R je okruh $\mathbb{Z}$ alebo $F[x]$, $a, b, c \in R$, $a, b \neq 0$. Ak $\gcd(a, b) = 1$ ($\gcd(a, b) \sim 1$) a $a \mid bc$, tak $a \mid c$.*

$$\gcd(a, b) = 1 \quad \wedge \quad a \mid bc \qquad \Rightarrow \qquad a \mid c$$

Dôkaz. Z tvrdenia 4.3.13 máme existenciu $x, y \in R$ takých, že

$$ax + by = 1.$$

Potom

$$a \mid ac \cdot x + bc \cdot y = (ax + by)c = c.$$

□

Ukážeme si postup na výpočet najväčšieho spoločného deliteľa pomoocou Euklidovho algoritmu na konkrétnych príkladoch – najprv v $\mathbb{Z}$. (Najväčší spoločný deliteľ v $\mathbb{Z}$ viete zo strednej školy rátať pomocou rozkladu na prvočísla – niečo podobné platí všeobecne, ako uvidíme v tvrdení 4.3.27. Takýto postup nám však neposkytuje najväčší spoločný deliteľ ako kombináciu daných čísel – v príklade 4.3.16 uvidíme, že takéto vyjadrenie pre n.s.d. môže byť užitočné. Navyše to predpokladá, že poznáme rozklad na ireducibilné prvky – čo zatiaľ v $F[x]$ nevieme robiť vôbec, v $\mathbb{Z}$ to vieme robiť pre malé čísla. Pre veľké čísla je výpočtovo efektívnejší Euklidov algoritmus.)

Príklad 4.3.15. Chceme vyrátať $d = \gcd(89, 16)$ a vyjadriť ho v tvare $89u + 16v$.

Keď použijeme viackrát vetu o delení so zvyškom, tak dostaneme:

$$\begin{aligned} 89 &= 5 \cdot 16 + 9 & 9 &= 89 - 5 \cdot 16 \\ 16 &= 1 \cdot 9 + 7 & 7 &= 16 - 9 = 6 \cdot 16 - 89 \\ 9 &= 1 \cdot 7 + 2 & 2 &= 9 - 7 = 2 \cdot 89 - 11 \cdot 16 \\ 7 &= 3 \cdot 2 + 1 & 1 &= 7 - 3 \cdot 2 = 39 \cdot 16 - 7 \cdot 89 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

Z lemy 4.3.12 potom vidíme, že $\gcd(89, 16) = \gcd(16, 9) = \gcd(9, 7) = \gcd(7, 2) = \gcd(2, 1) = 1$. V pravom stĺpci sme dostali hľadané vyjadrenie

$$1 = 39 \cdot 16 - 7 \cdot 89.$$

Tento postup môžeme prehľadne zapísať aj do tabuľky.

89	1	0	
16	0	1	
9	1	-5	`1r-5*2r`
7	-1	6	`2r-3r`
2	2	-11	`3r-4r`
1	-7	39	`4r-3*5r`

Tento postup do istej miery pripomína riadkové úpravy na matici. V každom riadku máme koeficienty, pomocou ktorých vieme číslo z prvého stĺpca vyjadriť ako celočíselnú kombináciu čísel 89 a 16.

Posledný stĺpec tabuľky sme doplnili len na to, aby bolo vidno, aké úpravy sme robili. Môže to byť užitočné pri hľadaní prípadnej chyby – tento stĺpec ale v podstate nie je nutný. Postupovali sme presne podľa vety o delení so zvyškom. Ak rátate niečo takéto ručne, pri malých číslach si občas môžete všimnúť aj nejaké veci, ktoré vám trochu urýchlia výpočet. Napríklad ak si všimnete, že $2 = 2 \cdot 9 - 16$, ušetríte jeden riadok. (Treba si ale dávať pozor, či zrýchlený postup je správny – v podstate si stačí pamätať lemu 4.3.12 a postupovať podľa nej.)

89	1	0	
16	0	1	
9	1	-5	`1r-5*2r`
2	2	-11	`2*4r-3r`
1	-7	39	`3r-4*4r`

V predošlom príklade sme našli jednu dvojicu (u, v) takú, že $89u + 16v = 1$. Je to jediná možnosť? Vedeli by ste nájsť všetky ostatné také dvojice?

Príklad 4.3.16. Inverzné prvky v poli $\mathbb{Z}_p$ (kde p je prvočíslo) sme zatiaľ vedeli počítať iba takým spôsobom, že sme postupne skúšali všetky prvky poľa. Euklidov algoritmus, ktorý sme sa teraz naučili, môžeme využiť na ten istý účel.

Pokúsme sa vypočítať 5^{-1} v $\mathbb{Z}_{13}$. Pretože 13 je prvočíslo platí $\gcd(5, 13) = 1$, čiže vieme nájsť čísla $x, y \in \mathbb{Z}$ také, že $1 = 5x + 13y$.

Postupným delením dostaneme

$$\begin{aligned} 13 &= 2 \cdot 5 + 3 & 3 &= 1 \cdot 13 - 2 \cdot 5 \\ 5 &= 1 \cdot 3 + 2 & 2 &= 5 - 3 = 3 \cdot 5 - 1 \cdot 13 \\ 3 &= 1 \cdot 2 + 1 & 1 &= 3 - 2 = 2 \cdot 13 - 5 \cdot 5 \end{aligned}$$

Ak pre všetky čísla v rovnosti $1 = 2.13 - 5.5$ urobíme zvyšok po delení 13, dostaneme rovnosť

$$1 = -5 \odot 5 = 8 \odot 5,$$

ktorá platí v $\mathbb{Z}_{13}$. Teda v $\mathbb{Z}_{13}$ platí $5^{-1} = 8$.

Opäť ten istý postup by sme mohli zapísať tabuľkou:

13	1	0	
5	0	1	
3	1	-2	`1r-2*2r`
2	-1	3	`2r-3r`
1	2	-5	`3r-4r`

Vyskúšajme si aspoň jeden konkrétny príklad v $\mathbb{Q}[x]$. Vieme, že najväčší spoločný deliteľ je určený jednoznačne až na asociovanosť – čiže v tomto prípade až na vynásobenie konštantou. Dohodnime sa, že si vyberieme ten, ktorý má vedúci koeficient 1 (tzv. normovaný polynóm) – potom už je najvúčší spoločný deliteľ určený jednoznačne.

Príklad 4.3.17. Vypočítajte $d(x) = \gcd(f(x), g(x))$ a vyjadrite ho v tvare $d(x) = u(x)f(x) + v(x)g(x)$ pre polynómy $f(x) = 3x^5 + 5x^4 - 16x^3 - 6x^2 - 5x - 6$, $g(x) = 3x^4 - 4x^3 - x^2 - x - 2$.

Podobne ako v predchádzajúcom príklade, budeme polynómy postupne deliť so zvyškom a zvyšok si v každom kroku vyjadríme ako kombináciu $f(x)$ a $g(x)$.

Kvôli prehľadnosti som zapísal zvlášť delenie polynómov a zvlášť vyjadrenie zvyšku v tvare kombinácie $f(x)$ a $g(x)$.

$$3x^5 + 5x^4 - 16x^3 - 6x^2 - 5x - 6 = (x + 3)(3x^4 - 4x^3 - x^2 - x - 2) - 3x^3 - 2x^2$$
$$3x^4 - 4x^3 - x^2 - x - 2 = (-3x^3 - 2x^2)(-x + 2) + 3x^2 - x - 2$$
$$-3x^3 - 2x^2 = (3x^2 - x - 2)(-x - 1) + (-3x - 2)$$

Vieme, že posledný nenulový zvyšok $-3x - 2$ v Euklidovom algoritme je hľadaný najväčší spoločný deliteľ. Pretože chceme dostať normovaný polynóm, vydelíme ho ešte vedúcim koeficientom -3.

$$\gcd(f(x), g(x)) = x + \frac{2}{3}$$

Zvyšky v jednotlivých deleniach vyjadríme pomocou $f(x)$ a $g(x)$ takto

$$-3x^3 - 2x^2 = f(x) - g(x)(x + 3)$$

$$\begin{aligned}3x^2 - x - 2 &= g(x) - (-3x^3 - 2x^2)(-x + 2) = \\ &g(x) - (f(x) - g(x)(x + 3))(-x + 2) = \\ &f(x)(x - 2) + [1 - (x - 2)(x + 3)g(x)] = \\ &(x - 2)f(x) - (x^2 + x - 7)g(x)\end{aligned}$$

$$\begin{aligned}-3x - 2 = &- 3x^3 - 2x^2 - (3x^2 - x - 2)(-x - 1) = \\ &f(x) - g(x)(x + 3) + [(x - 2)f(x) - (x^2 + x - 7)g(x)](x + 1) = \\ &f(x)[1 + (x - 2)(x + 1)] - g(x)[(x + 3) + (x + 1)(x^2 + x - 7)] = \\ &f(x)(x^2 - x - 1) - g(x)(x^3 + 2x^2 - 5x - 4)\end{aligned}$$

Po vydelení poslednej rovnosti číslom -3 dostávame

$$\gcd(f(x), g(x)) = x + \frac{2}{3} = -f(x)\frac{x^2 - x - 1}{3} + g(x)\frac{x^3 + 2x^2 - 5x - 4}{3}.$$

Opäť, pokiaľ by Vám to lepšie vyhovovalo, celý postup si môžete zapísať do tabuľky.

$f(x) = 3x^5 + 5x^4 - 16x^3 - 6x^2 - 5x - 6$	1	0
$g(x) = 3x^4 - 4x^3 - x^2 - x - 2$	0	1
$h_1(x) = f(x) - (x + 3)g(x) = -3x^3 - 2x^2$	1	$-(x + 3)$
$h_2(x) = g(x) + (x - 2)h_1(x) = 3x^2 - x - 2$	$x - 2$	$-(x^2 + x - 7)$
$h_3(x) = h_1(x) + (x + 1)h_2(x) = -3x - 2$	$x^2 - x - 1$	$-(x^3 + 2x^2 - 5x - 4)$
$h_2(x) + (x - 1)h_3(x) = 0$		

V predposlednom riadku sa naposledy vyskytol nenulový zvyšok, čiže ide o $\gcd(f(x), g(x))$. Z tohoto riadku vieme aj jeho vyčítať vyjadrenie – také isté, ako sme dostali v predchádzajúcom postupe. (Presnejšie povedané, dostali sme rovnaké vyjadrenie až na prenásobenie konštantou – vynormovanie.)

Pri výpočtoch takého typu ako sme robili v predchádzajúcom príklade sa celkom ľahko dá pomýliť – preto je užitočné občas (povedzme po každom kroku) vyskúšať, či rovnosti, ktoré sme dostali pre polynómy skutočne platí aj po dosadení nejakých čísel. (Je rozumné skúšať malé, čísla, napríklad 0, ± 1 – aby sa nám ľahko počítali hodnoty polynómu v týchto číslach.) Pri takejto čiastočnej skúške správnosti máme veľkú šancu prípadnú chybu odhaliť. (Samozrejme, dá sa urobiť skúška aj tak, že kombináciu $f(x)$ a $g(x)$, ktorú sme dostali, skutočne poroznásobujeme a zistíme, či vyjde rovnaký polynóm ako na druhej strane rovnosti – čo je však o dosť prácnejšie.)

Ak v priebehu výpočtu nám vyjde ako jeden zo zvyškov polynóm, v ktorom všetky koeficienty sú násobkom toho istého celého čísla, môžeme polynóm týmto číslom vydeliť – dostaneme opäť polynóm s celočíselnými koeficientami (teda sa nám s ním bude dobre počítať) a neovplyvníme hodnotu najväčšieho spoločného deliteľa (v okruhu $F[x]$ sme tento polynóm zmenili len o deliteľ jednotky). Je ale dôležité pri vyjadrovaní najväčšieho spoločného deliteľa pomocou $f(x)$ a $g(x)$ nezabudnúť zarátať aj toto vydelenie.

4.3.2 Rozklad polynómu na irebucibilné polynómy

Pojem analogický k pojmu prvočísla je v okruhu pojem ireducibilného prvku.

Definícia 4.3.18. Prvok $a \neq 0$ obore integrity R sa nazýva *ireducibilný,* ak a je nenulový, nie je to deliteľ jednotky a ak z rovnosti $a = bc$ vyplýva, že niektorý z prvkov b, c je deliteľ jednotky v R.

Inými slovami, ireducibilný prvok sa (až na asociovanosť a výmenu poradia) nedá zapísať ako súčin dvoch prvkov z R inak ako $1 \cdot a$. Zrejme, ak sú p, q dva ireducibilné prvky v R a $p \mid q$, tak $p \sim q$, t.j. p a q sú asociované.

Príklad 4.3.19. Vieme, že prvočísla boli definované tak, že ich rozklad na súčin $p = a \cdot b$ je možný iba vtedy, ak niektoré z čísel a, b je rovné 1. Z toho vidno, že ireducibilné prvky v $\mathbb{Z}$ sú práve čísla tvaru $\pm p$, kde p je prvočíslo.

Ireducibilné prvkami v okruhu $F[x]$ sa volajú ireducibilné polynómy. Je vidieť, že každý polynóm stupňa 1 je ireducibilný.

Naším najbližším cieľom je dokázať, že v okruhu $F[x]$ platí tvrdenie zodpovedajúce rozkladu prirodzených (celých) čísel na súčin prvočísel.

Definícia 4.3.20. *Okruh s jednoznačným rozkladom* (alebo tiež *Gaussov okruh*) je obor integrity, v ktorom pre každý prvok $x \in R$, ktorý je nenulový a nie je deliteľom jednotky, existuje rozklad

$$x = p_1 \dots p_k$$

na súčin ireducibilných prvkov a navyše je tento rozklad jednoznačný až na asociovanosť a poradie.

Z tvrdenia 4.3.14 vyplýva nasledujúci veľmi dôležitý vzťah.

Dôsledok 4.3.21. *Nech R je okruh $\mathbb{Z}$ alebo $F[x]$. Pre ľubovoľný ireducibilný prvok $p \in R$ platí implikácia*

$$p \mid ab \qquad \Rightarrow \qquad p \mid a \vee p \mid b,$$

a všeobecnejšie,

$$p \mid a_1 \dots a_n \qquad \Rightarrow \qquad (\exists i \in \{1, \dots, n\})\ p \mid a_i.$$

Dôkaz. Keďže $\gcd(p, a) \mid p$, v prípade, že $\gcd(p, a) \nsim 1$ z ireducibily p vyplýva, že $\gcd(p, a) \sim p$ a preto $p \mid a$. Nech teda $\gcd(p, a) \sim 1$. Potom z lemy 4.3.14 dostávame, že $p \mid b$.

Druhá, všeobecnejšia časť odtiaľto vyplýva jednoduchou indukciou. □

Teraz už sme schopní vysloviť a dokázať tvrdenie o rozklade na súčin ireducibilných prvkov.

Tvrdenie 4.3.22. *Každý okruh typu $F[x]$ (a aj okruh $\mathbb{Z}$) je okruhom s jednoznačným rozkladom.*

Dôkaz. Dôkaz spravíme len pre okruhy typu $F[x]$, dôkaz existencie pre $\mathbb{Z}$ je veľmi podobný, len sa použije absolútna hodnota namiesto stupňa polynómu. Dôkaz jednoznačnosti je pre obidva prípady úplne rovnaký — vyplýva totiž jednoduchým spôsobom z dôsledku 4.3.21 a z vety o krátení (tvrdenie 4.1.14) a teda vidieť, že vyplýva z viet/tvrdení, ktoré sme formulovali pre prípady okruhov $\mathbb{Z}$ a $F[x]$.

Existencia. Indukciou podľa stupňa polynómu. Nech by $p \in F[x]$ nie je nula ani deliteľ jednotky, to znamená, že je to polynóm stupňa aspoň 1.

Prvý krok indukcie: nech je $\operatorname{st} p = 1$. Potom je to ireducibilný polynóm.

Druhý krok indukcie. Zoberme $n > 1$, nech sa každý polynóm stupňa menšieho ako n dá rozložiť na súčin konečne veľa ireducibilných polynómov. Dokážeme, že aj p sa dá rozložiť na súčin konečne veľa ireducibilných polynómov.

Ak je p ireducibilný, nemámem čo dokázať. Nech nie je ireduciblinlý a nech $p = f \cdot g$, kde $f \nsim 1$, $g \nsim 1$. Preto je $1 \leq \operatorname{st} f$, $1 \leq \operatorname{st} g$ a keďže $\operatorname{st} f + \operatorname{st} g = \operatorname{st} p$, dostávame, že $\operatorname{st} f < \operatorname{st} p$, $\operatorname{st} g < \operatorname{st} p$. Podľa indukčného predpokladu teda existujú ireducibilné polynómy $p_1, \dots, p_m \in F[x]$ a $p_{m+1}, \dots, p_n \in F[x]$ také, že $f = p_1 \dots p_m$ a $g = p_{m+1} \dots p_n$ a preto $p = p_1 \dots p_n$, čiže p sa tiež dá napísať ako súčin konečne veľa ireducibilných polynómov. □

Z predchádzajúceho tvrdenia špeciálne dostávame, že každé prirodzené číslo vieme napísať ako súčin prvočísel jednoznačne až na poradie. (A po pridaní deliteľov jednotky ± 1 dostaneme všetky celé čísla.)

Skúsme nájsť príklad oboru integrity, ktorý nie je okruh s jednoznačným rozkladom.

Príklad 4.3.23. Budeme pracovať v okruhu $\mathbb{Z}[2i] = \{a + 2bi; a, b \in \mathbb{Z}\}$. Zrejme ide o obor integrity (je to podokruh poľa $\mathbb{C}$). Jediné delitele jednotky v tomto okruhu sú ± 1. Pozrime sa na rozklad $4 = 2.2 = (2i)(-2i)$.

Prvky 2 aj $\pm 2i$ sú ireducibilné. Ak totiž máme $2 = ab$, tak platí aj $2 = |a|.|b|$, a $|a|, |b|$ (budú) sú celé čísla ($|a|$ tu znamená absolútnu hodnotu komplexného čísla, je vidieť, že ak $z = c + 2di \in \mathbb{Z}[2i]$ a $d \neq 0$ tak, $|z| \geq 2$ a pre nenulové $z \in \mathbb{Z}[2i]$ je $|z| \geq 1$, čiže je len málo možností, ako dosiahnuť, aby $2 = |a||b|$ a pri každej z tých možností sú $|a|, |b|$ celé čísla - rozmyslite si to). Potom pre niektoré z čísel a, b musí platiť, že má veľkosť 1. Takéto prvky v $\mathbb{Z}[2i]$ sú však iba ± 1, zistili sme teda, že niektoré z čísel a, b je deliteľ jednotky. Tým sme overili, že 2 je ireducibilný prvok, zdôvodnenie pre $\pm 2i$ je presne rovnaké, opäť využijeme, že $|\pm 2i| = 2$.

Súčasne 2 je asociovaný iba s prvkami ± 2. Našli sme teda dva rozklady čísla 4 na súčin ireducibilných prvkov, ktoré sa nelíšia iba asociovanosťou. Teda $\mathbb{Z}[2i]$ nie je okruh s jednoznačným rozkladom.

Príklad 4.3.24. Ďalším takýmto príkladom je $\mathbb{Z}[\sqrt{5}i] = \{a + b\sqrt{5}i; a, b \in \mathbb{Z}\}$. V tomto okruhu máme rozklady

$$6 = 2.3 = (1 + \sqrt{5}i)(1 - \sqrt{5}i).$$

Vidno, že 2 nedelí žiaden z činiteľov na pravej strane. Ak ukážeme, že 2 je ireducibilný prvok, tak z dôsledku 4.3.21 vyplýva, že to nie je okruh s jednoznačným rozkladom.

Nech $2 = x.y$, kde $x, y \in \mathbb{Z}[\sqrt{5}i]$. Potom $|x| \leq 2$ aj $|y| \leq 2$, lebo všetky prvky tohoto okruhu majú vlastnosť $|x| \geq 1$. Ak $x = a + \sqrt{5}i$, tak sme dostali

$$|x|^2 = a^2 + 5b^2 \leq 4,$$

čo je možné jedine v prípade $b = 0$. Rozklad $2 = x.y$ je teda v skutočnosti rozklad na súčin dvoch celých čísel. V takomto rozklade musí byť nevyhnutne niektorý z činiteľov rovný ± 1.

Poznamenajme, že podobný spôsobom sa dá ukázať, že aj 3 a $1 \pm \sqrt{5}i$ sú ireducibilné.

Príklad 4.3.25. Dá sa dokázať, že ak R je okruh s jednoznačným rozkladom, tak aj okruh polynómov $R[x]$ je okruh s jednoznačným rozkladom. (Pozri napríklad [KGGS, Lema 7.4.1], [DF, Corollary 9.6]). Ak sme ochotní uveriť tomuto tvrdeniu, tak máme $\mathbb{Z}[x]$ ako príklad Gaussovho okruhu (ktorý nie je okruh hlavných ideálov — pojem okruhu hlavných ideálov budeme definovať v nasledujúcom semestri).

V prípade, že máme rozklad prvkov a, b Gaussovho okruhu R, môžeme z neho zistiť, či $a \mid b$ ako aj určiť rozklad ich najväčšieho spoločného deliteľa $\gcd(a, b)$.

Lema 4.3.26. *Nech R je Gaussov okruh a $a, b \in R$. Ak $a = p_1 \dots p_n$ a $b = q_1 \dots q_m$ sú rozklady týchto prvkov na súčin ireducibilných činiteľov, tak $a \mid b$ práve vtedy, keď existuje injekcia $f\colon \{1, 2, \dots, n\} \to \{1, 2, \dots, m\}$ s vlastnosťou $q_{f(m)} \sim p_m$.*

(*Toto tvrdenie je len formálny zápis faktu, že všetky ireducibilné prvky z rozkladu a sa musia vyskytnúť aj v rozklade b, pričom ak sa tam vyskytuje viackrát prvok z tej istej triedy asociovanosti, tak sa toľkokrát musí vyskytnúť aj v rozklade b.*)

Dôkaz. D.Ú. □

Tvrdenie 4.3.27. *Nech R je Gaussov okruh, $a, b \in R \setminus \{0\}$. Majme tieto prvky vyjadrené v tvare $a = up_1^{k_1} \dots p_n^{k_n}$ a $b = u'p_1^{l_1} \dots p_n^{l_n}$, kde $u, u' \in U(R)$ a $p_1, \dots, p_n$ sú po dvoch neasociované ireducibilné prvky v R. Potom*

$$d = p_1^{m_1} \dots p_n^{m_n},$$

kde $m_i = \min\{k_i, l_i\}$ pre $i = 1, \dots, n$ je ich najväčší spoločný deliteľ.

Dôkaz. D.Ú. □

Cvičenia

Úloha 4.3.1. Ak u je deliteľ jednotky v okruhu R, tak aj $-u$ je deliteľ jednotky.

Úloha 4.3.2.

Úloha 4.3.3. Nech R je euklidovský okruh a S je jeho podokruh, ktorý obsahuje jednotku. Musí byť aj S euklidovský okruh?

Úloha 4.3.4. Dokážte, že okruhy polynómov $\mathbb{Z}[x]$ a $\mathbb{Q}[x]$ nie sú izomorfné.

4.4 Okruhy polynómov II

V tejto časti sa budeme zaoberať polynómami, pričom často budeme využívať niektoré fakty, ktoré sme dokázali v predchádzajúcej podkapitole pre euklidovské okruhy, resp. pre okruhy s jednoznačným rozkladom. (Vieme, že $R[x]$ je euklidovský okruh, ak R je pole. Bez dôkazu sme si spomenuli, že ak R je Gaussov okruh, tak aj $R[x]$ je Gaussov okruh.)

4.4.1 Korene polynómov

Do polynómu $f(x) \in F[x]$ môžeme dosadiť ľubovoľný prvok c poľa F a vypočítať hodnotu polynómu v tomto prvku. (Zobrazenie, ktoré polynómu priradilo jeho hodnotu v c sme nazvali dosadzovací homomorfizmus – definícia 4.2.15.)

Definícia 4.4.1. Nech F je pole a F' je jeho nadpole. Prvok $c \in F'$ nazývame *koreňom* polynómu $f(x) \in F[x] \subset F'[x]$, ak $f(c) = 0$ (t.j. po dosadení c do polynómu F dostaneme 0).

V predchádzajúcej definícii dosadzujeme do polynómu z $F[x]$ prvok z nadpoľa F'. To však nie je problém – keďže koeficienty polynómu $f(x)$ sú z $F \subseteq F'[x]$, tento polynóm súčasne patrí do $F'[x]$.

Príklad 4.4.2. Číslo i je koreňom polynómu $x^2 + 1$, lebo $i^2 + 1 = 0$.

Všimnime si, aký je vzťah medzi koreňmi polynómu a deliteľnosťou lineárnymi polynómami.

Lema 4.4.3. *Ak $f(x) \in F[x]$, kde F je pole, a $c \in F$, tak zvyšok polynómu $f(x)$ po delení polynómom $x - c$ je rovný $f(c)$, t.j. existuje polynóm $g(x) \in F[x]$ taký, že*

$$f(x) = (x - c)g(x) + f(c). \tag{4.1}$$

Dôkaz. Z vety o delení so zvyškom vieme

$$f(x) = g(x)(x-c) + r,$$

pričom zvyšok je polynóm stupňa menšieho ako 1, preto je to nejaká konštanta $r \in F$.

Ak do predošlej rovnosti dosadíme c za x, tak máme

$$f(c) = g(c)(c-c) + r = r,$$

čiže táto konštanta musí byť rovná práve $f(c)$, t.j. hodnote polynómu f v bode c. □

Z predchádzajúcej lemy už ľahko dostaneme

Lema 4.4.4. *Nech F je pole a F' je jeho nadpole. Nech $f(x) \in F[x]$. Potom $c \in F'$ je koreňom $f(x)$ práve vtedy, keď $x - c \mid f(x)$ v $F'[x]$, t.j. existuje polynóm $g(x) \in F'[x]$ taký, že $f(x) = g(x)(x-c)$.*

Dôkaz. Podľa (4.4.3) máme $f(x) = (x-c)g(x)+f(c)$, čiže ak $f(c) = 0$, tak $f(x) = (x-c)g(x)$, čiže $x - c \mid f(x)$.

Obrátene, ak $x - c \mid f(x)$, tak zvyšok po delení polynómu $f(x)$ polynómom $x - c$ je 0, čiže (opäť z lemy 4.4.3) $f(c) = 0$ a c je koreň polynómu f. □

Definícia 4.4.5. Nech F' je nadpole poľa F, $f(x) \in F[x]$ a c je koreň $f(x)$. Hovoríme, že *násobnosť* koreňa c je k (alebo tiež, že c je k-násobný koreň $f(x)$), ak $(x-c)^k \mid f(x)$ (t.j. ak existuje polynóm $g(x) \in F'[x]$ taký, že $f(x) = g(x)(x-c)^k$) a súčasne $(x-c)^{k+1} \nmid f(x)$.

Pre $k = 1$ voláme k-násobný koreň *jednoduchý koreň* polynómu $f(x)$, ak $k > 1$ tak hovoríme o násobnom koreni.

Príklad 4.4.6. Čísla ± 1 sú dvojnásobné korene polynómu $x^4 - 2x^2 + 1$, lebo $x^4 - 2x^2 + 1 = (x^2-1)^2 = (x-1)^2(x+1)^2$

Jednoduchý spôsob ako ručne spočítať hodnotu polynómu v danom čísle (a tým zistiť, či toto číslo je koreňom polynómu) je použitie Hornerovej schémy.

Základná idea Hornerovej schémy je, že hodnotu polynómu môžeme vyjadriť ako

$$a_n c^n + a_{n-1}c^{n-1} + \cdots + a_0 = \left(a_n c^{n-1} + \cdots + a_1\right) c + a_0 = \\ ((\ldots(a_n c + a_{n-1})c + \ldots)c + a_1)c + a_0$$

Stačí nám teda postupne počítať čísla a_n, $a_n c + a_{n-1}$, $(a_n c + a_{n-1})c + a_{n-2}$ atď., t.j. predchádzajúci výsledok vždy vynásobíme číslom c a pripočítame k nemu nasledujúci koeficient.

Príklad 4.4.7. Vypočítajte hodnotu polynómu $f(x) = x^4 - 3x^3 + 2x - 1$ nad poľom $\mathbb{R}$ v bode $c = 2$.

Do tabuľky si zapíšeme koeficienty polynómu (dôležité je nezabudnúť na nulový koeficient pochádzajúci z člena $0x^2$) a postupujeme postupom, ktorý sme naznačili.

	1	-3	0	2	-1
2		2	-2	-4	-4
	1	-1	-2	-2	$\boxed{-5}$

Všimnime sme, že súčasne sme vypočítali, že

$$x^4 - 3x^3 + 2x - 1 = (x^3 - x^2 - 2x - 2)(x-2) - 5.$$

(Stačí si uvedomiť, že pri Hornerovej schéme vlastne robíme to isté, čo pri algoritme na delenie polynómov.)

Aby sme si uvedomili, čo vlastne v Hornerovej schéme počítame, pokúsme sa ju zapísať o čosi všeobecnejšie (kvôli šírke rozdelené na 2 tabuľky)

	a_n	a_{n-1}	a_{n-2}	$\dots$
c		a_nc	$(a_nc+a_{n-1})c$	$\dots$
	a_n	a_nc+a_{n-1}	$a_nc^2+a_{n-1}c+a_{n-2}$	$\dots$

$\dots$	a_1	a_0
$\dots$	$\dots$	$(a_nc^{n-1}+a_{n-1}c^{n-2}+\dots+a_1)c$
$\dots$	$a_nc^{n-1}+a_{n-1}c^{n-2}+\dots+a_1$	$a_nc^n+a_{n-1}c^{n-1}+\dots+a_1c+a_0=f(c)$

Príklad 4.4.8. Overte, že 1 je koreňom polynómu $f(x)=x^4-3x^3+3x-1\in\mathbb{R}[x]$. Zistite násobnosť tohoto koreňa.

Budeme postupovať pomocou Hornerovej schémy – pri vypočítaní hodnoty $f(1)$ súčasne nájdeme polynóm $g(x)$ taký, že $f(x)=g(x)(x-1)+f(1)$. Ak $f(1)=0$, na zistenie, či ide násobnosť tohoto koreňa je aspoň 2, stačí overiť, či aj $g(1)=0$. Analogicky postupujeme ďalej, až kým nedostaneme nenulový zvyšok.

	1	-3	0	3	-1
1		1	-2	-2	1
	1	-2	-2	1	$\boxed{0}$
1		1	-1	-3	
	1	-1	-3	$\boxed{-2}$	

Zistili sme, že 1 je jednoduchým (jednonásobným) koreňom polynómu $f(x)$ a že

$$f(x)=(x-1)(x^3-2x^2-2x+1),$$

pričom $x-1\nmid x^3-2x^2-2x+1$.

Rátať korene polynómov je vo všeobecnosti ťažká úloha. Zo strednej školy poznáte vzorec na hľadanie koreňov polynómov druhého stupňa – kvadratických polynómov. (Podobné vzorce, aj keď zložitejšie, sa dajú nájsť aj pre rovnice tretieho a štvrtého stupňa. Vo všeobecnosti však také vzorce neexistujú.) Okrem nich vieme ešte v komplexných číslach riešiť binomické rovnice, t.j. rovnice tvaru $x^n=a$, kde $a\in\mathbb{C}$ (pozri I-B.3.2 alebo [KGGS, kapitola 6.1]).

Povieme si, ako pre polynóm s celočíselnými koeficientami vieme nájsť všetky korene, ktoré sú racionálnymi číslami (t.j. všetky korene daného polynómu ležiace v poli $\mathbb{Q}$).

4.4.2 Racionálne korene polynómu s celočíselnými koeficientami

Tvrdenie 4.4.9. *Ak $f(x)=a_nx^n+a_{n-1}x^{n-1}+\dots+a_0\in\mathbb{Z}[x]$ je polynóm s celočíselnými koeficientami a racionálne číslo $c=\frac{p}{q}$ je koreň $f(x)$ (pričom $\gcd(p,q)=1$, t.j. racionálne číslo c je zapísané v základnom tvare), tak*

$$p\mid a_0 \qquad a \qquad q\mid a_n.$$

Dôkaz. Ak $c=\frac{p}{q}$ je koreň $f(x)$, tak máme rovnosť

$$f(c)=a_n\frac{p^n}{q^n}+a_{n-1}\frac{p^{n-1}}{q^{n-1}}+\dots+a_1\frac{p}{q}+a_0=0.$$

Ak túto rovnosť vynásobíme q^n, dostaneme

$$a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1} + a_0 q^n = 0.$$

(Všimnime si, že v predchádzajúcej rovnosti vystupujú iba celé čísla.)

Túto rovnosť môžeme upraviť ako

$$-a_n p^n = (a_{n-1} p^{n-1} + \cdots + a_1 p q^{n-2} + a_0 q^{n-1}) q,$$

čo znamená, že $q \mid a_n p^n$. Pretože $\gcd(p, q) = 1$ (p a q sú nesúdeliteľné), vyplýva z toho $q \mid a_n$ (dôsledok 4.3.14).

Pri dôkaze toho, že $p \mid a_0$ postupujeme takmer rovnako. Máme

$$-a_0 q^n = (a_n p^{n-1} + a_{n-1} p^{n-2} q + \cdots + a_1 q^{n-1}) p,$$

čiže $p \mid a_0 q^n$, a teda (na základe nesúdeliteľnosti) $p \mid a_0$. □

Predchádzajúce tvrdenie môžeme použiť na nájdenie všetkých racionálnych koreňov daného polynómu zo $\mathbb{Z}[x]$. Predchádzajúce tvrdenie nám poskytuje obmedzenie na všetkých možných kandidátov na korene v množine racionálnych čísel. Postupným vyskúšaním nájdeme všetky korene, ktoré patria do $\mathbb{Q}$.

Ďalšie obmedzenie, ktoré nám môže pomôcť pri skúšaní jednotlivých možností, nám poskytne nasledujúce pozorovanie (ktorého špeciálnym prípadom je tvrdenie 4.4.9).

Tvrdenie 4.4.10. *Nech $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ je polynóm s celočíselnými koeficientami a racionálne číslo $c = \frac{p}{q}$ je koreň $f(x)$ (pričom $\gcd(p, q) = 1$, t.j. racionálne číslo c je zapísané v základnom tvare). Nech $g(x) = b_{n-1} x^{n-1} + \cdots + b_0$ je polynóm z $\mathbb{Q}[x]$ taký, že*

$$f(x) = g(x) \left(x - \frac{p}{q} \right). \tag{4.2}$$

Potom aj $g(x) \in \mathbb{Z}[x]$, t.j. koeficienty polynómu $g(x)$ sú celočíselné.

Budeme sa snažiť dokázať toto tvrdenie indukciou. Ale začnime tým, že sa pozrieme aspoň na prvé dva prípady - z toho azda budeme vedieť vymyslieť, čo vlastne chceme indukciou dokazovať (čo všetko potrebujeme, aby prešiel indukčný krok).

Dôkaz. V dôkaze budeme samozrejme využívať rovnosť (4.2), ktorá nám vlastne dáva vzťah medzi koeficientami polynómu $f(x)$ a koeficientami polynómu $g(x)$.

Okrem toho budeme často používať to, že vieme

$$a_n \frac{p^n}{q^n} + a_{n-1} \frac{p^{n-1}}{q^{n-1}} + \cdots + a_1 \frac{p}{q} + a_0 = 0. \tag{4.3}$$

Pre najvyšší koeficient polynómu $g(x)$ platí $b_{n-1} = a_n$.

Všimnime si tiež, že z rovnosti (4.3) máme

$$b_{n-1} \frac{p^n}{q^n} = -a_{n-1} \frac{p^{n-1}}{q^{n-1}} - \cdots - a_1 \frac{p}{q} - a_0.$$

Ak túto rovnosť prenásobíme q^n, tak máme

$$b_{n-1} p^n = -(a_{n-1} p^{n-1} + a_{n-2} p^{n-2} q \cdots + a_1 p q^{n-2} + a_0 q^{n-1}) q.$$

Pretože výraz v zátvorke je celé číslo, máme $q \mid b_{n-1}p^n$. Z toho, že p a q sú nesúdeliteľné, dostávame $q \mid b_{n-1}$. (Vlastne sme zatiaľ iba zopakovali úvahu z dôkazu tvrdenia 4.4.9. Ale asi sa ju oplatí zopakovať, keďže podobnú úvahu budeme používať aj ďalej.)

Pozrime sa na ďalší koeficient. Tento koeficient môžeme vyjadriť ako

$$b_{n-2} = b_{n-1}\frac{p}{q} + a_{n-1} = a_n\frac{p}{q} + a_{n-1}.$$

(Prvú rovnosť dostaneme z Hornerovej schémy. Alebo tiež z porovnania koeficientov pri x^{n-1} v polynómoch $f(x)$ a $g(x)\left(x - \frac{p}{q}\right)$ vidíme, že $a_{n-1} = b_{n-2} - b_{n-1}\frac{p}{q}$.)

Pozrime sa na výraz

$$b_{n-2}\frac{p^{n-1}}{q^{n-1}} = a_n\frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}},$$

ktorý môžeme použitím (4.3) prepísať do tvaru

$$b_{n-2}\frac{p^{n-1}}{q^{n-1}} = -a_{n-2}\frac{p^{n-2}}{q^{n-2}} - \cdots - a_1\frac{p}{q} - a_0.$$

Opäť stačí túto rovnosť vynásobiť q^{n-1} a dostaneme

$$b_{n-2}p^{n-1} = -(a_{n-2}p^{n-2} + a_{n-3}p^{n-3}q \cdots + a_1pq^{n-3} + a_0q_{n-2})q.$$

A podobne ako pri predošlom koeficiente, z toho, že p a q sú nesúdeliteľné máme $q \mid b_{n-2}$.

Teraz sa už dá uhádnuť, že sa zrejme budeme snažiť indukciou dokázať tieto dve veci pre $k = 1, \ldots, n-1$: Platí rovnosť

$$b_{n-k} = a_n\frac{p^{k-1}}{q^{k-1}} + a_{n-1}\frac{p^{k-2}}{q^{k-2}} + \cdots + a_{n-k+1} \tag{4.4}$$

a navyše platí, že b_{n-k} je celé číslo, ktoré je deliteľné číslom q.

Indukčný krok bude vyzerať takto: Predpokladáme, že uvedené tvrdenie platí pre k, pričom $k < n-1$. Chceme dokázať, že platí aj pre $k+1$. Máme rovnosť

$$b_{n-(k+1)} = b_{n-k}\frac{p}{q} + a_{n-k}.$$

Ak za b_{n-k} dosadíme výraz, ktorý máme z indukčného predpokladu, tak dostaneme

$$\begin{aligned} b_{n-(k+1)} &= \left(a_n\frac{p^{k-1}}{q^{k-1}} + a_{n-1}\frac{p^{k-2}}{q^{k-2}} + \cdots + a_{n-k+1}\right)\frac{p}{q} + a_{n-k} \\ &= a_n\frac{p^k}{q^k} + a_{n-1}\frac{p^{k-1}}{q^{k-1}} + \cdots + a_{n-k+1}\frac{p}{q} + a_{n-k} \end{aligned}$$

Teda aj pre $k+1$ platí rovnosť (4.4).

Po vynásobení predošlej rovnosti číslom $\frac{p^{n-k}}{q^{n-k}}$ máme

$$b_{n-(k+1)}\frac{p^{n-k}}{q^{n-k)}} = a_n\frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + \cdots + a_{n-k+1}\frac{p^{n-k+1}}{q^{n-k+1}} + a_{n-k}\frac{p^{n-k}}{q^{n-k}}.$$

z čoho použitím (4.3) dostaneme

$$b_{n-(k+1)}\frac{p^{n-k}}{q^{n-k}} = -a_{n-k-1}\frac{p^{n-k-1}}{q^{n-k-1}} - a_{n-k-2}\frac{p^{n-k-2}}{q^{n-k-2}} - \cdots - a_1\frac{p}{q} - a_0.$$

Opäť stačí túto rovnosť vynásobiť číslom q^{n-k} a máme

$$b_{n-(k+1)}p^{n-k} = (-a_{n-k-1}p^{n-k-1} - a_{n-k-2}p^{n-k-2}q - \cdots - a_1pq^{n-k-2} - a_0q^{n-k-1})q.$$

A znovu si stačí všimnúť, že číslo v zátvorke na pravej strane rovnosti je celé, čiže pravá strana je násobok q. Na základe toho, že p a q sú nesúdeliteľné, dostaneme $q \mid b_{n-(k+1)}$. □

Z predchádzajúceho tvrdenia vyplýva, že ak overujeme, či nejaké racionálne číslo je koreňom polynómu s celočíselnými koeficientami, v okamihu, keď nám v priebehu výpočtu vyjde v spodnom riadku zlomok, už nemusíme rátať ďalej. (Vieme totiž, že čísla v spodnom riadku Hornerovej schémy sú presne koeficienty polynómu $g(x)$, teda ak je dané racionálne číslo koreňom, musia všetky tieto koeficienty podľa predchádzajúceho tvrdenia byť celé čísla.)

Ukážme si teda hľadanie racionálnych koreňov daného polynómu zo $\mathbb{Z}[x]$ na konkrétnom príklade.

Príklad 4.4.11. Nájdite racionálne korene polynómu $f(x) = 24x^5+10x^4-x^3-19x^2-5x+6$ (aj s násobnosťami).

Podľa tvrdenia 4.4.9 má platiť $p \mid 6$, $q \mid 24$. Dostávame teda možnosti:
$p \in \{\pm1, \pm2, \pm3, \pm6\}$
$q \in \{1, 2, 3, 4, 6, 8, 12, 24\}$
$\frac{p}{q} \in \{\pm1, \pm\frac{1}{2}, \pm\frac{1}{3}, \dots\}$
(Pre q nám stačí skúšať kladné hodnoty, pretože voľba znamienok pre číslo p nám zabezpečí obidve možnosti – kladné aj záporné korene.)

Začnime najprv skúšať tých kandidátov na korene, kde čitateľ je ±1.

	24	10	-1	-19	-5	6
1		24	34	33	14	9
	24	34	33	14	9	15

	24	10	-1	-19	-5	6
-1		-24	14	-13	32	-27
	24	-14	13	-32	27	−21

	24	10	-1	-19	-5	6
$\frac{1}{2}$		12	11	5	-7	-6
	24	22	10	-14	-12	0
$\frac{1}{2}$		12	17	$\frac{27}{2}$		
	24	34	27	$-\frac{1}{2}$	$\neq 0$	

Zistili sme, že $\frac{1}{2}$ je jednoduchý koreň polynómu $f(x)$. (V poslednom výpočte sme nerátali do konca – zastavili sme sa pri zlomku $-\frac{1}{2}$.)

Mohli by sme pokračovať v skúšaní možností ďalej, trochu nám však zjednoduší prácu, ak si uvedomíme, že všetky ďalšie korene musia byť koreňmi polynómu $g(x) = 24x^4 + 22x^3 + 10x^2 - 14x - 12$. (Tento polynóm je podiel polynómu $f(x)$ a polynómu $x - \frac{1}{2}$, jeho koeficienty vieme vyčítať z predchádzajúcej Hornerovej schémy.)

Každý koeficient tohoto polynómu je párny – môžeme teda celý polynóm vydeliť číslom 2 a dostaneme polynóm $12x^4 + 11x^3 + 5x^2 - 7x - 6$, ktorý má tiež celočíselné koeficienty a má rovnaké korene ako $g(x)$. Keď hľadáme racionálne korene tohoto polynómu, dostávame pre čitateľ a menovateľ podmienky $p \mid 6$, $q \mid 12$, čiže
$p \in \{\pm1, \pm2, \pm3, \pm6\}$
$q \in \{1, 2, 3, 4, 6, 12\}$

$\frac{p}{q} \in \{\pm 1, \pm\frac{1}{2}, \pm\frac{1}{3} \pm \frac{1}{4}, \dots\}$
Pritom samozrejme čísla, ktoré sme už vyskúšali pre $f(x)$, pre polynóm $g(x)$ skúšať nemusíme. Získali sme teda dve zjednodušenia – budeme pracovať s polynómom nižšieho stupňa a máme menej možností, ktoré treba vyskúšať.

	12	11	5	-7	-6
$-\frac{1}{2}$		-6	$-\frac{5}{2}$		
	12	5	$\frac{5}{2}$		$\neq 0$

	12	11	5	-7	-6
$\frac{1}{3}$		4	5	$\frac{10}{3}$	
	12	15	10	$\frac{-11}{3}$	$\neq 0$

	12	11	5	-7	-6
$-\frac{1}{3}$		-4	$-\frac{7}{3}$		
	12	7	$-\frac{28}{3}$		$\neq 0$

	12	11	5	-7	-6
$\frac{1}{4}$		3	$\frac{14}{4}$		
	12	14			$\neq 0$

	12	11	5	-7	-6
$-\frac{1}{4}$		-2	$\frac{9}{4}$		
	12	9			$\neq 0$

	12	11	5	-7	-6
$\frac{1}{6}$		2	$\frac{13}{6}$		
	12	13			$\neq 0$

	12	11	5	-7	-6
$-\frac{1}{6}$		-2	$\frac{9}{6}$		
	12	9			$\neq 0$

	12	11	5	-7	-6
2		24	70	150	286
	12	35	75	143	$\boxed{280}$

	12	11	5	-7	-6
-2		-24	26	-62	138
	12	-13	31	-69	$\boxed{132}$

	12	11	5	-7	-6
$\frac{2}{3}$		8	$\frac{38}{3}$		
	12	19			$\neq 0$

	12	11	5	-7	-6
$-\frac{2}{3}$		-8	-2	-2	6
	12	3	3	-9	$\boxed{0}$
$-\frac{2}{3}$		-8	$\frac{10}{3}$		
	12	-5		$\neq 0$	

Dostali sme ďalší jednoduchý koreň $-\frac{2}{3}$. Nový polynóm, s ktorým budeme pracovať, je $h(x) = 12x^3+3x^2+3x-9$. Po vydelení koeficientov číslom 3 dostaneme jednoduchší polynóm $4x^3 + x^2 + x - 3$ a podmienky pre korene $p \mid 3$, $q \mid 4$, čiže
$p \in \{\pm 1, \pm 3\}$
$q \in \{1, 2, 4\}$
$\frac{p}{q} \in \{\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm 3, \pm\frac{3}{2} \pm \frac{3}{4}\}$

	4	1	1	-3
3		12	39	120
	4	13	40	$\boxed{117}$

	4	1	1	-3
-3		-12	33	-102
	4	-11	34	$\boxed{-105}$

	4	1	1	-3
$\frac{3}{2}$		6	$\frac{21}{2}$	
	4	7		$\neq 0$

	4	1	1	-3
$-\frac{3}{2}$		-6	$-\frac{15}{2}$	
	4	-5		$\neq 0$

	4	1	1	-3
$\frac{3}{4}$		3	3	3
	4	4	4	$\boxed{0}$
$\frac{3}{4}$		3	$\frac{21}{4}$	
	4	7	$\neq 0$	

Našli sme ďalší jednoduchý koreň $\frac{3}{4}$

Ďalej môžeme pracovať s polynómom $x^2 + x + 1$. Tu sú však jediní možní kandidáti na korene čísla ± 1 a tie sme už vyskúšali.

Záver: Daný polynóm má tieto 3 racionálne korene: $\frac{1}{2}$, $-\frac{2}{3}$, $\frac{3}{4}$; násobnosť každého z nich je 1.

Všimnime si, že sme vlastne súčasne dostali, že

$$f(x) = 24x^5 + 10x^4 - x^3 - 19x^2 - 5x + 6 = 24(x - \frac{1}{2})(x + \frac{2}{3})(x - \frac{3}{4})(x^2 + x + 1).$$

(Pri poslednom delení nám vyšiel podiel $4(x^2 + x + 1)$ a v priebehu výpočtu sme polynóm vydelili raz číslom 2 a raz číslom 3.) Predchádzajúcu rovnosť môžeme tiež prepísať ako

$$f(x) = (2x - 1)(3x + 2)(4x - 3)(x^2 + x + 1).$$

Pozrime sa na to, ako z tvrdenia 4.4.9 vyplýva, že $\sqrt{2}$ nie je racionálne číslo.

Príklad 4.4.12. Číslo $\sqrt{2}$ je očividne koreňom polynómu $p(x) = x^2 - 2$.

Ak by tento polynóm mal racionálny koreň, tak na základe tvrdenia 4.4.9 to môže byť jedine niektoré z čísel ± 1, ± 2. Ľahko skontrolujeme, že čísla ± 1 ani ± 2 nevyhovujú danej rovnici.

Teda polynóm $p(x)$ nemá racionálne korene a číslo $\sqrt{2}$ je iracionálne.

Môžete si všimnúť, že zdôvodnenie z tohoto príkladu prejde bez zmeny ak číslo 2 nahradíme ľubovoľným prvočíslom.

4.4.3 Algebraicky uzavreté polia

Definícia 4.4.13. Pole F sa nazýva *algebraicky uzavreté,* ak každý polynóm $f(x) \in F[x]$ stupňa aspoň jedna má v poli F aspoň jeden koreň.

V prípade, že $f(x)$ má koreň c, môžeme ho vydeliť koreňovým činiteľom $x - c$ a dostaneme jeho deliteľ nižšieho stupňa. Ten opäť musí mať nejaký koreň (ak nie je konštatný), preto takýmto spôsobom postupne dostaneme rozklad polynómu $f(x)$ na koreňové činitele. Dostávame:

Tvrdenie 4.4.14. *Ak F je algebraicky uzavreté pole, tak každý polynóm $f(x)$ je v $F[x]$ rozložiteľný na koreňové činitele.*

Z toho ďalej vidno, že ak F je algebraicky uzavreté pole, tak súčet násobností koreňov polynómu $f(x)$ je rovný jeho stupňu. (Toto tvrdenie sa zvyčajne formuluje tak, že polynóm stupňa n má práve n koreňov, ak zarátame aj ich násobnosti.)

Vieme, že pole komplexných čísel $\mathbb{C}$ má túto vlastnosť (aj keď dôkaz tejto vety nie je jednoduchý).

Veta 4.4.15 (Základná veta algebry)**.** *Pole komplexných čísel $\mathbb{C}$ je algebraicky uzavreté.*

Spomeňme (opäť bez dôkazu), že ku každému poľu sa dá zostrojiť nadpole, v ktorom už každý polynóm z $F[x]$ bude mať koreň. Dokonca platí:

Veta 4.4.16 (Steinitz)**.** *Pre každé pole F existuje algebraicky uzavreté nadpole F'.*

Všimnime si ešte jednu užitočnú vlastnosť komplexných koreňov polynómov s reálnymi koeficientami.

Tvrdenie 4.4.17. *Ak $f(x) \in \mathbb{R}[x]$ je polynóm s reálnymi koeficientami a $z = a + bi \in \mathbb{C}$ je koreň polynómu $f(x)$, tak aj komplexne združené číslo $\overline{z} = a - bi$ je koreňom polynómu $f(x)$. Pritom násobnosť koreňa $\overline{z}$ je rovnaká ako násobnosť z.*

Dôkaz. Stačí si všimnúť, že zobrazenie $z \mapsto \overline{z}$ je homomorfizmus (súčet/súčin komplexne združených čísel je komplexne združené číslo k súčtu/súčinu) a že pre $z \in \mathbb{R}$ platí $\overline{z} = z$. Z toho potom dostávame rovnosť

$$\overline{f(z)} = \overline{a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0} = a_n (\overline{z})^n + a_{n-1} (\overline{z})^{n-1} + \cdots + a_0 = f(\overline{z})$$

pre ľubovoľné $z \in \mathbb{C}$.

Z tejto rovnosti špeciálne vyplýva, že ak $f(z) = 0$, tak aj $f(\overline{z}) = 0$.

Druhá časť vyplýva z prvej použitej pre polynóm zapísaný v tvare $f(x) = g(x)(x - z)^k$, kde k je násobnosť koreňa z. □

Veľmi prirodzeným zovšeobecnením tohoto výsledku je tvrdenie sformulované v úlohe 4.4.1.

Dôsledok 4.4.18. *Každý polynóm $f(x) \in \mathbb{R}[x]$ nepárneho stupňa má aspoň 1 reálny koreň.*

Dôkaz. Ak by polynóm mal iba komplexné korene, tak môžeme popárovať dvojice komplexne združených koreňov. Komplexne združené korene majú podľa predchádzajúceho tvrdenia rovnakú násobnosť. Preto súčet násobností všetkých komplexných koreňov je párne číslo. Súčet násobností sa však rovná stupňu polynómu $f(x)$ (pretože $\mathbb{C}$ je algebraicky uzavreté pole). □

4.4.4 Ireducibilné polynómy

Definícia 4.4.19. Polynóm $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ sa nazýva *normovaný* (alebo tiež *monický,*) ak $a_n = 1$ (vedúci koeficient sa rovná 1).

Pripomeňme si definíciu

Definícia 4.4.20. Ak R je obor integrity, tak ireducibilné prvky okruhu $R[x]$ nazývame *ireducibilné polynómy* v $R[x]$.

a tiež tvrdenie 4.3.22 (tu je formulácia o trochu špeciálnejšia a konkrétnejšia, ako je to v "referovanom"tvrdení)

Veta 4.4.21 (Rozklad na ireducibilné polynómy)**.** *Ak F je pole, tak každý polynóm $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ možno vyjadriť v tvare*

$$f(x) = a_n p_1(x) \dots p_n(x),$$

kde $p_1, \dots, p_n$ sú ireducibilné normované polynómy. Navyše, tento rozklad je (až na poradie činiteľov) jednoznačne určený.

Dôkaz. Pretože $F[x]$ je okruh s jednoznačným rozkladom, vieme, že každý polynóm sa dá rozložiť na súčin ireducibilných polynómov a ten rozklad je jednoznačný až na asociovanosť. V okruhu $F[x]$ sú dva prvky asociované práve vtedy, keď sa líšia iba konštantným násobkom. Tým, že vo vete požadujeme normované polynómy, sú teda už jednoznačne určené (z ľubovoľného polynómu dostaneme normovaný, keď ho vynásobíme b_m^{-1}, kde b_m je jeho vedúci koeficient; súčin vedúcich koeficientov sme dali pred súčin normovaných činiteľov – tento súčin sa rovná a_n). □

Zatiaľ však o ireducibilných polynómoch vieme iba to, že existujú – nevieme, ako overiť, či je daný polynóm ireducibilný ani ako rozklad na súčin ireducibilných polynómov hľadať.

Je zrejmé, že každý polynóm stupňa 1 je ireducibilný – nedá sa rozložiť na súčin polynómov nižších stupňov. Teda ak c je k-násobný koreň, v rozklade polynómu $f(x)$ sa musí vyskytnúť $(x-c)^k$. V prípade, že súčet násobností koreňov je rovný stupňu polynómu vieme teda ten polynóm rozložiť ako

$$f(x) = a_n(x-c_1)^{k_1}(x-c_2)^{k_2} \dots (x-c_m)^{k_m},$$

kde $c_1, \dots, c_m$ sú všetky korene $f(x)$ a $k_1, \dots, k_m$ sú ich násobnosti. Takýto rozklad (ak existuje) voláme rozklad na súčin *koreňových činiteľov.*

V niektorých prípadoch vieme o ireducibilite rozhodnúť, ak poznáme korene polynómu.

Tvrdenie 4.4.22. *Ak F je pole a $f(x) \in F[x]$ je polynóm stupňa 2 alebo 3, tak polynóm $f(x)$ je ireduciblný v F práve vtedy, keď $f(x)$ nemá koreň v F.*

Dôkaz. Stačí si všimnúť, že ak chceme polynóm stupňa 2 alebo 3 rozložiť ako súčin polynómov nižších stupňov, nevyhnutne sa tam musí vyskytnúť polynóm stupňa 1. Z lemy 4.4.4 vieme, ako súvisia lineárne delitele polynómu a jeho korene. □

Všimnime si, že ireducibilita polynómu závisí od toho, nad akým poľom ho uvažujeme (pretože polynóm nad poľom F môžeme súčasne chápať aj ako polynóm nad ľubovoľným nadpoľom $F' \supseteq F$).

Príklad 4.4.23. Uvažujme polynóm $f(x) = x^4+1$. Tento polynóm má celočíselné koeficienty, môžeme sa teda skúmať jeho ireducibilitu v okruhoch polynómov $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ aj $\mathbb{C}[x]$.

V poli $\mathbb{C}$ má tento polynóm 4 korene $\frac{\pm\sqrt{2}\pm\sqrt{2}i}{2}$ (vieme ich nájsť riešením binomickej rovnice $x^4 = -1$). Teda v $\mathbb{C}$ máme rozklad

$$x^4 + 1 = \left(x - \frac{\sqrt{2}+\sqrt{2}i}{2}\right)\left(x - \frac{\sqrt{2}-\sqrt{2}i}{2}\right)\left(x + \frac{\sqrt{2}+\sqrt{2}i}{2}\right)\left(x + \frac{\sqrt{2}-\sqrt{2}i}{2}\right)$$

Nad poľom $\mathbb{R}$ máme rozklad

$$x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1).$$

(Polynómy v rozklade môžeme získať napríklad ako súčin koreňových činiteľov pre komplexne združené korene. Alebo tento rozklad môžeme dostať tak, že si všimneme rovnosť $x^4 + 1 = (x^2+1)^2 - (\sqrt{2}x)^2$) Pritom oba polynómy $x^2 \pm \sqrt{2}x + 1$ sú už nad $\mathbb{R}$ nerozložiteľné – pretože nemajú reálne korene.

Nad poľom $\mathbb{Q}$ je tento polynóm ireducibilný. Ak by sa totiž dal rozložiť na súčin nejakých polynómov, bol by súčasne aj súčinom týchto polynómov v $\mathbb{R}[x]$. Ako sme však videli, jediný (až na poradie a asociovanosť) rozklad na súčin polynómov nižšieho stupňa v $\mathbb{R}[x]$ je $x^4+1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$ a polynómy, ktoré vystupujú v tomto rozklade, nepatria do $\mathbb{Q}[x]$ (lebo rozklad v $\mathbb{Q}[x]$ je zároveň rozkladom v $\mathbb{R}[x]$).

4.4.5 Ireducibilné polynómy nad $\mathbb{Q}$ a $\mathbb{R}$

Z toho, čo doteraz vieme, sme schopní aspoň v niektorých konkrétnych prípadoch nájsť rozklad daného polynómu na súčin ireducibilných polynómov.

Postupovať môžeme tak, že hľadáme korene polynómu – pomocou hľadania racionálnych koreňov, riešením kvadratickej alebo binomickej rovnice (prípadne iných typov rovníc, ktoré vieme riešiť, ako sú reciproké rovnice, bikvadratické rovnice, kubické rovnice, rovnice štvrtého stupňa). Po nájdení koreňov môžeme polynóm vydeliť koreňovými činiteľmi (a znovu sa pokúsiť riešiť novú rovnicu nižšieho stupňa než bola pôvodná). V prípade, že by polynóm mal násobné korene, dá sa znížiť jeho stupeň použitím derivácie – o tom si ešte v tejto kapitole povieme.

V prípade, že po vydelení dostaneme polynóm dostatočne nízkeho stupňa, ktorý nemá korene, vieme už, že je ireducibilný.

Príklad 4.4.24. V príklade 4.4.11 sme zistili, že

$$f(x) = 24x^5 + 10x^4 - x^3 - 19x^2 - 5x + 6 = 24\left(x - \frac{1}{2}\right)\left(x + \frac{2}{3}\right)\left(x - \frac{3}{4}\right)(x^2 + x + 1).$$

Pretože polynóm $x^2 + x + 1$ nemá reálne korene (a je to polynóm druhého stupňa), je to rozklad na ireducibilné polynómy nad $\mathbb{R}$ (a tým pádom aj nad $\mathbb{Q}$). Rozklad nad $\mathbb{C}$ by sme získali, keby sme ešte $x^2 + x + 1$ rozložili na ireducibilné činitele.

Všimnime si, že sme vlastne dostali aj rozklad

$$f(x) = (2x - 1)(3x + 2)(4x - 3)(x^2 + x + 1)$$

v $\mathbb{Z}[x]$.

Viac o rozklade polynómov na ireducibilné činitele (a o algoritmoch používaných na jeho výpočet) sa môžete dozvedieť na predmete počítačová algebra, pozri napríklad [G1, G2].

4.4.6 Derivácia a Taylorov rozvoj polynómov

Definícia 4.4.25. *Formálna derivácia* polynómu $f(x) = \sum_{k=0}^{n} a_k x^k$ je polynóm $Df(x) = \sum_{k=1}^{n} k \times a_k x^{k-1}$.

V prípade, že pracujeme nad ľubovoľným poľom, môže sa stať, že nenulový polynóm má nulovú deriváciu.

Príklad 4.4.26. Pre $f(x) = x^p$ v $\mathbb{Z}_p[x]$ dostávame $Df(x) = p \times x^{p-1} = 0$.

Priamo z definície sa dá overiť, že takto definovaná formálna derivácia má podobné vlastnosti, na aké sme zvyknutí z analýzy.

Tvrdenie 4.4.27. *Nech F je pole. Pre ľubovoľné $c \in F$, $f(x), g(x) \in F[x]$ platí*

$$D(f(x) + g(x)) = Df(x) + Dg(x)$$
$$D(cf(x)) = cDf(x)$$
$$D(f(x)g(x)) = Df(x).g(x) + f(x).Dg(x)$$

Dôkaz. Overme iba tretiu rovnosť (prvé dve sú skutočne jednoduché). Koeficient pri x^n v polynóme na ľavej strane tejto rovnosti je $(n+1)$-násobok koeficientu polynómu $f(x).g(x)$ pri x^n.

Označme koeficienty polynómu $f(x)$ ako a_k, koeficienty polynómu $g(x)$ ako b_k. Pre koeficienty polynómu na ľavej strane rovnosti potom máme

$$l_n = (n+1) \times \sum_{k=0}^{n+1} a_k b_{n+1-k}$$

Na pravej strane rovnosti dostávame

$$p_n = \sum_{k=0}^{n} (k+1) \times a_{k+1} b_{n-k} + \sum_{k=0}^{n} (n+1-k) \times a_k b_{n+1-k}.$$

Zmenou sumačného indexu v prvej sume dostaneme vyjadrenie

$$p_n = \sum_{k=1}^{n+1} k \times a_k b_{n+1-k} + \sum_{k=0}^{n} (n+1-k) \times a_k b_{n+1-k} = \sum_{k=0}^{n+1} (n+1) \times a_k b_{n+1-k} = l_n$$

(aby sme uvedené členy mohli zlúčiť do jednej sumy, pridali sme dva nulové členy – v prvej sume pre $k = 0$ člen $0 \times a_0 b_{n+1}$ a v druhej sume pre $k = n+1$ člen $0 \times a_{n+1} b_0$). □

Uvedieme si dve tvrdenia, ktoré ukazujú, prečo je tento pojem užitočný – prvé z nich je vyjadrenie Taylorovho polynómu v nejakom $c \in F$; druhé z nich hovorí o tom, či nejaký polynóm má násobné korene.

Tvrdenie 4.4.28. *Nech F je pole, $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in F[x]$. Potom existujú jednoznačne určené $b_0, b_1, \ldots, b_n \in F$ také, že*

$$f(x) = b_n (x-c)^n + \cdots + b_1 (x-c) + b_0. \tag{4.5}$$

Dôkaz. Indukciou vzhľadom na n. Ak $n = 0$, tak stačí položiť $a_0 = b_0$ (a inú možnosť očividne nemáme).

Predpokladajme, že uvedené tvrdenie platí pre polynómy stupňa nanajvýš $n - 1$. Podľa lemy 4.4.3

$$f(x) = g(x)(x - c) + f(c). \tag{4.6}$$

Polynóm $g(x)$ je stupňa najviac $n-1$- Podľa indukčného predpokladu existujú $b_1, \ldots, b_n \in F$ také, že $g(x) = b_n(x - c)^{n-1} + \cdots + b_2(x - c) + b_1$. Položme $b_0 = f(c)$. Potom pre $f(x)$ platí

$$f(x) = (b_n(x - c)^{n-1} + \cdots + b_2(x - c) + b_1)(x - c) + b_0 = b_n(x - c)^n + \cdots + b_1(x - c) + b_0.$$

Tým máme dokázanú existenciu.

Ak dosadíme do rovnosti (4.5) $x = c$, tak vidíme, že $b_0 = f(c)$. Ďalej polynóm $g(x)$ z (4.6) je podľa vety o delení so zvyškom jednoznačne určený. K tomuto polynómu sú podľa indukčného predpokladu jednoznačne určené $b_1, b_2, \ldots, b_n \in F$. □

Tvrdenie 4.4.29. *Ak F je pole charakteristiky ∞, tak koeficienty $b_0, \ldots, b_n$ z tvrdenia* 4.4.28 *možno vyjadriť ako*

$$b_n = \frac{D^{(n)} f(c)}{n!},$$

kde znak $D^{(n)}$ znamená, že polynóm $f(x)$ zderivujeme n-krát.

Dôkaz. Toto tvrdenie dostaneme priamo z rovnosti (4.5) viacnásobným zderivovaním (resp. ho môžeme ukázať pomocou indukcie). □

Rozvoj v tvare (4.5) môžeme dostať aj pomocou Hornerovej schémy – teda Hornerova schéma nám poskytuje možnosť vypočítať hodnoty $D^{(n)} f(c)$ pre daný polynóm $f(x)$ a $c \in F$.

Pred dôkazom nasledujúceho tvrdenia si všimnime jednu dôležitú vlastnosť najväčšieho spoločného deliteľa – konkrétne fakt, že zostane taký istý, aj keď prejdeme k nejakému nadpoľu.

Poznámka 4.4.30. Už sme spomínali, že ak $f(x), g(x) \in F[x]$ a $F' \supseteq F$ je nadpole poľa F, tak polynómy $f(x)$ a $g(x)$ sú súčasne aj prvkami $F'[x]$. To znamená, že sa môžeme pýtať na najväčší spoločný deliteľ týchto 2 polynómov v okruhu $F[x]$ i v okruhu $F'[x]$. V obidvoch prípadoch je tento polynóm rovnaký.

Vyplýva to z toho, že podiel a zvyšok pri delení dvoch polynómov z $F[x]$ vyjde rovnako, bez ohľadu na to, či delíme so zvyškom v $F[x]$ alebo v $F'[x]$. (V $F[x]$ sa dajú vydeliť tak, aby podiel i zvyšok mali koeficienty z F, podiel v $F'[x]$ je rovnaký, pretože vo vete o delení so zvyškom máme jednoznačnosť.)

Z toho vyplýva aj to, že relácia „delí“ nezávisí od toho, či sa na polynómy $f(x)$, $g(x)$ pozeráme ako na prvky $F[x]$ alebo ako na prvky $F'[x]$.

Tvrdenie 4.4.31. *Nech F je pole, $F' \supseteq F$ je jeho nadpole. Nech $f(x) \in F[x]$ je polynóm nad poľom F. Ak v nadpoli F' existuje násobný koreň polynómu $f(x)$, tak polynómy $f(x)$ a $Df(x)$ sú súdeliteľné, t.j.*

$$\mathrm{st}(\gcd(f(x), D(f(x)))) \geq 1.$$

Dôkaz. Ak c je násobný koreň $f(x)$, tak podľa definície 4.4.5 $f(x) = g(x)(x - c)^k$, kde $k > 1$. Potom

$$Df(x) = Dg(x)(x - c)^k + k \times g(x)(x - c)^{k-1} = (x - c)^{k-1}(Dg(x)(x - c) + k \times g(x)),$$

teda $x - c \mid Df(x)$. Keďže súčasne $x - c \mid f(x)$, máme

$$x - c \mid \gcd(f(x), Df(x))$$

a $\mathrm{st}(\gcd(f(x), D(f(x)))) \geq 1$. (Predchádzajúcu nerovnosť sme dokázali pre najväčší spoločný deliteľ v $F'[x]$. Na základe poznámky 4.4.30 je však najväčší spoločný deliteľ v $F[x]$ rovnaký.) □

Predchádzajúce tvrdenie nám umožní nájsť polynóm, ktorý má rovnaké korene ako daný polynóm, ale každý koreň má násobnosť 1. Pred uvedením tohoto výsledku však potrebujeme zaviesť pojem charakteristiky poľa.

Definícia 4.4.32. *Charakteristika poľa* F je najmenšie prirodzené číslo $k > 0$ s vlastnosťou $k \times 1 = 0$. Označujeme ju $\mathrm{char}(F)$. Ak neexistuje k s uvedenou vlastnosťou, tak definujeme $\mathrm{char}(F) = \infty$.

Ak $\mathrm{char}(F) = k$, tak pre každé $c \in F$ platí $k \times c = c.(k \times 1) = c.0 = 0$.

Tvrdenie 4.4.33. *Nech F je pole s nekonečnou charakteristikou. Nech $f(x) \in F[x]$ a $h(x)$ je najväčší spoločný deliteľ $f(x)$ a $Df(x)$. Potom existuje polynóm $g(x)$ s vlastnosťami*

(i) $f(x) = g(x).h(x)$,

(ii) $g(x)$ *má v každom nadpoli poľa F tie isté korene ako $f(x)$,*

(iii) *násobnosť každého koreňa $g(x)$ je 1.*

Dôkaz. Pretože $\mathrm{char}(F) = \infty$, máme $Df(x) \neq 0$. (Vedúci koeficient $Df(x)$ je $n \times a_n$, kde a_n je vedúci koeficient $f(x)$. V poli s nekonečnou charakteristikou z $a \neq 0$ vyplýva $n \times a \neq 0$.)

Potom aj $h(x)$ je nenulový polynóm. Navyše $h(x) \mid f(x)$, takže pri delení so zvyškom dostaneme

$$f(x) = g(x)h(x) + 0.$$

Ak c je násobný koreň $f(x)$ s násobnosťou k, tak platí $f(x) = (x - c)^k f_1(x)$, pričom c nie je koreňom $f_1(x)$. Z predchádzajúcej rovnosti dostaneme

$$Df(x) = Df_1(x)(x - c)^k + k \times f_1(x)(x - c)^{k-1} = (x - c)^{k-1}(Df_1(x)(x - c) + k \times f_1(x)).$$

Potom

$$h(x) = \gcd(f(x), Df(x)) = (x - c)^{k-1} \gcd((x - c)f_1(x), Df_1(x)(x - c) + k \times f_1(x)).$$

Pritom $x - c \nmid f_1(x)$, z čoho vyplýva $x - c \nmid Df_1(x)(x - c) + k \times f_1(x)$ a

$$x - c \nmid \gcd((x - c)f_1(x), Df_1(x)(x - c) + k \times f_1(x)).$$

Teda

$$(x - c)^k \nmid h(x)$$

(c je len $k - 1$-násobným koreňom $h(x)$). T.j., ak vyjadríme $h(x)$ v tvare $h(x) = (x - c)^{k-1}h_1(x)$, tak $x - c \nmid h(x)$. Potom máme

$$(x - c)^k \mid g(x)h(x) = g(x)h_1(x)(x - c)^{k-1}$$
$$x - c \mid g(x)h_1(x)$$

Pretože $x-c$ je ireducibilný a $x-c \nmid h_1(x)$, vyplýva z toho už $x-c \mid g(x)$, čiže c je koreňom $g(x)$.

Navyše, c je iba jednoduchý koreň $g(x)$, v opačnom prípade by sme mali $(x-c)^2 \mid g(x)$, a teda

$$(x-c)^{k+1} \mid g(x)h_1(x-c)^{k-1} = g(x)h(x) = f(x).$$

To je spor s tým, že násobnosť koreňa c je k. □

Príklad 4.4.34. Majme polynóm $f(x) = x^4 + 2x^2 + 1 \in \mathbb{R}[x]$. Potom $Df(x) = 4x^3 + 4x$ a ich normovaný najväčší spoločný deliteľ je

$$h(x) = \gcd(f(x), Df(x)) = x^2 + 1 = x^4 + 2x^2 + 1 - \frac{x}{4}(4x^3 + 4x).$$

Po vydelení $f(x)$ polynómom $h(x)$ dostaneme $g(x) = x^2 + 1$.

Skutočne, polynómy $f(x) = (x^2+1)^2$ a $g(x) = x^2 + 1$ majú v $\mathbb{C}$ tie isté korene $\pm i$, v prípade polynómu $g(x)$ sú to jednoduché korene.

Cvičenia

Úloha 4.4.1. Nech F je pole, F' je jeho nadpole a $\varphi\colon F' \to F'$ je homomorfizmus taký, že $\varphi(x) = x$ pre každé $x \in F$ (nemení prvky poľa F). Potom pre každý koreň c polynómu $f(x)$ je aj $\varphi(c)$ koreňom $f(x)$.

Úloha 4.4.2. Vedeli by ste dokázať dôsledok 4.4.18 na základe poznatkov, ktoré máte z analýzy?

Úloha 4.4.3. Vydeľte dané polynómy so zvyškom v $\mathbb{C}[x]$.
a) $f(x) = x^4 + 3x^3 - 4x + 2$, $g(x) = x^2 + x - 2$
b) $f(x) = x^5 + 2x^3 + 3x + 4$, $g(x) = x^3 + x + 1$
c) $f(x) = x^3 + (2+2i)x^2 + 3ix + 1$, $g(x) = x^2 + (2+i)x + i$

Úloha 4.4.4. Použitím Hornerovej schémy zistite, či c je koreň polynómu $f(x) \in \mathbb{C}[x]$ a vyjadrite tento polynóm v tvare $f(x) = g(x)(x-c) + f(c)$.
a) $f(x) = x^4 + 3x^3 - 4x + 2$, $c = -2$
b) $f(x) = x^5 + 2x^3 + 3x + 4$, $c = -1$
c) $f(x) = x^3 + (2+2i)x^2 + 3ix + 1$, $c = -i$

Úloha 4.4.5. Pomocou Hornerovej schémy vyjadriť:
a) $f(x+3)$ pre $f(x) = x^4 - x^3 + 1$
b) $(x-2)^4 + 4(x-2)^3 + 6(x-2)^2 + 10(x-2) + 20$

Úloha 4.4.6. Nájdite všetky racionálne korene daných polynómov (s pomocou Hornerovej schémy a tvrdenia dokázaného v predchádzajúcej úlohe). Aká je ich násobnosť?
a) $f(x) = 4x^4 - 7x^2 - 5x - 1$
b) $f(x) = 24x^5 + 10x^4 - x^3 - 19x^2 - 5x + 6$
c) $f(x) = 6x^4 + 19x^3 - 7x^2 - 26x + 12$

Úloha 4.4.7. Ukážte, že reálny polynóm $f(x) = (x-4)(x-1)(x+1)(x+4) - 1$ nemá racionálne korene.

Úloha 4.4.8. Vypočítajte $d(x) = \gcd(f(x), g(x))$ a vyjadrite ho v tvare $d(x) = u(x)f(x) + v(x)g(x)$.
a) $f(x) = 3x^5 + 5x^4 - 16x^3 - 6x^2 - 5x - 6$, $g(x) = 3x^4 - 4x^3 - x^2 - x - 2$;

b) $f(x) = 4x^4 - 2x^3 - 16x^2 + 5x + 9$, $g(x) = 2x^3 - x^2 - 5x + 4$;
c) $f(x) = x^4 + 6x^3 + 9x^2 - 2x - 9$, $g(x) = x^3 + 4x^2 + 2x - 7$;
d) $f(x) = x^8 - 1$, $g(x) = x^5 - 1$;
e) $f(x) = x^{10} - 1$, $g(x) = x^4 - 1$.
(Výsledky: a) $u(x) = -\frac{1}{3}x^2 + \frac{1}{3}x + \frac{1}{3}$, $v(x) = \frac{1}{3}x^3 + \frac{2}{3}x^2 - \frac{5}{3}x - \frac{4}{3}$, $d(x) = x + \frac{2}{3}$
b) $u(x) = -\frac{x-1}{3}$, $v(x) = \frac{2x^2-2x-3}{3}$, $d(x) = x - 1$
c) $d(x) = 1$, $u(x) = 1/30(2x^2 + 5x - 1)$, $v(x) = -1/30(2x^3 + 9x^2 + 7x + 3)$)

Úloha 4.4.9*. Nech $m, n > 1$ sú prirodzené čísla. Ukážte, že $\gcd(x^m - 1, x^n - 1) = x^d - 1$, kde $d = \gcd(m, n)$.

Úloha 4.4.10. Dokážte, že $x^2 + x + 1 \mid x^{3m} + x^{3n+1} + x^{3p+2}$ (v $F[x]$ pre ľubovoľné pole F).

Úloha 4.4.11. Dokážte, že $x^2 + x + 1 \mid x^{3m} + x^{3n+1} + x^{3p+2}$ v $\mathbb{C}[x]$. (Využite to, čo viete o koreňoch týchto polynómov.)

Úloha 4.4.12. Rozložiť na koreňové činitele (nad $\mathbb{C}$):
a) $x^3 - 6x^2 + 11x - 6$
b) $x^4 + 4$,
c) $x^4 + 4x^3 + 4x^2 - 1$,
d*) $x^4 + 4x^3 + 4x^2 + 1$,
e) $x^4 - 10x^2 + 1$,
f) $x^4 - 4x^3 + 4x - 1$.

Úloha 4.4.13. Rozložiť na súčin ireducibilných polynómov nad $\mathbb{R}$:
a) $x^4 + 4$
b) $x^6 + 27$
c) $x^4 + 4x^3 + 4x^2 - 1$
d) $x^5 + x^4 + x^3 + x^2 + x + 1$
e*) $x^{2n} - 2x^n + 2$
f*) $x^4 - ax^2 + 1$ pre $a \in (-2, 2)$
g*) $x^{2n} + x^n + 1$.

Úloha 4.4.14. Dokážte: Ak $a + bi$ je koreň polynómu $f(x) \in \mathbb{R}[x]$ a $b \neq 0$, tak $x^2 - 2ax + a^2 + b^2 \mid f(x)$.

Úloha 4.4.15. Nájdite všetky ireducibilné polynómy nad $\mathbb{Z}_2$ stupňov 2,3,4.

Úloha 4.4.16. Nájdite rozklad $f(x)$ na ireducibilné polynómy v $F[x]$.
a) $f(x) = 4x^4 + 3x^3 + 4x^2 + 4x + 6$, $F = \mathbb{Z}_7$
b) $f(x) = x^4 - 1$, $F = \mathbb{Z}_{11}$
c) $f(x) = x^4 - 1$, $F = \mathbb{Z}_{13}$

Úloha 4.4.17. Zistite, či dané ideály sú maximálne v $\mathbb{R}[x]$:
a) $I_1 = (x^2 - 1)$;
b) $I_2 = (x^2 + 1)$.

Úloha 4.4.18*. Nech $f(x) \in \mathbb{Z}[x]$ je polynóm s celočíselnými koeficientami. Dokážte, že ak $a + b\sqrt{3}$ je koreň $f(x)$, tak aj $a - b\sqrt{3}$ je koreň $f(x)$. Dokážte, že podobné tvrdenie platí, ak c nahradíme ľubovoľným prirodzeným číslom, ktoré nie je druhou mocninou prirodzeného čísla.

Úloha 4.4.19. Dokážte, že polynóm $f(x) = 1 + x + \frac{x^2}{2} + \frac{x^3}{3!} + \ldots + \frac{x^n}{n!}$ nemá viacnásobný koreň (nad $\mathbb{R}$ resp. nad $\mathbb{C}$).

Literatúra

[A] Tom M. Apostol. *Calculus II.* John Wiley and Sons, New York, 1969.

[BL] Kurt Bryan and Tanya Leise. The $25,000,000,000 eigenvector – the linear algebra behind Google. *SIAM Review*, 48(3):569–581, 2006. `http://www.rose-hulman.edu/~bryan/googleFinalVersionFixed.pdf`.

[BM] Garrett Birkhoff and Saunders MacLane. *Prehľad modernej algebry.* Alfa, Bratislava, 1979.

[CFR] Paul Cull, Mary Flahive, and Robby Robson. *Difference Equations - From Rabbits to Chaos.* Springer, New York, 2005. Undergraduate Texts in Mathematics.

[DF] David S. Dummit and Richard M. Foote. *Abstract Algebra.* John Willey and Sons, 3rd edition, 2004.

[FS1] D. K. Faddeev and I. C. Sominskii. *Sbornik zadači po vyššej algebre.* Nauka, Moskva, 1972.

[FS2] D. K. Faddeev and I. C. Sominskii. *Zadači po vyššej algebre.* Laň, St. Peterburg, 1999.

[G1] Jaroslav Guričan. Faktorizácia polynómov I. *Obzory matematiky, fyziky a informatiky.* `http://thales.doa.fmph.uniba.sk/katc/pages/member.php?clen=gurican`.

[G2] Jaroslav Guričan. Faktorizácia polynómov II. *Obzory matematiky, fyziky a informatiky.* `http://thales.doa.fmph.uniba.sk/katc/pages/member.php?clen=gurican`.

[G3] Jaroslav Guričan. Vybrané kapitoly z algebry. Poznámky k prednáške, `http://thales.doa.fmph.uniba.sk/katc/pages/member.php?clen=gurican`.

[GĎ] Milan Gera and Vladimír Ďurikovič. *Matematická analýza.* Alfa, Bratislava, 1990.

[GŠŠ] M. Greguš, M. Švec, and V. Šeda. *Obyčajné diferenciálne rovnice.*

[HJ] Roger A. Horn and Charles R. Johnson. *Matrix Analysis.* Cambridge University Press, Cambridge, 1985.

[J] B. Johnson. Fibonacci numbers and matrices. `http://www.dur.ac.uk/bob.johnson/fibonacci/`.

[Kor] Július Korbaš. *Lineárna algebra a geometria I.* UK, Bratislava, 2003.

[Kos] Thomas Koshy. *Discrete mathematics with applications.* Elsevier Academic Press, Burlington–San Diego–London, 2004.

[KGGS] Tibor Katriňák, Martin Gavalec, Eva Gedeonová, and Jaroslav Smítal. *Algebra a teoretická aritmetika 1.* UK, Bratislava, 2002.

[LM] Amy N. Langville and Carl D. Meyer. *Google's PageRank and Beyond: The Science of Search Engine Rankings.* Princeton University Press, Princeton, 2006.

[Me] Carl D. Meyer. *Matrix Analysis and Applied Linear Algebra.* SIAM, 2000.

[Mi] Ondrej Mikuláš. PageRank algoritmus, 2010. bakalárska práca, FMFI UK, Bratislava.

[Pro1] I. V. Proskurjakov. *Sbornik zadač po lineinoi algebre.* Moskva, 1966.

[Pro2] Murray H. Protter. *Basic Elements of Real Analysis.* Springer-Verlag, NY, 1998. Undergraduate Texts in Mathematics.

[Š] Beáta Štupáková. Fibonacciho a Lucasove čísla, 2008. bakalárska práca, FMFI UK, Bratislava.

[W] Michal Winczer. Diskrétna matematika. Poznámky k prednáške, `http://edi.fmph.uniba.sk/~winczer/diskretna.html`.

[Z] Pavol Zlatoš. Lineárna algebra a geometria. `http://thales.doa.fmph.uniba.sk/zlatos/`.

Register

Zoznam symbolov