Lineárna algebra 1-UMA-102

Martin Sleziak

3. novembra 2009

Obsah

1 Úvod **3**
1.1 Predhovor . . . 3
1.2 Sylaby a literatúra . . . 4
1.3 Základné označenia . . . 4

2 Množiny a zobrazenia **5**
2.1 Dôkazy . . . 6
2.1.1 Základné typy dôkazov . . . 6
2.1.2 Matematická indukcia . . . 7
2.1.3 Drobné rady ako dokazovať . . . 8
2.1.4 Výroky, logické spojky, tautológie . . . 9
2.1.5 Negácia výrokov s kvantifikátormi . . . 10
2.2 Množiny a zobrazenia . . . 11
2.2.1 Množiny . . . 11
2.2.2 Zobrazenia . . . 13
2.2.3 Vzor a obraz množiny* . . . 19
2.3 Permutácie . . . 20
2.3.1 Rozklad na súčin disjunktných cyklov* . . . 21

3 Grupy a polia **26**
3.1 Binárne operácie . . . 26
3.1.1 Zovšeobecnený asociatívny zákon* . . . 31
3.2 Grupy . . . 33
3.3 Polia . . . 37

4 Vektorové priestory **47**
4.1 Vektorový priestor . . . 47
4.2 Podpriestory . . . 51
4.3 Lineárna kombinácia, lineárna nezávislosť . . . 55
4.3.1 Lineárna kombinácia a lineárny obal . . . 55
4.3.2 Lineárna nezávislosť . . . 57
4.4 Báza a dimenzia . . . 62
4.5 Lineárne a direktné súčty podpriestorov . . . 66

5 Lineárne zobrazenia a matice **70**
5.1 Matice . . . 70
5.2 Riadková ekvivalencia a hodnosť matice . . . 72
5.3 Lineárne zobrazenia . . . 79

5.4 Súčin matíc . . . 84
5.5 Inverzná matica . . . 88
5.6 Elementárne riadkové operácie a súčin matíc* . . . 91
5.7 Sústavy lineárnych rovníc . . . 94
5.7.1 Homogénne sústavy lineárnych rovníc . . . 95
5.7.2 Gaussova eliminačná metóda . . . 98
5.7.3 Frobeniova veta . . . 99
5.8 Jadro a obraz lineárneho zobrazenia . . . 102
5.9 Hodnosť transponovanej matice . . . 105

6 Determinanty **107**
6.1 Motivácia . . . 107
6.2 Definícia determinantu . . . 109
6.3 Výpočet determinantov . . . 112
6.3.1 Laplaceov rozvoj . . . 112
6.3.2 Výpočet pomocou riadkových a stĺpcových operácií . . . 115
6.4 Determinant súčinu matíc . . . 119
6.5 Využitie determinantov . . . 121
6.5.1 Výpočet inverznej matice . . . 121
6.5.2 Cramerovo pravidlo . . . 122

7 Euklidovské vektorové priestory **125**
7.1 Skalárny súčin . . . 125
7.2 Gram-Schmidtov ortogonalizačný proces . . . 130

A Delenie so zvyškom **135**

B Komplexné čísla **136**
B.1 Definícia komplexných čísel, algebraický tvar komplexného čísla . . . 136
B.2 Geometrická interpretácia komplexných čísel, goniometrický tvar, Moivrova veta 139
B.3 Riešenie rovníc v komplexných číslach . . . 141
B.3.1 Kvadratické rovnice s reálnymi koeficientmi . . . 142
B.3.2 Binomické rovnice . . . 143
B.4 Zopár ďalších vecí súvisiacich s komplexnými číslami . . . 144

Register **149**

Zoznam symbolov **151**

Kapitola 1

Úvod

Verzia: 3. novembra 2009

1.1 Predhovor

Live as if you were to die tomorrow
Learn as if you were to live forever.
Mahátma Gándhí

Tento text obsahuje poznámky k prednáške lineárna algebra.

Nie všetky časti uvedené v týchto poznámkach na prednáške skutočne aj odznejú – na niektoré pravdepodobne nebudeme mať čas, iné necháme na cvičenia alebo si o nich povieme len celkom stručne. Práve v tom je výhoda učebného textu – snažil som sa v ňom viaceré veci rozobrať dostatočne podrobne, aby ste v prípade, že na ne nezvýši na prednáške čas alebo ich na nej nestihnete zachytiť, nemali problém doštudovať si ich samostatne.

Takisto poradie, v akom sú uvedené niektoré veci v tomto texte, nemusí byť úplne rovnaké ako na prednáške. Napríklad poznatky o dôkazoch, typoch dôkazov, logických spojkách a pod., ktoré sú zhrnuté v úvodnej kapitole, nebudeme preberať – povieme si o nich priebežne, keď ich na prednáške budeme potrebovať. V samostatnom texte je však oveľa výhodnejšie mať ich spolu na jednom mieste. (Navyše, veľa z vecí obsiahnutých v úvodnej kapitole už pravdepodobne poznáte zo strednej školy) Takisto v závislosti od toho, koľko bude času, niektoré veci možno preskočíme alebo odložíme na koniec semestra.

Časti označené hviezdičkou sú „nepovinné“, čo znamená, že na skúšku ich nemusíte vedieť. Každopádne sa vám ich môže oplatiť prečítať – môžu vám pomôcť získať lepší prehľad a lepšie porozumieť ostatným témam. Iné sa vám zasa môžu hodiť v budúcnosti. Samozrejme, dôležité je najprv zvládnuť základné – neohviezdičkované – časti. Pri častiach označených hviezdičkou je vždy uvedené s akou preberanou témou súvisia. Niektoré z nich sú náročnejšie – sú tu uvedené z toho dôvodu, že súvisia s preberanými témami, ale možno bude vhodnejšie sa k nim vrátiť v budúcnosti než ich preberať počas prvého kurzu z lineárnej algebry, ktorý absolvujete.

Takisto niektoré náročnejšie cvičenia sú označené hviezdičkou – keď zvládnete tie jednoduchšie (verím, že mnohým z vás to pôjde celkom ľahko) môžete sa do nich pustiť, aj v prípade, že sa vám ich nepodarí vyriešiť, čas investovaný do samostatného rozmýšľania v žiadnom prípade nie je stratený. Cvičenia, ktoré patria ku „nepovinným“ častiam prednášky, sú označené znamienkom +.

Je jasné, že pri texte takéhoto rozsahu sa nedá vyhnúť preklepom i závažnejším chybám. Dúfam, že ich nie je tak veľa, aby znemožňovali čítanie a pochopenie textu. Verím, že aj vďaka vám, budem môcť mnohé z nich opraviť. Za akékoľvek pripomienky k tomuto textu, či už sa týkajú chýb, zrozumiteľnosti, typografickej stránky alebo čohokoľvek iného, vám budem vďačný.

Za viaceré pripomienky a rady, ktoré mi pomohli pri príprave tejto prednášky, by som chcel poďakovať J. Činčurovi a J. Guričanovi.

1.2 Sylaby a literatúra

Sylaby predmetu: Binárne operácie, grupy, polia. Vektorové priestory. Lineárne podpriestory a lineárna nezávislosť. Báza a dimenzia. Matice a sústavy lineárnych rovníc. Lineárne zobrazenia a ich matice. Inverzná matica, hodnosť matice. Determinanty. Skalárny súčin a euklidovské priestory.

Literatúra: Štruktúra prednášky je v podstate totožná so spôsobom, akým je táto téma vysvetlená vo výbornej učebnici [KGGS]. Témy, ktoré budeme preberať na tejto prednáške (mnohé z nich podstatne podrobnejšie), môžete nájsť aj v knihe [K]. Pri príprave textu som použil aj knihu [A].

Ďalšia literatúra dostupná v slovenčine: [BM, SGZ]. Z literatúry dostupnej na internete spomeňme [Z1, O, Sl, H].

1.3 Základné označenia

Pre číselné obory budeme používať nasledujúce označenia:
$\mathbb{N} = \{0, 1, 2, \ldots\}$ = množina prirodzených čísel (Teda nulu považujeme za prirodzené číslo.)
$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ = množina celých čísel
$\mathbb{Z}^+ = \mathbb{N} \setminus \{0\}$ = množina kladných celých čísel
$\mathbb{Q}$=racionálne čísla, $\mathbb{R}$=reálne čísla, $\mathbb{C}$=komplexné čísla
$\mathbb{R}^+ = \{x \in \mathbb{R}; x > 0\}$
$\mathbb{R}_0^+ = \{x \in \mathbb{R}; x \geq 0\}$
$\mathbb{R}^- = \{x \in \mathbb{R}; x < 0\}$
$\mathbb{R}_0^- = \{x \in \mathbb{R}; x \leq 0\}$

Na pripomenutie zo strednej školy: *racionálne čísla* sú čísla tvaru $\frac{p}{q}$, kde $p, q \in \mathbb{Z}$ a $q \neq 0$. Inými slovami povedané, zlomky. Každé racionálne číslo sa dá upraviť do základného tvaru, teda do tvaru $\frac{p}{q}$, kde p a q sú nesúdeliteľné.

S komplexnými číslami ste na strednej škole pravdepodobne nie všetci stretli. Budeme používať niektoré ich základné vlastnosti (a aj v ďalšom štúdiu pre vás budú užitočné). To najzákladnejšie o nich je uvedené v dodatku B a budeme sa snažiť venovať im čas aj na cvičeniach.

Kapitola 2

Množiny a zobrazenia

Na vysokej škole sa stretnete s trochu iným prístupom k matematike ako doteraz. Pre modernú matematiku je typický axiomatický prístup, ktorý spočíva v tom, že vychádzame z niektorých pojmov, ktoré nedefinujeme (chápeme ich ako základné, zvyknú sa nazývať *primitívne pojmy*). Okrem nich zavedieme niekoľko axióm, ktoré hovoria o ich základných vlastnostiach. Všetky ďalšie výsledky musia byť odvodené len z týchto axióm, všetky ďalšie pojmy sú definované len pomocou primitívnych pojmov.

Prvou matematickou knihou, v ktorej sa používali axiómy, boli Euklidove Základy.[1] Priekopníkom používania axiomatickej metódy v modernej matematike bol David Hilbert.[2] V súčasnosti sa za základ matematiky, na základe ktorého sa dajú sformalizovať všetky študované disciplíny, považuje teória množín.

Jedným z cieľov snahy zachytiť matematiku ako celok pomocou axióm (tzv. Hilbertov program) bola snaha o dôkaz bezospornosti matematiky. Dnes je známe, že tento cieľ sa nedá naplniť v takom rozsahu, ako si to predstavoval Hilbert. (Viac sa o tom dá dozvedieť napríklad v knihe [Z2], ktorá však vyžaduje aspoň základné znalosti z teórie množín.) Napriek tomu mal však Hilbertov program obrovský vplyv na podobu modernej matematiky.

Axiomatický prístup má svoje výhody aj nevýhody. Formalizácia prináša výhodu v tom, že sa dôkazy dajú ľahšie skontrolovať (dokonca sa dajú, hoci pomerne pracne, prepísať do takej podoby, aby boli skontrolovateľné počítačovým programom). Takisto ak zadefinujeme nejaký pojem pomocou nejakého systému axióm a z týchto axióm dokážeme nejaké tvrdenia, vieme, že tieto tvrdenia platia pre každý matematický objekt, ktorý spĺňa tieto axiómy. Tento princíp bude v rámci tejto prednášky často používaný.

Za nevýhodu možno považovať to, že formalizáciou sa môže do istej miery stratiť intuitívne porozumenie pojmom s ktorými pracujeme. Preto je dôležité dbať na obe stránky – nielen naučiť sa pracovať s formalizmom, ktorý budeme používať, ale tvrdeniam a dôkazom aj rozumieť.

Zápis tvrdení i definícií nových pojmov bude o čosi formálnejší, než ste boli zvyknutí doteraz. Hoci matematický jazyk, ktorý sa používa v dôkazoch, môže byť pre vás nový a trochu neobvyklý, je veľmi dôležité, aby ste sa ho naučili používať, a ešte dôležitejšie aby ste tomuto jazyku a hlavne dôkazom, ktoré budeme robiť, aj porozumeli.

[1] Euklides (3.–2. stor. pr.n.l) bol grécky matematik a geometer. Jeho najvýznamnejšie dielo *Základy* sa počtom vydaní radí na druhé miesto medzi všetkými knihami v histórii, hneď po Biblii.

[2] David Hilbert (1862–1943) bol nemecký matematik. Je považovaný za jedného z najvýznamnešich matematikov v svojom období ale aj v celej histórii matematiky.

2.1 Dôkazy

Z toho, čo sme povedali o axiomatickom prístupe je zrejmé, že všetky tvrdenia, ktoré budeme používať, sa budeme snažiť aj dokázať. Preto je užitočné povedať si pár slov o dôkazoch. Veľmi dobrý úvodný text o tejto problematike je [KGGS, Kapitola 1.1]. Knihy [L] a [HS] sú venované rôznym postupom používaným pri dôkazoch matematických tvrdení, môžete tam nájsť (okrem iného) aj samostatnú kapitolu venovanú matematickej indukcii.

Ešte prv ako sa začneme venovať formálnej stránke dôkazov, mohli by sme sa zamyslieť nad tým, načo vlastne dokazujeme. Dôkaz poskytuje overenie správnosti tvrdenia – hoci sa vám niektoré tvrdenia môžu zdať intuitívne zrejmé, až podrobný dôkaz nám dá istotu, že je skutočne správne. Pre človeka, ktorý sa venuje matematike, je teda prirodzená potreba vidieť aj dôkaz vysloveného tvrdenia. Považoval by som za úspech tejto prednášky, keby na konci semestra boli pre vás matematické dôkazy väčšmi prostriedkom na overenie, či platí matematická veta, ktorá vás zaujíma, než nutným zlom, ktoré musíte zvládnuť kvôli úspešnému absolvovaniu skúšky.

2.1.1 Základné typy dôkazov

Hoci spôsob, ako dokazovať matematické tvrdenia, sa najlepšie naučíte na konkrétnych príkladoch, predsa len na tomto mieste zhrnieme terminológiu a ukážeme si na veľmi jednoduchých príkladoch niektoré základné typy dôkazov.

Najjednoduchším typom dôkazu je *priamy dôkaz.* Jednoducho postupujeme z predpokladov tvrdenia, až kým sa nám nepodarí dostať dokazovaný výrok. Vyskúšajme si to na príklade nasledujúceho tvrdenia.

Tvrdenie 2.1.1. *Nech n je celé číslo. Potom zvyšok čísla n^2 po delení 4 je 0 alebo 1. Pritom ak n je párne, tak n^2 je deliteľné 4 a ak n je nepárne tak n^2 má zvyšok 1.*

Dôkaz. Sú 2 možnosti. Buď n je párne, alebo n je nepárne.

Ak n je párne, tak $n = 2k$ (pre nejaké celé číslo k) a $n^2 = 4k^2$, čiže n^2 má zvyšok 0 po delení 4.

Ak n je nepárne, tak $n = 2k + 1$, čiže $n^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$ má zvyšok 1 po delení 4. □

Iný typ dôkazu je *dôkaz sporom.* Pri tomto type dôkazu začneme s predpokladom, že dokazované tvrdenie neplatí. Ak sa nám z tohoto tvrdenia podarí odvodiť niečo, čo určite platiť nemôže, musí byť predpoklad o neplatnosti dokazovaného tvrdenia chybný – a tým sme tvrdenie vlastne dokázali.

Tvrdenie 2.1.2. *Ak pre celé čísla a, b, c platí rovnosť $a^2 + b^2 = c^2$, tak aspoň jedno z čísel a, b je párne.*

Dôkaz. Sporom. Predpokladajme, že by a aj b boli nepárne. Potom podľa tvrdenia 2.1.1 majú a^2 aj b^2 zvyšok 1 po delení 4. Ich súčet $c^2 = a^2 + b^2$ má potom zvyšok 2. Podľa tvrdenia 2.1.1 sú však druhá mocnina môže mať ako zvyšok po delení 4 iba číslo 0 alebo 1 – dostali sme spor. □

Nepriamy dôkaz sa dosť podobá na dôkaz sporom. Väčšina tvrdení, ktoré dokazujeme majú tvar implikácie: snažíme sa dokázať, že ak platia predpoklady P, tak platí aj záver Z. Nepriamy dôkaz spočíva v tom, že namiesto toho dokazujeme: Ak neplatí záver Z, tak neplatí ani predpoklad P. (Skúste si rozmyslieť, prečo je to to isté ako dokazovať pôvodnú implikáciu. K implikáciam aj k princípu nepriameho dôkazu sa ešte vrátime v časti 2.1.4 venovanej tautológiám.)

Tvrdenie 2.1.3. *Nech n je prirodzené číslo. Ak n^2 je deliteľné štyrmi, tak n je párne.*

Dôkaz. Nepriamo. Nech n je nepárne, teda má tvar $n = 2k + 1$. Potom $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$ má zvyšok 1 po delení štyrmi, čiže nie je deliteľné štyrmi. □

Všimnite si, že v predchádzajúcom tvrdení sme namiesto výroku z tvrdenia dokazovali: Ak n nie je párne, tak n^2 nie je deliteľné štyrmi.

2.1.2 Matematická indukcia

Často používaný, a preto aj dosť dôležitý spôsob dôkazu, je dôkaz pomocou matematickej indukcie. Povedzme si teda o ňom pár slov a ilustrujeme si ho na niekoľkých príkladoch. (S matematickou indukciou ste sa už stretli na strednej škole, táto podkapitolka slúži len na pripomenutie.)

Dôkaz *matematickou indukciou* spočíva v tom, že ak chceme dokázať nejaký výrok $V(n)$ pre všetky prirodzené čísla $n \in \mathbb{N}$, dokážeme ho najprv pre $n = 0$ a ďalej dokážeme, že ak platí $V(n)$, tak tento výrok platí pre nasledujúce číslo, teda platí $V(n + 1)$. (Toto treba dokázať pre všetky prirodzené čísla n.)

Dôkaz, že z $V(n)$ vyplýva $V(n+1)$ nazývame *indukčný krok* a výrok $V(n)$ použitý v tomto kroku sa volá *indukčný predpoklad.*

Dokazovaný výrok môže obsahovať viacero premenných, preto pri dôkaze matematickou indukciou vždy treba uviesť, vzhľadom na ktorú premennú sa indukcia robí.

Niekedy sa indukčného kroku v tvare $V(n) \Rightarrow V(n+1)$ (z $V(n)$ vyplýva $V(n+1)$) používa tvar $V(n-1) \Rightarrow V(n)$ (z $V(n-1)$ vyplýva $V(n)$). Oba prístupy sú rovnocenné, v druhom prípade samozrejme dokazujeme indukčný krok len pre $n \geq 1$. (Pre $n = 0$ by ani nedával zmysel, lebo $V(-1)$ vôbec nemusí byť zadefinované.) My budeme používať prvý z týchto dvoch prístupov.

Niekedy (keď výrok dokazujeme pre všetky čísla počnúc od nejakého daného čísla n_0) nerobíme prvý krok indukcie pre $n = 0$ ale pre $n = n_0$. Aj v indukčnom kroku potom môžeme použiť predpoklad $n \geq n_0$ namiesto $n \geq 0$.

Príklad 2.1.4. Uvažujme geometrickú postupnosť určenú predpisom $a_0 = 1$ a $a_{n+1} = 2a_n$. (Teda členy tejto postupnosti sú $a_0 = 1, a_1 = 2, a_2 = 4, \ldots, a_n = 2^n, \ldots$) Dokážeme, že pre súčet prvých $n + 1$ členov tejto postupnosti platí

$$1 + 2 + \cdots + 2^n = \sum_{k=0}^{n} 2^k = 2^{n+1} - 1.$$

Budeme postupovať matematickou indukciou vzhľadom na n.

1° Pre $n = 0$ dostaneme rovnosť $2^0 = 2^1 - 1$, teda tvrdenie platí.

2° Indukčný krok. Predpokladajme, že rovnosť platí pre n. Potom pre $n + 1$ dostaneme

$$1+2+\cdots+2^n+2^{n+1} = (1+2+\cdots+2^n)+2^{n+1} \overset{\text{IP}}{=} 2^{n+1}-1+2^{n+1} = 2.2^{n+1}-1 = 2^{n+2}-1,$$

čo môžeme stručnejšie zapísať ako

$$\sum_{k=0}^{n+1} 2^k = 2^{n+1} + \sum_{k=0}^{n} 2^k \overset{\text{IP}}{=} 2^{n+1} + 2^{n+1} - 1 = 2.2^{n+1} - 1 = 2^{n+2} - 1.$$

Indukčný predpoklad sme použili na mieste označenom IP.

Takmer rovnakým spôsobom by ste mohli odvodiť vzorec pre súčet prvých $n + 1$ členov ľubovoľnej geometrickej postupnosti. (Teda a_0 bude ľubovoľné a aj dvojku nahradíme ľubovoľným kvocientom $q \neq 1$.) Vyskúšajte si to!

Poznámka 2.1.5. Okrem dôkazov sa matematická indukcia používa aj pri definíciach. Ak chceme zadefinovať nejaký matematický objekt pre ľubovoľné prirodzené číslo n, môžeme postupovať tak, že ho zadefinujeme pre $n = 0$ a ďalej zavedieme $(n+1)$-vý objekt pomocou n-tého. V takomto prípade hovoríme o *definícii matematickou indukciou.*

Definíciu matematickou indukciou sme už použili v predchádzajúcom príklade – postupnosť (a_n) bola určená tým, že $a_0 = 1$ a $a_{n+1} = 2a_n$.

Veľmi dôležitým variantom matematickej indukcie je *úplná indukcia.* V tomto prípade v indukčnom kroku dokazujeme platnosť nového tvrdenia nie pomocou platnosti pre predchádzajúce číslo, ale v dôkaze využijeme platnosť tvrdenia pre všetky (prípadne viaceré) menšie čísla.

Zatiaľ čo indukčný krok matematickej indukcie sme mohli schematicky zapísať ako

$$V(n) \Rightarrow V(n+1)$$

pri úplnej indukcii v indukčnom kroku dokazujeme

$$V(0), V(1), V(2), \ldots, V(n) \Rightarrow V(n+1);$$

inak povedané, treba dokázať že ak výrok $V(k)$ platí pre všetky $k < n$, tak platí aj pre číslo n. (Samozrejme, aj tu by sme mohli úplne rovnocenne použiť indukčný krok kde by sme dokazovali $V(n)$ z platnosti dokazovaného výroku pre $k = 0, 1, \ldots, n-1$. Niekedy budeme používať úplnú indukciu aj v takejto podobe.) Aj tu platí, že indukciu môžeme začať aj od iného prvku namiesto nuly.

Príklad 2.1.6. Uvažujme postupnosť určenú predpisom $a_0 = 1$ a $a_{n+1} = a_0 + a_1 + \cdots + a_n = \sum\limits_{k=0}^{n} a_k$. (Všimnite si, že sme túto postupnosť definovali pomocou úplnej indukcie – definícia $(n+1)$-vého prvku využíva všetky menšie prvky.) Dokážeme úplnou indukciou vzhľadom na n, že pre $n \geq 1$ platí $a_n = 2^{n-1}$.

1° Pre $n = 0$ máme $a_1 = 1 = 2^{1-1}$, teda v tomto prípade dokazovaná rovnosť platí.

2° Indukčný krok: Predpokladajme, že $a_k = 2^k$ pre $k = 0, 1, \ldots, n$. Potom

$$a_{n+1} = \sum_{k=0}^{n} a_k = a_0 + \sum_{k=1}^{n} a_k \overset{\text{IP}}{=} 1 + \sum_{k=1}^{n} 2^{k-1} \overset{(1)}{=} 1 + \sum_{j=0}^{n-1} 2^j \overset{(2)}{=} 1 + 2^n - 1 = 2^n.$$

(V rovnosti (1) sme zaviedli novú sumačnú premennú $j = k - 1$ a v rovnosti (2) sme využili výsledok dokázaný v príklade 2.1.4.)

Poznámka 2.1.7. Určite ste si všimli, že v príkladoch dôkazov matematickou indukciou sme používali zápisy typu $\sum\limits_{k=1}^{n} a_k = a_1 + \ldots + a_n$. (Pokiaľ nie ste na používanie znaku $\sum$ zvyknutí zo stednej školy, vo vysokoškolskej matematike sa s ním budete stretávať veľmi často, takže si naň treba čím skôr zvyknúť.) Zjednodušene sa dá povedať, že ak sa pri úprave výrazov vystkytne výraz obsahujúci tri bodky (...), v skutočnosti je za touto úpravou skrytý dôkaz matematickou indukciou. (Väčšinou natoľko jednoduchý, že dôkaz správnosti tejto úpravy samostatne nedokazujeme.)

2.1.3 Drobné rady ako dokazovať

Hoci nasledujúca rada na prvý pohľad znie veľmi naivne, pri hľadaní dôkazu nejakého tvrdenia je užitočné uvedomiť si, čo všetko máme zadané a čo potrebujeme dokázať. Pri jednoduchších

dôkazoch sa často stane, že keď si poriadne zapíšeme vlastnosť, ktorú chceme dokázať a takisto všetky predpoklady, takmer okamžite zbadáme, ako postupovať. Samozrejme, aj pri zložitejších dôkazoch je veľmi dobre nestrácať zo zreteľa aké predpoklady môžeme použiť a k čomu vlastne chceme dospieť.

Niekedy môže byť užitočné aj hľadanie protipríkladu, prípadne overenie tvrdenia na konkrétnych príkladoch. Môže sa stať, že si uvedomíte, prečo sa vám kontrapríklad nedarí zostrojiť alebo pri overovaní, či tvrdenie platí pre konkrétny príklad prídete na nejakú zákonitosť, ktorá vám nakoniec pomôže dané tvrdenie dokázať.

Ďalšia rada je, že občas nie je zle uvedomiť si, či ste skutočne v dôkaze použili všetky predpoklady. Tvrdenia a úlohy v učebniciach bývajú často formulované tak, že tam nie sú uvedené žiadne zbytočné predpoklady navyše. Preto dôkaz, kde ste nepoužili všetky predpoklady, je trochu podozrivý a treba ho skontrolovať. (Aj keď sa samozrejme môže stať, že zákerný autor úlohy či skúšajúci mohol pridať nejaké predpoklady navyše.)

2.1.4 Výroky, logické spojky, tautológie

Toto je ďalšia téma, ktorú by ste mali ovládať už zo strednej školy – napriek tomu však pripomenieme niektoré základné fakty.

Definícia 2.1.8. *Negáciou* výroku P rozumieme výrok „neplatí P“. Označujeme ju $\neg P$.

Pre dva výroky P a Q nazývame ich *konjunkciou* výrok „P a Q“, označujeme $P \wedge Q$.

Disjunkcia je výrok „P alebo Q“, označujeme $P \vee Q$.

Pod *implikáciou* rozumieme výrok „ak platí P, tak platí Q“, označujeme $P \Rightarrow Q$.

Ekvivalencia výrokov P a Q je výrok „P platí práve vtedy, keď platí Q“, označujeme $P \Leftrightarrow Q$.

Tieto definície logických spojok sú zhrnuté v nasledujúcich pravdivostných tabuľkách.[3]

P	$\neg P$
1	0
0	1

P	Q	$P \wedge Q$
1	1	1
1	0	0
0	1	0
0	0	0

P	Q	$P \vee Q$
1	1	1
1	0	1
0	1	1
0	0	0

P	Q	$P \Rightarrow Q$
1	1	1
1	0	0
0	1	1
0	0	1

P	Q	$P \Leftrightarrow Q$
1	1	1
1	0	0
0	1	0
0	0	1

Tautológie môžeme overovať jednoducho metódou, ktorú poznáte zo strednej školy.

Príklad 2.1.9. Overme napríklad tautológiu $P \vee (\neg P)$ (princíp vylúčenia tretieho).

P	$\neg P$	$P \vee \neg P$
1	0	1
0	1	1

Ako ďalší príklad si ukážeme overenie jedného z de Morganových pravidiel.

Príklad 2.1.10. *De Morganove pravidlá* sú pravidlá ako negovať konjunkciu a disjunkciu.

$$\neg(P \wedge Q) \quad \Leftrightarrow \quad \neg P \vee \neg Q$$
$$\neg(P \vee Q) \quad \Leftrightarrow \quad \neg P \wedge \neg Q$$

Samozrejme, pretože teraz vo výroku vystupuje viacero premenných, budeme potrebovať viac riadkov tabuľky na to, aby sme vyčerpali všetky možnosti.

[3] Na označovanie pravdivosti a nepravdivosti budeme v tabuľke používať symboly 1 a 0. Niekedy sa zvyknú používať aj T a F, ako skratky pre anglické true a false.

P	Q	$P \vee Q$	$\neg(P \vee Q)$	$\neg P \wedge \neg Q$	$\neg(P \vee Q) \Leftrightarrow (\neg P \wedge \neg Q)$
1	1	1	0	0	1
1	0	1	0	0	1
0	1	1	0	0	1
0	0	0	1	1	1

Niekedy si môžeme pri overovaní platnosti tautológie použiť aj jednoduchší postup. V predchádzajúcom príklade sme napríklad mohli na základe symetrie overovať o jeden riadok menej. Inú možnosť zjednodušenia ilustruje nasledujúci príklad.

Príklad 2.1.11. Dokážeme tautológiu $(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$. (Táto tautológia súvisí s princípom nepriameho dôkazu. Implikácia $\neg Q \Rightarrow \neg P$ sa zvykne nazývať *obmena implikácie* $P \Rightarrow Q$.)

Aby sme dokázali ekvivalenciu dvoch výrokov, stačí ukázať, že výrok na ľavej strane je nepravdivý práve v tých prípadoch, kedy je nepravdivý výrok na pravej strane.

Implikácia je nepravdivá jedine v prípade, že ľavý výrok je pravdivý a pravý je nepravdivý (prípad $1 \Rightarrow 0$). Teda výrok $P \Rightarrow Q$ je nepravdivý práve vtedy, keď $P = 1$ a $Q = 0$. Podobne, aby bol výrok $\neg Q \Rightarrow \neg P$ nepravdivý, musí byť $\neg Q = 1$ a $\neg P = 0$, čo je presne ten istý prípad $P = 1$ a $Q = 0$. Vidíme, že obe strany ekvivalencie majú vždy tú istú pravdivostnú hodnotu.

(Tento spôsob overenia tautológie sa až tak veľmi nelíši od tabuľkovej metódy – vlastne sme si len rozmysleli, v ktorých riadkoch tabuľky sa na oboch stranách uvedenej ekvivalencie vyskytne 0 – zdá sa mi byť bližší ku spôsobu, ako prirodzene uvažujeme o výrokoch.)

V cvičení 2.1.1 nájdete viacero tautológií. Je dobré si uvedomiť ako súvisia tautológie s niektorými typmi dôkazov. Tautológia z príkladu 2.1.11 je presne princíp nepriameho dôkazu, ktorý sme už spomínali. Tautológiu z cvičenia 2.1.1b) budeme tiež často používať pri dokazovaní – namiesto výroku tvaru $P \Leftrightarrow Q$ dokážeme zvlášť jednotlivé implikácie $P \Rightarrow Q$ a $Q \Rightarrow P$.

2.1.5 Negácia výrokov s kvantifikátormi

Okrem logických spojok budeme na zápis tvrdení používať aj kvantifikátory. Budeme používať všeobecný (univerzálny) kvantifikátor

$$(\forall x \in A)P(x)$$

vo význame „pre každý prvok x množiny A platí $P(x)$“ a existenčný kvanfitifkátor

$$(\exists x \in A)P(x),$$

ktorý znamená „existuje prvok x množiny A, pre ktorý platí $P(x)$“. (Tu $P(x)$ predstavuje *výrokovú funkciu* – výrok, v ktorom vystupuje „premenná“ x.)

Veľmi dôležité budú nasledovné pravidlá pre negáciu výrokov s kvantifikátormi.

$$\begin{aligned} \neg[(\forall x)P(x)] \quad &\Leftrightarrow \quad (\exists x)(\neg P(x)), \\ \neg[(\exists x)P(x)] \quad &\Leftrightarrow \quad (\forall x)(\neg P(x)). \end{aligned}$$

(Teda existenčný kvantifikátor sa mení na všeobecný a obrátene a výrok pod kvantifikátorom sa zneguje.)

Cvičenia

Úloha 2.1.1. Dokážte, že nasledujúce výroky sú tautológie:
a) $(\neg P \vee Q) \Leftrightarrow (P \Rightarrow Q)$
b) $(P \Leftrightarrow Q) \Leftrightarrow [(P \Rightarrow Q) \wedge (Q \Rightarrow P)]$
c) $\neg(P \wedge Q) \Leftrightarrow (\neg P \vee \neg Q)$
d) $((P \wedge Q) \Rightarrow R) \Leftrightarrow (P \Rightarrow (Q \Rightarrow R))$

2.2 Množiny a zobrazenia

2.2.1 Množiny

Už sme spomenuli, že základným stavebným kameňom súčasnej matematiky je teória množín. Viac sa o nej dozviete v 4. ročníku (viď. tiež [ŠS]). V tejto prednáške úplne vystačíme so základnými predstavami o množinách. (Takýto intuitívny prístup k teórii množín sa zvykne nazývať naivná teória množín – na rozdiel od axiomatickej teórie množín, ktorá systematicky definuje pojem množiny pomocou niekoľkých základných axióm.) Navyše, všetky množiny, s ktorými sa budeme stretávať budú množina komplexných čísel a rôzne jej podmnožiny (ako napríklad $\mathbb{R}$, $\mathbb{Z}$, $\mathbb{N}$). Tieto množiny poznáte zo strednej školy a mali by ste o nich mať dobrú intuitívnu predstavu, takže si až tak veľmi nemusíme robiť starosti s tým, že si celkom presne nevysvetlím, čo sa rozumie pod pojmom množina.

Pre naše účely stačí množinu chápať ako súhrn nejakých prvkov. Pričom prvky budú najčastejšie čísla, niekedy aj množiny alebo zobrazenia. A takisto sa budeme stretávať s množinami, ktoré sa dajú z množín čísel vytvoriť pomocou množinových operácií ako sú napríklad zjednotenie alebo karteziánsky súčin.

Každá množina je určená svojimi prvkami. Inak povedané, dve množiny sa rovnajú, ak majú rovnaké prvky.

Definícia 2.2.1. Vzťah byť prvok množiny zapisujeme ako $x \in A$, čítame „x patrí A."

Hovoríme, že množiny A a B sa *rovnajú* (označujeme $A = B$), ak platí

$$(x \in A) \qquad \Leftrightarrow \qquad (x \in B)$$

pre ľubovoľný prvok x.

Množiny, ktorá nemá nijaké prvky nazývame *prázdna množina* a označujeme $\emptyset$.

To znamená, že pre nijaké x neplatí $x \in \emptyset$.

Ďalej pripomenieme niektoré základné vzťahy a operácie s množinami. (Opäť ide o opakovanie – pravdepodobne ste o nich už počuli.)

Definícia 2.2.2. Hovoríme, že A je *podmnožinou* B, ak každý prvok množiny A patrí aj do B, označujeme $A \subseteq B$. Inak povedané, $A \subseteq B$ ak pre každé x platí

$$(x \in A) \qquad \Rightarrow \qquad (x \in B).$$

Vzťah množín A a B, pre ktoré platí $A \subseteq B$ sa tiež zvykne nazývať *inklúzia.*

Inklúziu budeme často používať pri dôkaze rovnosti nejakých množín. Platí totiž

$$A = B \qquad \Leftrightarrow \qquad (A \subseteq B) \wedge (B \subseteq A).$$

(Vyplýva to z tautológie uvedenej v cvičení 2.1.1b) v časti 2.1. Ak totiž za výroky vystupujúce v tejto tautológii dosadíme $x \in A$ a $x \in B$, tak dostaneme, že tvrdenie $(x \in A) \Leftrightarrow (x \in B)$,

čo je presne rovnosť množín A a B, je ekvivalentné s tvrdením $[(x \in A) \Rightarrow (x \in B)] \wedge [(x \in B) \Rightarrow (x \in A)]$, čo môžeme skrátene zapísať $(A \subseteq B) \wedge (B \subseteq A)$.)

Pripomenieme si teraz niekoľko spôsobov, ako môžeme z daných množín vytvárať nové množiny.

Často budeme definovať množiny zápisom tvaru

$$\{x \in A; P(x)\},$$

ktorý znamená množinu všetkých tých prvkov z A, pre ktoré platí výrok $P(x)$. (Pričom A je nejaká vopred daná množina.) Napríklad z množiny prirodzených čísel $\mathbb{N}$ môžeme vybrať párne čísla $E = \{n \in \mathbb{N}; n \text{ je deliteľné číslom } 2\}$.

Zo strednej školy poznáte základné operácie s množinami – prienik, zjednotenie a rozdiel množín – pripomeňme si však ich definície. Použijeme pri nich práve typ zápisu, ktorý sme pred chvíľou spomínali.

Definícia 2.2.3. *Zjednotenie* dvoch množín A a B je množina

$$A \cup B = \{x; x \in A \vee x \in B\}.$$

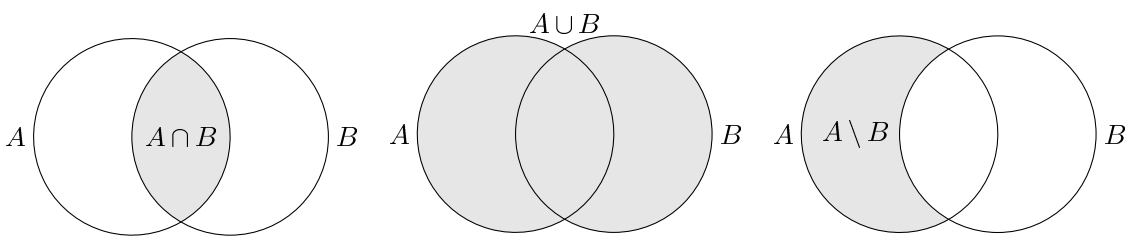
Prienik dvoch množín A a B je množina

$$A \cap B = \{x \in A; x \in B\}.$$

Rozdiel dvoch množín A a B je množina

$$A \setminus B = \{x \in A; x \notin B\}$$

Operácie s množinami znázorňujeme pomocou *Vennových diagramov* (obr. 2.1).



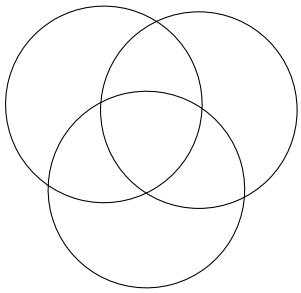
Obr. 2.1: Operácie s množinami

Keďže množiny často definujeme pomocou nejakého výroku, ktorý majú spĺňať všetky prvky množiny, dajú sa operácie s množinami chápať aj ako iný spôsob vyjadrovania o výrokoch. Aj identity s množinami môžeme overovať tak, že pracujeme s výrokmi typu $x \in A$. Iný spôsob je použiť Vennove diagramy – v tom prípade je potrebné nakresliť si množiny v všeobecnej (alebo tiež generickej polohe) – tak, aby sme na diagrame mali body pre každú možnú kombináciu pravdivostných hodnôt výrokov $x \in A$, $x \in B$ atď.

Často budeme používať aj zjednotenie a prienik nekonečného počtu množín. Ak $\{A_i; i \in I\}$ je nejaký systém množín (oindexovaný prvkami množiny I), tak používame označenia

$$\bigcup_{i \in I} A_i = \{x; (\exists i \in I) x \in A_i\}$$

$$\bigcap_{i \in I} A_i = \{x; (\forall i \in I) x \in A_i\}$$



Obr. 2.2: Generická poloha

V prípade, že indexová množina je $I = \{1, 2, \ldots\}$, budeme používať označenie $\bigcup_{n=1}^{\infty} A_n$ resp. $\bigcap_{n=1}^{\infty} A_n$.

Bude pre nás dôležité ešte jedna operácia s množinami – karteziánsky súčin.

Definícia 2.2.4. Ak A, B sú množiny, tak ich *karteziánsky súčin* je množina všetkých usporiadaných dvojíc (a, b) takých, že $a \in A$ a $b \in B$. Označujeme ho

$$A \times B = \{(a, b); a \in A, b \in B\}.$$

Hoci pojem *usporiadaná dvojica* sme nedefinovali, malo by byť intuitívne jasné, čo sa ním myslí. Slovíčko usporiadaná je v názve preto, že záleží na poradí. Usporiadanú dvojicu prvkov a a b budeme označovať (a, b).

Napríklad

$$\{0, 1\} \times \{0, 1\} = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$$

a dvojice $(0, 1)$ a $(1, 0)$ považujeme za rôzne. (Oproti tomu, množiny $\{0, 1\}$ a $\{1, 0\}$ sú rovnaké – pretože pri množinách záleží len na tom, ktoré prvky tam patria.)

2.2.2 Zobrazenia

Pod zobrazením z množiny X do množiny Y rozumieme akýkoľvek predpis, ktorý každému prvku množiny X priradí jediný prvok množiny Y. Formálne môžeme zobrazenie zadefinovať nasledovne:

Definícia 2.2.5. *Zobrazenie* $f\colon X \to Y$ z množiny X do množiny Y je podmnožina f množiny $X \times Y$ taká, že ku každému $x \in X$ existuje práve jedno $y \in Y$ s vlastnosťou $(x, y) \in f$.

Množinu X budeme tiež nazývať *definičný obor* zobrazenia f a množina Y je *obor hodnôt* zobrazenia f.

Namiesto zápisu $(x, y) \in f$ budeme používať zápis $y = f(x)$.

Podmienka, že ku každému $x \in X$ existuje práve jedno $y \in Y$, je presne formalizáciou toho, čo chápeme pod priradením (jediného) prvku $y = f(x)$ každému prvku $x \in X$.

Poznamenajme, že (podobne ako pri mnohých ďalších označeniach) pri použití inej literatúry je často nutné skontrolovať, či sa zhodujú použité definície. (V prípadoch, keď sa budeme hovoríť o pojmoch a označeniach, ktoré sa často zvyknú v matematickej literatúre líšiť, na to vždy upozorníme.)

V tomto prípade je vhodné spomenúť, že [KGGS] používa namiesto $y = f(x)$ zápis $y = xf$. (V súvislosti so zobrazeniami sa v [KGGS] vyskytujú aj ďalšie odlišnosti, ku ktorým sa o chvíľu dostaneme.)

Príklad 2.2.6. Uvedieme niekoľko príkladov zobrazení.
$f_1\colon \mathbb{N} \to \mathbb{N},\ f_1(n) = 2n + 1$
$f_2\colon \mathbb{N} \to \mathbb{N},\ f_2(n) = 2n$
$f_3\colon \mathbb{N} \to \mathbb{N},\ f_3(n) = \begin{cases} n+1, & \text{ak } n \text{ je párne} \\ n-1, & \text{ak } n \text{ je nepárne} \end{cases}$
$f\colon \mathbb{R} \to \mathbb{R},\ f(x) = x.\sin x$
$g\colon \mathbb{R} \to \mathbb{R},\ g(x) = \sin x$
$h\colon \mathbb{R} \to \mathbb{R},\ h(x) = x^2$

Definícia 2.2.7. Hovoríme, že dve zobrazenia $f\colon X \to Y$ a $g\colon Z \to W$ sa *rovnajú,* ak $X = Z$, $Y = W$ a $f(x) = g(x)$ pre každé $x \in X$. (Inými slovami, ak sa rovnajú ich definičné obory, obory hodnôt a obe zobrazenia nadobúdajú v každom bode rovnakú hodnotu.) Rovnosť zobrazení označujeme $f = g$.

Príklad 2.2.8. Dve zobrazenia sa môžu rovnať aj keď sú zapísané iným zápisom. Napríklad zobrazenia $k, l\colon \mathbb{R} \to \mathbb{R}$ určené predpismi $k(x) = \sin^2 x + \cos^2 x$ a $l(x) = 1$ sa rovnajú.

O celkom zaujímavom vývoji pojmu zobrazenia v histórií teórie množín sa viac môžete dozvedieť napríklad v úvodnej kapitole knihy [BŠ].

V tejto kapitole ešte zavedieme ďalšie dôležité pojmy, ako sú skladanie zobrazení, bijektívne, injektívne a surjektívne zobrazenia.

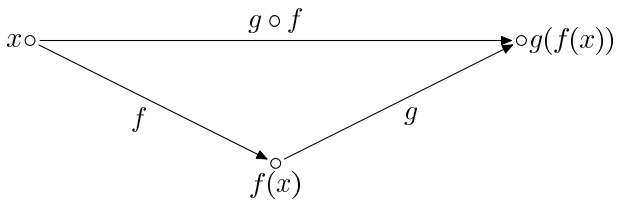
Definícia 2.2.9 (Skladanie zobrazení). Ak $f\colon X \to Y$, $g\colon Y \to Z$ sú zobrazenia, tak *zložením zobrazení f a g* nazývame zobrazenie $g \circ f\colon X \to Z$ také, že pre každé $x \in X$ platí

$$g \circ f(x) = g(f(x)).$$

Zobrazenia môžeme skladať iba vtedy, keď obor hodnôt prvého zobrazenia je rovnaký ako definičný obor druhého zobrazenia.

$$\begin{tikzcd} A \arrow[rr, "g\circ f"] \arrow[dr, "f"'] & & C \\ & B \arrow[ur, "g"'] & \end{tikzcd}$$

Ak si predstavíme zobrazenia ako šípku smerujúcu od x ku $f(x)$, tak skladanie zobrazení znamená, že z x prejdeme najprv po šípke f a potom po šípke g, čiže sa dostaneme do $g(f(x))$. Táto predstava o skladaní zobrazení je znázornená na obrázku 2.3.



Obr. 2.3: Skladanie zobrazení

Napríklad pre funkcie g a h z príkladu 2.2.6 dostaneme $h \circ g(x) = \sin^2 x$ a $g \circ h(x) = \sin x^2$. Vidíme, že pre zobrazenia $g, h\colon A \to A$ vo všeobecnosti neplatí $g \circ h = h \circ g$.

POZOR!!! V niektorej literatúre (napríklad v [KGGS]) nájdete skladanie zobrazení definované v opačnom poradí (t.j. $g \circ f(x) = f(g(x))$), my ho budeme používať tak, ako sme ho zaviedli v definícii 2.2.9. (Na prvý pohľad vyzerá zápis $g \circ f(x) = f(g(x))$ nelogicky; môžeme ho chápať tak, že píšeme zobrazenia v takom poradí, ako sa skladajú. Ak by ste sa pozreli do [KGGS], zistili by ste, že namiesto $f(x)$ používajú autori zápis xf. Pri takomto označení je skutočne logickejší zápis $x(g \circ f) = (xg)f$.)[4]

Teraz dokážeme veľmi dôležitú vlastnosť skladania zobrazení.

Tvrdenie 2.2.10 (Asociatívnosť skladania zobrazení). *Nech $f\colon X \to Y$, $g\colon Y \to Z$, $h\colon Z \to W$ sú zobrazenia, potom*

$$(h \circ g) \circ f = h \circ (g \circ f).$$

Dôkaz. Obe zobrazenia, ktoré porovnávame, sú zobrazenia z množiny X do množiny W. Majú teda rovnaké definičné obory i obory hodnôt.

Zostáva nám teda overiť, či nadobúdajú rovnaké hodnoty. To zistíme jednoduchým výpočtom:

$$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x)))$$
$$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x)))$$

□

V ďalších častiach tejto prednášky budú dosť dôležité typy zobrazení, ktoré teraz zadefinujeme.

Definícia 2.2.11. Nech $f\colon X \to Y$ je zobrazenie. Hovoríme, že f je *injektívne* (*prosté*) *zobrazenie* (alebo tiež injekcia), ak pre všetky $x, y \in X$ také, že $x \neq y$ platí $f(x) \neq f(y)$.

Hovoríme, že f je *surjekcia* (*surjektívne zobrazenie, zobrazenie na*), ak pre každé $y \in Y$ existuje také, $x \in X$, že $f(x) = y$.

Hovoríme, že f je *bijekcia* (*bijektívne zobrazenie*), ak f je súčasne injekcia aj surjekcia.

Ekvivalentná definícia injekcie by bola, ak by sme namiesto

$$x \neq y \ \Rightarrow f(x) \neq f(y)$$

uvažovali podmienku

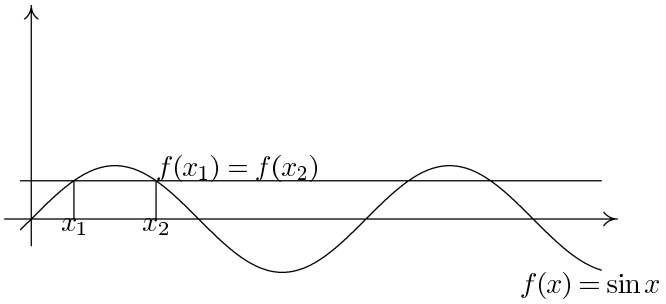
$$f(x) = f(y) \ \Rightarrow x = y.$$

(Lebo výroky $P \Rightarrow Q$ a $\neg Q \Rightarrow \neg P$ sú ekvivalentné, pozri príklad 2.1.11.)

Definíciu surjektívneho zobrazenia by sme mohli preformulovať tak, že každá hodnota y z oboru hodnôt Y sa nadobúda v aspoň jednom bode definičného oboru.

Z grafu zobrazenia $f\colon \mathbb{R} \to \mathbb{R}$ môžeme jednoducho vyčítať, či ide o injekciu alebo surjekciu. Stačí sa pozrieť na vodorovné priamky – rovnobežné s osou x. Zobrazenie je injektívne, ak každá takáto priamka pretína graf funkcie najviac raz (pozri Obr. 2.4). Zobrazenie je surjektívne, ak každá takáto priamka pretína graf funkcie aspoň raz. Zobrazenie je bijektívne, ak každá takáto priamka pretína graf funkcie práve raz.

[4] Pravdepodobne si budete musieť zvyknúť na to, že na rôznych prednáškach sa stretnete s rozličnými spôsobmi označenia; napríklad pri skladaní zobrazení ale aj pri ďalších iných veciach. Ja som zvolil používanie poradia skladania tak, aby bolo rovnaké s definíciou skladania zobrazení, ktorú používate na prednáške z matematickej analýzy v prvom ročníku – teda aby ste nemali problém s používaním 2 rozličných označení počas toho istého ročníka.



Obr. 2.4: Ak vodorovná priamka pretne graf v 2 bodoch, zobrazenie nie je injektívne

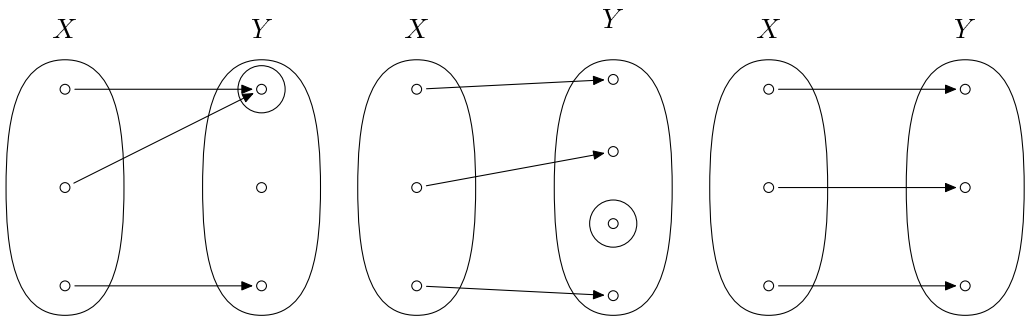
Príklad 2.2.12. Zobrazenie $f(x) = \sin x$, $f\colon \mathbb{R} \to \mathbb{R}$ nie je ani surjektívne ani injektívne. (Napríklad $f(0) = f(\pi) = f(2\pi) = 0$, preto f nie je injektívne. Hodnota $2 \in \mathbb{R}$ sa nenadobúda v žiadnom bode.)

Ak však zmeníme obor hodnôt $g(x) = \sin x$, $g\colon \mathbb{R} \to \langle -1, 1\rangle$, dostaneme už surjektívne zobrazenie.

Zobrazenie $h(x) = \sqrt{x}$, $h\colon \langle 0, \infty) \to \mathbb{R}$ je injektívne. Opäť, ak by sme zmenili obor hodnôt, dostaneme surjektívne zobrazenie $j(x) = \sqrt{x}$, $j\colon \langle 0, \infty) \to \langle 0, \infty)$. Zobrazenie j je bijekcia (je injektívne aj surjektívne.)

Iným príkladom bijektívneho zobrazenia je $k\colon (-\frac{\pi}{2}, \frac{\pi}{2}) \to \mathbb{R}$, $k(x) = \operatorname{tg} x$.

Opäť si môžeme pomôcť predstavou zobrazení ako šípok. Zobrazenie je injekcia, ak nenastane situácia znázornená na ľavom obrázku v 2.5, keď sa viaceré šípky stretnú v jednom bode. O surjekciu ide vtedy, ak do každého bodu ide aspoň jedna šípka, čiže nenastane situácia znázornená na prostrednom obrázku. V prípade bijekcie ide z každého prvku x jediná šípka do jediného bodu y, teda bijekcia určuje jedno-jednoznačné priradenie medzi prvkami.



Obr. 2.5: Ilustrácia injekcie, surjekcie a bijekcie

Tvrdenie 2.2.13. *Zloženie dvoch injekcií je injekcia, zloženie dvoch surjekcií je surjekcia, zloženie dvoch bijekcií je bijekcia.*

Dôkaz. Dané zobrazenia označme $f\colon X \to Y$, $g\colon Y \to Z$.

Najprv predpokladajme, že f aj g sú injekcie. Nech ďalej $x, y \in X$ majú tú vlastnosť, že

$$(g \circ f)(x) = (g \circ f)(y).$$

Túto rovnosť môžeme prepísať ako

$$g(f(x)) = g(f(y)).$$

Pretože g je injekcia, vyplýva z tejto rovnosti

$$f(x) = f(y).$$

Opäť použitím definície injekcie, ale tentokrát pre zobrazenie f, dostaneme

$$x = y.$$

Dokázali sme implikáciu $(g \circ f)(x) = (g \circ f)(y) \Rightarrow x = y$, teda $g \circ f$ je skutočne injekcia.

Teraz nech f aj g sú surjekcie. Máme dokázať, že ku každému $z \in Z$ existuje $x_0 \in X$ také, že $g(f(x_0)) = z$. Z toho, že g je surjekcia, vieme, že existuje $y_0 \in Y$ také, že $g(y_0) = z$. Podobne (pretože f je surjekcia), k tomuto y_0 vieme nájsť x_0 také, že $f(x_0) = y_0$. Spojením týchto dvoch rovností ale dostaneme

$$g(f(x_0)) = g(y_0) = z,$$

teda sme skutočne našli x_0, ktoré sa zobrazením $g \circ f$ zobrazí na z.

Posledná časť tvrdenia (ktorá hovorí o skladaní bijekcií) ľahko vyplýva z prvých dvoch častí. □

Ak chcete lepšie porozumieť predchádzajúcemu dôkazu (alebo sa pokúšate dokázať si toto tvrdenie samostatne), opäť môže byť užitočné pomôcť si kreslením šípok.

Definícia 2.2.14. Zobrazenie $id_X : X \to X$ také, že $id_X(x) = x$ pre každé $x \in X$ sa nazýva *identické zobrazenie* (*identita*).

Všimnime si, že pre ľubovoľné zobrazenie $f : X \to Y$ platí

$$f \circ id_X = f \qquad \text{a} \qquad id_Y \circ f = f.$$

Definícia 2.2.15. Nech $f : X \to Y$ a $g : Y \to X$ sú zobrazenia. Ak platí

$$g \circ f = id_X$$
$$f \circ g = id_Y$$

tak hovoríme, že zobrazenie g je *inverzné zobrazenie k f*. Inverzné zobrazenie k zobrazeniu f označujeme f^{-1}.

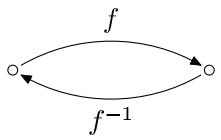
Ak k nejakému zobrazeniu existuje inverzné zobrazenie, tak takéto zobrazenie je jediné (úloha 2.2.5). Vďaka tejto jednoznačnosti má zmysel zaviesť označenie pre inverzné zobrazenie – znak f^{-1} skutočne označuje len jediné konkrétne zobrazenie.

Vzťahy definujúce inverzné zobrazenie môžeme ekvivalentne prepísať aj tak, že pre každé $x \in X$ a pre každé $y \in Y$ platí

$$f^{-1}(f(x)) = x,$$
$$f(f^{-1}(y)) = y.$$

V zmysle našej intuície o zobrazení ako systéme šípok vychádzajúcich z každého prvku x, zodpovedá inverzné zobrazenie šípkam idúcim opačným smerom (obr. 2.6).

Aby takéto zobrazenie existovalo, do každého prvku y musí ísť aspoň jedna šípka (aby sme sa mali kam vrátiť) a do žiadneho prvku y nesmie ísť viac ako jedna šípka (aby sme dostali zobrazenie, t.j. len jediný prvok, do ktorého sa vraciame.) Tento fakt je sformulovaný v nasledujúcom tvrdení.



Obr. 2.6: Inverzné zobrazenie

Tvrdenie 2.2.16. *Inverzné zobrazenie k f existuje práve vtedy, keď f je bijekcia.*

Dôkaz. $\boxed{\Rightarrow}$ Predpokladajme, že existuje inverzné zobrazenie k zobrazeniu $f\colon X \to Y$, označme ho g. Z definície inverzného zobrazenia dostaneme

$$f(x_1) = f(x_2) \;\Rightarrow\; g(f(x_1)) = g(f(x_2)) \;\Rightarrow\; g \circ f(x_1) = g \circ f(x_2) \;\Rightarrow\; x_1 = x_2,$$

čo znamená, že f je prosté.

Ešte potrebujeme ukázať, že ku každému $y \in Y$ existuje $x_0 \in X$ s vlastnosťou $f(x_0) = y$. Stačí zvoliť $x_0 = g(y)$, pretože (opäť podľa definície inverzného zobrazenia)

$$f(x_0) = f(g(y)) = y.$$

$\boxed{\Leftarrow}$ Predpokladajme, že $f\colon X \to Y$ je bijekcia, chceme dokázať, že existuje inverzné zobrazenie $g\colon Y \to X$. Majme ľubovoľné $y \in Y$. Pretože f je surjekcia, existuje aspoň jedno $x \in X$ také, že $f(x) = y$. Pretože f je injekcia, existuje najviac jedno také x – celkove teda dostávame, že existuje práve jedno x s touto vlastnosťou. Zobrazenie g teda môžeme definovať tak, že $g(y)$ je práve ten prvok x, pre ktorý platí $f(x) = y$. Inak povedané, g je určené podmienkou

$$g(y) = x \;\Leftrightarrow\; f(x) = y.$$

Ak zobrazenie g definujeme takýmto spôsobom dostaneme

$$g(f(x)) = x$$

(lebo $g(f(x))$ je práve ten prvok, ktorý sa zobrazí na $f(x)$, čo je presne prvok x) a

$$f(g(y)) = y$$

(lebo $g(y)$ sa, podľa definície zobrazenia g, zobrazí na y.) □

Tvrdenie 2.2.17. *Nech $f\colon X \to Y$ a $g\colon Y \to Z$ sú bijekcie. Potom*

$$(f^{-1})^{-1} = f$$
$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

Dôkaz. Použitím definície inverzného zobrazenia pre zobrazenie f máme $f^{-1} \circ f = id_X$ a $f \circ f^{-1} = id_Y$. To ale presne hovorí, že f je inverzné zobrazenie k f^{-1}.

Podobne vidíme, že

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ id_Y \circ f = f^{-1} \circ f = id_X.$$

Analogickým spôsobom overíme, že $(g \circ f) \circ (f^{-1} \circ g^{-1})$. Tým sme vlastne overili obe podmienky z definície inverzného zobrazenie k $g \circ f$. □

Dôsledok 2.2.18. *Ak f je bijekcia, tak aj f^{-1} je bijekcia.*

2.2.3 Vzor a obraz množiny*

Definícia 2.2.19. Nech $f\colon X \to Y$ je zobrazenie, $A \subseteq X$, $B \subseteq Y$. Množinu

$$f[A] = \{f(a); a \in A\}$$

nazývame *obrazom* množiny A v zobrazení f. Množinu

$$f^{-1}(B) = \{x \in X; f(x) \in B\}$$

nazývame *vzorom* množiny B v zobrazení f.

Cvičenia

Úloha 2.2.1. Dokážte: Ak $g \circ f$ je surjekcia, tak aj g je surjekcia. Platí aj opačná implikácia? Musí byť f surjekcia?

Úloha 2.2.2. Dokážte: Ak $g \circ f$ je injekcia, tak f je injekcia.

Úloha 2.2.3. Dokážte: Ak $g \circ f$ je bijekcia, tak f je injekcia a g je surjekcia.

Úloha 2.2.4. Nech $f\colon X \to Y$ je zobrazenie a $X \neq \emptyset$ (t.j. X je neprázdna množina). Potom:
a) f je injekcia práve vtedy, keď existuje g také, že $g \circ f = id_X$.
b) f je surjekcia práve vtedy, keď existuje g také, že $f \circ g = id_Y$.
c) K zobrazeniu f existuje inverzné zobrazenie práve vtedy, keď f je bijekcia. (Tým sme znovu dokázali tvrdenie 2.2.16.)

Úloha 2.2.5. Nech $f\colon X \to Y$, $g\colon Y \to X$, $h\colon Y \to X$ sú zobrazenia. Ak g aj h sú inverzné zobrazenia k f, tak $g = h$.

Úloha 2.2.6. Nech M, N sú konečné množiny, M má m prvkov a N má n prvkov. Koľko existuje zobrazení množiny M do množiny N?

Úloha 2.2.7. Nech A je konečná množina a $f\colon A \to A$ je zobrazenie. Dokážte:
a) Ak f je injekcia, tak f je bijekcia.
b) Ak f je surjekcia, tak f je bijekcia.

Úloha 2.2.8. Dokážte: Zobrazenie $f\colon X \to Y$ je surjekcia práve vtedy, keď pre každú množinu Z a všetky zobrazenia $g, h\colon Y \to Z$ platí: Ak $g \circ f = h \circ f$, tak $g = h$.

Úloha 2.2.9. Dokážte: Zobrazenie $f\colon X \to Y$ je injekcia práve vtedy, keď pre každú množinu Z a všetky zobrazenia $g, h\colon Z \to X$ platí: Ak $f \circ g = f \circ h$, tak $g = h$.

Úloha 2.2.10$^+$. Dokážte: $f[A \cup B] = f[A] \cup f[B]$, $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.

Úloha 2.2.11$^+$. Ktoré z nasledujúcich tvrdení platia a ktoré neplatia? Zdôvodnite.
a) $f[A \cap B] = f[A] \cap f[B]$
b) $f[A \cap B] \subset f[A] \cap f[B]$
c) $f[A \cap B] \supset f[A] \cap f[B]$
d) $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$
e) $f^{-1}(A \cap B) \subset f^{-1}(A) \cap f^{-1}(B)$
f) $f^{-1}(A \cap B) \supset f^{-1}(A) \cap f^{-1}(B)$
g) $f[f^{-1}(B)] = B$
h) $f[f^{-1}(B)] \subset B$
i) $f^{-1}(f[A]) = A$
j) $f^{-1}(f[A]) \subset A$
k) $g \circ f[A] = g[f[A]]$

Úloha 2.2.12$^+$. Ak X je množina, tak $P(X)$ budeme označovať množinu všetkých jej podmnožín. Nech $f\colon X \to Y$ je zobrazenie a $g\colon P(X) \to P(Y)$ je zobrazenie definované tak, že $g(A) = f[A]$ pre ľubovoľnú podmnožinu $A \subseteq X$. Dokážte, že f je prosté práve vtedy, keď g je prosté.

2.3 Permutácie

V tejto podkapitole sa budeme zaoberať istým typom zobrazení, ktorý budeme v ďalších častiach využívať.

Definícia 2.3.1. Ak M je konečná množina, tak bijekciu $\varphi\colon M \to M$ budeme nazývať *permutáciou* množiny M.

My sa budeme zaoberať (pre zjednodušenie) len permutáciami množiny $\{1, 2 \ldots, n\}$, kde n je prirodzené číslo. (Každú konečnú množinu M vieme očíslovať číslami od 1 po n, kde n je počet prvkov množiny M.)

Zo strednej školy (z kombinatoriky) poznáte termín permutácia v zmysle preusporiadanie nejakej (konečnej) množiny. Je to v istom zmysle, to isté, čo definujeme tu – zobrazenie z množiny $\{1, 2, \ldots, n\}$ vlastne určuje nejaké poradie prvkov tejto množiny, čiže skutočne zodpovedá nejakému jej preusporiadaniu.

Nie je ťažké si uvedomiť, že počet permutácií množiny $\{1, \ldots, n\}$ je práve $n! = n.(n-1).(n-2)\ldots 2.1$. Máme totiž práve n možností, ako môžeme vybrať prvok $\varphi(1)$. Pri výbere prvku $\varphi(2)$ však už nemôžeme použiť ten istý prvok ako v prvom prípade (inak by zobrazenie φ nebolo injektívne), teda nám zostáva práve $(n-1)$ možností. Pre výber obrazu ďalšieho prvku je už iba $(n-2)$ možností, atď.

Permutáciu $\varphi\colon \{1, \ldots, n\} \to \{1, \ldots, n\}$ budeme zapisovať v tvare

$$\left(\begin{smallmatrix} 1 & 2 & \ldots & n \\ \varphi(1) & \varphi(2) & \ldots & \varphi(n) \end{smallmatrix}\right),$$

čiže pod každé číslo $1, 2, \ldots, n$ zapíšeme jeho obraz v permutácii φ.

Napríklad permutáciu na množine $\{1, 2, 3\}$, pre ktorú $\varphi(1) = 1$, $\varphi(2) = 3$ a $\varphi(3) = 2$ zapíšeme ako $\left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right)$, identickú permutáciu zapíšeme ako $\left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix}\right)$. (Budeme ju tiež označovať id, keďže ide o identické zobrazenie.)

Niekedy sa kvôli stručnosti používa označenie, kde sa vynechá prvý riadok obsahujúci čísla $1, 2, \ldots, n$. (Napríklad [Bó] používa iba jednoriadkové označenie. Väčšina kníh s touto tématikou používa jednoriadkový aj dvojriadkový zápis – podľa toho, ktorý sa práve hodí.) My sa budeme pridržiavať označenia, ktoré sme zaviedli, z toho dôvodu, že spomínané zjednodušenie by sa mohlo pliesť s označením pre cykly, o ktorých sa viac dozviete na predmete algebra v 3. ročníku alebo v časti 2.3.1.

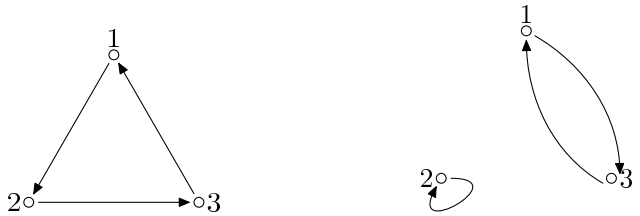
Ďalšou výhodou dvojriadkového zápisu je, že ho môžeme použiť pre ľubovoľnú množinu – jednoriadkový zápis môžeme použiť ak máme na množine M nejaké prirodzené usporiadanie, vďaka ktorému vieme prvý riadok jednoznačne doplniť.

Z tvrdenia 2.2.13 vyplýva, že zložením dvoch permutácií opäť dostaneme permutáciu. Pri skladaní permutácií (a takisto pri skladaní zobrazení) budeme často vynechávať znak $\circ$, teda píšeme $\varphi\tau$ namiesto $\varphi \circ \tau$.

Ak napríklad $\varphi = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)$, $\tau = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right)$, tak $\varphi\tau = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right)$, $\tau\varphi = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right)$. Vidíme, že skladanie permutácií vo všeobecnosti nie je komutatívne.

Skladanie permutácií $\varphi\tau$ si môžeme predstaviť tak, že ľavú permutáciu napíšeme pod pravú a preusporiadame stĺpce dolnej permutácie tak, aby jednotlivé čísla súhlasili.

$$\begin{matrix} \tau = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right) \\ \varphi = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right) \end{matrix} \quad \longrightarrow \quad \begin{matrix} \tau = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right) \\ \varphi = \left(\begin{smallmatrix} 3 & 2 & 1 \\ 1 & 3 & 2 \end{smallmatrix}\right) \end{matrix} \quad \longrightarrow \quad \varphi\tau = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right)$$



Obr. 2.7: Permutácie τ a φ

Permutácie φ a τ sú znázornené na obrázku 2.7.

To isté môžeme inak vyjadriť tak, že čísla, ktoré sú v dolnom riadku v zápise ľavej permutácie, napíšeme do dolného riadku výslednej permutácie v takom poradí, aké udáva pravá permutácia (tretie, druhé, prvé). Čiže číslo 3, ktoré je na prvom mieste v permutácii τ udáva, že na prvom mieste vo $\varphi\tau$ permutácii bude tretie číslo z φ, čiže 1, 2 na druhom mieste v τ určuje, že na druhom mieste bude to, čo je na druhom mieste vo φ, t.j. 2 a posledná jednotka určuje, že na treťom mieste má byť 2.

Pozor!!! V [KGGS] je skladanie zobrazení (a teda aj skladanie permutácií) definované v opačnom poradí, ako sme ho definovali my.

Inverzné zobrazenie k permutácii je permutácia. Vypočítať ju môžeme jednoducho takým spôsobom, že vymeníme riadky a preusporiadame stĺpce do požadovaného tvaru. Z $\varphi = \left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right)$ tak dostaneme

$$\varphi^{-1} = \left(\begin{smallmatrix}2&3&1\\1&2&3\end{smallmatrix}\right) = \left(\begin{smallmatrix}1&2&3\\3&1&2\end{smallmatrix}\right).$$

Ak φ je permutácia, tak namiesto $\varphi \circ \varphi$ budeme písať φ^2 a podobne namiesto $\underbrace{\varphi \circ \ldots \circ \varphi}_{n\text{-krát}}$ používame φ^n.

Matematicky správnejšie by bolo povedať, že φ^n definujeme matematickou indukciou:
1° $\varphi^0 = id$, $\varphi^1 = \varphi$
2° $\varphi^{n+1} = \varphi \circ \varphi^n$.

Príklad 2.3.2. Uvažujme permutáciu $\varphi = \left(\begin{smallmatrix}1&2&3&4\\1&3&4&2\end{smallmatrix}\right)$ množiny $\{1, 2, 3, 4\}$. Pokúsme sa vypočítať permutáciu φ^{50}.

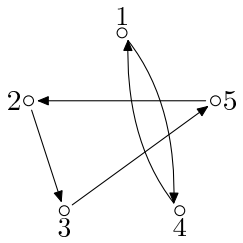
Ľahko zistíme, že

$$\varphi^1 = \varphi = \left(\begin{smallmatrix}1&2&3&4\\1&3&4&2\end{smallmatrix}\right)$$
$$\varphi^2 = \varphi \circ \varphi = \left(\begin{smallmatrix}1&2&3&4\\1&4&2&3\end{smallmatrix}\right)$$
$$\varphi^3 = \varphi \circ \varphi^2 = \left(\begin{smallmatrix}1&2&3&4\\1&2&3&4\end{smallmatrix}\right)$$

Ďalšími výpočtami by sme zistili, že sa stále budú opakovať tieto 3 permutácie. (Môžeme to dokázať matematickou indukciou.) Z toho dostaneme $\varphi^{50} = \varphi^{3.16+2} = \varphi^2 = \left(\begin{smallmatrix}1&2&3&4\\1&4&2&3\end{smallmatrix}\right)$. (Vlastne sme využili vzťah $\varphi^{m.n} = (\varphi^m)^n$, ktorého dôkaz sme ponechali ako cvičenie v úlohe 2.3.4.)

2.3.1 Rozklad na súčin disjunktných cyklov*

Uvedieme jednu nepovinnú podkapitolu – nebude odprednášaná na tejto prednáške. Môže byť pre Vás užitočná z toho dôvodu, že sa o týchto veciach budete učiť neskôr – môžete sa k nej vrátiť vtedy – ale aj preto, že ak si ju pozriete, môžeme Vám pomôcť pri výpočtoch s permutáciami.



Obr. 2.8: Príklad permutácie 5-prvkovej množiny. Vidíme, že z každého prvku vychádza aj do každého prvku vchádza práve jedna šípka.

Ak sa pozrieme na permutáciu na obrázku 2.8 vidíme, že na tomto obrázku sa po jednotlivých šípkach z prvku 1 dostaneme do prvku 4 a potom naspäť znovu do prvku 1. Podobne z prvku 2 sa dostaneme do 3 a 5 a potom opäť do 2.

Toto musí platiť pre ľubovoľnú permutáciu. Ak začneme s ľubovoľným prvkom, opakovaným aplikovaním tej istej permutácie po konečnom počte krokov dostaneme znovu ten istý prvok. Dôvodom je, že máme len konečný počet prvkov – teda po istom čase sa niektorý prvok zopakuje. Ak by to bol iný prvok, ako ten z ktorého sme začali, dané zobrazenie by nebola bijekcia. (Podrobnejšie tento argument vysvetlíme v dôkaze tvrdenia 2.3.8.) Vďaka tomu môžeme každú permutáciu rozdeliť na cykly.

Celá táto časť je venovaná spôsobu ako môžeme práve uvedený jednoduchý fakt formálne zapísať a dokázať. Tiež si povieme, prečo je tento poznatok užitočný.

Najprv potrebujeme zaviesť pojem cyklu.

Definícia 2.3.3. Permutáciu φ konečnej množiny M nazveme *cyklus,* ak existujú prvky $a_1, a_2, \ldots, a_k$ také, že

$$\begin{cases} \varphi(a_i) = a_{i+1} \text{ pre } i = 1, 2, \ldots, k-1, \\ \varphi(a_k) = a_1, \\ \varphi(a) = a \text{ pre ostatné prvky } a \neq a_i. \end{cases}$$

Pre cyklus tohoto tvaru budeme používať zápis $(a_1 a_2 \ldots a_k)$.

V definícii cyklu pripúšťame aj nulový počet prvkov. *Prázdny cyklus,* ktorý označujeme $()$, sa rovná identickej permutácii.

Všimnime si, že zápis pomocou cyklov môžeme použiť pre ľubovoľnú množinu. Tento zápis však neidentifikuje množinu, ktorej permutáciu robíme – tá musí byť zadaná zvlášť.

Príklad 2.3.4. Uvažujme permutácie množiny $\{1, 2, 3, 4, 5\}$

Zápis $\varphi = (14)$ označuje permutáciu s vlastnosťou $\varphi(1) = 4$ a $\varphi(4) = 1$, ktorá prvky 2, 3 a 5 nemení (teda $\varphi(2) = 2$, $\varphi(3) = 3$, $\varphi(5) = 5$).

Zápis $\tau = (235)$ znamená permutáciu určenú predpisom $\tau(1) = 1$, $\tau(2) = 3$, $\tau(3) = 5$, $\tau(4) = 4$, $\tau(5) = 5$.

Všimnime si, že ten istý cyklus môže byť zapísaný viacerými spôsobmi: $\tau = (235) = (352) = (523)$.

Príklad 2.3.5. Vieme, že inverzné zobrazenie k permutácii je tiež permutácia. Ak máme cyklus $\varphi = (a_1 a_2 \ldots a_n)$, tak inverzná permutácia je tiež cyklus $\varphi^{-1} = (a_n a_{n-1} \ldots a_1)$. Zodpovedá to tomu, že poprechádzame po tých istých šípkach tvoriacich cyklus, ale v opačnom poradí.

Pre cykly z predchádzajúceho príkladu máme $\varphi^{-1} = (14)$ a $\tau^{-1} = (253)$.

Definícia 2.3.6. Dve permutácie φ a τ tej istej množiny M nazveme *disjunktné,* ak pre každý prvok $a \in M$ platí $\varphi(a) = a$ alebo $\tau(a) = a$. (Teda každý prvok zostáva nezmenený pri aspoň jednej z týchto dvoch permutácií.)

Špeciálne, dva cykly $(a_1 a_2 \dots a_k)$ a $(b_1 b_2 \dots b_l)$ sú disjunktné, ak platí rovnosť $\{a_1, a_2, \dots, a_k\} \cap \{b_1, b_2, \dots, b_l\} = \emptyset$.

Nasledujúca lema hovorí, že poradie disjunktných permutácií môžeme pri skladaní vymeniť – disjunktné permutácie komutujú.

Lema 2.3.7. *Ak φ a τ sú disjunktné permutácie, tak*

$$\varphi \circ \tau = \tau \circ \varphi.$$

Dôkaz. Stačí priamym výpočtom overiť, že permutácia na ľavej aj pravej strane rovnosti nadobúda rovnaké hodnoty.

□

Tvrdenie 2.3.8. *Každú permutáciu možno zapísať ako zloženie disjunktných cyklov. Tento zápis je jednoznačný až na poradie cyklov (a vynechanie prázdneho cyklu). Nazývame ho* rozklad permutácie na súčin disjunktných cyklov.

Dôkaz. Uvažujme ľubovoľnú permutáciu φ množiny M.

Existenciu rozkladu permutácie φ na súčin disjunktných dokážeme indukciou vzhľadom na počet prvkov množiny M. Pre jednoprvkovú množinu máme jedinú možnú permutáciu id_M, ktorá sa rovná prázdnemu cyklu.

Predpokladajme teraz, že M má n prvkov a pre ľubovoľnú množinu s menej ako n prvkami tvrdenie platí. Zoberme teraz ľubovoľný prvok $a \in M$. Položme $a_1 = a$, $a_{i+1} = \varphi(a^i)$ pre všetky $i = 1, 2, \dots$. Nech k je najmenšie číslo také, že $k \geq 1$ a $a_{k+1} = a$. Ukážeme najprv, že také číslo musí existovať.

Pretože množina M je konečná, musia sa niektoré prvky v postupnosti (a_k) opakovať, t.j. existujú nejaké čísla s vlastnosťou $a_s = a_t$ a $s \neq t$. Tvrdíme, že ak s je najmenšie množné takéto číslo, tak $s = 1$. Skutočne, v opačnom prípade máme $\varphi(a_{s-1}) = \varphi(a_{t-1})$ a z injektívnosti zobrazenia φ dostaneme $a_{s-1} = a_{t-1}$.

Zistili sme, že existuje aspoň jedno číslo s horeuvedenými vlastnosťami, preto môžeme definovať k ako najmenšie číslo, ktoré má tieto vlastnosti. Pomocou neho definujeme cyklus

$$\tau = (a_1 a_2 \dots a_k).$$

Položme ďalej $\psi = \tau^{-1}\varphi$. Ukážeme, že permutácie ψ a τ sú disjunktné a že $\psi(a) = a$.

Skutočne, pre ľubovoľný z prvkov $a_1, a_2, \dots, a_{k-1}$ platí $\varphi(a_i) = a_{i+1}$ a $\tau^{-1}(a_{i+1}) = a_i$, teda $\psi(a_i) = \tau^{-1}(\varphi(a_i)) = a_i$. Podobne môžeme overiť, že $\psi(a_k) inv \tau(\varphi(a_k)) = \tau^{-1}(a_1) = a_k$. Vidíme, že permutácia ψ nemení žiadny z prvkov, ktoré mení cyklus τ teda tieto permutácie sú disjunktné. Špeciálne, ψ nemení prvok $a_1 = a$.

Teraz si stačí uvedomiť, že ψ (resp. zúženie tohoto zobrazenia) môžeme chápať ako permutáciu množiny $M \setminus \{a_1 \dots a_k\}$, ktorá má menej prvkov ako množina M. Podľa indukčného predpokladu teda existuje rozklad $\psi = \tau_1 \tau_2 \dots \tau_l$ tejto permutácie na disjunktné cykly. Potom

$$\varphi = \tau(\tau^{-1}\varphi) = \tau\psi = \tau\tau_1 \dots \tau_l$$

je rozklad permutácie φ na disjunktné cykly.

Jednoznačnosť. Predpokladajme, že máme 2 rozklady

$$\varphi_1 \dots \varphi_s = \psi_1 \dots \psi_t$$

tej istej permutácie na disjunktné cykly, pričom v rozkladoch sa nevyskytuje prázdny cyklus. Postupujme indukciou vzhľadom na s.

Ak $s = 0$, teda na ľavej strane rovnosti je identita, musí byť aj počet disjunktných cyklov na pravej strane nulový. V opačnom prípade by sme mali na pravej strane aspoň jeden neprázdny cyklus, teda permutácia na pravej strane by menila aspoň jeden prvok, čiže permutácia na pravej strane by nebola identita.

Predpokladajme teraz, že $s > 0$, čiže daná permutácia nie je identita. Nech a je nejaký prvok, ktorý táto permutácia mení. Tento prvok sa musí vyskytovať v aspoň jednom z cyklov, súčasne z disjunktnosti vyplýva, že sa nemôže vyskytovať vo viacerých cyklov. Teda prvok a sa vyskytuje práve v jednom z cyklov vystupujúcich na ľavej strane rovnosti, podobne v práve jednom z cyklov na pravej strane. Bez ujmy na všeobecnosti (cykly môžeme poprehadzovať) predpokladajme, že sú to cykly φ_1 a τ_1. Potom dostaneme $\varphi_1(a) = \varphi(a) = \tau_1(a)$, podobne $\varphi_1^2(a) = \varphi^2(a) = \tau_1^2(a)$ atď. Čiže všetky prvky vyskytujúce sa v cykle φ_1 sa zobrazia rovnako aj cyklom τ_1 a obrátene. Platí teda $\varphi_1 = \tau_1$. Z toho dostaneme rovnosť $\varphi_2 \dots \varphi_s = \psi_2 \dots \psi_t$. Pre tieto cykly už môžeme použiť indukčný predpoklad. □

Príklad 2.3.9. Pre permutáciu $\varphi = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{smallmatrix}\right)$ (obrázok 2.8) dostaneme rozklad $\varphi = (14)(235)$.
Z toho vieme hneď zistiť aj $\varphi^{-1} = (14)(253)$.

Rozklad na súčin disjunktných cyklov môže byť užitočný pri výpočte rádu permutácie.

Definícia 2.3.10. Ak φ je permutácia konečnej množiny M, tak *rád permutácie* φ je najmenšie prirozdené číslo $n \geq 1$ také, že

$$\varphi^n = id_M.$$

Napríklad v príklade 2.3.2 sme zistili, že rád permutácie $\varphi = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{smallmatrix}\right)$ je 3.

Lema 2.3.11. *Rád cyklu je rovný jeho dĺžke, t.j. ak $\varphi = (a_1 \dots a_n)$, tak rád φ je rovný n.*

Dôkaz. Pre $k = 2, \dots, n-1$ je $\varphi^k(a_1) = a_{k-1} \neq a_1$. Až pre $k = n$ prvýkrát dostaneme $\varphi^k(a_1) = a_1$. Úplne rovnaké zdôvodnenie prejde aj pre ostatné prvky cyklu, čiže máme $\varphi^n = id$ a navyše n je najmenšie číslo z množiny $\{1, 2, 3, \dots\}$ s touto vlastnosťou. □

Veta 2.3.12. *Rád permutácie je najmenší spoločný násobok dĺžok disjunktných cyklov, ktoré vystupujú v jej rozklade.*

Dôkaz. Nech $\varphi = \tau_1 \dots \tau_m$ je rozklad permutácie na φ na disjunktné cykly. Pretože disjunktné cykly komutujú, mocniny permutácie φ môžeme vyjadriť ako

$$\varphi^n = \tau_1^n \dots \tau_m^n.$$

Pritom permutácie $\tau_1^n, \dots, \tau_m^n$ sú opäť disjunktné. Z toho vyplýva, že aby sme dostali identické zobrazenie, musí pre každé $i = 1, 2, \dots, m$ platiť $\tau_i^n = id_M$. To nastane práve vtedy, keď n je násobkom rádu τ_i (pre všetky i). Teda najmenšie možné n s takouto vlastnosťou je najmenší spoločný násobok rádov jednotlivých disjunktných cyklov. Podľa lemy 2.3.11 sú to presne dĺžky jednotlivých cyklov. □

Cvičenia

Úloha 2.3.1. Uvažujme o permutáciach na množine $M = \{1, 2, 3, 4, 5\}$. Aká je inverzná permutácia ku: $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{smallmatrix}\right)$? Urobte aj skúšku správnosti, t.j. po vypočítaní φ^{-1} overte, či $\varphi^{-1}\varphi = \varphi\varphi^{-1} = id$. [$\left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 3 & 5 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{smallmatrix}\right)$]

Úloha 2.3.2. $M = \{1, 2, 3, 4\}$. Vypočítajte: $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{smallmatrix}\right)$. Určte inverznú permutáciu k výsledku.

Úloha 2.3.3. Čomu sa rovná φ^{120}, ak $\varphi = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{smallmatrix}\right)$?

Úloha 2.3.4. Matematickou indukciou dokážte, že $\varphi^{n+m} = \varphi^n \circ \varphi^m$, $\varphi^{nm} = (\varphi^n)^m$.

Úloha 2.3.5$^+$. Vyslovte a dokážte zovšeobecnenie lemy 2.3.7 pre ľubovoľný počet permutácií.

Úloha 2.3.6$^+$. Pre dané permutácie určte rád, a rozklad na disjunktné cykly:
$\varphi = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{smallmatrix}\right)$, $\tau = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{smallmatrix}\right)$, $\psi = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{smallmatrix}\right)$.
Ďalej vypočítajte permutácie $\varphi\tau\psi$, φ^{-1}, τ^{-1}, ψ^{-1}.

Kapitola 3

Grupy a polia

Naším cieľom je dostať sa k definícii vektorového priestoru a lineárneho zobrazenia. Ich dôležitosť je v tom, že sú vhodným aparátom na popis lineárnych javov.

Predtým nás ale čaká ešte veľmi dlhá cesta, na ktorej sa však naučíme veľmi veľa užitočných vecí. Na definíciu vektorových priestorov použijeme pojem poľa. Na definíciu poľa použijeme pojem grupy. A navyše, predtým než sa dostaneme k definícii grupy, potrebujeme uviesť niektoré základné poznatky o binárnych operáciach.

Táto dlhá cesta k definícii vektorového priestoru je cenou za to, že chceme vektorové priestory definovať v čo najväčšej obecnosti – budeme pracovať s vektorovými priestormi nad ľubovoľným poľom. Keby sme sa rozhodli pracovať iba s vektorovými priestormi nad poľom reálnych čísel, mohli by sme si túto námahu ušetriť – len by sme stručne zopakovali vlastnosti reálnych čísel a hneď by sme zadefinovali vektorový priestor. (V niektorých učebniciach sa takto aj naozaj postupuje.)

Výhoda tohoto postupu je v tom, že dostaneme všeobecnejšie výsledky. Ďalší, vôbec nie zanedbateľný, prínos je, že sa naučíte mnohé užitočné veci a zvyknete si na axiomatický prístup k definovaniu nových pojmov a dokazovaniu ich vlastností.

3.1 Binárne operácie

Hlavným cieľom tejto kapitoly je zadefinovať grupy a polia. Hoci najčastejšie budeme pracovať s reálnymi a komplexnými číslami, je užitočné uvedomiť si, že tvrdenia, ktoré dokážeme budú platiť pre ľubovoľné pole. Aby sme však vôbec mohli zaviesť pojmy grupa a pole, potrebujeme najprv vedieť, čo sú to binárne operácie.

Definícia 3.1.1. *Binárna operácia* $*$ na množine A je zobrazenie z množiny $A \times A$ do A.

Namiesto $*(a, b)$ budeme používať označenie $a * b$, tento zápis budeme niekedy skracovať ako ab.

Opäť, podobne ako pri zobrazeniach, môžeme binárnu operáciu chápať ako predpis, ktorý však v tomto prípade priradí dvom prvkom z množiny A priradí nejaký prvok z tej istej množiny. Takisto zápis $a * b$ resp. ab zodpovedá tomu, na čo sme zvyknutí pri binárnych operáciach, s ktorými sme sa stretli doteraz, ako je sčitovanie a násobenie.

Tiež si všimnime, že v definícii vystupujú *usporiadané* dvojice (prvky množiny $X \times Y$), teda výsledok operácie $a * b$ a $b * a$ nemusí predstavovať ten istý prvok.

Príklad 3.1.2. Operácie $+$ a $\cdot$ sú binárne operácie na množine $\mathbb{R}$ reálnych čísel.

Operácia $\cdot$ je binárna operácia na množine $\mathbb{R} \setminus \{0\}$, pretože nulu nemôžeme dostať ako súčin dvoch nenulových čísel. Naopak, $+$ nie je binárna operácia na $\mathbb{R} \setminus \{0\}$, lebo $-1+1=0$, teda dvom číslam z množiny $\mathbb{R} \setminus \{0\}$ operácia $+$ priradí číslo, ktoré do tejto množiny nepatrí.

Operácie $+$ aj $\cdot$ sú binárne operácie na množine $\mathbb{R}^+$. Na množine $\mathbb{R}^-$ predstavuje $+$ binárnu operáciu, $\cdot$ však už nie je binárna operácia na tejto množine.

Príklad 3.1.3. Ako ďalší príklad definujme operáciu $\oplus$ na množine $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ takto: $a \oplus b$ takto: $a \oplus b = (a + b) \bmod 5$. Operácia mod tu predstavuje zvyšok (v tomto prípade po delení piatimi). Napríklad $1 \oplus 2 = 3$, $2 \oplus 3 = 0$, $3 \oplus 3 = 1$ (čísla najprv sčítame a potom urobíme zvyšok po delení 5).

Podobne môžeme definovať binárnu operáciu $\odot$ ako $a \odot b = (a.b) \bmod 5$.

Binárnu operáciu na konečnej množine môžeme tiež určiť tabuľkou: (do riadku a a stĺpca b píšeme výsledok operácie $a \oplus b$.)

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\odot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Podobná operácia by sa dala definovať aj pre ľubovoľné prirodzené číslo $n \geq 2$. S množinami $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ a binárnymi operáciami $\oplus$ a $\odot$ (čiže sčitovanie a násobenie modulo n) sa v priebehu tejto prednášky stretnete ešte dosť často.

Príklad 3.1.4. Binárna operácia nemusí byť vždy daná predpisom – ak ide o konečnú množinu môže byť zadaná tabuľkou. (Dalo by sa povedať, že tabuľka binárnej operácie vlastne do istej miery zodpovedá zobrazeniu definovanému rôznymi predpismi pre rôzne prípady. Tu však sú jednotlivé časti definičného oboru len jednoprvkové.)

Napríklad môžeme definovať takúto binárnu operáciu $\triangle$ na množine $\{0, 1, 2\}$:

$\triangle$	0	1	2
0	0	1	2
1	0	1	2
2	0	2	1

Teraz sa budeme zaoberať niektorými základnými vlastnosťami binárnych operácií. Aby sme si ich lepšie ozrejmili, pre každú z nich overíme, či túto vlastnosť majú binárne operácia $+$ a $\cdot$ na množine $\mathbb{R}$, $\oplus$ na množine $\mathbb{Z}_5$ a operácia $\triangle$ z príkladu 3.1.4.

Vlastnosti, ktoré budeme definovať budú komutatívnosť, asociatívnosť, existencia neutrálneho prvku a existencia inverzného prvku. Pri overovaní, či uvedené binárne operácie majú túto vlastnosť, postupne vyplníme nasledujúcu tabuľku

	NP	K	A	IP
$(\mathbb{R}, +)$				
$(\mathbb{R}, \cdot)$				
$(\mathbb{Z}_5, \oplus)$				
$(\mathbb{Z}_3, \triangle)$				

Definícia 3.1.5. Nech $*$ je binárna operácia na množine M. Hovoríme, že $e \in M$ je *neutrálny prvok* operácie $*$, ak pre všetky $m \in M$ platí

$$e * m = m * e = m.$$

Zo strednej školy vieme, že $0 + m = m + 0 = m$, $1.m = m.1 = m$. To znamená, že 0 je neutrálny prvok pre operáciu $+$ a 1 je neutrálny prvok pre operáciu $\cdot$ na množine $\mathbb{R}$. Pretože rovnosť $0 + m = m + 0 = m$ zostane v platnosti aj keď zo všetkých prvkov urobíme zvyšok po delení 5, 0 je aj neutrálnym prvkom operácie $\oplus$ na množine $\mathbb{Z}_5$.

Prv než sa pozrieme na operáciu $\triangle$, skúsme si ozrejmiť ako sa prejaví existencia neutrálneho prvku na tabuľke binárnej operácie. Rovnosť $e * m = m$ znamená, že v riadku e sa vyskytnú rovnakú prvky ako v hlavičke tabuľky. To isté, ale pre stĺpce, vyplýva z rovnosti $m * e = m$. Skutočne, môžeme si všimnúť v tabuľke operácie $\oplus$ na $\mathbb{Z}_5$, že v riadku 0 a v stĺpci 0 sa opakujú prvky 0,1,2,3,4. Ak sa v prípade operácie $\triangle$ pozrieme na riadky, možnými kandidátmi by boli prvky 0 a 1. Ani v jednom z týchto prípadov to však neplatí pre stĺpce. Teda táto operácia nemá neutrálny prvok.

	NP	K	A	IP
$(\mathbb{R}, +)$	0			
$(\mathbb{R}, \cdot)$	1			
$(\mathbb{Z}_5, \oplus)$	0			
$(\mathbb{Z}_3, \triangle)$	x			

Teraz si dokážeme, že binárna operácia nemôže mať viac ako jeden neutrálny prvok. Spôsob dôkazu je typický pre prípad, keď chceme dokázať, že nejaký objekt je danou vlastnosťou jednoznačne určený. Pri dôkaze tvrdení takéhoto typu sa veľmi často postupuje tak, že uvažujeme dva objekty, ktoré majú túto vlastnosť a snažíme sa dokázať, že sa rovnajú.

Tvrdenie 3.1.6. *Ak má binárna operácia $*$ na množine M neutrálny prvok, tak tento neutrálny prvok je jediný.*

Dôkaz. Nech e_1, e_2 sú neutrálne prvky operácie $*$. Potom

$$e_1 \overset{(1)}{=} e_1 * e_2 \overset{(2)}{=} e_2,$$

pričom rovnosť (1) platí vďaka tomu, že e_1 je neutrálny prvok a rovnosť (2) platí vďaka tomu, že e_2 je neutrálny prvok. □

Definícia 3.1.7. Binárna operácia $*$ na množine M je *komutatívna,* ak pre všetky $x, y \in M$ platí

$$x * y = y * x.$$

Komutatívnosť vlastne znamená, že môžeme dvojice prvkov vymieňať. Väčšina operácií, s ktorými budeme pracovať, je komutatívna.

Opäť operácia $+$ a $\cdot$ na $\mathbb{R}$ sú komutatívne. V prípade operácie $\oplus$ si stačí uvedomiť, že rovnosť $x + y = y + x$ sa zachová, aj keď urobíme zvyšok modulo 5, teda dostaneme

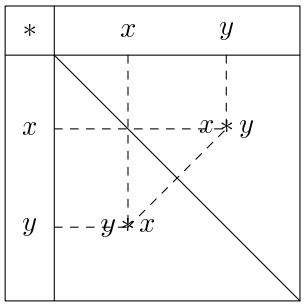
$$(x + y) \bmod 5 = (y + x) \bmod 5,$$
$$x \oplus y = y \oplus x.$$

Operácia $\triangle$ nie je komutatívna. Stačí si všimnúť, že

$$0 \triangle 2 \neq 2 \triangle 0,$$
$$2 \neq 0.$$

	NP	K	A	IP
$(\mathbb{R}, +)$	0	✓		
$(\mathbb{R}, \cdot)$	1	✓		
$(\mathbb{Z}_5, \oplus)$	0	✓		
$(\mathbb{Z}_3, \triangle)$	x	x		

Opäť je užitočné si všimnúť, ako sa komutatívnosť prejaví na tabuľke binárnej operácie. Ak je binárna operácia komutatívna, musí byť tabuľka symetrická podľa hlavnej diagonály (pretože prvky $x * y$ a $y * x$ sú na diagonálne symetrických pozíciach).



Obr. 3.1: Komutatívnosť a tabuľka binárnej operácie

Definícia 3.1.8. Binárna operácia $*$ na množine M je *asociatívna,* ak pre všetky $x, y, z \in M$ platí

$$(x * y) * z = x * (y * z).$$

Uzátvorkovanie v predchádzajúcej rovnosti znamená, ktorú operáciu robíme ako prvú. Formálne sa môžeme na asociatívny zákon pozerať ako na „prehadzovanie zátvoriek“.

$$\begin{array}{ccccccccc} (& x & * & y &) & * & z \\ & \searrow & & & & \searrow & \\ x & * & (& y & * & z &) \end{array}$$

Niekedy, v zložitejších výrazoch, aby sme znázornili, kde presne sme použili asociatívny zákon, podčiarkneme na <u>ľavej</u> strane rovnosti tie zátvorky, ktoré „prehadzujeme“.

$$\underline{(}x * y\underline{)} * z = x * (y * z).$$

Vlastnosť asociatívnosti vlastne hovorí to, že nezáleží na uzátvorkovaní, inak povedané zápis $x * y * z$ predstavuje ten istý prvok, bez ohľadu na to, aké uzátvorkovanie zvolíme. Preto zátvorky môžeme vynechávať.

Hoci vlastnosť asociatívnosti tak, ako sme ju definovali, hovorí len o tom, že zátvorky môžeme vynechať, ak ide o súčin 3 prvkov, nie je ťažké si uvedomiť, že to platí aj pre viac prvkov. K tomuto faktu sa ešte vrátime na konci tejto podkapitoly.

O operáciach $+$ a $\cdot$ vieme, že sú asociatívne. Pre operáciu $\oplus$ môžeme použiť podobnú úvahu ako pri komutatívnosti. Keď si všimneme, že

$$2\triangle(0\triangle 2) = 2\triangle 2 = 1,$$
$$(2\triangle 0)\triangle 2 = 0\triangle 2 = 2,$$

vidíme, že operácia $\triangle$ nie je asociatívna a môžeme doplniť ďalší stĺpec našej tabuľky.

	NP	K	A	IP
$(\mathbb{R}, +)$	0	✓	✓	
$(\mathbb{R}, \cdot)$	1	✓	✓	
$(\mathbb{Z}_5, \oplus)$	0	✓	✓	
$(\mathbb{Z}_3, \triangle)$	x	x	x	

Teraz nasleduje definícia inverzného prvku. O inverznom prvku má zmysel hovoriť iba vtedy, ak má binárna operácia neutrálny prvok.

Definícia 3.1.9. Nech $*$ je binárna operácia na množine M. Nech $a \in M$ a nech e je neutrálny prvok operácie $*$. Prvok $b \in M$ je *inverzný* k prvku a, ak platí

$$a * b = b * a = e.$$

Všimnite si, že v definícii sú obe rovnosti, $a*b = e$ aj $b*a = e$! (Samozrejme, ak je operácia $*$ komutatívna, stačilo by nám požadovať len jednu z nich. Preto aj v príkladoch, keď budeme overovať existenciu inverzného prvku nejakej binárnej operácie, o ktorej už budeme vedieť, že je komutatívna, uľahčíme si prácu tým, že budeme dokazovať len jednu z uvedených rovností, druhá z nej vyplynie automaticky. Ako sme už spomenuli, najčastejšie budeme pracovať s komutatívnymi binárnymi operáciami.)

Príklad 3.1.10. Pre operáciu $+$ platí

$$a + (-a) = 0 = (-a) + a,$$

teda ľubovoľný prvok $a \in \mathbb{R}$ má inverzný prvok a je to prvok $-a$. (Ako sme spomenuli pred chvíľou, pretože táto operácia je komutatívna, stačí vlastne overovať len jednu z uvedených rovností.)

Podobne pre komutatívnu operáciu $\cdot$ bude inverzným prvkom ku $a \neq 0$ prvok $\frac{1}{a}$, lebo

$$a \cdot \frac{1}{a} = 1.$$

Číslo 0 nemá v tejto operácii inverzný prvok, lebo $0.b = 0$ pre ľubovoľné $b \in \mathbb{R}$.

V prípade množiny $\mathbb{Z}_5$ a operácie $\oplus$ platí $0 \oplus 0 = 1 \oplus 4 = 2 \oplus 3 = 0$, teda ku každému prvku sme našli inverzný prvok. (Všimnime si, že inverzný prvok k a je práve zvyšok čísla $-a$ po delení 5. Vedeli by ste tento fakt zdôvodniť?)

Pre operáciu $\triangle$ nemá zmysel hovoriť o inverznom prvku, lebo táto operácia nemá ani neutrálny prvok. Teraz už teda môžeme konečne vyplniť celú našu tabuľku.

	NP	K	A	IP
$(\mathbb{R}, +)$	0	✓	✓	$-a$
$(\mathbb{R}, \cdot)$	1	✓	✓	$\frac{1}{a}$ pre $a \neq 0$
$(\mathbb{Z}_5, \oplus)$	0	✓	✓	✓
$(\mathbb{Z}_3, \triangle)$	x	x	x	x

Tvrdenie 3.1.11. *Nech $*$ je asociatívna operácia na množine M a $*$ má neutrálny prvok e. Ak existuje inverzný prvok k a, tak je jednoznačne určený.*

Dôkaz. Predpokladajme, že b_1 a b_2 sú inverzné prvky ku a. Postupnými úpravami nasledujúcej rovnosti (ktorá vyplýva z asociatívnosti) dostaneme

$$b_1 * (a * b_2) = (b_1 * a) * b_2$$
$$b_1 * e = e * b_2$$
$$b_1 = b_2$$

□

Pretože pre asociatívnu operáciu je inverzný prvok jednoznačne určený prvkom a, môžeme preň zaviesť označenie. Budeme ho označovať a^{-1}.

V tabuľke binárnej operácie vieme inverzný prvok nájsť tak, že v riadku a vyhľadáme stĺpec, kde sa vyskytuje neutrálny prvok. To isté urobíme v stĺpci a – nájdeme riadok, v ktorom je neutrálny prvok. Ak sa nájdený riadok a stĺpec zhodujú, tak sme našli inverzný prvok k a.

3.1.1 Zovšeobecnený asociatívny zákon*

Ako sme sľúbili, vrátime sa na chvíľu ešte k asociatívnemu zákonu. Pôjde nám o to, aby sme si uvedomili, že pre asociatívnu operáciu môžeme skutočne vynechávať zátvorky, aj keď vo výraze vystupuje viac prvkov ako 3.

Najprv si to ukážeme pre 4 prvky a potom podáme aj formálny dôkaz, že to platí pre ľubovoľný počet prvkov.

Na začiatok sa pokúste nájsť všetky možné uzátvorkovania výrazu $a \circ b \circ c \circ d$. V nasledujúcej úlohe si môžete overiť, či ste skutočne našli všetky.

Pokúste sa potom pomocou asociatívneho zákona odvodiť, že všetky tieto vyjadrenia sa rovnajú. (Možností ako to dokazovať je veľmi veľa, jednu nájdete v nasledujúcej úlohe.)

Príklad 3.1.12. Dokážte, že ak $\circ$ je binárna operácia na množine A a $\circ$ je asociatívna, tak ľubovoľné uzátvorkovanie výrazu $a \circ b \circ c \circ d$ predstavuje ten istý prvok.

Všetky možné uzátvorkovania sú[1]
(1) $a \circ ((b \circ c) \circ d)$
(2) $a \circ (b \circ (c \circ d))$
(3) $(a \circ b) \circ (c \circ d)$
(4) $((a \circ b) \circ c) \circ d$
(5) $(a \circ (b \circ c)) \circ d$
Sú to skutočne všetky možné uzátvorkovania – najprv sme uviedli tie, kde sa ako posledná operácia vykoná vynásobenie prvkom a zľava, výraz (3) predstavuje jediné uzátvorkovanie, kde sú prvky rozdelené na dve dvojice a výrazy (4) a (5) sú tie uzátvorkovania, kde sa ako posledné vykoná vynásobenie prvkom d.

Podľa asociatívneho zákona platí

$$(b \circ c) \circ d = b \circ (c \circ d).$$

Ak vynásobíme túto rovnosť zľava prvkom a, dostaneme

$$a \circ ((b \circ c) \circ d) = a \circ (b \circ (c \circ d)),$$

čo je vlastne rovnosť (1) = (2).

Podobne, ak použijeme asociatívnosť pre prvky a, b, c a vzniknutú rovnosť vynásobíme sprava prvkom d, dostaneme (4) = (5).

Dvojnásobným použitím asociatívneho zákona (podčiarknutím sú zvýraznené zátvorky, ktoré sme v príslušnej rovnosti „prehodili“) dostaneme

$$a \circ \underline{(b \circ (c \circ d))} = (a \circ b) \circ \underline{(c \circ d)} = ((a \circ b) \circ c) \circ d,$$

čo je vlastne rovnosť (2) = (3) = (4).

Spojením všetkých týchto rovností dostaneme, že všetky uvedené výrazy sa rovnajú.

[1] V prípade, že vám vyšiel iný počet alebo iné uzátvorkovania, skúste si ozrejmiť čo presne rozumieme pod uzátvorkovaním – je to taký zápis, ktorý jednoznačne určuje poradie vykonaných operácií. Pritom poradie prvkov a, b, c, d nesmieme prehadzovať.

Predchádzajúci príklad by vás snáď mohol presvedčiť o tom, že niečo podobné platí aj pre uzátvorkovanie ľubovoľného počtu prvkov. Ale vôbec nie je jasné, ako by sa takéto niečo dalo dokázať. To si ukážeme v nasledujúcom (nepovinnom) dôkaze.

Tvrdenie 3.1.13 (Zovšeobecnený asociatívny zákon). *Nech $\cdot$ je asociatívna binárna operácia na množine A. Potom súčin $a_1 * a_2 * \cdots * a_n$ nezávisí od spôsobu uzátvorkovania.*

Dôkaz. Tvrdenie budeme dokazovať úplnou indukciou vzhľadom na n. Pri dôkaze budeme postupovať tak, že si vyberieme jedno uzátvorkovanie, konkrétne $a_1*(a_2*(a_3*\ldots(a_{n-1}*a_n)))$, a budeme sa snažiť dokázať, že všetky ostatné možné uzátvorkovania predstavujú ten istý prvok.

1° Pre $n = 2$ máme jediné možné uzátvorkovanie, preto tvrdenie platí.

2° Predpokladajme teraz, že tvrdenie platí pre ľubovoľný počet prvkov menší ako n.

Ak máme nejako uzátvorkovaný výraz $a_1 * a_2 * \ldots * a_n$, sú dve možnosti ako môže vyzerať. Buď má tvar

$$a_1 * \underbrace{(a_2 * a_3 * \ldots * a_n)}_{\text{nejako uzátvorkované}}$$

alebo

$$(a_1 * \ldots * a_k) * (a_{k+1} * \ldots * a_n),$$

kde opäť prvá a druhá zátvorka môžu byť uzátvorkované ľubovoľným spôsobom.

V prvom prípade, podľa indukčného predpokladu

$$a_2 * a_3 * \cdots * a_n = a_2 * (a_3 * \cdots (a_{n-1} * a_n)).$$

(Inými slovami, ľubovoľné uzátvorkovanie $n-1$ prvkov $a_2, a_3, \ldots, a_n$ sa rovná prvku určenému nami zvoleným usporiadaním.) Vynásobením tejto rovnosti zľava prvkom a_1 dostaneme

$$a_1 * (a_2 * a_3 * \cdots * a_n) = a_1 * (a_2 * (a_3 * \cdots * (a_{n-1} * a_n))).$$

Zostáva nám ešte druhý prípad. V tomto prípade najprv použijeme indukčný predpoklad pre obe zátvorky

$$(a_1 * \cdots * a_k) * (a_{k+1} * \cdots * a_n) = (a_1 * (a_2 * \cdots * a_k)) * (a_{k+1} * (a_{k+2} * \cdots * a_n)).$$

Využitím asociatívnosti dostaneme

$$(a_1 * (a_2 * \cdots * a_k)) * (a_{k+1} * (a_{k+2} * \cdots * a_n)) = a_1 * ((a_2 * \cdots * a_k) * (a_{k+1} * (a_{k+2} * \cdots * a_n))),$$

čím sme upravili daný výraz na tvar súčinu prvku a_1 a nejako uzátvorkovaných ostatných prvkov (čo je presne prvý prípad, ktorý sme už vyriešili).

Teraz teda opäť stačí použiť indukčný predpoklad na prvky v zátvorke a dostaneme požadovaný tvar

$$a_1 * ((a_2 * \cdots * a_k) * (a_{k+1} * (a_{k+2} * \cdots * a_n))) = a_1 * (a_2 * (a_3 * \cdots * (a_{n-1} * a_n))).$$

□

Poznámka* 3.1.14. Ako zaujímavosť môžeme spomenúť, že počet uzátvorkovaní $n + 1$ symbolov určuje n-té *Catalanove číslo*

$$C_n = \frac{1}{n+1}\binom{2n}{n}.$$

Dôkaz tohoto faktu nie je jednoduchý. Pri niektorých odvodeniach uvedenej formuly sa používa rovnosť

$$C_{n+1} = \sum_{i=0}^{n} C_i C_{n-i},$$

môžete sa skúsiť zamyslieť nad tým, či by ste ju vedeli odvodiť. Súvisí táto rovnosť s nejakým spôsobom (algoritmom) na vymenovanie všetkých možných uzátvorkovaní?

Cvičenia

Úloha 3.1.1. Vypíšte všetky možné binárne operácie na množine $\{0, 1\}$. Ktoré z nich sú asociatívne, komutatívne, majú neutrálny prvok? Pre ktoré existuje ku každému prvku aj inverzný?

Úloha 3.1.2. Na $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ definujme operácie $\oplus$ a $\odot$ podobne ako pre $\mathbb{Z}_5$ v príklade 3.1.3. (Teda ako obvyklé sčitovanie a násobenie, ibaže po urobení tejto operácie urobíme zvyšok po delení 7, čím dostaneme prvok zo $\mathbb{Z}_7$.) Zistite, či sú tieto operácie asociatívne, komutatívne, či existuje neutrálny prvok a či má každý prvok inverzný. Vedeli by ste to v prípade operácie $\oplus$ nájsť inverzný prvok aj bez toho, že by ste skúšali jednotlivé prvky?

3.2 Grupy

V tejto časti sa konečne dostávame k definícii grupy. Pre nás síce grupy poslúžia len ako pomocný aparát – na to, aby sme mohli jednoduchšie zadefinovať pojem poľa a dokázať niektoré vlastnosti polí – od svojho vzniku sa teória grúp stala samostatnou, veľmi rozsiahlou matematickou disciplínou, zasahujúcou do najrozličnejších oblastí matematiky. Viac sa o grupách dozviete na predmete algebra v druhom ročníku. (V prípade, že ste už veľmi netrpezliví, môžete si o nich dosť veľa prečítať v [K, KGGS, Z1].) Podobne aj o poliach sa v priebehu Vášho štúdia dozviete aj ďalšie zaujímavé fakty, na tejto prednáške uvedieme len tie, ktoré budeme potrebovať pri práci s vektorovými priestormi.

Definícia 3.2.1. Dvojica $(G, *)$, kde G je množina a $*$ je binárna operácia na G, sa nazýva *grupa,* ak

(i) operácia $*$ je asociatívna,

(ii) operácia $*$ má neutrálny prvok, (neutrálny prvok budeme spravidla označovať e)

(iii) ku každému prvku $g \in G$ existuje inverzný prvok vzhľadom na operáciu $*$. (Tento inverzný prvok budeme označovať g^{-1}.)

Poznámka 3.2.2. Pretože požadujeme existenciu neutrálneho prvku $e \in G$, z definície grupy automaticky vyplýva, že množina G je neprázdna, $G \neq \emptyset$.

Príklad 3.2.3. Na základe tabuľky, ktorú sme vyplnili v príklade 3.1.10 vidíme, že $(\mathbb{R}, +)$ aj $(\mathbb{Z}_5, \oplus)$ sú grupy.

Naopak, $(\mathbb{R}, \cdot)$ nie je grupa, pretože 0 nemá inverzný prvok. V tomto prípade môžeme situáciu zachrániť, ak zmeníme množinu, na ktorej budeme túto binárnu operáciu uvažovať. Tvrdíme, že $(\mathbb{R} \setminus \{0\}, \cdot)$ je grupa.

O tom, že $\cdot$ je binárna operácia aj na množine $\mathbb{R} \setminus \{0\}$ sme už hovorili v príklade 3.1.2. Neutrálny prvok je 1, toto číslo patrí do množiny $\mathbb{R} \setminus \{0\}$. Takisto asociatívnosť sa neporuší pri prechode ku menšej množine. Pretože sme vynechali nulu, každý prvok $a \in \mathbb{R} \setminus \{0\}$, už teraz má inverzný prvok $\frac{1}{a}$, ktorý tiež patrí do množiny $\mathbb{R} \setminus \{0\}$.

Definícia 3.2.4. Grupa $(G, *)$ sa nazýva *komutatívna,* ak operácia $*$ na G je komutatívna. (Tiež sa používa termín *abelovská grupa.*)

Nie každá grupa je komutatívna. Príkladom nekomutatívnej grupy je grupa S_n všetkých permutácií n-prvkovej množiny pre $n \geq 2$ (úloha 3.2.2).

Veta 3.2.5 (Zákony o krátení). *Ak $(G, *)$ je grupa, tak pre ľubovoľné $a, b, c \in G$ platí*

$$\begin{aligned} a * b = a * c \quad &\Rightarrow \quad b = c \\ b * a = c * a \quad &\Rightarrow \quad b = c \end{aligned}$$

Inak povedané, zákony o krátení hovoria, že v grupe môžeme krátiť ľubovoľným prvkom zľava aj sprava.

Dôkaz. Z rovnosti $a * b = a * c$ dostaneme vynásobením prvkom a^{-1} zľava

$$\begin{aligned} a^{-1} * (a * b) &= a^{-1} * (a * c) \\ (a^{-1} * a) * b &= (a^{-1} * a) * c \\ e * b &= e * c \\ b &= c \end{aligned}$$

(V jednotlivých krokoch sme využili asociatívnosť, definíciu inverzného a neutrálneho prvku.)

Implikácia $b * a = c * a \Rightarrow b = c$ sa dokáže analogicky, ibaže prvkom a^{-1} budeme násobiť sprava. □

Zákony o krátení môžeme zapísať aj v ekvivalentnej podobe (obmenená implikácia, pozri príklad 2.1.11):

$$\begin{aligned} b \neq c \quad &\Rightarrow \quad a * b \neq a * c \\ b \neq c \quad &\Rightarrow \quad b * a \neq c * a \end{aligned}$$

Skúsme si premyslieť, ako sa prejavia zákony o krátení v tabuľke binárnej operácie. Prvky tvaru $a * b$, kde $b \in G$, sú práve prvky v riadku a. Zákon o krátení v tvare $b \neq c \Rightarrow a * b \neq a * c$ teda znamená, že v rôznych stĺpcoch riadku a sa objavia rôzne výsledky operácie $*$. Inak povedané, v žiadnom riadku sa nesmie viackrát vyskytnúť ten istý prvok. Podobne, zákon o krátení zľava hovorí, že v žiadnom stĺpci sa nezopakuje nijaký prvok viackrát.

Veta 3.2.6. *Nech $(G, *)$ je grupa. Potom pre ľubovoľné $a, b \in G$ platí*

$$\begin{aligned} (a^{-1})^{-1} &= a \\ (a * b)^{-1} &= b^{-1} * a^{-1} \end{aligned}$$

Dôkaz. Najprv použijeme dvakrát definíciu inverzného prvku. Inverzný prvok a^{-1} musí spĺňať rovnosť

$$(a^{-1})^{-1} * a^{-1} = e.$$

Definícia inverzného prvku pre a nám dáva

$$a * a^{-1} = e.$$

Porovnaním týchto 2 rovností dostaneme

$$(a^{-1})^{-1} * a^{-1} = a * a^{-1}$$

a zo zákona o krátení vyplýva

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

Aj na dôkaz druhej rovnosti chceme využiť zákony o krátení. Z definície inverzného prvku máme

$$(a * b)^{-1} * (a * b) = e.$$

Aby sme mohli využiť zákon o krátení bolo by dobre, keby sme nejako upravili výraz $(b^{-1} * a^{-1}) * (a * b)$, tak sa pokúsme upraviť ho (budeme používať asociatívny zákon a definíciu inverzného a neutrálneho prvku).

$$\underline{(}b^{-1} * a^{-1}\underline{)} * (a * b) = b^{-1} * (a^{-1} * \underline{(}a * b\underline{)}) = b^{-1} * ((a^{-1} * a) * b) = b^{-1} * (e * b) = b^{-1} * b = e$$

Zistili sme teda, že $(a * b)^{-1} * (a * b) = (b^{-1} * a^{-1}) * (a * b)$ a zo zákona o krátení potom vyplýva

$$(a * b)^{-1} = b^{-1} * a^{-1}.$$

□

V predchádzajúcom dôkaze sme podrobne rozpisovali každé použitie asociatívneho zákona. Pretože sme už v používaní asociatívneho zákona ostrieľaní, môžeme si prácu zjednodušiť vynechávaním zátvoriek (ktoré si vieme na patričných miestach domyslieť) a uvedenú úpravu zapísať stručnejšie ako

$$b^{-1} * a^{-1} * a * b = b^{-1} * e * b = b^{-1} * b = e.$$

Poznámka 3.2.7. Grupy, s ktorými ste sa doteraz najčastejšie stretli, sú asi $(\mathbb{R}, +)$ a $(\mathbb{R} \setminus \{0\}, \cdot)$. Aj pre grupy vo všeobecnosti sa veľmi často zvykne grupová operácia často označovať $+$ alebo $\cdot$. Vtedy hovoríme o *aditívnom* (pomocou znamienka $+$) alebo *multiplikatívnom* (pomocou $\cdot$) zápise grupovej operácie.

Pri aditívnom zápise sa zvykne inverzný prvok zapisovať ako $-a$, pri multiplikatívnom ako a^{-1} alebo aj $\frac{1}{a}$. Takisto neutrálny prvok sa v závislosti od použitej symboliky niekedy označuje ako 0 alebo 1.

Rozdiel medzi týmito dvoma druhmi zápisu sa napríklad prejaví aj vtedy, ak chceme zapísať n-násobné použitie operácie na prvok a (pozri úlohu 3.2.16). Pri aditívnom zápise sa spravidla používa symbol $n \times a$, pri multiplikatívnom a^n.

My budeme používať označenia tak, ako sme ich zaviedli v tejto kapitole. Teda keď budeme pracovať s grupou vo všeobecnosti, budeme neutrálny prvok označovať e a inverzný prvok a^{-1}. V prípade konkrétnych grúp a hlavne v prípade polí a vektorových priestorov, kde sa priamo v definícii vyskytne binárna operácia označovaná ako $+$ však uprednostníme aditívny zápis. (V oboch spomínaných definíciach na to výslovne upozorníme). Takisto budeme používať aditívny zápis pre grupu $(\mathbb{Z}_n, \oplus)$ a mnohé ďalšie grupy, kde je prirodzené označiť grupovú operáciu znakom $+$. (Napríklad v úlohe 3.2.8, kde sa zaoberáme sčitovaním funkcií, je prirodzené označovať neutrálny prvok znakom 0.)

Cvičenia

Úloha 3.2.1. Ktoré z uvedených množín tvoria vzhľadom na dané operácie grupu? V ktorých prípadoch je táto grupa komutatívna?
a) $(\mathbb{Z}, \cdot)$ (celé čísla s obvyklým násobením)
b) $(\mathbb{R}, \cdot)$ (reálne čísla s obvyklým násobením)
c) $(\mathbb{R} - \{0\}, \cdot)$, d) $(\mathbb{C}, +)$, e) $(\mathbb{C}, \cdot)$, f) $(\mathbb{C} \setminus \{0\}, \cdot)$
g) $(\mathbb{R}^2, +)$ (so sčitovaním definovaným po zložkách)

h) $\mathbb{R}$ s operáciou $*$, $a * b = a + b - 1$
i) Množina všetkých párnych celých čísel vzhľadom na sčitovanie.
j) Množina všetkých nepárnych celých čísel vzhľadom na sčitovanie.
k) $(\mathbb{Z}_5, \oplus)$

Úloha 3.2.2. Tvoria všetky permutácie na konečnej množine M grupu? Je táto grupa komutatívna? Urobte tabuľku grupovej operácie v prípade $M = \{1, 2, 3\}$.

Úloha 3.2.3. Je $(\mathbb{R}, *)$, kde $a * b = ab + a + b$, grupa? Ak nie, vedeli by ste vynechať niektorý prvok a z množiny $\mathbb{R}$ tak, aby $(\mathbb{R} \setminus \{a\}, *)$ bola grupa?

Úloha 3.2.4. Nech G je množina všetkých funkcií $f_{a,b} \colon \mathbb{R} \to \mathbb{R}$, ktoré sú tvaru $f_{a,b}(x) = ax + b$ pre nejaké reálne čísla $a, b \in \mathbb{R}$. Tvorí táto množina funkcií s operáciou skladania grupu? Je množina $\{f_{a,b}; a, b \in \mathbb{R}, a \neq 0\}$ s operáciou skladania zobrazení grupa? Dostaneme grupu, ak vezmeme len také $a, b \in \mathbb{R}$, že $a = 1$? V tých prípadoch, keď dostaneme grupu, je táto grupa komutatívna?

Úloha 3.2.5. Nech $G = \{z \in \mathbb{C} : |z| = 1\}$. Je G s operáciou $\cdot$ (násobenie komplexných čísel) grupa? Označme $C_n = \{z \in \mathbb{C} : z^n = 1\}$. Je $(C_n, \cdot)$ grupa?

Úloha 3.2.6*. Budeme uvažovať o nasledujúcich operáciach s množinami:
$A \cup B = \{x; x \in A \vee x \in B\}$ (zjednotenie)
$A \cap B = \{x; x \in A \wedge x \in B\}$ (prienik)
$A \setminus B = \{x; x \in A \wedge x \notin B\}$ (rozdiel)
$A \div B = \{x; x \in A \Leftrightarrow x \in B\}$ (symetrická diferencia - ekvivalentne ju môžeme definovať ako $A \div B = (A \setminus B) \cup (B \setminus A)$)
Ak X je ľubovoľná množina, $P(X)$ označíme množinu všetkých jej podmnožín. Potom $\cup$, $\cap$, $\setminus$, $\div$ sú binárne operácie na $P(X)$. Je $P(X)$ s niektorou z týchto operácií grupa?

Úloha 3.2.7. Označme:
$M_1 = \{f \colon \mathbb{Z} \to \mathbb{Z}; f \text{ je bijekcia}\}$
$M_2 = \{f \in M_1; f(n) = n \text{ pre všetky celé čísla } n \text{ až na konečný počet}\}$
$M_3 = \{f \in M_1; f(n) = n \text{ len pre konečný počet } n\}$.
Ktoré z množín M_1, M_2, M_3 tvoria grupu spolu s operáciou skladania zobrazení?

Úloha 3.2.8. Nech G je množina všetkých zobrazení $f \colon \mathbb{R} \to \mathbb{R}$. Na tejto množine definujeme operáciu $\oplus$ tak, že $(f \oplus g)(x) = f(x) + g(x)$. Je G s touto operáciou grupa? Ak definujeme $(f \odot g)(x) = f(x) \cdot g(x)$, bude $(G, \odot)$ grupa? Ktoré funkcie treba vynechať, aby sme dostali grupu?

Úloha 3.2.9. Nech $M \neq \emptyset$ je množina a $(G, \circ)$ je grupa. Nech H je množina všetkých zobrazení $f \colon M \to G$. Definujme na H binárnu operáciu $*$ tak, že $(f * g)(x) = f(x) \circ g(x)$. Je $(H, *)$ grupa?

Úloha 3.2.10. Na množine $\mathbb{R}^n$ (teda na množine všetkých usporiadaných n-tíc reálnych čísel) definujeme binárnu operáciu $+$ ako $(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$. Je $\mathbb{R}^n$ s touto operáciou grupa? (Použili sme symbol $+$ v dvoch rôznych významoch – raz ako operáciu na $\mathbb{R}^n$, ktorú definujeme, a raz ako dobre známe sčitovanie na množine $\mathbb{R}$. Keby sme chceli byť dôslední, zaviedli by sme nový symbol pre operáciu na $\mathbb{R}^n$, napríklad $(x_1, \ldots, x_n) \oplus (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$. K tomuto problému – používanie rovnakého symbolu v rôznych významoch – sa ešte vrátime.)

Úloha 3.2.11. Ak $(G, \circ)$ je grupa a $a \in G$ je nejaký jej prvok, tak zobrazenie $f_a \colon G \to G$ definované ako $f_a(b) = a \circ b$ je bijekcia.

Úloha 3.2.12. Nech $(G, \circ)$ je grupa. Dokážte, že zobrazenie $f\colon G \to G$ definované ako $f(a) = a^{-1}$ je bijekcia.

Úloha 3.2.13*. Nech G je ľubovoľná množina a $\circ$ je asociatívna binárna operácia na G. Potom G je grupa práve vtedy, keď pre ľubovoľné $a, b \in G$ majú rovnice

$$a \circ x = b$$
$$y \circ a = b$$

riešenie v G (inými slovami, pre ľubovoľné $a, b \in G$ existujú $x, y \in G$, ktoré spĺňajú tieto dve rovnosti.)

Úloha 3.2.14*. Nech G je konečná množina a $\circ$ je binárna operácia na G taká, že platí asociatívny zákon a zákony o krátení. Dokážte, že G je grupa.

Úloha 3.2.15*. Dokážte, že v konečnej grupe, ktorá má párny počet prvkov, existuje prvok rôzny od neutrálneho prvku taký, že $a \circ a = e$.

Úloha 3.2.16. Nech $(G, *)$ je grupa a $a \in G$. Potom pre ľubovoľné $n \in \mathbb{N}$ definujeme matematickou indukciou prvok a^n nasledovne:
$a^0 = e$
$a^{n+1} = a^n * a$.
(Je to presne to, čo by sme intuitívne chápali pod zápisom $\underbrace{a * a * \ldots * a}_{n\text{-krát}}$.)

Túto definíciu môžeme rozšíriť aj na záporné čísla tak, že pre $n \in \mathbb{N}$ položíme $a^{-n} = (a^{-1})^n$. Tým je a^n definované pre ľubovoľné $a \in G$ a $n \in \mathbb{Z}$. (Všimnite si, že to korešponduje s označením a^{-1}, ktoré používame pre inverzný prvok.)

Dokážte, že pre ľubovoľné $a, b \in G$ a $m, n \in \mathbb{Z}$ platí:
a) $a^{m+n} = a^m * a^n$,
b) $(a^m)^n = a^{mn}$,
c) ak $a * b = b * a$, tak $a^n * b^n = (a * b)^n$,

Úloha 3.2.17. Nech $*$ je binárna operácia na množine A, taká, že pre každé $a, b, c \in A$ platí $a * (b * c) = (a * c) * b$ a $*$ má neutrálny prvok. Dokážte, že operácia $*$ je komutatívna a asociatívna.

Úloha 3.2.18. Nech $(G, \circ)$ je grupa. Dokážte, že ak $x \circ x = x$, tak $x = e$.

Úloha 3.2.19. Zistite, či $(\mathbb{R}^+ \times \mathbb{R}, \square)$, kde pre každé $(a, b), (c, d) \in \mathbb{R}^+ \times \mathbb{R}$ $(a, b)\square(c, d) = (2ac, b + d)$ je grupa.

Úloha 3.2.20. Ak pre každý prvok x grupy $(G, \circ)$ platí $x \circ x = e$, tak táto grupa je komutatívna.

3.3 Polia

V tejto podkapitole zadefinujeme polia. Základnými príkladmi polí sú reálne čísla, racionálne čísla a komplexné čísla. Väčšina vlastností, o ktorých budeme hovoriť, vám preto bude dobre známa.

Výhoda toho, že sa budeme mnohé užitočné vlastnosti týchto známych číselných oborov dokázať niekoľkých jednoduchých základných axióm spočíva v tom, že aj pre iné číselné množiny, ktoré spĺňajú axiómy z definície poľa, budeme môcť automaticky použiť všetky výsledky, ktoré si dokážeme o poliach vo všeobecnosti.

Definícia 3.3.1. Nech F je množina, $+$ a $\cdot$ sú binárne operácie na F. Hovoríme, že trojica $(F, +, \cdot)$ je *pole,* ak

(i) $(F, +)$ je komutatívna grupa, jej neutrálny prvok budeme označovať 0;

(ii) $(F \setminus \{0\}, \cdot)$ je komutatívna grupa, jej neutrálny prvok budeme označovať 1;

(iii) pre ľubovoľné $a, b, c \in F$ platí

$$a(b + c) = ab + ac,$$
$$(a + b)c = ac + bc.$$

(Túto vlastnosť nazývame *distributívnosť.*)

Pre inverzný prvok v grupe $(F, +)$ budeme používať označenie $-a$, t.j. pre túto grupu používame aditívny zápis. Prvok $-a$ nazývame *opačný prvok* k prvku a.

Pre grupu $(F \setminus \{0\}, \cdot)$ budeme používať multiplikatívny zápis, teda inverzný prvok k prvku $a \neq 0$ poľa F vzhľadom na operáciu $\cdot$ budeme značiť a^{-1}. Ak použijeme termín *inverzný prvok* v súvislosti s poľom a nešpecifikujeme binárnu operáciu, myslí sa tým práve prvok a^{-1}.

Namiesto $b + (-c)$ budeme používať stručnejší zápis $b - c$.

O operáciach $+$ a $\cdot$ v poli F budeme niekedy hovoriť ako o sčitovaní a násobení (súčte a súčine), presne tak ako je to v najzákladnejších príkladoch polí.

Aby bolo jasné, ktorá operácia sa vykoná najskôr, mali by sme používať zápis ako napríklad $(a.b) + (c.d)$. Budeme používať rovnakú konvenciu, aká je zaužívaná pre reálne čísla – operácia $\cdot$ má vyššiu prioritu ako operácia $+$, teda predchádzajúci zápis môžeme stručnejšie zapísať ako $ab + cd$.

Príklad 3.3.2. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ a $(\mathbb{C}, +, \cdot)$ sú polia. Vlastnosti (i) a (ii) sme overili v časti o grupách (resp. v cvičeniach za ňou), zo strednej školy vieme, že pre tieto číselné obory platí aj distributívnosť.

Pole by sme mohli ekvivalentne definovať aj nasledujúcim spôsobom. (Všimnite si, že pojem grupy nám umožnil túto definíciu zapísať oveľa stručnejšie.)

Definícia 3.3.3. Pole je množina F, na ktorej sú definované 2 binárne operácie $+$ a $\cdot$ spĺňajúce:

(i) pre všetky $a, b, c \in F$ platí $a + (b + c) = (a + b) + c$,

(ii) pre všetky $a, b \in F$ platí $a + b = b + a$,

(iii) existuje prvok $0 \in F$ taký, že pre každé $a \in F$ sa $a + 0 = a$,

(iv) ku každému $a \in F$ existuje $b \in F$ tak, že $a + b = 0$,

(v) pre všetky $a, b, c \in F$ platí $a.(b.c) = (a.b).c$,

(vi) pre všetky $a, b \in F$ platí $a.b = b.a$,

(vii) existuje prvok $1 \in F$ taký, že pre každé $a \in F$ sa $a.1 = a$,

(viii) ku každému $a \in F$, $a \neq 0$ existuje $b \in F$ tak, že $a.b = 1$,

(ix) pre všetky $a, b, c \in F$ sa $a.(b + c) = a.b + a.c$.

Overenie ekvivalentnosti týchto 2 definícií ponechávame ako cvičenie (úloha 3.3.1). Možno vám pri tom pomôžu niektoré zo základných vlastností poľa, ktoré odvodíme v nasledujúcom tvrdení. (My budeme používať definíciu 3.3.1. Samozrejme, akonáhle viete dokázať ekvivalentnosť oboch definícií, môžete používať ktorúkoľvek z nich.)

Tvrdenie 3.3.4. *Nech $(F, +, \cdot)$ je pole. Potom pre $a, b, c \in F$ platí*

(i) $a.0 = 0$, $0.a = 0$,

(ii) $a.b = b.a$,

(iii) $(-a).b = -a.b$,

(iv) $(-a).(-b) = a.b$,

(v) $a.b = 0 \Rightarrow a = 0 \vee b = 0$,

(vi) $a.b = a.c \wedge a \neq 0 \Rightarrow b = c$,

(vii) $a.a = a \Rightarrow a = 0 \vee a = 1$.

Dôkaz. (i) Rovnosť

$$0 + 0 = 0$$

vynásobíme zľava prvkom a. Po použití distributívneho zákona dostaneme

$$a.0 = a.(0 + 0) = a.0 + a.0$$
$$a.0 = 0$$

(V poslednej úprave sme využili zákon o krátení – môžeme ho použiť vďaka tomu, že $(F, +)$ je grupa.)

Rovnosť $0.a = 0$ sa ukáže takmer rovnako. (Prvkom a budeme násobiť sprava.)

(ii) Ak a aj b sú rôzne od nuly, tak tvrdenie vyplýva z komutatívnosti grupy $(F \setminus \{0\}, \cdot)$. Prípad, že niektoré z nich je nulové, je vyriešený v (i).

(iii) Použitím distributívnosti a definície opačného prvku dostaneme

$$a.b + (-a).b = (a + (-a)).b = 0.b \overset{(i)}{=} 0.$$

Teda $(-a).b$ je skutočne opačný prvok k $a.b$, čiže naozaj platí

$$(-a).b = -(a.b).$$

(iv) Dvojnásobným použitím rovnosti (iii) dostaneme

$$(-a).(-b) = -a.(-b) = -(-a.b) = a.b.$$

(V poslednej rovnosti sme použili fakt, že $-(-a) = a$, čo je vlastne tvrdenie $(a^{-1})^{-1} = a$ z vety 3.2.6 prepísané do aditívneho zápisu.)

(v) Fakt, že $\cdot$ je binárna operácia na množine $F \setminus \{0\}$ (ktorý je v definícii 3.3.1 ukrytý v tom, že $(F \setminus \{0\}, \cdot)$ je grupa) vlastne hovorí, že

$$a \neq 0 \wedge b \neq 0 \Rightarrow a.b \neq 0.$$

Z tejto implikácie dostane tvrdenie (vi) ako obmenenú implikáciu.

(vi) Z rovnosti $ab = ac$ dostaneme

$$a(b - c) = ab - ac = 0.$$

Pretože $a \neq 0$, z (v) vyplýva $b - c = 0$ a $b = c$.

(vii) Rovnosť $a.a = a$ môžeme upraviť na tvar

$$a.a - a.1 = 0$$
$$a(a - 1) = 0$$

Na základe (v) potom dostaneme $a = 0$ alebo $a = 1$. □

Teda tvrdenie 3.3.4(vii) by sme mohli zapísať aj v tvare $a^2 = a \Rightarrow a = 1 \vee a = 0$. (Namiesto $a.a$ budeme stručnejšie písať a^2, pozri definíciu 3.3.12.)

Zistiť, že racionálne, reálne a komplexné čísla spĺňajú vlastnosti poľa bolo pomerne jednoduché. Ďalším základným príkladom poľa bude pre nás pole $(\mathbb{Z}_p, \oplus, \odot)$, kde p je prvočíslo. Teraz sa preto budeme venovať definícii operácií $\oplus$ a $\odot$ na množine $\mathbb{Z}_n$ a dokážeme, že ak n je prvočíslo, tak to je skutočne pole.

Definícia 3.3.5. Nech $n \in \mathbb{N}$, $n \geq 2$. Množinu $\mathbb{Z}_n$ definujeme ako $\mathbb{Z}_n := \{0, 1, \ldots, n - 1\}$. (Teda množina $\mathbb{Z}_n$ obsahuje všetky možné zvyšky po delení číslom n.)

Na množine $\mathbb{Z}_n$ zavedieme operácie $\oplus$ a $\odot$ predpisom

$$a \oplus b = (a + b) \bmod n,$$
$$a \odot b = (ab) \bmod n,$$

kde operácia mod označuje zvyšok po delení číslom n (pozri dodatok A).

Delenie so zvyškom poznáte zo strednej školy, na pripomenutie si uveďme zopár príkladov.

Príklad 3.3.6. V tomto príklade budeme počítať v $\mathbb{Z}_7$.

$2 \oplus 4 = 6$

$3 \oplus 6 = 2$, pretože $3 + 6 = 9$ a zvyšok 9 po delení 7 je 2 $(9 = 1.7 + 2)$.

$2 \odot 3 = 6$

$2 \odot 4 = 1$, lebo $2.4 = 8$ a $8 = 1.7 + 1$ (Tým sme vlastne zistili, že 4 je inverzný prvok k 2 v poli $\mathbb{Z}_7$; čiže $2^{-1} = 4$ a $4^{-1} = 2$.)

$3 \odot 6 = 4$, pretože $3.6 = 18$ a $18 = 2.7 + 4$

Pokúsme sa vyrátať aj nejaký zložitejší výraz ako napríklad
$3 \odot (4 \oplus 2) \oplus 5 \odot (3 \oplus 6) = 3 \odot 6 \oplus 5 \odot 2 = 4 \oplus 3 = 0.$

Všimnime si, že ten istý výsledok by sme dostali, keby sme najprv použili obvyklé sčitovanie aj násobenie a až na záver urobili zvyšok modulo 7.
$3.(4 + 2) + 5.(3 + 6) = 3.6 + 5.9 = 18 + 45 = 63 = 9.7 + 0$
Nie je to náhoda – takto to funguje vždy. Viac sa o tom môžete dočítať v dodatku A.

Ak budete mať na pamäti túto zákonitosť, môže vám to niekedy pomôcť pri výpočtoch operácií v $\mathbb{Z}_n$. Využijeme ju aj v nasledujúcom dôkaze (povinnom pre tých, ktorí si trúfajú na A-čko; jediná náročnejšia časť je tam dôkaz existencie inverzného prvku – overenie ostatných podmienok by mal zvládnuť každý).

Budeme potrebovať pripomenúť aj pojem prvočísla, ktorý poznáte zo strednej školy.

Definícia 3.3.7. Číslo $n \in \mathbb{N}$, $n > 1$, nazývame *zloženým číslom,* ak $n = m.k$ pre nejaké $m, k \in \mathbb{N}$ také, že $1 < m, k < n$.

Ak $n \in \mathbb{N}$, $n > 1$, nie je zložené, tak ho nazývame *prvočíslo.*

Číslo 1 nepovažujeme ani za prvočíslo ani za zložené číslo.

Inými slovami, číslo n je prvočíslo, ak nie je deliteľné žiadnymi inými prirodzenými číslami okrem 1 a n. Napríklad 9 je zložené číslo, lebo 9 je násobkom 3, ale 7 je prvočíslo (číslo 7 nie je deliteľné nijakým menším číslom okrem 1).

Veta 3.3.8. *Ak p je prvočíslo, tak $(\mathbb{Z}_p, \oplus, \odot)$ je pole.*

Dôkaz. Overíme podmienky (i,ii,iii) z definície 3.3.1.

$(\mathbb{Z}_p, \oplus)$ je komutatívna grupa

Ľahko vidno, že $\oplus$ je binárna operácia na množine $\mathbb{Z}_p$.

Asociatívnosť: Pre ľubovoľné $a, b, c \in \mathbb{Z}_p$ platí

$$\begin{aligned}(a+b)+c &= a+(b+c)\\ ((a+b)+c) \bmod p &= (a+(b+c)) \bmod p\\ (((a+b) \bmod p)+c) \bmod p &= (a+((b+c) \bmod p)) \bmod p\\ (a \oplus b) \oplus c &= a \oplus (b \oplus c)\end{aligned}$$

(Pri poslednej úprave sme využili, že nezáleží na tom, že zvyšok po delení číslom p urobíme po každej operácii, alebo najprv urobíme obvyklé sčitovanie/násobenie a až z takto získaného výsledku urobíme zvyšok po delení číslom p.)

Komutatívnosť:

$$\begin{aligned}a+b &= b+a\\ (a+b) \bmod p &= (b+a) \bmod p\\ a \oplus b &= b \oplus a\end{aligned}$$

Neutrálny prvok je 0.

$$\begin{aligned}a+0 &= a\\ (a+0) \bmod p &= a \bmod p = a\\ a \oplus 0 &= a\end{aligned}$$

Inverzný prvok k a je $(-a) \bmod p$, čiže zvyšok čísla $-a$ po delení p. Skutočne

$$a \oplus (-a) \bmod p = (a+((-a) \bmod p)) \bmod p = (a+(-a)) \bmod p = 0 \bmod p = 0.$$

Všimnite si, že sme zatiaľ nikde nevyužili predpoklad, že p je prvočíslo. Táto prvá časť tvrdenia teda platí aj pre zložené čísla. Spomínaný predpoklad však budeme potrebovať v nasledujúcej časti dôkazu.

$(\mathbb{Z}_p \setminus \{0\}, \odot)$ je komutatívna grupa

Pri dôkaze asociatívnosti, komutatívnosti a existencie neutrálneho prvku budeme postupovať takmer rovnako ako v predchádzajúcej časti. V tomto prípade však budeme musieť dať pozor aj na to, či $\odot$ je skutočne binárna operácia na množine $\mathbb{Z}_p \setminus \{0\}$.

Binárna operácia: Chceme ukázať, že ak $a, b \in \mathbb{Z}_p \setminus \{0\}$, tak $a \odot b \neq 0$. Ak by platilo $a \odot b = (a.b) \bmod p = 0$, znamená to, že $p \mid a.b$ (zvyšok čísla $a.b$ po delení p je 0). Keďže p je prvočíslo, tak musí platiť $p \mid a$ alebo $p \mid b$. Lenže v množine $Z_p \setminus \{0\} = \{1, 2, \ldots, p-1\}$ nie je žiadny násobok p.

Asociatívnosť:

$$\begin{aligned}a.(b.c) &= (a.b).c\\ (a.(b.c)) \bmod p &= ((a.b).c) \bmod p\\ (a.(b.c) \bmod p) \bmod p &= ((a.b \bmod p).c) \bmod p\\ a \odot (b \odot c) &= (a \odot b) \odot c\end{aligned}$$

Komutatívnosť:

$$a.b = b.a$$
$$(a.b) \bmod p = (b.a) \bmod p$$
$$a \odot b = b \odot a$$

Neutrálny prvok je 1:

$$a.1 = a$$
$$(a.1) \bmod p = a \bmod p = a$$
$$a \odot 1 = a$$

Existencia inverzného prvku. V tejto časti dôkazu konečne vstúpi do hry fakt, že p je prvočíslo.

Nech $a \neq 0$. Chceme vedieť, či existuje $b \in \mathbb{Z}_p$ také, že $a \odot b = 1$. Najprv si všimnime, že pre $k, l \in \mathbb{Z}_p$ platí implikácia

$$a \odot k = a \odot l \qquad \Rightarrow \qquad k = l$$

(inak povedané, môžeme krátiť nenulovým číslom.)

Ak $(a.k) \bmod p = (a.l) \bmod p$, čiže ak aj al dávajú rovnaký zvyšok po delení p, tak platí $p \mid a.(k - l)$. Pretože p je prvočíslo, nemá vlastných deliteľov, a teda musí deliť buď a alebo $k - l$. Pritom $a \neq 0$ a iné násobky čísla p v $\mathbb{Z}_p$ už nie sú. Teda $p \mid k - l$. Pretože $k, l \in \mathbb{Z}_p$, ich rozdiel je z množiny $\{-(p-1), -(p-2), \ldots, 0, 1, \ldots, p-2, p-1\}$. V tejto množine je jediným násobkom čísla p opäť nula, preto $k - l = 0$ a $k = l$.

Implikácia, ktorú sme práve dokázali, ale znamená, že $a \odot k$, kde $k \in \mathbb{Z}_p$, nadobúda k rôznych hodnôt. (Nemôže nadobudnúť rovnakú hodnotu pre dve rôzne čísla $k \neq k'$.) Pre vhodné číslo $k \in \mathbb{Z}_p$ sa teda objaví každá hodnota zo $\mathbb{Z}_p$, špeciálne aj 1, čo sme chceli dokázať.

Distributívnosť:

$$a.(b + c) = ab + ac,$$
$$(a.(b + c)) \bmod p = (ab + ac) \bmod p,$$
$$a \odot (b \oplus c) = a \odot b \oplus a \odot c.$$

□

Všimnite si, že sme v najdôležitejšej časti dôkazu najprv dokázali zákon o krátení a z neho sme odvodili existenciu inverzného prvku. Tento postup súvisí s postupom, ktorý sa dá použiť v úlohe 3.2.14 *.

Tiež si môžeme všimnúť, že dôkaz je len existenčný – ukázali sme existenciu inverzných prvkov, ale v dôkaze sme neuviedli nijaký algoritmus, ako ich hľadať. Zatiaľ teda budeme postupovať tak, že jednoducho vyskúšame všetky možnosti (príklad 3.3.11), čo nie je až také hrozné, keď má pole, ktoré skúmame, málo prvkov. Iná možnosť, ako hľadať inverzný prvok, by bolo použitie malej Fermatovej vety (príklad 3.3.13). Neskôr, v rámci predmetu algebra, sa dozviete o Euklidovom algoritme na hľadanie najväčšieho spoločného deliteľa. Ten sa takisto dá použiť na tento účel.

Ak n je zložené, $(\mathbb{Z}_n, \oplus, \odot)$ nie je pole.

Pozrime sa najprv na $\mathbb{Z}_4$ s násobením modulo 4.

Príklad 3.3.9. $(\mathbb{Z}_4, \oplus, \odot)$ nie je pole.

$\odot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Z tabuľky si môžeme všimnúť, že neplatí viacero vlastností poľa:

- ku prvku 2 neexistuje inverzný prvok vzhľadom na operáciu $\odot$;
- platí $2 \odot 1 = 2 \odot 3$, teda v $\mathbb{Z}_4 \setminus \{0\}$ neplatí zákon o krátení, čiže $(\mathbb{Z}_4 \setminus \{0\}, \odot)$ nie je grupa;
- rovnosť $2 \odot 2 = 0$ ukazuje, že v $\mathbb{Z}_4$ neplatí tvrdenie 3.3.4(vi).

Práve posledná zo spomenutých vlastností sa dá pomerne jednoducho zovšeobecniť na ľubovoľné zložené číslo.

Príklad 3.3.10. Ak n je zložené číslo, tak $(\mathbb{Z}_n, \oplus, \odot)$ nie je pole.

Ak n je zložené, znamená to, že $n = m.k$ pre nejaké celé čísla m, k s vlastnosťou $1 < m, k < n$. Špeciálne to znamená, že $m, k \in \mathbb{Z}_n \setminus \{0\}$. Ak na obe strany rovnosti $n = m.k$ použijeme operáciu zvyšok po delení n, dostaneme

$$0 = m \odot k,$$

pričom $m \neq 0$ a $k \neq 0$. Teda aj v tomto prípade sme zistili, že neplatí tvrdenie 3.3.4(vi) a $(\mathbb{Z}_n, \oplus, \odot)$ nemôže byť pole.

Označenie $\oplus$ a $\odot$ korešponduje s našou dohodou, že v poli budeme používať aditívny zápis pre operáciu $+$ a pre operáciu $\cdot$ multiplikatívny zápis. (Jediný rozdiel je, že kvôli odlíšeniu týchto operácií ich dávame do krúžku.) V súlade s touto dohodou budeme označovať inverzný prvok k prvku a vzhľadom na operáciu $\oplus$ ako $-a$ a inverzný prvok vzhľadom na $\odot$ ako a^{-1}.

V nasledujúcom príklade sa budeme zaoberať práve inverznými prvkami vzhľadom na operácie $\oplus$ a $\odot$ v poli $\mathbb{Z}_p$. (Pre jednoduchosť si vyberieme $p = 7$.)

Príklad 3.3.11. Na základe dohody o označovaní opačného prvku v $\mathbb{Z}_7$ platí $-1 = 6$, $-2 = 5$, $-3 = 4$, $-4 = 3$, $-5 = 2$, $-6 = 1$, $-0 = 0$. (Teda inverzný prvok k $a \in \mathbb{Z}_7$ je $7 - a$.) V predchádzajúcom zápise -1 neznamená celé číslo -1 ale opačný prvok k prvku $1 \in \mathbb{Z}_7$.

Využívanie opačných prvkov môže niekedy zjednodušiť výpočty s operáciami $\oplus$ a $\odot$. Napríkad v $\mathbb{Z}_7$ máme
$3 \odot 6 = 3 \odot (-1) = -3 = 4$.
(Súčin $3.(-1)$ sa vyráta ľahšie ako 3.6. Je to len ilustračný príklad – výraznejšie zjednodušenie to prinesie až vtedy, keď počítame viacero operácií a vychádzajú tam väčšie čísla.) Iný príklad: $(2 \oplus 3) \odot (2 \odot 3) = 5 \odot 6 = (-2) \odot (-1) = 2 \odot 1 = 2$. (Využili sme Tvrdenie 3.3.4(iv). Pretože sme už dokázali, že $\mathbb{Z}_7$ je pole, môžeme pri výpočtoch používať čokoľvek, čo sme dokázali o poliach vo všeobecnosti.)

Videli sme, že nájsť opačný prvok v $\mathbb{Z}_7$ je jednoduché. S inverzným prvkom je to o niečo komplikovanejšie. Zatiaľ jediný spôsob, ako to môžeme urobiť je vyskúšať všetky možnosti. Skúsme napríklad vypočítať 3^{-1} v $\mathbb{Z}_7$. Kandidáti na inverzný prvok sú 1,2,3,4,5,6. Vypočítame:
$1 \odot 3 = 3$
$2 \odot 3 = 6$
$3 \odot 3 = 2$

$4 \odot 3 = 5$
$5 \odot 3 = 1$
Na piaty pokus sa nám podarilo nájsť prvok, ktorý dáva v súčin s trojkou rovný 1. Teda práve tento prvok je inverzný k 3:
$3^{-1} = 5$.

Ak by sme boli o niečo pozornejší, mohli sme prestať už po druhom kroku. V ňom sme totiž dostali:
$2 \odot 3 = 6 = -1$
z čoho vyplýva
$1 = -(2 \odot 3) = (-2) \odot 3$, čiže $3^{-1} = -2 = 5$. (Takto to funguje aj vo všeobecnosti – vždy nám stačí vyskúšať iba prvú polovicu možností, určite sa tam vyskytne buď 1 alebo -1.)

Definícia 3.3.12. Ak n je celé číslo a a, b sú prvky poľa F, tak definujeme $n \times a$ takto:
$0 \times a = 0$,
$(n+1) \times a = n \times a + a$ (zatiaľ sme to indukciou definovali pre prirodzené čísla),
Ak $n > 0$ tak definujeme $(-n) \times a = -(n \times a)$ (tým sme rozšírili definíciu aj na záporné čísla).
Podobne definujeme pre $a \neq 0$:
$a^0 = 1$,
$a^{n+1} = a^n.a$,
$a^{-n} = (a^n)^{-1}$ $(n > 0)$.

Predchádzajúca definícia je príkladom definície matematickou indukciou (poznámka 2.1.5). Menej formálne to môžeme vyjadriť ako $n \times a = \underbrace{a + a + \cdots + a}_{n\text{-krát}}$ a $a^n = \underbrace{a \cdot a \cdot \cdots \cdot a}_{n\text{-krát}}$.

Nulu sme z definície a^n vynechali preto, že by bol problém definovať 0^z pre $z \leq 0$. Pre prirodzené čísla je výraz 0^n zmysluplný.

Niektoré základné vlastnosti týchto dvoch operácií nájdete v úlohe 3.3.5. (Viaceré z nich použijeme v nasledujúcom príklade.)

Príklad 3.3.13. Vypočítajme a^6 pre prvky $a \in \mathbb{Z}_7$.
$0^6 = 0$
$1^6 = 1$
$2^6 = (2^3)^2 = 1^2 = 1$
$3^6 = (3^2)^3 = 2^3 = 1$
$4^6 = (-3)^6 = 3^6 = 1$
$5^6 = (-2)^6 = 2^6 = 1$
$6^6 = (-1)^6 = 1^6 = 1$

To, že pre všetky $a \neq 0$ sme dostali $a^6 = 1$ nie je náhoda. Pre ľubovoľné prvočíslo v poli $\mathbb{Z}_p$ platí $a^{p-1} = 1$ (pre nenulové $a \in \mathbb{Z}_p$). Toto tvrdenie je známe ako *malá Fermatova veta,* stretnete sa s ním ešte viackrát. Najbližšie v rámci predmetu elementárna teória čísel (pozri [Č, kapitola 1.5]). Návod na iný dôkaz tejto vety (využívajúci algebraické idey) nájdete v úlohe 3.3.14 alebo [KGGS, 174/9*].

Z rovnosti $a^{p-1} = 1$ špeciálne vyplýva, že v $\mathbb{Z}_p$ platí $a^{-1} = a^{p-2}$.

Cvičenia

Úloha 3.3.1. Dokážte ekvivalenciu definície 3.3.1 a 3.3.3.

Úloha 3.3.2. Ktoré z uvedených množín tvoria spolu s obvyklým sčitovaním a násobením pole?
a) $F = \{a + ib; a \in \mathbb{R}, b \in \mathbb{R}, b \geq 0\}$

b) $F = \{a + ib; a \in \mathbb{Q}, b \in \mathbb{Q}\}$
c) $F = \{a + ib; a \in \mathbb{Z}, b \in \mathbb{Z}\}$
d) $F = \{a + b\sqrt{5}; a \in \mathbb{Q}, b \in \mathbb{Q}\}$
e) $F = \{a + \sqrt{3}ib; a \in \mathbb{Q}, b \in \mathbb{Q}\}$
f) $F = \{a + \frac{b}{\sqrt{2}}; a \in \mathbb{Q}, b \in \mathbb{Q}\}$
g*) $F = \{a + b\sqrt[3]{5}; a \in \mathbb{Q}, b \in \mathbb{Q}\}$

Úloha 3.3.3. V poli $\mathbb{Z}_5$ vyrátajte $2^{-1} \oplus 4$, $(-2) \oplus 4$, $2^{-1} \odot 3$ a $-4 \odot 3^{-1}$.

Úloha 3.3.4. V $\mathbb{Z}_5$ vyrátajte 2^3, $(2^{-1})^4$, $2 \odot (4^{-1})^3$, $(4 \odot 2^{-1})^3$, $(-1)^5 \odot (4 \odot 3^{-1})^2$.

Úloha 3.3.5. Nech m, n sú celé čísla, a, b, $b_1, \ldots, b_n$ sú prvky poľa F. V úlohách f) až j) predpokladáme, že $a \neq 0$. Dokážte:[2]
a) $m \times a + n \times a = (m + n) \times a$
b) $m \times a + m \times b = m \times (a + b)$
c) $m \times (n \times a) = (mn) \times a$
d) $a.(n \times b) = n \times (a.b)$
e) $(m \times a)(n \times b) = (mn) \times (a.b)$
f) $m \times (m \times a)^{-1} = a^{-1}$
g) $a^m.a^n = a^{m+n}$
h) $a^m.b^m = (a.b)^m$
i) $(a^m)^n = a^{mn}$
j) $a^{2k} = (-a)^{2k}$
k) $n \times 0 = 0$
l) $1^n = 1$

Úloha 3.3.6. V ľubovoľnom poli F platí:

$$a + b = a + c \Rightarrow b = c$$
$$(a + b)(c + d) = ac + ad + bc + bd$$
$$-(-a) = a$$
$$-0 = 0$$
$$-(a + b) = (-a) + (-b)$$
$$(a - b)c = ac - bc$$
$$1 \neq 0$$
$$a.a = 1 \Leftrightarrow a = 1 \vee a = -1$$
$$a.(b_1 + \ldots + b_n) = a.b_1 + \ldots + a.b_n$$

Úloha 3.3.7. Na množine $\mathbb{R}^+$ všetkých kladných reálnych čísel zadefinujme operácie $\oplus$ a $\odot$ tak, že $x \oplus y = x.y$ a $x \odot y = x^y$. Ktoré z axióm poľa spĺňa $(\mathbb{R}^+, \oplus, \odot)$?

Úloha 3.3.8. Nech F je pole a $a \in F$. Definujeme zobrazenie $f_a \colon F \to F$ tak, že $f_a(b) = a+b$. Je f_a bijekcia? Ak áno, ako vyzerá zobrazenie f_a^{-1}? Čomu sa rovná $f_a \circ f_b$?

Ďalej definujeme $g_a \colon F \to F$ pre $a \neq 0$ tak, že $g_a(b) = a.b$. Je to bijekcia?

Úloha 3.3.9. Nech na množine $M = \{0, 1\}$ sú operácie $+$ a $\cdot$ dané tabuľkami

[2] Podúlohy by mali byť usporiadané tak, že ak v dôkaze niektorej z nich potrebujeme nejaké pomocné tvrdenie, máme ho už dokázané v niektorej z predchádzajúcich častí tejto úlohy. Ak by sa Vám zdalo, že poradie nie je správne, ozvite sa mi. Môžeme sa spolu pozrieť na to, či som sa pomýlil alebo či je dôvodom odlišného poradia to, že sa to dá dokazovať aj inak.

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	1	1

Ukážte, že $(M, +)$ a $(M \setminus \{0\}, \cdot)$ sú komutatívne grupy a že platí distributívny zákon $(a+b)c = ac + bc$. Je $(M, +, \cdot)$ pole?

Úloha 3.3.10. Zistite, či $(\mathbb{R}, +, *)$, kde $+$ je obvyklé sčitovanie reálnych čísel a pre každé $a, b \in \mathbb{R}$ $a * b = -2ab$, je pole.

Úloha 3.3.11. Na $\mathbb{R} \times \mathbb{R}$ definujeme operácie $+$ a $\cdot$ takto:
a) $(a, b) + (c, d) = (a + c, b + d)$ a $(a, b).(c, d) = (ac, bd)$,
b) $(a, b) + (c, d) = (a + c, b + d)$ a $(a, b).(c, d) = (ac - bd, ad + bc)$.
Je potom $(\mathbb{R} \times \mathbb{R}, +, \cdot)$ pole?

Úloha 3.3.12*. Pre ktoré prvky a poľa $\mathbb{Z}_7$ má riešenie rovnica $x^2 = a$? Koľko je takých prvkov v poli $\mathbb{Z}_{109}$?

Úloha 3.3.13*. Dokážte, že:
a) V ľubovoľnom poli platí $(a+b)^m = a^m + \binom{m}{1} \times a^{m-1}b + \binom{m}{2} \times a^{m-2}b^2 + \ldots + \binom{m}{m-1} ab^{m-1} + b^m$.
(Súčet na pravej strane sa zvykne označovať takto: $\sum_{k=0}^{m} \binom{m}{k} \times a^{m-k}b^k$.)
b) V poli $\mathbb{Z}_p$ platí: $(a \oplus b)^p = a^p \oplus b^p$.

Úloha 3.3.14*. Pomocou úlohy 3.3.13 sa dokážte matematickou indukciou vzhľadom na a, že v $\mathbb{Z}_p$ platí rovnosť $a^p = a$ (pre ľubovoľné $a \in \mathbb{Z}_p$). (Toto je vlastne iná formulácia malej Fermatovej vety.)

Kapitola 4

Vektorové priestory

4.1 Vektorový priestor

Na strednej škole ste sa už stretli s pojmom vektoru. Pracovali ste hlavne s vektormi v rovine a v trojrozmernom priestore. Tieto vektory budú tvoriť špeciálny prípad toho, čo budeme nazývať vektorový priestor.

Náš prístup bude opäť axiomatický, čo nám umožní používať dokázané výsledky okrem týchto vektorov aj na mnohé iné prípady. Okrem toho všeobecnosť našich úvah bude väčšia i vďaka tomu, že budeme pracovať nad ľubovoľným poľom.

Definícia 4.1.1. Nech F je pole a $V \neq \emptyset$ je množina. Nech $+$ je binárna operácia na V a každej dvojici $c \in F$, $\vec{\alpha} \in V$ je priradený prvok $c.\vec{\alpha} \in V$, pričom platí pre ľubovoľné $c, d \in F$ a $\vec{\alpha}, \vec{\beta} \in V$:

(i) $(V, +)$ je komutatívna grupa,

(ii) $c.(\vec{\alpha} + \vec{\beta}) = c.\vec{\alpha} + c.\vec{\beta}$,

(iii) $(c + d).\vec{\alpha} = c.\vec{\alpha} + d.\vec{\alpha}$,

(iv) $(c.d).\vec{\alpha} = c.(d.\vec{\alpha})$,

(v) $1.\vec{\alpha} = \vec{\alpha}$.

Potom hovoríme, že V je *vektorový priestor* nad poľom F.

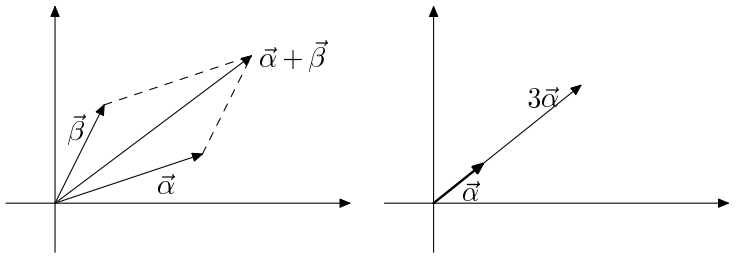
Prvky množiny V budeme nazývať *vektory* a spravidla ich budeme označovať gréckymi písmenami a šípkou. Pre prvky poľa F budeme niekedy používať termín *skaláry.*

Všimnite si, že hoci pre násobenie v poli F aj pre násobenie vektoru skalárom používame rovnaký symbol, z toho, medzi akými objektami sa tento symbol vyskytuje je jasné, ktorú z týchto dvoch možností máme na mysli. (Dalo by sa povedať, že vlastnosť (iv) z definície 4.1.1 hovorí o kompatibilite týchto dvoch operácií.)

Neutrálny prvok komutatívnej grupy $(V, +)$ budeme označovať $\vec{0}$ a nazývať *nulový vektor.*

Inverzný prvok v grupe $(V, +)$ budeme označovať $-\vec{\alpha}$ a nazývame *opačný vektor* k vektoru $\vec{\alpha}$. Vektor $\vec{\alpha} - \vec{\beta} := \vec{\alpha} + (-\vec{\beta})$ sa nazýva *rozdiel* vektorov $\vec{\alpha}$ a $\vec{\beta}$.

Príklad 4.1.2. Vektory v rovine so sčitovaním a násobením ako ho poznáte zo strednej školy, tvoria vektorový priestor nad poľom $\mathbb{R}$ (obr. 4.1).



Obr. 4.1: Operácie s vektormi v rovine

Príklad 4.1.3. Nech $n \in \mathbb{N}$ a $V = \mathbb{R}^n$, teda V pozostáva z usporiadaných n-tíc reálnych čísel, kde n je nejaké prirodzené číslo. Potom $\mathbb{R}^n$ je vektorový priestor nad poľom $\mathbb{R}$.

Sčitovanie vektorov a násobenie skalárom definujeme po zložkách, čím sa myslí

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2 \ldots, y_n) = (x_1 + y_1, x_2 + y_2 \ldots, x_n + y_n)$$

(teda sčítame príslušné súradnice oboch n-tíc)

$$c(x_1, x_2, \ldots, x_n) = (cx_1, cx_2 \ldots, cx_n)$$

(každú súradnicu vynásobíme skalárom c).

Sčitovanie a násobenie použité na jednotlivých súradniciach je už obvyklé sčitovanie a násobenie reálnych čísel (c, x_k aj y_k sú reálne čísla). [1]

Aby sme ukázali, že takto skutočne dostaneme vektorový priestor, treba overiť podmienky z definície 4.1.1. Princíp overenia je v podstate rovnaký u všetkých podmienok z tejto definície: aby sme overili rovnosť dvoch n-tíc, stačí overiť rovnosť na ľubovoľnej súradnici. Keď už pracujeme s niektorou konkrétnou súradnicou, dostaneme rovnosť v poli $\mathbb{R}$, ktorej platnosť vyplýva z toho, že $\mathbb{R}$ spĺňa definíciu poľa.

Vlastnosť (i) sme už overovali v úlohe 3.2.10. Pretože dôkazy ostatných vlastností sú skutočne veľmi podobné, overme pre ilustráciu len vlastnosť (iii) z definície vektorového priestoru. Majme teda ľubovoľný vektor $\vec{\alpha} = (x_1, \ldots, x_n) \in \mathbb{R}^n$ a skaláry $c, d \in F$. Potom

$$(c + d)\vec{\alpha} = ((c + d)x_1, \ldots, (c + d)x_n) = (cx_1 + dx_1, \ldots, cx_n + dx_n) = c\vec{\alpha} + d\vec{\alpha}.$$

(Rovnosť medzi súradnicovými vyjadreniami platí vďaka tomu, že c, d, x_i sú prvky poľa $\mathbb{R}$, teda rovnosť $(c + d)x_i = cx_i + dx_i$ vyplýva z distributívneho zákona.)

V prípade $n = 2$ dostaneme vektorový priestor $\mathbb{R}^2$, čo je vlastne vektorový priestor z predchádzajúceho príkladu v prípade, že vektory v rovine zapíšeme pomocou súradníc.

Príklad 4.1.4. Nech $V = \{f \colon \mathbb{R} \to \mathbb{R}\}$, teda V je množina všetkých zobrazení z $\mathbb{R}$ do $\mathbb{R}$. Túto množinu budeme obvykle označovať ako $\mathbb{R}^{\mathbb{R}}$.

Pre $f, g \in V$ a $c \in \mathbb{R}$ zadefinujeme sčitovanie a násobenie nasledovne:

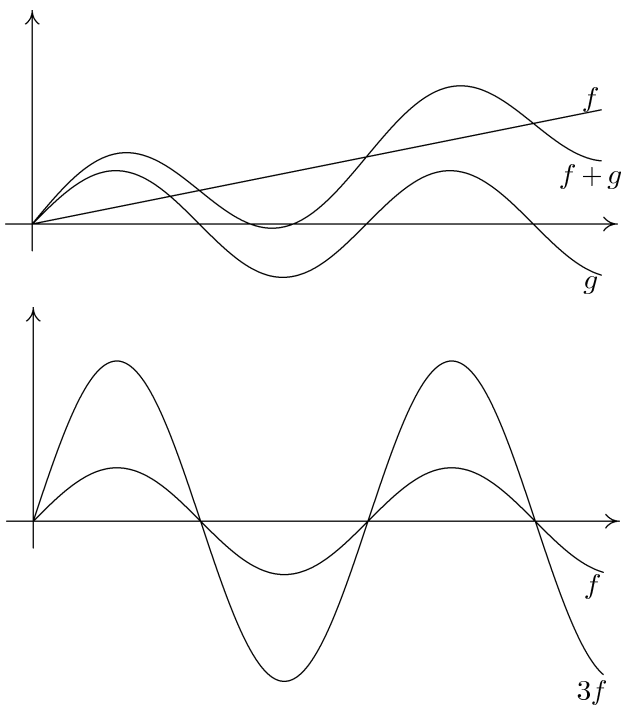
$$(f + g)(x) := f(x) + g(x),$$
$$(c.f)(x) := c.f(x),$$

[1] Všimnite si, že symbol + používame v dvoch významoch: na ľavej strane rovnosti označuje operáciu na množine $\mathbb{R}^n$ a na pravej strane rovnosti operáciu na $\mathbb{R}$. Podobne aj $\cdot$ sa tu vyskytuje v dvoch rozličných významoch. Keby sme chceli byť veľmi dôslední, mali by sme pre operácie s n-ticami zaviesť iné označenie. S podobnou situáciou sme sa už stretli aj v prípade násobenia v poli a vo vektorovom priestore nad týmto poľom. Kvôli stručnosti a jednoduchosti označenia budeme často používať zápisy takéhoto typu. Treba si na to zvyknúť.

kde $x \in \mathbb{R}$. (Na vysvetlenie: v uvedených rovnostiach sú na ľavej strane operácie, ktoré definujeme. Na pravej strane rovnosti ide už o obvyklé sčitovanie a násobenie reálnych čísel – vieme, že $f(x), g(x) \in \mathbb{R}$. Tým, že sme zadefinovali funkčnú hodnotu v každom bode $x \in \mathbb{R}$, sú zobrazenia $f + g, c.f \colon \mathbb{R} \to \mathbb{R}$ jednoznačne určené. Symboly $+$ a $\cdot$ tu vystupujú opäť v dvoch rôznych významoch – podobne ako v predchádzajúcom príklade.)

Inak môžeme predchádzajúcu definíciu preformulovať tak, že v každom bode sčítame funkčné hodnoty resp. prenásobíme funkčnú hodnotu konštantou.

S týmito operáciami tvorí množina $\mathbb{R}^{\mathbb{R}}$ vektorový priestor. Dôkaz tohoto faktu je do istej miery podobný ako pre priestor $\mathbb{R}^n$. V tomto prípade pri dôkaze vlastností vektorového priestoru overujeme rovnosť funkcií, čím sa dostaneme k rovnosti funkcií po dosadení ľubovoľného $x \in \mathbb{R}$ a keď už pracujeme s funkčnými hodnotami, sú to prvky poľa $\mathbb{R}$, čiže môžeme využiť vlastnosti poľa (úloha 4.1.4).



Obr. 4.2: Operácie v priestore $\mathbb{R}^{\mathbb{R}}$

(V tomto prípade sme nepoužili označenie pomocou gréckych písmen, ale označenie, ktoré obvykle používame pre funkcie. Tento príklad by mal ilustrovať, že prvkami vektorového priestoru skutočne môžu byť najrozličnejšie objekty.)

Poznámka 4.1.5. Podobným spôsobom ako pre reálne čísla by sme mohli definovať pre vektorové priestory F^n a F^F nad ľubovoľným poľom F. Overenie, že sú to naozaj vektorové priestory by bolo takmer rovnaké ako v prípade $F = \mathbb{R}$. (Všimnite si, že sme nepoužili žiadnu vlastnosť, ktorá by bola špecifická pre $\mathbb{R}$ a neplatila v ľubovoľnom poli.) S priestorom F^n sa ešte stretneme neskôr.

Podobne ako v prípade polí budú nasledovať niektoré základné vlastnosti, ktoré sa dajú ľahko odvodiť priamo z definície vektorového priestoru.

Veta 4.1.6. *Nech V je vektorový priestor nad poľom F, $c \in F$ a $\vec{\alpha} \in V$.*

(a) $0.\vec{\alpha} = \vec{0}$,

(b) $c.\vec{0} = \vec{0}$,

(c) $c.\vec{\alpha} = \vec{0}$ *práve vtedy, keď* $c = 0$ *alebo* $\vec{\alpha} = \vec{0}$,

(d) $(-c).\vec{\alpha} = -c.\vec{\alpha}$.

Dôkaz. (a) Keď rovnosť $0 = 0 + 0$ vynásobíme vektorom $\vec{\alpha}$, dostaneme

$$0.\vec{\alpha} = (0+0)\vec{\alpha} \overset{(iii)}{=} 0.\vec{\alpha} + 0.\vec{\alpha}$$

(Využili sme aj vlastnosť (iii) z definície vektorového priestoru.) Zo zákona o krátení (v grupe $(V, +)$) dostaneme $0.\vec{\alpha} = \vec{0}$.

(b) Budeme postupovať veľmi podobne, tentokrát skalárom $c \in F$ vynásobíme rovnosť $\vec{0} = \vec{0} + \vec{0}$ a použijeme vlastnosť (ii) z definície vektorového priestoru. Dostaneme

$$c.\vec{0} = c.(\vec{0} + \vec{0}) \overset{(ii)}{=} c.\vec{0} + c.\vec{0},$$

z čoho vyplýva (opäť na základe zákona o krátení v grupe $(V, +)$), že $c.\vec{0} = \vec{0}$.

(c) Nech $c.\vec{\alpha} = \vec{0}$ a $c \neq 0$. Potom existuje k prvku c inverzný prvok c^{-1}. Vynásobením uvedenej rovnosti prvkom c^{-1} zľava dostaneme

$$c^{-1}(c.\vec{\alpha}) = c^{-1}.\vec{0}.$$

Ľavú stranu môžeme upraviť ako

$$c^{-1}(c.\vec{\alpha}) \overset{(iv)}{=} (c^{-1}.c)\vec{\alpha} = 1.\vec{\alpha} \overset{(v)}{=} \vec{\alpha}.$$

Pre pravú stranu máme

$$c^{-1}.\vec{0} \overset{(b)}{=} \vec{0}$$

podľa prvej časti tejto vety. Dostali sme teda rovnosť $\vec{\alpha} = \vec{0}$.

(d) Jednoduchou úpravou dostaneme

$$c.\vec{\alpha} + (-c).\vec{\alpha} \overset{(iii)}{=} (c - c)\vec{\alpha} = 0.\vec{\alpha} \overset{(a)}{=} \vec{0}.$$

□

Cvičenia

Úloha 4.1.1. Nech $\vec{\alpha} = (1, 3, 6)$, $\vec{\beta} = (2, 1, 5)$, $\vec{\gamma} = (4, -3, 3)$. Vypočítajte $7\vec{\alpha} - 3\vec{\beta} - 2\vec{\gamma}$, $2\vec{\alpha} - 3\vec{\beta} + \vec{\gamma}$ vo vektorovom priestore $\mathbb{R}^3$. [(-7,24,21), (0,0,0)]

Úloha 4.1.2. Ukážte, že F je vektorový priestor nad F.

Úloha 4.1.3. Nech V je množina všetkých postupností reálnych čísel. Pre postupnosti $a = (a_n)_{n=1}^{\infty}$ a $b = (b_n)_{n=1}^{\infty}$ definujeme $a + b = (a_n + b_n)_{n=1}^{\infty}$ a $c.a = (c.a_n)_{n=1}^{\infty}$. Overte, že V s týmito operáciami tvorí vektorový priestor nad poľom $\mathbb{R}$.

Úloha 4.1.4. Nech M je neprázdna množina, F je pole. Potom množina všetkých zobrazení $f\colon M \to F$ so sčitovaním a násobením definovaným po bodoch (pozri príklad 4.1.4) tvorí vektorový priestor nad poľom F. (Ak sa Vám zdá táto úloha príliš zložitá, riešte ju iba pre $F = M = \mathbb{R}$.)

Skúste si tiež uvedomiť, že týmto spôsobom sme súčasne overili, že priestory F^n (príklad 4.1.3 a poznámka 4.1.5), F^F (príklad 4.1.4 a poznámka 4.1.5) a postupnosti prvkov z F (úloha 4.1.3) tvoria vektorové priestory. (Postupnosti môžeme chápať ako zobrazenia z $\mathbb{N}$ do F. Usporiadané n-tice môžeme chápať ako zobrazenia z $\{1, 2, \ldots, n\}$ do F.)

Úloha 4.1.5. Nech F je ľubovoľné pole a nech $\vec{\alpha}$ je ľubovoľný prvok. Nech $V = \{\vec{\alpha}\}$. Na V zavedieme operáciu sčitovania ako $\vec{\alpha} + \vec{\alpha} = \vec{\alpha}$ a násobenie skalárom $c.\vec{\alpha} = \vec{\alpha}$ (pre každé $c \in F$). Dokážte, že V je vektorový priestor nad poľom F.

Úloha 4.1.6. Overte, že $\mathbb{Z}_2 \times \mathbb{Z}_2$ so sčitovaním a násobením skalárom definovaným po zložkách tvorí vektorový priestor nad poľom $\mathbb{Z}_2$.

Úloha 4.1.7. Nech F je pole, $V = F^n$. Definujeme $(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$, $c(x_1, \ldots, x_n) = (cx_1, \ldots, cx_n)$ pre $c, x_1, \ldots, x_n, y_1, \ldots, y_n \in F$. Potom V je vektorový priestor nad poľom F.

Úloha 4.1.8. Koľko prvkov má vektorový priestor $(\mathbb{Z}_3)^n$? Čomu sa v tomto priestore rovná $\vec{\alpha} + \vec{\alpha} + \vec{\alpha}$?

Úloha 4.1.9. Overte, že všetky zobrazenia $f\colon \langle 0, 1\rangle \to \mathbb{R}$ so sčitovaním a násobením skalárom definovaným po bodoch tvoria vektorový priestor nad poľom $\mathbb{R}$.

Úloha 4.1.10. Overte, že $\mathbb{R}$ je vektorový priestor nad $\mathbb{Q}$, $\mathbb{C}$ je vektorový priestor nad $\mathbb{R}$, $\mathbb{C}$ je vektorový priestor nad $\mathbb{Q}$. Je $\mathbb{C}$ vektorový priestor nad $\mathbb{Z}$?

Úloha 4.1.11. Nech V je vektorový priestor nad poľom F, $c, c_1 \ldots c_k \in F$, $\vec{\alpha}, \vec{\alpha}_1, \ldots, \vec{\alpha}_n \in V$. Dokážte, že potom platí $c(\vec{\alpha}_1 + \ldots \vec{\alpha}_n) = c\vec{\alpha}_1 + \ldots + c\vec{\alpha}_n$, $(c_1 + \ldots + c_k)\vec{\alpha} = c_1\vec{\alpha} + \ldots + c_k\vec{\alpha}$. Čomu sa rovná $(c_1 + \ldots + c_k)(\vec{\alpha}_1 + \ldots \vec{\alpha}_n)$?

Úloha 4.1.12. Dokážte, že vo vektorovom priestore V nad poľom F pre každé $\vec{\alpha}, \vec{\beta} \in V$, $c \in F$ platí:
a) $c(\vec{\alpha} - \vec{\beta}) = c\vec{\alpha} - c\vec{\beta}$
b) $c(-\vec{\alpha}) = -c\vec{\alpha}$
c) $(c - d)\vec{\alpha} = c\vec{\alpha} - d\vec{\alpha}$
d) $(-c)(-\vec{\alpha}) = c\vec{\alpha}$
e) $\vec{\gamma} - (\vec{\alpha} + \vec{\beta}) = (\vec{\alpha} - \vec{\beta}) + \vec{\gamma}$
f) $-(\vec{\alpha} + \vec{\beta}) = (-\vec{\alpha}) + (-\vec{\beta})$

Úloha 4.1.13. Pre celé číslo n a vektor $\vec{\alpha}$ definujeme $n \times \vec{\alpha}$ podobným spôsobom, ako sme definovali $n \times a$ pre prvok a nejakého poľa F. Dokážte, že potom platí $n \times (c.\vec{\alpha}) = c.(n \times \vec{\alpha})$.

Úloha 4.1.14. Zistite, či $\mathbb{R} \times \mathbb{R}$ s operáciami $+$ a $\cdot$ definovanými tak, že $(a, b) + (c, d) = (a + c, b + d)$ pre ľubovoľné $(a, b), (c, d) \in \mathbb{R} \times \mathbb{R}$ a $r.(a, b) = (ra, 2rb)$ pre ľubovoľné $r \in \mathbb{R}$, je vektorový priestor nad $\mathbb{R}$.

4.2 Podpriestory

Definícia 4.2.1. Ak V je vektorový priestor nad poľom F, $S \neq \emptyset$ a $S \subseteq V$, tak S nazveme *podpriestorom* (alebo tiež *vektorovým podpriestorom*) priestoru V, ak

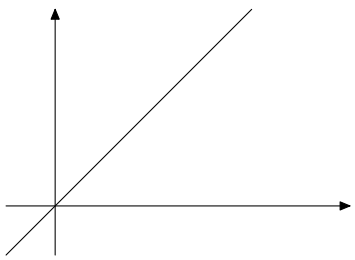
(i) pre ľubovoľné $\vec{\alpha}, \vec{\beta} \in S$ platí $\vec{\alpha} + \vec{\beta} \in S$,

(ii) pre ľubovoľné $\vec{\alpha} \in S$ a $c \in F$ platí $c.\vec{\alpha} \in S$.

Inými slovami, podpriestor vektorového priestoru V je taká podmnožina S, ktorá je uzavretá vzhľadom sčitovanie aj vzhľadom na násobenie skalárom.

Poznámka 4.2.2. Všimnime si, že každý podpriestor S priestoru V musí obsahovať nulový vektor $\vec{0}$. Vyplýva to z toho, že $S \neq \emptyset$, teda obsahuje aspoň jeden vektor $\vec{\alpha}$. Z uzavretosti na násobenie skalárom vyplýva, že musí obsahovať aj vektor $\vec{0} = 0.\vec{\alpha}$.

Príklad 4.2.3. Priamku v rovine, ktorá prechádza počiatkom súradnicovej sústavy, môžeme chápať ako množinu vektorov (obrázok 4.3). Táto množina tvorí jej vektorový podpriestor.



Obr. 4.3: Priamka v rovine ako príklad vektorového podpriestoru

Príklad 4.2.4. Nech $V = \mathbb{R}^3$ a

$$S = \{(x, y, z) \in \mathbb{R}^3; x + y + z = 0\}.$$

Potom S je podpriestor priestoru V. Overíme podmienky z definície podpriestoru.

Ak $\vec{\alpha} = (x, y, z) \in S$ a $\vec{\beta} = (x', y', z')$, znamená to, že

$$\begin{aligned} x + y + z &= 0, \\ x' + y' + z' &= 0. \end{aligned}$$

Sčítaním týchto 2 rovníc dostaneme

$$(x + x') + (y + y') + (z + z') = 0,$$

preto aj vektor $\vec{\alpha}+\vec{\beta} = (x+x', y+y', z+z')$ spĺňa podmienku, pomocou ktorej sme definovali podmnožinu S.

Ak $x + y + z = 0$, tak prenásobením konštantou c dostaneme

$$cx + cy + cz = 0,$$

teda $c.\vec{\alpha} = (cx, cy, cz) \in S$.

Príklad 4.2.5. Ak V je ľubovoľný vektorový priestor, tak $S = \{\vec{0}\}$ je podpriestor priestoru V.

Skutočne, jediný možný súčet, ktorý môžeme dostať z prvkov S je $\vec{0} + \vec{0} = \vec{0}$, a táto množina je uzavretá aj vzhľadom na násobenie skalárom, $c.\vec{0} = \vec{0}$.

Ľahko sa dá overiť aj to, že V je podpriestor V, t.j. každý vektorový priestor je podpriestorom samého seba.

Poznámka 4.2.6. Ak S je podpriestor vektorového priestoru V nad poľom F, tak aj S je vektorový priestor nad F (s operáciami rovnako definovanými ako v priestore V, inak povedané, „zdedenými“ z V).

To nám dáva ďalšiu možnosť, ako overiť, že nejaká množina je vektorový priestor nad F. V prípade, že ide o podmnožinu nejakého iného vektorového priestoru (pre ktorý sme už overili všetky vlastnosti), stačí nám len overiť podmienky z definície podpriestoru.

Pri vysvetlení, prečo to platí, si môžeme uvedomiť aj o niečo všeobecnejšie pravidlá, ktoré fungujú pri overovaní axióm nejakého tvaru. Chceme overiť, či S je vektorový priestor – pri tom máme overiť viacero vlastností.

Ako prvé vlastnosti máme podmienky, že $+$ je binárna operácia na S a násobenie má prvku $c \in F$ a vektoru $\vec{\alpha} \in S$ priradiť opäť prvok z S. To zabezpečia podmienky (i), (ii) z definície vektorového podpriestoru.

Ďalšou podmienkou je, že $(V, +)$ je komutatívna grupa. Požiadavku asociatívnosti môžeme zapísať v tvare

$$(\forall \vec{\alpha}, \vec{\beta}, \vec{\gamma} \in S)(\vec{\alpha} + \vec{\beta}) + \vec{\gamma} = \vec{\alpha} + (\vec{\beta} + \vec{\gamma}).$$

Teda je to výrok, ktorý hovorí, že pre <u>všetky</u> prvky z S má platiť nejaká rovnosť. Pretože ale už vieme, že táto vlastnosť platí pre ľubovoľné prvky z väčšej množiny V, tým skôr musí platiť pre ľubovoľné prvky z jej podmnožiny S.

Analogický argument samozrejme funguje aj pre každú vlastnosť, ktorú môžeme zapísať len pomocou všeobecného kvantifikátora a nejakej rovnosti. Vďaka tomu pre S nemusíme overovať ani vlastnosti (ii,iii,iv,v) z definície vektorového priestoru (definícia 4.1.1) a komutatívnosť operácie $+$.

Keď overujeme existenciu neutrálneho a inverzného prvku v $(S, +)$, sme v trochu inej situácii. Existenciu neutrálneho prvku môžeme zapísať v tvare

$$(\exists \vec{\varepsilon} \in S)\ (\forall \vec{\alpha} \in S)\ \vec{\varepsilon} + \vec{\alpha} = \vec{\alpha},$$

tentokrát v našej podmienke vystupuje okrem všeobecného kvantifikátora aj existenčný kvantifikátor. Z poznámky 4.2.2 vieme, že $\vec{0}$ patrí do S. Vieme, že $\vec{0}$ je neutrálny prvok vo $(V, +)$. Teda spĺňa podmienku

$$(\forall \vec{\alpha} \in S)\ \vec{0} + \vec{\alpha} = \vec{\alpha}.$$

O podmienkach takéhoto tvaru sme sa pred chvíľou už presvedčili, že sa dedia na podmnožiny. Súčasne vieme, že $\vec{0} \in S$. Preto $\vec{0}$ je neutrálny prvok aj v $(S, +)$.

Existenciu inverzného prvku môžeme zapísať podmienkou

$$(\forall \vec{\alpha} \in S)\ (\exists \vec{\beta} \in S) \vec{\alpha} + \vec{\beta} = \vec{0},$$

ktorá hovorí, že ku každému vektoru $\vec{\alpha}$ má existovať inverzný prvok na sčitovanie. Vieme však, že $\vec{\alpha}$ má inverzný prvok $-\vec{\alpha}$ vo $(V, +)$. Podobným spôsobom, akým sme dokázali jednoznačnosť neutrálneho prvku v tvrdení 3.1.11, by sme vedeli dokázať, že aj inverzný prvok v S musí byť ten istý, ako inverzný prvok vo V. Teda jediné, čo potrebujeme zistiť, je či aj vektor $-\vec{\alpha}$ patrí do S. To však vyplýva z toho, že $-\vec{\alpha} = (-1).\vec{\alpha}$, teda podľa podmienky (i) patrí do S.

Tvrdenie 4.2.7 (Kritérium vektorového podpriestoru). *Nech V je vektorový priestor nad poľom F a $S \subseteq V$, $S \neq \emptyset$. Potom S je podpriestor V práve vtedy, keď pre ľubovoľné $c, d \in F$ a $\vec{\alpha}, \vec{\beta} \in V$ platí*

$$\vec{\alpha}, \vec{\beta} \in S \qquad \Rightarrow \qquad c\vec{\alpha} + d\vec{\beta} \in S. \tag{4.1}$$

Dôkaz. Ako sme už niekoľkokrát spomenuli, ekvivalenciu 2 výrokov môžeme dokázať tak, že dokážeme implikácie oboma smermi.

To, že S je neprázdna, overovať nemusíme, pretože táto podmienka sa vyskytuje v oboch prípadoch.

$\boxed{\Rightarrow}$ Ak $\vec{\alpha}, \vec{\beta} \in S$, tak podľa (ii) platí $c.\vec{\alpha} \in S$ a $d.\vec{\beta} \in S$. Z toho na základe (i) dostaneme $c\vec{\alpha} + d\vec{\beta} \in S$.

$\boxed{\Leftarrow}$ Ak množina S spĺňa podmienku (4.1), tak dosadením $c = d = 1$ dostaneme, že S spĺňa (i). Ak zvolíme $d = 0$, dostaneme podmienku (ii). □

Ďalšia vlastnosť, ktorá bude pre nás užitočná, je fakt, že prienik dvoch podpriestorov vektorového priestoru je opäť podpriestor.

Veta 4.2.8. *Ak S a T sú podpriestory vektorového priestoru V, tak aj $S \cap T$ je podpriestor V.*

Dôkaz. Pretože $\vec{0} \in S$ aj $\vec{0} \in T$, platí $\vec{0} \in S \cap T$, čiže $S \cap T \neq \emptyset$.

Overíme podmienku (4.1). Ak $\vec{\alpha}, \vec{\beta} \in S \cap T$, tak platí $c\vec{\alpha} + d\vec{\beta} \in S$ (lebo S je podpriestor V) a súčasne $c\vec{\alpha} + d\vec{\beta} \in T$ (lebo T je podpriestor V). To znamená, že $c\vec{\alpha} + d\vec{\beta} \in S \cap T$. □

Tvrdenia takéhoto typu sa jednoduchým spôsobom dajú rozšíriť z dvoch objektov na ľubovoľný konečný počet. (Pokúste sa to overiť podrobne.)

Dôsledok 4.2.9. *Nech $n \in \mathbb{N}$. Ak $S_1, S_2, \ldots, S_n$ sú podpriestory priestoru V, tak aj $\bigcap_{i=1}^{n} S_i$ je podpriestor priestoru V.*

Veľmi podobným spôsobom, ako sme dokázali vetu 4.2.8, sa dá overiť, že podobné tvrdenie platí aj pre nekonečne veľa podpriestorov.

Veta 4.2.10. *Nech I je ľubovoľná množina a S_i je podpriestor priestoru V pre každé $i \in I$. Potom aj $\bigcap_{i \in I} S_i$ je podpriestor priestoru V.*

Dôkaz$^{\triangle}$. Označme $S = \bigcap_{i \in I} S_i$. Stačí si uvedomiť, že vektor $\vec{\gamma} \in S$ práve vtedy, keď pre všetky $i \in I$ platí $\vec{\gamma} \in S_i$. Na základe toho dostaneme

$$\vec{\alpha}, \vec{\beta} \in S \;\Rightarrow\; (\forall i \in I)\vec{\alpha}, \vec{\beta} \in S_i \;\Rightarrow\; (\forall i \in I) c\vec{\alpha} + d\vec{\beta} \in S_i \;\Rightarrow\; c\vec{\alpha} + d\vec{\beta} \in S.$$

Podľa tvrdenia 4.2.7 je teda S vektorový podpriestor priestoru V. □

Cvičenia

Úloha 4.2.1. Podrobne dokážte dôsledok 4.2.9.

Úloha 4.2.2. Dokážte, že množina všetkých funkcií $f\colon \mathbb{R} \to \mathbb{R}$, ktoré sú tvaru $a + b\cos x + c\sin x$ pre nejaké $a, b, c \in \mathbb{R}$ tvoria vektorový podpriestor priestoru všetkých reálnych funkcií $\mathbb{R}^{\mathbb{R}}$.

Úloha 4.2.3. Ktoré z týchto množín tvoria vektorový podpriestor priestoru $\mathbb{R}^3$?
a) $M = \{(x_1, x_2, x_3) \in \mathbb{R}^3; x_1 \in \mathbb{Z}\}$
b) $M = \{(x_1, x_2, x_3) \in \mathbb{R}^3; x_1 = 0\}$
c) $M = \{(x_1, x_2, x_3) \in \mathbb{R}^3; x_1 = 0 \vee x_2 = 0\}$
d) $M = \{(x_1, x_2, x_3) \in \mathbb{R}^3; 3x_1 + 4x_2 = 1\}$
e) $M = \{(x_1, x_2, x_3) \in \mathbb{R}^3; 7x_1 - x_2 = 0\}$
f) $M = \{(x_1, x_2, x_3) \in \mathbb{R}^3; x_1 + x_2 = x_3\}$
g) $M = \{(x_1, x_2, x_3) \in \mathbb{R}^3; |x_1| = |x_2|\}$
h) $M = \{(x_1, x_2, x_3) \in \mathbb{R}^3; x_1 + x_2 + x_3 \geq 0\}$
i) $M = \{(x_1, x_2, x_3) \in \mathbb{R}^3; 2x_1 = -x_2 = x_3\}$
j) $M = \{(x_1, x_2, x_3) \in \mathbb{R}^3; x_1 + x_2 + x_3 = 0\}$.

Úloha 4.2.4. Ktoré z týchto podmnožín tvoria vektorový podpriestor priestoru reálnych funkcií $\mathbb{R}^{\mathbb{R}}$?
a) funkcie $f\colon \mathbb{R} \to \mathbb{R}$ s vlastnosťou $2f(0) = f(1)$
b) nezáporné funkcie
c) funkcie $f\colon \mathbb{R} \to \mathbb{R}$ s vlastnosťou $f(1) = 1 + f(0)$
d) funkcie $f\colon \mathbb{R} \to \mathbb{R}$ s vlastnosťou $(\forall x \in \langle 0, 1\rangle) f(x) = f(1-x)$
e) ohraničené funkcie $f\colon \mathbb{R} \to \mathbb{R}$
f) spojité funkcie $f\colon \mathbb{R} \to \mathbb{R}$
h) funkcie $f\colon \mathbb{R} \to \mathbb{R}$ také, že existuje konečná $\lim\limits_{n\to\infty} f(x)$
i*) funkcie $f\colon \mathbb{R} \to \mathbb{R}$ také, že existuje konečná alebo nekonečná $\lim\limits_{n\to\infty} f(x)$.

Úloha 4.2.5. Overte, či
a) množina všetkých polynómov s reálnymi koeficientami,
b) množina všetkých polynómov s reálnymi koeficientami stupňa najviac n,
c) množina všetkých polynómov párneho stupňa,
d) množina všetkých polynómov stupňa práve n
sú vektorové priestory. Sčitovanie a násobenie skalárom definujeme rovnako ako pre reálne funkcie.

4.3 Lineárna kombinácia, lineárna nezávislosť

4.3.1 Lineárna kombinácia a lineárny obal

Definícia 4.3.1. Nech V je vektorový priestor nad poľom F. Hovoríme, že vektor $\vec{\alpha}$ je *lineárnou kombináciou* vektorov $\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n$, ak existujú skaláry $c_1, c_2, \ldots, c_n \in F$ také, že

$$\vec{\alpha} = c_1\vec{\alpha}_1 + c_2\vec{\alpha}_2 + \cdots + c_n\vec{\alpha}_n.$$

Skaláry $c_1, c_2, \ldots, c_n$ nazývame *koeficienty lineárnej kombinácie.*

Príklad 4.3.2. $(1,0) + (0,1) = (1,1)$, teda vektor $(1,1)$ je lineárna kombinácia vektorov $(1,0)$ a $(0,1)$ v $\mathbb{R}^2$.

$2.(1,0,0) + 3.(0,1,0) = (2,3,0)$, teda vektor $(2,3,0)$ je lineárna kombinácia vektorov $(1,0,0)$ a $(0,1,0)$ v $\mathbb{R}^3$.

Tvrdenie 4.3.3. *Nech V je vektorový priestor nad poľom F. Ak $\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n \in V$, tak množina*

$$M = \{c_1\vec{\alpha}_1 + c_2\vec{\alpha}_2 + \cdots + c_n\vec{\alpha}_n; n \in \mathbb{N}, c_i \in F, \vec{\alpha}_i \in V \text{ pre } i = 1, 2 \ldots, n\}$$

je podpriestor vektorového priestoru V.

Tento podpriestor nazývame lineárny obal *vektorov $\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n$ alebo* podpriestor generovaný vektormi $\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n$. *Označujeme ho*

$$M =: [\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n].$$

Ak platí $[\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n] = V$, hovoríme, že vektory $\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n$ generujú *vektorový priestor V.*

Definícia množiny $[\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n]$ vlastne hovorí, že $[\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n]$ je množina všetkých lineárnych kombinácií vektorov $\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n$.

Dôkaz. Aby sme dokázali, že M je podpriestor vektorového priestoru V, stačí nám overiť, že táto množina je uzavretá na sčitovanie a skalárne násobky.

Ak máme dva vektory

$$\vec{\alpha} = c_1\vec{\alpha}_1 + c_2\vec{\alpha}_2 + \cdots + c_n\vec{\alpha}_n$$
$$\vec{\beta} = d_1\vec{\alpha}_1 + d_2\vec{\alpha}_2 + \cdots + d_n\vec{\alpha}_n$$

tak aj vektor $\vec{\alpha} + \vec{\beta} = c_1\vec{\alpha}_1 + c_2\vec{\alpha}_2 + \cdots + c_n\vec{\alpha}_n + d_1\vec{\alpha}_1 + d_2\vec{\alpha}_2 + \cdots + d_n\vec{\alpha}_n = (c_1 + d_1)\vec{\alpha}_1 + (c_2 + d_2)\vec{\alpha}_1 + \cdots + (c_n + d_n)\vec{\alpha}_n$ má tvar, aký požadujeme v definícii množiny M. Takisto pre $c \in F$ dostaneme

$$c\vec{\alpha} = c(c_1\vec{\alpha}_1 + c_2\vec{\alpha}_2 + \cdots + c_n\vec{\alpha}_n) = cc_1\vec{\alpha}_1 + cc_2\vec{\alpha}_2 + \cdots + cc_n\vec{\alpha}_n,$$

čiže aj vektor $c\vec{\alpha}$ patrí do M. □

Príklad 4.3.4. Pre vektorový priestor $\mathbb{R}^3$ platí $\mathbb{R}^3 = [(1,0,0),(0,1,0),(0,0,1)]$.

Skutočne, ľubovoľný vektor $(x,y,z) \in \mathbb{R}^3$ sa dá vyjadriť ako lineárna kombinácia $x.(1,0,0) + y.(0,1,0) + z.(0,0,1)$.

Podobne sa dá dokázať, že $[(1,0,\ldots,0),(0,1,0,\ldots,0),\ldots,(0,\ldots,0,1)] = \mathbb{R}^n$.

Na vygenerovanie podpriestoru $S = \{(x,y,z) \in \mathbb{R}^3; x+y+z = 0\}$ dokonca stačia 2 vektory. Všimnime si, že rovnica $x+y+z = 0$ je ekvivalentná s rovnicou $z = -x-y$, teda podpriestor S môžeme zapísať aj v tvare $S = \{(x,y,-x-y); x,y \in \mathbb{R}\}$. Teraz už vidíme, že každý vektor z S sa dá zapísať ako lineárna kombinácia $(x,y,-x-y) = x.(1,0,-1) + y.(0,1,-1)$ a platí $S = [(1,0,-1),(0,1,-1)]$.

Všimnime si, že každý podpriestor, ktorý obsahuje vektory $\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n$ musí obsahovať aj všetky ich lineárne kombinácie (pretože ich vieme dostať opakovaním sčitovania a násobenia skalárom a na tieto 2 operácie sú podpriestory uzavreté). Teda podpriestory sú uzavreté vzhľadom na lineárne kombinácie vektorov. Toto tvrdenie sformalizujeme a dokážeme v nasledujúcej leme.

Lema 4.3.5. *Ak $\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n \in S$, kde S je podpriestor vektorového priestoru V nad poľom F, aj ich ľubovoľná lineárna kombinácia $c_1\vec{\alpha}_1 + c_2\vec{\alpha}_2 + \cdots + c_n\vec{\alpha}_n$ patrí do podpriestoru S.*

Dôkaz. Chceme ukázať, že ľubovoľné lineárna kombinácia $c_1\vec{\alpha}_1 + c_2\vec{\alpha}_2 + \cdots + c_k\vec{\alpha}_k$ patrí do S. Budeme postupovať indukciou vzhľadom na k.

1° Pre $k = 1$ prakticky niet čo dokazovať. (Dokazovaný výrok pre $k = 1$ je $\vec{\alpha} \in S \Rightarrow c\vec{\alpha} \in S$.)

Pre $k = 2$ dostaneme tvrdenie $\vec{\alpha}_1, \vec{\alpha}_2 \in S \Rightarrow c_1\vec{\alpha}_1 + c_2\vec{\alpha}_2 \in S$, ktoré vyplýva z kritéria vektorového podpriestoru (tvrdenie 4.2.7).

2° Predpokladajme, že tvrdenie platí pre lineárnu kombináciu k vektorov. Dokážeme, že platí aj pre $(k+1)$ vektorov.

$$c_1\vec{\alpha}_1 + c_2\vec{\alpha}_2 + \cdots + c_{k+1}\vec{\alpha}_{k+1} = \underbrace{(c_1\vec{\alpha}_1 + c_2\vec{\alpha}_2 + \cdots + c_k\vec{\alpha}_k)}_{\in S} + c_{k+1}\vec{\alpha}_{k+1} \in S$$

Podľa indukčného predpokladu lineárna kombinácia k vektorov (prvá zátvorka) patrí do S a po pripočítaní vektora $c_{k+1}\vec{\alpha}_{k+1}$ (ktorý tiež patrí do S) dostaneme opäť vektor z S. □

Veta 4.3.6. *Ak $\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n \in S$, kde S je podpriestor vektorového priestoru V nad poľom F, tak $[\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n] \subseteq S$.*

Dôkaz. Vyplýva z predchádzajúcej lemy. □

Poznámka 4.3.7. Predchádzajúca veta hovorí, že podpriestor $[\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n]$ je najmenší podpriestor priestoru V, ktorý obsahuje vektory $\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n$.

Pod slovom *najmenší* tu rozumieme, že ak S je taký podpriestor V, že $\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n \in S$, tak $[\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n] \subseteq S$. (Často sa používa aj termín *najmenší vzhľadom na inklúziu.*)

Tento podpriestor je prienikom všetkých podpriestorov V, ktoré obsahujú vektory $\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n$. Pretože prienik podpriestorov je opäť podpriestor (veta 4.2.10) dostaneme takto podpriestor priestoru V. Pretože sme urobili prienik <u>všetkých</u> podpriestorov, je takto získaný prienik najmenší podpriestor vzhľadom na inklúziu, ktorý obsahuje $\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n$.

Veta 4.3.8. *Nech $\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n \in V$, $\vec{\beta} \in V$, kde V je vektorový priestor nad poľom F. Potom $\vec{\beta}$ je lineárnou kombináciou vektorov $\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n$ práve vtedy, keď*

$$[\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n] = [\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n, \vec{\beta}].$$

Dôkaz. $\boxed{\Rightarrow}$ Chceme ukázať rovnosť 2 množín – to môžeme dokazovať tak, že dokážeme obe inklúzie. Pritom inklúzia $[\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n] \subseteq [\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n, \vec{\beta}]$ je zrejmá. Opačná inklúzia vyplýva z toho, že ak máme nejaký vektor $\vec{\gamma} \in [\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n, \vec{\beta}]$, čo znamená, že

$$\vec{\gamma} = c_1\vec{\alpha}_1 + c_2\vec{\alpha}_2 + \cdots + c_n\vec{\alpha}_n + c\vec{\beta}$$

pre nejaké $c_1, c_2, \ldots, c_n, c \in F$ a ak vieme, že β je lineárna kombinácia vektorov $\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n$, čiže

$$\vec{\beta} = d_1\vec{\alpha}_1 + d_2\vec{\alpha}_2 + \cdots + d_n\vec{\alpha}_n$$

pre nejaké $d_1, d_2, \ldots, d_n$, tak úpravou dostaneme

$$\vec{\gamma} = c_1\vec{\alpha}_1 + c_2\vec{\alpha}_2 + \cdots + c_n\vec{\alpha}_n + cd_1\vec{\alpha}_1 + cd_2\vec{\alpha}_2 + \cdots + cd_n\vec{\alpha}_n = (c_1 + cd_1)\vec{\alpha}_1 + (c_2 + cd_2)\vec{\alpha}_1 + \ldots + (c_n + cd_n)\vec{\alpha}_n,$$

čo znamená, že

$$\vec{\gamma} \in [\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n].$$

(Stručne: Lineárna kombinácia lineárnych kombinácií je opäť lineárna kombinácia.)

$\boxed{\Leftarrow}$ Podľa predpokladu $\vec{\beta} \in [\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n]$, teda $\vec{\beta}$ je lineárna kombinácia vektorov $\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n$. □

4.3.2 Lineárna nezávislosť

V tejto podkapitole zadefinujeme pojem, ktorý bude pre nás v ďalšom štúdiu veľmi dôležitý.

Definícia 4.3.9. Nech V je vektorový priestor nad poľom F. Vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ sú *lineárne závislé,* ak existujú $c_1, \ldots, c_n \in F$, ktoré nie sú všetky nulové a platí

$$c_1\vec{\alpha}_1 + \cdots + c_n\vec{\alpha}_n = \vec{0}.$$

(Stručne: $\vec{0}$ je nenulovou lineárnou kombináciou vektorov $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$.)

V opačnom prípade hovoríme, že vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ *lineárne nezávislé.*

Príklad 4.3.10. Najprv sa pozrime na niektoré špeciálne prípady. Ak $n = 1$, teda ak máme len jediný vektor $\vec{\alpha}$, tento vektor tvorí lineárne závislú množinu práve vtedy, keď $\vec{\alpha} = \vec{0}$ (vyplýva to z vety 4.1.6 (c)).

Ak $n = 2$, čiže máme 2 vektory $\vec{\alpha}$ a $\vec{\beta}$, tak sú lineárne závislé práve vtedy, keď jeden z nich je násobkom druhého, čiže $\vec{\alpha} = c.\vec{\beta}$ alebo $\vec{\beta} = c\vec{\alpha}$ pre nejaké $c \in F$ (úloha 4.3.8).

Vektory $(0,1), (1,0), (1,1) \in \mathbb{R}^2$ sú lineárne závislé, lebo $1.(0,1) + 1.(0,1) - 1.(1,1) = (0,0)$. (Nulový vektor v $\mathbb{R}^2$ je $(0,0)$.)

Ekvivalentne môžeme lineárnu nezávislosť definovať tak, že vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ sú lineárne nezávislé práve vtedy, keď platí implikácia

$$c_1\vec{\alpha}_1 + c_2\vec{\alpha}_2 + \cdots + c_n\vec{\alpha}_n = \vec{0} \qquad \Rightarrow \qquad c_1 = c_2 = \ldots = c_n = 0. \tag{4.2}$$

Táto formulácia lineárnej nezávislosti bude pre nás často výhodnejšia pri overovaní, či nejaké vektory sú lineárne nezávislé.

Príklad 4.3.11. Vektory $(1,0),(0,1)$ vo vektorovom priestore $\mathbb{R}^2$ sú lineárne nezávislé. Skutočne, z rovnosti $c_1(1,0) + c_2(0,1) = (c_1, c_2) = (0,0)$ vyplýva $c_1 = c_2 = 0$.

Poznámka 4.3.12. Aby sme si ozrejmili, že uvedené dve definície lineárnej nezávislosti sú skutočne ekvivalentné, potrebujeme si najprv pripomenúť, ako sa negujú výroky s kvantifikátormi.[2]

Pre negácie výrokov s kvantifikátormi platia dve jednoduché pravidlá (pozri 2.1.5):

$$\begin{aligned} \neg[(\forall x)P(x)] \quad &\Leftrightarrow \quad (\exists x)(\neg P(x)), \\ \neg[(\exists x)P(x)] \quad &\Leftrightarrow \quad (\forall x)(\neg P(x)). \end{aligned}$$

(Teda existenčný kvantifikátor sa mení na všeobecný a obrátene a výrok pod kvantifikátorom sa zneguje.)

My by sme radi overili, či (4.2) je skutočne negáciou definície lineárne závislých vektorov. Pokúsme sa teda najprv prepísať definíciu lineárne závislých vektorov. (Snáď jediným drobným problémom je, ako zapísať, že aspoň jeden zo skalárov $c_1, \ldots, c_n \in F$ je nenulový.)

Spomínanú definíciu by sme mohli zapísať takto

$$(\exists c_1, \ldots, c_n \in F)[c_1\vec{\alpha}_1 + \cdots + c_n\vec{\alpha}_n = 0 \wedge (c_1 \neq 0 \vee c_2 \neq 0 \vee \ldots \vee c_n \neq 0)].$$

Teraz už použitím pravidiel o negovaní výrokov s kvantifikátormi a de Morganových zákonov dostaneme

$$(\forall c_1, \ldots, c_n \in F)[c_1\vec{\alpha}_1 + \cdots + c_n\vec{\alpha}_n \neq 0 \vee (c_1 = 0 \wedge c_2 = 0 \wedge \ldots \wedge c_n = 0)].$$

Keď si uvedomíme, že $\neg P \vee Q$ je vlastne iný zápis implikácie $P \Rightarrow Q$ (inak povedané, $(\neg P \vee Q) \Leftrightarrow (P \Rightarrow Q)$ je tautológia, pozri úlohu 2.1.1) vidíme, že sme dostali

$$(\forall n \in \mathbb{N})(\forall c_1, \ldots, c_n \in F)(c_1\vec{\alpha}_1 + \cdots + c_n\vec{\alpha}_n = 0 \Rightarrow c_1 = c_2 = \ldots = c_n = 0),$$

čiže implikáciu (4.2).

Nasledujúce výsledky budú pre nás veľmi užitočné v nasledujúcej podkapitole.

Veta 4.3.13. *Nech V je vektorový priestor nad poľom F. Nech n je prirodzené číslo, $n \geq 2$ a $\vec{\alpha}_1, \ldots, \vec{\alpha}_n \in V$. Vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ sú lineárne závislé práve vtedy, keď niektorý z nich je lineárnou kombináciou ostatných.*

Dôkaz. $\boxed{\Rightarrow}$ Ak sú vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ lineárne závislé, znamená to, že platí rovnosť

$$c_1\vec{\alpha}_1 + \cdots + c_n\vec{\alpha}_n = \vec{0}$$

[2] Ako sme si už kedysi povedali, kvantifikátory sú len spôsobom na zápis istého druhu výrokov. Tu síce odvodíme ekvivalenciu týchto 2 definícií pomocou formálnych pravidiel pre prácu s kvantifikátormi, je to však presne to isté, čo dostaneme aj logickou úvahou, kvantifikátory nám poslúžia len na stručnejší, jednoduchší a prehľadnejší zápis týchto úvah.

pre nejaké $c_1, \ldots, c_n \in F$, ktoré nie sú všetky nulové. Zvoľme si niektorý nenulový index $c_i \neq 0$. Pretože $c_i \neq 0$, existuje inverzný prvok c_i^{-1}. Úpravou predchádzajúcej rovnosti dostaneme

$$\begin{aligned} -c_i\vec{\alpha}_i =& c_1\vec{\alpha}_1 + \cdots + c_{i-1}\vec{\alpha}_{i-1} + c_{i+1}\vec{\alpha}_{i+1} + \cdots + c_n\vec{\alpha}_n \\ -\vec{\alpha}_i =& c_i^{-1}c_1\vec{\alpha}_1 + \cdots + c_i^{-1}c_{i-1}\vec{\alpha}_{i-1} + c_i^{-1}c_{i+1}\vec{\alpha}_{i+1} + \cdots + c_i^{-1}c_n\vec{\alpha}_n \\ \vec{\alpha}_i =& -c_i^{-1}c_1\vec{\alpha}_1 - \ldots - c_i^{-1}c_{i-1}\vec{\alpha}_{i-1} - c_i^{-1}c_{i+1}\vec{\alpha}_{i+1} - \ldots - c_i^{-1}c_n\vec{\alpha}_n \end{aligned}$$

Teda $\vec{\alpha}_i$ je lineárna kombinácia ostatných vektorov.

$\boxed{\Leftarrow}$ Bez ujmy na všeobecnosti,[3] nech vektor, ktorý je lineárnou kombináciou ostatných, je vektor $\vec{\alpha}_1$. To znamená, že

$$\vec{\alpha}_1 = c_2\vec{\alpha}_2 + \cdots + c_n\vec{\alpha}_n,$$

čiže

$$-1.\vec{\alpha}_1 + c_2\vec{\alpha}_2 + \cdots + c_n\vec{\alpha}_n = \vec{0}.$$

Zistili sme, že $\vec{0}$ sa dá získať ako lineárna kombinácia vektorov $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$, pričom hneď prvý koeficient -1 je nenulový. □

Veta 4.3.14. *Nech V je vektorový priestor nad poľom F. Nech $\vec{\alpha}_1, \ldots, \vec{\alpha}_n \in V$ sú vektory také, že $\vec{\alpha}_1 \neq \vec{0}$. Vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ sú lineárne závislé práve vtedy, keď niektorý z nich je lineárnou kombináciou predchádzajúcich.*

Dôkaz. Implikácia $\boxed{\Leftarrow}$ vyplýva z predchádzajúcej vety.

Implikáciu $\boxed{\Rightarrow}$ dokážeme veľmi podobným spôsobom ako v predchádzajúcom dôkaze.

Ak vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ sú lineárne závislé, znamená to podľa (4.2), že

$$c_1\vec{\alpha}_1 + \cdots + c_n\vec{\alpha}_n = \vec{0}$$

pre nejaké $c_1, \ldots, c_n \in F$, pričom aspoň jedno c_i, $i \in \{1, 2, \ldots, n\}$ je nenulové.

Nech $k \in \{1, 2, \ldots, n\}$ je posledný index z tejto množiny, pre ktorý je c_k nenulové. (Taký index existuje, pretože množina $\{1, 2, \ldots, n\}$ je konečná. Navyše, platí $k \geq 2$, pretože $\vec{\alpha}_1 \neq \vec{0}$.)

Potom predchádzajúcu rovnicu môžeme prepísať do tvaru

$$c_1\vec{\alpha}_1 + c_2\vec{\alpha}_2 + \cdots + c_k\vec{\alpha}_k = \vec{0}$$

a úpravou dostaneme

$$c_k\vec{\alpha}_k = -c_1\vec{\alpha}_1 - c_2\vec{\alpha}_2 - \cdots - c_{k-1}\vec{\alpha}_{k-1}.$$

Pretože $c_k \neq 0$, existuje inverzný prvok c_k^{-1}. Keď predchádzajúcu rovnosť prenásobíme c_k^{-1} dostaneme

$$\vec{\alpha}_k = -c_k^{-1}c_1\vec{\alpha}_1 - c_k^{-1}c_2\vec{\alpha}_2 - \cdots - c_k^{-1}c_{k-1}\vec{\alpha}_{k-1},$$

teda $\vec{\alpha}_k$ je skutočne lineárnou kombináciou predchádzajúcich vektorov. □

Nasledujúca veta bude kľúčová pri definovaní dimenzie vektorového priestoru v nasledujúcej kapitole.

[3] Frázu „bez ujmy na všeobecnosti“ nájdete v matematických textoch dosť často. Myslí sa tým, že použijeme dodatočný argument, ktorý môže o niečo zjednodušiť zápis dôkazu alebo dôkaz, ale je zrejmé, že analogický dôkaz by platil aj bez tohoto predpokladu. Napríklad v tomto prípade nám výber vektora $\vec{\alpha}_1$ umožní jednoduchší zápis a navyše všeobecnú situáciu vieme previesť na tento prípad vhodným prečíslovaním vektorov. Iná možnosť by bola postupovať podobným postupom ako v predchádzajúcej časti dôkazu, znamenalo by to však o niečo komplikovanejší zápis.

Veta 4.3.15 (Steinitzova veta o výmene). *Nech V je vektorový priestor nad poľom F. Ak $V = [\vec{\alpha}_1, \ldots, \vec{\alpha}_n]$ (vektorový priestor V je generovaný vektormi $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$) a $\vec{\beta}_1, \ldots, \vec{\beta}_s \in V$ sú lineárne nezávislé vektory, tak*

(i) *$s \leq n$,*

(ii) *z vektorov $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ sa dá vybrať $n - s$ vektorov, ktoré spolu s vektormi $\vec{\beta}_1, \ldots, \vec{\beta}_s$ generujú V.*

Dôkaz. Matematickou indukciou vzhľadom na s.

1° Najprv uvažujme prípad, že $s = 1$. Vektor $\vec{\beta}_1$ je lineárne nezávislý, teda nenulový. Pretože $\vec{\beta}_1 \in V$, je vektor $\vec{\beta}_1$ lineárna kombinácia vektorov $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$. To znamená, že vektory $\vec{\beta}_1, \vec{\alpha}_1, \ldots, \vec{\alpha}_n$ sú lineárne závislé. Preto niektorý z nich je lineárnou kombináciou predchádzajúcich. Pritom to nemôže byť vektor $\vec{\beta}_1$, lebo $\vec{\beta}_1 \neq \vec{0}$.

Ak $\vec{\alpha}_i$ je lineárna kombinácia predchádzajúcich vektorov, tak podľa vety 4.3.8 $V = [\vec{\alpha}_1, \ldots, \vec{\alpha}_n] = [\vec{\beta}_1, \vec{\alpha}_1, \ldots, \vec{\alpha}_n] = [\vec{\beta}_1, \vec{\alpha}_1, \ldots, \vec{\alpha}_{i-1}, \vec{\alpha}_{i+1}, \ldots, \vec{\alpha}_n]$.

Pretože $V = [\vec{\alpha}_1, \ldots, \vec{\alpha}_n]$ obsahuje aspoň jeden nenulový vektor $\vec{\beta}_1$, platí $V \neq \{\vec{0}\}$ a $n \geq 1$.

2° Predpokladajme, že tvrdenie patrí pre číslo s. Budeme sa snažiť dokázať, že platí aj pre $s + 1$.

Máme teda daných $s+1$ lineárne nezávislých vektorov $\vec{\beta}_1, \ldots, \vec{\beta}_{s+1} \in V$. Podľa indukčného predpokladu vieme vektory $\vec{\beta}_1, \ldots, \vec{\beta}_s$ doplniť $n - s$ vektormi spomedzi vektorov $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ tak, aby generovali celý priestor. Ďalej platí $s \leq n$.

Predpokladajme, že by platilo $s = n$. To by znamenalo, že (podľa indukčného predpokladu) sa dajú vektory $\vec{\beta}_1, \ldots, \vec{\beta}_s$ doplniť $n - s = 0$ vektormi, čiže $V = [\vec{\beta}_1, \ldots, \vec{\beta}_s]$. Pretože $\vec{\beta}_{s+1} \in [\vec{\beta}_1, \ldots, \vec{\beta}_s]$, vektor $\vec{\beta}_{s+1}$ je lineárna kombinácia vektorov $\vec{\beta}_1, \ldots, \vec{\beta}_s$, čo je spor s tým, že vektory $\vec{\beta}_1, \ldots, \vec{\beta}_{s+1}$ sú lineárne nezávislé. Musí teda platiť $s < n$, čiže

$$s + 1 \leq n.$$

Bez ujmy na všeobecnosti môžeme predpokladať, že vektory, ktorými môžeme doplniť $\vec{\beta}_1, \ldots, \vec{\beta}_s$ sú vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_{n-s}$. (Takúto situáciu vieme dosiahnuť vhodným prečíslovaním vektorov $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$.) Platí teda $\vec{\beta}_{s+1} \in V = [\vec{\beta}_1, \ldots, \vec{\beta}_s, \vec{\alpha}_1, \ldots, \vec{\alpha}_{n-s}]$.

Z toho vyplýva, že vektory $\vec{\beta}_1, \ldots, \vec{\beta}_{s+1}, \vec{\alpha}_1, \ldots, \vec{\alpha}_{n-s}$ sú lineárne závislé, čiže niektorý z nich je lineárnou kombináciou predchádzajúcich vektorov. Nemôže to však byť žiadny z vektorov $\vec{\beta}_1, \ldots, \vec{\beta}_{s+1}$, lebo tieto vektory sú lineárne nezávislé. Musí to byť niektorý z $\vec{\alpha}_1, \ldots, \vec{\alpha}_{n-s}$, bez ujmy na všeobecnosti nech je to $\vec{\alpha}_{n-s}$. Z vety 4.3.8 potom dostaneme

$$V = [\vec{\beta}_1, \ldots, \vec{\beta}_{s+1}, \vec{\alpha}_1, \ldots, \vec{\alpha}_{n-s}] = [\vec{\beta}_1, \ldots, \vec{\beta}_{s+1}, \vec{\alpha}_1, \ldots, \vec{\alpha}_{n-(s+1)}].$$

□

Z dôkazu môžeme vidieť, prečo sa predchádzajúca veta nazýva veta o výmene. V indukčnom kroku sme vymenili jeden z vektorov $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ za vektor $\vec{\beta}_{s+1}$.

Všimnime si, že na konci predchádzajúceho dôkazu môže nastať aj situácia $n = s + 1$, vtedy zápis $\vec{\alpha}_1, \ldots, \vec{\alpha}_{n-(s+1)}$ predstavuje 0 vektorov. Možno trochu neobvyklý zápis – ale dá sa ľahko si uvedomiť, že prípad $n = s + 1$ by fungoval v podstate rovnako. (Nie sú tam problémy s tým, že by sme uvažovali lineárny obal prázdnej množiny vektorov – sú tam totiž aj vektory $\vec{\beta}_1, \ldots, \vec{\beta}_{s+1}$.)

Podobne podmienka $n \geq 2$ vo vete 4.3.13 a podmienka $\vec{\alpha}_1 \neq \vec{0}$ vo vete 4.3.14 slúžia práve nato, aby sme sa vyhli prípadu, že v dôkaze (alebo už priamo v tvrdení vety) sa vyskytne lineárny obal prázdnej množiny vektorov (ten sme totiž nedefinovali). Môžete si rozmyslieť, že keby sme definitoricky položili $[\emptyset] = \{\vec{0}\}$, teda lineárny obal prázdnej množiny by bol nulový vektorový priestor, prešli by dôkazy týchto viet aj po vynechaní spomínaných podmienok.

Cvičenia

Úloha 4.3.1. Dokážte, že vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n \in V$, kde $n \geq 2$, sú lineárne závislé práve vtedy, keď niektorý z nich je lineárnou kombináciou nasledujúcich.

Úloha 4.3.2. Nech $\vec{\alpha}, \vec{\beta}, \vec{\gamma}$ sú ľubovoľné vektory z vektorového priestoru V nad poľom $\mathbb{R}$. Potom $[\vec{\alpha}, \vec{\beta}, \vec{\gamma}] = [\vec{\alpha} + \vec{\beta}, \vec{\alpha} - \vec{\beta}, \vec{\gamma}]$.

Úloha 4.3.3. Nech $M = \{(x, y, z) \in \mathbb{R}^3; 2x + 3y + 5z = 0\}$. Ukážte, že M je vektorový podpriestor $\mathbb{R}^3$ a nájdite vektory, ktoré ho generujú.

Úloha 4.3.4. P_n označme množinu všetkých polynómov stupňa najviac n s reálnymi koeficientami. P_n je podpriestor vektorového priestoru všetkých zobrazení $f\colon \mathbb{R} \to \mathbb{R}$. Platí $P_n = [1, x, \ldots, x^n]$?

Úloha 4.3.5. Zistite, či dané vektory sú lineárne závislé v príslušnom vektorovom priestore:
a) (1,2,3), (1,3,2), (2,1,5) v $\mathbb{R}^3$,
b) (1,2,3), (1,3,2), (2,1,5), (1,127,3) v $\mathbb{R}^3$,
c) (1,3,4), (2,1,3), (3,1,4) v $\mathbb{Z}_5^3$
d) (1,3,4), (2,1,3), (3,1,4) v $\mathbb{Z}_7^3$.

Úloha 4.3.6. Zistite, či sú nasledujúce funkcie lineárne závislé vo vektorovom priestore všetkých funkcií z $\mathbb{R}$ do $\mathbb{R}$:
a) $x + 1$, x^2, x^3,
b) 1, $x + a$, $x^2 + bx + c$ (a, b, c môžu byť ľubovoľné reálne čísla),
c*) 1, $\cos x$, $\cos^2(\frac{x}{2})$,
d) x, $x(x-1)$, $x(x-1)(x-2)$,
e) 1, $\cos x$, $\cos 2x$.

Úloha 4.3.7. Ak $\vec{\alpha}$, $\vec{\beta}$, $\vec{\gamma}$ sú lineárne nezávislé vo vektorovom priestore V nad poľom $\mathbb{R}$, tak aj $\vec{\alpha} + \vec{\beta}$, $\vec{\alpha} + \vec{\gamma}$, $\vec{\beta} + \vec{\gamma}$ sú lineárne nezávislé. (Platilo by to aj vo vektorovom priestore nad poľom $\mathbb{Z}_2$?)

Úloha 4.3.8. Množina $\{\vec{\alpha}\}$ je lineárne nezávislá práve vtedy, keď $\vec{\alpha} \neq \vec{0}$. Dva vektory $\vec{\alpha}, \vec{\beta}$ sú lineárne závislé práve vtedy, keď jeden z nich je násobkom druhého (t.j. existuje $c \in F$ tak, že $c.\vec{\alpha} = \vec{\beta}$), alebo jeden z nich je $\vec{0}$.

Ak vektory $\vec{\alpha}, \vec{\beta}$ sú lineárne nezávislé, tak $\vec{\alpha}, \vec{\beta}, \vec{\gamma}$ sú lineárne závislé práve vtedy, keď $\vec{\gamma}$ je lineárna kombinácia vektorov $\vec{\alpha}, \vec{\beta}$.

Úloha 4.3.9*. Overte, že $\mathbb{R}$ je vektorový priestor nad poľom $\mathbb{Q}$. Dokážte, že v tomto priestore sú 1, $\sqrt{2}$ a $\sqrt{3}$ lineárne nezávislé.

Úloha 4.3.10. Nech $\vec{\alpha}, \vec{\beta}, \vec{\gamma}$ sú ľubovoľné vektory. Zistite, či sú tieto systémy vektorov lineárne závislé:
a) $\vec{\alpha}, \vec{\beta}, \vec{\alpha} + \vec{\beta}, \vec{\gamma}$, b) $\vec{\alpha}, \vec{\beta}, 0$, c) $\vec{\alpha}, \vec{\alpha}, \vec{\beta}, \vec{\gamma}$, d) $\vec{\alpha} + \vec{\beta} + \vec{\gamma}, \vec{\alpha} + \vec{\beta}, \vec{\alpha} + \vec{\gamma}, \vec{\beta} + \vec{\gamma}$.

Úloha 4.3.11. Nájdite 4 vektory v $\mathbb{R}^2$ tak, aby každé dva z nich boli lineárne nezávislé.

Úloha 4.3.12. Nech vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ sú lineárne nezávislé vektory v nejakom vektorovom priestore nad poľom $\mathbb{R}$. Sú aj vektory $\vec{\alpha}_1, \vec{\alpha}_1 + 2\vec{\alpha}_2, \ldots, \vec{\alpha}_1 + 2\vec{\alpha}_2 + \ldots + n\vec{\alpha}_n$ lineárne nezávislé?

4.4 Báza a dimenzia

V tejto podkapitole zadefinujeme pojmy báza a dimenzia vektorového priestoru. Pri dôkazoch základných výsledkoch o nich bude pre nás základným prostriedkom Steinitzova veta o výmene.

Definícia 4.4.1. Nech V je vektorový priestor. Hovoríme, že V je *konečnorozmerný* ak existuje taká konečná množina vektorov $\{\vec{\alpha}_1, \ldots, \vec{\alpha}_n\}$, že platí $[\vec{\alpha}_1, \ldots, \vec{\alpha}_n] = V$.

Inými slovami: konečnorozmerný vektorový priestor je priestor, ktorý je generovaný nejakou konečnou množinou vektorov.

Definícia 4.4.2. Nech V je vektorový priestor nad poľom F. Množinu vektorov $\{\vec{\alpha}_1, \ldots, \vec{\alpha}_n\}$ nazývame *bázou* priestoru V, ak

(i) vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ sú lineárne nezávislé,

(ii) $V = [\vec{\alpha}_1, \ldots, \vec{\alpha}_n]$.

(Stručne: Báza je taká množina <u>lineárne nezávislých</u> vektorov, ktorá <u>generuje</u> celý priestor.)

Príklad 4.4.3. Priestor $V = \{\vec{0}\}$ nemá bázu (pretože v ňom neexistujú žiadne lineárne nezávislé vektory). Je však konečnorozmerný, keďže $V = [\vec{0}]$.

Príklad 4.4.4. Nech F je pole. Ako F^n budeme označovať vektorový priestor všetkých usporiadaných n-tíc prvkov poľa F. Sčitovanie a násobenie skalárom definujeme po súradniciach (podobne ako v príklade 4.1.4 pre $F = \mathbb{R}$).

Ako $\vec{\varepsilon}_i$ označíme vektor, ktorý má na všetkých súradniciach 0, iba na i-tej súradnici 1, teda

$$\begin{aligned}
\vec{\varepsilon}_1 &= (1, 0, \ldots, 0),\\
\vec{\varepsilon}_2 &= (0, 1, \ldots, 0),\\
&\ldots\\
\vec{\varepsilon}_n &= (0, \ldots, 0, 1).
\end{aligned}$$

Vektory $\vec{\varepsilon}_1, \vec{\varepsilon}_2, \ldots, \vec{\varepsilon}_n$ tvoria bázu vektorového priestoru F^n. Túto bázu nazývame *štandardná báza F^n*.

Overme, že táto množina vektorov spĺňa podmienky z definície 4.4.2.

Ak $c_1.(1, 0, \ldots, 0) + c_2.(0, 1, \ldots, 0) + \ldots + c_n(0, \ldots, 0, 1) = (c_1, c_2, \ldots, c_n) = (0, 0, \ldots, 0)$, tak platí $c_1 = c_2 = \ldots = c_n = 0$, teda vektory $\vec{\varepsilon}_1, \vec{\varepsilon}_2, \ldots, \vec{\varepsilon}_n$ sú naozaj lineárne nezávislé.

Ak máme ľubovoľný vektor $(x_1, x_2, \ldots, x_n) \in F^n$, dá sa získať ako lineárna kombinácia $(x_1, x_2, \ldots, x_n) = x_1.(1, 0, \ldots, 0) + x_2.(0, 1, \ldots, 0) + \ldots + x_n(0, \ldots, 0, 1) = x_1\vec{\varepsilon}_1 + x_2\vec{\varepsilon}_2 + \cdots + x_n\vec{\varepsilon}_n$. Teda vektory $\vec{\varepsilon}_1, \vec{\varepsilon}_2, \ldots, \vec{\varepsilon}_n$ skutočne generujú celý priestor F^n.

Ako neskôr ukážeme, všetky konečnorozmerné vektorové priestory nad poľom F sú v istom zmysle podobné ako priestory F^n.

Veta 4.4.5. *Ľubovoľné dve bázy konečnorozmerného vektorového priestoru V majú rovnaký počet prvkov.*

Dôkaz. Nech $\{\vec{\alpha}_1, \ldots, \vec{\alpha}_n\}$ a $\{\vec{\beta}_1, \ldots, \vec{\beta}_s\}$ sú dve bázy toho istého vektorového priestoru V. Pretože $V = [\vec{\alpha}_1, \ldots, \vec{\alpha}_n]$ a vektory $\vec{\beta}_1, \ldots, \vec{\beta}_s$ sú lineárne nezávislé, podľa Steinitzovej vety o výmene platí

$$s \leq n.$$

Analogicky môžeme dokázať opačnú nerovnosť $n \leq s$. Tieto dve nerovnosti spolu dávajú rovnosť $n = s$. □

Veta 4.4.6. *Nech V je konečnorozmerný vektorový priestor. Ak $\vec{\beta}_1, \ldots, \vec{\beta}_s \in V$ sú lineárne nezávislé, tak sa dajú doplniť na bázu priestoru V.*

Dôkaz. Ak V je konečnorozmerný, tak podľa definície existujú vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ také, že $V = [\vec{\alpha}_1, \ldots, \vec{\alpha}_n]$. Na základe Steinitzovej vety môžeme vektory $\vec{\beta}_1, \ldots, \vec{\beta}_s$ doplniť niektorými z týchto vektorov tak, aby generovali celý priestor. Nech k je najmenší možný počet vektorov, ktorými ich môžeme takto doplniť. (Steinitzova veta hovorí, že sa to určite dá $n - s$ vektormi, nevylučuje však, že niekedy môže stačiť aj menší počet.) Bez ujmy na všeobecnosti, nech $V = [\vec{\beta}_1, \ldots, \vec{\beta}_s, \vec{\alpha}_1, \ldots, \vec{\alpha}_k]$.

Chceme dokázať, že vektory $\vec{\beta}_1, \ldots, \vec{\beta}_s, \vec{\alpha}_1, \ldots, \vec{\alpha}_k$ tvoria bázu priestoru V. Pretože sme ich vybrali tak, že generujú celý priestor, zostáva nám dokázať, že sú lineárne nezávislé. Postupujme sporom – predpokladajme, že by boli lineárne závislé. Potom je niektorý z nich lineárnou kombináciou predchádzajúcich vektorov. Bez ujmy na všeobecnosti, nech je to $\vec{\alpha}_k$. (Nemôže to byť žiadny z vektorov $\vec{\beta}_1, \ldots, \vec{\beta}_s$, pretože tieto vektory sú lineárne nezávislé.) Potom ale platí

$$V = [\vec{\beta}_1, \ldots, \vec{\beta}_s, \vec{\alpha}_1, \ldots, \vec{\alpha}_k] = [\vec{\beta}_1, \ldots, \vec{\beta}_s, \vec{\alpha}_1, \ldots, \vec{\alpha}_{k-1}],$$

čo je v spore s tým, že k je najmenší možný počet vektorov, ktorými sa vektory $\vec{\beta}_1, \ldots, \vec{\beta}_s$ dajú doplniť tak, aby generovali celý priestor V. □

Dôsledok 4.4.7. *Každý konečnorozmerný vektorový priestor $V \neq \{\vec{0}\}$ má bázu.*

Definícia 4.4.8. *Dimenziou* konečnorozmerného vektorového priestoru V nazývame počet prvkov ľubovoľnej jeho bázy. (Pre nulový priestor dodefinujeme $d(\{\vec{0}\}) = 0$.) Toto číslo označujeme $d(V)$.

Poznámka 4.4.9. Aby mala predchádzajúca definícia zmysel, museli sme najprv dokázať, že v konečnorozmernom vektorovom priestore existuje báza a že ľubovoľné dve bázy musia mať rovnaký počet prvkov; teda naša definícia nezávisí od voľby bázy.

S podobnou situáciou – že sa nejaký objekt zadefinuje, ale bude potrebné overiť správnosť definície – sa v matematike stretnete ešte veľakrát.

Príklad 4.4.10. Pretože vektory $\vec{\varepsilon}_1, \vec{\varepsilon}_2, \ldots, \vec{\varepsilon}_n$ tvoria bázu vektorového priestoru F^n, platí $d(F^n) = n$.

Dôsledok 4.4.11. *Ak V je konečnorozmený vektorový priestor a $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ sú lineárne nezávislé vo V, tak $n \leq d(V)$.*

Poznámka 4.4.12. Ak sme nejaký pojem definovali, vôbec to nemusí znamenať, že taký objekt aj naozaj existuje. Preto je predchádzajúci dôsledok dôležitý. (Hoci táto poznámka znie nesmierne naivne, skutočne sa možno často stretnúť s chybami takéhoto typu.)

Príklad 4.4.13. Vektory $(1, 2, 3), (2, 3, 4), (3, 4, 5), (4, 5, 6)$ sú lineárne závislé v $\mathbb{R}^3$.

Pretože vieme, že $d(\mathbb{R}^3) = 3$, nemôžu byť podľa predchádzajúcej vety v tomto priestore viac ako 3 lineárne nezávislé vektory.

Bázu sme definovali pomocou dvoch podmienok. Nasledujúca, veľmi užitočná veta hovorí, že ak už vieme, že nejaká množina vektorov má „správny“ počet prvkov, môžeme jednu z týchto podmienok vynechať.

Veta 4.4.14. *Nech V je konečnorozmerný vektorový priestor a $d(V) = n$. Nasledujúce podmienky sú ekvivalentné:*

(i) $\{\vec{\alpha}_1, \ldots, \vec{\alpha}_n\}$ *je báza priestoru V,*

(ii) *vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ sú lineárne nezávislé,*

(iii) $V = [\vec{\alpha}_1, \ldots, \vec{\alpha}_n]$.

Dôkaz. Implikácie (i) $\Rightarrow$ (ii), (i) $\Rightarrow$ (iii) vyplývajú priamo z definície.

(ii) $\Rightarrow$ (i): Ak máme n lineárne nezávislých vektorov $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$, podľa Steinitzovej vety ich môžeme doplniť $n - n = 0$ vektormi na množinu generujúcu celý priestor V. Teda nemusíme pridávať žiadne vektory a už množina $\{\vec{\alpha}_1, \ldots, \vec{\alpha}_n\}$ je báza (generuje V a je aj lineárne nezávislá).

(iii)$\Rightarrow$ (i): Sporom. Ak by boli vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ lineárne závislé, dali by sa niektoré z nich vynechať tak, aby stále tieto vektory generovali celý priestor V. Dostali by sme k vektorov, ktoré generujú V, pričom $k < n$. Súčasne by priestor V mal n-prvkovú bázu, ktorá je tvorená lineárne nezávislými vektormi. Zo Steinitzovej vety potom vyplýva $n < k$. Odvodili sme súčasnú platnosť nerovností $k < n$ aj $n < k$ – spor. □

Príklad 4.4.15. S použitím predchádzajúcej vety by sme mohli overiť, že vektory $\vec{\varepsilon}_1, \ldots, \vec{\varepsilon}_n$ tvoria bázu priestoru F^n. Prvý spôsob: Overili by sme, že generujú celý priestor. Druhý spôsob: Sú lineárne nezávislé. (Kým sme nevedeli, že $d(V) = n$, potrebovali sme overiť obe tieto vlastnosti.)

Veta 4.4.16. *Nech V je vektorový priestor. Vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ tvoria bázu priestoru V práve vtedy, keď každý vektor $\vec{\beta}$ sa dá <u>jednoznačne</u> vyjadriť ako*

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

Dôkaz. $\boxed{\Rightarrow}$ Pretože $V = [\vec{\alpha}_1, \ldots, \vec{\alpha}_n]$, každý vektor sa dá vyjadriť ako lineárna kombinácia vektorov $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$. Ešte treba overiť jednoznačnosť takéhoto vyjadrenia. Nech $\vec{\beta} = c_1\vec{\alpha}_1 + \cdots + c_n\vec{\alpha}_n = d_1\vec{\alpha}_1 + \cdots + d_n\vec{\alpha}_n$ sú dve vyjadrenia vektoru $\vec{\beta}$. Úpravou tejto rovnosti dostaneme

$$(c_1 - d_1)\vec{\alpha}_1 + \ldots + (c_n - d_n)\vec{\alpha}_n = \vec{0}.$$

Z lineárnej nezávislosti vektorov $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ vyplýva $c_i - d_i = 0$, čiže $c_i = d_i$ pre $i = 1, 2, \ldots, n$.

$\boxed{\Leftarrow}$ Pretože každý vektor z V sa dá vyjadriť pomocou vektorov $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$, tieto vektory generujú priestor V, čiže $V = [\vec{\alpha}_1, \ldots, \vec{\alpha}_n]$.

Ďalej vieme, že $\vec{0}$ sa dá vyjadriť ako lineárna kombinácia vektorov $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ jediným spôsobom. Z rovnosti $c_1\vec{\alpha}_1 + \cdots + c_n\vec{\alpha}_n = 0 = 0.\vec{\alpha}_1 + \ldots + 0.\vec{\alpha}_n$ teda vyplýva $c_1 = \ldots = c_n = 0$. Zistili sme, že vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ sú lineárne nezávislé. □

Ešte si ukážeme pár užitočných tvrdení o podpriestoroch konečnorozmerných priestorov.

Veta 4.4.17. *Ľubovoľný podpriestor S konečnorozmerného priestoru V je konečnorozmerný. Navyše, $d(S) \leq d(V)$.*

Dôkaz. Pretože $S \subseteq V$ a $d(V) = n$, číslo n udáva horné ohraničenie pre počet lineárne nezávislých vektorov z S. Nech $\vec{\alpha}_1, \ldots, \vec{\alpha}_k$ je najväčší systém lineárne nezávislých vektorov z S. Platí $k \leq n$. Stačí nám dokázať, že $\vec{\alpha}_1, \ldots, \vec{\alpha}_k$ tvorí bázu priestoru S, čiže $S = [\vec{\alpha}_1, \ldots, \vec{\alpha}_k]$.

Predpokladajme, že by existoval vektor $\vec{\alpha} \in S$, ktorý nepatrí do $[\vec{\alpha}_1, \ldots, \vec{\alpha}_k]$. Teda $\vec{\alpha}$ sa nedá vyjadriť ako lineárna kombinácia vektorov $\vec{\alpha}_1, \ldots, \vec{\alpha}_k$, čo znamená, že $\vec{\alpha}_1, \ldots, \vec{\alpha}_k, \vec{\alpha}$ sú lineárne nezávislé. To však je spor s predpokladom, že $\vec{\alpha}_1, \ldots, \vec{\alpha}_k$ je najväčší systém lineárne nezávislých vektorov v S. □

Úloha 4.4.1. Viete povedať, na ktorom mieste predchádzajúceho dôkazu sme využili, že V je konečnorozmerný?

Tvrdenie 4.4.18. *Ak S je podpriestor konečnorozmerného vektorového priestoru V a $d(S) = d(V)$, tak $S = V$.*

Dôkaz. Označme $n := d(S) = d(V)$. Nech $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ je báza S. Keďže je to n vektorov vo V, ktoré sú lineárne nezávislé, podľa vety 4.4.14 je to súčasne báza V. Teda $S = [\vec{\alpha}_1, \ldots, \vec{\alpha}_n] = V$. □

V tejto časti sme sa zaoberali iba konečnorozmernými vektorovými priestormi. (A takisto aj v nasledujúcich častiach nájdete veľa výsledkov, ktoré dokážeme iba pre konečnorozmerné vektorové priestory.) Nebolo by zle vyskúšať nájsť nejakého príkladu, ktorý nie je konečnorozmerný.

Príklad 4.4.19. Vektorový priestor $\mathbb{R}^{\mathbb{R}}$ všetkých zobrazení z $\mathbb{R}$ do $\mathbb{R}$ (príklad 4.1.4) nie je konečnorozmerný.

Predpokladajme, že by bol konečnorozmerný. Potom by existoval konečný počet funkcií $g_1, \ldots, g_n \colon \mathbb{R} \to \mathbb{R}$ tak, že $[g_1, \ldots, g_n] = \mathbb{R}^{\mathbb{R}}$. Ak sa nám podarí zostrojiť $n+1$ funkcií, ktoré sú v $\mathbb{R}^{\mathbb{R}}$ lineárne nezávislé, tak pomocou Steinitzovej vety ľahko dostaneme spor ($n+1 \leq n$).

Pokúsme sa teda definovať takéto funkcie. Pre $k = 0, 1, \ldots, n$ definujme zobrazenie $f_k \colon \mathbb{R} \to \mathbb{R}$ ako

$$f_k(x) = \begin{cases} 1, & \text{ak } x = k \\ 0, & \text{ak } x \neq k \end{cases}$$

Tvrdíme, že $f_0, \ldots, f_n$ sú lineárne nezávislé. Skutočne, ak platí rovnosť $c_0 f_0 + c_1 f_1 + \cdots + c_n f_n = 0$ (kde 0 označuje nulovú funkciu), tak pre každé $x \in \mathbb{R}$ máme

$$c_0 f_0(x) + c_1 f_1(x) + \cdots + c_n f_n(x) = 0.$$

Špeciálne, musí to platiť aj keď za x dosadíme $k = 0, 1, \ldots, n$. V takom prípade však dostávame $f_k(k) = 1$ a $f_j(k) = 0$, teda z predchádzajúce rovnosti priamo dostávame

$$c_k = 0.$$

Poznámka 4.4.20. Možno vám napadla otázka, či sa dá definovať báza aj pre nekonečnorozmerné vektorové priestory. Dá sa to, v tomto prípade sa zvykne nazývať *Hamelova báza.* Na jej zavedenie by sme však potrebovali podstatne väčšie vedomosti z teórie množín. Dokonca platí aj analógia vety 4.4.5, čiže aj ľubovoľné 2 Hamelove bázy majú rovnaký „počet“ prvkov – s tým rozdielom, že pre nekonečné množiny najprv treba definovať nový pojem, ktorý by zodpovedal počtu prvkov konečných množín (nazýva sa kardinalita množiny, viac sa o nej dozviete na predmete teória množín). Pre prípad, že by vás to zaujímalo a chceli by ste sa k tomuto problému časom vrátiť uvediem aj niekoľko odkazov na literatúru. V [NS] je pekným spôsobom dokázané, že ľubovoľná Hamelova báza toho istého priestoru musí mať rovnakú

„veľkosť“ (kardinalitu). V [ŠS, Kapitola 10.3] autori definujú Hamelovu bázu v špeciálnom prípade – pre reálne čísla ako vektorový priestor nad poľom $\mathbb{Q}$ (úloha* 4.3.9).

Ešte raz zdôrazňujem, že túto poznámku som sem vložil len kvôli tomu, aby ste vedeli, kde môžete hladať v prípade, že by ste sa k takémuto niečomu chceli neskôr vrátiť. (Zatiaľ by to pre vás bolo pomerne ťažké, potrebujete na to najprv poznať základné fakty o kardinalite množín. Tie sa dozviete na prednáške z teórie množín v 4. ročníku.)

Cvičenia

Úloha 4.4.2. Zistite, či dané vektory tvoria bázu v $\mathbb{R}^3$:
a) (1,2,3), (1,-2,3), (1,2,-3)
b) (1,1,1), (1,1,0), (1,0,1)
c) (1,0,0), (0,1,0), (0,0,1), (1,1,1).

Úloha 4.4.3. Zistite, či dané vektory tvoria bázu v $\mathbb{Z}_5^3$:
a) (1,2,3), (2,3,4), (0,3,1)
b) (1,0,0), (0,1,2), (2,1,3)
c) (0,1,2), (3,0,1), (1,0,2).

Úloha 4.4.4. P_n označme priestor všetkých polynómov stupňa najviac n. Overte, že $d(P_n) = n+1$ a že $1, x-1, \dots (x-1)^n$ je báza tohoto priestoru.

Úloha 4.4.5. Určte dimenziu priestoru $[\vec{\alpha}, \vec{\beta}, \vec{\gamma}]$, ak $\vec{\alpha} = (1,3,2,1)$, $\vec{\beta} = (4,9,5,4)$ a $\vec{\gamma} = (3,7,4,3)$.

Úloha 4.4.6. Ak sa to dá, doplňte dané vektory na bázu príslušného vektorového priestoru:
a) (1,1,2), (2,1,3) v $\mathbb{R}^3$,
b) x^2-1, x^2+1 v priestore polynómov stupňa najviac 3,
c) (1,2,3,0), (3,4,1,2) v $\mathbb{Z}_5^4$.

Úloha 4.4.7. Ak každý z vektorov $\vec{\beta}_1, \dots, \vec{\beta}_k$ je lineárnou kombináciou vektorov $\vec{\alpha}_1, \dots, \vec{\alpha}_m$, tak $d([\vec{\beta}_1, \dots, \vec{\beta}_k]) \leq d([\vec{\alpha}_1, \dots, \vec{\alpha}_m])$.

Úloha 4.4.8. Overte, že množina $S = \{f\colon \mathbb{R} \to \mathbb{R} : (\exists a, b \in \mathbb{R})(\forall x \in \mathbb{R}) f(x) = ax + b\}$ je podpriestor priestoru všetkých funkcií z $\mathbb{R}$ do $\mathbb{R}$. Nájdite funkcie $g, h \in S$ také, že $S = [g, h]$.

Úloha 4.4.9. Zistite, či $S = \{f\colon \mathbb{R} \to \mathbb{R}; f(x) = ax^2 + bx + c, a, b, c \in \mathbb{R}\}$ je vektorový podpriestor priestoru reálnych funkcií. Ak áno, nájdite, $g_1, g_2, g_3 \in S$ také, že $S = [g_1, g_2, g_3]$.

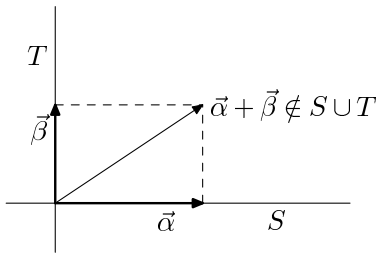
Úloha 4.4.10. Nájdite bázu pre každý vektorový podpriestor z úlohy 4.2.3.

4.5 Lineárne a direktné súčty podpriestorov

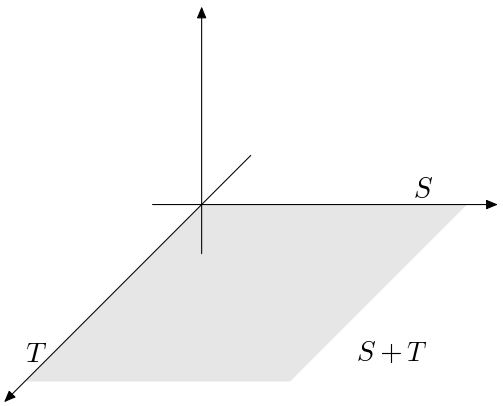
Už vieme, že prienik podpriestorov vektorového priestoru je tiež podpriestor (vety 4.2.8 a 4.2.10). Ako je to so zjednotením? Ak si zvolíme podpriestory $S = [(1,0,0)]$ a $T = [(0,1,0)]$ priestoru R^3, tak vidíme, že $S \cup T$ nie je vektorový podpriestor, lebo $(1,0,0) \in S \cup T$, $(0,1,0) \in S \cup T$, ale $(1,0,0) + (0,1,0) = (1,1,0) \notin S \cup T$.

Zaujímalo by nás, ako vyzerá najmenší podpriestor, ktorý obsahuje S aj T. Z obrázku 4.5 môžeme zistiť, že v tomto prípade je to podpriestor $[(1,0,0),(0,1,0)]$.

Ukážeme si, ako možno nájsť takýto podpriestor vo všeobecnosti, pre ľubovoľné dva podpriestory daného vektorového priestoru V.



Obr. 4.4: Zjednotenie 2 podpriestorov nemusí byť podpriestor



Obr. 4.5: Najmenší podpriestor obsahujúci S aj T

Veta 4.5.1. *Nech S, T sú vektorové podpriestory vektorového priestoru V nad poľom F. Potom*

$$S+T=\{\vec{\alpha}+\vec{\beta};\vec{\alpha}\in S,\vec{\beta}\in T\}$$

je podpriestorom vektorového priestoru V.

Táto veta vlastne hovorí, že množina všetkých vektorov, ktoré sa dajú získať ako súčty vektorov z S a z T, tvorí vektorový podpriestor. Všimnite si, že v predchádzajúcom príklade bolo $S+T=[(1,0,0),(0,1,0)]$.

Dôkaz. Overíme podmienky z definície vektorového podpriestoru. Množina $S+T$ je *neprázdna,* lebo $\vec{0}\in S$, $\vec{0}\in T$, čiže $\vec{0}=\vec{0}+\vec{0}\in S+T$.

$S+T$ je uzavretá na súčty: Ak $\vec{\gamma}_1,\vec{\gamma}_2\in S+T$, tak vektory $\vec{\gamma}_1$, $\vec{\gamma}_2$ sa dajú napísať v tvare $\vec{\gamma}_1=\vec{\alpha}_1+\vec{\beta}_1$, $\vec{\gamma}_2=\vec{\alpha}_2+\vec{\beta}_2$, kde $\vec{\alpha}_1,\vec{\alpha}_2\in S$ a $\vec{\beta}_1,\vec{\beta}_2\in T$. Potom $\vec{\gamma}_1+\vec{\gamma}_2=(\vec{\alpha}_1+\vec{\beta}_1)+(\vec{\alpha}_2+\vec{\beta}_2)=(\vec{\alpha}_1+\vec{\alpha}_2)+(\vec{\beta}_1+\vec{\beta}_2)$. (Využili sme komutatívnosť a asociatívnosť sčitovania.) Pretože S je vektorový podpriestor vektor $\vec{\alpha}_1+\vec{\alpha}_2$ patrí do S, podobne $\vec{\beta}_1+\vec{\beta}_2\in T$. Ukázali sme, že vektor $\vec{\gamma}_1+\vec{\gamma}_2$ sa dá napísať ako súčet vektora z S a vektora z T, teda $\vec{\gamma}_1+\vec{\gamma}_2\in S+T$.

$S+T$ je uzavretá na násobenie skalárom: Ak $\vec{\gamma}\in S+T$, tak $\vec{\gamma}=\vec{\alpha}+\vec{\beta}$ pre nejaké $\vec{\alpha}\in S$ a $\vec{\beta}\in T$. Nech $c\in F$ je ľubovoľný skalár. Potom $c\vec{\gamma}=c\vec{\alpha}+c\vec{\beta}$. Pritom $c\vec{\alpha}\in S$, $c\vec{\beta}\in T$, čiže $c\vec{\gamma}\in S+T$. □

Definícia 4.5.2. Ak S, T sú podpriestory vektorového podpriestoru V, tak vektorový podpriestor $S+T$ sa nazýva *lineárny súčet* podpriestorov S a T.

Vidno, že S aj T sú podmnožiny $S+T$, čiže $S+T$ obsahuje oba podpriestory S aj T. ($\vec{\alpha} \in S \Rightarrow \vec{\alpha} = \vec{\alpha} + \vec{0} \in S+T$, podobne pre T.) Priestor $S+T$ je skutočne najmenší vektorový podpriestor priestoru V, ktorý obsahuje S aj T. Ak totiž $S, T \subseteq U$ a U je vektorový podpriestor V, tak U musí obsahovať všetky súčty tvaru $\vec{\alpha} + \vec{\beta}$, pretože $\vec{\alpha} \in S \subseteq S+T$ a $\vec{\beta} \in T \subseteq S+T$.

Veta 4.5.3. *Nech S a T sú podpriestory vektorového priestoru V nad poľom F. Nech $S = [\vec{\alpha}_1, \ldots, \vec{\alpha}_n]$, $T = [\vec{\beta}_1, \ldots, \vec{\beta}_m]$. Potom $S+T = [\vec{\alpha}_1, \ldots, \vec{\alpha}_n, \vec{\beta}_1, \ldots, \vec{\beta}_m]$.*

Dôkaz. Je zrejmé, že vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n, \vec{\beta}_1, \ldots, \vec{\beta}_m$ patria do $S+T$. Keďže $S+T$ je vektorový podpriestor, musí potom platiť $[\vec{\alpha}_1, \ldots, \vec{\alpha}_n, \vec{\beta}_1, \ldots, \vec{\beta}_m] \subseteq S+T$.

Ešte treba dokázať opačnú inklúziu, čiže chceme ukázať, že

$$\vec{\gamma} \in S+T \;\Rightarrow\; \vec{\gamma} \in [\vec{\alpha}_1, \ldots, \vec{\alpha}_n, \vec{\beta}_1, \ldots, \vec{\beta}_m].$$

Ak $\vec{\gamma} \in S+T$, tak $\vec{\gamma} = \vec{\alpha} + \vec{\beta}$, kde $\vec{\alpha} \in [\vec{\alpha}_1, \ldots, \vec{\alpha}_n]$ a $\vec{\beta} \in [\vec{\beta}_1, \ldots, \vec{\beta}_m]$. To znamená, že existujú $c_1, \ldots, c_n, d_1, \ldots, d_m \in F$ tak, že $\vec{\alpha} = c_1\vec{\alpha}_1 + \ldots + c_n\vec{\alpha}_n$ a $\vec{\beta} = d_1\vec{\beta}_1 + \cdots + d_m\vec{\beta}_m$. Potom $\vec{\gamma} = c_1\vec{\alpha}_1 + \cdots + c_n\vec{\alpha}_n + d_1\vec{\beta}_1 + \cdots + d_m\vec{\beta}_m$, čiže $\vec{\gamma} \in [\vec{\alpha}_1, \ldots, \vec{\alpha}_n, \vec{\beta}_1, \ldots, \vec{\beta}_m]$. □

Veta 4.5.4. *Nech S, T sú podpriestory konečnorozmerného priestoru V. Potom*[4]

$$d(S) + d(T) = d(S+T) + d(S \cap T).$$

Dôkaz. Podľa vety 4.4.17 každý podpriestor konečnorozmerného priestoru je tiež konečnorozmerný, teda všetky dimenzie, ktoré vystupujú vo vete, sú skutočne definované.

V prípade, že $S \subseteq T$ máme $S+T = T$ a $S \cap T = S$, z čoho je zrejmé, že tvrdenie vety platí. Prípad $T \subseteq S$ je symetrický.

Zostáva teda prípad, že $S \nsubseteq T$ a $T \nsubseteq S$. Môžeme potom predpokladať, že $S \cap T$ má bázu $\vec{\gamma}_1, \ldots, \vec{\gamma}_r$. (V prípade, že $S \cap T = \{\vec{0}\}$, tak tento podpriestor nemá bázu – vtedy stačí zobrať $r = 0$ a vo zvyšku dôkazu môžeme postupovať úplne rovnako.) Tieto vektory patria do priestoru S a sú lineárne nezávislé, preto ich možno doplniť na bázu priestoru S, čiže $S = [\vec{\gamma}_1, \ldots, \vec{\gamma}_r, \vec{\alpha}_1, \ldots, \vec{\alpha}_s]$. Podobne môžeme v T zvoliť bázu $\vec{\gamma}_1, \ldots, \vec{\gamma}_r, \vec{\beta}_1, \ldots, \vec{\beta}_t$. Podľa vety 4.5.3 dostaneme

$$S+T = [\vec{\gamma}_1, \ldots, \vec{\gamma}_r, \vec{\alpha}_1, \ldots, \vec{\alpha}_s, \vec{\beta}_1, \ldots, \vec{\beta}_t].$$

Stačí, ak dokážeme, že tieto vektory sú lineárne nezávislé, lebo potom tvoria bázu v $S+T$ a máme $d(S+T) + d(S \cap T) = r + s + t + r = (r+s) + (r+t) = d(S) + d(T)$.

Nech $c_1\vec{\gamma}_1 + \cdots + c_r\vec{\gamma}_r + d_1\vec{\alpha}_1 + \cdots + d_s\vec{\alpha}_s + e_1\vec{\beta}_1 + \cdots + e_t\vec{\beta}_t = \vec{0}$. Potom $\vec{\delta} = c_1\vec{\gamma}_1 + \cdots + c_r\vec{\gamma}_r + d_1\vec{\alpha}_1 + \cdots + d_s\vec{\alpha}_s = -e_1\vec{\beta}_1 + \cdots + -e_t\vec{\beta}_t$ patrí do podpriestoru $S \cap T$. (Patrí do S, lebo je lineárnou kombináciou vektorov $\vec{\gamma}_1, \ldots, \vec{\gamma}_r, \vec{\alpha}_1, \ldots, \vec{\alpha}_s$. Do T patrí preto, že je lineárnou kombináciou vektorov $\vec{\beta}_1, \ldots, \vec{\beta}_t$.) Teda $\vec{\delta} = c'_1\vec{\gamma}_1 + \ldots + c'_2\vec{\gamma}_r$. Vďaka tomu, že vyjadrenie vektora pomocou prvkov bázy je jednoznačné, dostaneme, že $d_1 = \ldots = d_s = 0$ a $e_1 = \ldots = e_t = 0$. Potom máme $c_1\vec{\gamma}_1 + \cdots + c_r\vec{\gamma}_r = \vec{0}$ a (pretože $\vec{\gamma}_1, \ldots, \vec{\gamma}_r$ je báza) $c_1 = \ldots = c_r = 0$. □

Definícia 4.5.5. Nech S, T sú podpriestory vektorového priestoru V nad poľom F a nech $S \cap T = \{\vec{0}\}$. Potom podpriestor $S+T$ nazývame *direktný* (*priamy*) *súčet* podpriestorov S a T a označujeme ho $S \oplus T$.

[4] Tento vzorec pripomína vzorec pre počet prvkov zjednotenia dvoch množín $|S \cup T| = |S| + |T| - |S \cap T|$.

Veta 4.5.6. *Nech S, T, P sú podpriestory konečnorozmerného vektorového priestoru V nad poľom F. Tieto podmienky sú potom ekvivalentné:*

(i) $P = S \oplus T$

(ii) $P = S + T$ *a* $d(P) = d(S) + d(T)$

(iii) Ak $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ *je báza podpriestoru* S *a* $\vec{\beta}_1, \ldots, \vec{\beta}_m$ *je báza podpriestoru* T*, tak* $\vec{\alpha}_1, \ldots, \vec{\alpha}_n, \vec{\beta}_1, \ldots, \vec{\beta}_m$ *je báza podpriestoru* P*.*

(iv) $P = S + T$ *a každý vektor* $\vec{\gamma} \in P$ *sa dá jediným spôsobom vyjadriť v tvare* $\vec{\alpha} + \vec{\beta}$*, kde* $\vec{\alpha} \in S$ *a* $\vec{\beta} \in T$*. (T.j. ak* $\vec{\gamma} = \vec{\alpha}_1 + \vec{\beta}_1 = \vec{\alpha}_2 + \vec{\beta}_2$*, pričom* $\vec{\alpha}_1, \vec{\alpha}_2 \in S$ *a* $\vec{\beta}_1, \vec{\beta}_2 \in T$*, tak* $\vec{\alpha}_1 = \vec{\alpha}_2$ *a* $\vec{\beta}_1 = \vec{\beta}_2$*.)*

Dôkaz. $(i) \Rightarrow (ii)$ Podľa vety 4.5.4 dostaneme $d(S) + d(T) = d(S + T) + d(S \cap T) = d(P) + d(\{\vec{0}\}) = d(P)$.

$(ii) \Rightarrow (iii)$ Podľa vety 4.5.3 je $S + T = [\vec{\alpha}_1, \ldots, \vec{\alpha}_n, \vec{\beta}_1, \ldots, \vec{\beta}_m]$. Pretože $d(P) = n + m$ a našli sme $n + m$ vektorov, ktoré sú ho generujú, musia byť tieto vektory lineárne nezávislé a tvoria bázu.

$(iii) \Rightarrow (iv)$ Z vety 4.5.3 vyplýva, že $S+T = [\vec{\alpha}_1, \ldots, \vec{\alpha}_n, \vec{\beta}_1, \ldots, \vec{\beta}_m]$, teda $P = S+T$. Nech $\vec{\gamma} = \vec{\alpha}+\vec{\beta} = \vec{\alpha}'+\vec{\beta}'$. Potom $\vec{\alpha}-\vec{\alpha}'+\vec{\beta}-\vec{\beta}' = \vec{0}$. Ak vyjadríme vektory $\vec{\alpha}-\vec{\alpha}' \in S$ a $\vec{\beta}-\vec{\beta}' \in T$ pomocou báz týchto podpriestorov, čiže $\vec{\alpha}-\vec{\alpha}' = c_1\vec{\alpha}_1+\cdots+c_n\vec{\alpha}_n$ a $\vec{\beta}-\vec{\beta}' = d_1\vec{\beta}_1+\cdots+d_m\vec{\beta}_m$ dostaneme

$$c_1\vec{\alpha}_1 + \cdots + c_n\vec{\alpha}_n + d_1\vec{\beta}_1 + \cdots + d_m\vec{\beta}_m = \vec{0}.$$

Pretože vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n, \vec{\beta}_1, \ldots, \vec{\beta}_m$ tvoria bázu v P, sú lineárne nezávislé a $c_1 = \ldots = c_n = d_1 = \ldots = d_m = 0$. Z toho vyplýva, že $\vec{\alpha} - \vec{\alpha}' = \vec{0}$ a $\vec{\beta} - \vec{\beta}' = \vec{0}$, čiže $\vec{\alpha} = \vec{\alpha}'$ a $\vec{\beta} = \vec{\beta}'$.

$(iv) \Rightarrow (i)$ Potrebujeme ukázať iba že $S \cap T = \{\vec{0}\}$. Ak $\vec{\gamma} \in S \cap T$, tak $\vec{\gamma}$ môžeme vyjadriť ako súčet vektora z S a vektora z T týmito dvoma spôsobmi: $\vec{\gamma} = \vec{\gamma} + \vec{0} = \vec{0} + \vec{\gamma}$. Z jednoznačnosti potom vyplýva, že $\vec{\gamma} = \vec{0}$. □

Cvičenia

Úloha 4.5.1. Zistite[5] $d(U)$, $d(V)$, $d(U + V)$, $d(U \cap V)$, bázu $U + V$ a bázu $U \cap V$
a) v $\mathbb{R}^2$ pre $U = [(2, 5)]$, $V = [(1, 3)]$
b) v $\mathbb{R}^3$ pre $U = [(1, 2, 3), (-1, 2, 3)]$, $V = [(2, 1, 4), (-2, 1, 4)]$
c) v $\mathbb{R}^4$ pre $U = [(1, 0, 1, 0), (1, 0, 0, 1)]$, $V = [(1, 1, 1, 0), (1, 0, 1, 1)]$
d) v $\mathbb{R}^4$ pre $U = [(1, 2, 3, 4), (1, 1, 1, 1), (4, 3, 2, 1)]$, $V = [(1, 1, 0, 0), (0, 0, 1, 1), (1, 0, 0, 0)]$.
[a)1,1,2,0; b)2,2,3,1; c)2,2,3,1; d)2,3,4,1]

Úloha 4.5.2. Nech $T = [(1, 3, 2), (2, 1, 3), (3, 4, 0)]$ je podpriestor $(\mathbb{Z}_5)^3$. Existuje podpriestor S taký, že $(\mathbb{Z}_5)^3 = T \oplus S$? Ak áno, nájdite ho! Je tento podpriestor jednoznačne určený?

Úloha 4.5.3. Nech $S \neq T$ sú dva podpriestory vektorového priestoru F^3 nad poľom F a $d(S) = 2$, $d(T) = 2$. Dokážte, že $d(S \cap T) \geq 1$.

Úloha 4.5.4. Dokážte, že ak $\vec{e_1}, \ldots, \vec{e_k}$ je báza vektorového priestoru V, tak $V = [\vec{e_1}] \oplus \ldots \oplus [\vec{e_k}]$.

[5] Túto úlohu budeme riešiť neskôr, keď sa (v časti 5.2) naučíme jednoduchý spôsob ako nájsť dimenziu a bázu daného podpriestoru $\mathbb{R}^n$. Zaradil som ju však sem, pretože súvisí s témou tejto podkapitoly.

Kapitola 5

Lineárne zobrazenia a matice

5.1 Matice

Definícia 5.1.1. *Maticou* typu $m \times n$ nad poľom F nazývame ľubovoľnú tabuľku pozostávajúcu z prvkov poľa F, ktorá má m riadkov a n stĺpcov.

Matice zapisujeme v tvare

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

pričom a_{ij} označuje prvok v i-tom riadku a j-tom stĺpci.

Niekedy bude výhodné použiť stručnejší zápis $||a_{ij}||$, čím myslíme, že pre stručnosť niekedy len uvedieme predpis pre prvok i-teho riadku a j-teho stĺpca.

Príklad 5.1.2. $\left(\begin{smallmatrix} 2 & -1 & 3 \\ 4 & -2 & 5 \end{smallmatrix}\right)$ je matica typu 2×3 nad $\mathbb{R}$.

Definícia 5.1.3. Nech A, B sú matice typu $m \times n$ nad poľom F a $c \in F$.

(a) *Súčet matíc* $A = ||a_{ij}||$ a $B = ||b_{ij}||$ je matica $A + B = ||a_{ij} + b_{ij}||$.

(b) Matica $c.A = ||ca_{ij}||$ sa nazýva *c-násobok* matice A.

(Teda sčitovanie matíc a násobenie matice skalárom definujeme po súradniciach.)

Všimnime si, že súčet matíc definujeme len pre matice rovnakého typu.

Príklad 5.1.4. Uvažujme matice typu 2×2 nad $\mathbb{R}$.
$\left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)$
2. $\left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 2 & -2 \\ 0 & 2 \end{smallmatrix}\right)$

Veta 5.1.5. *Matice typu $m \times n$ nad poľom F s takto definovaným sčitovaním a násobením skalármi tvoria vektorový priestor nad poľom F.*

Dôkaz. Úloha 5.1.1. (Vlastne si stačí uvedomiť, že je to to isté ako priestor F^{mn} – matice typu $m \times n$ tvoria len inak zapísané mn-tice prvkov z F, operácie sú definované tak, že korešpondujú s priestorom F^{mn}.) □

Vďaka tomu, že matice tvoria vektorový priestor nad F môžeme využívať všetky vlastnosti, ktoré poznáme z vektorových priestorov, ako napríklad identitu $c(A + B) = cA + cB$.

Budeme používať označenie $-A = || - a_{ij}||$ pre *opačnú maticu* k matici A a $0 = ||0||$ pre *nulovú maticu.*

Definícia 5.1.6. Maticu typu $n \times n$ (teda takú, ktorá má rovnaký počet riadkov a stĺpcov) nazývame *štvorcová matica.*

Maticu

$$I = I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix}$$

typu $n \times n$, ktorá má na diagonále jednotky a mimo diagonály nuly, nazývame *jednotková matica.*

Štvorcová matica, ktorá má mimo diagonály iba nuly (t.j. $a_{ij} = 0$ pre $i \neq j$) sa nazýva *diagonálna matica.* (Príkladom diagonálnej matice je jednotková matica.)

Poznámka* 5.1.7. Jednotkovú maticu by sme mohli definovať ako $I = ||\delta_{ij}||$, kde

$$\delta_{ij} = \begin{cases} 1 & \text{ak } i = j, \\ 0 & \text{ak } i \neq j. \end{cases}$$

Takto definovaný symbol sa v matematike často používa, nazýva sa *Kroneckerov symbol.*

Často budeme používať aj pojem transponovanej matice.

Definícia 5.1.8. *Transponovaná matica* k matici A typu $m \times n$ je matica A^T typu $n \times m$ určená ako

$$A^T = ||a_{ji}||.$$

Štvorcová matica A sa nazýva *symetrická,* ak $A = A^T$ a *antisymetrická,* ak $A = -A^T$.

Teda A^T je vlastne matica A prevrátená symetricky podľa hlavnej diagonály.

Môžeme si všimnúť, že platí $I^T = I$, $(A^T)^T = A$, $(A + B)^T = A^T + B^T$ a $(cA)^T = cA^T$ (úloha 5.1.3).

Cvičenia

Úloha 5.1.1. Overte, že matice typu $m \times n$ nad poľom F (spolu so sčitovaním matíc a násobením matice skalárom) tvoria vektorový priestor nad F.

Úloha 5.1.2. Dokážte, že diagonálne matice tvoria podpriestor vektorového priestoru všetkých matíc typu $n \times n$.

Úloha 5.1.3. Nech matice A a B sú rovnakého typu. Dokážte, že potom $(A+B)^T = A^T + B^T$ a $(A^T)^T = A$. Čomu sa rovná $(c_1A + c_2B)^T$?

Úloha 5.1.4. Dokážte, že
a) množina všetkých symetrických matíc typu $n \times n$ a
b) množina všetkých antisymetrických matíc typu $n \times n$
tvoria podpriestory vektorového priestoru všetkých matíc typu $n \times n$. Je vektorový priestor matíc typu $n \times n$ direktný súčet týchto podpriestorov?

Úloha 5.1.5. Dokážte, že každá štvorcová matica sa dá napísať ako súčet symetrickej a antisymetrickej matice. Je vektorový priestor všetkých matíc typu $n \times n$ direktným súčtom priestorov z úlohy 5.1.4.

5.2 Riadková ekvivalencia a hodnosť matice

Definícia 5.2.1. *Podpriestorom prislúchajúcim matici* A typu $m \times n$ nad poľom F nazývame podpriestor priestoru F^n generovaný riadkami matice A. Označujeme ho V_A.

Aby sme rozumeli predchádzajúcej definícii, uvedomme si, že každý riadok matice je vlastne n-tica prvkov z F, čiže ho môžeme chápať ako vektor z F^n.

Ak matica A má riadky $\vec{\alpha}_1, \ldots, \vec{\alpha}_m$, tak podpriestor prislúchajúci tejto matici je vlastne $V_A = [\vec{\alpha}_1, \ldots, \vec{\alpha}_m]$.

Príklad 5.2.2. Pozrime sa na pár príkladov nad poľom $\mathbb{R}$.

$A = \left(\begin{smallmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{smallmatrix}\right) \quad V_A = [(1,0,1),(0,1,1)]$

$I = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \quad V_I = [(1,0,0),(0,1,0),(0,0,1)] = \mathbb{R}^3$

Vidíme, že jednotkovej matici I zodpovedá štandardná báza priestoru $\mathbb{R}^3$, preto jej prislúcha celý priestor $\mathbb{R}^3$.

Zavedieme teraz úpravy, ktoré nám umožnia jednoduchšie popísať priestor prislúchajúci danej matici.

Definícia 5.2.3. *Elementárne riadkové operácie* na matici A nad poľom F sú:

1. výmena 2 riadkov matice,
2. vynásobenie niektorého riadku matice <u>nenulovým</u> prvkom c poľa F,
3. pripočítanie násobku niektorého riadku k inému riadku.

Hovoríme, že matice A a B sú *riadkovo ekvivalentné* ak maticu B možno z A dostať pomocou konečnej postupnosti elementárnych riadkových operácií. Ak matice A a B sú riadkovo ekvivalentné, zapisujeme to ako $A \sim B$.

Príklad 5.2.4. Nasledujúce matice sme dostali z prvej pomocou elementárnych riadkových operácií. Sú to teda riadkovo ekvivalentné matice.

$$A = \begin{pmatrix} 1 & 2 & 5 \\ 2 & -2 & 1 \\ 3 & -2 & 3 \end{pmatrix} \overset{(1)}{\sim} \begin{pmatrix} 1 & 2 & 5 \\ 0 & -6 & -9 \\ 3 & -2 & 3 \end{pmatrix} \overset{(2)}{\sim} \begin{pmatrix} 1 & 2 & 5 \\ 0 & -6 & -9 \\ 0 & -8 & -12 \end{pmatrix} \overset{(3)}{\sim} \begin{pmatrix} 1 & 2 & 5 \\ 0 & 2 & 3 \\ 0 & 2 & 3 \end{pmatrix} \overset{(4)}{\sim} \begin{pmatrix} 1 & 2 & 5 \\ 0 & 2 & 3 \\ 0 & 0 & 0 \end{pmatrix} \overset{(5)}{\sim} \begin{pmatrix} 1 & 0 & 2 \\ 0 & 2 & 3 \\ 0 & 0 & 0 \end{pmatrix} \overset{(6)}{\sim} \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & \frac{3}{2} \\ 0 & 0 & 0 \end{pmatrix}$$

Elementárne riadkové operácie, ktoré sme použili sú:
(1) k 2.riadku sme pripočítali (-2)-násobok prvého (inak povedané, odčítali sme dvojnásobok),
(2) od 3.riadku sme odčítali 3-násobok prvého,
(3) 2.riadok sme vynásobili $-\frac{1}{3}$, 3.riadok sme vynásobili $-\frac{1}{4}$,
(4) od 2.riadku sme odpočítali tretí,
(5) od prvého riadku sme odpočítali druhý,
(6) druhý riadok sme vynásobili $\frac{1}{2}$ (čiže sme vlastne ho vydelili 2).

Poznámka 5.2.5. Podobným spôsobom sa dajú definovať aj elementárne stĺpcové operácie.

Poznámka 5.2.6. Je zrejmé, že ak $A \sim B$ a $B \sim C$, tak platí aj $A \sim C$. (Postupnosťou elementárnych riadkových operácií vieme z A dostať najprv B a potom z B dostať C.)

Okrem toho elementárne riadkové operácie možno obrátiť, preto ak $A \sim B$, tak platí aj $B \sim A$.

(Nie je ťažké si uvedomiť, že ak B dostaneme s A výmenou 2 riadkov, tak výmenou tých istých riadkov dostaneme z matice B pôvodnú maticu A. Takisto, ak použijeme vynásobenie niektorého riadku prvkom $c \neq 0$ poľa F, tak pôvodnú maticu dostaneme tak, že tento riadok vynásobíme c^{-1}. Ak sme v matici B získali k-ty riadok pripočítaním c-násobku j-teho riadku, čiže k-ty riadok novej matice pomocou riadkov pôvodnej matice vieme vyjadriť ako $\vec{\alpha}_k + c\vec{\alpha}_j$, tak $(\vec{\alpha}_k + c\vec{\alpha}_j) - c\vec{\alpha}_j = \vec{\alpha}_k$, čiže pripočítaním $(-c)$-násobku j-teho riadku ku k-temu dostaneme z B pôvodnú maticu.)

Veta 5.2.7. *Elementárne riadkové operácie nemenia podpriestor prislúchajúci danej matici.* (*Teda riadkovo ekvivalentným maticiam zodpovedá rovnaký podpriestor.*)

Dôkaz. Chceme ukázať, že ak na matici A, ktorej riadky sú $\vec{\alpha}_1, \ldots, \vec{\alpha}_m$, urobíme ktorúkoľvek z 3 elementárnych riadkových operácií, podpriestor prislúchajúci novej matici bude rovnaký ako podpriestor $V_A = [\vec{\alpha}_1, \ldots, \vec{\alpha}_m]$.

V prípade výmeny 2 riadkov je to jasné – ak vektory napíšeme v inom poradí, tak vygenerujú ten istý podpriestor.

Ďalšou elementárnou operáciou je vynásobenie niektorého riadku skalárom $c \neq 0$. Potom priestor prislúchajúci novej matici je $V_B = [\vec{\alpha}_1, \ldots, \vec{\alpha}_{i-1}, c\vec{\alpha}_i, \vec{\alpha}_{i+1}, \ldots, \vec{\alpha}_n]$. Pretože $c\vec{\alpha}_i \in V_A$, všetky vektory generujúce priestor V_B patria do V_A, preto tam patria aj všetky ich lineárne kombinácie, čo znamená $V_B \subseteq V_A$. Obrátenú inklúziu $V_A \subseteq V_B$ dostaneme rovnakým spôsobom: vektor $\vec{\alpha} = c^{-1}.(c\vec{\alpha})$ totiž patrí do V_B.

Zostáva nám posledná operácia – pripočítanie násobku niektorého riadku k inému riadku. Bez ujmy na všeobecnosti predpokladajme, že sme pripočítavali c-násobok druhého riadku k prvému (vektory môžeme ľubovoľne preusporiadať bez toho, aby sme zmenili podpriestor, ktorý generujú). Chceme teda ukázať, že $V_A = [\vec{\alpha}_1, \ldots, \vec{\alpha}_m] = [\vec{\alpha}_1 + c\vec{\alpha}_2, \vec{\alpha}_2, \ldots, \vec{\alpha}_m] = V_B$. Každý z vektorov generujúcich V_B je lineárna kombinácia vektorov $\vec{\alpha}_1, \ldots, \vec{\alpha}_m$, preto platí $V_B \subseteq V_A = [\vec{\alpha}_1, \ldots, \vec{\alpha}_m]$. Obrátene, vektor $\vec{\alpha}_1 = (\vec{\alpha}_1 + c\vec{\alpha}_2) - c\vec{\alpha}_2$ je lineárna kombinácia vektorov, ktoré generujú V_B, preto platí aj $V_A \subseteq V_B$. □

Definícia 5.2.8. Matica A je *redukovaná trojuholníková matica,* ak:

(i) Vedúci (=prvý nenulový) prvok každého riadku matice je 1.

(ii) Každý stĺpec obsahujúci vedúci prvok niektorého riadku má prvky v ostatných riadkoch nulové.

(iii) Nulové riadky ležia pod nenulovými riadkami.

(iv) Vedúci prvok ľubovoľného nenulového riadku je napravo od vedúcich prvkov všetkých nenulových riadkov nad ním a naľavo od vedúcich prvkov riadkov pod ním (t.j. vedúce riadky sú usporiadané zľava doprava).

Napríklad matica $\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & \frac{3}{2} \\ 0 & 0 & 0 \end{pmatrix}$, ktorú sme dostali v príklade 5.2.4 je redukovaná trojuholníková matica.

Ľubovoľná redukovaná trojuholníková matica vyzerá zhruba takto:

$$\begin{pmatrix} 0 & \ldots & 0 & \boxed{1} & * & 0 & * & 0 & * & \ldots & * \\ 0 & \ldots & 0 & 0 & 0 & \boxed{1} & * & 0 & * & \ldots & * \\ 0 & \ldots & 0 & 0 & 0 & 0 & 0 & \boxed{1} & * & \ldots & * \\ 0 & \ldots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots & 0 \\ 0 & \ldots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots & 0 \end{pmatrix}$$

V predchádzajúcej schéme $*$ označuje miesta, kde môže byť ľubovoľný prvok (nulový alebo nenulový). Vidíme, že vedúce jednotky (vyznačené štvorčekom) idú zľava doprava

Veta 5.2.9. *Každá matica nad poľom F je riadkovo ekvivalentná s nejakou redukovanou trojuholníkovou maticou.*

Dôkaz. Nech A je matica typu $m \times n$.

Tvrdenie vety dokážeme indukciou vzhľadom na m – počet riadkov matice A.

Ak $m = 1$, tak máme jediný riadok. V prípade, že je tento riadok nulový, matica už je v redukovanom trojuholníkovom tvare. Ak nie, tak tento riadok má tvar $(0, \ldots, 0, a_{1s}, a_{1,s+1}, \ldots, a_{1n})$,

kde a_{1s} je prvý nenulový prvok v danom riadku. Vynásobením a_{1s}^{-1} dostaneme maticu $(0, \ldots, 0, 1, a_{1s}^{-1}a_{1,s+1}, \ldots, a_{1s}^{-1}a_{1n})$, čiže vedúci prvok jej jediného riadku je 1 a táto matica je v redukovanom trojuholníkovom tvare.

Indukčný krok: predpokladáme, že tvrdenie vety platí pre každú maticu, ktorá má m riadkov, chceme dokázať, že platí aj pre ľubovoľnú maticu A typu $(m+1) \times n$.

Ak A je nulová matica, tak je v redukovanom trojuholníkovom tvare. V opačnom prípade, nech s je prvý stĺpec, ktorý je nenulový. Teda tento stĺpec obsahuje aspoň jeden nenulový prvok.

$$\begin{pmatrix} 0 & \ldots & 0 & a_{1s} & * & * & * & a_{1n} \\ 0 & \ldots & 0 & * & * & * & * & * \\ 0 & \ldots & 0 & a_{ks} \neq 0 & * & * & * & a_{ks} \\ 0 & \ldots & 0 & * & * & * & * & * \\ 0 & \ldots & 0 & a_{m+1,s} & * & * & * & a_{ns} \end{pmatrix}$$

Výmenou riadkov vieme dostať maticu, ktorá má v s-tom stĺpci nenulový prvok už v prvom riadku. (Ak to spĺňa už pôvodná matica, nie je potrebné vymieňať riadky.)

$$\begin{pmatrix} 0 & \ldots & 0 & b_{1s} \neq 0 & * & * & * & * \\ 0 & \ldots & 0 & b_{2s} & * & * & * & * \\ 0 & \ldots & 0 & \vdots & * & * & * & * \\ 0 & \ldots & 0 & b_{ks} & * & * & * & * \\ 0 & \ldots & 0 & \vdots & * & * & * & * \\ 0 & \ldots & 0 & b_{m+1,s} & * & * & * & * \end{pmatrix}$$

Aby sme v prvom riadku dostali vedúcu jednotku, vynásobíme ho b_{1s}^{-1}.

$$\begin{pmatrix} 0 & \ldots & 0 & 1 & * & * & * & * \\ 0 & \ldots & 0 & b_{2s} & * & * & * & * \\ 0 & \ldots & 0 & \vdots & * & * & * & * \\ 0 & \ldots & 0 & b_{ks} & * & * & * & * \\ 0 & \ldots & 0 & \vdots & * & * & * & * \\ 0 & \ldots & 0 & b_{m+1,s} & * & * & * & * \end{pmatrix}$$

Teraz vieme vynulovať všetky ostatné prvky v s-tom stĺpci – na to stačí od k-teho riadku (pre $k = 2, 3, \ldots, m+1$) odpočítať b_{ks}-násobok prvého riadku.

$$\begin{pmatrix} 0 & \ldots & 0 & 1 & * & * & * & * \\ 0 & \ldots & 0 & 0 & c_{2,s+1} & \ldots & \ldots & c_{2,n} \\ 0 & \ldots & 0 & \vdots & * & * & * & * \\ 0 & \ldots & 0 & 0 & c_{k,s+1} & \ldots & \ldots & c_{k,n} \\ 0 & \ldots & 0 & \vdots & * & * & * & * \\ 0 & \ldots & 0 & 0 & c_{m+1,s+1} & \ldots & \ldots & c_{m,n} \end{pmatrix}$$

Teraz nastala správna chvíľa použiť indukčný predpoklad – podľa neho vieme podmaticu pozostávajúcu zo všetkých riadkov predchádzajúcej matice okrem prvého upraviť na redukovanú trojuholníkovú maticu. Takto dostaneme maticu tvaru, ktorý schematicky znázorníme takto:

$$\begin{pmatrix} 0 & \ldots & 0 & 1 & * & * & * & * \\ 0 & \ldots & 0 & 0 & \boxed{1} & 0 & * & 0 \\ 0 & \ldots & 0 & 0 & 0 & \boxed{1} & * & 0 \\ 0 & \ldots & 0 & 0 & 0 & 0 & 0 & \boxed{1} \\ 0 & \ldots & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \ldots & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Inak povedané, podmatica pozostávajúca z riadkov 2 až $m+1$ spĺňa definíciu redukovanej trojuholníkovej matice. Jediná podmienka, z definície redukovanej trojuholníkovej matice, ktorá môže byť narušená v celej matici, je, že v niektorom zo stĺpcov obsahujúcich vedúcu jednotku môže táto matica obsahovať nenulový prvok. Pripočítaním vhodného násobku týchto riadkov vieme aj tieto prvky matice vynulovať. (Presnejšie to môžeme zapísať takto: označme prvky prvého riadku v $(s+1)$-vom až n-tom stĺpci. Nech stĺpce obsahujúce vedúce jednotky sú $i_2, i_3, \ldots, i_k$. Potom od prvého riadku odpočítame c_{1,i_2}-násobok 2.riadku, c_{1,i_3}-násobok 3.riadku, atď.)

$$\begin{pmatrix} 0 & \ldots & 0 & 1 & 0 & 0 & * & 0 \\ 0 & \ldots & 0 & 0 & \boxed{1} & 0 & * & 0 \\ 0 & \ldots & 0 & 0 & 0 & \boxed{1} & * & 0 \\ 0 & \ldots & 0 & 0 & 0 & 0 & 0 & \boxed{1} \\ 0 & \ldots & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \ldots & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Z naznačených úprav je vidno, že výsledná matica je skutočne redukovaná trojuholníková matica. □

Predchádzajúci dôkaz vlastne súčasne popisuje aj algoritmus, ako môžeme upraviť ľubovoľnú maticu na redukovaný trojuholníkový tvar.

Ako príklad úpravy na redukovanú trojuholníkovú maticu nám môže opäť poslúžiť príklad 5.2.4.

Zatiaľ sme si povedali, čo sú redukované trojuholníkové matice a vysvetlili sme si postup, akým môžeme z ľubovoľnej matice pomocou elementárnych riadkových úprav dostať redukovanú trojuholníkovú maticu. Teraz by sme chceli ukázať, prečo sú redukované trojuholníkové matice užitočné.

Veta 5.2.10. *Nenulové riadky redukovanej trojuholníkovej matice sú lineárne nezávislé.*

Najprv ilustrujme túto vetu na príklade. Opäť použijeme redukovanú trojuholníkovú maticu z príkladu 5.2.4.

Príklad 5.2.11. Riadky redukovanej trojuholníkovej matice z príkladu 5.2.4 sú $\vec{\alpha} = (1, 0, 2)$ a $\vec{\beta} = (0, 1, \frac{3}{2})$. Rovnosť $c\vec{\alpha} + d\vec{\beta} = \vec{0}$ znamená, že

$$c(1, 0, 2) + d(0, 1, \frac{3}{2}) = (c, d, 2c + \frac{3}{2}d) = (0, 0, 0),$$

z čoho dostaneme (porovnaním prvých 2 súradníc) $c = 0$ a $d = 0$. Platí teda implikácia $c\vec{\alpha} + d\vec{\beta} = \vec{0} \Rightarrow c = d = 0$, čiže vektory $\vec{\alpha}$ a $\vec{\beta}$ sú lineárne nezávislé.

Videli sme, že dôležité boli tie súradnice, na ktorých sa nachádzajú vedúce jednotky. V nasledujúcom dôkaze postupujeme takmer identicky ako v príklade, ktorý sme práve uviedli.

Dôkaz. Nech $\vec{\alpha}_1, \ldots, \vec{\alpha}_k$ sú nenulové riadky redukovanej trojuholníkovej matice A. Nech $i_1, \ldots, i_k$ sú stĺpce s vedúcimi jednotkami.

Vektor $c_1\vec{\alpha}_1 + \cdots + c_k\vec{\alpha}_k$ má na mieste i_j prvok c_j (pre $j = 1, 2, \ldots, k$), takže rovnosť $c_1\vec{\alpha}_1 + \cdots + c_k\vec{\alpha}_k = \vec{0}$ implikuje $c_j = 0$ (pretože nulový vektor má na tomto mieste nulu). Zistili sme, že platí $c_1\vec{\alpha}_1 + \cdots + c_k\vec{\alpha}_k = \vec{0} \Rightarrow c_1 = c_2 = \ldots = c_k = 0$, čiže vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_k$ sú skutočne lineárne nezávislé. □

Definícia 5.2.12. *Hodnosť matice A* je dimenzia priestoru V_A prislúchajúceho tejto matici. Označujeme ju $h(A)$.

Z tejto definície máme rovnosť $h(A) = d(V_A)$ a pretože elementárne riadkové operácie nemenia priestor prislúchajúci danej matici (veta 5.2.7), nemenia ani hodnosť matice.

Z vety 5.2.10 vyplýva, že hodnosť redukovanej trojuholníkovej matice je počet jej nenulových riadkov. Teda hodnosť matice môžeme rátať pomocou úpravy na redukovanú trojuholníkovú maticu. Pre maticu z príkladu 5.2.4 dostaneme $h(A) = 2$.

Okrem toho, že redukované trojuholníkové matice sú užitočné na výpočet hodnosti (a tým aj výpočet dimenzie podpriestoru generovaného nejakými zadanými vektormi), dajú sa využiť aj na to, aby sme zistil, či nejaký vektor patrí do podpriestoru V_A.

Príklad 5.2.13. V príklade 5.2.4 sme ukázali, že matice $A = \begin{pmatrix} 1 & 2 & 5 \\ 2 & -2 & 1 \\ 3 & -2 & 3 \end{pmatrix}$ a $B = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & \frac{3}{2} \\ 0 & 0 & 0 \end{pmatrix}$ sú riadkovo ekvivalentné čo znamená, že $V_A = V_B = [(1, 0, 2), (0, 1, \frac{3}{2})]$.

Pokúsme sa zistiť, či vektor $\vec{\alpha} = (1, 4, 4)$ patrí do V_A. Ak to platí, musí byť tento vektor lineárnou kombináciou vektorov $(1, 0, 2)$ a $(0, 1, \frac{3}{2})$. Dostávame teda rovnosť

$$(1, 4, 4) = c_1(1, 0, 2) + c_2(0, 1, \frac{3}{2}) = (c_1, c_2, 2c_1 + \frac{3}{2}c_2).$$

Porovnaním prvých dvoch súradníc dostaneme $c_1 = 1$ a $c_2 = 4$. Vektor na pravej strane poslednej rovnice má potom ale tretiu súradnicu rovnú $2.1 + \frac{3}{2}.4 = 8 \neq 4$, čiže vektor $\vec{\alpha}$ nepatrí do V_A.

Postup z predchádzajúceho príkladu sa dá použiť na dôkaz tohoto tvrdenia:

Lema 5.2.14. *Nech A je redukovaná trojuholníková matica typu $m \times n$ nad poľom F. Označme jej nenulové riadky $\vec{\alpha}_1, \ldots, \vec{\alpha}_k$ a ako $i_1, \ldots, i_k$ označme čísla stĺpcov, v ktorých sú vedúce jednotky. Potom $\vec{\alpha} = (c_1, \ldots, c_n) \in V_A$ práve vtedy, keď $\vec{\alpha} = c_{i_1}\vec{\alpha}_1 + c_{i_2}\vec{\alpha}_2 + \ldots + c_{i_k}\vec{\alpha}_k$.*

Dôkaz. Ak $\vec{\alpha} \in V_A$, tak $\vec{\alpha}$ je lineárnou kombináciou vektorov $\vec{\alpha}_1, \ldots, \vec{\alpha}_k$, čiže $\vec{\alpha} = d_1\vec{\alpha}_1 + \cdots + d_k\vec{\alpha}_k$

Pozrime sa, aká je i_j-ta súradnica vektoru $\vec{\alpha} = d_1\vec{\alpha}_1 + \cdots + d_k\vec{\alpha}_k$, pre ľubovoľné $j = 1, 2, \ldots, k$. Na tejto zložke majú vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_k$ nulu s výnimkou vektora α_j, ktorý tam má 1. Preto na i_j-tej súradnici vektora $d_1\vec{\alpha}_1 + \cdots + d_k\vec{\alpha}_k$ je d_j, dostávame rovnosť $d_j = c_{i_j}$. Zistili sme, že koeficienty lineárnej kombinácie sú skutočne rovné $c_{i_1}, c_{i_2}, \ldots, c_{i_k}$.

Obrátená implikácia je zrejmá. □

Veta 5.2.15. *Ak A a B sú redukované trojuholníkové matice rovnakého typu $m \times n$ nad poľom F a $V_A = V_B$, tak $A = B$.*

Dôkaz. Aby sme ukázali, že 2 redukované trojuholníkové matice sa rovnajú, stačí dokázať, že vedúce jednotky sú v rovnakých stĺpcoch a v ostatných stĺpcoch obsahujú matice rovnaké prvky.

Pretože $h(A) = h(B)$, tieto matice majú rovnaký počet nenulových riadkov. Označme ho k. Nenulové riadky matice A označme $\vec{\alpha}_1, \ldots, \vec{\alpha}_k$ a $i_1 < i_2 < \ldots < i_k$ nech sú čísla stĺpcov, ktoré obsahujú vedúce jednotky. Podobne nenulové riadky matice B označme $\vec{\beta}_1, \ldots, \vec{\beta}_k$ a nech vedúce jednotky tejto matice sú v stĺpcoch $j_1 < j_2 < \ldots < j_k$.

Postupujme sporom. Predpokladajme, že by vedúce jednotky neboli v rovnakých stĺpcoch. Nech t je prvý index, kde $i_t \neq j_t$. Bez ujmy na všeobecnosti môžeme predpokladať $i_t < j_t$. Vektor $\vec{\alpha}_t$ má na miestach $i_1, \ldots, i_{t-1}$ nuly. Preto

$$\vec{\alpha}_t = 0\vec{\beta}_1 + \ldots + 0\vec{\beta}_{t-1} + c_t\vec{\beta}_t + c_{t+1}\vec{\beta}_{t+1} + \ldots + c_k\vec{\beta}_k.$$

Vektor na pravej strane tejto rovnosti má na prvých $j_t - 1$ miestach 0, čiže ju má aj na mieste i_t, čo je spor (keďže sa má rovnať vektoru $\vec{\alpha}_t$, ktorý tam má prvok 1).

Zistili sme, že predpoklad $i_t \neq j_t$ vedie k sporu, preto $i_t = j_t$.

Teraz stačí ukázať, že pre všetky $t = 1, 2, \ldots, k$ platí $\vec{\alpha}_t = \vec{\beta}_t$ – to znamená, že aj ostatné prvky matíc A a B sa rovnajú.

Vektor $\vec{\alpha}_t$ má 0 na miestach $i_1, \ldots, i_{t-1}$ aj $i_{t+1}, \ldots, i_k$ a na mieste i_t má jednotku. Podľa lemy 5.2.14 teda $\vec{\alpha}_t = 0\vec{\beta}_1 + \ldots + 0\vec{\beta}_{t-1} + 1\vec{\beta}_t + 0\vec{\beta}_{t+1} + 0\vec{\beta}_k$, čiže $\vec{\alpha}_t = \vec{\beta}_t$. □

Na získanie lepšieho porozumenia predchádzajúceho dôkazu je možno dobre si ukázať jeho najdôležitejší krok na konkrétnom príklade.

Príklad 5.2.16. Majme redukovanú trojuholníkovú maticu

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

ktorá má vedúce jednotky v prvom a treťom stĺpci.

Predpokladajme, že by existovala redukovaná trojuholníková matica taká, že $V_A = V_B$ ale táto matica by mala vedúce jednotky v prvom a štvrtom stĺpci, čiže by mala tvar

$$B = \left(\begin{smallmatrix} 1 & b_{12} & b_{13} & 0 & b_{15} \\ 0 & 0 & 0 & 1 & b_{25} \end{smallmatrix}\right)$$

To by znamenalo, že $(0, 0, 1, 1, 2) \in V_B$ a podľa lemy 5.2.14 z toho dostaneme $(0, 0, 1, 1, 2) = 0.(1, b_{12}, b_{13}, 0, b_{15}) + 1.(0, 0, 0, 1, b_{25})$, čiže $(0, 0, 1, 1, 2) = (0, 0, 0, 1, b_{25})$; ale tieto vektory sa líšia na tretej súradnici, teda uvedená rovnosť nemôže platiť.

Iný spôsob, ako môžeme ukázať, že $V_A \neq V_B$: Ak by sa tieto podpriestory rovnali, tak by platilo $(0, 0, 0, 1, b_{25}) \in V_A = [(1, 1, 0, 2, 1), (0, 0, 1, 1, 2)]$. Z lemy 5.2.14 potom dostaneme $(0, 0, 0, 1, b_{25}) = 0.(1, 1, 0, 2, 1) + 0.(0, 0, 1, 1, 2) = (0, 0, 0, 0, 0)$. Dostali sme teda rovnosť nulového a nenulového vektoru, čo je spor.

Predchádzajúce vety môžeme zhrnúť nasledovne.

Dôsledok 5.2.17. *Nech A a B sú matice typu $m \times n$ nad poľom F. Nasledovné podmienky sú ekvivalentné:*

(i) *A a B sú riadkovo ekvivalentné,*

(ii) *$V_A = V_B$,*

(iii) *A a B sú riadkovo ekvivalentné s tou istou redukovanou trojuholníkovou maticou.*

Dôkaz. Veta 5.2.7 vlastne znamená implikáciu (i) ⇒ (ii).

Podľa vety 5.2.9 je A riadkovo ekvivalentná s nejakou redukovanou trojuholníkovou maticou A' a B je ekvivalentná s redukovanou trojuholníkovou maticou B'. Pretože $V_{B'} = V_B = V_A = V_{A'}$, podľa vety 5.2.15 $A' = B'$. Tým je dokázaná implikácia (ii) ⇒ (iii).

Podľa poznámky 5.2.6, ak $A \sim T$ a $B \sim T$ (T je redukovaná trojuholníková matica), tak aj $A \sim B$. Teda platí aj implikácia (iii) ⇒ (i). □

Poznámka 5.2.18. Postup z príkladu 5.2.13 a lemy 5.2.14 môžeme použiť na akúsi „polovičnú skúšky správnosti“ pri počítaní redukovanej trojuholníkovej matice. Pretože podobný postup sa dá použiť aj v iných situáciach, vysvetlime si ho trochu podrobnejšie.

Z dôsledku 5.2.17 vieme, že ak matica A je podobná redukovanej trojuholníkovej matici B, tak $V_A = V_B$. Túto rovnosť síce nevieme priamo overiť, vieme však ľahko zistiť, či $V_A \subseteq V_B$ (tak, že postupne overíme, či jednotlivé riadky matice A patria do V_B; použijeme na to rovnaký postup ako v príklade 5.2.13).

Ak nám takáto „poloskúška“ nevyjde vieme dokonca pomerne jednoducho nájsť poslednú úpravu od konca, v ktorej sme spravili chybu. Skúsme urobiť v úprave nejakej matice na redukovaný trojuholníkový tvar náročky chybu a ilustrovať si, ako ju vieme nájsť.

$$\begin{pmatrix} 1 & -2 & -2 & 2 \\ 2 & 0 & -1 & -1 \\ 3 & 0 & -4 & -4 \end{pmatrix} \overset{(1)}{\sim} \begin{pmatrix} 1 & -2 & -2 & 2 \\ 0 & 4 & 3 & -5 \\ 0 & 0 & -\frac{5}{2} & -\frac{5}{2} \end{pmatrix} \overset{(2)}{\sim} \begin{pmatrix} 1 & -2 & -2 & 2 \\ 0 & 4 & 3 & -5 \\ 0 & 0 & 1 & 1 \end{pmatrix} \overset{(3)}{\sim} \begin{pmatrix} 1 & -2 & -2 & 2 \\ 0 & 4 & 0 & -2 \\ 0 & 0 & 1 & 1 \end{pmatrix} \overset{(4)}{\sim} \begin{pmatrix} 1 & -2 & -2 & 2 \\ 0 & 1 & 0 & -\frac{1}{2} \\ 0 & 0 & 1 & 1 \end{pmatrix} \overset{(5)}{\sim}$$
$$\begin{pmatrix} 1 & 0 & 0 & 3 \\ 0 & 1 & 0 & -\frac{1}{2} \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Keď urobíme skúšku pre prvú maticu, nevyjde. (Konkrétne pre druhý riadok dostaneme $2(1,0,0,3)-(0,0,1,1)=(2,0,-1,5)$.)

Aby sme našli chybu, robíme skúšku pre matice, ktoré sme dostali ako medzivýsledky, až kým nenarazíme na situáciu, že pred niektorou úpravou skúška nesedí a po nej už áno. To znamená, že v tejto úprave sa zmenil podpriestor prislúchajúci matici, a teda táto úprava nemôže byť správna.

Napríklad pre maticu po úprave (2) skúška nesedí $(4.(0,1,0,-\frac{1}{2})+3.(0,0,1,1)=(0,4,3,1))$. Musíme teda chybu hľadať napravo od tejto matice.

Vyskúšame maticu po úprave (4) – skúška vyjde. Vyskúšame maticu po úprave (3) – skúška opäť vyjde. Keďže pre maticu pred úpravou (3) nám skúška vyšla, ale po nej nie, museli sme spraviť v tejto úprave chybu.

Samozrejme, môže sa stať, že urobíme chybu takého typu, ktorú takáto poloskúška neodhalí.

Správny postup je

$$\begin{pmatrix} 1 & -2 & -2 & 2 \\ 2 & 0 & -1 & -1 \\ 3 & 0 & -4 & -4 \end{pmatrix} \overset{(1)}{\sim} \begin{pmatrix} 1 & -2 & -2 & 2 \\ 0 & 4 & 3 & -5 \\ 0 & 0 & -\frac{5}{2} & -\frac{5}{2} \end{pmatrix} \overset{(2)}{\sim} \begin{pmatrix} 1 & -2 & -2 & 2 \\ 0 & 4 & 3 & -5 \\ 0 & 0 & 1 & 1 \end{pmatrix} \overset{(3)}{\sim} \begin{pmatrix} 1 & -2 & -2 & 2 \\ 0 & 4 & 0 & -8 \\ 0 & 0 & 1 & 1 \end{pmatrix} \overset{(4)}{\sim} \begin{pmatrix} 1 & -2 & -2 & 2 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & 1 \end{pmatrix} \overset{(5)}{\sim}$$
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

(1) `3.r-=(3/2)*2.r; 2.r-=2*1.r` (Týmto zápisom sa myslí to, že od tretieho riadku sa odpočíta (3/2)-násobok druhého a od druhého dvojnásobok prvého) (2) `3.r*=-2/5` (3) `2.r-=3*3.r` (4) `2.r*=1/4` (5) `1.r+=2*2.r+2*3.r`

Cvičenia V nasledujúcich úlohách, ak nie je uvedené inak, uvažujeme matice nad poľom $\mathbb{R}$.

Úloha 5.2.1. Nájdite redukované trojuholníkové matice riadkovo ekvivalentné s nasledujúcimi maticami a) nad poľom $\mathbb{R}$ b) nad poľom $\mathbb{Z}_5$

$$\begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 1 \\ 3 & 4 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 & 3 \\ 3 & 2 & 2 \\ 0 & 4 & 3 \\ 4 & 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 2 & 3 & 4 & 1 \\ 3 & 2 & 3 & 2 \\ 1 & 4 & 0 & 0 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

Úloha 5.2.2. Ak sa to dá, doplňte dané vektory na bázu vektorového priestoru $(\mathbb{Z}_5)^4$:
a) (1,2,0,0), (3,4,0,1)
b) (1,2,3,4), (1,1,1,1), (3,2,1,0)
c) (2,3,4,1), (3,2,4,1), (0,2,3,2)
d) (1,3,1,4,), (3,10,4,3), (2,3,1,1)

Úloha 5.2.3. Zistite, či nasledujúce matice tvoria bázu vektorového priestoru všetkých matíc typu 2×2 nad poľom $\mathbb{R}$:
a) $\left(\begin{smallmatrix} 1 & 2 \\ 0 & 4 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 2 & 3 \\ 5 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 3 & 0 \\ 1 & 2 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 5 \\ 4 & 2 \end{smallmatrix}\right)$ b) $\left(\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 2 & 3 \\ 1 & 2 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 1 \\ 4 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 4 \\ 0 & 5 \end{smallmatrix}\right)$

Úloha 5.2.4. Zistite, ktoré z daných vektorov patria do podpriestoru [(1,4,1,0),(2,3,-2,-3), (0,2,−5,−6)] priestoru $\mathbb{R}^4$: a) (4,11,-3,-3), b)(1,0,11,12), c) (3,0,4,1), d) (1,-1,2,-2).

Úloha 5.2.5. Zistite, či $[\vec{\beta}_1,\vec{\beta}_2]\subseteq[\vec{\gamma}_1,\vec{\gamma}_2,\vec{\gamma}_3]$ vo vektorovom priestore $\mathbb{R}^4$ nad poľom $\mathbb{R}$, ak $\vec{\gamma}_1=(1,1,5,1)$, $\vec{\gamma}_2=(1,0,2,1)$, $\vec{\gamma}_3=(2,1,0,1)$, $\vec{\beta}_1=(1,1,5,1)$ a $\vec{\beta}_2=(-1,1,6,-2)$.

Úloha 5.2.6. Zistite hodnosti matíc

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & -1 & 3 & 8 & 0 \\ 0 & 0 & 2 & 3 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & -1 & 2 & 3 \\ 0 & 0 & 5 & 0 & 1 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 7 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \\ 1 & 1 & \dots & 1 \end{pmatrix} \quad \begin{pmatrix} 2 & -1 & 3 & -2 & 4 \\ 4 & -2 & 5 & 1 & 7 \\ 2 & -1 & 1 & 8 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 3 & 5 & -1 \\ 2 & -1 & -3 & 4 \\ 5 & 1 & -1 & 7 \\ 7 & 7 & 9 & 1 \end{pmatrix}$$

Úloha 5.2.7. Upravte danú maticu nad poľom $\mathbb{R}$ na redukovaný trojuholníkový tvar a určte hodnosť matice

$$\begin{pmatrix} 1 & -2 & -2 & 2 \\ 2 & 2 & -1 & -1 \\ 3 & 3 & -4 & -4 \end{pmatrix} \quad \begin{pmatrix} 3 & -1 & 3 & 2 & 5 \\ 5 & -3 & 2 & 3 & 4 \\ 1 & -3 & -5 & 0 & -7 \\ 7 & -5 & 1 & 4 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 3 & 0 & 5 & 0 & -1 \\ 2 & 6 & 1 & 10 & 0 & 0 \\ 5 & 15 & 2 & 25 & -1 & -4 \\ 3 & 9 & 1 & 15 & 0 & -1 \end{pmatrix} \quad \begin{pmatrix} 4 & 3 & -5 & 2 & 3 \\ 8 & 6 & -7 & 4 & 2 \\ 4 & 3 & -8 & 2 & 7 \\ 4 & 3 & 1 & 2 & -5 \\ 8 & 6 & -1 & 4 & -6 \end{pmatrix}$$

Úloha 5.2.8. Určte hodnosť danej matice v závislosti od parametra $c \in \mathbb{R}$

$$A = \begin{pmatrix} 1 & c & -1 & 2 \\ 2 & -1 & c & 5 \\ 1 & 10 & -6 & 1 \end{pmatrix} \begin{pmatrix} 3 & 2 & c & 2c \\ 1 & -1 & 3 & -c \\ 2 & 3 & 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & c{+}1 & 0 \\ 2 & c{-}1 & 2c \\ c & c & c \end{pmatrix} \begin{pmatrix} 2 & c{+}1 & 0 \\ 4 & c{-}1 & 2c \\ c & c & c \end{pmatrix}$$

Úloha 5.2.9. Zistite, či priestor [(2,4,4,2,4),(3,1,1,2,2),(4,3,3,2,0)] je podpriestor priestoru [(1,1,0,1,4),(2,1,3,3,1),(3,2,1,1,3)] a) nad $\mathbb{Q}$, b) nad $\mathbb{Z}_5$, c) nad $\mathbb{Z}_7$.

Úloha 5.2.10. Zistite, ktoré z daných matíc sú navzájom riadkovo ekvivalentné:

$$\begin{pmatrix} 2 & 3 & 1 \\ 4 & 3 & 3 \\ 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 3 & 1 \\ 2 & 4 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 0 & 3 & 1 \\ 2 & 0 & 3 \\ 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 0 & 1 \\ 0 & 3 & 2 \\ 1 & 0 & 3 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 3 & 2 & 1 \\ 4 & 2 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

Úloha 5.2.11*. Určite hodnosť matice:

$$\begin{pmatrix} 1 & a_1 & a_1^2 & \dots & a_1^n \\ 1 & a_2 & a_2^2 & \dots & a_2^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \dots & a_n^n \\ 1 & a_{n+1} & a_{n+1}^2 & \dots & a_{n+1}^n \end{pmatrix}$$

ak viete, že $a_1, \dots, a_{n+1}$ sú navzájom rôzne reálne čísla (t.j. $a_i \neq a_j$ pre všetky $i \neq j$).

Všetky príklady, v ktorých vystupujú len celé čísla, si môžete upraviť tak, že jednotlivé členy matice nahradíte ich zvyškami po delení 3 (5 , 7) a riešite rovnakú úlohu nad $\mathbb{Z}_3$ ($\mathbb{Z}_5$, $\mathbb{Z}_7$).

5.3 Lineárne zobrazenia

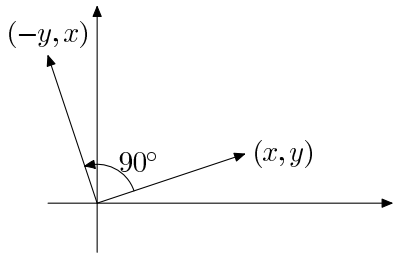
V tejto časti zavedieme vlastne najdôležitejší koncept tejto prednášky – lineárne zobrazenia. Ak by sme povedali, že všetko čo sme robili doteraz sme robili iba s cieľom, aby sme si pripravili vhodné prostriedky na popis lineárnych zobrazení, neboli by sme ďaleko od pravdy. Táto prednáška totiž do veľkej miery smeruje k tomu, aby sme pochopili lineárne javy, ktoré sa v matematike (ale aj vo fyzike a ďalších aplikáciach) popisujú práve pomocou lineárnych zobrazení.

Definícia 5.3.1. Ak V a W sú vektorové priestory nad poľom F a $f\colon V \to W$ je zobrazenie z V do W, tak hovoríme, že f je *lineárne zobrazenie,* ak pre ľubovoľné $\vec{\alpha}, \vec{\beta} \in V$ a ľubovoľné $c \in F$ platí

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

(ii) $f(c\vec{\alpha}) = cf(\vec{\alpha})$.

Inými slovami, lineárne zobrazenia sú tie zobrazenia, ktoré zachovávajú základné operácie popisujúce vektorový priestor.



Obr. 5.1: Otočenie v rovine o 90°

Príklad 5.3.2. Otočenie v rovine o 90° je lineárne zobrazenie.

Otočenie v rovine o 90° má vyjadrenie v súradniciach[1]

$$f(x, y) = (y, -x).$$

Overme podmienky z definície lineárneho zobrazenia:

$$f(x, y) + f(x', y') = (y, -x) + (y', -x') = (y + y', -(x + x')) = f(x + x', y + y'),$$
$$f(cx, cy) = (cy, -cx) = cf(x, y).$$

Príklad 5.3.3. Zobrazenie $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ určené predpisom $f(x, y) = (2x + y, x + 3y)$ je lineárne zobrazenie. (V istom zmysle je typickým príkladom lineárneho zobrazenia, ako uvidíme neskôr.)

$$f(x, y) + f(x', y') = (2x + y, x + 3y) + (2x' + y', x' + 3y') =$$
$$(2(x + x') + y + y', x + x' + 3(y + y')) = f(x + x', y + y'),$$

$$f(cx, cy) = (2cx + cy, cx + 3cy) = c(2x + y, x + 3y) = cf(x, y).$$

Veta 5.3.4. *Nech V, W sú vektorové priestory nad poľom F a $f\colon V \to W$ je zobrazenie. Nasledujúce podmienky sú ekvivalentné:*

(a) *zobrazenie f je lineárne,*

(b) *$f(c\vec{\alpha} + d\vec{\beta}) = cf(\vec{\alpha}) + df(\vec{\beta})$ pre ľubovoľné $c, d \in F$ a ľubovoľné $\vec{\alpha}, \vec{\beta} \in V$,*

(c) *$f(c_1\vec{\alpha}_1 + \cdots + c_n\vec{\alpha}_n) = c_1 f(\vec{\alpha}_1) + \ldots + c_n f(\vec{\alpha}_n)$ pre ľubovoľné $c_1, \ldots, c_n \in F$, $\vec{\alpha}_1, \ldots, \vec{\alpha}_n \in V$.*

Posledná podmienka v predchádzajúcej vete hovorí, že lineárne zobrazenia sú práve zobrazenia zachovávajúce lineárne kombinácie.

Dôkaz. (a) $\Rightarrow$ (b) Vyplýva priamo z definície lineárneho zobrazenia.

$$f(c\vec{\alpha} + d\vec{\beta}) \overset{(i)}{=} f(c\vec{\alpha}) + f(d\vec{\beta}) \overset{(ii)}{=} cf(\vec{\alpha}) + df(\vec{\beta})$$

(b) $\Rightarrow$ (c) Dostaneme opakovaným použitím (b). (Formálny dôkaz by sme urobili pomocou matematickej indukcie.)

(c) $\Rightarrow$ (a) Ak dosadíme $n = 1$ dostaneme podmienku (ii) z definície lineárneho zobrazenia. Pre $n = 2$ a $c_1 = c_2 = 1$ máme podmienku (i). □

[1] Keby sme boli presní, mali by sme písať $f((x, y))$ – jednu zátvorku kvôli zobrazeniu a druhú z označenia vektora. Rozhodli sme sa, že si zápis trochu zjednodušíme.

Tvrdenie 5.3.5. *Ak f je lineárne zobrazenie, tak $f(\vec{0}) = \vec{0}$.*

Dôkaz.

$$f(\vec{0}) = f(\vec{0} + \vec{0}) = f(\vec{0}) + f(\vec{0})$$

Vykrátením $f(\vec{0})$ dostaneme $f(\vec{0}) = \vec{0}$. □

Veta 5.3.6. *Nech V, W sú vektorové priestory. Nech $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ je báza priestoru V a nech $\vec{\beta}_1, \ldots, \vec{\beta}_n \in W$. Potom existuje práve jedno lineárne zobrazenie $f\colon V \to W$ také, že*

$$f(\vec{\alpha}_i) = \vec{\beta}_i$$

pre $i = 1, 2, \ldots, n$.

Dôkaz. Nech $\vec{\alpha} \in V$. Pretože $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ tvorí bázu priestoru V, existujú jednoznačne určené skaláry $c_1, \ldots, c_n \in F$ také, že

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

Potom $f(\vec{\alpha})$ definujeme ako

$$f(\vec{\alpha}) = c_1\vec{\beta}_1 + \cdots + c_n\vec{\beta}_n.$$

(Pretože $c_1, \ldots, c_n$ sú jednoznačne určené, je f dobre definované, t.j., nemôže sa stať, že by sme takto tomu istému $\vec{\alpha}$ priradili dve rôzne hodnoty. Súčasne $f(\vec{\alpha})$ nemôže mať inú hodnotu, ak to má byť lineárne zobrazenie – vyplýva to z toho, že lineárne zobrazenia zachovávajú lineárne kombinácie. Z toho vyplýva jednoznačnosť zobrazenia f.)

Ukážeme, že takto definované zobrazenie je skutočne lineárne. Uvažujme dva vektory

$$\vec{\alpha} = c_1\vec{\alpha}_1 + \cdots + c_n\vec{\alpha}_n$$
$$\vec{\alpha'} = d_1\vec{\alpha}_1 + \cdots + d_n\vec{\alpha}_n$$

Potom platí

$$\vec{\alpha} + \vec{\alpha'} = (c_1 + d_1)\vec{\alpha}_1 + \ldots + (c_n + d_n)\vec{\alpha}_n$$
$$f(\vec{\alpha} + \vec{\alpha'}) = (c_1 + d_1)\vec{\beta}_1 + \ldots + (c_n + d_n)\vec{\beta}_n = c_1\vec{\beta}_1 + \cdots + c_n\vec{\beta}_n + d_1\vec{\beta}_1 + \cdots + d_n\vec{\beta}_n = f(\vec{\alpha}) + f(\vec{\alpha'})$$

Podobne dostaneme

$$c.\vec{\alpha} = cc_1\vec{\alpha}_1 + \cdots + cc_n\vec{\alpha}_n$$
$$f(c.\vec{\alpha}) = cc_1\vec{\beta}_1 + \cdots + cc_n\vec{\beta}_n = c(c_1\vec{\beta}_1 + \cdots + c_n\vec{\beta}_n) = c.f(\vec{\alpha})$$

□

Lineárne zobrazenie je jednozačne určené obrazmi prvkov (ľubovoľnej) bázy.

V priestore F^n máme štandardnú bázu

$$\vec{\varepsilon}_1 = (1, 0, \ldots, 0), \vec{\varepsilon}_2 = (0, 1, \ldots, 0), \ldots, \vec{\varepsilon}_n = (0, \ldots, 0, 1).$$

Táto báza nám umožní popísať ľubovoľné zobrazenie z F^n do F^k spôsobom, ktorý je v istom zmysle kanonický.

Definícia 5.3.7. Nech F je pole. *Matica lineárneho zobrazenia $f\colon F^m \to F^n$* je matica typu $m \times n$ ktorej k-ty riadok je vektor $f(\vec{\varepsilon}_k)$.

Maticu zobrazenia f budeme označovať A_f.

Každému lineárnemu zobrazeniu $f\colon F^m \to F^n$ sme takto priradili nejakú maticu A_f typu $m \times n$.

Obrátene, ľubovoľnou maticou typu $m \times n$ je jednoznačne určené lineárne zobrazenie $f\colon F^m \to F^n$. (Riadky matice určujú obrazy bázových vektorov, jednoznačnosť a existencia takéhoto zobrazenia vyplývajú z vety 5.3.6.) Lineárne zobrazenie prislúchajúce matici A budeme označovať f_A.

Príklad 5.3.8. Uvažujme lineárne zobrazenie $f\colon \mathbb{R}^2 \to \mathbb{R}^3$ dané predpisom $f(x,y) = (2x + y, x + y, x + 2y)$. Dosadením zistíme, že platí

$$f(\vec{\varepsilon}_1) = f(1,0) = (2,1,1)$$
$$f(\vec{\varepsilon}_2) = f(0,1) = (1,1,2)$$

Teda matica tohoto zobrazenia je

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

Veta 5.3.9. *Nech U, V, W sú vektorové priestory nad tým istým poľom F. Ak $f\colon U \to V$ a $g\colon V \to W$ sú lineárne zobrazenia, tak aj $g \circ f$ je lineárne zobrazenie.*

Dôkaz. Na overenie použijeme podmienku (b) z vety 5.3.4. Nech $\vec{\alpha}, \vec{\beta} \in U$ a $c, d \in F$. Potom dostaneme

$$g(f(c\vec{\alpha} + d\vec{\beta})) = g(cf(\vec{\alpha}) + df(\vec{\beta})) = cg(f(\vec{\alpha})) + dg(f(\vec{\beta})).$$

(Využili sme najprv linearitu zobrazenia f a potom linearitu zobrazenia g.) □

Poznámka 5.3.10. Ľahko sa overí, že ak $f, g\colon V \to W$ sú lineárne zobrazenia, tak aj zobrazenia $f + g$ a $c.f$ sú lineárne.

Teraz si ukážeme na konkrétnom príklade, ako vieme nájsť maticu lineárneho zobrazenia, ak máme dané obrazy niektorých vektorov. (V prípade, že tieto vektory tvoria bázu, také zobrazenie existuje podľa vety 5.3.6.)

Úloha 5.3.1. Nájdite maticu lineárneho zobrazenia $f\colon \mathbb{R}^3 \to \mathbb{R}^4$, pre ktoré platí:
a) $f(2,0,3) = (1,2,-1,1)$, $f(4,1,5) = (4,5,-2,1)$, $f(3,1,2) = (1,-1,1,-1)$,
b) $f(2,0,3) = (1,2,-1,1)$, $f(4,1,5) = (4,5,-2,1)$, $f(2,-1,4) = (-1,1,-1,2)$,
c) $f(2,0,3) = (1,2,-1,1)$, $f(4,1,5) = (4,5,-2,1)$, $f(2,-1,4) = (1,-1,1,-1)$.

Postupujeme tak, že si napíšeme do matice vektory a ich obrazy a ľavú časť sa snažíme upraviť riadkovými úpravami na jednotkovú maticu (aby sme našli obrazy vektorov $\vec{\varepsilon}_i$)

$$\left(\begin{array}{ccc|cccc} 2 & 0 & 3 & 1 & 2 & -1 & 1 \\ 4 & 1 & 5 & 4 & 5 & -2 & 1 \\ 3 & 1 & 2 & 1 & -1 & 1 & -1 \end{array}\right) \sim \left(\begin{array}{ccc|cccc} 1 & 0 & \frac{3}{2} & \frac{1}{2} & 1 & -\frac{1}{2} & \frac{1}{2} \\ 0 & 1 & -1 & 2 & 1 & 0 & -1 \\ 0 & 1 & -\frac{5}{2} & -\frac{1}{2} & 4 & \frac{5}{2} & -1 \end{array}\right) \sim \left(\begin{array}{ccc|cccc} 1 & 0 & \frac{3}{2} & \frac{1}{2} & 1 & -\frac{1}{2} & \frac{1}{2} \\ 0 & 1 & -1 & 2 & 1 & 0 & -1 \\ 0 & 0 & -\frac{3}{2} & -\frac{5}{2} & -5 & \frac{5}{2} & -\frac{3}{2} \end{array}\right) \sim \left(\begin{array}{ccc|cccc} 1 & 0 & 0 & -2 & -4 & 2 & -1 \\ 0 & 1 & 0 & \frac{11}{3} & \frac{13}{3} & -\frac{5}{3} & 0 \\ 0 & 0 & 1 & \frac{5}{3} & \frac{10}{3} & -\frac{5}{3} & 1 \end{array}\right)$$

Hľadaná matica je $\begin{pmatrix} -2 & -4 & 2 & -1 \\ \frac{11}{3} & \frac{13}{3} & -\frac{5}{3} & 0 \\ \frac{5}{3} & \frac{10}{3} & -\frac{5}{3} & 1 \end{pmatrix}$.

Základná myšlienka algoritmu, ktorý sme práve popísali, je v tom, že po každom kroku platí, že vektor na ľavej strane sa zobrazením s danými vlastnosťami zobrazí na vektor napravo od neho. Skutočne, ak máme v nejako kroku $f(\vec{\alpha}_i) = \vec{\beta}_i$ a $f(\vec{\alpha}_j) = \vec{\beta}_j$ (kde $\vec{\alpha}_k$ a $\vec{\beta}_k$ označuje k-ty riadok ľavej resp. pravej časti matice) a pripočítame k i-temu riadku c-násobok j-teho riadku, platí tento vzťah aj pre riadky novej matice:

$$f(\vec{\alpha}_i + c\vec{\alpha}_j) = f(\vec{\alpha}_i) + cf(\vec{\alpha}_j) = \vec{\beta}_i + c\vec{\beta}_j.$$

Podobne sa to dá overiť pre ostatné elementárne riadkové operácie.[2]

Skúšku správnosti môžeme urobiť tak, že overíme, či f naozaj nadobúda zadané hodnoty, napríklad $f(3,1,2) = 3(-2,-4,2,-1) + 1(\frac{11}{3}, \frac{13}{3}, -\frac{5}{3}, 0) + 2(\frac{5}{3}, \frac{10}{3}, -\frac{5}{3}, 1) = (1,-1,1,-1)$.

V prípade, že skúška nevyjde, chybu môžeme hľadať tak, že skúšame pre medzivýsledky, či sa vektor na ľavej strane zobrazí na vektor ležiaci od neho napravo v zobrazení určenom maticou, ktorá nám vyšla. Samozrejme chybu môžeme hľadať aj tak, že kontrolujeme jednotlivé úpravy.

b) $\left(\begin{array}{ccc|cccc} 2 & 0 & 3 & 1 & 2 & -1 & 1 \\ 4 & 1 & 5 & 4 & 5 & -2 & 1 \\ 2 & -1 & 4 & -1 & 1 & -1 & 2 \end{array}\right) \sim \left(\begin{array}{ccc|cccc} 2 & 0 & 3 & 1 & 2 & -1 & 1 \\ 0 & 1 & -1 & 2 & 1 & 0 & -1 \\ 0 & -1 & 1 & -2 & -1 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|cccc} 2 & 0 & 3 & 1 & 2 & -1 & 1 \\ 0 & 1 & -1 & 2 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$

Vidíme, že môžeme $f(0,0,1)$ zvoliť ľubovoľne. Označme $f(0,0,1) = (a,b,c,d)$. Potom dostaneme

$\left(\begin{array}{ccc|cccc} 2 & 0 & 3 & 1 & 2 & -1 & 1 \\ 0 & 1 & -1 & 2 & 1 & 0 & -1 \\ 0 & 0 & 1 & a & b & c & d \end{array}\right) \sim \left(\begin{array}{ccc|cccc} 1 & 0 & 0 & \frac{1-3a}{2} & 1-\frac{3}{2}b & \frac{1-3c}{2} & 1-\frac{3}{2}d \\ 0 & 1 & 0 & 2+a & 1+b & c & -1+d \\ 0 & 0 & 1 & a & b & c & d \end{array}\right)$

Pre každé $a,b,c,d \in \mathbb{R}$ je táto matica maticou zobrazenia f s požadovanými vlastnosťami.

c) $\left(\begin{array}{ccc|cccc} 2 & 0 & 3 & 1 & 2 & -1 & 1 \\ 4 & 1 & 5 & 4 & 5 & -2 & 1 \\ 2 & -1 & 4 & 1 & -1 & 1 & -1 \end{array}\right) \sim \left(\begin{array}{ccc|cccc} 2 & 0 & 3 & 1 & 2 & -1 & 1 \\ 0 & 1 & -1 & 2 & 1 & 0 & -1 \\ 0 & -1 & 1 & 0 & -3 & -2 & -2 \end{array}\right) \sim \left(\begin{array}{ccc|cccc} 2 & 0 & 3 & 1 & 2 & -1 & 1 \\ 0 & 1 & -1 & 2 & 1 & 0 & -1 \\ 0 & 0 & 0 & 2 & -2 & -2 & -2 \end{array}\right)$

Pre lineárne zobrazenie f, ktoré by spĺňalo podmienky zo zadania by muselo platiť $f(0,0,0) = (2,-2,-2,-2)$, ale také lineárne zobrazenie neexistuje. (Lineárne zobrazenie vždy zobrazuje nulový vektor na nulový vektor.)

Cvičenia

Úloha 5.3.2. Nájdite maticu lineárneho zobrazenia $f\colon (\mathbb{Z}_7)^2 \to (\mathbb{Z}_7)^2$ a napíšte jeho predpis.
a) $f(1,1) = (0,1)$, $f(6,1) = (3,2)$
b) $f(2,3) = (1,0)$, $f(3,2) = (6,1)$

Úloha 5.3.3. Nájdite maticu lineárneho zobrazenia $f\colon \mathbb{R}^4 \to \mathbb{R}^4$ takého, že:
a) $f(1,2,3,1) = (1,3,1,0)$, $f(2,1,3,0) = (0,1,3,1)$, $f(3,2,1,0) = (1,0,3,0)$, $f(2,2,3,4) = (3,1,0,4)$
b) $f(1,2,3,4) = (0,0,0,0)$, $f(2,1,3,1) = (1,0,3,1)$, $f(0,1,2,0) = (2,0,1,0)$, $f(1,0,3,1) = (2,1,3,1)$
c) $f(0,1,1,1) = (1,0,0,0)$, $f(1,0,1,1) = (0,1,0,0)$, $f(1,1,0,1) = (0,0,1,0)$, $f(1,1,1,0) = (0,0,0,1)$

Úloha 5.3.4. Nech V a W sú vektorové priestory nad poľom F. Dokážte, že zobrazenie $f\colon V \to W$ je lineárne práve vtedy, keď pre každé $\vec{\alpha}, \vec{\beta} \in V$ a pre každé $c, d \in F$ platí $f(c\vec{\alpha} + d\vec{\beta}) = cf(\vec{\alpha}) + df(\vec{\beta})$.

Úloha 5.3.5. Nech V a W sú vektorové priestory nad poľom F a $f\colon V \to W$ je lineárne zobrazenie. Ak $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ sú lineárne závislé vektory, tak aj $f(\vec{\alpha}_1), \ldots, f(\vec{\alpha}_n)$ sú lineárne závislé vektory.

Úloha 5.3.6. Nech $f\colon V \to W$ je lineárne zobrazenie z vektorového priestoru V do vektorového priestoru W nad poľom F. Dokážte:
Ak S je podpriestor vektorového priestoru V, tak $f[S] = \{f(\vec{\alpha}); \vec{\alpha} \in S\}$ je podpriestor vektorového priestoru W.
Ak T je podpriestor vektorového priestoru W, tak $f^{-1}(T) = \{\vec{\alpha} \in V : f(\vec{\alpha}) \in T\}$ je podpriestor vektorového priestoru V.

[2] Takýto postup je typický pri dokazovaní správnosti algoritmov. Našli sme tvrdenie, ktoré platí po každom kroku algoritmu. (Nazývame ho *invariant.*) O tomto invariante treba dokázať, že: a) platí na začiatku výpočtu; b) vykonanie jedného kroku algoritmu nezmení platnosť invariantu; c) ak platí invariant na konci výpočtu, tak algoritmus skutočne robí, to čo má.

5.4 Súčin matíc

V predchádzajúcej časti sme sa naučili, že lineárne zobrazenie $F^m \to F^n$ je jednoznačne určené maticou typu $m \times n$ a obrátene, každému takémuto lineárnemu zobrazeniu prislúcha jeho matica. Tiež sme sa dozvedeli, že zložením lineárnych zobrazení opäť vznikne lineárne zobrazenie. Preto je prirodzená otázka ako vyzerá matica prislúchajúca zloženému zobrazeniu.

Príklad 5.4.1. Uvažujme zobrazenie $f\colon \mathbb{R}^2 \to \mathbb{R}^3$ určené maticou $\left(\begin{smallmatrix} 1 & 0 & 2 \\ 2 & 1 & 1 \end{smallmatrix}\right)$ a zobrazenie $g\colon \mathbb{R}^3 \to \mathbb{R}^2$ určené maticou $\left(\begin{smallmatrix} 3 & 1 \\ 1 & 1 \\ 0 & -1 \end{smallmatrix}\right)$. Pokúsme sa vypočítať maticu zloženého zobrazenia $A_{g\circ f}$.

Budeme označovať štandardnú bázu v $\mathbb{R}^2$ ako $\vec{\delta}_1, \vec{\delta}_2$ a štandardnú bázu v $\mathbb{R}^3$ ako $\vec{\varepsilon}_1, \vec{\varepsilon}_2, \vec{\varepsilon}_3$.

Vypočítajme obrazy vektorov štandardnej bázy:

$$g(f(\vec{\delta}_1)) = g(1,0,2) = g(\vec{\varepsilon}_1 + 2\vec{\varepsilon}_3) = g(\vec{\varepsilon}_1) + 2g(\vec{\varepsilon}_3) = (3,1) + 2.(0,-1) = (3,-1)$$
$$g(f(\vec{\delta}_2)) = g(2,1,1) = g(2\vec{\varepsilon}_1 + \vec{\varepsilon}_2 + \vec{\varepsilon}_3) = 2g(\vec{\varepsilon}_1) + g(\vec{\varepsilon}_2) + g(\vec{\varepsilon}_3) = 2.(3,1) + (1,1) + (0,-1) = (7,2)$$

Z toho dostávame

$$A_{g\circ f} = \left(\begin{smallmatrix} 3 & -1 \\ 7 & 2 \end{smallmatrix}\right).$$

Pokúsme sa zopakovať tento výpočet vo všeobecnosti. Máme teda dve lineárne zobrazenia a im prislúchajúce matice:

$$f\colon F^m \to F^n \qquad A_f = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \text{ typu } m \times n$$
$$g\colon F^n \to F^k \qquad A_g = \begin{pmatrix} b_{11} & \dots & b_{1k} \\ \vdots & \ddots & \vdots \\ b_{n1} & \dots & b_{nk} \end{pmatrix} \text{ typu } n \times k$$

Opäť nech $\vec{\delta}_1, \dots, \vec{\delta}_m$ je štandardná báza F^m a $\vec{\varepsilon}_1, \dots, \vec{\varepsilon}_n$ je štandardná báza F^n.

Pretože $g \circ f\colon F^m \to F^k$ je matica zloženého zobrazenia matica typu $m \times k$. Riadky matice $A_{g\circ f}$ sú vektory $g(f(\vec{\delta}_1)), g(f(\vec{\delta}_2)), \dots, g(f(\vec{\delta}_m))$.

Nech $i \in \{1, 2, \dots m\}$. Vypočítajme príslušný riadok matice $A_{g\circ f}$.

$$\begin{aligned} g(f(\vec{\delta}_i)) = g(a_{i1}, a_{i2}, \dots, a_{in}) = \\ g(a_{i1}\vec{\varepsilon}_1 + a_{i2}\vec{\varepsilon}_2 + \dots + a_{in}\vec{\varepsilon}_n) = g(a_{i1}\vec{\varepsilon}_1) + g(a_{i2}\vec{\varepsilon}_2) + \dots + g(a_{in}\vec{\varepsilon}_n) = \\ a_{i1}(b_{11}, b_{12}, \dots, b_{1k}) + \\ a_{i2}(b_{21}, b_{22}, \dots, b_{2k}) + \\ \vdots \\ a_{in}(b_{n1}, b_{n2}, \dots, b_{nk}) = \\ (a_{i1}b_{11} + a_{i2}b_{21} + \dots + a_{in}b_{n1}, a_{i1}b_{12} + a_{i2}b_{22} + \dots + a_{in}b_{n2}, \dots, a_{ik}b_{1k} + a_{i2}b_{2k} + \dots + a_{in}b_{nk}) \end{aligned}$$

Vektor $g(f(\vec{\delta}_i))$ má na j-tej súradnici hodnotu

$$c_{ij} := a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{in}b_{nj} = \sum_{t=1}^{n} a_{it}b_{tj}.$$

Matica zloženého zobrazenia je matica $A_{g\circ f} = ||c_{ij}||$ typu $m \times k$.

Všimnime si, že prvok c_{ij} vlastne získame tak, že vezmeme i-ty riadok matice A a j-ty stĺpec matice B (dostaneme tak 2 vektory rovnakej dĺžky n), vynásobíme hodnoty na rovnakých súradniciach a takto získané hodnoty sčítame. (Je to vlastne skalárny súčin i-teho riadku matice A a j-teho stĺpca a matice B – o skalárnom súčine ešte budeme hovoriť neskôr.)

Definícia 5.4.2. Ak A je matica typu $m \times n$ a B je matica typu $n \times k$ nad poľom F, tak maticu $C = ||c_{ij}||$ typu $m \times k$, kde

$$c_{ij} = \sum_{t=1}^{n} a_{it} b_{tj}$$

pre $i = 1, 2, \ldots, m$ a $j = 1, 2, \ldots, k$, nazývame *súčin matíc* A a B. Označujeme ju $A.B$.

Dôležité je si všimnúť, že súčin matíc definujeme iba v prípade, že počet stĺpcov prvej matice sa rovná počtu riadkov druhej matice.

$$m \times \boxed{n \quad n} \times k$$

Výsledok je matica typu $m \times k$.

Príklad 5.4.3. $\left(\begin{smallmatrix} 1 & 0 & 2 \\ 2 & 1 & 1 \end{smallmatrix}\right) . \begin{pmatrix} 3 & 1 \\ 1 & 1 \\ 0 & -1 \end{pmatrix} = \left(\begin{smallmatrix} 3 & -1 \\ 7 & 2 \end{smallmatrix}\right)$

Veta 5.4.4. *Nech F je pole, $f\colon F^m \to F^n$ a $g\colon F^n \to F^k$ sú lineárne zobrazenia. Potom platí*

$$A_{g\circ f} = A_f.A_g$$

Dôkaz. Súčin matíc sme definovali práve tak, aby platil predchádzajúci vzťah. (Dôkaz tejto vety spočíva vlastne v odvodení vzťahu pre $A_{g\circ f}$, ktoré sme uviedli za príkladom 5.4.1.) □

POZOR na zmenu poradia v predchádzajúcej vete. T.j. matice na pravej strane rovnosti sú zapísané v inom poradí ako je zápis skladania zobrazení. (Opäť platí, že niektoré knihy ako napríklad [KGGS] definujú poradie skladania zobrazení inak, čo samozrejme ovplyvní aj poradie v predhádzajúcej rovnosti.)

Dôsledok 5.4.5. *Násobenie matíc je asociatívne, teda*

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

pre ľubovoľné matice také, že ich možno násobiť v uvedenom poradí.

Dôkaz. Ľubovoľná matica je matica nejakého lineárneho zobrazenia. Označme zobrazenia prislúchajúce daným maticiam f, g a h. Dostaneme

$$A_f.(A_g.A_h) = A_f.(A_{h\circ g}) = A_{(h\circ g)\circ f} = A_{h\circ(g\circ f)} = A_{g\circ f}.A_h = (A_f.A_g).A_h.$$

(Inak povedané, vďaka tomu, že poznáme vzťah medzi násobením matíc a skladaním zobrazení, asociatívnosť násobenia matíc ľahko vyplýva z asociatívnosti skladania zobrazení.) □

To isté tvrdenie môžeme dokázať aj priamo z definície súčinu.

Dôkaz. Majme matice A, B, C typov $m \times n$, $n \times k$, $k \times l$. Vyjadrime prvok v i-tom riadku a j-tom stĺpci matice $A(BC)$. Dostaneme

$$\sum_{t=1}^{n} a_{it} \sum_{u=1}^{k} b_{tu} c_{uj} = \sum_{t=1}^{n} \sum_{u=1}^{k} a_{it}(b_{tu} c_{uj}).$$

Keď vypočítame prvok v i-tom riadku a j-tom stĺpci matice $(AB)C$ dostaneme

$$\sum_{u=1}^{k} \left(\sum_{t=1}^{n} a_{it} b_{tu} \right) c_{uj} = \sum_{u=1}^{k} \sum_{t=1}^{n} (a_{it} b_{tu}) c_{uj},$$

čiže presne tú istú sumu, len s iným poradím sčitovania. □

Príklad 5.4.6. Násobenie matíc nie je komutatívne. (Vyplýva to aj z toho, že nie vždy, keď je definovaný súčin $A.B$ je definovaný aj súčin $B.A$. Ukážeme si však aj príklad, kde sú súčiny v oboch poradiach definované, ale rôzne.)

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

Veta 5.4.7. *Nech matice A, B, C nad poľom F sú majú také rozmery, že uvedené súčty a súčiny majú zmysel.*

$$I_m A = A = A I_n$$
$$A(B + C) = AB + AC$$
$$(B + C)D = BD + CD$$

Dôkaz. Rovnosť dvoch výrazov obsahujúcich matice môžeme overiť tak, že vypočítame prvok v i-tom riadku a j-tom stĺpci matice na ľavej a pravej strane rovnosti a výsledky porovnáme.

Prvok v i-tom riadku a j-tom stĺpci matice $I_m A$ má tvar

$$c_{ij} = \delta_{i1} a_{1j} + \delta_{i2} a_{2j} + \ldots + \delta_{im} a_{mj},$$

kde ako δ_{ij} sme označili prvok i-teho riadku a j-teho stĺpca jednotkovej matice I_m (pozri tiež poznámku 5.1.7). Pretože z čísel δ_{ij} je len $\delta_{ii} = 1$ a ostatné sú nulové, dostávame z predchádzajúcej rovnosti priamo

$$c_{ij} = a_{ij}.$$

Vzťah pre násobenie jednotkovou maticou sprava sa overí rovnako.

Označme $D := A(B + C)$. Potom

$$d_{ij} = a_{i1}(b_{1j} + c_{1j}) + a_{i2}(b_{2j} + c_{2j}) + \ldots + a_{in}(b_{nj} + c_{nj}) =$$
$$a_{i1} b_{1j} + a_{i2} b_{2j} + \ldots + a_{in} b_{nj} + a_{i1} c_{1j} + a_{i2} c_{2j} + \ldots + a_{in} c_{nj},$$

čo je presne súčet prvkov i-teho riadku a j-teho stĺpca matíc AB a AC. Teda skutočne platí

$$A(B + C) = AB + AC.$$

Predchádzajúce odvodenie by sme mohli stručnejšie a prehľadnejšie zapísať ako

$$d_{ij} = \sum_{t=1}^{n} a_{it}(b_{tj} + c_{tj}) = \sum_{t=1}^{n} a_{it} b_{tj} + \sum_{t=1}^{n} a_{it} c_{tj}.$$

Vzťah $(B + C)D = BD + CD$ sa overí úplne analogicky. □

Vidíme, že matica I má podobnú vlastnosť ako neutrálny prvok nejakej binárnej operácie. Mohla by nám napadnúť otázka, či štvorcové matice náhodou netvoria grupu – už vieme, že násobenia matíc je asociatívne, chýba nám teda ešte inverzný prvok. K otázke existencie inverznej matice sa dostaneme v ďalšej podkapitole.

Poznámka* **5.4.8.** Aj tu by sme mohli postupovať tak, že by sme namiesto matíc porovnávali zobrazenia, ktoré zodpovedajú maticiam vystupujúcim v uvedených rovnostiach. (Môžete si to vyskúšať.) Treba si pritom uvedomiť, že zobrazenie zodpovedajúce súčtu matíc je súčet zobrazení a jednotkovej matici zodpovedá identické zobrazenie.

Pri overovaní distributívnosti sa takýmto spôsobom dostanete ku vzťahom medzi skladaním zobrazení a súčtom zobrazení, ktoré neplatia všeobecne, platia však pre lineárne zobrazenia (čo nám úplne stačí).

Poznámka 5.4.9. Vektor môžeme chápať ako maticu typu $1 \times m$. Vďaka tomu môže mať zmysel aj násobenie matice a vektora.

Nech $f\colon F^m \to F^n$ je lineárne zobrazenie a $\vec{\alpha} \in F^m$. Potom platí nasledujúca veľmi užitočná rovnosť

$$f(\vec{\alpha}) = \vec{\alpha}.A_f.$$

Ak $\vec{\alpha}$ chápeme ako maticu typu $1 \times m$ nad poľom F, tak uvedená rovnosť skutočne má zmysel – vynásobením matíc typu $1 \times m$ a $m \times n$ dostaneme maticu typu $1 \times n$. Túto maticu môžeme chápať ako vektor z F^n.

Platnosť uvedenej rovnosti vyplýva priamo z definície násobenia matíc. Stačí si uvedomiť, že ak riadky matice A označíme ako $\vec{\alpha}_1, \ldots, \vec{\alpha}_m$, tak

$$\vec{\alpha}.A = (a_1, \ldots, a_m).\begin{pmatrix} \vec{\alpha}_1 \\ \vdots \\ \vec{\alpha}_m \end{pmatrix} = a_1\vec{\alpha}_1 + \cdots + a_m\vec{\alpha}_m =$$

$$a_1 f(\vec{\varepsilon}_1) + \cdots + a_n f(\vec{\varepsilon}_n) = f(a_1\vec{\varepsilon}_1 + \cdots + a_n\vec{\varepsilon}_n) = f(a_1, \ldots, a_n) = f(\vec{\alpha}).$$

Všimnime si, že pomocou predchádzajúceho zápisu dostaneme

$$g(f(\vec{\alpha})) = g(\vec{\alpha}A_f) = \vec{\alpha}(A_f A_g),$$

čiže

$$A_{g \circ f} = A_f A_g.$$

Ak si teda zapamätáme, že lineárne zobrazenie je vlastne násobenie maticou *sprava,* tak si ľahko zapamätáme aj to, že sa poradie skladania zobrazení pri súčine matíc musí meniť.

V súvislosti so súčinom matíc bude pre nás často užitočná aj rovnosť

$$(AB)^T = B^T A^T, \tag{5.1}$$

ktorej dôkaz je ponechaný ako cvičenie (úloha 5.4.1).

Cvičenia

Úloha 5.4.1. Dokážte:
a) $(AB)^T = B^T A^T$
b) Ak A je symetrická matica, tak aj A^n pre každé $n \in N$ je symetrická matica.

Úloha 5.4.2. Vypočítajte $A^2 + 2AB + B^2$, $A^2 + 2BA + B^2$, $A^2 + AB + BA + B^2$, $(A+B)^2$, ak $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ $B = \left(\begin{smallmatrix} 1 & 3 \\ 2 & 1 \end{smallmatrix}\right)$

Úloha 5.4.3. Vyrátajte $E.A$ a $A.E$ pre $A = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 0 & -1 \\ -1 & -2 & 1 \end{pmatrix}$ a a) $E = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ b) $E = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ c) $E = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ d) $E = \begin{pmatrix} 1 & 0 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Vedeli by ste nájsť riadkovú/stĺpcovú operáciu, pomocou ktorej dostaneme z matice A maticu $E.A$ resp. $A.E$? (Viac sa o súvise násobenia matíc a elementárnych riadkových/stĺpcových operácií môžete dozvedieť v podkapitole 5.6).

5.5 Inverzná matica

Pripomeňme, že zobrazenie $g\colon Y \to X$ nazývame inverzným zobrazením k zobrazeniu $f\colon X \to Y$, ak

$$g \circ f = id_X$$
$$f \circ g = id_Y$$

(definícia 2.2.15) a označujeme ho f^{-1}. Ďalej vieme, že inverzné zobrazenie k zobrazeniu f existuje práve vtedy, keď f je bijekcia (tvrdenie 2.2.16).

Veta 5.5.1. *Ak $f\colon V \to W$ je lineárne zobrazenie a existuje inverzné zobrazenie $f^{-1}\colon W \to V$, tak f^{-1} je lineárne zobrazenie.*

Dôkaz. Nech $\vec{\alpha}, \vec{\beta} \in W$. Označme $\vec{\alpha}_1 = f^{-1}(\vec{\alpha})$ a $\vec{\beta}_1 = f^{-1}(\vec{\beta})$. To znamená, že $\vec{\alpha}_1$, $\vec{\beta}_1$ sú (jednoznačne určené) vektory z V, pre ktoré platí $f(\vec{\alpha}_1) = \vec{\alpha}$ a $f(\vec{\beta}_1) = \vec{\beta}$. Potom (pre ľubovoľné $c, d \in F$) platí

$$f(c\vec{\alpha}_1 + d\vec{\beta}_1) = cf(\vec{\alpha}_1) + df(\vec{\beta}_1) = c\vec{\alpha} + d\vec{\beta}.$$

Zistili sme, že vektor $c\vec{\alpha}_1 + d\vec{\beta}_1$ sa zobrazením f zobrazí na vektor $c\vec{\alpha} + d\vec{\beta}$, čo znamená

$$f^{-1}(c\vec{\alpha} + d\vec{\beta}) = c\vec{\alpha}_1 + d\vec{\beta}_1.$$

Pretože táto rovnosť platí pre ľubovoľné $c, d \in F$, podľa vety 5.3.4 je zobrazenie f^{-1} lineárne. □

Vieme, že inverzné zobrazenie existuje iba k bijektívnym zobrazeniam. V prípade, že je zobrazenie f lineárne, vieme odvodiť pomerne jednoduché kritérium na zistenie či je to bijekcia. Najprv dokážeme lemu, ktorá charakterizuje injektívne a surjektívne lineárne zobrazenia.

Lema 5.5.2. *Nech $f\colon V \to W$ je lineárne zobrazenie a $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ je báza priestoru V.*

(i) *Zobrazenie f je injekcia práve vtedy, keď vektory $f(\vec{\alpha}_1), \ldots, f(\vec{\alpha}_n)$ sú lineárne nezávislé.*

(ii) *Zobrazenie f je surjekcia práve vtedy, keď $[f(\vec{\alpha}_1), \ldots, f(\vec{\alpha}_n)] = W$ (teda ak vektory $f(\vec{\alpha}_1), \ldots, f(\vec{\alpha}_n)$ generujú celý priestor W).*

Dôkaz časti (i). $\boxed{\Rightarrow}$ Nech

$$c_1 f(\vec{\alpha}_1) + \ldots + c_n f(\vec{\alpha}_n) = \vec{0}.$$

Z linearity zobrazenia f dostaneme

$$f(c_1\vec{\alpha}_1 + \cdots + c_n\vec{\alpha}_n) = f(\vec{0}).$$

Pretože f je prosté, vyplýva z tejto rovnosti

$$c_1\vec{\alpha}_1 + \cdots + c_n\vec{\alpha}_n = \vec{0}$$

a keďže vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ sú lineárne nezávislé, dostávame $c_1 = \ldots = c_n = 0$. Z rovnosti $c_1 f(\vec{\alpha}_1) + \ldots + c_n f(\vec{\alpha}_n) = \vec{0}$ sme odvodili, že všetky koeficienty vystupujúce v tejto lineárnej kombinácii sú nulové, teda vektory $f(\vec{\alpha}_1), \ldots, f(\vec{\alpha}_n)$ sú skutočne lineárne nezávislé.

$\boxed{\Leftarrow}$ Nech pre nejaké vektory $\vec{\alpha}, \vec{\beta} \in V$ platí $f(\vec{\alpha}) = f(\vec{\beta})$. Vektory $\vec{\alpha}$ a $\vec{\beta}$ vieme vyjadriť pomocou bázových vektorov

$$\vec{\alpha} = c_1\vec{\alpha}_1 + \cdots + c_n\vec{\alpha}_n$$
$$\vec{\beta} = d_1\vec{\alpha}_1 + \cdots + d_n\vec{\alpha}_n$$

Odčítaním týchto 2 rovností dostaneme $\vec{\alpha} - \vec{\beta} = (c_1 - d_1)\vec{\alpha}_1 \ldots + (c_n - d_n)\vec{\alpha}_n$. Ak zobrazíme obe strany tejto rovnosti lineárnym zobrazením f, dostaneme

$$\vec{0} = f(\vec{\alpha}) - f(\vec{\beta}) = f(\vec{\alpha} - \vec{\beta}) = (c_1 - d_1)f(\vec{\alpha}_1) + \ldots + (c_n - d_n)f(\vec{\alpha}_n).$$

Pretože podľa predpokladu sú $f(\vec{\alpha}_1), \ldots, f(\vec{\alpha}_n)$ lineárne nezávislé, vyplýva z toho $c_i - d_i = 0$, čo znamená, že $c_i = d_i$ (pre $i = 1, 2, \ldots, n$) a $\vec{\alpha} = \vec{\beta}$.

Dôkaz časti (ii). $\boxed{\Rightarrow}$ Inklúzia $[f(\vec{\alpha}_1), \ldots, f(\vec{\alpha}_n)] \subseteq W$ je zrejmá, potrebujeme dokázať obrátenú inklúziu. Nech $\vec{\alpha}$ je ľubovoľný vektor z W. Pretože zobrazenie f je surjektívne, existuje vektor $\vec{\beta} \in V$ taký, že $f(\vec{\beta}) = \vec{\alpha}$. Vektor $\vec{\beta}$ sa dá vyjadriť ako lineárna kombinácia bázových vektorov

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

Z toho dostaneme

$$\vec{\alpha} = f(\vec{\beta}) = c_1 f(\vec{\alpha}_1) + \ldots + c_n f(\vec{\alpha}_n),$$

čo znamená, že $\vec{\alpha} \in [f(\vec{\alpha}_1), \ldots, f(\vec{\alpha}_n)]$.

$\boxed{\Leftarrow}$ Nech $\vec{\gamma} \in W = [f(\vec{\alpha}_1), \ldots, f(\vec{\alpha}_n)]$. Potom existujú skaláry $c_1, \ldots, c_n \in F$ také, že

$$\gamma = c_1 f(\vec{\alpha}_1) + \ldots + c_n f(\vec{\alpha}_n) = f(c_1\vec{\alpha}_1 + \cdots + c_n\vec{\alpha}_n).$$

Našli sme vzor pre ľubovoľný vektor $\vec{\gamma} \in W$, čo znamená, že zobrazenie f je surjektívne. □

Z predchádzajúcej lemy priamo vyplýva

Veta 5.5.3. *Nech $f\colon V \to W$ je lineárne zobrazenie a $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ je báza priestoru V. Zobrazenie f je bijekcia práve vtedy, keď vektory $f(\vec{\alpha}_1), \ldots, f(\vec{\alpha}_n)$ tvoria bázu vektorového priestoru W.*

Dôsledok 5.5.4. *Nech $f\colon F^n \to F^n$ je lineárne zobrazenie. Nasledujúce podmienky sú ekvivalentné:*

(i) *f je bijekcia,*

(ii) *f je prosté,*

(iii) *f je surjektívne.*

Dôkaz. V priestore s dimenziou n je $f(\vec{\alpha}_1), \ldots, f(\vec{\alpha}_n)$ báza $\Leftrightarrow$ tieto vektory sú lineárne nezávislé $\Leftrightarrow$ $[f(\vec{\alpha}_1), \ldots, f(\vec{\alpha}_n)] = F^n$. □

Dôsledok 5.5.5. *Nech $f\colon F^n \to F^n$ je lineárne zobrazenie. Nasledujúce podmienky sú ekvivalentné:*

(a) *zobrazenie f je bijekcia,*

(b) *existuje inverzné zobrazenie* f^{-1},

(c) $h(A_f) = n$.

Dôkaz. Stačí si uvedomiť, že hodnosť matice je dimenzia priestoru prislúchajúceho tejto matici, čo je v našom prípade celý priestor F^n.

Obrátene, ak je hodnosť matice A_f rovná n, tak jej riadky tvoria n lineárne nezávislých vektorov v priestore dimenzie n, sú teda bázou celého priestoru. Riadky matice A_f sú však práve obrazy vektorov štandardnej bázy. □

Definícia 5.5.6. Nech A je matica typu $n \times n$. Hovoríme, že matica B je *inverzná* k matici A, ak platí

$$AB = BA = I_n.$$

Označujeme ju $B =: A^{-1}$.

Poznámka 5.5.7. Predchádzajúca definícia vlastne hovorí, že $f_A \circ f_B = f_B \circ f_A = id$, čiže inverzná matica je práve matica zodpovedajúca inverznému zobrazeniu. Práve tento fakt využijeme pri výpočte inverznej matice – budeme postupovať takým spôsobom, že vypočítame maticu inverzného zobrazenia postup z úlohy 5.3.1. (Čiže začneme s maticou $(A|I)$ a upravujeme ju kým nedostaneme maticu $(I|A^{-1})$.)

Poznámka 5.5.8. Je užitočné si uvedomiť, že akonáhle platí niektorá z rovností $AB = I$ alebo $BA = I$, tak už B musí byť inverzná matica k A.

Aby sme to overili, preložme tieto rovnosti do rečí skladania zobrazení. Dostaneme

$$f_B \circ f_A = id$$
$$f_A \circ f_B = id$$

Využijeme úlohy 2.2.1 a 2.2.2. V prvom prípade vidíme, že f_A je injekcia (lebo zložené zobrazenie je injekcia) a podľa dôsledku 5.5.4 je potom f_A bijekcia. Podobne, v druhom prípade dostaneme, že f_A je surjekcia, čiže aj bijekcia.

Preto (v oboch prípadoch) má matica A inverznú maticu A^{-1}. Ak ňou vynásobíme rovnosť $AB = I$ zľava, dostaneme $B = A^{-1}$. Ak predpokladáme platnosť rovnosti $BA = I$, môžeme ju vynásobiť A^{-1} sprava a opäť máme $B = A^{-1}$.

V oboch prípadoch sme dostali rovnosť $B = A^{-1}$, čiže pre matice $n \times n$ stačí overiť jednu z uvedených rovností. (Môže však existovať matica typu $m \times n$ pre $m \neq n$ taká, že $BA = I$, tá samozrejme nie je inverznou maticou k A.)

Definícia 5.5.9. Štvorcová matica typu $n \times n$ sa nazýva *regulárna,* ak $h(A) = n$.

Z dôsledku 5.5.5 vyplýva nasledujúca veta.

Veta 5.5.10. *Nech A je matica typu $n \times n$. K matici A existuje inverzná matica práve vtedy, keď A je regulárna.*

Definícia 5.5.11. Bijektívne lineárne zobrazenie $f\colon V \to W$ nazývame *izomorfimus vektorových priestorov* V a W (alebo tiež *lineárny izomorfizmus*).

Ak existuje bijektívne zobrazenie $f\colon V \to W$, hovoríme, že vektorové priestory V a W sú izomorfné. Fakt, že V a W sú izomorfné označujeme $V \cong W$.

Poznámka 5.5.12. Vieme, že bijektívne zobrazenie je jedno-jednoznačné priradenie medzi prvkami množiny V a prvkami množiny W. Ak je toto zobrazenie navyše lineárne, znamená

to, že táto jedno-jednoznačná korešpondencia navyše rešpektuje operácie definované na vektorových priestoroch V a W.

Fakt, že 2 vektorové priestory sú izomorfné, teda znamená, že sú v podstate rovnaké, len ich prvky sú inak označené (pomenované). Izomorfizmus poskytuje „preklad“ medzi týmito dvoma pomenovaniami.

Nasledujúca veta hovorí, že každý priestor dimenzie n je izomorfný priestoru F^n. (A teda každý konečnorozmerný priestor je izomorfný s F^n pre niektoré n.)

Veta 5.5.13. *Nech V je vektorový priestor nad poľom F a $d(V) = n$. Potom V je izomorfný s priestorom F^n.*

Dôkaz. Ak $d(V) = n$, znamená to, že V má n-prvkovú bázu $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$. Podľa vety 5.3.6 existuje jediné lineárne zobrazenie $f\colon V \to F^n$ s vlastnosťou $f(\vec{\alpha}_1) = \vec{\varepsilon}_1, \ldots, f(\vec{\alpha}_n) = \vec{\varepsilon}_n$. Podľa vety 5.5.3 je toto zobrazenie bijekcia, čiže je to izomorfizmus medzi V a F^n. $\square$

Cvičenia

Úloha 5.5.1. Nájdite inverznú maticu k daným maticiam nad R:
$\begin{pmatrix} 2 & 3 & 1 \\ 4 & 3 & 3 \\ 1 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 3 & 1 \\ 2 & 4 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 0 & 3 & 1 \\ 2 & 0 & 3 \\ 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 0 & 1 \\ 0 & 3 & 2 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 2 & -1 & 3 \end{pmatrix} \begin{pmatrix} 3 & 2 & 1 \\ 4 & 2 & 1 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \sqrt{2} & \sqrt{6} \\ 0 & 1 & \sqrt{3} \\ 0 & 0 & 1 \end{pmatrix}$ Výsledky:
$\begin{pmatrix} \frac{3}{4} & \frac{1}{4} & -\frac{3}{2} \\ \frac{1}{4} & -\frac{1}{4} & \frac{1}{2} \\ -\frac{5}{4} & \frac{1}{4} & \frac{3}{2} \end{pmatrix} \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{10} & -\frac{1}{10} \\ -1 & \frac{4}{5} & -\frac{1}{5} \end{pmatrix} \begin{pmatrix} 3 & 5 & -9 \\ 1 & 1 & -2 \\ -2 & -3 & 6 \end{pmatrix} \begin{pmatrix} \frac{1}{2} & 0 & -\frac{1}{2} \\ \frac{1}{3} & \frac{1}{3} & -1 \\ -\frac{1}{2} & 0 & \frac{3}{2} \end{pmatrix} \begin{pmatrix} 2 & -\frac{1}{2} & -\frac{1}{2} \\ 1 & \frac{1}{2} & -\frac{1}{2} \\ -1 & \frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} -1 & 1 & 0 \\ \frac{3}{2} & -1 & -\frac{1}{2} \\ 1 & -1 & -1 \end{pmatrix} \begin{pmatrix} 1 & -\sqrt{2} & 0 \\ 0 & 1 & -\sqrt{3} \\ 0 & 0 & 1 \end{pmatrix}$

Úloha 5.5.2. Nech $f\colon (\mathbb{Z}_5)^4 \to (\mathbb{Z}_5)^4$ je lineárne zobrazenie také, že $f(1,2,3,1) = (2,0,1,0)$, $f(0,2,3,1) = (1,2,0,3)$, $f(1,0,3,4) = (3,2,1,0)$, $f(4,1,3,2) = (2,3,1,1)$. Nájdite maticu zobrazenia f^{-1}.

Úloha 5.5.3. Zistite, či $\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ je regulárna a) nad $\mathbb{Z}_2$ b) nad $\mathbb{Z}_3$, ak áno, nájdite inverznú.

Úloha 5.5.4*. Vypočítajte $A^{-1}B$ a $B^{-1}A$. Skúste to urobiť bez výpočtu A^{-1} resp. B^{-1}.
$A = \begin{pmatrix} 0 & 3 & 1 \\ 2 & 0 & 3 \\ 1 & 1 & 2 \end{pmatrix}$ $B = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & -1 \\ 0 & -1 & 2 \end{pmatrix}$
Ako skúšku správnosti môžete vyskúšať, či po vynásobení výsledku zľava maticou A (resp. B) dostanete maticu B (resp. A).

5.6 Elementárne riadkové operácie a súčin matíc*

V tejto časti si povieme, ako môžeme elementárne riadkové (stĺpcové) operácie vyjadriť pomocou násobenia matíc.

Definícia 5.6.1. Pre ľubovoľnú elementárnu riadkovú operáciu na matici typu $m \times n$ nazveme *maticou elementárnej riadkovej operácie* maticu typu $m \times m$, ktorá vznikne vykonaním tejto operácie na jednotkovej matici I_m.

Podobne môžeme definovať maticu sĺpcovej operácie.

Príklad 5.6.2. Uvažujme matice s 3 riadkami. Potom výmene prvého a tretieho riadku zodpovedá matica E_1, pripočítaniu dvojnásobku druhého riadku k prvému matica E_2 a vynásobeniu prvého riadku číslom 3 matica E_3.

$$E_1 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \qquad E_2 = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad E_3 = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Vedeli by ste nájsť stĺpcové operácie, ktorým by zodpovedali tieto 3 matice? (Odpoveď: Výmena prvého a tretieho stĺpca, pripočítanie 2-násobku prvého stĺpca k druhému a vynásobenie prvého stĺpca číslom 3.)

Tvrdenie 5.6.3. *Ak matica B vznikne z matice A vykonaním nejakej elementárnej riadkovej operácie a E je matica tejto riadkovej operácie, tak $B = E.A$.*

Príklad 5.6.4. Ak $A = \begin{pmatrix} 1 & 0 \\ 1 & 2 \\ -1 & -1 \end{pmatrix}$ a E_2 je matica z predchádzajúceho príkladu, tak $E_2A = \begin{pmatrix} 3 & 4 \\ 1 & 2 \\ -1 & -1 \end{pmatrix}$ je skutočne matica, ktorá vznikne z A pripočítaním dvojnásobku druhého riadku k prvému.

Dôkaz. Tvrdenie overíme jednoducho priamym výpočtom. Budeme postupovať pre každý typ elementárnej riadkovej operácie zvlášť.

Nech $A = ||a_{ij}||$ je matica typu $m \times n$.

Výmene k-teho a l-teho riadku zodpovedá matica $E = ||e_{ij}||$, ktorej prvky sú len nuly a jednotky, pričom jednotky sú iba na pozíciach e_{ii} pre $i \neq k, l$ a tiež e_{kl} a e_{lk}. Vidíme, že v súčine $E.A$ budú všetky riadky okrem k-teho a l-teho rovnaké ako v matici A. (Vo výraze $\sum_{t=1}^{m} e_{it}a_{tj}$ jediný nenulový sčítanec je $e_{ii}a_{ij} = a_{ij}$.) Podobne v k-tom riadku dostaneme prvky l-teho riadku a obrátene.

$$\sum_{t=1}^{m} e_{kt}a_{tj} = e_{kl}a_{lj} = a_{lj},$$
$$\sum_{t=1}^{m} e_{lt}a_{tj} = e_{lk}a_{kj} = a_{kj}.$$

Matica $E.A$ je teda skutočne matica, ktorá vznikne výmenou týchto 2 riadkov.

Vynásobeniu k-teho riadku skalárom c zodpovedá matica E, ktorá má mimo diagonály nuly a na diagonále jednotky s výnimkou prvkov $e_{kk} = c$. Opäť sa nezmenia ostatné riadky a v k-tom riadku dostávame

$$\sum_{t=1}^{m} e_{kt}a_{tj} = e_{kk}a_{kj} = ca_{kj}.$$

Teda k-ty riadok novej matice je skutočne c-násobok k-teho riadku pôvodnej matice.

Teraz uvažujme pripočítanie c-násobku l-teho riadku ku k-temu. V tomto prípade má matica E na diagonále jednotky a mimo diagonály je jediný nenulový prvok $e_{kl} = c$. Opäť vidno, že mimo k-teho riadku sa prvky nezmenia. V k-tom riadku dostaneme

$$\sum_{t=1}^{m} e_{kt}a_{tj} = e_{kk}a_{kj} + e_{kl}a_{lj} = a_{kj} + ca_{lj}.$$

Teda k-ty riadok matice $E.A$ je skutočne súčet k-teho riadku matice A a c-násobku l-tého riadku matice A. □

Úplne analogicky sa dá dokázať podobné tvrdenie pre stĺpcové operácie.

Tvrdenie 5.6.5. *Ak matica B vznikne z matice A vykonaním nejakej elementárnej stĺpcovej operácie a E je matica tejto stĺpcovej operácie, tak $B = A.E$.*

Užitočné je si všimnúť, že matica ľubovoľnej elementárnej riadkovej operácie je regulárna a inverzná matica k nej je tiež matica elementárnej riadkovej operácie. (Dalo by sa povedať, že je to matica „inverznej“ riadkovej operácie – pozri poznámku 5.2.6. Práve fakt, že elementárne riadkové operácie sú invertovateľné môžeme použiť ako jednu z možností na zdôvodnenie, že matice elementárnych riadkových operácií sú regulárne.)

Poznámka 5.6.6. Ak A je ľubovoľná matica, tak pomocou elementárnych riadkových operácií z nej vieme dostať redukovanú trojuholníkovú maticu

$$R = E_1 E_2 \dots E_k A.$$

Potom platí

$$A = E_k^{-1} \dots E_2^{-1} E_1^{-1} R.$$

Takto sme maticu A vyjadrili ako súčin pomerne jednoduchých matíc (jedna z nich je v redukovanom trojuholníkovom tvare, ostatné sú matice elementárnych riadkových operácií). To môže byť užitočné v dôkazoch niektorých tvrdení – hlavne v prípade, že dokazované tvrdenie vieme ľahko dokázať pre matice takéhoto tvaru a tiež vieme dokázať, že platnosť tvrdenia sa zachová ak prejdeme k súčinu matíc.

Ilustráciou tohoto prístupu je napríklad alternatívny dôkaz vety 5.7.2.

Pomocou tohoto vzťahu medzi násobením matíc a môžeme lepšie porozumieť spôsobu, akým sme počítali inverzné matice.

Začali sme s maticou

$$(A|I)$$

a v každom kroku sme urobili nejakú riadkovú operáciu, ktorá zodpovedá vynásobeniu oboch častí matice zľava nejakou maticou riadkovej operácie.

$$(A|I) \sim (E_1 A|E_1 I) \sim (E_2 E_1 A|E_2 E_1 I) \sim \dots \sim (E_n \dots E_2 E_1 A|E_n \dots E_2 E_1 I) = (I|E),$$

kde ako E sme označili maticu $E := E_n \dots E_2 E_1$. Pretože táto matica spĺňa rovnosť $EA = I$ (túto rovnosť vidíme z ľavej časti matice), je to inverzná matica k A. Tiež si môžeme všimnúť, že v každom kroku dostaneme maticu tvaru $(DA|D)$, t.j. ak vynásobíme pravú časť sprava maticou A, dostaneme ľavú časť matice.

Podobne sa dá pozerať aj na riešenie sústav lineárnych rovníc, ktorými sa budeme zaoberať v nasledujúcej kapitole.

Takisto pri výpočte matice zobrazenia sme mali zadaných viacero podmienok tvaru $\vec{\beta}_i A = \vec{\gamma}_i$. Ak poukladáme vektory $\vec{\beta}_i$ do matice B ako riadky a podobne z vektorov $\vec{\gamma}_i$ vytvoríme maticu C, tieto podmienky môžeme zapísať ako jedinú maticovú rovnosť

$$BA = C.$$

Pri výpočte sme postupovali tak, že sme maticu C zľava násobili nejakými maticami riadkových operácií, a to konkrétne takými, že z matice B vytvoria jednotkovú maticu, čiže ich súčin je matica I.

To znamená, že $A = B^{-1}C$ (ak B je regulárna) alebo presnejšie, $A = B'C$, kde B' je taká matica, že $B'B = I$.

Poznámka 5.6.7. Ďalší užitočný fakt, ktorý by nám mal byť po prečítaní tejto kapitoly jasný, je, že násobenie maticou A zľava zodpovedá vytvoreniu lineárnych kombinácii riadkov v matici B (riadky matice A určujú koeficienty).

Podobne, ak maticu B násobíme maticou A sprava, tak stĺpce v BA budú lineárne kombinácie stĺpcov B s koeficientmi určenými stĺpcami matice A.

(Videli sme, že niečo takéto platí pre matice riadkových operácií. Priamo z definície násobenia matíc sa dá overiť, že to platí aj pre ľubovoľné matice.)

5.7 Sústavy lineárnych rovníc

Definícia 5.7.1. *Sústavou lineárnych rovníc* rozumieme systém rovníc tvaru

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= c_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= c_2 \\ &\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n &= c_m \end{aligned} \tag{5.2}$$

kde $a_{ij}, c_i \in F$ pre všetky prípustné hodnoty indexov i a j.

Riešenie sústavy lineárnych rovníc je n-tica $(x_1, \ldots, x_n)$ ktorá spĺňa všetky uvedené rovnice. Ak existuje aspoň jedno riešenie sústavy lineárnych rovníc, hovoríme, že táto sústava je *riešiteľná.* Skaláry $c_1, \ldots, c_n$ nazývame *pravé strany,* a_{ij} sú *koeficienty* a x_i sú neznáme.

Maticu

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

nazývame *matica sústavy* (5.2).

Maticu

$$A' = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} & c_1 \\ a_{21} & a_{22} & \ldots & a_{2n} & c_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} & c_m \end{pmatrix}$$

nazývame *rozšírená matica sústavy* (5.2).

Pomocou matice sústavy môžeme zadefinovať *maticový zápis* sústavy

$$A\vec{x}^T = \vec{c}^T$$

alebo

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_m \end{pmatrix}$$

Skutočne, $(x_1, \ldots, x_n)$ je riešením sústavy (5.2) práve vtedy, keď platí uvedená maticová rovnosť.

Veta 5.7.2. *Ak rozšírené matice dvoch sústav lineárnych rovníc sú riadkovo ekvivalentné, tak tieto dve sústavy majú rovnakú množinu riešení.*

Dôkaz. Predpokladajme, že z rozšírenej matice sústavy $(A|c)$ sme dostali nejakou elementárnou riadkovou operáciou maticu $(B|d)$. Vďaka tomu, že elementárne riadkové operácie sú invertibilné (t.j. možno ich obrátiť, pozri poznámku 5.2.6) stačí nám dokázať, že každé riešenie sústavy $(A|c)$ je aj riešením sústavy $(B|d)$.

Výmena riadkov je vlastne výmena 2 rovníc, čo samozrejme neovplyvní, či $(x_1, \ldots, x_n)$ je riešením sústavy.

Ak prenásobíme i-ty riadok skalárom $c \neq 0$, znamená to, že z rovnice $a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n = c_i$ dostaneme rovnicu $ca_{i1}x_1 + ca_{i2}x_2 + \ldots + ca_{in}x_n = cc_i$. Pretože druhá rovnica je

c-násobkom prvej, je jasné, že ak $x_1, x_2, \ldots, x_n$ spĺňa prvú uvedenú rovnicu, musí spĺňať aj druhú z nich.

Zostáva nám posledný typ elementárnych riadkových úprav. Predpokladajme, že sme novú maticu získali pripočítanim c-násobku j-teho riadka k i-temu riadku. To znamená, že i-ta rovnica sústavy sa zmenila na rovnicu

$$(a_{i1} + ca_{j1})x_1 + (a_{i2} + ca_{j2})x_2 + \ldots + (a_{in} + ca_{jn})x_n = c_i + cc_j.$$

Ak však $x_1, \ldots, x_n$ spĺňa rovnosť $a_{j1}x_1 + a_{j2}x_2 + \ldots + a_{jn}x_n = c_j$, tak spĺňa aj jej c-násobok $ca_{j1}x_1 + ca_{j2}x_2 + \ldots + ca_{jn}x_n = cc_j$. Sčítaním tejto rovnice a rovnice $a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n = c_i$ dostaneme práve i-ty riadok novej sústavy. Pretože $x_1, \ldots, x_n$ spĺňa obe uvedené rovnice, musí spĺňať aj rovnicu, ktorú dostaneme ich sčítaním. □

Pomocou toho, čo sme sa dozvedeli o súvise elementárnych riadkových úprav s násobením matíc v časti 5.6 môžeme dokázať tú istú vetu aj iným spôsobom, ktorý je snáď do istej miery jasnejší (alebo prinajmenšom stručnejšie zapísaný – lebo hovorí to isté, čo predchádzajúci dôkaz, iba používa trochu iný pohľad na elementárne riadkové operácie).

Dôkaz.* Označme maticu uvažovanej elementárnej riadkovej operácie E. Uvedomme si najprv, že urobiť elementárnu riadkovú úpravu na rozšírenej matici sústavy je presne to isté, ako keby sme túto úpravu urobili zvlášť na matici A a zvlášť na stĺpcovom vektore $\vec{c}^T$. To znamená, že ak pôvodná sústava bola (pri zápise v maticovom tvare) $A\vec{x}^T = \vec{c}^T$, tak po úprave dostaneme.

$$EA\vec{x}^T = E\vec{c}^T.$$

Z toho vidíme, že každé riešenie pôvodnej sústavy je aj riešením sústavy s upravenou maticou (obe strany rovnosti sme vynásobili zľava tou istou maticou E, tým sme nezmenili platnosť rovnosti).

Obrátene, ak pre $\vec{x}$ platí $EA\vec{x}^T = E\vec{c}^T$, tak prenásobením tejto rovnosti maticou E^{-1} zľava dostaneme, že $\vec{x}$ je aj riešením pôvodnej sústavy. □

5.7.1 Homogénne sústavy lineárnych rovníc

V prípade, že pravé strany sú nulové ($c_1 = c_2 = \ldots = c_n = 0$), nazývame sústavu (5.2) *homogénna* sústava lineárnych rovníc. Ľahko si môžeme všimnúť, že v prípade homogénnej sústavy je nulový vektor $(0, 0, \ldots, 0)$ riešením sústavy. Toto riešenie nazývame *triviálne riešenie.*

Veta 5.7.3. *Množina všetkých riešení homogénnej sústavy lineárnych rovníc tvorí podpriestor priestoru F^n.*

Dôkaz. Stačí overiť vlastnosti z definície podpriestoru.

Ak $\vec{\alpha}$ a $\vec{\beta}$ sú riešeniami homogénnej sústavy s maticou A, znamená to, že $A.\vec{\alpha}^T = \vec{0}^T$ a $A.\vec{\beta}^T = \vec{0}^T$.

Sčítaním týchto rovností dostaneme $A.(\vec{\alpha} + \vec{\beta})^T = \vec{0}^T$, teda aj $\vec{\alpha} + \vec{\beta}$ je riešením tejto sústavy. Ak prvú rovnosť vynásobíme skalárom F, máme $A.(c\vec{\alpha})^T = \vec{0}^T$, čo znamená, že aj $c.\vec{\alpha}$ je riešením sústavy. □

Rozšírenú maticu sústavy lineárnych rovníc môžeme teda upraviť na redukovanú trojuholníkovú maticu. Predpokladajme, že sme navyše preusporiadali premenné (čo vlastne zodpovedá permutácii niektorých stĺpcov) tak, aby vo výslednej matici boli ako prvé tie stĺpce, kde vystupujú vedúce jednotky. Navyše môžeme vynechať všetky nulové riadky bez

toho, aby sme nejako ovplyvnili množinu riešení. Dostaneme takto maticu, ktorej zodpovedá sústava

$$\begin{aligned} x_1 + c_{1,r+1}x_{r+1} + c_{1,r+2}x_{r+2} + \ldots + c_{1,n}x_n &= 0 \\ x_2 + c_{2,r+1}x_{r+1} + c_{2,r+2}x_{r+2} + \ldots + c_{2,n}x_n &= 0 \\ &\ldots \\ x_r + c_{r,r+1}x_{r+1} + c_{r,r+2}x_{r+2} + \ldots + c_{r,n}x_n &= 0 \end{aligned} \tag{5.3}$$

pričom r označuje hodnosť pôvodnej matice (a teda aj matice C).

Vidíme, že ak si zvolíme hodnotu neznámych $x_{r+1}, x_{r+2} \ldots, x_n$, dá sa z týchto rovníc dorátať hodnota neznámych $x_1, x_2, \ldots, x_n$. Ak postupne dosadíme 1 za x_{r+k} a 0 za ostatné neznáme, ktoré si môžeme voliť (pre $k = 1, 2, \ldots, n - r$) dostaneme tieto riešenia sústavy sústavy (5.3):

$$\begin{aligned} \vec{\gamma}_{r+1} &= (-c_{1,r+1}, -c_{2,r+1}, \ldots, -c_{r,r+1}, 1, 0, \ldots, 0), \\ \vec{\gamma}_{r+2} &= (-c_{1,r+2}, -c_{2,r+2}, \ldots, -c_{r,r+2}, 0, 1, \ldots, 0), \\ &\ldots \\ \vec{\gamma}_n &= (-c_{1,n}, -c_{2,n}, \ldots, -c_{r,n}, 0, \ldots, 0, 1). \end{aligned} \tag{5.4}$$

Veta 5.7.4. *Vektory $\vec{\gamma}_{r+1}, \vec{\gamma}_{r+2}, \ldots, \vec{\gamma}_n$ tvoria bázu priestoru riešení homogénnej sústavy* (5.3).

Dôkaz. Z toho, ako sme ich získali, vieme, že tieto vektory sú riešenia (5.3).

Ich lineárnu nezávislosť overíme tiež pomerne jednoducho: ak

$$\vec{\alpha} = d_{r+1}\vec{\gamma}_{r+1} + d_{r+2}\vec{\gamma}_{r+2} + \cdots + d_n\vec{\gamma}_n = \vec{0}$$

tak vektor $\vec{\alpha}$ má na $(r + k)$-tej súradnici hodnotu d_{r+k}, z čoho dostaneme $d_{r+k} = 0$ pre $k = 1, 2, \ldots, n - r$.

Zostáva dokázať, že vektory $\vec{\gamma}_{r+1}, \vec{\gamma}_{r+2}, \ldots, \vec{\gamma}_n$ generujú celý priestor riešení, teda že každé riešenie homogénnej sústavy (5.3) možno získať ako ich lineárnu kombináciu.

Nech teda $b_1, b_2, \ldots, b_n$ je riešením (5.3). Z toho dostaneme

$$b_i = -c_{i,r+1}b_{r+1} - c_{i,r+2}b_{r+2} - \ldots - c_{i,n}b_n$$

pre $i = 1, 2, \ldots, r$. Z týchto rovností priamo vyplýva

$$\vec{\beta} = b_{r+1}\vec{\gamma}_{r+1} + b_{r+2}\vec{\gamma}_{r+2} + \ldots + b_n\vec{\gamma}_n,$$

teda vektor $\vec{\beta}$ je lineárnou kombináciou vektorov $\vec{\gamma}_{r+1}, \vec{\gamma}_{r+2}, \ldots, \vec{\gamma}_n$. □

Dôsledok 5.7.5. *Nech A je matica typu $m \times n$ a S je priestor riešení homogénnej sústavy lineárnych rovníc s maticou A. Potom*

$$d(S) = n - h(A).$$

Dôsledok 5.7.6. *Homogénna sústava lineárnych rovníc s n neznámymi, ktorej matica má hodnosť n, má len triviálne riešenie.*

Ilustrujme si predchádzajúci postup na dvoch veľmi jednoduchých príkladoch homogénnych sústav lineárnych rovníc nad $\mathbb{R}$.

Príklad 5.7.7. $\left(\begin{array}{ccc|c} 1&1&1&0\\ 1&0&1&0\\ 0&1&1&0 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1&0&1&0\\ 0&1&0&0\\ 0&1&1&0 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1&0&1&0\\ 0&1&0&0\\ 0&0&1&0 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1&0&0&0\\ 0&1&0&0\\ 0&0&1&0 \end{array}\right)$

V tomto prípade nám nezostali žiadne premenné, ktoré by sme mohli voliť – vo všetkých stĺpcoch máme vedúce jednotky. Prepísaním sústavy z maticového zápisu priamo dostaneme (ako jediné možné riešenie) triviálne riešenie $x_1 = 0$, $x_2 = 0$, $x_3 = 0$.

Poznámka 5.7.8. Všimnime si, že na pravé strany pri všetkých elementárnych riadkových úpravách zostávajú nulové. Kvôli stručnejšiemu zápisu, pri riešení homogénnych sústav budeme vynechávať pravé strany a budeme namiesto rozšírenej matice sústavy písať len maticu sústavy. (Budeme si pamätať, že pravé strany sú nuly, ale nebudeme ich po každom kroku znovu písať.)

Príklad 5.7.9. Vynechajme teraz z predchádzajúcej sústavy jednu rovnicu. Úpravou na redukovanú trojuholníkovú maticu dostaneme

$\left(\begin{array}{ccc} 1&1&1\\ 1&0&1 \end{array}\right) \sim \left(\begin{array}{ccc} 1&0&1\\ 0&1&0 \end{array}\right)$

Vidíme, že sústava je ekvivalentná so sústavou $x_1+x_3 = 0$ a $x_2 = 0$. Premennú x_3 môžeme voliť (v treťom stĺpci nie je vedúca jednotka). Nech teda $x_3 = t$, kde $t \in \mathbb{R}$ je parameter. Keď z predchádzajúcich rovníc vyjadríme x_1 a x_2, máme $x_1 = -t$ a $x_2 = 0$. Množina riešení tejto sústavy je teda $\{(t, 0, -t); t \in \mathbb{R}\}$.

Ľahko môžeme overiť, že množina riešení je skutočne podpriestor priestoru $\mathbb{R}^3$. Pretože každý vektor z množiny riešení má tvar $t.(1, 0, -1)$, môžeme ju zapísať aj ako $\{(t, 0, -t); t \in \mathbb{R}\} = [(1, 0, -1)]$.

Aj postup riešenia nehomogénnych sústav je veľmi podobný – podrobnejšie ho rozoberieme v nasledujúcej podkapitole. Predtým však ešte dokážeme vetu, ktorú môžeme chápať ako obrátenie vety 5.7.3.

Veta 5.7.10. *Každý podpriestor priestoru F^n je množinou riešení nejakého homogénneho systému lineárnych rovníc.*

Dôkaz. Ak S je podpriestor F^n, tak S je konečnorozmerný (veta 4.4.17). Má teda konečnú bázu $\vec{\alpha}_1, \ldots, \vec{\alpha}_r$.

Nech B je matica, ktorej riadky tvoria vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_r$,

$$B = \begin{pmatrix} \vec{\alpha}_1 \\ \vdots \\ \vec{\alpha}_r \end{pmatrix}.$$

Podľa predchádzajúcej vety má podpriestor riešení homogénnej sústavy

$$B \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \vec{0}^T$$

bázu $\vec{\gamma}_{r+1}, \ldots, \vec{\gamma}_n$.

Označme ako A maticu, ktorej riadkami sú vektory $\vec{\gamma}_{r+1}, \ldots, \vec{\gamma}_n$,

$$A = \begin{pmatrix} \vec{\gamma}_{r+1} \\ \vdots \\ \vec{\gamma}_n \end{pmatrix}.$$

Pretože každý vektor $\vec{\gamma}_i$ je riešením sústavy s maticou B, platí $B.\vec{\gamma}_i^T = \vec{0}^T$. Z toho dostaneme

$$B.A^T = 0$$

(treba si uvedomiť, že i-ty stĺpec matice A je $\vec{\gamma}_i^T$, z čoho vyplýva, že stĺpce matice $B.A^T$ môžeme vypočítať ako $B.\vec{\gamma}_i^T$). Transponovaním predchádzajúceho vzťahu dostaneme (na základe (5.1))

$$A.B^T = 0.$$

Keď porovnáme i-ty stĺpec matice na ľavej a pravej strane predchádzajúcej rovnosti, dostaneme

$$A\vec{\alpha}_i^T = \vec{0}^T,$$

teda vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_r$ sú riešeniami homogénnej sústavy $A\vec{x}^T = \vec{0}^T$.

Označme ako M priestor riešení tejto sústavy. Jeho dimenzia je

$$d(M) = n - h(A) = n - (n - r) = r.$$

Súčasne platí $S \subseteq M$ (pretože všetky vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_r$ patria do M) a $d(S) = d(M)$, teda podľa tvrdenia 4.4.18 platí $S = M$. □

5.7.2 Gaussova eliminačná metóda

Gaussovou eliminačnou metódou nazývame algoritmus na riešenie sústav lineárnych rovníc, o ktorom sme hovorili v predchádzajúcej kapitole. Ide teda o postup, pri ktorom rozšírenú maticu sústavy najprv upravíme na redukovanú trojuholníkovú maticu a z nej už potom vieme zistiť riešenie pôvodnej sústavy.

V prípade, že počas úprav dostaneme riadok tvaru $(0 \ldots 0|c)$, kde $c \neq 0$, sústava nemá riešenie. (Takýto riadok zodpovedá rovnici $0x_1 + \ldots + 0x_n = c$.) V takomto prípade samozrejme nemusíme ďalej pokračovať v upravovaní na RTM.

Ak niektoré stĺpce (v upravenej matici) neobsahujú vedúcu jednotku, tak im prislúchajúce premenné zvolíme za parametre.

Ukážeme si tento postupu na niekoľkých jednoduchých príkladoch. V prípade homogénnych sústav sme mali dve možnosti – buď existovalo jediné riešenie (pri homogénnej sústave to bolo triviálne riešenie) alebo riešení bolo viac (tvorili podpriestor). Pri nehomogénnej sústave lineárnych rovníc už množina riešení netvorí vektorový podpriestor a navyše pribudne ešte ďalšia možnosť – môže sa stať, že sústava nemá nijaké riešenie.

Príklad 5.7.11. Riešme sústavu

$$\begin{array}{rrrrl} x_1 & -2x_2 & +3x_3 & -4x_4 & = 4 \\ & x_2 & -x_3 & +x_4 & = -3 \\ x_1 & +3x_2 & & -3x_4 & = 1 \\ & -7x_2 & +3x_3 & +x_4 & = 3 \end{array}$$

nad poľom $\mathbb{R}$.

Danú sústavu najprv prepíšeme do matice a potom upravujeme rozšírenú maticu sústavy až kým nedostaneme redukovaný trojuholníkový tvar.

$$\begin{pmatrix} 1 & -2 & 3 & -4 & | & 4 \\ 0 & 1 & -1 & 1 & | & -3 \\ 1 & 3 & 0 & -3 & | & 1 \\ 0 & -7 & 3 & 1 & | & -3 \end{pmatrix} \overset{(1)}{\sim} \begin{pmatrix} 1 & -2 & 3 & -4 & | & 4 \\ 0 & 1 & -1 & 1 & | & -3 \\ 0 & 5 & -3 & 1 & | & -3 \\ 0 & -7 & 3 & 1 & | & -3 \end{pmatrix} \overset{(2)}{\sim} \begin{pmatrix} 1 & -2 & 3 & -4 & | & 4 \\ 0 & 1 & -1 & 1 & | & -3 \\ 0 & 0 & 2 & -4 & | & 12 \\ 0 & 0 & -4 & 8 & | & -24 \end{pmatrix} \overset{(3)}{\sim} \begin{pmatrix} 1 & -2 & 3 & -4 & | & 4 \\ 0 & 1 & -1 & 1 & | & -3 \\ 0 & 0 & 1 & -2 & | & 6 \\ 0 & 0 & 1 & -2 & | & 6 \end{pmatrix}$$

$$\overset{(4)}{\sim} \begin{pmatrix} 1 & -2 & 3 & -4 & | & 4 \\ 0 & 1 & -1 & 1 & | & -3 \\ 0 & 0 & 1 & -2 & | & 6 \\ 0 & 0 & 0 & 0 & | & 0 \end{pmatrix} \overset{(5)}{\sim} \begin{pmatrix} 1 & -2 & 3 & -4 & | & 4 \\ 0 & 1 & 0 & -1 & | & -3 \\ 0 & 0 & 1 & -2 & | & 6 \\ 0 & 0 & 0 & 0 & | & 0 \end{pmatrix} \overset{(6)}{\sim} \begin{pmatrix} 1 & 0 & 0 & 0 & | & -8 \\ 0 & 1 & 0 & -1 & | & 3 \\ 0 & 0 & 1 & -2 & | & 6 \\ 0 & 0 & 0 & 0 & | & 0 \end{pmatrix}$$

(1) `3.r-=1.r` (Týmto zápisom myslím to, že od tretieho riadku sa odčíta prvý.)
(2) `3.r-=5*2.r; 4.r+=7*1.r`
(3) `3.r*=1/2; 4.r*=-1/4`
(4) `3.r-=4.r`
(5) `2.r+=3.r`
(6) `1.r+=2*2.r-3*3.r`

Štvrtý stĺpec neobsahuje vedúcu jednotku. Preto x_4 zvolíme za parameter - položíme $x_4 = t$. Dostaneme potom $x_1 = -8$, $x_2 = t+3$, $x_3 = 2t+6$. Množina všetkých riešení je teda $\underline{\underline{\{(-8, 3+t, 6+2t, t); t \in \mathbb{R}\}}}$.

(Ak by bola vedúca jednotka v každom stĺpci redukovanej trojuholníkovej matice, ktorú sme dostali z matice sústavy, mali by sme situáciu ešte jednoduchšiu – dostali by sme jediné riešenie. Jedine v prípade, že by bola vedúca jednotka aj v stĺpci pravých strán, čo zodpovedá rovnici $0 = 1$, by sústava nemala žiadne riešenie.)

Skúšku správnosti urobíme tak, že dosadíme výsledok do pôvodnej sústavy. V prípade, že v riešení vystupuje parameter, buď dosadíme výsledok aj s parametrom, alebo to vyskúšame pre nejaké dve hodnoty parametra (také, aby sa nám dobre rátalo). Ak je parametrov viac, môžeme napríklad zvoliť najprv všetky parametre za nulu (tým skontrolujeme riešenie nehomogénneho systému) a potom vždy jeden z parametrov položíme rovný 1 a ostatné 0.

Úpravu, v ktorej sme spravili chybu, môžeme nájsť tak, že skúšame, pre ktoré z matíc získaných počas upravovania náš výsledok ešte vyhovuje a pre ktoré už nie. (Ak nejaká n-tica $(x_1, \ldots, x_n)$ vyhovuje sústave, ktorú sme dostali v jednom kroku alebo sústave v nasledujúcom kroku už nevyhovuje (alebo je to obrátene), táto úprava musí byť chybná. Vyplýva to z toho, že elementárne riadkové operácie nemenia množinu riešení.)

Príklad 5.7.12. Riešme v $\mathbb{Z}_5$ určenú maticou

$$\begin{pmatrix} 1 & 1 & 0 & 0 & | & 1 \\ 1 & 2 & 4 & 0 & | & 2 \\ 0 & 1 & 3 & 4 & | & 3 \\ 0 & 0 & 4 & 4 & | & 4 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 0 & 0 & | & 1 \\ 1 & 2 & 4 & 0 & | & 2 \\ 0 & 1 & 3 & 4 & | & 3 \\ 0 & 0 & 4 & 4 & | & 4 \end{pmatrix} \overset{(1)}{\sim} \begin{pmatrix} 1 & 1 & & & | & 1 \\ & 1 & 4 & & | & 1 \\ & 1 & 3 & 4 & | & 3 \\ & & 4 & 4 & | & 4 \end{pmatrix} \overset{(2)}{\sim} \begin{pmatrix} 1 & 1 & & & | & 1 \\ & 1 & 4 & & | & 1 \\ & & 4 & 4 & | & 2 \\ & & 4 & 4 & | & 4 \end{pmatrix} \overset{(3)}{\sim} \begin{pmatrix} 1 & 1 & & & | & 1 \\ & 1 & 4 & & | & 1 \\ & & 4 & 4 & | & 2 \\ 0 & 0 & 0 & 0 & | & 2 \end{pmatrix}$$

(1) `2.r+=4*1.r`(2) `3.r+=4*2.r` (3) `4.r+=4*3.r` (Kvôli stručnosti a prehľadnsoti som v matici vynechával nulové koeficienty.)

Pretože sme dostali riadok zodpovedajúci rovnici $0x_1 + 0x_2 + 0x_3 + 0x_4 = 2$, sústava nemá riešenie.

5.7.3 Frobeniova veta

V tejto časti dokážeme vetu, ktorá poskytuje kritérium na riešiteľnosť nehomogénnych sústav lineárnych rovníc. Predtým však potrebujeme ukázať, že hodnosť matice je rovnaká ako hodnosť transponovanej matice. (Túto vetu neskôr ešte dokážeme dvoma odlišnými spôsobmi v časti 5.9.)

Veta 5.7.13. *Pre každú maticu A nad poľom F platí $h(A) = h(A^T)$.*

Dôkaz. Nech A je matica typu $m \times n$.

Ak označíme i-ty stĺpec matice A ako $\vec{\alpha}_i$, tak platí

$$h(A^T) = d[\vec{\alpha}_1, \ldots, \vec{\alpha}_n].$$

Bez toho, aby sme zmenili hodnosť, môžeme preusporiadať stĺpce matice tak, aby po úprave na redukovanú trojuholníkovú maticu boli vedúce jednotky v prvých r stĺpcoch, kde $r = h(A)$.

Budeme sa zaoberať riešeniami homogénnej sústavy

$$A\vec{x}^T = \vec{0}^T,$$

ktorú môžeme ekvivalentne prepísať ako

$$x_1\vec{\alpha}_1 + \cdots + x_n\vec{\alpha}_n = \vec{0}. \tag{5.5}$$

(Rozmyslite si prečo – vyplýva to priamo z definície súčinu matíc.)

Všetky riešenia tejto sústavy sú určené bázou (5.4). Špeciálne z toho, že

$$\vec{\gamma}_i = (-c_{1,i}, -c_{2,i}, \ldots, -c_{r,i}, 0, \ldots, 0, 1, 0, \ldots, 0)$$

(kde $i \in \{r+1, r+2, \ldots, n\}$) je riešením (5.5), vyplýva

$$\begin{gathered} -c_{1,i}\vec{\alpha}_1 - c_{2,i}\vec{\alpha}_2 - \ldots - c_{r,i}\vec{\alpha}_r + \vec{\alpha}_i = \vec{0}, \\ \vec{\alpha}_i = c_{1,i}\vec{\alpha}_1 + c_{2,i}\vec{\alpha}_2 + \ldots + c_{r,i}\vec{\alpha}_r, \end{gathered}$$

a teda $\vec{\alpha}_i$ je lineárna kombinácia vektorov $\vec{\alpha}_1, \ldots, \vec{\alpha}_r$ pre všetky $i = r+1, r+2, \ldots, n$.

Teda

$$[\vec{\alpha}_1, \ldots, \vec{\alpha}_n] = [\vec{\alpha}_1, \ldots, \vec{\alpha}_r]$$

a

$$h(A^T) = d([\vec{\alpha}_1, \ldots, \vec{\alpha}_n]) \leq r,$$

čo znamená, že

$$h(A) \geq h(A^T).$$

Použitím tejto nerovnosti pre maticu A^T však dostaneme

$$h(A^T) \geq h((A^T)^T) = h(A),$$

a teda $h(A^T) = h(A)$. □

Poznámka 5.7.14. Pretože vykonanie riadkovej operácie na transponovanej matici A^T zodpovedá stĺpcovej operácii na matici A, z práve dokázanej vety vyplýva, že pri výpočte hodnosti matice môžeme ľubovoľne kombinovať riadkové a stĺpcové operácie.

Veta 5.7.15 (Frobeniova). *Nehomogénna sústava lineárnych rovníc* (5.2) *je riešiteľná práve vtedy, keď matica sústavy a rozšírená matica sústavy majú rovnakú hodnosť, t.j.*

$$h(A) = h(A').$$

Dôkaz. Označme $\vec{\gamma} = (c_1, \ldots, c_m)$ vektor pozostávajúci z pravých strán, čiže naša sústava má tvar $A\vec{x}^T = \vec{\gamma}^T$. Ďalej označme stĺpce matice A ako $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$.

$\boxed{\Rightarrow}$ Ak $x_1, \ldots, x_n$ je riešením tejto sústavy, znamená to, že

$$\vec{\gamma} = x_1\vec{\alpha}_1 + \cdots + x_n\vec{\alpha}_n.$$

Z toho vyplýva

$$\begin{gathered} [\vec{\alpha}_1, \ldots, \vec{\alpha}_n] = [\vec{\alpha}_1, \ldots, \vec{\alpha}_n, \vec{\gamma}] \\ h(A^T) = d([\vec{\alpha}_1, \ldots, \vec{\alpha}_n]) = d([\vec{\alpha}_1, \ldots, \vec{\alpha}_n, \vec{\gamma}]) = h(A'^T) \end{gathered}$$

Pretože podľa predchádzajúcej vety má každá matica rovnakú hodnosť ako jej transponovaná matica, dostali sme

$$h(A) = h(A').$$

$\boxed{\Leftarrow}$ Predpokladajme teraz, že $h(A) = h(A')$. To znamená, že podpriestory $[\vec{\alpha}_1, \ldots, \vec{\alpha}_n]$ a $[\vec{\alpha}_1, \ldots, \vec{\alpha}_n, \vec{\gamma}]$ majú rovnakú dimenziu. Pretože jeden z nich je navyše podpriestorom druhého, podľa tvrdenia 4.4.18 z toho vyplýva rovnosť

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

To znamená, že $\vec{\gamma}$ je lineárnou kombináciou vektorov $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$, teda existujú $x_1, \ldots, x_n \in F$ také, že

$$\vec{\gamma} = x_1\vec{\alpha}_1 + \cdots + x_n\vec{\alpha}_n.$$

Ako sme si už uvedomili v predchádzajúcej časti dôkazu, táto rovnosť je ekvivalentná s tým, že $x_1, \ldots, x_n$ je riešenie sústavy (5.2). □

Nasledujúca veta hovorí, že ak máme jedno konkrétne (partikulárne) riešenie nehomogénnej lineárnej sústavy, tak všetky ostatné riešenia nehomogénnej sústavy môžeme získať ako súčet tohoto riešenia a ľubovoľného riešenia príslušnej homogénnej sústavy.

Oveľa dôležitejší ako samotné znenie vety je veľmi dôležitý koncept rozdelenia riešenia na homogénnu a nehomogénnu časť. S týmto prístupom sa stretnete ešte veľakrát – dá sa využiť v podstate všade, kde sa vyskytuje linearita, napríklad pri lineárnych diferenciálnych rovniciach, pri lineárnych rekurentných rovniciach alebo tiež pri afinných priestoroch a afinných zobrazeniach – čo je niečo podobné ako vektorové priestory a lineárne zobrazenia, len sú doplnené o „nehomogénnu“ zložku (stretnete sa s nimi na predmete geometria v druhom ročníku [HZK]).

Veta 5.7.16. *Nech $\vec{\alpha}$ je riešenie sústavy lineárnych rovníc*

$$A.\vec{\alpha}^T = \vec{\gamma}^T \tag{N}$$

a S je podpriestor pozostávajúci zo všetkých riešení homogénneho systému

$$A.\vec{\alpha}^T = \vec{0}^T. \tag{H}$$

Potom $T = \{\vec{\alpha} + \vec{\beta}; \vec{\beta} \in S\}$ je množina všetkých riešení (N).

Inak povedané, ľubovoľné riešenie (N) sa dá získať ako súčet vektora $\vec{\gamma}$ (partikulárneho riešenia (N)) a nejakého riešenia homogénnej sústavy (H).

Dôkaz. Rovnosť dvoch množín (množiny T a množiny všetkých riešení) budeme dokazovať tak, že dokážeme obe inklúzie.

Najprv ukážeme, že každý prvok množiny T je riešením sústavy (N). Skutočne, pre prvok tvaru $\vec{\alpha} + \vec{\beta}$ platí

$$A(\vec{\alpha} + \vec{\beta})^T = A\vec{\alpha}^T + A\vec{\beta}^T = \vec{\gamma}^T + \vec{0}^T = \vec{\gamma}^T.$$

Zostáva ukázať, že každé riešenie (N) má uvedený tvar. Nech teda $\vec{\delta}$ je ľubovoľné riešenie (N), čiže platí $A\vec{\delta}^T = \vec{\gamma}^T$. Potom platí

$$A(\vec{\delta} - \vec{\alpha})^T = A\vec{\delta}^T - A\vec{\alpha}^T = \vec{\gamma}^T - \vec{\gamma}^T = \vec{0}^T.$$

Potom

$$\vec{\delta} = \vec{\alpha} + \underbrace{(\vec{\delta} - \vec{\alpha})}_{\in S},$$

teda je to súčet vektora $\vec{\alpha}$ a prvku z S. Ukázali sme, že ľubovoľné riešenie (N) patrí do T. □

Cvičenia

Úloha 5.7.1. Nájdite všetky riešenia daných sústav rovníc nad poľom $\mathbb{R}$:

$$\begin{array}{rrrrl} x_1 & -x_2 & +2x_3 & -3x_4 & = 1 \\ & x_2 & -x_3 & +x_4 & = -3 \\ x_1 & +3x_2 & & -3x_4 & = 1 \\ & -7x_2 & +3x_3 & +x_4 & = 3 \end{array} \qquad \begin{array}{rl} x_1 + x_2 & = 1 \\ x_1 + x_2 + x_3 & = 4 \\ x_2 + x_3 + x_4 & = -3 \\ x_3 + x_4 + x_5 & = 2 \\ x_4 + x_5 & = -1 \end{array}$$

$$\begin{array}{rrrrl} 3x_1 & -2x_2 & +5x_3 & +x_4 & = 3 \\ 2x_1 & -3x_2 & +x_3 & +5x_4 & = -3 \\ x_1 & +2x_2 & & -4x_4 & = -3 \\ x_1 & -x_2 & -4x_3 & +9x_4 & = 22 \end{array} \qquad \begin{array}{rrrrl} 2x_1 & +7x_2 & +3x_3 & +x_4 & = 5 \\ x_1 & +3x_2 & +x_3 & +5x_4 & = 3 \\ x_1 & +5x_2 & -9x_3 & +8x_4 & = 1 \\ 5x_1 & +2x_2 & +4x_3 & +5x_4 & = 12 \end{array}$$

$$\begin{array}{rrrrl} 2x & -5y & +3z & +t & = 5 \\ 3x & -7y & +3z & -t & = -1 \\ 5x & -9y & +6z & +2t & = 7 \\ 4x & -6y & +3z & +t & = 8 \end{array} \qquad \begin{array}{rrrrl} x & +2y & +4z & -3t & = 0 \\ 3x & +5y & +6z & -4t & = 0 \\ 4x & +5y & -2z & +3t & = 0 \\ 3x & +8y & +24z & -19t & = 0 \end{array}$$

Úloha 5.7.2. Riešte v $\mathbb{Z}_5$ sústavu určenú maticou:

$$\left(\begin{array}{rrrr|r} 1 & 1 & 0 & 3 & 1 \\ 1 & 2 & 4 & 0 & 2 \\ 2 & 1 & 3 & 4 & 3 \\ 3 & 0 & 4 & 4 & 4 \end{array}\right) \left(\begin{array}{rrrr|r} 3 & 1 & 2 & 2 & 1 \\ 4 & 4 & 2 & 1 & 0 \\ 0 & 1 & 2 & 4 & 1 \\ 2 & 1 & 1 & 2 & 3 \end{array}\right) \left(\begin{array}{rrrr|r} 2 & 4 & 1 & 1 & 2 \\ 3 & 3 & 3 & 2 & 1 \\ 1 & 4 & 2 & 1 & 1 \\ 4 & 2 & 0 & 3 & 2 \end{array}\right) \left(\begin{array}{rrrr|r} 1 & 2 & 3 & 2 & 4 \\ 2 & 3 & 1 & 1 & 3 \\ 4 & 3 & 1 & 3 & 2 \\ 3 & 4 & 3 & 2 & 1 \end{array}\right)$$

Úloha 5.7.3. Riešte v $\mathbb{R}$ sústavu určenú maticou:

$$\left(\begin{array}{rrr|r} 3 & -2 & 1 & 11 \\ 1 & 1 & -3 & 7 \\ 11 & -4 & -3 & 10 \end{array}\right) \left(\begin{array}{rrr|r} 1 & 2 & -1 & 2 \\ 3 & -1 & 2 & 7 \\ 1 & 0 & -1 & -2 \\ 2 & 1 & 1 & 7 \end{array}\right) \left(\begin{array}{rrr|r} 1 & 2 & -3 & 1 \\ -1 & 3 & -2 & 3 \\ 0 & 5 & -5 & 4 \end{array}\right) \left(\begin{array}{rrr|r} 1 & -2 & 1 & 0 \\ 4 & 1 & -1 & 2 \\ 1 & 2 & 4 & 0 \end{array}\right) \left(\begin{array}{rrr|r} 1 & 4 & -3 & 0 \\ 1 & -3 & -1 & 0 \\ 2 & 1 & -4 & 0 \end{array}\right)$$

Riešenie: a) nemá riešenie, b) (1,2,3) c) $(t - \frac{3}{5}, t + \frac{4}{5}, t)$, d) $(\frac{20}{47}, \frac{6}{47}, -\frac{8}{47})$, e) $(\frac{13}{7}t, \frac{2}{7}t, t)$

Úloha 5.7.4. Riešte v $\mathbb{Z}_7$ sústavu určenú maticou:

$$\left(\begin{array}{rrrr|r} 1 & 0 & 1 & 1 & 5 \\ 0 & 1 & 1 & 1 & 6 \\ 3 & 1 & 2 & 3 & 0 \\ 0 & 3 & 6 & 1 & 4 \end{array}\right) \left(\begin{array}{rrrr|r} 1 & 1 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 & 1 \\ 3 & 1 & 1 & 1 & 5 \\ 0 & 1 & 2 & 3 & 6 \end{array}\right) \left(\begin{array}{rrrr|r} 2 & 1 & 4 & 1 & 4 \\ 1 & 3 & 3 & 1 & 5 \\ 4 & 1 & 5 & 1 & 6 \\ 2 & 3 & 1 & 4 & 2 \end{array}\right) \left(\begin{array}{rrrr|r} 1 & 2 & 1 & 3 & 1 \\ 2 & 1 & 2 & 3 & 2 \\ 3 & 1 & 1 & 1 & 1 \\ 0 & 6 & 5 & 3 & 3 \end{array}\right)$$

Úloha 5.7.5. Môžete si vymyslieť kopec vlastných sústav. Stačí najprv zvoliť riešenie, koeficienty a dorátať pravé strany. Skúste vymyslieť aj také sústavy, ktoré nemajú riešenie alebo majú viac než jedno riešenie.

Úloha 5.7.6. Nájdite reálne čísla a, b, c tak, aby graf funkcie $f(x) = ax^2 + bx + c$ prechádzal bodmi (1,2), (-1,6) a (2,3).

Úloha 5.7.7$^+$. V závislosti od parametra $a \in \mathbb{R}$ riešte systém daný maticou:
a) $\left(\begin{array}{rr|r} a & 1 & a^2 \\ 1 & a & 1 \end{array}\right)$ b) $\left(\begin{array}{rr|r} a & 1 & a^3 \\ 1 & a & 1 \end{array}\right)$

Úloha 5.7.8*. O sústave n rovníc o n neznámych nad poľom $\mathbb{R}$ vieme, že jej koeficienty tvoria aritmetickú postupnosť (ako napríklad pre maticu $\left(\begin{array}{rrr|r} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{array}\right)$) a že táto sústava má jediné riešenie. Nájdite riešenie sústavy.

5.8 Jadro a obraz lineárneho zobrazenia

Definícia 5.8.1. Nech V a W sú vektorové priestory nad poľom F a $f\colon V \to W$ je lineárne zobrazenie. Potom *jadrom lineárneho zobrazenia* f nazývame množinu

$$\operatorname{Ker} f = \{\vec{\alpha} \in V; f(\vec{\alpha}) = \vec{0}\}$$

a *obrazom lineárneho zobrazenia* f nazývame množinu

$$\operatorname{Im} f = \{f(\vec{\alpha}); \vec{\alpha} \in V\}.$$

Inými slovami, $\operatorname{Ker} f$ obsahuje práve tie vektory z V, ktoré sa zobrazia na nulový vektor a $\operatorname{Im} f$ obsahuje obrazy všetkých vektorov z V. Ľahko sa overí, že $\operatorname{Ker} f$ aj $\operatorname{Im} f$ sú vektorové podpriestory.

Tvrdenie 5.8.2. *Nech V a W sú vektorové priestory nad poľom F a $f\colon V \to W$ je lineárne zobrazenie. Potom* $\operatorname{Ker} f$ *je vektorový podpriestor priestoru V a* $\operatorname{Im} f$ *je vektorový podpriestor priestoru W.*

Dôkaz. Pretože $f(\vec{0}) = \vec{0}$, platí $\vec{0} \in \operatorname{Ker} f$, teda $\operatorname{Ker} f \neq \emptyset$.

Ak $\vec{\alpha}, \vec{\beta} \in \operatorname{Ker} f$, znamená to, že $f(\vec{\alpha}) = f(\vec{\beta}) = \vec{0}$. Z linearity potom dostaneme

$$f(\vec{\alpha} + \vec{\beta}) = f(\vec{\alpha}) + f(\vec{\beta}) = \vec{0} + \vec{0} = \vec{0},$$

čiže aj $\vec{\alpha} + \vec{\beta} \in \operatorname{Ker} f$.

Podobne, ak $c \in F$ a $\vec{\alpha} \in \operatorname{Ker} f$, dostaneme

$$f(c.\vec{\alpha}) = c.f(\vec{\alpha}) = c.\vec{0} = \vec{0}$$

a $c.\vec{\alpha} \in \operatorname{Ker} f$.

Pretože $f(\vec{0}) = \vec{0}$, platí $\vec{0} \in \operatorname{Im} f$, teda $\operatorname{Im} f \neq \emptyset$.

Ak $\vec{\alpha}, \vec{\beta} \in \operatorname{Im} f$, znamená to, že tieto vektory sú obrazmi nejakých vektorov z V, označme ich $\vec{\alpha}_1$ a $\vec{\beta}_1$. Máme teda

$$\begin{aligned} f(\vec{\alpha}_1) &= \vec{\alpha} \\ f(\vec{\beta}_1) &= \vec{\beta} \\ f(\vec{\alpha}_1 + \vec{\beta}_1) &= \vec{\alpha} + \vec{\beta} \end{aligned}$$

Teda vektor $\vec{\alpha} + \vec{\beta}$ je obrazom vektora $\vec{\alpha}_1 + \vec{\beta}_1$, čiže patrí do $\operatorname{Im} f$.

Podobne sa ukáže

$$c\vec{\alpha} = cf(\vec{\alpha}_1) = f(c\vec{\alpha}_1),$$

teda aj $c\vec{\alpha} \in \operatorname{Im} f$. □

Teraz si povieme, ako súvisí jadro a obraz lineárneho zobrazenia s tým, či je toto zobrazenie surjektívne alebo injektívne.

Tvrdenie 5.8.3. *Nech V s W sú vektorové priestory nad poľom F a $f\colon V \to W$ je lineárne zobrazenie.*

Zobrazenie f je injektívne práve vtedy, keď $\operatorname{Ker} f = \{\vec{0}\}$.

Dôkaz. $\boxed{\Rightarrow}$ Predpokladajme, že f je injektívne. Vieme, že $f(\vec{0}) = \vec{0}$. Z injektívnosti vyplýva, že iný vektor sa už na nulový vektor nemôže zobraziť, preto $\operatorname{Ker} f = \{\vec{0}\}$.

$\boxed{\Leftarrow}$ Nech $\operatorname{Ker} f = \{\vec{0}\}$. Ak $f(\vec{\alpha}) = f(\vec{\beta})$, tak $f(\vec{\alpha} - \vec{\beta}) = \vec{0}$, čiže $\vec{\alpha} - \vec{\beta} \in \operatorname{Ker} f$. To ale znamená, že $\vec{\alpha} - \vec{\beta} = \vec{0}$, a teda $\vec{\alpha} = \vec{\beta}$. □

Dôkaz nasledujúceho tvrdenia vynecháme, ide vlastne len o inak prepísanú definíciu surjektívnosti.

Tvrdenie 5.8.4. *Nech V a W sú vektorové priestory nad poľom F a $f\colon V \to W$ je lineárne zobrazenie.*

Zobrazenie f je surjektívne práve vtedy, keď $\operatorname{Im} f = W$.

Dôsledok 5.8.5. *Lineárne zobrazenie $f\colon V \to W$ je izomorfizmus práve vtedy, keď* $\operatorname{Im} f = W$ *a* $\operatorname{Ker} f = \{\vec{0}\}$.

Veta 5.8.6. *Nech V a W sú konečnorozmerné vektorové priestory a $f\colon V \to W$ je lineárne zobrazenie. Potom*

$$d(V) = d(\operatorname{Ker} f) + d(\operatorname{Im} f).$$

Dôkaz. Nech $\vec{\alpha}_1, \ldots, \vec{\alpha}_k$ je báza $\operatorname{Ker} f$ (teda $d(\operatorname{Ker} f) = k$). Bázu $\operatorname{Ker} f$ vieme doplniť na bázu celého priestoru V vektormi $\vec{\beta}_1, \ldots, \vec{\beta}_l$. (Teda $d(V) = k + l$.) Označme $S = [\vec{\beta}_1, \ldots, \vec{\beta}_l]$.

Definujme zobrazenie $g\colon S \to \operatorname{Im} f$ ako zúženie zobrazenia f, t.j. $g(\vec{\alpha}) = f(\vec{\alpha})$ pre všetky $\vec{\alpha} \in S$. Toto zobrazenie je surjektívne (pretože ako druhý priestor sme zobrali $\operatorname{Im} f$) aj injektívne (lebo $\operatorname{Ker} g = \operatorname{Ker} f \cap S = \{\vec{0}\}$). Je aj lineárne, teda ide o izomorfizmus. Izomorfizmus zachováva dimenziu (pretože zobrazuje bázu na bázu), teda máme

$$l = d(S) = d(\operatorname{Im} f)$$

a z toho dostaneme

$$d(V) = k + l = d(\operatorname{Ker} f) + d(\operatorname{Im} f).$$

□

Cvičenia

Úloha 5.8.1. Nájdite bázu obrazu a bázu jadra lineárneho zobrazenia $f\colon (\mathbb{Z}_5)^4 \to (\mathbb{Z}_5)^4$ s danou maticou. V ktorých prípadoch je toto zobrazenie surjektívne a v ktorých injektívne?
$\begin{pmatrix} 3&1&2&2\\4&3&2&1\\0&1&2&4\\2&0&1&2 \end{pmatrix}$ $\begin{pmatrix} 2&4&1&1\\3&3&3&2\\1&4&2&1\\4&2&0&3 \end{pmatrix}$ $\begin{pmatrix} 1&2&3&4\\2&3&1&4\\4&3&2&1\\3&4&1&2 \end{pmatrix}$

Úloha 5.8.2. Nájdite lineárne zobrazenie (ak také existuje), ktoré je prosté a spĺňa podmienky:
a) $f(1,0,1) = (2,2,1)$, $f(1,-1,1) = (1,2,-2)$, $f(0,1,-2) = (0,-1,2)$,
b) $f(1,0,1) = (2,2,1)$, $f(1,-1,1) = (1,2,-2)$, $f(1,1,1) = (3,2,4)$,
c) $f(1,0,1) = (2,2,1)$, $f(0,-1,2) = (0,1,1)$, $f(1,1,-1) = (2,3,2)$.

Úloha 5.8.3. Nájdite lineárne zobrazenie $f\colon \mathbb{R}^3 \to \mathbb{R}^3$ (ak také existuje), pre ktoré: $f(3,2,3) = (5,-3,-2)$, $f(0,2,1) = (2,0,-2)$, $f(3,0,3) = (3,-3,0)$. Určte bázu a dimenziu jeho jadra a obrazu.

Úloha 5.8.4. Nech $f\colon V \to V$ je lineárne zobrazenie. Ako f^2 budeme označovať $f \circ f$. Dokážte

(a) $\operatorname{Ker} f^2 \supseteq \operatorname{Ker} f$,

(b) $\operatorname{Im} f^2 \subseteq \operatorname{Im} f$,

(c) $f^2 = 0 \Leftrightarrow \operatorname{Ker} f \supseteq \operatorname{Im} f$.

5.9 Hodnosť transponovanej matice

Už sme jedným spôsobom ukázali, že

$$h(A) = h(A^T)$$

(veta 5.7.13). Tu uvedieme dva ďalšie spôsoby. Prvý z nich bude využívať práve dokázanú vetu 5.8.6.

Dôkaz vety 5.7.13. Ku matici A typu $m \times n$ prislúcha lineárne zobrazenie $f\colon F^m \to F^n$. Vieme, že toto zobrazenie je určené predpisom

$$f(\vec{\alpha}) = \vec{\alpha}A$$

(poznámka 5.4.9).

Súčasne vieme, že podpriestor $\operatorname{Im} f$ je generovaný riadkami tejto matice. Preto $h(A) = d(\operatorname{Im} f)$.

Do $\operatorname{Ker} f$ patria práve vektory, pre ktoré platí

$$\vec{\alpha}A = \vec{0},$$

z čoho transponovaním dostávame

$$A^T\vec{\alpha}^T = \vec{0}^T,$$

teda sú to práve riešenia homogénneho systému s maticou A^T. Podľa dôsledku 5.7.5 je dimenzia množiny riešení takéhoto systému rovná $m - h(A^T)$ (pretože počet stĺpcov matice A je m).

Z vety 5.8.6 potom dostaneme

$$m = m - h(A^T) + h(A),$$

z čoho vyplýva $h(A^T) = h(A)$. □

Uvedieme ešte jeden, pomerne jednoduchý dôkaz tejto vety.

Dôkaz vety 5.7.13. Dôkaz bude pozostávať z 2 častí: Najprv ukážeme, že táto veta platí pre redukované trojuholníkové matice. Ďalej si uvedomíme, že stĺpcové operácie nemenia hodnosť matice. Z toho už potom vyplynie tvrdenie vety.

Ak B je redukovaná trojuholníková matica typu $m \times n$ a $h(B) = k$, znamená to, že B má k nenulových riadkov a navyše, má k stĺpcov, ktoré obsahujú jedinú (vedúcu) jednotku. Potom B^T je matica typu $n \times m$, v ktorej sú nenulové prvky iba v prvých k stĺpcoch a navyše obsahuje ako svoje riadky vektory $\vec{e}_1, \ldots, \vec{e}_k$ štandardnej bázy priestoru F^m (tieto riadky zodpovedajú tým stĺpcom pôvodnej matice, v ktorých boli vedúce jednotky). Z toho je zrejmé, že priestor V_{B^T} prislúchajúci tejto matici je generovaný vektormi $\vec{e}_1, \ldots, \vec{e}_k$ a teda $h(B^T) = d(V_{B^T}) = k = h(B)$.

Skúsme sa teraz zamyslieť nad tým ako menia dimenziu stĺpcové operácie. Každá stĺpcová operácia zodpovedá nejakému lineárnemu zobrazeniu $F^m \to F^m$ (vykonanie stĺpcovej operácie znamená zobrazenia každého riadku týmto zobrazením). Konkrétne, výmene dvoch stĺpcov i-teho a j-teho stĺpca zodpovedá zobrazenie (pre $i < j$)

$$(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_{i-1}, x_j, x_{i+1}, \ldots, x_{j-1}, x_i, x_{j+1}, \ldots, x_n)$$

pripočítaniu c-násobku i-teho stĺpca k j-temu zodpovedá

$$(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_{j-1}, x_j + cx_i, x_{j+1}, \ldots, x_n)$$

a vynásobeniu j-teho riadku konštantou $c \neq 0$ zodpovedá zobrazenie

$$(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_{j-1}, cx_j, x_{j+1}, \ldots, x_n).$$

Každé z týchto zobrazení je lineárne a navyše k nemu existuje inverzné (to vyplýva napríklad z toho, že stĺpcové operácie sú invertovateľné, ale dá sa to ľahko overiť aj priamo). Všetky takéto zobrazenia sú teda izomorfizmy.

Pretože stĺpcová úprava zodpovedá zobrazeniu podpriestoru prislúchajúceho danej matici nejakým izomorfizmom a izomorfizmus nemení dimenziu, je zrejmé, že stĺpcové operácie nemenia hodnosť matice.

Majme teraz maticu A. Matica A je riadkovo ekvivaletná s nejakou redukovanou trojuholníkovou maticou B. Platí $h(A) = h(B) = h(B^T)$. Z matice B^T však vieme dostať maticu A^T pomocou elementárnych stĺpcových operácií. (Riadkové operácie na pôvodnej matici totiž zodpovedajú stĺpcovým operáciam na transponovanej matici.) Preto máme aj rovnosť $h(B^T) = h(A^T)$ a spojením týchto dvoch rovností dostaneme

$$h(A) = h(A^T).$$

$\square$

Kapitola 6

Determinanty

6.1 Motivácia

Na začiatku tejto kapitoly uvedieme dva motivačné príklady. Ako neskôr uvidíme, v oboch nich určitým spôsobom vystupujú determinanty, jeden z nich nám ponúka aj istú geometrickú predstavu o pojme determinantu.

Príklad 6.1.1. Pokúsme sa nájsť všeobecné riešenie sústavy

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 &= c_1 \\ a_{21}x_1 + a_{22}x_2 &= c_2 \end{aligned}$$

Prvú rovnicu vynásobíme a_{22} a odčítame od nej a_{12}-násobok druhej rovnice. Dostaneme:

$$\begin{aligned} (a_{11}a_{22} - a_{12}a_{21})x_1 &= c_1a_{22} - c_2a_{12} \\ x_1 &= \frac{c_1a_{22} - c_2a_{12}}{a_{11}a_{22} - a_{12}a_{21}} \end{aligned}$$

v prípade, že $a_{11}a_{22} - a_{12}a_{21} \neq 0$.

Ak zavedieme označenie

$$\begin{vmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{vmatrix} = b_{11}b_{22} - b_{12}b_{21},$$

tak predchádzajúcu rovnosť môžeme vyjadriť ako

$$x_1 = \frac{\begin{vmatrix} c_1 & a_{12} \\ c_2 & a_{22} \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}}.$$

Podobným spôsobom by sme mohli odvodiť, že platí

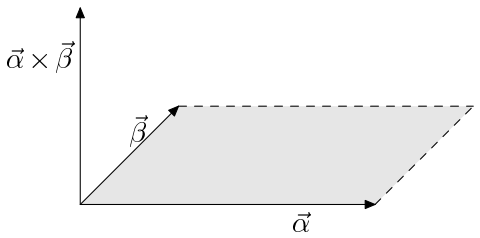
$$x_2 = \frac{\begin{vmatrix} a_{11} & c_1 \\ a_{21} & c_2 \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}}.$$

Definíciu, ktorú sme zaviedli v predchádzajúcom príklade, neskôr rozšírime aj na štvorcové matice väčších rozmerov ako 2×2 a práve tento výraz budeme nazývať determinant.

Príklad 6.1.2. Dva vektory v rovine určujú rovnobežník. Zo strednej školy viete, že jeho obsah možno vypočítať pomocou vektorového súčinu (obrázok 6.1). Konkrétne, ak je rovnobežník určený vektormi $\vec{\alpha} = (a_{11}, a_{12})$ a $\vec{\beta} = (a_{21}, a_{22})$, tak tieto vektory najprv doplníme treťou súradnicou 0 na vektory $(a_{11}, a_{12}, 0)$ a $(a_{21}, a_{22}, 0)$ a potom vypočítame ich vektorový súčin $(0, 0, a_{11}a_{22} - a_{12}a_{21})$. Obsah rovnobežníka je veľkosť vektora, ktorý sme vyrátali, čiže

$$S = |a_{11}a_{22} - a_{12}a_{21}|.$$

Až na znamienko sme opäť dostali výraz z predchádzajúceho príkladu (čiže determinant). (Pričom znamienko má tiež svoj význam – určuje orientáciu vektorov.)



Obr. 6.1: Vektorový súčin

Pokúsme sa ešte pokúsiť o riešenie analogickej úlohy v trojrozmernom priestore. V tomto prípade 3 vektory $\vec{\alpha}$, $\vec{\beta}$, $\vec{\gamma}$ určia rovnobežnosten. Jeho objem by sme vedeli vyrátať ako súčin obsahu podstavy a jeho výšky. Pritom výšku môžeme určiť ako priemet vektora $\vec{\gamma}$ do smeru vektora $\vec{\alpha} \times \vec{\beta}$. Tento priemet sa dá vyrátať ako $|\vec{\gamma}| \cos \alpha$, kde α je uhol, ktorý zvierajú vektory $\vec{\alpha} \times \vec{\beta}$ a $\vec{\gamma}$.

Teda až na znamienko je jeho objem určený výrazom

$$|\vec{\alpha} \times \vec{\beta}||\vec{\gamma}| \cos \alpha = (\vec{\alpha} \times \vec{\beta}).\vec{\gamma},$$

kde $\cdot$ označuje skalárny súčin vektorov. (Budeme sa ním zaoberať neskôr, ale už ste sa s ním stretli aj na strednej škole a poznáte niektoré jeho základné vlastnosti.)

Pokúsme sa vyčísliť tento výraz pre

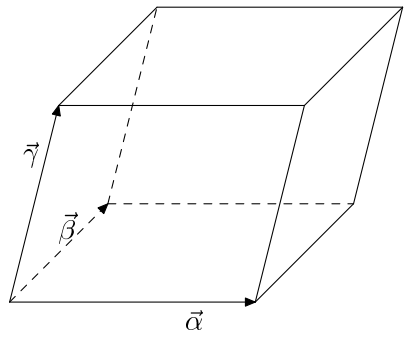
$$\begin{aligned} \vec{\alpha} &= (a_{11}, a_{12}, a_{13}) \\ \vec{\beta} &= (a_{21}, a_{22}, a_{23}) \\ \vec{\gamma} &= (a_{31}, a_{32}, a_{33}) \end{aligned}$$

Vieme, že $\vec{\alpha} \times \vec{\beta} = (\left|\begin{smallmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{smallmatrix}\right|, -\left|\begin{smallmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{smallmatrix}\right|, \left|\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right|)$.

Dostaneme teda

$$a_{31} \begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix} - a_{32} \begin{vmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{vmatrix} + a_{33} \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} =$$

$$a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31}$$



Obr. 6.2: Rovnobežnosten určený 3 vektormi v $\mathbb{R}^3$

Odvodili sme výrazy, ktoré predstavujú determinant štvorcovej matice 2×2 a 3×3. Ako by sme mohli túto definíciu rozšíriť na vyššie rozmery?

Mohli by sme postupovať analogicky ako v predchádzajúcich príkladoch. Jedna možnosť, ako by sme definovali determinanty, by bolo všeobecné riešenie rovníc vyšších stupňov. Vychádzali by nám síce čoraz komplikovanejšie výrazy, ale snáď by sme v nich časom objavili nejakú zákonitosť.

Príklad 6.1.2 nám dáva dobrú geometrickú predstavu determinantu – ako objem telesa určeného danými vektormi v $\mathbb{R}^n$. Nie je však úplne jasné, čo chápať pod objemom v n-rozmernom priestore. Ale snáď by sme na to vedeli prísť. Objem jednotkovej kocky – čiže n-rozmerného rovnobežnostena určeného vektormi $\vec{\varepsilon}_1, \ldots, \vec{\varepsilon}_n$ – je zrejme 1. A vieme celkom dobre popísať (na základe analógie s dvojrozmerným a trojrozmerným prípadom), ako sa tento objem zmení pri transformáciach ako je skosenie, natiahnutie v smere niektorej z jeho strán alebo súmernosť podľa roviny (či skôr „nadroviny“, ako sa zvykne nazývať $(n-1)$-rozmerný podpriestor v $\mathbb{R}^n$). A pomocou týchto transformácií by sme vedeli dostať z jednotkovej kocky ľubovoľný n-rozmerný rovnobežnosten (prinajmenšom v trojrozmere máme o tom celkom dobrú geometrickú predstavu; neskôr si niečo povieme aj o tom ako súvisia tieto transformácie s riadkovými operáciami na matici), takže takýmto spôsobom by sme tiež boli schopný vyrátať objem každého rovnobežnostena – a teda ľubovoľný determinant.

Nebudeme postupovať ani jedným z naznačených spôsobov – naša definícia determinantu bude celkom iná a na prvý pohľad veľmi zvláštna. Neskôr však uvidíme, že pri našej definícií budú platiť pre riešenie sústavy n rovníc o n neznámych analogické vzťahy ako sme dostali v príklade 6.1.1 a takisto sa determinant správa vzhľadom na niektoré transformácie spôsobom, ktorý sme pred chvíľou spomenuli.

6.2 Definícia determinantu

Definícia 6.2.1. V tejto kapitole budeme označovať ako S_n množinu všetkých permutácií množiny $\{1, 2, \ldots, n\}$.

Dvojica $(\varphi(k), \varphi(s))$ sa volá *inverzia* permutácie φ, ak $k < s$ ale $\varphi(k) > \varphi(s)$. Počet inverzií permutácie φ budeme označovať $i(\varphi)$.

Príklad 6.2.2. Permutácia $\left(\begin{smallmatrix}1&2&3&4\\4&1&3&2\end{smallmatrix}\right)$ má 4 inverzie (4,1), (4,3), (4,2), (3,2):

$$\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}$$

$$\begin{array}{cccc} 4 & 1 & & \\ 4 & & 3 & \\ 4 & & & 2 \\ & & 3 & 2 \end{array}$$

Definícia 6.2.3. Nech A je matica typu $n \times n$ nad poľom F, $A = ||a_{ij}||$. *Determinant matice* A je

$$|A| = \sum_{\varphi \in S_n} (-1)^{i(\varphi)} a_{1\varphi(1)} a_{2\varphi(2)} \dots a_{n\varphi(n)}. \tag{6.1}$$

Symbolom $\sum\limits_{\varphi \in S_n}$ rozumieme, že sčitujeme cez celú množinu S_n, teda pre každú permutáciu $\varphi \in S_n$ pripočítame jeden sčítanec uvedeného tvaru. (Množina S_n je konečná, teda takýto súčet je jednoznačne definovaný.)

Príklad 6.2.4. Ak máme maticu typu 1×1 tak dostaneme $|A| = |a_{11}| = a_{11}$.

Pre maticu typu 2×2 tiež dostaneme jednoduchý vzorec. S_2 obsahuje len 2 permutácie $\left(\begin{smallmatrix}1&2\\1&2\end{smallmatrix}\right)$ a $\left(\begin{smallmatrix}1&2\\2&1\end{smallmatrix}\right)$. Prvá z nich nemá inverzie, druhá má jednu inverziu. Z (6.1) dostaneme v tomto prípade

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}.$$

V prípade matice typu 3×3 obsahuje množina S_3 už 6 prvkov. V nasledujúcej tabuľke sú vypísané všetky permutácie z S_3, ich inverzie a počet inverzií.

φ	$i(\varphi)$	inverzie
$\left(\begin{smallmatrix}1&2&3\\1&2&3\end{smallmatrix}\right)$	0	
$\left(\begin{smallmatrix}1&2&3\\1&3&2\end{smallmatrix}\right)$	1	$(3,2)$
$\left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right)$	1	$(2,1)$
$\left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right)$	2	$(2,1)$ $(3,1)$
$\left(\begin{smallmatrix}1&2&3\\3&1&2\end{smallmatrix}\right)$	2	$(3,1)$ $(3,2)$
$\left(\begin{smallmatrix}1&2&3\\3&2&1\end{smallmatrix}\right)$	3	$(3,2)$ $(3,1)$ $(2,1)$

Z (6.1) teda dostaneme (permutácie uvedieme v takom poradí, aby išli najprv tie, ktoré majú kladné znamienko, čiže párny počet inverzií)

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

Tento vzorec pre výpočet determinantu matice 3×3 nazývame *Sarrusovo pravidlo.*

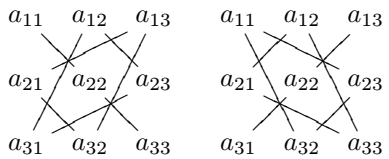
Spôsob, ako si ho možno ľahko zapamätať, je pridať ešte raz k matici A je prvé 2 stĺpce. Súčiny na hlavných diagonálach dávame do vzorca s kladným znamienkom, súčiny na vedľajších diagonálach so záporným znamienkom.

$$\begin{array}{ccccc} a_{11} & a_{12} & a_{13} & a_{11} & a_{12} \\ a_{21} & a_{22} & a_{23} & a_{21} & a_{22} \\ a_{31} & a_{32} & a_{33} & a_{31} & a_{32} \end{array} \qquad \begin{array}{ccccc} a_{11} & a_{12} & a_{13} & a_{11} & a_{12} \\ a_{21} & a_{22} & a_{23} & a_{21} & a_{22} \\ a_{31} & a_{32} & a_{33} & a_{31} & a_{32} \end{array}$$

$$+ \quad + \quad + \qquad - \quad - \quad -$$

Ten istý výsledok dostaneme ako pod maticu podpíšeme ešte raz jej prvé 2 riadky.

Inou mnemotechnickou pomôckou je vyznačiť si „kladné“ a „záporné“ diagonály v pôvodnej matici – bez pripisovania prvkov matice.



Príklad 6.2.5. $\begin{vmatrix} 1 & 3 & 2 \\ 1 & 3 & 1 \\ 0 & 1 & 2 \end{vmatrix} = 1.3.2 + 3.1.0 + 2.1.1 - 2.3.0 - 1.1.1 - 2.3.1 = 1$

Priamo z definície sa dá dokázať užitočná vlastnosť determinantu: determinant transponovanej matice je rovnaký ako determinant pôvodnej matice.

Veta 6.2.6. *Nech A je matica typu $n \times n$. Potom*

$$|A| = |A^T|.$$

Dôkaz. V definícii determinantu (6.1) vystupujú súčiny tvaru $a_{1\varphi(1)}a_{2\varphi(2)} \dots a_{n\varphi(n)}$. Okamžite vidíme, že v takomto súčine sa objaví práve raz prvok prvého riadku matice A (konkrétne na prvom mieste), práve raz prvok druhého riadku, atď.

Ako je to so stĺpcami? Druhé súradnice, ktoré predstavujú stĺpce, sú $\varphi(1), \varphi(2), \dots, \varphi(n)$. Vďaka tomu, že φ je bijekcia, objaví sa každý stĺpec práve raz. Konkrétne prvok j-teho stĺpca sa vyskytne v činiteli $a_{\varphi^{-1}(j)j}$ (lebo $i = \varphi^{-1}(j)$ je presne to číslo, ktoré sa zobrazí na j, čiže spĺňa $\varphi(i) = j$).

Ak teda usporiadame činitele vystupujúce v takomto súčine nie podľa prvých, ale podľa druhých súradnic, dostaneme iný zápis pre ten istý súčin.

$$a_{1\varphi(1)}a_{2\varphi(2)} \dots a_{n\varphi(n)} = a_{\varphi^{-1}(1)1}a_{\varphi^{-1}(2)2} \dots a_{\varphi^{-1}(n)n}.$$

Sčítaním takýchto rovností cez všetky permutácie $\varphi \in S_n$ dostaneme

$$|A| = \sum_{\varphi \in S_n} (-1)^{i(\varphi)} a_{1\varphi(1)}a_{2\varphi(2)} \dots a_{n\varphi(n)} = \sum_{\varphi \in S_n} (-1)^{i(\varphi)} a_{\varphi^{-1}(1)1}a_{\varphi^{-1}(2)2} \dots a_{\varphi^{-1}(n)n}.$$

Označme prvok v i-tom riadku a j-tom stĺpci transponovanej matice ako a'_{ij}, t.j. $a'_{ij} = a_{ji}$.

Potom poslednú rovnosť môžeme prepísať ako

$$|A| = \sum_{\varphi \in S_n} (-1)^{i(\varphi)} a'_{1\varphi^{-1}(1)}a'_{2\varphi^{-1}(2)} \dots a'_{n\varphi^{-1}(n)}.$$

Ďalej si uvedomme, že priradenie $\varphi \mapsto \varphi^{-1}$ je bijekcia z S_n do S_n. (Ľahko to môžete overiť na základe vlastností inverzného zobrazenia. Vyplýva to napríklad aj z toho, že $(S_n, \circ)$ je grupa (úloha 3.2.2) a z úlohy 3.2.12.) Teda, ak v predchádzajúcej sume namiesto φ^{-1} použijeme všade φ, znamená to len preusporiadanie sčítancov, ale hodnotu súčtu to neovplyvní.

$$|A| = \sum_{\varphi \in S_n} (-1)^{i(\varphi^{-1})} a'_{1\varphi(1)}a'_{2\varphi(2)} \dots a'_{n\varphi(n)}.$$

Na to, aby sme vpravo dostali determinant matice A^T, stačilo by dokázať, že $i(\varphi) = i(\varphi^{-1})$. To skutočne platí. Inverzie permutácie φ sú totiž určené takými dvojicami indexov, pre ktoré platí

$$i < j \qquad \wedge \qquad \varphi(i) > \varphi(j).$$

Ak označíme $i' = \varphi(i)$ a $j' = \varphi(j)$, tak predchádzajúca podmienka je ekvivalentná podmienke

$$\varphi^{-1}(i') < \varphi^{-1}(j') \qquad \wedge \qquad i' > j'.$$

Našli sme teda jedno-jednoznačné priradenie medzi dvojicami, ktoré určujú inverzie permutácií φ a φ^{-1}. Teda skutočne platí $i(\varphi) = i(\varphi^{-1})$ a

$$|A| = |A^T|.$$

□

6.3 Výpočet determinantov

Doteraz sme uviedli ako počítať determinanty rozmeru maximálne 3×3, pričom sme vlastne postupovali priamo z definície. Na výpočet determinantov vyššieho stupňa sa naučíme dva postupy. Prvý z nich je Laplaceov rozvoj a druhý je použitie elementárnych riadkových a stĺpcových operácií.

6.3.1 Laplaceov rozvoj

Nech A je štvorcová matica typu $n \times n$. Zvoľme si (pevne) nejaké $i \in \{1, 2, \ldots, n\}$. Potom determinant matice A sa dá upraviť na tvar

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

Vyplýva to z toho, že v každom sčítanci v sume (6.1) vystupuje práve jeden prvok tvaru a_{ik} (konkrétne je to $a_{i\varphi(i)}$). Aby sme získali uvedenú rovnosť, stačí vyňať a_{ij} z tých sčítancov v ktorých sa vyskytuje.

Podobne by sme mohli postupovať aj pre prvky niektorého stĺpca $a_{1j}, a_{2j}, \ldots, a_{nj}$. Dostali by sme

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

Výraz A_{ij} nazývame *algebraický doplnok prvku* a_{ij}.

Naším najbližším cieľom bude zistiť, čomu sa rovná A_{ij}.

Pokúste sa sami si vyskúšať zistiť všetky možné hodnoty A_{ij} pre maticu 3×3, výsledky si môžete skontrolovať v nasledujúcom príklade.

Príklad 6.3.1. Pre maticu typu 3×3 sme odvodili

$$|A| = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31}.$$

Skúsme v tomto konkrétnom prípade urobiť spomínaný rozvoj pre druhý riadok a druhý stĺpec.

Pre druhý riadok dostaneme:

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

Pre druhý stĺpec dostaneme:

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

Z uvedených výrazov vieme vyčítať hodnoty A_{12}, A_{21}, A_{22}, A_{23}, A_{32}. Keby sme urobili ešte 2 ďalšie rozvoje (povedzme podľa prvého a tretieho riadku), zistili by sme aj ostatné hodnoty algebraických doplnkov.

$$
\begin{aligned}
A_{11} &= a_{22}a_{33} - a_{23}a_{32}\\
A_{12} &= a_{23}a_{31} - a_{21}a_{33}\\
A_{13} &= a_{21}a_{32} - a_{22}a_{31}\\
A_{21} &= a_{13}a_{32} - a_{12}a_{33}\\
A_{22} &= a_{11}a_{33} - a_{13}a_{31}\\
A_{23} &= a_{12}a_{31} - a_{11}a_{32}\\
A_{31} &= a_{12}a_{23} - a_{13}a_{22}\\
A_{32} &= a_{13}a_{21} - a_{11}a_{23}\\
A_{33} &= a_{11}a_{22} - a_{12}a_{21}
\end{aligned}
$$

Možno by ste z hodnôt vyrátaných v predchádzajúcom príklade vedeli uhádnúť nejakú všeobecnú zákonitosť. Váš tip sa potvrdí dokázaním nasledujúcej vety.

Pre maticu A typu $n \times n$ a $i, j \in \{1, 2, \ldots, n\}$ označíme ako M_{ij} maticu, ktorá vznikne z matice A vynechaním i-teho riadku a j-teho stĺpca.

Veta 6.3.2. *Pre algebraický doplnok prvku a_{rs} štvorcovej matice A platí*

$$A_{rs} = (-1)^{r+s}|M_{rs}|$$

Dôkaz. Priamo z definície vyplýva, že

$$A_{rs} = \sum_{\varphi' \in S_n^{rs}} (-1)^{i(\varphi')} a_{1,\varphi'(1)} a_{2\varphi'(2)} \ldots a_{r-1}\varphi'(r-1) a_{r+1}\varphi'(r+1) \ldots a_n\varphi'(n),$$

kde ako S_n^{rs} sme označili množinu tých permutácií z S_n, pre ktoré $\varphi'(r) = s$.

Pre maticu M_{rs} tejto permutácii zodpovedá permutácia φ, ktorá je určená predpisom

$$\varphi(k) = \begin{cases} \varphi'(k), & \text{ak } \varphi'(k) < s \\ \varphi'(k) - 1, & \text{ak } \varphi'(k) > s \end{cases} \qquad \text{pre } k < r$$

$$\varphi(k) = \begin{cases} \varphi'(k+1), & \text{ak } \varphi'(k+1) < s \\ \varphi'(k+1) - 1, & \text{ak } \varphi'(k+1) > s \end{cases} \qquad \text{pre } k \geq r.$$

Chceli by sme zistiť, aký je vzťah medzi $i(\varphi')$ a $i(\varphi)$. Každá inverzia permutácie φ zodpovedá nejakej inverzii pôvodnej permutácie φ'. Niektoré inverzie sme však stratili:

a) Ak platí $\varphi'(j) > s$ pre $j < r$, tak dvojica $(\varphi'(j), s)$ tvorí inverziu pôvodnej permutácie, ale v permutácií φ nemáme inverziu, ktorá by jej zodpovedala. Označme počet takýchto inverzií k. Znamená to, že medzi prvkami $j \in \{1, 2, \ldots, r-1\}$ je k prvkov takých, že $\varphi'(j) > s$. Pre zostávajúcich $(r-1) - k$ prvkov teda platí $\varphi'(j) < s$. (Nemôže platiť $\varphi'(j) = s$, lebo na s sa zobrazí jedine r.)

b) Ak $\varphi'(j) < s$ pre $j > r$, tak opäť dostaneme inverziu, ku ktorej nemáme zodpovedajúcu inverziu v permutácii φ. Prvkov s vlastnosťou $\varphi'(j) < s$ je práve $s - 1$. Pritom, ako sme videli v prípade a), z nich práve $(r-1) - k$ spĺňa nerovnosť $j < r$. Inverzií typu b) je teda $(s-1) - [(r-1) - k] = s - r + k$.

Spolu sme „stratili“ $s - r + 2k$ inverzií. Teda $i(\varphi') = i(\varphi) + s - r + 2k$ a

$$(-1)^{i(\varphi')} = (-1)^{i(\varphi)} + (-1)^{s-r} + (-1)^{2k} = (-1)^{i(\varphi)} + (-1)^{s+r}.$$

Dosadením do vyjadrenia pre A_{rs}, ak navyše zavedieme označenie $M_{rs} = ||b_{ij}||$, získame dokazovanú rovnosť

$$A_{rs} = (-1)^{r+s} \sum_{\varphi \in S_{n-1}} (-1)^{i(\varphi)} b_{1\varphi(1)} \ldots b_{n\varphi(n)} = (-1)^{r+s}|M_{ij}|.$$

$\square$

Pretože predchádzajúci dôkaz nie je úplne jednoduchý, uvedieme ešte iný, do istej miery podobný (v nádeji, že keď uvidíte viacero pohľadov na dôkaz tej istej vety, bude to o čosi jasnejšie).

Dôkaz. Kvôli jednoduchosti začnime s prípadom $r = s = n$. Priamo z definície determinantu vidíme, že a_{nn} sa vyskytne v tých sčítancoch, kde $\varphi(n) = n$. To ale znamená, že permutácia φ zobrazí $\{1, 2, \ldots, n-1\}$ na $\{1, 2, \ldots, n-1\}$, čiže takéto permutácie sú v jednojednoznačnej korešpondencii s permutáciami množiny $\{1, 2, \ldots, n-1\}$. Navyše počet inverzií zodpovedajúcich si permutácií je očividne rovnaký. (Vynechali sme len $\varphi(n) = n$, tento prvok nevystupoval v žiadnej inverzii.) Máme teda

$$A_{nn} = \sum_{\varphi \in S_{n-1}} (-1)^{i(\varphi)} a_{1\varphi(1)} a_{2\varphi(2)} \ldots a_{n-1,\varphi(n-1)} = |M_{nn}|.$$

(Opäť, priamo z definície dostaneme, že výraz na pravej strane rovnosti je determinant matice, ktorá vznikne vynechaním posledného riadku a posledného stĺpca.)

Ďalej sa pozrime na to, ako sa zmení algebraický doplnok A_{rs} ak vymeníme r-tý riadok matice A s nasledujúcim. Nech teda matica B vznikne z matice A tak, že vymeníme r-tý a $(r+1)$-vý riadok. Chceme porovnať sčítance vystupujúce v determinante matice A obsahujúce prvok a_{rs} s tými sčítancami v determinante matice B, ktoré obsahujú $b_{r+1,s} = a_{r,s}$. V prvom prípade sčitujeme cez všetky permutácie také, že $\varphi(r) = s$ (množinu týchto permutácie označíme opäť S_n^{rs}).

$$A_{rs} = \sum_{\varphi \in S_n^{rs}} (-1)^{i(\varphi)} a_{1,\varphi(1)} \ldots a_{r-1,\varphi(r-1)} a_{r+1,\varphi(r+1)} \ldots a_{n,\varphi(n)}.$$

Pri výpočte $B_{r+1,s}$ sčitujeme cez všetky permutácie také, že $\varphi(r+1) = s$:

$$B_{r+1,s} = \sum_{\varphi \in S_n^{r+1,s}} (-1)^{i(\varphi)} b_{1,\varphi(1)} \ldots b_{r-1,\varphi(r-1)} b_{r,\varphi(r)} b_{r+2,\varphi(r+2)} \ldots b_{n,\varphi(n)}.$$

Súčase, z definície matice B máme $b_{ij} = a_{ij}$ pre $i \neq r, r+1$ a $b_{rs} = a_{r+1,s}$, teda

$$B_{r+1,s} = \sum_{\varphi \in S_n^{r+1,s}} (-1)^{i(\varphi)} a_{1,\varphi(1)} \ldots a_{r-1,\varphi(r-1)} a_{r+1,\varphi(r)} a_{r+2,\varphi(r+2)} \ldots a_{n,\varphi(n)}.$$

Uvedomme si ďalej, že výmena prvkov na r-tej a $(r+1)$-vej pozícii dáva korešpondenciu medzi množinami S_n^{rs} a $S_n^{r+1,s}$. Konkrétne, z permutácie

$$\varphi = \begin{pmatrix} 1 & \ldots & r & r{+}1 & \ldots & n \\ \varphi(1) & \ldots & s & \varphi(r{+}1) & \ldots & \varphi(n) \end{pmatrix}$$

patriacej do S_n^{rs} dostaneme permutáciu

$$\varphi' = \begin{pmatrix} 1 & \ldots & r & r{+}1 & \ldots & n \\ \varphi(1) & \ldots & \varphi(r{+}1) & s & \ldots & \varphi(n) \end{pmatrix}$$

patriacu do $S_n^{r+1,s}$ a obrátene. Vďaka tejto bijektívnej korešpondencii môžeme predchádzajúcu sumu prepísať ako

$$B_{r+1,s} = \sum_{\varphi \in S_n^{r,s}} (-1)^{i(\varphi')} a_{1,\varphi(1)} \ldots a_{r-1,\varphi(r-1)} a_{r+1,\varphi(r+1)} a_{r+2,\varphi(r+2)} \ldots a_{n,\varphi(n)}.$$

Vidíme, že v oboch sumách sa vyskytujú presne tie isté členy, zostáva len zistiť aký je vzťah medzi $i(\varphi)$ a $i(\varphi')$. Tieto permutácie sa líšia len na r-tom a $(r+1)$-mieste, čiže jediná inverzia, ktorou sa môžu líšiť, je $(\varphi(r), \varphi(r+1))$. Skutočne, ak $(s, \varphi(r+1))$ tvoria inverziu permutácie φ, tak v novej permutácii nebudeme mať na tomto mieste inverziu a obrátene, ak tu φ nemá inverziu, vo φ' dostaneme inverziu. Počet permutácií sa teda líši o túto jednu inverziu, čiže $i(\varphi') = i(\varphi) \pm 1$, a teda

$$B_{r+1,s} = -\sum_{\varphi \in S_n^{r,s}} (-1)^{i(\varphi)} a_{1,\varphi(1)} \dots a_{r-1,\varphi(r-1)} a_{r+1,\varphi(r+1)} a_{r+2,\varphi(r+2)} \dots a_{n,\varphi(n)} = -A_{rs}.$$

Vďaka vete 6.2.6 vieme, že to isté sa stane pri výmene susedných stĺpcov.

Posledné pozorovanie potrebné na dokončenie dôkazu je, že podmatica M_{rs} matice A je rovnaká ako podmatica $M_{r+1,s}$ matice B. (Z matice B vynechávame $(r+1)$-vý riadok, čo je presne r-tý riadok pôvodnej matice.)

Ak teraz chceme zistiť algebraický doplnok A_{rs} prvku a_{rs} matice A, môžeme postupovať tak, že $n-r-1$ výmenami susedných riadkov presunieme prvok a_{rs} do n-tého riadku, a potom urobíme ešte $n-s-1$ výmen stĺpcov, po ktorých prvok a_{rs} pôvodnej matice bude prvkom c_{nn} matice C, ktorú takto dostaneme. Už vieme, že algebraický doplnok tohoto prvku je

$$A_{nn} = |M_{rs}|$$

(podmatica, ktorá vznikne z C vynechaním posledného riadku a posledného stĺpca je presne tá podmatica pôvodnej matice, ktorú sme dostali vynechaním r-tého riadku a s-tého stĺpca.) Súčasne sme pri každej výmene riadku/stĺpca zmenili znamienko, preto

$$A_{rs} = (-1)^{n-r+n-s} A_{nn} = (-1)^{2(n-r-s)+r+s} A_{nn} = (-1)^{r+s} A_{nn} = (-1)^{r+s} |M_{rs}|.$$

□

Dôsledok 6.3.3 (Laplaceov rozvoj determinantu). *Nech A je matica typu $n \times n$. Potom*

$$|A| = (-1)^{i+1} a_{i1} |M_{i1}| + (-1)^{i+2} a_{i2} |M_{i2}| + \ldots + (-1)^{i+n} a_{in} |M_{in}| \tag{6.2}$$

$$|A| = (-1)^{j+1} a_{1j} |M_{1j}| + (-1)^{j+2} a_{2j} |M_{2j}| + \ldots + (-1)^{j+n} a_{nj} |M_{nj}| \tag{6.3}$$

Prvú rovnosť uvedenú v predchádzajúcom dôsledku nazývame *Laplaceov rozvoj determinantu matice A podľa i-teho riadku,* druhú *Laplaceov rozvoj podľa j-teho stĺpca.*

Príklad 6.3.4. Nasledujúci determinant vypočítame Laplaceovým rozvojom podľa druhého stĺpca.

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

6.3.2 Výpočet pomocou riadkových a stĺpcových operácií

V časti 5.2 sme si ukázali, ako možno pomocou elementárnych riadkových úprav upraviť ľubovoľnú maticu na redukovanú trojuholníkovú maticu. Ak by sme vedeli, ako elementárne riadkové úpravy ovplyvňujú hodnotu determinantu a ak by sme vedeli vypočítať determinat redukovanej trojuholníkovej matice, tak by sme získali ďalšiu metódu na výpočet determinantov. Práve to je naším najbližším cieľom.

Začneme s tým, že overíme, ako menia hodnotu determinantu jednotlivé elementárne riadkové operácie.

Veta 6.3.5. *Ak maticu B získame z A vynásobením k-teho riadku skalárom $c \in F$, tak*

$$|B| = c|A|.$$

Dôkaz. Označme $B = ||b_{ij}||$ a $A = ||a_{ij}||$. Potom platí $b_{ij} = a_{ij}$ pre $i \neq k$ a $b_{kj} = ca_{kj}$. Priamo z definície determinantu potom dostaneme

$$\begin{aligned}|B| = &\sum_{\varphi \in S_n} (-1)^{i(\varphi)} b_{1,\varphi(1)} b_{2,\varphi(2)} \dots b_{k-1,\varphi(k-1)} b_{k,\varphi(k)} b_{k+1,\varphi(k+1)} \dots b_{n,\varphi(n)} = \\ &\sum_{\varphi \in S_n} (-1)^{i(\varphi)} a_{1,\varphi(1)} a_{2,\varphi(2)} \dots a_{k-1,\varphi(k-1)} c a_{k,\varphi(k)} a_{k+1,\varphi(k+1)} \dots a_{n,\varphi(n)} = \\ &c \sum_{\varphi \in S_n} (-1)^{i(\varphi)} a_{1,\varphi(1)} a_{2,\varphi(2)} \dots a_{k-1,\varphi(k-1)} a_{k,\varphi(k)} a_{k+1,\varphi(k+1)} \dots a_{n,\varphi(n)} = c|A|.\end{aligned}$$

□

Dôsledok 6.3.6. *Ak matica A má nulový riadok, tak $|A| = 0$.*

Dôkaz. Stačí v predchádzajúcej vete dosadiť $c = 0$. □

Veta 6.3.7. *Ak má matica A dva rovnaké riadky, tak $|A| = 0$.*

Dôkaz. Matematickou indukciou vzhľadom na n.

1° Pre $n = 2$ tvrdenie platí:

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{11} & a_{12} \end{vmatrix} = a_{11}a_{12} - a_{11}a_{12} = 0.$$

2° Predpokladajme, že tvrdenia platí pre ľubovoľnú maticu typu $n \times n$. Nech A je matica typu $(n+1) \times (n+1)$, ktorej i-ty a j-ty riadok sú rovnaký. Ak urobíme rozvoj determinantu matice A podľa niektorého iného riadku (okrem i-teho a j-teho), tak všetky matice M_{rs} vystupujúce v Laplaceovom rozvoji sú matice typu $n \times n$ a majú dva rovnaké riadky. Podľa indukčného predpokladu $|M_{rs}| = 0$ pre všetky prípustné hodnoty r, s, a teda z Laplaceovho rozvoja (6.2) vidíme, že aj $|A| = 0$. □

Veta 6.3.8. *Nech matice A a B sú matice typu $n \times n$, ktoré sa líšia len v k-tom riadku. Potom $|A| + |B| = |C|$, kde $c_{ij} = a_{ij} = b_{ij}$ pre $i \neq k$ a $c_{kj} = a_{kj} + b_{kj}$.*

Dôkaz. Urobme rozvoj matice C podľa k-teho riadku. Dostaneme

$$|C| = (-1)^{k+1}(a_{k1} + b_{k1})|M_{k1}| + (-1)^{k+2}(a_{k2} + b_{k2})|M_{k2}| + \ldots + (-1)^{k+n}(a_{kn} + b_{kn})|M_{kn}|.$$

Pritom podmatice $M_{k1}, M_{k2}, \ldots, M_{kn}$ už pozostávajú len z tých prvkov, ktoré sú vo všetkých troch maticiach rovnaké. Teda tie istú podmatice budú vystupovať v rozvojoch matíc A a B podľa k-teho riadku. Pomocou nich dostaneme:

$$\begin{aligned}|A| &= (-1)^{k+1}a_{k1}|M_{k1}| + (-1)^{k+2}a_{k2}|M_{k2}| + \ldots + (-1)^{k+n}a_{kn}|M_{kn}|, \\ |B| &= (-1)^{k+1}b_{k1}|M_{k1}| + (-1)^{k+2}b_{k2}|M_{k2}| + \ldots + (-1)^{k+n}b_{kn}|M_{kn}|.\end{aligned}$$

Sčítaním týchto dvoch rovností a porovnaním s rozvojom determinantu matice C dostaneme

$$|A| + |B| = |C|.$$

□

Predchádzajúcu vetu by sme mohli ľahko overiť aj priamo na základe definície determinantu.

Dôkaz.

$$|C| = \sum_{\varphi \in S_n} (-1)^{i(\varphi)} c_{1\varphi(1)} \dots c_{k-1,\varphi(k-1)} c_{k\varphi(k)} c_{k+1,\varphi(k+1)} \dots c_{n\varphi(n)} =$$
$$\sum_{\varphi \in S_n} (-1)^{i(\varphi)} a_{1\varphi(1)} \dots a_{k-1,\varphi(k-1)} (a_{k\varphi(k)} + b_{k\varphi(k)}) a_{k+1,\varphi(k+1)} \dots a_{n\varphi(n)} =$$
$$\sum_{\varphi \in S_n} (-1)^{i(\varphi)} a_{1\varphi(1)} \dots a_{k-1,\varphi(k-1)} a_{k\varphi(k)} a_{k+1,\varphi(k+1)} \dots a_{n\varphi(n)} +$$
$$\sum_{\varphi \in S_n} (-1)^{i(\varphi)} a_{1\varphi(1)} \dots a_{k-1,\varphi(k-1)} b_{k\varphi(k)} a_{k+1,\varphi(k+1)} \dots a_{n\varphi(n)} = |A| + |B|$$

□

Veta 6.3.9. *Ak matica B vznikne z A pripočítaním c-násobku niektorého riadku k inému (pričom $c \in F$), tak $|B| = |A|$.*

Dôkaz. Nech B vznikne z A pripočítaním c-násobku k-teho riadku k l-temu riadku, pričom $k \neq l$. Teda B má všetky riadky rovnaké ako matica A, len prvky l-teho riadku majú tvar $b_{lj} = ca_{kj} + a_{lj}$.

Nech A' je matica, ktorá má všetky riadky rovnaké ako matica A len l-ty riadok matice A' sa rovná k-temu riadku matice A. (Teda $a'_{ij} = a_{ij}$ pre $i \neq l$ a $a'_{lj} = a_{kj}$.) Táto matica má dva rovnaké riadky, teda podľa vety 6.3.7 je $|A'| = 0$.

Uvažujme ďalej maticu A'', ktorá vznikne z A' vynásobením k-teho riadku skalárom c. (Teda $a''_{ij} = a_{ij}$ pre $i \neq l$ a $a''_{lj} = ca_{kj}$.) Z vety 6.3.5 máme $|A''| = c|A'| = 0$.

Teraz si stačí všimnúť, že maticu B dostaneme z matíc A a A'' spôsobom popísaným vo vete 6.3.8. Teda

$$|B| = |A| + |A''| = |A|.$$

□

Veta 6.3.10. *Ak matica B vznikne z A vzájomnou výmenou dvoch riadkov, tak $|B| = -|A|$. (Výmena 2 riadkov matice mení znamienko determinantu.)*

Dôkaz. Označme $\vec{\alpha}_1, \dots, \vec{\alpha}_n$ riadky matice A. Uvažujme maticu, ktorá má rovnaké riadky ako A, len namiesto i-teho aj namiesto j-teho riadku má $\vec{\alpha}_i + \vec{\alpha}_j$. Pretože táto matica má rovnaký i-ty a j-ty riadok, podľa vety 6.3.7

$$\begin{vmatrix} \vec{\alpha}_1 \\ \vec{\alpha}_i + \vec{\alpha}_j \\ \vec{\alpha}_i + \vec{\alpha}_j \\ \vec{\alpha}_n \end{vmatrix} = 0$$

(Kvôli stručnosti označenia sme vynechali sme všetky riadky, ktoré sú rovnaké ako v matici A, okrem prvého a posledného. Toto označenie rozhodne nie je korektné, snáď je však dostatočne zrozumiteľné.)

Tento determinant súčasne vieme prepísať pomocou vety 6.3.8 a vety 6.3.7

$$\begin{vmatrix} \vec{\alpha}_1 \\ \vec{\alpha}_i + \vec{\alpha}_j \\ \vec{\alpha}_i + \vec{\alpha}_j \\ \vec{\alpha}_n \end{vmatrix} = \begin{vmatrix} \vec{\alpha}_1 \\ \vec{\alpha}_i + \vec{\alpha}_j \\ \vec{\alpha}_i \\ \vec{\alpha}_n \end{vmatrix} + \begin{vmatrix} \vec{\alpha}_1 \\ \vec{\alpha}_i + \vec{\alpha}_j \\ \vec{\alpha}_j \\ \vec{\alpha}_n \end{vmatrix} = \begin{vmatrix} \vec{\alpha}_1 \\ \vec{\alpha}_i \\ \vec{\alpha}_i \\ \vec{\alpha}_n \end{vmatrix} + \begin{vmatrix} \vec{\alpha}_1 \\ \vec{\alpha}_j \\ \vec{\alpha}_i \\ \vec{\alpha}_n \end{vmatrix} + \begin{vmatrix} \vec{\alpha}_1 \\ \vec{\alpha}_i \\ \vec{\alpha}_j \\ \vec{\alpha}_n \end{vmatrix} + \begin{vmatrix} \vec{\alpha}_1 \\ \vec{\alpha}_j \\ \vec{\alpha}_j \\ \vec{\alpha}_n \end{vmatrix} = \begin{vmatrix} \vec{\alpha}_1 \\ \vec{\alpha}_j \\ \vec{\alpha}_i \\ \vec{\alpha}_n \end{vmatrix} + \begin{vmatrix} \vec{\alpha}_1 \\ \vec{\alpha}_i \\ \vec{\alpha}_j \\ \vec{\alpha}_n \end{vmatrix}$$

Porovnaním týchto 2 vzťahov dostaneme

$$0 = |A| + |B|,$$

čiže skutočne $|B| = -|A|$. $\square$

Teraz už vieme, ako ovplyvňujú hodnotu determinantu jednotlivé elementárne riadkové operácie. Podľa vety 6.2.6 platí $|A| = |A^T|$. Pretože riadkové operácie použité na transponovanú maticu A^T zodpovedajú stĺpcovým operáciam na pôvodnej matici A, všetky dokázané tvrdenia platia aj pre stĺpcové operácie. (Pri výpočte determinantov môžeme teda kombinovať riadkové aj stĺpcové operácie.)

Doteraz dokázané vety nám však len umožňujú porovnať determinant danej matice s determinantom redukovanej trojuholníkovej matice, ktorú dostaneme. Aby sme mohli túto metódu naozaj použiť na výpočet determinantu, potrebujeme ešte vedieť určiť determinant matice, ktorá je v redukovanom trojuholníkovom tvare. Na to nám poslúžia nasledujúce dva výsledky.

Veta 6.3.11. *Ak A je horná trojuholníková matica (pod hlavnou diagonálou má nuly), tak determinant matice A sa rovná súčinu prvkov na diagonále.*

$$|A| = a_{11}a_{22}\dots a_{nn}$$

Dôkaz. Stačí ukázať, že pre každú permutáciu $\varphi \in S_n$ okrem identickej premutácie je súčin $a_{1\varphi(1)}a_{2\varphi(2)}\dots a_{n\varphi(n)}$ nulový. Na to stačí, aby bol nulový niektorý činiteľ $a_{i\varphi(i)}$. Pretože predpokladáme, že A je horná trojuholníková matica, určite platí $a_{i\varphi(i)} = 0$ pre $i > \varphi(i)$. Zostáva nám teda ukázať, že aspoň jedno také i existuje.

Ak $\varphi \in S_n$ a $\varphi \neq id$, tak existuje $i \in \{1, 2, \dots, n\}$ také, že $i \neq \varphi(i)$. Nech i je najväčšie také číslo, čiže $i = \max\{k; \varphi(k) \neq k\}$. Označme $j = \varphi(i)$. Nemôže platiť $\varphi(j) = j$, lebo potom by sa na j zobrazili 2 rôzne prvky, čo je v spore s predpokladom, že φ je bijekcia. Teda platí $i > j = \varphi(i)$. $\square$

Dôsledok 6.3.12. *Determinant diagonálnej matice sa rovná súčinu diagonálnych prvkov.*

$$\begin{vmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{vmatrix} = d_1 d_2 \dots d_n$$

Príklad 6.3.13. Vypočítajme determinant z príkladu 6.3.4 tentokrát použitím riadkových a stĺpcových úprav.

$$\begin{vmatrix} 2 & 2 & 0 & 1 \\ 1 & 0 & -1 & 1 \\ 2 & 3 & 1 & 1 \\ 2 & 0 & -1 & 2 \end{vmatrix} \overset{(1)}{=} \begin{vmatrix} 2 & 2 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 3 & 3 & 1 & 2 \\ 1 & 0 & -1 & 1 \end{vmatrix} \overset{(2)}{=} - \begin{vmatrix} 2 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 3 & 3 & 0 & 2 \\ 1 & 0 & 0 & 1 \end{vmatrix} \overset{(3)}{=} - \begin{vmatrix} 2 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 3 & 3 & 0 & 2 \\ 1 & 0 & 0 & 1 \end{vmatrix} \overset{(4)}{=} - \begin{vmatrix} 2 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{vmatrix} \overset{(5)}{=} - \begin{vmatrix} 2 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{vmatrix} \overset{(6)}{=} \begin{vmatrix} 2 & 2 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{vmatrix} \overset{(7)}{=}$$
$$\begin{vmatrix} 2 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{vmatrix} \overset{(8)}{=} \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{vmatrix} \overset{(9)}{=} \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix} = 1$$

Elementárne riadkové a stĺpcové operácie, ktoré sme použili sú:

(1) 3. stĺpec sme pripočítali k prvému a štvrtému stĺpcu
(2) 2. riadok sme vynásobili -1
(3) odčítali sme druhý riadok od tretieho a pripočítali sme ho k štvrtému
(4) odpočítali sme 1. riadok od tretieho
(5) odpočítali sme 4. riadok od tretieho
(6) výmena druhého a tretieho riadku
(7) odpočítali sme 2-násobok 2. riadku od prvého

(8) odpočítali sme 4. riadok od prvého
(9) odčítali sme 1. riadok od štvrtého

Asi najviac si zjednodušíme prácu, ak budeme kombinovať oba postupy – riadkové a stĺpcové úpravy aj Laplaceov rozvoj. Napríklad namiesto kroku (2) alebo (3) v predchádzajúcom postupe sme mohli použiť Laplaceov rozvoj podľa 2. riadku a dostali by sme sa tak k determinantu 3×3.

Poznámka 6.3.14. Všetky výsledky, ktoré sme odvodili pre zmeny determinantu pri elementárnych riadkových úpravách zodpovedajú geometrickej intuícii, ktorú sme spomínali – že determinant môžeme chápať (až na znamienko) ako objem.

Konkrétne vynásobenie niektorého riadku konštantou znamená c-násobné natiahnutie rovnobežnostena v smere niektorej z jeho hrán, pričom sa aj objem zväčší c-krát. Podobne pripočítanie násobku i-teho riadku k j-temu predstavuje vlastne skosenie rovnobežnostena v smere i-tej hrany. Pri ňom sa nemení objem. (Podobne – snáď ešte jednoduchšie – si môžete rozmyslieť, že to funguje pre dvojrozmerný rovnobežník.)

Veta 6.3.15. *Nech A je štvorcová matica typu $n \times n$. Matica A je regulárna práve vtedy, keď $|A| \neq 0$.*

Dôkaz. Pripomeňme, že matica A je regulárna práve vtedy, keď hodnosť matice je n. Vieme, že hodnosť matice sa rovná počtu nenulových riadkov v redukovanej trojuholníkovej matici M, ktorá je riadkovo ekvivalentná s A.

Ak matica A nie je regulárna, tak príslušná redukovaná trojuholníková matica má aspoň jeden nulový riadok. Podľa dôsledku 6.3.6 má teda nulový determinant. Ako sme dokázali v predchádzajúcich vetách, žiadna z elementárnych riadkových úprav nemení nulovosť a nenulovosť determinantu. Preto aj determinant matice A je nulový.

Ak A je regulárna, tak príslušná redukovaná trojuholníková matica má n nenulových riadkov. Pretože ide o maticu typu $n \times n$, priamo z definície redukovanej trojuholníkovej matice vyplýva, že to je jednotková matica I_n, ktorá má nenulový determinant $|I_n| = 1$. $\square$

Teraz, keď už vieme, že sú pre nás podstatné len regulárne matice, mohli by sme vetu 6.3.11 a dôsledok 6.3.12 odvodiť v opačnom poradí. Priamy dôkaz dôsledku 6.3.12 by sa podobal na dôkaz vety 6.3.11, bol by však jednoduchší v tom, že teraz už máme nuly aj nad diagonálou a nepotrebujeme hľadať i také, že $i > \varphi(i)$. (Stačí nám, že $i \neq \varphi(i)$.) Akonáhle už máme dokázaný dôsledok 6.3.12 a chceme overiť vetu 6.3.11 pre regulárnu hornú trojuholníkovú maticu, stačí si uvedomiť, že takúto maticu vieme upraviť na diagonálnu už len používaním pripočítavania niektorého riadku k inému a pri tejto úprave sa hodnota determinantu nemení (veta 6.3.9).

6.4 Determinant súčinu matíc

Teraz dokážeme ešte jeden dôležitý výsledok týkajúci sa determinantov. Stručne povedané, tento výsledok hovorí, že determinant súčinu matíc sa rovná súčinu determinantov.

Veta 6.4.1. *Nech A, B sú dve matice typu $n \times n$ nad poľom F. Potom platí*

$$|A.B| = |A|.|B|.$$

Dôkaz. Označme riadky matice A ako $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$. Teda

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix} = \begin{pmatrix} \vec{\alpha}_1 \\ \vec{\alpha}_2 \\ \vdots \\ \vec{\alpha}_n \end{pmatrix}$$

Priamo z definície súčinu matíc (rozmyslite si to!) sa dá zistiť, že riadky matice $A.B$ majú tvar $\vec{\alpha}_k B$, čiže

$$A.B = \begin{pmatrix} \vec{\alpha}_1 B \\ \vec{\alpha}_2 B \\ \vdots \\ \vec{\alpha}_n B \end{pmatrix}$$

Pretože $\vec{\alpha}_k = \sum_{i=1}^n a_{ki}\vec{e}_i$, môžeme túto rovnosť upraviť na tvar

$$A.B = \begin{pmatrix} \sum_{i_1=1}^n a_{1i_1}\vec{e}_{i_1} B \\ \vdots \\ \sum_{i_n=1}^n a_{ni_n}\vec{e}_{i_n} B \end{pmatrix}$$

Pomocou viacnásobného použitia vety 6.3.8 postupne dostaneme

$$|A.B| = \sum_{i_1=1}^n a_{1i_1} \begin{vmatrix} \vec{e}_{i_1} B \\ \sum_{i_2=1}^n a_{2i_2}\vec{e}_{i_2} B \\ \vdots \\ \sum_{i_n=1}^n a_{ni_n}\vec{e}_{i_n} B \end{vmatrix} = \ldots = \sum_{i_1=1}^n \ldots \sum_{i_n=1}^n a_{1i_1}a_{2i_2}\ldots a_{ni_n} \begin{vmatrix} \vec{e}_{i_1} B \\ \vec{e}_{i_2} B \\ \vdots \\ \vec{e}_{i_n} B \end{vmatrix}$$

Teraz si uvedomme, že ak $i_j = i_k$ pre nejaké $j \neq k$, tak príslušný determinant v predchádzajúcej sume je nulový (lebo má 2 rovnaké riadky). Teda nenulové sčítance budú iba tie, kde n-tica $(i_1, i_2, \ldots, i_n)$ predstavuje permutáciu čísel $1, \ldots, n$. Dostávame teda

$$|A.B| = \sum_{\varphi \in S_n} a_{1\varphi(1)}a_{2\varphi(2)}\ldots a_{n\varphi(n)} \begin{vmatrix} \vec{e}_{\varphi(1)} B \\ \vec{e}_{\varphi(2)} B \\ \vdots \\ \vec{e}_{\varphi(n)} B \end{vmatrix}$$

Matica vystupujúca v predchádzajúcej rovnosti je vlastne matica B s poprehadzovanými riadkami. Pomocou výmen niektorých riadkov z nej vieme dostať maticu B. O chvíľu si ukážeme, že sa to dá urobiť pomocou $i(\varphi)$ výmen. Na základe toho prejde predchádzajúca rovnosť na tvar

$$|A.B| = \sum_{\varphi \in S_n} a_{1\varphi(1)}a_{2\varphi(2)}\ldots a_{n\varphi(n)}(-1)^{i(\varphi)}|B| = |A|.|B|.$$

Zostáva nám teda overiť, že potrebný počet výmen je skutočne $i(\varphi)$. Pri upravovaní „poprehadzovanej matice na maticu“ B môžeme postupovať tak, že najprv premiestníme prvý riadok na prvé miesto a to tak, že ho vždy vymieňame s predchádzajúcim, až kým sa nedostane na správnu pozíciu. (Ak už je na prvom mieste, nerobíme žiadne výmeny.) Takto sme urobili toľko výmen riadkov, koľko má permutácia φ inverzií obsahujúcich číslo 1. Teraz môžeme podobným spôsobom presunúť druhý riadok na druhé miesto. Počet výmen je rovnaký ako počet tých invzerzií, ktoré obsahujú 2 ale nie 1 (pretože prvý riadok sme už presunuli). Takto postupujeme ďalej. Vidíme, že pri takomto algoritme dostaneme maticu B pomocou presne $i(\varphi)$ výmen riadkov. □

Dôkaz, ktorý sme uviedli, je v princípe rovnaký ako v [A, Theorem 10.31]. V [K, Veta 6.2.18] môžete nájsť dôkaz, ktorý využíva rozloženie matice na súčin redukovanej trojuholníkovej matice a matíc elementárnych riadkových operácií. Ešte jeden, úplne iný dôkaz, môžete nájsť v [KGGS, Veta 2.14.7].

Hovorili sme o tom, že ako geometrický význam determinantu si môžeme predstaviť objem rovnobežnostena určeného riadkami matice. V prípade, že danú maticu chápeme ako maticu lineárneho zobrazenia, je to presne objem rovnobežnostena na ktorý sa zobrazí jednotková kocka (určená vektormi štandardnej bázy). Determinant nám teda hovorí, koľkokrát sa pri zobrazení daným lineárnym zobrazením zväčší objem jednotkovej kocky. Pretože ide o lineárne zobrazenie, aj objem ľubovoľného rovnobežnostena sa zväčší v rovnakom pomere. A presne toto tvrdenie vlastne hovorí veta, ktorú sme práve dokázali. (V poznámke 6.3.14 sme hovorili o súvise medzi touto geometrickou predstavou a elementárnymi riadkovými operáciami. Spomínaný dôkaz z [K] teda vlastne zodpovedá tejto geometrickej intuícii – ľubovoľné lineárne zobrazenie sme najprv rozložili na jednoduchšie zobrazenia, o ktorých vieme ukázať koľkokrát zväčšujú objem. Pomocou toho vieme určiť, koľkokrát sa zväčší objem pri použití pôvodného zobrazenia.)

6.5 Využitie determinantov

6.5.1 Výpočet inverznej matice

Veta 6.5.1. *Ak A je regulárna matica typu $n \times n$, tak*

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

kde A_{ij} označuje algebraický doplnok prvku a_{ij}.

Poznámka 6.5.2. Maticu

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

nazývame *adjungovaná matica* k matici A a označuje $\operatorname{adj} A$. Teda vyjadrenie inverznej matice z predchádzajúcej vety môžeme zapísať aj v tvare

$$A^{-1} = \frac{\operatorname{adj} A}{|A|}.$$

POZOR na výmenu poradia indexovania – algebraické doplnky v adjungovanej matici nie sú indexované tak, ako v pôvodnej matici ale podobným spôsobom ako v transponovanej matici.

Dôkaz. Treba dokázať, že $A.\frac{\operatorname{adj}(A)}{|A|} = I$. Označme maticu $A.\frac{\operatorname{adj}(A)}{A}$ ako C. Pre jej prvky platí

$$c_{ij} = \frac{1}{|A|} \sum_{k=1}^{n} a_{ik} A_{jk}.$$

Potrebujeme vlastne ukázať, že $c_{ii} = 1$ a $c_{ij} = 0$ pre $i \neq j$.

Pre $i = j$ dostávame

$$c_{ii} = \frac{1}{|A|} \sum_{k=1}^{n} a_{ik} A_{ik}.$$

Suma v predchádzajúcej rovnosti je presne rozvoj matice A podľa i-teho riadku, čiže sme dostali $c_{ii} = \frac{|A|}{|A|} = 1$.

Pre $i \neq j$ si všimneme, že suma vo výraze

$$c_{ij} = \frac{1}{|A|} \sum_{k=1}^{n} a_{ik} A_{jk}.$$

predstavuje Laplaceov rozvoj matice, ktorá vznikne z A nahradením j-teho riadku i-tym, podľa (nového) j-teho riadku. Pretože táto matica má dva riadky rovnaké, jej determinant je nulový, z čoho $c_{ij} = 0$. □

V predchádzajúcom dôkaze sme overili pre maticu $B = \frac{\operatorname{adj}(A)}{A}$ rovnosť $AB = I$. V definícii inverznej matice však vystupuje aj rovnosť $BA = I$. Nie je to chyba? Zabudli sme ju overiť?

Nie, nie je to chyba. V predpokladoch vety totiž máme, že A je regulárna, teda A^{-1} existuje. Vďaka tomu z rovnosti $AB = I$ po vynásobení A^{-1} dostaneme $B = A^{-1}$.

Príklad 6.5.3. Nech $A = \begin{pmatrix} 1 & -1 & 1 \\ 2 & 1 & 1 \\ 2 & -1 & 2 \end{pmatrix}$. Priamym výpočtom dostaneme $|A| = 1$ a $\operatorname{adj} A = \begin{pmatrix} 3 & 1 & -2 \\ -2 & 0 & 1 \\ -4 & -1 & 3 \end{pmatrix}$.

Z toho dostávame, že

$$A^{-1} = \frac{1}{|A|} \operatorname{adj} A = \begin{pmatrix} 3 & 1 & -2 \\ -2 & 0 & 1 \\ -4 & -1 & 3 \end{pmatrix}.$$

Vynásobením matíc sa môžeme presvedčiť, že skutočne platí $A.A^{-1} = A^{-1}.A = I$.

6.5.2 Cramerovo pravidlo

Na začiatku kapitoly sme si ukázali, ako sa dá pomocou determinantu vyjadriť riešenie sústavy 2 lineárne nezávislých rovníc o 2 neznámych. Teraz odvodíme analogický výsledok pre sústavy n rovníc s n neznámymi.

Majme sústavu

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & | & c_1 \\ a_{21} & a_{22} & \dots & a_{2n} & | & c_2 \\ \dots & \dots & \dots & \dots & | & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} & | & c_n \end{pmatrix}$$

Označme maticu sústavy ako A a $C := (c_1, c_2, \dots, c_n)^T$ maticu, v ktorej sú do stĺpca zapísané pravé strany. Hľadáme vlastne takú maticu X, pre ktorú platí

$$AX = C.$$

Ak je matica A regulárna, vynásobením A^{-1} zľava dostaneme

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = A^{-1}C = \frac{1}{|A|} \begin{pmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \dots & \dots & \dots & \dots \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}$$

Z predchádzajúcej rovnosti dostaneme

$$x_i = \frac{1}{|A|} \sum_{j=1}^{n} A_{ji} c_j.$$

Nech A_i označuje maticu, ktorú dostaneme ak v matici A nahradíme i-ty stĺpec stĺpcom $(c_1, c_2, \ldots, c_n)^T$ (čiže pravými stranami). Potom si môžeme všimnúť, že výraz vystupujúci v predchádzajúcej rovnosti je presne Laplaceov rozvoj matice A_i podľa i-teho stĺpca. (Iné stĺpce sme nemenili, preto algebraické doplnky vystupujúce v Laplaceovom rozvoji sú rovnaké ako pre maticu A.) Platí teda

$$|A_i| = \sum_{j=1}^{n} A_{ji} c_j,$$

z čoho dostaneme

$$x_i = \frac{|A_i|}{|A|}.$$

Tým sme odvodili vzorec pre riešenia sústavy lineárnych rovníc, ktorá má regulárnu maticu. Tento vzorec sa nazýva *Cramerovo pravidlo.*

Príklad 6.5.4. Majme sústavu $\left(\begin{array}{ccc|c} 1 & -1 & 1 & 1 \\ 2 & 1 & 1 & 2 \\ 2 & -1 & 2 & 3 \end{array}\right)$. V príklade 6.5.3 sme vypočítali determinant $|A| = 1$.

Ostatné determinanty, ktoré potrebujeme na použitie Cramerovho pravidla sú

$\begin{vmatrix} 1 & -1 & 1 \\ 2 & 1 & 1 \\ 3 & -1 & 2 \end{vmatrix} = \begin{vmatrix} 1 & -1 & 1 \\ 2 & 1 & 1 \\ 0 & -1 & 0 \end{vmatrix} = -2 + 1 = -1$

(Úprava, ktorú sme použili, bolo odčítanie prvých dvoch riadkov od tretieho.)

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

$\begin{vmatrix} 1 & -1 & 1 \\ 2 & 1 & 2 \\ 2 & -1 & 3 \end{vmatrix} = \begin{vmatrix} 1 & -1 & 0 \\ 2 & 1 & 0 \\ 2 & -1 & 1 \end{vmatrix} = 1 + 2 = 3$

Z toho dostaneme riešenie sústavy $(-1, 1, 3)$.

Cvičenia

Úloha 6.5.1. Vypočítajte determinanty: $\begin{vmatrix} -2 & 3 & -3 & -1 \\ 1 & -2 & 3 & 2 \\ 0 & 1 & 1 & 1 \\ 1 & -1 & -1 & -2 \end{vmatrix}$ $\begin{vmatrix} -2 & 3 & -2 & -1 \\ 1 & -2 & 1 & 2 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{vmatrix}$ $\begin{vmatrix} -2 & 3 & -1 & -1 \\ 1 & -2 & 1 & 2 \\ 1 & 1 & 2 & -1 \\ 0 & 1 & -1 & -1 \end{vmatrix}$
Ak existuje inverzná matica, aký bude jej determinant. Výsledky (bez záruky): 0,8,8.

Úloha 6.5.2. Vyriešte v $\mathbb{Z}_5$ pomocou Cramerovho pravidla: $\left(\begin{array}{ccc|c} 3 & 4 & 0 & 1 \\ 1 & 1 & 2 & 1 \\ 3 & 4 & 1 & 0 \end{array}\right)$ $\left(\begin{array}{ccc|c} 1 & 1 & 4 & 1 \\ 0 & 1 & 2 & 2 \\ 1 & 0 & 3 & 3 \end{array}\right)$ $\left(\begin{array}{ccc|c} 1 & 2 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 2 & 1 & 3 & 2 \end{array}\right)$

Úloha 6.5.3. Pomocou Cramerovho pravidla riešte:

$$\begin{array}{rrrrl} x_1 & +5x_2 & +4x_3 & +3x_4 & = 1 \\ 2x_1 & -x_2 & +2x_3 & -x_4 & = 0 \end{array} \qquad \begin{array}{rrrl} x_1 & +2x_2 & +x_3 & = 1 \\ 2x_1 & +x_2 & -x_3 & = 0 \end{array}$$

(Návod: Skúste zvoliť x_3, x_4 za parametre.)

Úloha 6.5.4. Určte determinanty daných matíc. Viete na základe výsledku určiť ich hodnosť?

$\begin{vmatrix} 1 & 2 & c-1 \\ c-2 & 1 & 0 \\ c & 1 & 0 \end{vmatrix}$ $\begin{vmatrix} 1 & 1 & c-1 \\ c-2 & 1 & 0 \\ 0 & 1 & c \end{vmatrix}$ $\begin{vmatrix} 2 & c+1 & 0 \\ 2 & c-1 & 2c \\ 1 & 1 & 1 \end{vmatrix}$

Úloha 6.5.5. Nájdite inverznú maticu k maticiam z úlohy 5.5.1 pomocou determinantu.

Úloha 6.5.6. Vypočítajte inverznú maticu:
$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$ $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & -1 \\ 1 & 4 & 9 & 1 \\ 1 & 8 & 27 & -1 \end{pmatrix}$

Úloha 6.5.7*. $\begin{vmatrix} 1 & a_1 & a_1^2 & \dots & a_1^n \\ 1 & a_2 & a_2^2 & \dots & a_2^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \dots & a_n^n \\ 1 & a_{n+1} & a_{n+1}^2 & \dots & a_{n+1}^n \end{vmatrix} = ?$

Úloha 6.5.8*. $D_n = \begin{vmatrix} 2 & 1 & 0 & 0 & \dots & 0 \\ 1 & 2 & 1 & 0 & \dots & 0 \\ 0 & 1 & 2 & 1 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & 2 & 1 \\ 0 & \dots & 0 & 0 & 1 & 2 \end{vmatrix} = ?$

Úloha 6.5.9*. $D_n = \begin{vmatrix} a+b & ab & 0 & 0 & \dots & 0 \\ 1 & a+b & ab & 0 & \dots & 0 \\ 0 & 1 & a+b & ab & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & a+b & ab \\ 0 & \dots & 0 & 0 & 1 & a+b \end{vmatrix} = ?$

Úloha 6.5.10*. $D_n = \begin{vmatrix} n & 1 & 1 & \dots & 1 \\ 1 & n & 1 & \dots & 1 \\ \dots & \dots & \dots & \dots & \\ 1 & \dots & 1 & 1 & n \end{vmatrix} = ?$

Kapitola 7

Euklidovské vektorové priestory

7.1 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:

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

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 7.1.1. 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 $c \in F$ platí

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

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

(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.*

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

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

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

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

Príklad 7.1.2. 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 7.1.3. Definujme na $\mathbb{R}^2$ skalárny súčin nasledovne:

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

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

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

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

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

kde C je matica typu $n \times n$. Takýto predpis priradí 2 vektorom $\vec{\alpha} = (a_1, \ldots, a_n), \vec{\beta} = (b_1, \ldots, b_n) \in \mathbb{R}^n$ 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.

Príklad 7.1.5. 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 7.1.6. 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 7.1.7. *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*)

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 c a môžeme ju chápať ako kvadratickú nerovnicu s neznámou c, diskriminant tejto nerovnice musí byť nezáporný

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

Z tejto nerovnosti dostaneme

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

(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). □

Definícia 7.1.8. 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 7.1.9. 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 7.1.10. *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 si ľubovoľné $i \in \{1, 2, \ldots, k\}$. Potom dostaneme

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

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

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

sa nazýva *ortogonálny doplnok* množiny M.

Tvrdenie 7.1.12. *Nech V je euklidovský priestor a $M \subseteq V$. Potom $M^{\perp}$ je vektorový priestor 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 7.1.13. *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 7.1.14. *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 7.1.15. *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

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

□

7.2 Gram-Schmidtov ortogonalizačný proces

Definícia 7.2.1. 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

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

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

Z tvrdenia 7.1.10 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 7.2.2. Ak vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ sú ortonormálne a tvoria bázu vektorového priestoru V, tak túto bázu nazývame *ortonormálna báza.*

Príklad 7.2.3. 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 7.2.4. *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

$$\begin{aligned}
0 = \langle \vec{\gamma}_{k+1}, \vec{\gamma}_1 \rangle &= \langle \vec{\alpha}_{k+1}, \vec{\gamma}_1 \rangle + c_{k+1,1}\langle \vec{\gamma}_1, \vec{\gamma}_1 \rangle \\
0 = \langle \vec{\gamma}_{k+1}, \vec{\gamma}_2 \rangle &= \langle \vec{\alpha}_{k+1}, \vec{\gamma}_2 \rangle + c_{k+1,2}\langle \vec{\gamma}_2, \vec{\gamma}_1 \rangle \\
0 = \langle \vec{\gamma}_{k+1}, \vec{\gamma}_3 \rangle &= \langle \vec{\alpha}_{k+1}, \vec{\gamma}_3 \rangle + c_{k+1,3}\langle \vec{\gamma}_3, \vec{\gamma}_1 \rangle \\
&\vdots \\
0 = \langle \vec{\gamma}_{k+1}, \vec{\gamma}_k \rangle &= \langle \vec{\alpha}_{k+1}, \vec{\gamma}_k \rangle + c_{k+1,k}\langle \vec{\gamma}_k, \vec{\gamma}_1 \rangle
\end{aligned} \tag{7.1}$$

(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 $c_{k+1,i}$:

$$c_{k+1,i} = -\frac{\langle \vec{\alpha}_{k+1}, \vec{\gamma}_i \rangle}{\langle \vec{\gamma}_1, \vec{\gamma}_1 \rangle}$$

pre každé $i = 1, 2, \ldots, k$.

Z rovníc (7.1) 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 $\vec{\gamma}_{k+1} = \vec{\alpha}_{k+1} + c_{k1}\vec{\gamma}_1 + c_{k2}\vec{\gamma}_2 + \ldots + c_{k+1,k}\vec{\gamma}_k$ 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 $\vec{\alpha}_{k+1} = \vec{\gamma}_{k+1} - (c_{k1}\vec{\gamma}_1 + c_{k2}\vec{\gamma}_2 + \ldots + c_{k+1,k}\vec{\gamma}_k)$ 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 7.2.5. 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 $\vec{\gamma}_3 = \vec{\alpha}_3 + d\vec{\gamma}_1 + e\vec{\gamma}_3$ tak, aby

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

z čoho

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

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

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

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

$$\begin{aligned} |\vec{\gamma}_1| &= \sqrt{2} \\ |\vec{\gamma}_2| &= \frac{\sqrt{11}}{\sqrt{2}} \\ |\vec{\gamma}_3| &= \frac{\sqrt{672}}{11} = \frac{4\sqrt{41}}{11} \end{aligned}$$

a teda ortonormálna báza priestoru V je

$$\begin{aligned} \vec{\beta}_1 &= \frac{1}{\sqrt{2}}(1, 0, 1, 0) \\ \vec{\beta}_2 &= \frac{\sqrt{2}}{\sqrt{11}}(\frac{1}{2}, 2, -\frac{1}{2}, 1) \\ \vec{\beta}_3 &= \frac{11}{4\sqrt{41}}\left(-\frac{12}{11}, -\frac{4}{11}, \frac{12}{11}, \frac{20}{11}\right) = \frac{1}{4\sqrt{41}}(-12, -4, 12, 20) = \frac{1}{\sqrt{41}}(-3, -1, 3, 5). \end{aligned}$$

Vidíme, že vektory, ktoré sme dostali vyzerajú pomerne zložito. Nevedeli by sme si nejako zjednodušiť tieto výpočty? Možno 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 $\vec{\gamma}_3 = \vec{\alpha}_3 + d\vec{\gamma}_1 + e\vec{\gamma}_1$. 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.

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

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

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

Cvičenia

Úloha 7.2.1. 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 7.2.2. 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 7.2.3. Zistite, či $\sin \pi x$ a $\cos \pi x$ sú kolmé v priestore $C(0,1)$ so skalárnym súčinom z príkladu 7.1.5. Akú majú tieto vektory veľkosť?

Úloha 7.2.4. Nájdite ortonormálnu bázu pre priestory z úlohy 7.2.1.

Dodatok A

Delenie so zvyškom

O veciach, ktoré spomenieme v tomto dodatku, sa oveľa viac dozviete na predmete Elementárna teória čísel v letnom semestri, pozri napríklad [Č]. Tu zhrnieme základné veci, ktoré budeme potrebovať a podrobnejšie si na príkladoch ukážeme viacero postupov, ktoré sa v tejto prednáške objavia častejšie.

TODO

Dodatok B

Komplexné čísla

Základné vlastnosti komplexných čísel môžete nájsť vo veľkom množstve vysokoškolských i stredoškolských učebníc, ako napríklad [I, Kapitola 13], [KMŠ, Kapitola II.10], [Sm], [Bl] a mnoho iných. Kniha [AA] sa venuje komplexným číslam od základných poznatkov až po ich použitie v úlohách olympiádneho charakteru.

Niektorí z vás preberali komplexné čísla na strednej škole, pre tých, ktorí ich nemali, sa tu pokúsime zhrnúť ich najdôležitejšie vlastnosti, ktoré budete potrebovať.

B.1 Definícia komplexných čísel, algebraický tvar komplexného čísla

Vieme, že v reálnych číslach nemá rovnica

$$x^2 = -1$$

riešenie. (Pre každé reálne číslo platí $x^2 \geq 0$.) Čo by sme potrebovali urobiť, keby sme chceli dostať číselný obor, v ktorom táto rovnica bude mať riešenie? Znamená to vlastne, že chceme k reálnym číslam pridať nejaké „nové“ čísla a zadefinovať na nich sčitovanie a násobenie tak, aby sa tieto operácie správali podobne ako pre reálne čísla. (Pod slovom „podobne“ rozumieme to, že novovytvorený číselný obor má byť pole.) Ideme sa teraz pokúsiť zadefinovať takéto pole, ktoré potom nazveme poľom komplexných čísel.

Určite musíme teda pridať aspoň jedno riešenie rovnice $x^2 = -1$. Označíme ho i a budeme ho nazývať *imaginárna jednotka*. Teda

$$i^2 = -1. \tag{B.1}$$

Pretože chceme, aby komplexné čísla obsahovali všetky reálne čísla musíme potom pridať aj čísla tvaru $b.i$, pre ľubovoľné $b \in \mathbb{R}$ a aj čísla tvaru $a + bi$ pre ľubovoľné $a \in \mathbb{R}$. Ukážeme si, že tieto čísla už postačia na to, aby sme vytvorili pole.

Definícia B.1.1. *Komplexným číslom* budeme nazývať ľubovoľné číslo tvaru

$$a + bi,$$

kde $a, b \in \mathbb{R}$. Množinu všetkých komplexných čísel označujeme

$$\mathbb{C} = \{a + bi; a, b \in \mathbb{R}\}.$$

Zápis komplexného čísla v tvare $a + bi$ nazývame *algebraický zápis* komplexného čísla. Pritom a sa nazýva *reálna časť* komplexného čísla a bi sa nazýva *imaginárna časť* komplexného čísla. Pre komplexné číslo $z = a + bi$ označujeme jeho reálnu časť $\operatorname{Re} z = a$ a imaginárnu časť $\operatorname{Im} z = bi$. (Niekedy sa tiež používa označenie $\Re z$ a $\Im z$.) Číslo, ktoré má nulovú reálnu časť, sa nazýva *rýdzoimaginárne.*

Komplexné číslo je jednoznačne určené svojou reálnou a imaginárnou časťou, teda dve komplexné čísla $z_1 = a_1 + b_1 i$ a $z_2 = a_2 + b_2 i$ sa rovnajú práve vtedy, keď

$$a_1 = a_2 \quad \text{a} \quad b_1 = b_2.$$

Poznámka B.1.2. Definíciu komplexných čísel môžeme chápať takým spôsobom, že sme zaviedli nejaký nový symbol i a komplexné čísla sú formálne zápisy tvaru $a + bi$, pričom a, b sú ľubovoľné reálne čísla.

Iná možnosť by bola definovať komplexné čísla ako usporiadané dvojice reálnych čísel a dohodnúť sa, že namiesto (a, b) budeme používať zápis $a + bi$. (Všimnite si, že takýto prístup zodpovedá tomu, že 2 komplexné čísla považujeme za rovnaké práve vtedy, keď majú rovnaké obe zložky.)

Pri prvom prístupe (formálne zápisy tvaru $a + bi$) je jasné, že reálne čísla sú podmnožinou komplexných čísel. (Každé reálne číslo a sa dá vyjadriť ako $a + 0i$, teda je prvkom množiny $\mathbb{C}$.) Pri druhom prístupe reálne čísla stotožníme s množinou $\{(a, 0); a \in \mathbb{R}\}$. Sčitovanie a násobenie definujeme tak, aby korešpondovali so sčitovaním a násobením reálnych čísel.

Pomocou nového symbolu i sme zaviedli nejakú množinu, ktorej prvky sme nazvali komplexné čísla. Ďalej by sme na tejto množine chceli zaviesť operácie sčitovania a násobenia tak, aby množina $\mathbb{C}$ s týmito operáciami tvorila pole.

Súčet 2 komplexných čísel definujeme veľmi prirodzeným spôsobom – sčítame ich reálne časti aj imaginárne časti:

$$(a + bi) + (c + di) = (a + c) + (b + d)i \tag{B.2}$$

Ak chceme, aby platila distributívnosť, tak pre súčin čísel $a + bi$ a $c + di$ musí platiť

$$(a + bi)(c + di) = ac + bci + adi + bdi^2$$

a z rovnosti (B.1) potom máme

$$(a + bi)(c + di) = (ac - bd) + (bc + ad)i \tag{B.3}$$

Príklad B.1.3. $(2 + 3i) + (2 - i) = 4 + 2i$
$(2 + 3i)(2 - i) = 4 - 2i + 6i + 3 = 7 + 4i$
$(\sqrt{2} + \sqrt{2}i)(\sqrt{2} + \sqrt{2}i) = 2 + 2i + 2i - 2 = 4i$

Oplatí sa zapamätať si, že

$$\begin{array}{cccc} i^1 = i & i^2 = -1 & i^3 = -i & i^4 = 1 \\ i^{4k+1} = i & i^{4k+2} = -1 & i^{4k+3} = -i & i^{4k} = 1 \end{array} \tag{B.4}$$

Poznámka B.1.4. Násobenie a sčitovanie by sme definovali analogicky, keby sme komplexné čísla chápali ako dvojice reálnych čísel, pozri úloha 3.3.11.

Dôležité je, že takto definované operácie + a · sa správajú „rozumne“. Inak povedané, radi by sme ukázali, že $(\mathbb{C}, +, \cdot)$ je pole.

Niektoré z vlastností poľa sú zrejmé takmer okamžite. Komutatívnosť a asociatívnosť operácie + sa overí ľahko. Neutrálny prvok tejto operácie je $0 = 0 + 0i$ a inverzný prvok k $a + bi$ je $-(a + bi) = (-a) + (-b)i$. Z toho špeciálne vyplýva, že komplexné čísla vieme aj odčitovať,

$$(a + bi) - (c + di) = (a - c) + (b - d)i.$$

(Môžete si všimnúť, že ak sa na komplexné čísla pozeráme ako na dvojice reálnych čísel, tak je to tá istá operácia, ktorú sme zaviedli v úlohe 3.2.1g), resp. v príklade 4.1.3, kde sme videli, že dvojice reálnych čísel môžeme chápať ako vektorový priestor.)

V prípade operácie · máme o trochu komplikovanejšiu situáciu. Jej komutatívnosť je jasná priamo z definície. Skúsme overiť asociatívnosť. Teda máme 3 komplexné čísla $z_1 = a + bi$, $z_2 = c + di$ a $z_3 = e + fi$ a chceme priamym výpočtom (teda na základe definície násobenie) overiť $z_1(z_2z_3) = (z_1z_2)z_3$.

$$\begin{aligned} z_1(z_2z_3) &= (a + bi)[(c + di)(e + fi)] = (a + bi)[(ce - df) + (cf + de)i] = \\ &= (ace - adf - bcf - bde) + (acf + ade + bce - bdf)i \\ (z_1z_2)z_3 &= [(a + bi)(c + di)](e + fi) = [(ac - bd) + (bc + ad)i](e + fi) = \\ &= (ace - bde - bcf - adf) + (acf - bdf + bce + ade)i \end{aligned}$$

Vidíme, že v oboch prípadoch sme dostali taký istý výsledok.

Ľahko sa overí, že neutrálny prvok pre násobenie je $1 = 1 + 0i$.

Potrebovali by sme ešte zistiť, či vieme komplexné čísla deliť (z toho dostaneme existenciu inverzného prvku). Deliť komplexným číslom $c + di$ môžeme iba vtedy, ak je toto číslo rôzne od nuly. Teda $c + di \neq 0 + 0i$, čo znamená, že buď $c \neq 0$ alebo $d \neq 0$. Spôsob, akým to urobíme, sa podobá na trik, ktorým obvykle odstraňujeme z menovateľa odmocninu.

$$\frac{a + bi}{c + di} = \frac{a + bi}{c + di}\frac{c - di}{c - di} = \frac{(a + bi)(c - di)}{(c + di)(c - di)} = \frac{(ac + bd) + (bc - ad)i}{c^2 + d^2} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}i \tag{B.5}$$

Všimnime si, že ak je aspoň jedno z reálnych čísel c, d nenulové, tak $c^2 + d^2 > 0$, čiže v predchádzajúcom výraze nevystupuje v menovateli nula.

Príklad B.1.5. $\frac{1+2i}{2-i} = \frac{(1+2i)(2+i)}{(2-i)(2+i)} = \frac{5i}{5} = i$

Jediná vlastnosť z definície poľa, ktorú sme zatiaľ neoverili, je distributívnosť, t.j.

$$z_1(z_2 + z_3) = z_1z_3 + z_2z_3.$$

Táto vlastnosť sa opäť dá overiť priamym výpočtom (úloha B.4.3).

Overením jednotlivých vlastností sme dokázali:

Veta B.1.6. *Komplexné čísla s operáciami + a · definovanými vzťahmi* (B.2) *a* (B.3) *tvoria pole.*

Akonáhle máme dokázanú túto vetu, vieme, že pre komplexné čísla môžeme používať všetky vlastnosti z tvrdenia 3.3.4 a takisto vlastnosti, ktoré sme dokázali v cvičeniach v časti 3.3. (Takisto, keďže sme sa naučili riešiť sústavy lineárnych rovníc, počítať determinanty, inverzné matice a mnohé ďalšie veci v ľubovoľnom poli, vieme to robiť aj v poli komplexných čísel.)

Číslo $a - bi$, ktorým sme rozšírili čitateľ aj menovateľ pri výpočte podielu dvoch komplexných čísel (pozri (B.5) a príklad B.1.5) sa vyskytuje v súvislosti s číslom $a + bi$ pomerne často.

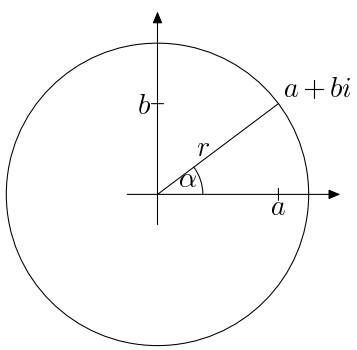
Definícia B.1.7. *Komplexne združeným číslom* k číslu $z = a + bi$ nazývame číslo $\overline{z} = a - bi$.

Úloha B.1.1. Overte, že platí (pre ľubovoľné $z, z_1, z_2 \in \mathbb{C}$)

$$\begin{aligned} \overline{z_1 + z_2} &= \overline{z_1} + \overline{z_2} \\ \overline{z_1 . z_2} &= \overline{z_1} . \overline{z_2} \\ z . \overline{z} &= |z|^2 \\ z = \overline{z} \quad &\Leftrightarrow \quad z \text{ je reálne} \\ z = -\overline{z} \quad &\Leftrightarrow \quad z \text{ je rýdzoimaginárne} \end{aligned}$$

B.2 Geometrická interpretácia komplexných čísel, goniometrický tvar, Moivrova veta

Ako sme už spomenuli, komplexné čísla môžeme stotožniť s dvojicami reálnych čísel. Takisto vieme, že dvojiciam reálnych čísel vieme jednojednoznačne priradiť aj body v rovine. Čiže komplexné čísla môžeme chápať aj ako body v rovine. V tejto podkapitole uvidíme, že takáto interpretácia komplexných čísel poskytuje zaujímavú interpretáciu pre sčitovanie a násobenie komplexných čísel.



Obr. B.1: Znázornenie komplexného čísla v rovine

Keď stotožníme komplexné číslo s bodom v rovine, môžeme sa pozrieť na jeho vzdialenosť od počiatku súradnicovej sústavy a na uhol, ktorý zviera s osou x. Majme komplexné číslo $z = a + bi$, ktorému zodpovedá bod (a, b). Z Pytagorovej vety vieme vzdialenosť od počiatku určiť ako

$$r = \sqrt{a^2 + b^2}$$

a uhol medzi spojnicou bodov $(0, 0)$, (a, b) a osou x sa dá zistiť z rovností $\cos\varphi = \frac{a}{r}$ a $\sin\varphi = \frac{a}{r}$. Pre tieto hodnoty r a φ platí

$$a + bi = r(\cos\varphi + i\sin\varphi).$$

Definícia B.2.1. Zápis komplexného čísla v tvare

$$z = r(\cos\varphi + i\sin\varphi)$$

nazývame *goniometrický zápis* komplexného čísla. Číslo $r = \sqrt{a^2+b^2}$ nazývame *absolútna hodnota* alebo tiež *modul* komplexného čísla z a označujeme ho $|z|$. Číslo φ také, že $a = r\cos\varphi$ a $b = r\sin\varphi$ nazývame *argument* komplexného čísla z.

Príklad B.2.2. Pokúsme sa previesť do goniometrického tvaru číslo $z = 1-\sqrt{3}i$. Dostávame $r = |z| = \sqrt{1+3} = 2$. Z toho dostávame, že pre argument čísla z musí platiť

$$\cos\varphi = \frac{1}{2}$$
$$\sin\varphi = -\frac{\sqrt{3}}{2}$$

Riešeniami prvej rovnice sú práve uhly

$$\varphi = \pm\frac{\pi}{3} + 2k\pi$$

pre $k \in \mathbb{Z}$. Keď vezmeme do úvahy, že sínus má byť záporný, dostaneme

$$\varphi = -\frac{\pi}{3} + 2k\pi.$$

(Tým je uhol φ určený až na násobok 2π. Otočenie o uhol 2π okolo počiatku samozrejme bod v rovine nemení.)

Obrátene, ak máme daný goniometrický tvar komplexného čísla, ľahko ho prevedieme na algebraický tvar. Napríklad

$$\sqrt{2}.\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right) = \sqrt{2}\left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right) = 1+i.$$

Nasledujúca veta hovorí, že ak máme komplexné čísla zapísané v goniometrickom tvare, tak pri ich vynásobení sa vynásobia ich absolútne hodnoty a ich argumenty sa sčítajú.

Veta B.2.3 (Moivrova veta). *Nech* $z_1 = r_1(\cos\alpha + i\sin\alpha)$ *a* $z_2 = r_2(\cos\beta + i\sin\beta)$. *Potom pre ich súčin platí*

$$z_1z_2 = r_1r_2(\cos(\alpha+\beta) + i\sin(\alpha+\beta)). \tag{B.6}$$

Špeciálne z toho vyplýva, že pre absolútne hodnoty platí

$$|z_1z_2| = |z_1|.|z_2|. \tag{B.7}$$

Dôkaz. Overme najprv rovnosť (B.7). Označme $z_1 = a+bi$ a $z_2 = c+di$, teda $z_1z_2 = (ac-bd)+(ad+bc)i$. Upravujme najprv $|z_1z_2|$. Lepšie sa nám bude pracovať bez druhej odmocniny, preto tento výraz umocnime na druhú.

$$|z_1z_2|^2 = (ac-bd)^2+(ad+bc)^2 = (a^2c^2-2abcd+b^2d^2)+(a^2d^2+2abcd+b^2c^2) = (ac)^2+(bd)^2+(ad)^2+(bc)^2$$

Teraz sa pokúsime upraviť $|z_1|^2.|z_2|^2$

$$|z_1|^2.|z_2|^2 = (a^2+b^2)(c^2+d^2) = (ac)^2+(ad)^2+(bc)^2+(bd)^2$$

Vidíme, že v oboch prípadoch sme dostali rovnaký výsledok. Teda $|z_1 z_2|^2 = (|z_1|.|z_2|)^2$. Pretože ide o nezáporné čísla, môžeme túto rovnosť odmocniť a máme

$$|z_1 z_2| = |z_1|.|z_2|.$$

Súčin čísel $z_1 = r_1(\cos\alpha + i\sin\alpha)$ a $z_2 = r_2(\cos\beta + i\sin\beta)$ môžeme upraviť ako

$$z_1 z_2 = r_1 r_2(\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta) = r_1 r_2[(\cos\alpha\cos\beta - \sin\alpha\sin\beta) + i(\cos\alpha\sin\beta + \sin\alpha\cos\beta)].$$

Na základe goniometrických identít (známych zo strednej školy) vidíme, že

$$z_1 z_2 = r_1 r_2(\cos(\alpha+\beta) + i\sin(\alpha+\beta)).$$

Už vieme, že $|z_1 z_2| = r_1 r_2$. Teda číslo $z_1 z_2$ skutočne možno vyjadriť pomocou argumentu $\alpha + \beta$. □

Dôsledok B.2.4. *Ak $n \in \mathbb{N}$ a $z = r(\cos\alpha + i\sin\alpha)$, tak*

$$z^n = r^n\left(\cos(n\alpha) + i\sin(n\alpha)\right)$$

Tento vzťah medzi násobením komplexných čísel a sčitovaním uhlom umožňuje elegantné odvodenie mnohých trigonometrických identít.

Príklad B.2.5. Umocnením čísla $\cos\alpha + i\sin\alpha$ na n-tú pre $n \in \mathbb{N}$ dostaneme

$$(\cos\alpha + i\sin\alpha)^n = \cos(n\alpha) + i\sin(n\alpha) = \sum_{j=0}^{n}\binom{n}{j} i^{n-j}\cos^j\alpha\sin^{n-j}\alpha$$

Keď teraz použijeme (B.4) a rozdelíme súčet na pravej strane na reálnu a imaginárnu časť, vidíme, že

$$\cos nx = \cos^n x - \binom{n}{2}\cos^{n-2}x\sin^2 x + \binom{n}{4}\cos^{n-4}x\sin^4 x - \dots$$
$$\sin nx = n\cos^{n-1}x\sin x - \binom{n}{3}\cos^{n-3}x\sin^3 x + \binom{n}{5}\cos^{n-5}x\sin^5 x - \dots$$

B.3 Riešenie rovníc v komplexných číslach

Dôležitá vlastnosť komplexných čísel je vyjadrená v nasledujúcej vete:

Veta B.3.1 (Základná veta algebry). *Každý polynóm s komplexnými koeficientami má koreň v $\mathbb{C}$. T.j. ak*

$$f(x) = c_n x^n + \dots + c_1 x + c_0,$$

tak existuje $z \in \mathbb{C}$ také, že $f(z) = 0$.

Dokonca platí, že ak polynóm $f(x)$ je stupňa $n > 1$, tak počet koreňov vrátane násobnosti je práve n. (Ak $f(x) = (x-z)^k g(x)$ pre nejaký polynóm $g(x)$ a z nie je koreňom polynómu g, hovoríme, že *násobnosť* koreňa z je k. K polynómom a násobnosti koreňov sa ešte dostanete neskôr v rámci predmetu algebra.)

Nie všetky rovnice takéhoto tvaru však vieme jednoducho riešiť. Ukážeme si len dva typy rovníc, ktoré sa dajú riešiť vcelku ľahko. Najprv uvidíme, že pri kvadratických rovniciach s reálnymi koeficientmi môžeme postupovať podobne ako v reálnych číslach.

B.3.1 Kvadratické rovnice s reálnymi koeficientmi

Najprv si všimnime, že v komplexných číslach (na rozdiel od reálnych) vieme riešiť aj rovnicu $x^2 = r$, kde r je záporné reálne číslo.

Všimnime si, že každé záporné reálne číslo vieme zapísať v tvare $-a^2$ pre nejaké $a \in \mathbb{R}$. Teda vlastne riešime rovnicu

$$\begin{aligned} x^2 &= -a^2, \\ x^2 + a^2 &= 0, \\ (x - ia)(x + ia) &= 0, \end{aligned}$$

ktorej riešeniami sú práve $x = \pm ia$.

Predpokladajme teraz, že máme rovnicu tvaru

$$ax^2 + bx + c = 0,$$

kde $a, b, c \in \mathbb{R}$ a $a \neq 0$.

Zopakujeme presne ten istý postup, ktorým sa zvykne na strednej škole odvodzovať vzorec pre výpočet koreňov kvadratickej rovnice – použijeme doplnenie na štvorec.

$$\begin{aligned} ax^2 + bx + c &= 0 \\ a\left(x + \frac{b}{2a}\right)^2 + c - \frac{b^2}{4a} &= 0 \\ a\left(x + \frac{b}{2a}\right)^2 &= \frac{b^2 - 4ac}{4a} \\ \left(x + \frac{b}{2a}\right)^2 &= \frac{b^2 - 4ac}{4a^2} \end{aligned}$$

Označíme $D = b^2 - 4ac$. Ak $D > 0$, tak dostaneme

$$x_{1,2} = \frac{-b \pm \sqrt{D}}{2a}.$$

Ak $D = 0$, tak máme dvojnásobný koreň $x = -\frac{b}{2a}$. V prípade $D < 0$ máme rovnicu tvaru $z^2 = -(\sqrt{-D})^2$, pre $z = x + \frac{b}{2a}$, o ktorej už vieme, že jej riešeniami sú $z_{1,2} = \pm i\sqrt{-D}$. Z toho dostaneme

$$x_{1,2} = \frac{-b \pm i\sqrt{-D}}{2a}.$$

(Pretože $D < 0$, je $-D$ je kladné reálne číslo a výraz $\sqrt{-D}$ má zmysel.)

Príklad B.3.2. Riešme rovnicu $x^2 + 4x + 5 = 0$.

Dostaneme $D = 16 - 20 = -4$ a

$$x_{1,2} = \frac{-4 \pm 2i}{2} = -2 \pm i.$$

Mohli by sme rovnaký postup ako v odvodení vzorca pre korene kvadratickej rovnice použiť, keby boli koeficienty komplexné? V podstate áno – ale na mieste, kde sme použili odmocninu (inak povedané, riešili sme rovnicu $z^2 = \frac{D}{4a^2}$), zatiaľ nevieme, čo robiť v prípade, že D je komplexné číslo. Práve o niečom, čo sa dá nazvať „odmocninou“ z komplexného čísla, sa dozvieme o chvíľu.

B.3.2 Binomické rovnice

Rovnicu tvaru $x^2 = a$ vieme vyriešiť pre $a \in \mathbb{R}$ (či už kladné alebo záporné). Skúsme sa zamyslieť nad tým, čo by sa stalo, keby sme na pravej strane mali nejaké komplexné číslo.

Riešime teda rovnicu

$$x^n = z,$$

v obore komplexných čísel. Skúsme čísla vystupujúce v rovnici upraviť na goniometrický tvar. Nech teda $x = r(\cos\alpha + i\sin\alpha)$ a $z = |z|(\cos\varphi + i\sin\varphi)$. Potom dostaneme

$$r^n\left(\cos(n\alpha) + i\sin(n\alpha) = |z|(\cos\varphi + i\sin\varphi)\right).$$

Predchádzajúca rovnosť je splnená práve vtedy, keď $r^n = |z|$, čiže

$$r = \sqrt[n]{|z|}$$

a $n\alpha = \varphi + 2k\pi$ čiže

$$\alpha = \frac{\varphi}{n} + \frac{2k}{n}\pi,$$

pre $k = 0, \ldots, n-1$. (Ten istý bod znamená rovnakú vzdialenosť od počiatku, uhol sa môže líšiť o 2π, lebo otočenie o násobok 2π je identické zobrazenie. Stačí použiť k od 0 po $n-1$, lebo potom sa už body začnú opakovať – uhly sa budú líšiť o násobok $\frac{2n}{n}\pi = 2\pi$.)

Príklad B.3.3. Riešme rovnicu $x^4 = 1+i$. Najprv prevedieme pravú stranu na goniometrický tvar: $x^4 = \sqrt{2}(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4})$. Pre $x = r(\cos\varphi + i\sin\varphi)$ dostaneme

$$x^4 = r^4(\cos 4\varphi + i\sin 4\varphi),$$

čiže

$$r^4 = \sqrt{2} \qquad \Rightarrow \qquad r = \sqrt[8]{2}.$$

Pre uhol φ dostávame

$$4\varphi = \frac{\pi}{4} + 2k\pi \qquad \Rightarrow \qquad \varphi = \frac{\pi}{16} + k\frac{\pi}{2}.$$

Všetky riešenia danej rovnice sú teda $\sqrt[8]{2}\left(\cos(\frac{\pi}{16} + k\frac{\pi}{2}) + i\sin(\frac{\pi}{16} + k\frac{\pi}{2})\right)$ pre $k = 0, 1, 2, 3$.

Niekedy sa zvyknú všetky riešenia rovnice $x^n = z$ nazývať *n-tými odmocninami* komplexného čísla z. Môžeme si všimnúť, že vzorec

$$x = \frac{-b + \sqrt{D}}{2a}$$

bude platiť aj teraz ak symbol $\sqrt{D}$ chápeme v takom zmysle, že zaň možno dosadiť ktorúkoľvek z druhých odmocnín čísla D. (Teda ktorékoľvek komplexné čísla také, že $x^2 = D$.)

Príklad B.3.4. Vyriešme rovnicu $x^2 - (1+i)x - 2 - i = 0$.

Dostaneme $D = (1+i)^2 + 4(2+i) = 2i + 8 + 4i = 8 + 6i$. Diskriminant prevedieme na goniometrický tvar. Dostaneme

$$8 + 6i = 10(\cos\varphi + i\sin\varphi), \text{ kde } \cos\varphi = \frac{4}{5}, \sin\varphi = \frac{3}{5}.$$

Komplexné odmocniny z tohto čísla sú

$$u_{1,2} = \sqrt{10}\left(\cos\left(\frac{\varphi}{2} + k\pi\right) + i\sin\left(\frac{\varphi}{2} + k\pi\right)\right),$$

pre $k = 1, 2$. Pritom $|\cos\frac{\varphi}{2}| = \sqrt{\frac{1+\cos\varphi}{2}} = \sqrt{\frac{9}{10}} = \frac{3}{\sqrt{10}}$ a $|\sin\frac{\varphi}{2}| = \sqrt{\frac{1-\cos\varphi}{2}} = \sqrt{\frac{1}{10}} = \frac{1}{\sqrt{10}}$.

Z jednotkovej kružnice (na základe kvadrantu, v ktorom je φ) vieme určiť aj znamienko kosínu a sínu, čiže dostaneme

$$u_{1,2} = \pm(3 + i).$$

Z toho dostaneme riešenia kvadratickej rovnice ako

$$x_{1,2} = \frac{1 + i \pm (3 + i)}{2}$$
$$x_1 = 2 + i \qquad x_2 = -1$$

O správnosti riešenia sa môžeme presvedčiť dosadením alebo roznásobením $(x-2-i)(x+1) = x^2 - (1 + i)x - 2 - i$.

Spôsoby riešenia niektorých ďalších typov rovníc (kubické, bikvadratické, reciproké) nájdete napríklad v [KGGS, Kapitola 6].

B.4 Zopár ďalších vecí súvisiacich s komplexnými číslami

Spomenieme veľmi stručne niekoľko ďalších faktov o komplexných číslach.

Exponenciálny tvar komplexného čísla. Často sa stretnete so zápisom komplexného čísla v tvare

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

alebo

$$\cos\varphi + i\sin\varphi = i\varphi.$$

Bez toho, aby sme sa tým zaoberali hlbšie, tento zápis môžeme považovať jednoducho za skratku zápisu goniometrického zápisu. (Z Moivrovej vety vieme, že násobenie komplexných čísel s veľkosťou 1 funguje ako sčitovanie exponentov = sčitovanie uhlov.)

Kvaternióny. Podobným spôsobom ako komplexné čísla sa dajú vybudovať *kvaternióny.* V tomto prípade sa pridajú 3 nové prvky i, j, k, ktorých druhá mocnina je -1 a vhodne sa pre ne zadefinuje súčin. Kvaternióny tiež majú geometrický význam, ich násobenie súvisí s vektorovým súčinom. Na rozdiel od komplexných čísel však netvoria pole (násobenie nie je komutatívne.) Viac sa o nich môžete dočítať napríklad v [KGGS, Podkapitola 4.7].

Komplexné čísla sa nedajú usporiadať. Na reálnych číslach existuje relácia $\leq$, ktorí (okrem iných vlastností) spĺňa

(i) Ľubovoľné dve reálne čísla sú porovnateľné, teda platí aspoň 1 z možností $x \leq y$ a $y \leq x$.

(ii) $x \leq y \wedge y \leq x \Rightarrow x = y$.

(iii) $x \leq y \Rightarrow x + z \leq y + z$.

(iv) $0 \leq z \wedge x \leq y \Rightarrow xz \leq yz$.

Na komplexných číslach sa nedá zadefinovať relácia $\leq$, ktorá by mala podobné vlastnosti. Z uvedených vlastností totiž pre každé x vieme odvodiť $x^2 \geq 0$. (Ak $x \geq 0$, tak túto rovnosť vynásobíme číslom x, ak $x \leq 0$, tak vynásobením číslom $-x$ dostaneme $-x^2 \leq 0$, z čoho vyplýva $0 \leq x^2$.)

Dostaneme teda, že $i^2 = -1 \geq 0$ a po pripočítaní 1 máme $0 \geq 1$. Súčasne však $(-1)^2 = 1 \geq 0$, teda $0 = 1$, čo je spor.

Vlastnosti, ktoré sme uviedli, sú niektoré z vlastností usporiadaných polí. O usporiadaných poliach sa viac môžete dočítať napríklad v [ŠHHK]. S pojmom relácia usporiadania ste sa pravdepodobne už stretli.

Cvičenia

Úloha B.4.1. Vypočítajte

a) $(3+2i)+(2-i)$	b) $(1+i)+(1-i)$	c) $(1+3i)+(\sqrt{3}+i)$
d) $(3+2i).(2-i)$	e) $(1+i).(1-i)$	f) $(1+\sqrt{3}i).(\sqrt{3}+i)$
e) $(3+2i)-(2-i)$	f) $(1+i)-(1-i)$	g) $(1+3i)-(\sqrt{3}+i)$
h) $(3+2i)/(2-i)$	i) $(1+i)/(1-i)$	j) $(1+\sqrt{3}i)/(\sqrt{3}+i)$

Úloha B.4.2. Overte výpočtom, že pri oboch uzátvorkovaniach výrazu $(1+2i)(1-i)(2-i)$ dostaneme ten istý výsledok.

Úloha B.4.3. Overte, že pre sčitovanie a násobenie komplexných čísel platí distributívnosť.

Úloha B.4.4. Overte, že pre komplexné čísla platí trojuholníková nerovnosť $|z_1 + z_2| \leq |z_1| + |z_2|$. Čo predstavuje táto nerovnosť geometricky?

Úloha B.4.5. Vieme, že na reálnej osi predstavujú riešenia nerovnice $|x - a| < r$ interval $(a - r, a + r)$ (pre $a, r \in \mathbb{R}$ a $r > 0$). Aký geometrický útvar v komplexnej rovine tvoria komplexné čísla vyhovujúce podmienke:
a) $|z - z_0| < r$,
a) $|z - z_0| = r$,
a) $|z - z_0| \leq r$,
kde z_0 je dané komplexné číslo a r je dané kladné reálne číslo?

Úloha B.4.6*. Ak $z_1, z_2 \in \mathbb{C}$ a $r \in \mathbb{R}$, $r > 0$, aký geometrický útvar tvoria body zodpovedajúce komplexným číslam s vlastnosťou $|z - z_1| + |z - z_2| = r$? Načrtnite ho pre $z_1 = 0$ a $z_2 = 3 + 2i$.

Úloha B.4.7. Nájdite goniometrický tvar daných komplexných čísel:
a) $1 - i$; b) $\sqrt{3} + i$; c) $-i$; d) $2 + i$; e) $(1 + i)(1 - i)$

Úloha B.4.8. Vyriešte rovnice:
a) $x^2-4x+13 = 0$ b) $4x^2+4x+2 = 0$ c) $x^2-6x+13 = 0$ d) $x^2+2x+50 = 0$ e) $x^2+x+1 = 0$

Úloha B.4.9. Vyriešte rovnice:
a) $z^2 = \frac{1-3i}{1+3i} - \frac{1}{5} + \frac{3}{5}i$; b) $z^6 = i$; c) $\frac{z^4}{8} + i\sqrt{3} = -1$; d) $z^4 = 1 + i$

Úloha B.4.10. Vyriešte rovnice:
a) $x^2 - (1 + 2i)x - 3 + i = 0$ b)$x^2 - 2x + 1 - 2i = 0$ c) $x^2 - (4 + 3i)x + 1 + 5i = 0$ d) $x^2 - 3(1 + i)x + 5i = 0$ e) $x^2 + (1 + i)x - 4i = 0$

Úloha B.4.11. Riešte rovnice:
a) $z^3 - iz^2 + 4z - 4i = 0$ b) $x^4 + x^2 + 1 = 0$ c) $x^3 - (3 + 2i)x^2 + 2(1 + 3i)x - 4i = 0$ d) $x^3 - 2ix^2 - x + 2i = 0$

Úloha B.4.12. Riešte sústavy (môžete napr. použiť Gaussovu eliminačnú metódu, vyrátať inverznú maticu, použiť Cramerovo pravidlo):
$\left(\begin{array}{cc|c} 1+i & 1-i & 1 \\ 1 & -1 & i \end{array}\right)$ $\left(\begin{array}{cc|c} 1+i & -i & 0 \\ i & -1 & 1 \end{array}\right)$ $\left(\begin{array}{cc|c} i & 1 & 0 \\ 1 & 1-i & 2i \end{array}\right)$ $\left(\begin{array}{cc|c} -1+i & 2-i & 1+i \\ -1+2i & 3-2i & 1-i \end{array}\right)$

Úloha B.4.13. Nájdite všetky $x \in \mathbb{R}$, pre ktoré platí $\left(\frac{1+xi}{1-xi}\right)^6 = \frac{3+4i}{3-4i}$

Literatúra

[A] Sheldon Axler. *Linear Algebra Done Right.* Springer-Verlag, New York, 2nd edition, 1997.

[AA] Titu Andreescu and Dorin Andrica. *Complex Numbers from A to ...Z.* Birkhäuser, Boston, 2006.

[Bl] Rudolf Blaško. Matematická analýza. `http://frcatel.fri.utc.sk/~beerb`.

[Bó] Miklós Bóna. *Combinatorics of Permutations.* CRC, Boca Raton, 2004.

[BM] Garrett Birkhoff and Saunders MacLane. *Prehľad modernej algebry.* Alfa, Bratislava, 1979.

[BŠ] Bohuslav Balcar and Petr Štěpánek. *Teorie množin.* Academia, Praha, 2001.

[Č] Juraj Činčura. Elementárna teória čísel. Poznámky k prednáške, `http://thales.doa.fmph.uniba.sk/sleziak/cvicenia/tc/`.

[H] Jim Hefferon. Linear algebra. `http://joshua.smcvt.edu/linearalgebra/`.

[HS] T. Hecht and Z. Sklenáriková. *Metódy riešenia matematických úloh.* SPN, Bratislava, 1992.

[HZK] Milan Hejný, Valent Zaťko, and Pavel Kršňák. *Geometria 1.* SPN, Bratislava, 1985.

[I] Ján Ivan. *Matematika 1.* Alfa, Bratislava, 1983.

[K] Július Korbaš. *Lineárna algebra a geometria I.* UK, Bratislava, 2003.

[KGGS] Tibor Katriňák, Martin Gavalec, Eva Gedeonová, and Jaroslav Smítal. *Algebra a teoretická aritmetika 1.* UK, Bratislava, 2002.

[KMŠ] Igor Kluvánek, Ladislav Mišík, and Marko Švec. *Matematika I.* Alfa, Bratislava, 4th edition.

[L] Loren C. Larson. *Metódy riešenia matematických problémov.* ALFA, Bratislava, 1990.

[NS] A. Naylor and G. Sell. *Teória lineárnych operátorov v technických a prírodných vedách (Linear Operator Theory in Engineering and Science).* Alfa, Bratislava.

[O] Petr Olšák. Lineární algebra. `http://math.feld.cvut.cz/olsak/linal.html`.

[Sl] Jan Slovák. Lineární algebra. `http://www.math.muni.cz/~slovak/`.

[Sm] Jozef Smida. *Komplexné čísla, matematika pre 4. ročník gymnázií.* SPN, Bratislava, 1987.

[SGZ] Jaroslav Smítal, Eva Gedeonová, and Štefan Znám. *Úvod do lineárnej algebry.* UK, Bratislava, 1978. `http://cyril-244.fmph.uniba.sk/mffuk/studium/stud_materialy/stud_materi%aly/UVOD_LA/`.

[ŠHHK] T. Šalát, A. Haviar, T. Hecht, and T. Katriňák. *Algebra a teoretická aritmetika 2.* Alfa, Bratislava, 1986.

[ŠS] Tibor Šalát and Jaroslav Smítal. *Teória množín.* UK, Bratislava, 1995.

[Z1] Pavol Zlatoš. Lineárna algebra a geometria. `http://thales.doa.fmph.uniba.sk/zlatos/`.

[Z2] Pavol Zlatoš. *Ani matematika si nemôže byť istá sama sebou.* IRIS, Bratislava, 1995. `http://thales.doa.fmph.uniba.sk/zlatos/animat/animat.pdf`.

Register

aditívny zápis, 35
adjungovaná matica, 121
algebraický doplnok, 112
asociatívnosť, 29
asociatívnosť skladania zobrazení, 15

bijekcia, 15
binárna operácia, 26
báza, 62
    ortonormálna, 130

Cramerovo pravidlo, 123
cyklus, 22
    prázdny, 22
cykly
    disjunktné, 23

de Morganove pravidlá, 9
definičný obor, 13
definícia matematickou indukciou, 8
determinant, 110
diagonálna matica, 71
dimenzia, 63
direktný súčet, 68
disjunkcia, 9
distributívnosť, 38
dôkaz
    nepriamy, 6
    priamy, 6
    sporom, 6

ekvivalencia, 9
elementárna riadková operácia, 72
euklidovský vektorový priestor, 125

Gaussova eliminačná metóda, 98
generovanie vektorového priestoru, 55
Gram-Schmidtov ortogonalizačný proces, 130
grupa, 33
    abelovská, 34
    komutatívna, 34

hodnosť matice, 75

identické zobrazenie, 17
identita, 17
imaginárna jednotka, 136
implikácia, 9
    obmena, 10
indukcia
    matematická, 7
    úplná, 8
indukčný krok, 7
indukčný predpoklad, 7
injekcia, 15
inklúzia, 11
inverzia, 109
inverzná matica, 90
inverzný prvok, 30
inverzný prvok v poli, 38
izomorfimus vektorových priestorov, 90

jednotková matica, 71

komplexné číslo, 136
    algebraický zápis, 137
    goniometrický zápis, 140
    imaginárna časť, 137
    reálna časť, 137
    rýdzoimaginárne, 137
komutatívnosť, 28
konjunkcia, 9
Kritérium vektorového podpriestoru, 53
Kroneckerov symbol, 71

Laplaceov rozvoj, 115
lineárna kombinácia, 55
lineárne nezávislé vektory, 57
lineárne zobrazenie, 79
lineárne závislé vektory, 57
lineárny izomorfizmus, 90

lineárny obal, 55
lineárny súčet, 67

matica, 70
    elementárnej riadkovej operácie, 91
    regulárna, 90
    transponovaná, 71
    štvorcová, 71
matica lineárneho zobrazenia, 81
matica sústavy, 94
    rozšírená, 94
množina, 11
    prázdna, 11
množiny
    karteziánsky súčin, 13
    prienik, 12
    rozdiel, 12
    zjednotenie, 12
multiplikatívny zápis, 35

negácia, 9
nerovnosť
    Schwarzova, 127
    trojuholníková, 127
neutrálny prvok, 27
nulový vektor, 47

obor hodnôt, 13
obraz množiny, 19
opačný prvok, 38
opačný vektor, 47
ortogonálny doplnok, 129

permutácia, 20
    rozklad na súčin disjunktných cyklov, 23
permutácie
    disjunktné, 23
podmnožina, 11
podpriestor, 51
podpriestor prislúchajúci matici, 72
pole, 38
priamy súčet, 68
prvočíslo, 40

racionálne číslo, 4
redukovaná trojuholníková matica, 73
riadková ekvivalencia matíc, 72
rovnosť množín, 11
rovnosť zobrazení, 14
rozdiel vektorov, 47
rád permutácie, 24

Sarrusovo pravidlo, 110
skalár, 47
skalárny súčin, 125
skladanie zobrazení, 14
surjekcia, 15
sústava
    homogénna, 95
    riešiteľná, 94
sústava lineárnych rovníc, 94
súčet matíc, 70
súčin matíc, 85

triviálne riešenie homogénnej sústavy, 95

uhol vektorov, 128
usporiadaná dvojica, 13

vedúci prvok, 73
vektor, 47
vektorový priestor, 47
    konečnorozmerný, 62
vektory
    kolmé, 128
    ortogonálne, 128
    ortonormálne, 130
Vennove diagramy, 12
veta
    Frobeniova, 100
    malá Fermatova, 44, 46
    Steinitzova o výmene, 60
veľkosť vektora, 127
vzor množiny, 19

zložené číslo, 40
zobrazenie, 13
    bijektívne, 15
    injektívne, 15
    inverzné, 17
    na, 15
    prosté, 15
    surjektívne, 15
zákony o krátení, 34

štandardná báza F^n, 62

číslo
    komplexne združené, 139

Zoznam symbolov

$\mathbb{N}$	4
$\mathbb{Z}$	4
$\mathbb{Z}^+$	4
$\mathbb{Q}$	4
$\mathbb{R}$	4
$\mathbb{C}$	4
$\mathbb{R}^+$	4
$\mathbb{R}_0^+$	4
$\mathbb{R}^-$	4
$\mathbb{R}_0^-$	4
$\neg$	9
$\wedge$	9
$\vee$	9
$\Rightarrow$	9
$\Leftrightarrow$	9
$\in$	11
$\emptyset$	11
$\subseteq$	11
$A \cup B$	12
$A \cap B$	12
$A \setminus B$	12
$A \times B$	13
(a, b)	13
$f\colon X \to Y$	13
$f(x)$	13
$f = g$	14
$g \circ f$	14
id_X	17
f^{-1}	17
$f[A]$	19
$f^{-1}(B)$	19
$(a_1 a_2 \dots a_k)$	22
$()$	22
$a * b$	26
$\mathbb{Z}_5$	27
a^{-1}	31
0	38
1	38
$-a$	38
a^{-1}	38
$b - c$	38
$\mathbb{Z}_n$	40
$n \times a$	44
a^n	44
$\vec{0}$	47
$-\vec{\alpha}$	47
$\vec{\alpha} - \vec{\beta}$	47
$\mathbb{R}^n$	48
$\mathbb{R}^{\mathbb{R}}$	48
$f + g$	48
$c.f$	48
$[\vec{\alpha}_1, \vec{\alpha}_2, \dots, \vec{\alpha}_n]$	55
F^n	62
$\vec{\varepsilon}_i$	62
$d(V)$	63
$S + T$	67
$S \oplus T$	68
$\|\|a_{ij}\|\|$	70
$c.A$	70
I	71
I_n	71
δ_{ij}	71
A^T	71
V_A	72
$A \sim B$	72
$h(A)$	75
A_f	82
f_A	82
$A.B$	85
A^{-1}	90
S_n	109
$i(\varphi)$	109
A_{ij}	112
M_{ij}	113
$\operatorname{adj} A$	121
$\langle \vec{\alpha}, \vec{\beta} \rangle$	125
$\|\vec{\alpha}\|$	127
$M^\perp$	129
i	136
$\mathbb{C}$	137
$\operatorname{Re} z$	137
$\operatorname{Im} z$	137
$\overline{z}$	139
$\|z\|$	140