Lineárna algebra 2
doc. Michal Zajac

1 Polia

Definícia. Poľom nazývame neprázdnu množinu K, ktorá obsahuje dva (osobitné) prvky $0, 1 \in K$ a na K sú definované operácie
$+\colon K \times K \to K$ (sčítanie), $\cdot : K \times K \to K$ (násobenie) také, že pre $\forall\, a, b, c \in K$ platí:

1. $a + b = b + a$ (komutatívnosť sčítania)
2. $(a + b) + c = a + (b + c)$ (asociatívnosť sčítania)
3. $a + 0 = a$ (0 je neutrálny prvok vzhľadom na sčítanie)
4. $\forall a \in K\, \exists d \in K\colon a + d = 0$ ($d = -a$, opačný prvok vzhľadom na sčítanie)
5. $a \cdot b = b \cdot a$ (komutatívnosť násobenia)
6. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (asociatívnosť násobenia)
7. $a \cdot (b + c) = a \cdot b + a \cdot c$ (distributívnosť)
8. $1 \cdot a = a$
9. $\forall a \neq 0 \exists d \in K\colon a \cdot d = 1$ ($d = a^{-1}$ je inverzný prvok k prvku a)
10. $0 \neq 1$

Ľahko sa dá overiť, že množina všetkých racionálnych čísel Q aj množina všetkých reálnych čísel R tvorí spolu s obvyklým sčítaním a násobením pole.

Úloha. Ukážte, že poľom $K = \{a + b\sqrt{2} : a, b \in Q\}$ (s obvyklými $+$, $\cdot$) je pole.

K je pole skonštruované tak, že k poľu Q pridáme ešte číslo $\sqrt{2}$ a všetky výsledky násobení a sčítaní racionálnych čísel a $\sqrt{2}$. Číslo $\sqrt{2}$ je riešenie rovnice $x^2 - 2 = 0$. Inými slovami rozšírime pole všetkých racionálnych čísel na pole v ktorom má polynóm $x^2 - 2$ koreň.

2 Vlastnosti komplexných čísel

Vieme, že neexistuje $x \in R$, pre ktoré by $x^2 = -1$. Tento „nedostatok” reálnych čísel odstránili matematici tak, že si také číslo vymysleli. Volá sa imaginárna jednotka a označovať ho budeme písmenom i (v elektrotechnických aplikáciách je zaužívané aj označenie j). Najprv pripomenieme definíciu z predmetu LA1:

Definícia. Nech $x, y \in R$. Výraz tvaru iy sa nazýva *imaginárne číslo*,
výraz tvaru $x+iy$ sa nazýva *komplexné číslo* (*algebraický tvar* komplexného čísla). Množinu všetkých komplexných čísel budeme označovať C.

V množine všetkých komplexných čísel sú operácie sčítania a násobenia určené vzťahom $i^2 = -1$ a vlastnosťami (i)–(ix). Teda ak $a, b, a_1, b_1, a_2, b_2 \in R$, tak

$$
\begin{aligned}
a + ib = 0 &\iff a = b = 0 \\
(a_1 + ib_1) + (a_2 + ib_2) &= (a_1 + a_2) + i(b_1 + b_2) \\
(a_1 + ib_1)(a_2 + ib_2) &= (a_1a_2 - b_1b_2) + i(a_1b_2 + b_1a_2) \\
-(a + ib) &= (-a) + i(-b) \\
(a + ib)(a - ib) &= a^2 + b^2 \in R \\
\text{ak } a + ib \neq 0 \text{ tak } \frac{1}{a + ib} &= \frac{1}{a + ib}\,\frac{a - ib}{a - ib} = \frac{a}{a^2 + b^2} + i\frac{-b}{a^2 + b^2}
\end{aligned}
$$

Predchádzajúce vzťahy sa ľahko overia priamym výpočtom, napr.:

$$
(a_1 + ib_1)(a_2 + ib_2) = a_1(a_2 + ib_2) + ib_1(a_2 + ib_2) = a_1a_2 + ia_1b_2 + ib_1a_2 + i^2b_1b_2 = \\
(a_1a_2 - b_1b_2) + i(a_1b_2 + b_1a_2)
$$

Ukázali sme, že sčítaním, násobením a delením dvoch komplexných čísel dostaneme znova komplexné číslo (t.j. výraz tvaru $x + iy$, kde $x, y \in R$ a tieto operácie sme definovali tak, že aj komplexné čísla spĺňajú vlastnosti (i)–(ix) reálnych čísel.

Definícia. Nech $x, y \in R$, $z = x + iy \in C$. Potom sa x nazýva *reálna časť* a y *imaginárna časť* komplexného čísla z, označujeme: $x = \operatorname{Re} z$, $y = \operatorname{Im} z$, číslo $\overline{z} = x - iy$ sa nazýva číslo *komplexne združené* s číslom z.

Priamym výpočtom sa dá overiť, že platí

Veta. *Nech $z, z_1, z_2 \in C$. Potom platí*
(i) $\overline{\overline{z}} = z$,
(ii) $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$,
(iii) $\overline{z_1 z_2} = \overline{z}_1 \overline{z}_2$,
(iv) $\operatorname{Re} z = \frac{1}{2}(z + \overline{z})$, $\operatorname{Im} z = \frac{1}{2i}(z - \overline{z})$.

Príklad. Vypočítajte (t.j. napíšte v tvare $x + iy$, $x \in R, y \in R$) čísla
a) i^{23} b) $\frac{1}{i}$ c) $\frac{2+3i}{i}$
d) $\frac{1+i}{2-i}$ e) $\frac{(2-i)^2}{1+i}$ f) $(1-i)^6$

Riešenie. a) Všimnime si, že $i^2 = -1$, $i^3 = -i$, $i^4 = 1$, potom dostaneme $i^{23} = i^{5\cdot 4+3} = (i^4)^5 i^3 = 1^5(-i) = -i$,
b) $\frac{1}{i} = \frac{1}{i}\frac{-i}{-i} = \frac{-i}{1} = -i$,
c) $\frac{2+3i}{i} = \frac{1}{i}(2+3i) = -i(2+3i) = -2i - 3i^2 = 3 - 2i$,
d) $\frac{1+i}{2-i} = \frac{1+i}{2-i}\frac{2+i}{2+i} = \frac{(1+i)(2+i)}{4+1} = \frac{2+i+2i+i^2}{5} = \frac{1}{5} + i\frac{3}{5}$,
e) $\frac{(2-i)^2}{1+i} = \frac{4-4i+i^2}{1+i} = \frac{(3-4i)(1-i)}{(1+i)(1-i)} = \frac{3-3i-4i+4i^2}{2} = -\frac{1}{2} - i\frac{7}{2}$
f) $(1-i)^6 = ((1-i)^2)^3 = (1 - 2i + i^2)^3 = (-2i)^3 = (-2)^3 i^3 = -8(-i) = 8i$.

Geometrická interpretácia komplexných čísel.

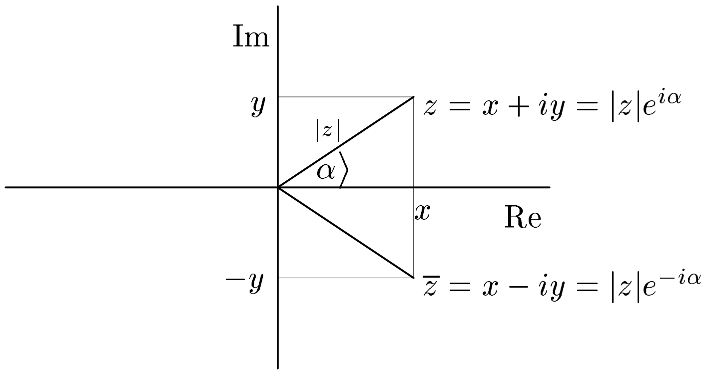
Komplexné číslo je určené usporiadanou dvojicou reálnych čísel. Teda k $z \in C$ môžeme priradiť dvojicu reálnych čísel ($x = \operatorname{Re} z, y = \operatorname{Im} z$) a tej zasa bod v rovine. Je tým tiež určený vektor v rovine, ktorého počiatočný bod je $(0, 0)$ a koncový bod je (x, y).

Komplexné číslo $z = x + iy$ stotožníme s týmto vektorom. Pritom aj obvyklé sčítanie vektorov v rovine zodpovedá sčítaniu komplexných čísel. Používame pravouhlé súradnice v rovine, ale na zdôraznenie, že v nej kreslíme komplexné čísla budeme os x nazývať reálna os a os y imaginárna os.

Dĺžka tohoto vektora sa nazýva absolútna hodnota komplexného čísla z. Ak je $z \neq 0$ je tento vektor jednoznačne určený svojou dĺžkou a orientovaným uhlom, ktorého počiatočným ramenom je vektor $(1, 0)$ (teda kladná časť reálnej osi) a koncovým ramenom je vektor $z = (x, y)$. Pripomeňme, že orientácia uhla je kladná ak sa jeho počiatočné rameno dostane do koncového ramena otáčaním okolo vrchola proti smeru hodinových ručičiek. Veľkosť orientovaného uhla $\varphi > 0$ budeme určovať v oblúkovej miere, radiánoch, teda je určená dĺžkou cesty, ktorú prejde koncový bod vektora dĺžky 1 pri otáčaní o uhol φ proti smeru hodinových ručičiek, záporné uhly rovnako zodpovedajú otáčaniu v smere hodinových ručičiek.

Tabuľka hodnôt $\cos\alpha$ a $\sin\alpha$

stupne	α	360	180	90	60	45	30
radiány	$\frac{2\pi}{360}\alpha$	2π	π	$\frac{\pi}{2}$	$\frac{\pi}{3}$	$\frac{\pi}{4}$	$\frac{\pi}{6}$
cos	$\cos\alpha$	1	-1	0	$\frac{1}{2}$	$\frac{1}{2}\sqrt{2}$	$\frac{1}{2}\sqrt{3}$
sin	$\sin\alpha$	0	0	1	$\frac{1}{2}\sqrt{3}$	$\frac{1}{2}\sqrt{2}$	$\frac{1}{2}$



Obr. 1 Geometrická interpretácia komplexného čísla.

Definícia. Nech $z = x + iy \in C$, $x, y \in R$.

(i) Nezáporné číslo $|z| = \sqrt{x^2 + y^2}$ sa nazýva *absolútna hodnota* komplexného čísla z,

(ii) Ak je navyše $z \neq 0$, tak orientovaný uhol φ, pre ktorý $z = |z|(\cos\varphi + i\sin\varphi)$, nazývame *argument* komplexného čísla z.

(iii) $z = |z|(\cos\varphi + i\sin\varphi)$ sa nazýva *goniometrický tvar* komplexného čísla z.

Poznamenajme, že ak φ je argument čísla z, tak je $\varphi + 2k\pi$ pre $\forall k \in Z$ tiež argumentom čísla z. Vyjadrenie čísla z v goniometrickom tvare je vlastne len preformulovaním definície funkcie $\sin\varphi$ a $\cos\varphi$ pre orientované uhly. Goniometrický tvar komplexného čísla sa skrátene zapisuje v exponenciálnom tvare:

$$z = |z|(\cos\varphi + i\sin\varphi) = |z|e^{i\varphi}, \quad \text{kde číslo } e \text{ je základ prirodzeného logaritmu.}$$

Oprávnenosť tohoto zápisu je vidieť z geometrickej interpretácie násobenia komplexných čísel:

Veta 2. *Ak $\alpha, \beta \in R$, tak*

$$(\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta) = \cos(\alpha + \beta) + i\sin(\alpha + \beta)\,.$$

Toto tvrdenie sa dá dokázať pomocou geometrických úvah a je ekvivalentné so súčtovými vzorcami známymi zo strednej školy (overte si to):

$$\sin(\alpha + \beta) = \sin\alpha\cos\beta + \cos\alpha\sin\beta\,, \qquad \sin(\alpha - \beta) = \sin\alpha\cos\beta - \cos\alpha\sin\beta\,,$$
$$\cos(\alpha + \beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta\,, \qquad \cos(\alpha - \beta) = \cos\alpha\cos\beta + \sin\alpha\sin\beta\,.$$

Geometrická interpretácia vety 2 hovorí: pri násobení komplexných čísel sa ich argumenty sčítajú. Absolútne hodnoty sa násobia, čo je jedným z tvrdení nasledujúcej vety:

Veta 3. *Pre $\forall z, w \in C$ platí:*

(i) $|z + w| \leq |z| + |w|$ *(trojuholníková nerovnosť)*

(ii) $|zw| = |z||w|$.

Obe tvrdenia sa dajú ľahko overiť výpočtom. Ak nie sú vektory z, w rovnobežné, tak je vektor $z + w$ uhlopriečka vo vhodnom rovnobežníku (nakreslite ho) nerovnosť (i) je známe tvrdenie, že strana trojuholníka je kratšia ako súčet dĺžok zvyšných dvoch strán.

Veta dva má nasledujúci dôsledok, ktorý je známy ako

Moivreova veta. *Ak $r, \phi \in R$, $r > 0$, $n \in N$, tak*

$$[r(\cos\varphi + i\sin\varphi)]^n = r^n[\cos(n\varphi) + i\sin(n\varphi)]\,,\ \textit{v exponenciálnom tvare}\ (re^{i\varphi})^n = r^n e^{in\varphi}.$$

Moivreova veta sa používa na riešenie rovnice

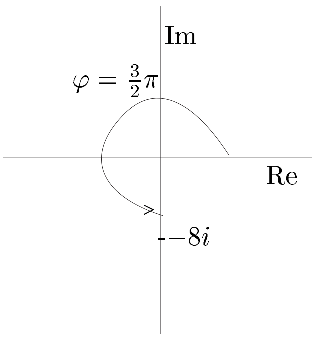
$$z^n = c\,,$$

kde $c \neq 0$ je známe komplexné číslo, $n \in N$ a neznáma z sa hľadá v množine C. Popíšeme teraz ako sa binomická rovnica rieši:

1. pravú stranu vyjadríme v goniometrickom tvare a riešime rovnicu
$$z^n = |c|(\cos\varphi + i\sin\varphi) = |c|[\cos(\varphi + 2k\pi) + i\sin(\varphi + 2k\pi)]\,, \quad k \in Z\,.$$
2. Neznámu z budeme hľadať v goniometrickom tvare, teda hľadáme kladné číslo r a uhol $\alpha \in R$, tak aby $z = r(\cos\alpha + i\sin\alpha)$ bolo riešenie rovnice $z^n = c$, t.j.
$$r^n[\cos(n\alpha) + i\sin(n\alpha) = |c|[\cos(\varphi + 2k\pi) + i\sin(\varphi + 2k\pi)]\,, \quad k \in Z\,.$$
3. Vidieť, že predchádzajúca rovnosť platí pre $r = \sqrt[n]{|c|}$ a $\alpha = \frac{\varphi+2k\pi}{n} = \frac{\varphi}{n} + k\frac{2\pi}{n}$, $k \in Z$ a teda
$$z_k = \sqrt[n]{|c|}\Big[\cos\big(\frac{\varphi}{n} + k\frac{2\pi}{n}\big) + i\sin\big(\frac{\varphi}{n} + k\frac{2\pi}{n}\big)\Big] = \sqrt[n]{|c|}e^{i(\frac{\varphi}{n} + k\frac{2\pi}{n})}\,, \quad k = 0, 1, 2, \ldots, n-1$$
je n rôznych riešení danej binomickej rovnice. Z predmetu LA1 vieme, že polynóm (stupňa n) $z_n - c$ má najviac n koreňov, teda viac riešení rovnica nemá. Stručne to môžeme zapísať:
$$z^n = |c|e^{i\varphi} \iff z_k = \sqrt[n]{|c|}e^{i(\frac{\varphi}{n} + k\frac{2\pi}{n})}\,, \quad k = 0, 1, 2, \ldots, n-1\,.$$

Poznamenajme ešte, že riešenia binomickej rovnice ležia na kružnici so stredom v bode 0 a polomerom $\sqrt[n]{|c|}$ a tvoria vrcholy pravidelného n-uholníka.

Príklad. Riešte rovnicu $z^3 = -8i$ a výsledok napíšte v algebraickom tvare a znázornite.

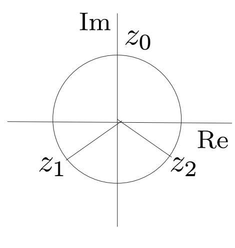


Najprv pravú stranu znázorníme a z obrázku určíme absolútnu hodnotu $|-8i| = 8$ a argument $\varphi = \frac{3}{2}\pi$ a teda riešime rovnicu

$$z^3 = 8\Big[\cos\Big(\frac{3}{2}\pi + 2k\pi\Big) + i\sin\Big(\frac{3}{2}\pi + 2k\pi\Big)\Big]$$

Odmocnením absolútnej hodnoty a delením argumentu dostaneme riešenie:

$$z_k = 2\big[\cos\tfrac{1}{3}\big(\tfrac{3}{2}\pi + 2k\pi\big) + i\sin\tfrac{1}{3}\big(\tfrac{3}{2}\pi + 2k\pi\big)\big]\,, k = 0, 1, 2$$
$$z_0 = 2\big[\cos\tfrac{1}{2}\pi + i\sin\tfrac{1}{2}\pi\big] = 2i$$
$$z_1 = 2\big[\cos\big(\tfrac{\pi}{2} + \tfrac{2\pi}{3}\big) + i\sin\big(\tfrac{\pi}{2} + \tfrac{2\pi}{3}\big)\big] = 2\big[\cos\tfrac{7}{6}\pi + i\sin\tfrac{7}{6}\pi\big] = -\sqrt{3} - i$$
$$z_2 = 2\big[\cos\big(\tfrac{\pi}{2} + \tfrac{4\pi}{3}\big) + i\sin\big(\tfrac{\pi}{2} + \tfrac{4\pi}{3}\big)\big] = 2\big[\cos\tfrac{11}{6}\pi + i\sin\tfrac{11}{6}\pi\big] = \sqrt{3} - i$$



Úlohy.

1. Nájdite výsledok operácie v tvare $x + yi$, kde $x, y \in R$.
   a. $3 + 7i - (5 - 2i)(4 - i)$
   b. $i(1 + i)(1 - i)(1 + 2i)(1 - 2i)$
   c. $\frac{(1-7i)}{(2+3i)}$
   d. $\frac{a+bi}{a-bi}$, $a, b \in R$
   e. $\frac{i(2+3i)}{3+5i}$
2. Nájdite všetky $x, y \in R$ také, že
   a. $(2x + 3y) + i(x - y) = -1 + 2i$
   b. $(ix + y)(2x - 3iy) = 2i$
   c. $\dfrac{-y + ix}{1 - 2i} + \dfrac{x + iy}{2 + 3i} = 1$
3. Dané komplexné číslo znázornite a nájdite jeho goniometrický tvar.
   a. -5 b. $1 - i$ c. $\sqrt{3} - i$ d. $-5i$ e. $2 + 3i$ f. $-3 - 7i$
4. Vypočítajte zu, $\frac{z}{u}$, z^n.
   a. $z = \sqrt{3}(\cos \frac{7\pi}{5} + i \sin \frac{7\pi}{5})$, $u = 2(\cos \frac{\pi}{3} + i \sin \frac{\pi}{3})$, $n = 5$
   b. $z = 3(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4})$, $u = 6(\cos \frac{3\pi}{8} + i \sin \frac{3\pi}{8})$, $n = 2004$
5. V obore komplexných čísel riešte rovnicu. Výsledok vyjadrite v algebraickom aj goniometrickom tvare a znázornite.
   a. $z^4 = 4$
   b. $z^4 = -4$
   c. $z^3 = -8i$
   d. $z^4 = -1 - i\sqrt{3}$
6. Vypočítajte.
   a. i^{101} b. $(1 + i)^4$ c. $\left(\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right)^8$

3 Polia Z_p

Celé čísla majú nasledujúcu vlastnosť (delenie so zvyškom):

Ak $n \in Z$, $m \in N$, tak $\exists!\, a \in Z$, $r \in \{0, 1, \ldots, m - 1\}$, pre ktoré $n = am + r$. Teda celé čísla sa dajú rozdeliť na m podmnožín, podľa toho aký je zvyšok po delení číslom m (zvyškové triedy):

Definícia. Hovoríme, že čísla $a, b \in Z$ sú kongruentné modulo m ($a \equiv b \pmod{m}$), ak dostaneme po ich delení číslom m rovnaký zvyšok, t.j

$$a \equiv b \pmod{m}, \text{ vtedy a len vtedy, keď je } m \text{ deliteľom čísla } a-b \text{ (označenie: } m|(a-b)).$$

Úlohy.

1. Zistite, či platí $14 \equiv 131 \pmod 3$
2. Nájdite $a \in \{0, 1, 2, 3, 4)$, pre ktoré $28 \equiv a \pmod 5$
3. Nájdite $a \in \{0, 1, 2, 3, 4, 6)$, pre ktoré $2a \equiv 1 \pmod 6$.

Relácia $k_1 \equiv k_2 \pmod m$ má nasledujúce vlastnosti:

1. reflexívnosť: $k \equiv k \pmod m$, $\forall\, k \in Z$,
2. symetria: $k_1 \equiv k_2 \pmod m \iff k_2 \equiv k_1 \pmod m$
3. tranzitívnosť: $\left.\begin{array}{l} k_1 \equiv k_2 \pmod m \\ k_2 \equiv k_3 \pmod m \end{array}\right\} \implies k_1 \equiv k_3 \pmod m$,
4. Pre všetky $k_1, k_2; \ell_1, \ell_2 \in Z$:
   $$\left.\begin{array}{l} k_1 \equiv k_2 \pmod m \\ \ell_1 \equiv \ell_2 \pmod m \end{array}\right\} \implies \begin{array}{c} k_1 + \ell_1 \equiv k_2 + \ell_2 \pmod m, \\ k_1\ell_1 \equiv k_2\ell_2 \pmod m. \end{array}$$

Tieto vlastnosti sa dajú ľahko dokázať, tu ukážem len poslednú:

$$\left.\begin{array}{c} k_1\ell_1 - k_2\ell_2 = k_1\ell_1 - k_2\ell_1 + k_2\ell_1 - k_2\ell_2 \\ = (k_1 - k_2)\ell_1 + k_2(\ell_1 - \ell_2) \\ k_1 \equiv k_2 \pmod m \\ \ell_1 \equiv \ell_2 \pmod m \end{array}\right\} \implies m|k_1\ell_1 - k_2\ell_2 \implies k_1\ell_1 \equiv k_2\ell_2 \pmod m.$$

Tieto vlastnosti teraz použijeme na definovanie operácií sčítania a násobenia v množine $Z_n = \{0, 1, 2, \dots, n-1\}$:

$$\begin{aligned} \forall\, a, b \in Z_n, \quad & a \oplus b = c \iff c \in Z_n \wedge a + b \equiv c \pmod{n}, \\ & a \odot b = d \iff d \in Z_n \wedge ab \equiv d \pmod{n}. \end{aligned}$$

Úloha. Dokážte, že pre každé $n \in N$ operácie $\oplus$, $\odot$ spĺňajú axiómy 1–8 z definície poľa.

Najväčší spoločný deliteľ $\gcd(n_0, n_1)$ dvoch celých čísel n_0, n_1 je prirodzené číslo, pre ktoré

1. $\gcd(n_0, n_1) | n_0 \wedge \gcd(n_0, n_1) | n_1$,
2. Ak $d \in N$, $d | n_0 \wedge d | n_1 \implies d | \gcd(n_0, n_1)$.

Popíšeme teraz algoritmus, ktorým sa dá najväčší spoločný deliteľ vypočítať a navyše aj vyjadriť pomocou čísel n_0, n_1.

Veta Euklidov algoritmus. *Nech n_0, n_1 sú prirodzené čísla. Potom existujú celé čísla a_0, a_1, pre ktoré*

$$\gcd(n_0, n_1) = a_0 n_0 + a_1 n_1$$

Dôkaz. Ak $n_0 = n_1$, tak $\gcd(n_0, n_1) = n_1 = 1 \cdot n_0 + 0 \cdot n_1$, t.j. $a_0 = 1$, $a_1 = 0$. Ďalším triviálnym príkladom je $n_1 = 1 = \gcd(n_0, n_1) = 0 \cdot n_0 + 1 \cdot n_1$.

Pretože $\gcd(n_0, n_1) = \gcd(n_1, n_0)$, vetu treba eešte dokázať v prípade $n_0 > n_1 > 1$. Potom delením $n_0 : n_1$ dostaneme (q je podiel a n_2 je zvyšok po delení)

$$n_0 = q n_1 + n_2\,, \quad n_2 < n_1\,, \quad q = \left\lfloor \frac{n_0}{n_1} \right\rfloor \quad \text{(celá časť podielu } n_0/n_1\text{)}$$

Ak $d | n_0 \wedge d | n_1$, tak je d aj deliteľom čísla $n_2 = n_0 - q n_1$ a zrejme platí aj opačná implikácia, t.j.

$$\big((d|n_0 \wedge d|n_1) \iff (d|n_1 \wedge d|n_2)\big) \implies \gcd(n_0, n_1) = \gcd(n_1, n_2)\,.$$

Tento postup zopakujeme ($n_1 : n_2$) a dostaneme $n_1 > n_2 > n_3 > n_4 \dots$. Je zrejmé, že musíme skončiť po konečnom počte krokov, t.j. keď bude $n_k = 0$, vtedy je $n_{k-1} = \gcd(n_0, n_1)$.

Ako získame čísla a_0 a a_1 ukážeme na konkrétnom príklade $n_0 = 123$, $n_1 = 57$.

$$\begin{array}{llll} n_0 : n_1 = 2\,,\ \text{zv. } n_2 = 9 & & n_0 = 2n_1 + n_2 & n_2 = n_0 - 2n_1 \\ n_1 : n_2 = 6\,,\ \text{zv. } n_3 = 3 & & n_1 = 6n_2 + n_3 & n_3 = n_1 - 6n_2 \\ n_2 : n_3 = 3\,,\ \text{zv. } n_4 = 0 & \implies & \gcd(n_1, n_2) = n_3 & \end{array}$$

A teraz dosadzujeme spätne:
$n_3 = n_1 - 6n_2 = n_1 - 6(n_0 - 2n_1) = n_1 - 6n_0 + 12n_1 = 13n_1 - 6n_0$, t.j. $a_0 = -6$, $a_1 = 13$.

Z predchádzajúceho dôkazu vidieť, že každý (nielen posledný nenulový) zvyšok n_k po delení $n_{k-2} : n_{k-1}$ sa dá napísať v tvare $n_k = s_k n_0 + t_k n_1$, kde $s_k, t_k \in \mathbb{Z}$. Pritom na výpočet s_k, t_k (pre $k \geq 3$) potrebujeme poznať dva predchádzajúce výsledky. Delením (so zvyškom) dostaneme $n_{k-2} = q n_{k-1} + n_k$, t.j. $n_k = n_{k-2} - q n_{k-1}$ (inými slovami $q = \lfloor n_{k-2}/n_{k-1} \rfloor$, t.j dolná celá časť podielu n_{k-2}/n_{k-1})

$$\begin{aligned} & \left.\begin{aligned} n_{k-2} &= s_{k-2} n_1 + t_{k-2} n_2 \\ n_{k-1} &= s_{k-1} n_1 + t_{k-1} n_2 \end{aligned}\right. \implies \\ & n_k = n_{k-2} - q n_{k-1} = s_{k-2} n_1 + t_{k-2} n_2 - q(s_{k-1} n_1 + t_{k-1} n_2) \\ & \quad = \underbrace{(s_{k-2} - q s_{k-1})}_{s_k} n_1 + \underbrace{(t_{k-2} - q t_{k-1})}_{t_k} n_2 \end{aligned} \tag{1}$$

Dostanme tak algoritmus (rozšírený Euklidov algoritmus):

1. Vstup a prvý krok
   $n_0,\ s_0 = 1,\ t_0 = 0$
   $n_1,\ s_1 = 0,\ t_1 = 1,\ q = \lfloor n_0/n_1 \rfloor,\ n_2 = n_0 - qn_1$
   $s_2 = 1 = s_0 - qs_1,\ t_2 = -q = t_0 - qt_1$
2. Pre $k > 2$ vypočítame čísla $n_k,\ s_k,\ t_k$ pomocou vzťahu (1)

Algoritmus končí, keď $n_{k+1} = 0$ a výsledkom je posledný nenulový zvyšok n_k a koeficienty s_k, t_k, $n_k = s_k n_0 + t_k n_1$.

Môžeme to zapisovať do tabuľky:

Prvý riadok tabuľky je ($q = \lfloor n_0/n_1 \rfloor$):

n_0	n_1	q	1	0	0	1

Ďalšie riadky dostaneme vždy z predchádzajúceho riadku:

a	b	q	a_0	b_0	a_1	b_1

znamená $a = a_0 n_0 + a_1 n_1$, $b = b_0 n_0 + b_1 n_1$, $q = \lfloor a/b \rfloor$ a ďalší riadok bude

a	b	q	a_0	b_0	a_1	b_1
b	$a - qb$		b_0	$a_0 - qb_0$	b_1	$a_1 - qb_1$

Napríklad pre $n_0 = 34, n_1 = 12$ potrebujeme 3 riadky ($n_3 | n_2 \implies n_3 = \gcd(n_0, n_1)$):

k	$a = n_k$	$b = n_{k+1}$	q	a_0	b_0	a_1	b_1
0	34	12	2	1	0	0	1
1	12	10	1	0	1	1	−2
2	10	$\boxed{2}$	5	1	−1	−2	3

$$\gcd(n_0, n_1) = \gcd(34, 12) = n_3 = -1n_0 + 3n_1 = 2 = (-1) \cdot 34 + 3 \cdot 12$$

Veta. *Z_p je pole vtedy a len vtedy, keď je p prvočíslo.*

Dôkaz. Ak p nie je prvočíslo, tak $p = m \cdot n$, $m \neq 1, n \neq 1$. Potom pre $a = m \cdot 1 = \underbrace{1 \oplus 1 \oplus \cdots \oplus 1}_{m \text{ krát}}$, $b = n \cdot 1$ platí $a \odot b \equiv 0 \pmod p$, ale $a \not\equiv 0 \pmod p$ aj $b \not\equiv 0 \pmod p$. Preto Z_p nie je pole.

Ak p je prvočíslo a $n \not\equiv 0 \pmod p$, t.j. $n \in \{1, 2, \ldots, p-1\}$, tak treba ukázať, že existuje k n inverzný prvok vzhľadom na násobenie v Z_p. Ostatné axiomy poľa platia pre každé p. Použijeme Euklidov algoritmus: Pretože je p prvočíslo, $\gcd(n, p) = 1$. Podľa predchádzajúcej vety

$$\exists\, a_0, a_1 \text{ také, že } 1 = a_0 p + a_1 n \implies$$
$$1 \equiv a_0 \underbrace{p \pmod p}_{\equiv 0} \oplus a_1 n \equiv a_1 n \pmod p \implies a_1 \equiv n^{-1} \pmod p\,.$$

V ďalšom texte budeme písať $a = b$, alebo $a = b \pmod p$ namiesto $a \equiv b \pmod p$.

4. Vlastnosti polynómov s komplexnými koeficientami a s koeficientami v poliach Z_p

Polynómy s reálnymi alebo komplexnými koeficientami sa dajú chápať ako funkcie $R \to R$ ($C \to C$) špeciálneho tvaru $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, $a_n \neq 0$. Číslo n sa potom nazýva stupeň polynómu $f(x)$. Pritom ak majú dva polynómy rôzne koeficienty, tak určujú aj rôzne funkcie. Vo všetkých poliach to ale neplatí. Napr. $f(x) = x^2 + x + 1$ a $g(x) = 1$ určujú tú istú funkciu $Z_2 \to Z_2$, $f(0) = g(0) = 1$, $f(1) = g(1) = 1$.

Nech K je pole. Polynómom s koeficientami z poľa K (nad K) nazývame výraz $f(x)$ tvaru

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n\,, a_n \neq 0\,.\ n \text{ sa nazýva stupeň polynómu } f\,.$$

$\deg f(x)$ bude označovať stupeň polynómu f. Množinu všetkých polynómov nad K označíme $P(K)$. Polynóm, ktorého všetky koeficienty sa rovnajú 0 sa nazýva nulový a má stupeň $-\infty$.

Definícia.
1) Polynóm $f(x) \in P(K)$ sa nazýva ireducibilný, ak neexistujú $g(x), h(x) \in P(K)$, stupňa aspoň 1, pre ktoré $f(x) = g(x)h(x)$.
2) $c \in K$ je koreň polynómu $f(x) \in P(K)$, ak je hodnota $f(c) = 0$.

Veta. *Ak $f(x) \in P(K)$ a je dané $c \in K$, tak zvyšok po delení $f(x) : (x - c)$ je hodnota $f(c)$; špeciálne, ak c je koreň polynómu f, tak sa dá deliť $f(x) : (x - c)$ bezo zvyšku.*

Dôkaz. Delením dostaneme podiel $g(x)$ a zvyšok je polynóm $r(x)$, $\deg r(x) < deg(z - c) = 1$. Teda $r(x) = r \in K$ $f(x) = (x - c)(g(x) + r \implies f(c) = (c - c)g(c) + r = r$.

Teraz môžeme ešte spresniť definíciu koreňa polynómu z $P(K)$

Definícia. Nech $f(x) \in P(K)$. Prvok $c \in K$ sa nazýva *koreň násobnosti k* (k-násobný koreň) polynómu f, ak $(x - c)^k | f(x)$, ale $(x - c)^{k+1}$ nie je deliteľom polynómu f. Všeobecnejšie, ireducibilný polynóm $g(x)$ sa nazýva *k-násobný ireducibilný deliteľ* polynómu f, ak $[g(x)]^k | f(x)$, ale g^{k+1} nie je deliteľom polynómu f.

Teraz pripomenieme dôležitú vlastnosť poľa komplexných čísel (z predmetu LA1).

Veta (Základná veta algebry)**.** *Každý polynóm s komplexnými koeficientami stupňa aspoň 1 má koreň $c \in C$.*

Kanonický rozklad. *Každý polynóm stupňa n nad C sa dá napísať v tvare*

$$a_nz^n + a_{n-1}z^{n-1} + \cdots + a_1z + a_0 = a_n(z - c_1)^{k_1}(z - c_2)^{k_2} \ldots (z - c_m)^{k_m}\,,$$
$$kde\ k_1 + k_2 + \cdots + k_m = n\,,$$

čísla $c_1, c_2, \ldots, c_m$ sú korene polynómu f. Číslo k_j sa nazýva násobnosť koreňa c_j ($j = 1, 2, \ldots, m$).

Úlohy.
2.1a. Napíšte zvyšok po delení $(z^{10} - z^5 + 1) : (z + i)$
2.1b. Napíšte rozklad nad C polynómov $f_1(z) = z^4 + 1$, $f_2(z) = z^3 - 1$, $f_3(z) = z^2 + z + 1$, $f_4(z) = 2z^2 + 2z + 1$.

Euklidov algoritmus, ktorý sme popísali pre celé čísla, „funguje" aj pre polynómy (v priestore $P(K)$). Ukážeme si to na konkrétnom prípade dvoch polynómov $f_1(x), f_2(x) \in P(Z_2)$.

Úloha. $f_1(x) = x^7 + x^5 + x^4 + x^2 + 1$, $f_2(x) = x^4 + x^2 + 1 \in P(Z_2)$. Nájdite polynómy $a_1(x)$, $a_2(x) \in P(Z_2)$, pre ktoré $\gcd(f_1, f_2) = a_1(x)f_1(x) + a_2(x)f_2(x)$.

Riešenie (v Z_2 je $-1 = +1$, odčítanie je to isté ako sčítanie):

$$\text{delíme } f_1 : f_2, \quad (x^7 + x^5 + x^4 + x^2 + 1) : (x^4 + x^2 + 1) = x^3 + 1$$
$$\underline{(x^7 + x^5 \quad + x^3)}$$
$$x^4 + x^3 + x^2 + 1$$
$$\underline{x^4 + x^2 + 1}$$
$$x^3 = f_3 \implies f_1 = (x^3 + 1)f_2 + f_3 \implies f_3 = f_1 + (x^3 + 1)f_2$$

$$f_2 : f_3, \quad (x^4 + x^2 + 1) : x^3 = x$$
$$\underline{x^4}$$
$$x^2 + 1 = f_4 \implies f_2 = xf_3 + f_4 \implies f_4 = f_2 + xf_3$$

$$f_3 : f_4, \quad (x^3 \quad) : (x^2 + 1) = x$$
$$\underline{x^3 + x}$$
$$x = f_5 \implies f_3 = xf_4 + f_5 \implies f_5 = f_3 + xf_4$$

$$f_4 : f_5, \quad (x^2 + 1) : x = x$$
$$\underline{x^2 \quad}$$
$$1 = f_6 | f_5 \implies 1 = \gcd(f_1, f_2) = f_4 + xf_5$$

A teraz postupne dosadzujeme (od konca) za $f_5, f_4, \ldots$:

$$\gcd(f_1, f_2) = f_4 + xf_5 = f_4 + x(f_3 + xf_4) = xf_3 + (1 + x^2)f_4 = xf_3 + (1 + x^2)(f_2 + xf_3) =$$
$$= xf_3 + (1 + x^2)f_2 + (x + x^3)f_3 = (1 + x^2)f_2 + (x + x + x^3)f_3 = (1 + x^2)f_2 + x^3 f_3 =$$
$$= (1 + x^2)f_2 + x^3(f_1 + (x^3 + 1)f_2) = (1 + x^2)f_2 + x^3 f_1 + (x^6 + x^3)f_2 = x^3 f_1 + (x^6 + x^3 + x^2 + 1)f_2$$

Teda $\gcd(f_1, f_2) = a_1 f_1 + a_2 f_2$, kde $a_1(x) = x^3$, $a_2 = x^6 + x^3 + x^2 + 1$.

Úlohy.

2.1 Napíšte kanonický rozklad nad C polynómu $f(z) =$
(a) $z^6 + 1$, (b) $z^6 - 1$, (c) $z^2 + z + 1$,
(d) $z^3 - 2z^2 + 2z - 1$ ($c = 1$ je koreň), (e) $z^3 + 8i$, (f) $z^3 - 8i$

2.2 Nájdite $\gcd\big(f_1(z), f_2(z)\big)$ v $P(C)$ pre
(a) $f_1(z) = 2z^3 - z^2 + 2, \quad f_2(z) = z^4 + z^3 + z^2 - 1$;
(b) $f_1(z) = 2z^4 + z^3 + z^2 - 2, \quad f_2(z) = z^3 + 2z^2 + 3z + 2$;
(c) $f_1(z) = z^4 + z^3 + 2z^2 + 1, \quad f_2(z) = z^3 - 2z^2 + z - 2$.

Euklidov algoritmus sa dá použiť aj na rozhodnutie, či má polynóm viacnásobný ireducibilný koreň. Najprv definujeme „algebraickú" deriváciu: Ak $f(x) = x^n \in P(K)$ tak, definujeme $f'(x) = nx^{n-1}$. n v exponente je prirodzené číslo a $n \in K$ znamená súčet n jednotiek z poľa K. Derivácia ľubovoľného polynómu sa definuje pomocou pravidiel $(f + g)' = f' + g'$ a $(af)' = af'$ ($a \in K$, $f \in P(K)$). Potom platí aj vzorec $[f(x)g(x)]' = f'(x)g(x) + f(x)g'(x)$.

Predpokladajme teraz, že $f(x) = [g(x)]^k h(x)$, $k > 1$. Potom
$f'(x) = k[g(x)]^{k-1}g'(x)h(x) + [g(x)]^k h'(x) = g^{k-1}(x)[kg'(x)h(x) + g(x)h'(x)] =$
$g^{k-1}(x)h_1(x)$. Teda g^{k-1} je deliteľom polynómov f aj f' a preto $g^{k-1} | \gcd(f, f')$.

Odvodili sme tvrdenie f má viacnásobný ireducibilný deliteľ vtedy a len vtedy, keď $\deg \gcd(f, f') > 0$.

Jednou z najdôležitejších aplikácií Euklidovho algoritmu v (lineárnej) algebre je konštrukcia rozšírení polí podobná konštrukciám polí Z_p.

Definícia. Nech $g(x) \in P(K)$ je ireducibilný polynóm. Označme $P(K)/g(x)$ množinu všetkých zvyškov po delení polynómov $f \in P(K)$ polynómom $g(x)$ a rovnako ako v Z kongruenciu $\pmod p$ definujme kongruenciu $\pmod{g(x)}$:

$$f_1, f_2 \in P(K) \implies f_1 \equiv f_2 \pmod g \iff g|(f_1 - f_2)$$

Spolu s násobením a sčítanim modulo $g(x)$ je potom $P(K)/g(x)$ pole. Ak $g \in P(Z_p)$ pre nejaké prvočíslo a $\deg g(x) = k > 1$, tak $P(K)/g(x)$ má p^k prvkov (všetky polynómy z $P(Z_p)$ stupňa najviac $k-1$).

Všeobecne platí

Veta. *Každé pole K má buď nekonečne veľa prvkov alebo sa jeho počet prvkov rovná mocnine prvočísla.*

Príklad. Polynóm $f(x) = x^2 + x + 1 \in P(Z_2)$ je ireducibilný.
Popíšte (t.j. prvky a operácie $+, \cdot$) pole $F = P(Z_2)/(x^2 + x + 1)$

Prvky tohoto poľa môžeme stotožniť so zvyškami po delení polynómom $f(x)$, t.j. s

$$F = P_1(Z_2) = \{e_0, e_1, e_2, e_3\}: \quad e_0(x) = 0\,,\ e_1(x) = 1\,,\ e_2(x) = x\,,\ e_3(x) = x + 1$$

Pre toto pole napíšte tabuľku násobenia a sčítania.

Úlohy.
1. Napíšte všetky ireducibilné polynómy z $P(Z_2)$ stupňa a) 2, b) 3, c) 4.
2. Pomocou Euklidovho algoritmu nájdite v $P(Z_2)/(x^3+x+1)$ prvok inverzný k $(x+1)$.
3. Vysvetlite tvrdenie: pole komplexných čísel sa rovná $P(R)/(x^2 + 1)$.

Hornerova schéma, ktorú poznáme z predmetu LA1 (pre polynómy nad $\mathbb{R}$ a $\mathbb{C}$) platí v každom poli:

Hornerova schéma. Delenie $f(x) : (x - c) = g(x)$ so zvyškom r sa dá napísať do nasledujúcej tabuľky

	a_n	a_{n-1}	a_{n-2}	$\dots$	a_1	a_0	koeficienty polynómu f	
c		cb_{n-1}	cb_{n-2}	$\dots$	cb_1	cb_0		
	b_{n-1}	b_{n-2}	b_{n-3}	$\dots$	b_0	$r = f(c)$	koeficienty polynómu g	zvyšok

V treťom riadku je súčet čísel v prvých dvoch riadkoch.

Nasledujúce dve kapitoly sú rozšírením látky z LA1 na prípad ľubovoľných polí.

5. Sústavy lineárnych rovníc a matice

5.1. Jedna rovnica s jednou neznámou (v poli K).

$ax = b$, kde $a, b \in K$ sú dané čísla,

máme nájsť všetky $x \in K$, ktoré spĺňajú danú rovnicu.

Riešenie:
a. Ak $a \neq 0$, tak $\exists!\, x = \frac{b}{a}$ (práve jedno riešenie),
b. Ak $a = 0 \wedge b \neq 0$, tak žiadne $x \in K$ nespĺňa $0 \cdot x = b$ (žiadne riešenie),
c. Ak $a = 0 \wedge b = 0$, tak každé $x \in K$ spĺňa $0 \cdot x = b$ (pre $K = \mathbb{R}$ alebo $\mathbb{C}$ nekonečne veľa riešení).

Rovnaké tri možnosti sú pre počet riešení všetkých sústav s komplexnými (aj reálnymi) koeficientami. Inak je to v prípade, že K je konečné pole.

V prípade reálnych koeficientov a, b vieme, že pre vzájomú polohu priamok $p \equiv y = ax$ a $q \equiv y = b$ sú presne 3 možnosti:

1. môžu sa pretínať v jednom bode $p \cap q = \left[\frac{b}{a}, b\right]$,
2. môžu byť rovnobežné rôzne $(p \parallel q)$ alebo 3. totožné $(p = q)$

Podobne ako v prípade rovníc s reálnymi koeficientami, môžeme zaviesť maticu sústavy a rozšírenú maticu sústavy nad poľom K.

5.2. Sústava m lineárnych rovníc s n neznámymi $m, n \in N$, $m \geq 1$, $n > 1$.

Nech $a_{ij} \in K$, $b_j \in K$, $i \in \{1, \ldots, m\}$, $j \in \{1, \ldots, n\}$ sú dané čísla. Sústavou m lineárnych rovníc s n neznámymi nazývame:

$$\begin{array}{c} a_{11}x_1 + a_{12}x_2 + \ \ldots \ + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ \ldots \ + a_{2n}x_n = b_2 \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{array} \tag{S}$$

Riešiť sústavu (S) znamená nájsť množinu P všetkých usporiadaných n-tíc prvkov z K, pre ktoré po dosadení do každej rovnice zo sústavy (S) za $(x_1, x_2, \ldots, x_n)$ vznikne rovnosť.

Definícia. K^n označuje množinu všetkých usporiadaných n-tíc prvkov (čísel) z poľa K. Nech $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in K^n$, $\mathbf{y} = (y_1, y_2, \ldots, y_n) \in K^n$ a $\alpha \in K$. Potom

(i) $\mathbf{x} + \mathbf{y} = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$ sa nazýva súčet n-tíc $\mathbf{x}$ a $\mathbf{y}$.
(ii) $\alpha\mathbf{x} = (\alpha x_1, \alpha x_2, \ldots, \alpha x_n)$ sa nazýva násobok n-tice $\mathbf{x}$ číslom α.
(iii) n-tica $\mathbf{0} = (0, 0, \ldots, 0) \in R^n$ (C^n) sa nazýva nulová n-tica.
(iv) $-\mathbf{x} = (-x_1, -x_2, \ldots, -x_n)$ sa nazýva n-tica opačná k n-tici x.

Definícia. Tabuľku zostavenú z čísel $a_{ij} \in K$, $i \in \{1, 2, \ldots m\}$, $j \in \{1, 2, \ldots n\}$

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix} = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq \leq n}}$$

nazývame matica typu $m \times n$. Množinu všetkých matíc typu $m \times n$ budeme označovať $K^{m \times n}$. Usporiadané n-tice $A_{i*} = (\, a_{i1} \quad a_{i2} \quad \ldots \quad a_{in} \,)$ sa nazývajú riadky a usporiadané m-tice $A_{*j} = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}$ sa nazývajú stĺpce matice A.

Pri riešení sústavy (S) budeme používať jej zápis pomocou matíc:

matica sústavy (S): $A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}$,

rozšírená matica sústavy (S): $\tilde{A} = \left(\begin{array}{cccc|c} a_{11} & a_{12} & \ldots & a_{1n} & b_1 \\ a_{21} & a_{22} & \ldots & a_{2n} & b_2 \\ \ldots & \ldots & \ldots & \ldots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} & b_m \end{array}\right)$,

Potom sústavu (S), resp. jej rozšírenú maticu $\tilde{A}$ upravíme na maticu zodpovedajúcu sústave, ktorá má tú istú množinu P všetkých riešení, ale je pomocou nej jednoduchšie popísať množinu P.

Nasledujúce úpravy matice A nemenia množinu všetkých riešení zodpovedajúcej sústavy, nazývame ich elementárne riadkové operácie (ERO).

ERO1 Vzájomná výmena riadkov ($A_{i*} \leftrightarrow A_{j*}$, $i \neq j$), alebo stručne $R_i \leftrightarrow R_j$

ERO2 Násobenie niektorého riadku matice A nenulovým číslom ($A_{i*} \to \alpha A_{i*}$, $\alpha \neq 0$) alebo αR_i

ERO3 Pričítanie násobku niektorého riadka k inému riadku ($A_{i*} \to A_{i*} + \alpha A_{j*}$, $i \neq j$) alebo $R_i + \alpha R_j$.

Definícia. Prvý (zľava) nenulový prvok a_{ij} v riadku A_{i*} matice A sa nazýva vedúci prvok (pivot) riadku A_{i*}. Matica A sa nazýva stupňovitá, ak platí

1) pivot $(i+1)$-ého riadka je v stĺpci napravo od stĺpca, v ktorom je pivot i-teho riadka (v stĺpci pod každým pivotom sú iba nuly).
2) každý nulový riadok je pod každým nenulovým riadkom matice A (t.j. nulové riadky sú premiestnené do spodnej časti matice).

A sa nazýva redukovaná stupňovitá, ak je stupňovitá a navyše všetky jej pivoty sa rovnajú 1 a aj nad nimi sú v stĺpci len nuly.

Ľahko vidieť, že pomocou ERO vznikne matica sústavy so zhodnou množinou všetkých riešení. Budem teda upravovať rozšírenú maticu danej sústavy na stupňovitú alebo redukovanú stupňovitú. Dá sa tiež dokázať, že každá matica A typu $m \times n$ sa dá upraviť pomocou ERO na jednoznačne určenú redukovanú stupňovitú maticu B typu $m \times n$, budeme písať $A \sim B$ (matice A, B sú riadkovo ekvivalentné). Postup ukážeme na príklade sústavy a jej rozšírenej matice (s prvkami z R):

$$\begin{aligned} 3x_1 - 2x_2 + x_3 &= 11 \\ x_1 + x_2 - 3x_3 &= 7 \\ 11x_1 - 4x_2 - 3x_3 &= 10 \end{aligned} \to A = \left(\begin{array}{ccc|c} 3 & -2 & 1 & 11 \\ 1 & 1 & -3 & 7 \\ 11 & -4 & -3 & 10 \end{array}\right) \sim_{R_1 \leftrightarrow R_2} \left(\begin{array}{ccc|c} 1 & 1 & -3 & 7 \\ 3 & -2 & 1 & 11 \\ 11 & -4 & -3 & 10 \end{array}\right)$$

Pivot R_1 je teraz číslo 1 (to sme mohli dosiahnúť aj vynásobením prvého riadka číslom $\frac{1}{3}$, ale takto sa vyhneme zlomkom). Pomocou ERO $R_2 - 3R_1$ a $R_3 - 11R_1$ dostaneme

$$A \sim \left(\begin{array}{ccc|c} 1 & 1 & -3 & 7 \\ 0 & -5 & 10 & -10 \\ 0 & -15 & 30 & -67 \end{array}\right) \sim_{R_3 - 3R_2} \left(\begin{array}{ccc|c} 1 & 1 & -3 & 7 \\ 0 & -5 & 10 & -10 \\ 0 & 0 & 0 & -37 \end{array}\right) = B$$

B je stupňovitá matica, ktorej posledný riadok zodpovedá rovnici $0x_1 + 0x_2 + 0x_3 = -37$ a je zrejmé, že nemá riešenie, teda $P = \emptyset$.

Pri úpravách sme postupovali „zľava a zhora” „doprava a dole”. Na úpravu na redukovanú stupňovitú maticu budeme maticu B upravovať od posledného pivota vpravo dole naspäť vľavo hore.

$$B \sim_{-\frac{1}{37}R_3} \left(\begin{array}{ccc|c} 1 & 1 & -3 & 7 \\ 0 & -5 & 10 & -10 \\ 0 & 0 & 0 & 1 \end{array}\right) \sim_{-\frac{1}{5}R_2} \left(\begin{array}{ccc|c} 1 & 1 & -3 & 7 \\ 0 & 1 & -2 & 2 \\ 0 & 0 & 0 & 1 \end{array}\right) \sim_{\substack{R_2 - 2R_3 \\ R_1 - 7R_3}} \left(\begin{array}{ccc|c} 1 & 1 & -3 & 0 \\ 0 & 1 & -2 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right) \sim_{R_1 - R_2} \left(\begin{array}{ccc|c} 1 & 0 & -1 & 0 \\ 0 & 1 & -2 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right)$$

Posledná matica je už redukovaná stupňovitá.

Ak by sme poslednú rovnicu vynechali jej rozšírená matica sa pomocou ERO dá upraviť na

$$\left(\begin{array}{ccc|c} 1 & 1 & -3 & 7 \\ 0 & 1 & -2 & 2 \end{array}\right) \sim_{R_1 - R_3} \left(\begin{array}{ccc|c} 1 & 0 & -1 & 5 \\ 0 & 1 & -2 & 2 \end{array}\right)$$

Teraz je ľahké napísať riešenie (za neznámu zodpovedajúca stĺpcu bez pivota zvolíme ľubovoľné číslo):

$$x_3 = a \in R\,, \; x_2 - 2a = 2 \implies x_2 = 2 + 2a\,, \; x_1 - a = 5 \implies x_1 = 5 + a \implies$$
$$\underline{P = \{(5 + a, 2 + 2a, a)\; a \in R\}}$$

Popísaný postup sa v prípade, že úpravu matice ukončíme dosiahnutím stupňovitej matice, nazýva Gaussova eliminačná metóda (GEM). Ak pokračujeme po získanie redukovanej stupňnovitej matice, hovoríme o Gaussovej-Jordanovej eliminačnej metóde.

Príklad. Napíšte množinu P všetkých riešení sústavy, ktorej rozšírená matica je

a) $\left(\begin{array}{ccccc|c} 2 & 1 & 0 & -1 & 3 & -1 \\ 0 & 1 & 3 & 1 & 3 & 2 \\ 0 & 0 & 0 & -1 & 1 & 1 \end{array}\right)$ b) $\left(\begin{array}{ccccc|c} 1 & 0 & -3/2 & 0 & -1 & -5/2 \\ 0 & 1 & 3 & 0 & 4 & 3 \\ 0 & 0 & 0 & 1 & -1 & -1 \end{array}\right)$

a)

$$\left(\begin{array}{ccccc|c} 2 & 1 & 0 & -1 & 3 & -1 \\ 0 & 1 & 3 & 1 & 3 & 2 \\ 0 & 0 & 0 & -1 & 1 & 1 \end{array}\right) \to \begin{aligned} 2x_1 + x_2 - x_4 + 3x_5 &= -1 \\ x_2 + 3x_3 + x_4 + 3x_5 &= 2 \\ -x_4 + x_5 &= 1 \end{aligned}$$

Začneme od poslednej rovnice, v ktorj sú dve neznáme jednu zvolíme ľubovoľne,
$\underline{x_5 = a} \implies \underline{x_4 = -1 + a}$,
dosadíme to do druhej rovnice:
$x_2 + 3x_3 + (-1 + a) + 3a = 2$. Ak zvolíme $\underline{x_3 = b}$, dostaneme
$x_2 + 3b - 1 + 4a = 2 \implies \underline{x_2 = 3 - 4a - 3b}$
nakoniec doteraz získané výsledky dosadíme do prvej rovnice:
$2x_1+(3-4a-3b)-(-1+a)+3a = -1 \iff 2x_1+4-2a-3b = -1 \implies x_1 = \frac{1}{2}(-5+2a+3b)$
$\underline{x_1 = -\frac{5}{2} + a + \frac{3}{2}b}$, teda

$$P = \left\{ \left(\frac{5}{2} + a + \frac{3}{2}b, 3 - 4a - 3b, b, -1 + a, a \right) : a, b \in R \right\}$$

Poznamenajme, že za voľné parametre a, b sme zvolili tie neznáme, ktoré zodpovedajú stĺpcom bez pivotov. Matica z príkladu b) je redukovaá stupňnovitá, na ktorú sme upravili prvú maticu. V tomto prípade môžeme množinu P napísať priamo z matice, lebo po zvolení parametrov obsahujú všetky tri rovnice sústavy už len jednu neznámu.

Rovnako môžeme riešiť aj sústavy nad konečnými poľami.

Úloha. Riešte sústavu lineárnych rovníc a) v poli Z_2

$$\begin{aligned} x_1 + x_3 + x_4 &= 0 \\ x_1 + x_2 + x_4 &= 1 \\ x_2 + x_4 &= 1 \end{aligned} \quad \text{má rozšírenú maticu} \quad \left(\begin{array}{cccc|c} 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{array}\right) \sim_{R_2+R_1} \left(\begin{array}{cccc|c} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{array}\right)$$

$$\sim_{R_3+R_2} \left(\begin{array}{cccc|c} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{array}\right) \sim_{\substack{R_2+R_3 \\ R_1+R_3}} \left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{array}\right)$$

Maticu me upravili na redukovanú stupňovitú, zvolíme $x_4 = a \in Z_2$,
potom $P = \{(0, 1 + a, a, a) \colon a \in Z_2\} = \{(0, 1, 0, 0); (0, 0, 1, 1)\}$.

b) v poli Z_3

$$\begin{aligned} 2x_1 + x_3 + x_4 &= 0 \\ x_1 + x_2 + 2x_4 &= 1 \\ x_2 + x_4 &= 2 \end{aligned} \quad \to \quad \left(\begin{array}{cccc|c} 2 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 2 & 1 \\ 0 & 1 & 0 & 1 & 2 \end{array}\right) \sim_{R_2+R_1} \left(\begin{array}{cccc|c} 2 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 2 \end{array}\right)$$

$$\sim_{R_3+2R_2} \left(\begin{array}{cccc|c} 2 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 2 & 1 & 1 \end{array}\right) \sim_{\substack{R_2+R_3 \\ R_1+R_3}} \left(\begin{array}{cccc|c} 2 & 0 & 0 & 2 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 2 & 1 & 1 \end{array}\right) \sim_{\substack{2R_1 \\ 2R_3}} \left(\begin{array}{cccc|c} 1 & 0 & 0 & 1 & 2 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 2 & 2 \end{array}\right)$$

a z tejto redukovanej stupňovitej matice dostaneme
$P = (2 - a, 2 - a, 2 - 2a, a) \colon a \in \{0, 1, 2\}\} = \{(2, 2, 2, 0); (1, 1, 0, 1); (0, 0, 1, 2)\}$.

V nasledujúcej kapitole pripomenieme niektoré definície a vlastnosti matíc a maticovej algebry nad $\mathbb{R}$ a $\mathbb{C}$. Obdobné tvrdenia platia aj v konečných poliach, napr. v Z_p, kde p je prvočíslo.

6. Maticová algebra a determinnty

Najprv zavedieme pojem lineárnej závislosti a nezávislosti

6.1. Lineárna závislosť a nezávislosť v R^n a C^n.

Definícia. Nech $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_k \in R^n$ a $\alpha_1, \alpha_2, \dots, \alpha_k \in R$.
1. $\alpha_1\mathbf{x}_1 + \alpha_2\mathbf{x}_2 + \cdots + \alpha_k\mathbf{x}_k$ sa nazýva lineárna kombinácia vektorov $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_k$.
2. Hovoríme, že k-tica $\{\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_k\}$ je linárne nezávislá, ak $\alpha_1\mathbf{x}_1 + \alpha_2\mathbf{x}_2 + \cdots + \alpha_k\mathbf{x}_k = \mathbf{0} \implies \alpha_1 = \alpha_2 = \cdots = \alpha_k = 0$.
3. Ak nie je k-tica $\{\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_k\}$ lineárne nezávislá, tak sa nazýva lineárne závislá.

Podobne hovoríme o lineárnej kombinácii, závislosti a nezávislosti k-tice matíc, polynómov alebo, všeobecnjšie, funkcií.

6.2. súčet a súčin matíc.

Operácie síce budeme dfinovať pre matice s reálnymi prvkami, ale rovnaké definície a tvrdenia sú platné aj pre komplexné matice. Najprv definujeme sčítanie matíc rovnakého typu (je vlastne zhodné so sčítaním v R^{mn}, resp. C^{mn}):

Súčet matíc. Nech $m, n \in N$, $A = (a_{ij})_{\substack{1\le i\le m\\ 1\le j\le n}} \in R^{m\times n}$, $B = (b_{ij})_{\substack{1\le i\le m\\ 1\le j\le n}} \in R^{m\times n}$. Potom $A + B \in R^{m\times n}$ definujeme rovnosťou $A + B = (a_{ij} + b_{ij})_{\substack{1\le i\le m\\ 1\le j\le n}}$

Príklad. $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 1 & 0 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 3 \\ 4 & 3 & 2 \end{pmatrix}$, ale $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}$ nie je definované.

Skôr, než definujeme súčin matíc zavedieme pojem matice $A^\top$ transponovanej k matici A. $A^\top$ vznikne „preklopením" matice A okolo hlavnej diagonály, resp. zámenou úloh stĺpcov a riadkov, napr.

$$(\,x_1 \quad x_2 \quad x_3\,)^\top = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \quad \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix}^\top = \begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \\ a_{13} & a_{23} \end{pmatrix}$$

Všeobecne, ak $A = (a_{ij}) \in R^{m\times n}$, tak $A^\top = B = (b_{ji}) \in R^{n\times m}$, pričom $b_{ji} = a_{ij}$ pre všetky $i \in \{1, 2, \dots, m\}$, $j \in \{1, 2, \dots, n\}$.

Súčin matíc. Najprv definujeme súčin matice A typu $m \times n$ a stĺpca x $(n \times 1)$:

pre $A = (a_{ij})_{\substack{1\le i\le m\\ 1\le j\le n}}$, $x = (x_1, x_2, \dots, x_n)^\top$ definujeme $Ax = x_1A_{*1} + x_2A_{*2} + \cdots + x_nA_{*n}$.

Pomocou vzťahu $x \mapsto Ax$ je tak definované jednoznačné priradenie (zobrazenie) stĺpca $Ax \in R^{m\times 1}$ k stĺpcu $x \in R^{n\times 1}$, napr. pre $A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 0 & 1 \end{pmatrix}$, $x = \begin{pmatrix} -1 \\ 1 \\ 2 \end{pmatrix}$ je $Ax = -\begin{pmatrix} 1 \\ 2 \end{pmatrix} + \begin{pmatrix} 2 \\ 0 \end{pmatrix} + 2\begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} -1+2+6 \\ -2+0+2 \end{pmatrix} = \begin{pmatrix} 5 \\ 0 \end{pmatrix}$

Ak namiesto jedného stĺpca x zoberieme maticu B typu $n \times k$ a definujeme AB tak, že maticu A násobíme sprava každým stĺpcom matice B a zo sískaných stĺpcov „poskladáme" jednu maticu $AB = D = (d_{ij})_{\substack{1\le i\le m\\ 1\le j\le k}}$.

Teda násobíme maticu $A \in R^{m\times n}$ sprava maticou $B \in R^{n\times k}$ a výsledok je matica $D \in R^{m\times k}$ s prvkami $d_{ij} = A_{i*}B_{*j}$ (i-ty riadok matice A krát j-ty stĺpec matice B). Ak sa počet riadkov matice A nerovná počtu stĺpcov matice B, tak nie je súčin AB definovaný.

Veta (vlastnosti súčtu a súčinu matíc.
1) Ak $A, B \in R^{m\times n}$, $D \in R^{n\times k}$, tak $(A+B)D = AD + BD$,
2) Ak $A, B \in R^{m\times n}$, $D \in R^{k\times m}$, tak $D(A+B) = DA + DB$,
3) Ak $A \in R^{m\times n}$, $B \in R^{n\times k}$, tak $(AB)^\top = B^\top A^\top$.
4) Násobenie matíc nie je komutatívne, t.j. nemusí platiť $AB = BA$ (ani keď sú obe strany definované).

Definícia. Matice, ktoré majú rovnaký počet riadkov ako stĺpcov sa nazývajú *štvorcové*. Hovoríme, že prvky a_{ii}, $i = 1, 2, \dots n$ matice $A = (a_{ij}) \in R^{n\times n}$ tvoria *hlavnú diagonálu* matice A. Matica $I_n \in R^{n\times n}$, ktorá má všetky čísla na hlavnej diagonále rovné 1 a ostatné prvky nulové, sa nazýva *jednotková.*

Poznamenajme, že $A \in R^{m\times n}$, tak $I_m A = AI_n = A$, to vysvetľuje názov jednotková matica.

Podobne pre štvorcovú maticu $A \in R^{n\times n}$ definujeme inverznú maticu ako $B \in R^{n\times n}$, pre ktorú $AB = I_n$. K danej matici A existuje najviac jedna inverzná, navyše ak $AB = I_n$, tak aj $BA = I_n$.

6.3. Výpočet inverznej matice.

Postup vysvetlíme na maticiach typu 3×3, nech $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$, hľadáme maticu $B = \begin{pmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{pmatrix}$, pre ktorú platí

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \begin{pmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Ak označíme x, y, z prvý, druhý a tretí stĺpec neznámej matice B, máme vlastne riešiť tri sústavy rovníc

$$Ax = (1,0,0)^\top, \quad Ay = (0,1,0)^\top, \quad Az = (0,0,1)^\top,$$

ktoré majú tú istú maticu, ale rôzne pravé strany, t.j. rôzne rozšírené matice. Takže maticu A rozšírime o všetky tri pravé strany a upravíme na riadkovo ekvivalentnú redukovanú stupňovitú maticu, jej hodnosť sa rovná hodnosti pravej strany, t.j. n, teda buď majú všetky tri sústavy práve jedno riešenie, alebo aspoň jedna z nich nemá riešenie a inverzná matica neexistuje. Maticu inverznú k matici A označujeme A^{-1}

Príklad.. Nájdite A^{-1} pre $A = \begin{pmatrix} 1 & -1 & 2 \\ 1 & -2 & 0 \\ 0 & 1 & 1 \end{pmatrix}$.

$$\left(\begin{array}{ccc|ccc} 1 & -1 & 2 & 1 & 0 & 0 \\ 1 & -2 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right) \sim_{R_2 - R_1} \left(\begin{array}{ccc|ccc} 1 & -1 & 2 & 1 & 0 & 0 \\ 0 & -1 & -2 & -1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right) \sim_{R_3 + R_2} \left(\begin{array}{ccc|ccc} 1 & -1 & 2 & 1 & 0 & 0 \\ 0 & -1 & -2 & -1 & 1 & 0 \\ 0 & 0 & -1 & -1 & 1 & 1 \end{array}\right) \sim_{\substack{-R_2 \\ -R_3}}$$

$$\left(\begin{array}{ccc|ccc} 1 & -1 & 2 & 1 & 0 & 0 \\ 0 & 1 & 2 & 1 & -1 & 0 \\ 0 & 0 & 1 & 1 & -1 & -1 \end{array}\right) \sim_{\substack{R_2 - 2R_3 \\ R_1 - 2R_3}} \left(\begin{array}{ccc|ccc} 1 & -1 & 0 & -1 & 2 & 2 \\ 0 & 1 & 0 & -1 & 1 & 2 \\ 0 & 0 & 1 & 1 & -1 & -1 \end{array}\right) \sim_{R_1 + R_2} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -2 & 3 & 4 \\ 0 & 1 & 0 & -1 & 1 & 2 \\ 0 & 0 & 1 & 1 & -1 & -1 \end{array}\right)$$

Teda upravili sme $\big(A \,|\, I_3\big) \sim \big(I_3 \,|\, A^{-1}\big)$. Dostali sme $A^{-1} = \begin{pmatrix} -2 & 3 & 4 \\ -1 & 1 & 2 \\ 1 & -1 & -1 \end{pmatrix}$

(overte $AA^{-1} = A^{-1}A = I_3$).

Ukážte, že k matici $A = \begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix}$ neexistuje inverzná matica.

Veta. *Nech $A \in R^{n\times n}$. Potom sú nasledujúce tvrdenia ekvivalentné.*

a) existuje matica A^{-1},
b) A má hodnosť n,
c) riadky matice A sú lineárne nezávislé,
d) stĺpce matice A sú lineárne nezávislé.

Definícia. Štvorcová matica, ktorá má inverznú sa nazýva *regulárna.*

6.4. Determinanty štvorcových matíc.

Determinant štvorcovej matice A je číslo $\det A$, určené nasledujúcou (induktívnou) definíciou.

Definícia. Nech $A \in C^{n\times n}$, $n \in N$.

1. Ak $n = 1$, $A = (a_{11})$, tak $\det A = a_{11}$
2. Ak $n > 1$ označíme A_{ij} maticu, ktorá vznikne z matice A odstránením stĺpca A_{*j} a riadka A_{i*}.
   $\det A = a_{11}\det A_{11} - a_{12}\det A_{12} + \cdots + (-1)^{1+n} a_{1n}\det A_{1n}$ (rozvoj podľa prvého riadku).

Podľa bodu 2. sa počíta determinant, ak vieme počítať determinanty matíc typu $(n-1)\times(n-1)$, teda

Ak $n = 2$, $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$, tak $\det A = a_{11}\det(a_{22}) - a_{12}\det(a_{21}) = a_{11}a_{22} - a_{12}a_{21}$.

Determinant označujeme aj ako maticu ohraničenú kolmými čiarami namiesto zátvoriek, $\det A = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}$. Pre $n = 2$ teda je determinant súčin čísel na hlavnej diagonále mínus súčin čísel na vedľajšej diagonále.

Ak $n = 3$. $\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}\begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12}\begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13}\begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix} =$

$a_{11}(a_{22}a_{33} - a_{23}a_{32}) - a_{12}(a_{21}a_{33} - a_{23}a_{31}) + a_{13}(a_{21}a_{32} - a_{22}a_{31}) =$
$(a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32}) - (a_{11}a_{23}a_{32} + a_{12}a_{21}a_{33} + a_{13}a_{22}a_{31})$.

Pre determinant matice 3×3 sa dá sformulovať Sarusovo pravidlo. Prvé dva stĺpce pripíšeme ako štvrtý a piaty a determinant je súčet všetkých troch súčinov na hlavných diagonálach zľava hore doprava dole minus súčest súčinov na 3 vedľajších diagonálach.

$$\left|\begin{matrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{matrix}\right|\begin{matrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ a_{31} & a_{32} \end{matrix} \qquad \begin{aligned} \det A = {} & (a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32}) \\ & -(a_{13}a_{22}a_{31} + a_{11}a_{23}a_{32} + a_{12}a_{21}a_{33}). \end{aligned}$$

Pre väčšie matice žiadne analogické pravidlo neexistuje a najvhodnejší je spôsob výpočtu pomocou ERO.

Najprv definujeme ďalšie špecialne typy matíc.

Definícia. Matica $A = (a_{ij}) \in C^{n\times n}$ sa nazýva

(i) dolná trojuholníková, ak $j > i \implies a_{ij} = 0$ (všetky prvky nad hlavnou diagonálou sú nulové),
(ii) horná trojuholníková, ak $j < i \implies a_{ij} = 0$ (všetky prvky pod hlavnou diagonálou sú nulové),
(iii) trojuholníková, ak je dolná alebo horná trojuholníková,
(iV) diagonálna, ak $j \neq i \implies a_{ij} = 0$ (všetky prvky mimo hlavnej diagonály sú nulové).

Vlastnosti determinantu zhrnieme v nasledujúcej vete, ktorej dôkaz sa dá urobiť matematickou indukciou.

Veta. *Nech $A \in C^{n\times n}$. Potom platí*

1.
$$\forall\, i \in \{a,\dots,n\} \quad \det A = \sum_{j=1}^{n} a_{ij}(-1)^{i+j}\det A_{ij} \quad (\textit{rozvoj podľa i-teho riadku})\,,$$
$$\forall\, j \in \{a,\dots,n\} \quad \det A = \sum_{i=1}^{n} a_{ij}(-1)^{i+j}\det A_{ij} \quad (\textit{rozvoj podľa j-teho stĺpca})\,.$$

2. *Ak $B \sim A$ vznikla z matice A pomocou* ERO
 2.1. *násobenia niektorého riadka číslom α, tak* $\det B = \alpha \det A$,
 2.2. *vzájomnou výmenou dvoch riadkov, tak* $\det B = -\det A$,
 2.3. *pričítaním násobku niektorého riadka k inému riadku, tak* $\det B = \det A$,
3. $\det A^\top = \det A$

Dôsledok.
(i) *Determinant trojuholníkovej matice sa rovná súčinu jej prvkov na hlavnej diagonále.*
(ii) *Ak má matica A dva rovnaké riadky alebo stĺpce, tak* $\det A = 0$.
(iii) $A, B \in C^{n\times n} \implies \det(AB) = (\det A)(\det B)$.

Prvé dôsledky sa pomocou predchádzajúcej vety dajú dokázať jednoducho, dôkaz tvrdenia o determinante súčinu je podstatne náročnejší.

6.5 Výpočet inverznej matice pomocou determinantov a Cramerovo pravidlo.

Pre maticu $A = (a_{ij}) \in C^{n\times n}$ označíme $\tilde a_{ij} = (-1)^{i+j}\det A_{ij}$. $\tilde a_{ij}$ sa nazýva algebraický doplnok prvku a_{ij} v matici A, výstižnejie by bolo povedať algebraický doplnok pozície (ij), lebo od hodnoty samotného prvku a_{ij} ani od čísel v celom riadku A_{i*} a stĺpci A_{*j} číslo $\tilde a_{ij}$ nezávisí.

Počítajme teraz súčin matíc

$$\begin{pmatrix} a_{11} & a_{12} & a_{13}\\ a_{21} & a_{22} & a_{23}\\ a_{31} & a_{32} & a_{33}\end{pmatrix}\begin{pmatrix} \tilde a_{11} & \tilde a_{12} & \tilde a_{13}\\ \tilde a_{21} & \tilde a_{22} & \tilde a_{23}\\ \tilde a_{31} & \tilde a_{32} & \tilde a_{33}\end{pmatrix}^\top = \begin{pmatrix} a_{11} & a_{12} & a_{13}\\ a_{21} & a_{22} & a_{23}\\ a_{31} & a_{32} & a_{33}\end{pmatrix}\begin{pmatrix} \tilde a_{11} & \tilde a_{21} & \tilde a_{31}\\ \tilde a_{12} & \tilde a_{22} & \tilde a_{32}\\ \tilde a_{13} & \tilde a_{23} & \tilde a_{33}\end{pmatrix} =$$
$$= \begin{pmatrix} (a_{11}\tilde a_{11} + a_{12}\tilde a_{12} + a_{13}\tilde a_{13}) & (a_{11}\tilde a_{21} + a_{12}\tilde a_{22} + a_{13}\tilde a_{23}) & (a_{11}\tilde a_{31} + a_{12}\tilde a_{32} + a_{13}\tilde a_{33})\\ (a_{21}\tilde a_{11} + a_{22}\tilde a_{12} + a_{23}\tilde a_{13}) & (a_{21}\tilde a_{21} + a_{22}\tilde a_{22} + a_{23}\tilde a_{23}) & (a_{21}\tilde a_{31} + a_{22}\tilde a_{32} + a_{23}\tilde a_{33})\\ (a_{31}\tilde a_{11} + a_{32}\tilde a_{12} + a_{33}\tilde a_{13}) & (a_{31}\tilde a_{21} + a_{32}\tilde a_{22} + a_{33}\tilde a_{23}) & (a_{31}\tilde a_{31} + a_{32}\tilde a_{32} + a_{33}\tilde a_{33})\end{pmatrix} =$$
$$= \begin{pmatrix} \det A & 0 & 0\\ 0 & \det A & 0\\ 0 & 0 & \det A\end{pmatrix} = (b_{ij})_{1\le i,j\le n} = (\det A) I_3\,.$$

Čísla na hlavnej diagonále $b_{11} = b_{22} = b_{33} = \det A$ sú rozvoje $\det A$ podľa prvého, druhého a tretieho riadka. Na ostatných miestach sú rozvoje determinaantov matíc, ktoré majú dva rovnaké riadky, napr

$$\text{rozvoj podľa druhého riadka} \quad 0 = \begin{vmatrix} a_{11} & a_{12} & a_{13}\\ a_{11} & a_{12} & a_{13}\\ a_{31} & a_{32} & a_{33}\end{vmatrix} = (a_{11}\tilde a_{21} + a_{12}\tilde a_{22} + a_{13}\tilde a_{23}) = b_{12}$$

(algebraické doplnky druhého riadka posledného determinantu sú rovnaké ako v matici A). Ak je $\det A \neq 0$, tak z predchádzajúcich výpotčov vyplýva

$$A^{-1} = \frac{1}{\det A}(\tilde a_{ij})^\top = \frac{1}{\det A}\begin{pmatrix} \begin{vmatrix} a_{22} & a_{23}\\ a_{32} & a_{33}\end{vmatrix} & -\begin{vmatrix} a_{12} & a_{13}\\ a_{32} & a_{33}\end{vmatrix} & \begin{vmatrix} a_{12} & a_{13}\\ a_{22} & a_{23}\end{vmatrix}\\ -\begin{vmatrix} a_{21} & a_{23}\\ a_{31} & a_{33}\end{vmatrix} & \begin{vmatrix} a_{11} & a_{13}\\ a_{31} & a_{33}\end{vmatrix} & -\begin{vmatrix} a_{11} & a_{13}\\ a_{21} & a_{23}\end{vmatrix}\\ \begin{vmatrix} a_{21} & a_{22}\\ a_{31} & a_{32}\end{vmatrix} & -\begin{vmatrix} a_{11} & a_{12}\\ a_{31} & a_{32}\end{vmatrix} & \begin{vmatrix} a_{11} & a_{12}\\ a_{21} & a_{22}\end{vmatrix}\end{pmatrix}.$$

Pre matice typu 3×3 sme tým dokázali nasledujúcu vetu, pre matice $n\times n$ sa dá dokázať analogicky.

Veta. *Nech* $A = (a_{ij}) \in C^{n\times n}$ *a nech* $\operatorname{adj} A = (\tilde{a}_{ij})^\top$ *(matica adjungovaná k matici* A*). Potom platí*

$$A(\operatorname{adj} A) = (\det A) I_n\,.$$

Ak, navyše, $\det A \neq 0$*, tak*

$$A^{-1} = \frac{1}{\det A} \operatorname{adj} A\,.$$

Tým je súčasne dokázané aj tvrdenie

Veta. $A \in C^{n\times n}$ *je regulárna vtedy a len vtedy, keď* $\det A \neq 0$.

Priamym dôsledkom vzťahu $A^{-1} = \frac{1}{\det A} \operatorname{adj} A$ je

Cramerovo pravidlo. *Ak* $A \in C^{n\times n}$ *je regulárna matica a* $\mathbf{b} \in C^{n\times 1}$*, tak má sústava lineárnych rovníc*

$$A\mathbf{x} = \mathbf{b}$$

práve jedno riešenie $\mathbf{x} = \left(\frac{d_1}{d}, \frac{d_2}{d}, \dots, \frac{d_n}{d}\right)$*, kde* $d = \det A$ *a* d_j $(j = 1, 2, \dots n)$ *je determinant matice, ktorá vznikne z matice* A *zámenou stĺpca* A_{*j} *za* $\mathbf{b}$ *(pravú stranu).*

7. Vektorové (lineárne) priestory

Definícia. Trojica $(L, \oplus, \odot)$ sa nazýva lineárny (vektorový) priestor nad poľom $(K, +, \cdot)$, ak
L je neprázdna množina (vektorov) a $\oplus\colon L\times L \to L$; $\odot\colon K \times L \to L$ sú operácie také, že platí:
pre $\forall\, x, y, z \in L$ a pre $\forall\, \alpha, \beta \in K$
(L1) $x \oplus y = y \oplus x$ (komutatívny zákon pre sčítanie)
(L2) $(x \oplus y) \oplus z = x \oplus (y \oplus z)$ (asociatívny zákon pre sčítanie)
(L3) $\exists\, \mathbf{0} \in L$: $x \oplus \mathbf{0} = x$ (existuje neutrálny prvok pre sčítanie)
(L3) $\forall x \in L\ \exists y \in L$ taký, že $x \oplus y = \mathbf{0}$ ($\exists\, y = -x$ opačný prvok k x)
(L5) $\alpha \odot (x \oplus y) = (\alpha \odot x) \oplus (\alpha \odot y)$
(L6) $(\alpha + \beta) \odot x = (\alpha \odot x) \oplus (\beta \odot y)$
(L7) $(\alpha\beta) \odot x = \alpha \odot (\beta \odot x)$
(L8) $1 \odot x = x$

Príkladmi lineárnych priestorov nad R sú priestory funkcií $f\colon A \to R$ s obvyklými operáciami sčítania funkcií a násobenia funkcie reálnym číslom. Rovnako aj množina všetkých funkciíi $f\colon A \to K$ je lioneárny priestor nad poľom K. Špeciálne, ak $A = \{1, 2, \dots, n\}$, tento priestor označujeme K^n a je to lineárny priestor n-tíc prvkov z poľa K.

Úloha. Vypočítajte $(1, 0, 1, 1) \oplus (1, 1, 0, 1)$ v lineárnom priestore K^n, kde
a. $K = R$, b. $K = Z_3$, c. $K = Z_2$.

Definícia. Nech $(L, +, \cdot)$ je lineárny priestor nad poľom K. Podmnožina $M \subset L$ sa nazýva podpriestor lineárneho priestoru $(L, +, \cdot)$, ak je $(M, +, \cdot)$ tiež lineárnym priestorom.

Veta. *Neprázdna podmnožina* $M \subset L$ *je podpriestor lineárneho priestoru* $(L, +, \cdot)$ *vtedy a len vtedy, ak*
(1) $x, y \in M \implies x + y \in M$
(2) $x \in M$, $\alpha \in K \implies \alpha \cdot x \in M$.

Príklady. Ukážte, že
1. $M = \{(x_1, x_2, x_3) \in K^3 : x_1 - x_2 + x_3 = 0\}$ je podpriestor lineárneho priestoru K^3.
2. $M = \{(1, 1, , x) : x \in Z_2\} = \{(1, 1, , 0), (1, 1, , 1)\}$ nie je podpriestor Z_2^3.
3. $M = \{(0, x, y) : x, y \in Z_2\}$ je podpriestor Z_2^3.
4. Priestor všetkých polynómov nad R najviac tretieho stupňa je podpriestor LP všetkých funkcií $R \to R$.
5. Priestor všetkých polynómov nad R tretieho stupňa nie je podpriestor LP všetkých funkcií $R \to R$.

Definícia. Nech $(L, +, \cdot)$ je LP nad poľom K.

a. Ak $x_1, x_2, \dots, x_n \in L$; $\alpha_1, \alpha_2, \dots, \alpha_n \in K$, tak sa $x = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n \in L$ nazýva *lineárna kombinácia* vektorov $x_1, x_2, \dots, x_n$ s koeficientami $\alpha_1, \alpha_2, \dots, \alpha_n$.

b. Ak $\emptyset \neq M \subset L$, tak sa množina všetkých lineárnych kombinácií prvkov z množiny M nazýva *lineárny obal množiny* M. Označujeme ho $\operatorname{span} M$.

c. Konečná podmnožina vektorov $\{x_1, x_2, \dots, x_n\} \subset L$ sa nazýva *lineárne nezávislá*, ak

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = 0 \implies \alpha_1 = \alpha_2 = \cdots = \alpha_n = 0\,.$$

Množina $M \subset L$ sa nazýva lineárne nezávislá, ak je každá konečná podmnožina $M_1 \subset M$ lineárne nezávislá. Množina $M \subset L$, ktorá nie je lineárne nezávislá sa nazýva lineárne závislá.

d. $B \subset L$ sa nazýva báza lineárneho priestoru L, ak
1) $\operatorname{span} B = L$, 2) B je lineárne nezávislá.

Ľahko sa dá ukázať, že platí:

Veta. *Podmnožina $M \subset L$ je podpriestor lineárneho priestoru $(L, +, \cdot)$ vtedy a len vtedy, ak $\exists A \subset L$ také, že $M = \operatorname{span} A$.*

Príklad. Ukážte, že
1. V R^3 je $\mathcal{E} = \{\mathbf{e}_1 = (1, 0, 0), \mathbf{e}_2 = (0, 1, 0), \mathbf{e}_3 = (0, 0, 1)\}$ tzv. štandardná báza.
2. V LP funkcií $f : R \to R$ je množina $\{\sin t, \sin 2t, \sin 3t, \cos t\}$ lineárne nezávislá.
3. $\{x^0, x^1, x^2, \dots\}$ je lineárne nezávislá množina.
3. $\{\sin^2 t, \cos^2 t, \cos 2t\}$ je lineárne závislá množina.

Veta. *Ak v lineárnom priestore existuje n-prvková báza, tak každá $(n{+}1)$-prvková množina je lineárne závislá.*

Dôsledok.
Ak v lineárnom priestore existuje jedna n-prvková báza, tak aj každá jeho báza je n-prvková množina.

Definícia. Nech $(L, +, \cdot)$ je LP nad poľom K. Ak existuje konečná báza priestoru L, tak hovoríme, že L je konečnorozmerný priestor. Počet prvkov bázy sa nazýva dimenzia lineárneho priestoru L a označuje sa $\dim L$.

Príklad. Určte $\dim M$ pre podpriestor
$M = \{(x_1, x_2, x_3, x_4) \in C^4 : x_1 - x_2 = x_2 + x_3 - x_4 = 0\}$.

M je priestor riešení homogénnej sústavy lineárnych rovníc, môžeme vyjadriť:

$$M = \{(b - a, b - a, a, b) : a, b \in C\} = \{a(-1, -1, 1, 0) + b(1, 1, 0, 1) : a, b \in C\} = \operatorname{span}\{(-1, -1, 1, 0), (1, 1, 0, 1)\}\,.$$

Okrem toho

$$a(-1, -1, 1, 0) + b(1, 1, 0, 1) = (b - a, b - a, a, b) = (0, 0, 0, 0) \implies a = b = 0\,.$$

Teda $B = \{(-1, -1, 1, 0), (1, 1, 0, 1)\}$ je lineárne nezávislá množina a $\operatorname{span} B = M$, t.j. B je báza priestoru M. Počet prvkov množiny B je 2, t.j. $\underline{\dim M = 2}$.

Veta. *Nech $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\}$ je usporiadaná báza lineárneho priestoru L nad poľom K. Potom sa každé $\mathbf{x} \in L$ dá jediným spôsobom vyjadriť ako lineárna kombinácia*

$$\mathbf{x} = x_1\mathbf{b}_1 + x_2\mathbf{b}_2 + \cdots + x_n\mathbf{b}_n\,, \quad x_1, x_2, \dots, x_n \in K$$

Dôkaz. Ak by sa dalo $\mathbf{x}$ vyjadriť dvoma spôsobmi:

$$\mathbf{x} = x_1\mathbf{b}_1 + x_2\mathbf{b}_2 + \cdots + x_n\mathbf{b}_n = y_1\mathbf{b}_1 + y_2\mathbf{b}_2 + \cdots + y_n\mathbf{b}_n$$

tak by platilo

$$\begin{aligned}\mathbf{x} - \mathbf{x} &= (x_1\mathbf{b}_1 + x_2\mathbf{b}_2 + \cdots + x_n\mathbf{b}_n) - (y_1\mathbf{b}_1 + y_2\mathbf{b}_2 + \cdots + y_n\mathbf{b}_n)\\ &= (x_1 - y_1)\mathbf{b}_1 + (x_2 - y_2)\mathbf{b}_2 + \cdots + (x_n - y_n)\mathbf{b}_n = \mathbf{0}\end{aligned}$$

Z lineárnej nezávislosti $\mathcal{B}$ potom vyplýva:

$$(x_1 - y_1) = (x_2 - y_2) = \cdots = (x_n - y_n) = 0 \implies x_1 = y_1\,,\ x_2 = y_2\,, \dots\ x_n = y_n\,.$$

Príklad. $A = \begin{pmatrix} 1 & 2 & -1 & 1 & 2 & 2\\ -1 & -2 & 2 & 1 & -3 & -3\\ 1 & 2 & -2 & -1 & 4 & 5\\ 2 & 4 & -1 & 4 & 1 & -1 \end{pmatrix} \in R^{4\times 6}$. Označme
$\mathcal{L}_r(A) = \operatorname{span}\{A_{1*}, A_{2*}, A_{3*}, A_{4*}\}$ (riadkový priestor matice A),
$\mathcal{L}_s(A) = \operatorname{span}\{A_{*1}, A_{*2}, A_{*3}, A_{*4}, A_{*5}, A_{*6}\}$ (stĺpcový priestor).
Určte bázu $\mathcal{B}_r$, $\mathcal{B}_s$ a dimenziu priestorov $\mathcal{L}_r(A)$, $\mathcal{L}_s(A)$.

Riešenie. Najprv pomocou ERO upravíme maticu A na stupňovitú. Vykonaním ERO sa nezmení riadkový priestor (lineárny obal riadkov) matice

$$A = \begin{pmatrix} 1 & 2 & -1 & 1 & 2 & 2\\ -1 & -2 & 2 & 1 & -3 & -3\\ 1 & 2 & -2 & -1 & 4 & 5\\ 2 & 4 & -1 & 4 & 1 & -1 \end{pmatrix} \sim_{\substack{r_2+r_1\\ r_3-r_1\\ r_4-2r_1}} \begin{pmatrix} 1 & 2 & -1 & 1 & 2 & 2\\ 0 & 0 & 1 & 2 & -1 & -1\\ 0 & 0 & -1 & -2 & 2 & 3\\ 0 & 0 & 1 & 2 & -3 & -5 \end{pmatrix} \sim_{\substack{r_3+r_2\\ r_4-r_2}}$$
$$\begin{pmatrix} 1 & 2 & -1 & 1 & 2 & 2\\ 0 & 0 & 1 & 2 & -1 & -1\\ 0 & 0 & 0 & 0 & 1 & 2\\ 0 & 0 & 0 & 0 & -2 & -4 \end{pmatrix} \sim_{r_4+2r_3} \begin{pmatrix} \underline{1} & 2 & -1 & 1 & 2 & 2\\ 0 & 0 & \underline{1} & 2 & -1 & -1\\ 0 & 0 & 0 & 0 & \underline{1} & 2\\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} = B$$

Pivoty sú v prvom, treťom a piatom stĺpci matice B. Keď zmeníme poradie stĺpcov matice A tak, že prvými troma stĺpcami budú A_{*1}, A_{*3}, A_{*5} a vykonáme tie isté ERO, dostaneme

$$\left(\begin{array}{ccc|ccc} 1 & -1 & 2 & 2 & 1 & 2\\ -1 & 2 & -3 & -2 & 1 & -3\\ 1 & -2 & 4 & 2 & -1 & 5\\ 2 & -1 & 1 & 4 & 4 & -1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & -1 & 2 & 2 & 1 & 2\\ 0 & 1 & -1 & 0 & 2 & -1\\ 0 & 0 & 1 & 0 & 0 & 2\\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Vidíme, že každá zo sústav lineárnych rovníc $x_1A_{*1} + x_2A_{*3} + x_3A_{*5} = A_{*2}$;
$x_1A_{*1} + x_2A_{*3} + x_3A_{*5} = A_{*4}$; $\quad x_1A_{*1} + x_2A_{*3} + x_3A_{*5} = A_{*6}$
má práve jedno riešenie, alebo inak $\{A_{*2}, A_{*4}, A_{*6}\} \subset \operatorname{span}\{A_{*1}, A_{*3}, A_{*5}\}$.
Preto je $\operatorname{span}\{A_{*1}, A_{*3}, A_{*5}\} = \operatorname{span}\{A_{*1}, A_{*2}, A_{*3}, A_{*4}, A_{*5}, A_{*6}\} = \mathcal{L}_s$
a $\{A_{*1}, A_{*3}, A_{*5}\}$ je LNZ množina. Teda $\underline{\mathcal{B}_s = \{A_{*1}, A_{*3}, A_{*5}\}\,,\ \dim\mathcal{L}_s(A) = 3}$ (počet pivotov (nenulových riadkov) v matici B).

$\mathcal{L}_r(A) = \mathcal{L}_r(B) \implies \underline{\mathcal{B}_r = \{B_{*1}, B_{*2}, B_{*3}\}\,,\ \dim\mathcal{L}_r(A) = 3}$

Tento postup môžeme použiť na každú maticu $A \in K^{m\times n}$, potom dostaneme

1. $A \in K^{m\times n} \implies \dim\mathcal{L}_r(A) = \dim\mathcal{L}_s(A)$,
2. Ak $N(A) = \{\mathbf{x} \in K^{n\times 1} \colon A\mathbf{x} = 0_{m\times 1}\} \implies \dim N(A) + \dim\mathcal{L}_s(A) = n$.

Definícia. Nech $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ je usporiadaná báza lineárneho priestoru L nad poľom K a $\mathbf{x} \in L$. Potom sa usporiadaná n-tica $[\mathbf{x}]_\mathcal{B} = (x_1, x_2, \ldots, x_n)^\top \in K^{n\times 1}$, pre ktorú platí $\mathbf{x} = x_1\mathbf{b}_1 + x_2\mathbf{b}_2 + \cdots + x_n\mathbf{b}_n$, nazýva n-tica súradníc vektora $\mathbf{x}$ vyhľadom na bázu $\mathcal{B}$.

Príklad. V R^3 je daná báza $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3\}$; $\mathbf{b}_1 = (1,1,0)$, $\mathbf{b}_2 = (1,-1,1)$, $\mathbf{b}_3 = (0,1,1)$ a $\mathbf{x} = (2,1,-1)$. Vypočítajte $[\mathbf{x}]_\mathcal{B}$.

Máme teda určiť čísla x_1, x_2, x_3 tak, aby $\mathbf{x} = x_1\mathbf{b}_1 + x_2\mathbf{b}_2 + x_3\mathbf{b}_3$. Prepíšeme to na sústavu rovníc:

$$x_1\begin{pmatrix}1\\1\\0\end{pmatrix} + x_2\begin{pmatrix}1\\-1\\1\end{pmatrix} + x_3\begin{pmatrix}0\\1\\1\end{pmatrix} = \begin{pmatrix}x_1+x_2\\x_1-x_2+x_3\\x_2+x_3\end{pmatrix} = \begin{pmatrix}2\\1\\-1\end{pmatrix}$$

Túto sústavu riešime úpravou jej rozšírenej matice na redukovanú stupňovitú maticu pomocou ERO.

$$\left(\begin{array}{ccc|c}1&1&0&2\\1&-1&1&1\\0&1&1&-1\end{array}\right) \sim\cdots\sim \left(\begin{array}{ccc|c}1&0&0&2\\0&1&0&0\\0&0&1&-1\end{array}\right) \implies [\mathbf{x}]_\mathcal{B} = \begin{pmatrix}2\\0\\-1\end{pmatrix}.$$

Stĺpce matice sústavy tvoria prvky bázy $\mathcal{B}$, rošírená je o stĺpec vektora $\mathbf{x}$, ktorého súradnice počítame. Po úprave dostaneme jednotkovú maticu roz šírenú o stĺpec súradníc $[\mathbf{x}]_\mathcal{B}$.

Veta. *Nech $(L,+,\cdot)$ je lineárny priestor nad poľom K a $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ je jeho usporiadaná báza. Zobrazenie $\varphi\colon L \to K^{n\times 1}$, $\varphi(\mathbf{x}) = [\mathbf{x}]_\mathcal{B}$ má vlastnosti.*
(1) $\mathbf{x}, \mathbf{y} \in L \implies [\mathbf{x}+\mathbf{y}]_\mathcal{B} = [\mathbf{x}]_\mathcal{B} + [\mathbf{y}]_\mathcal{B}$.
(2) $\mathbf{x} \in L, \alpha \in K \implies [\alpha\mathbf{x}]_\mathcal{B} = \alpha[\mathbf{x}]_\mathcal{B}$.
(3) $[\mathbf{x}]_\mathcal{B} = [\mathbf{y}]_\mathcal{B} \iff \mathbf{x} = \mathbf{y}$.

Prvé dve vlastnosti vyjadrujú, že φ je lineárne zobrazenie. Tretia hovorí, že je to bijektívne zobrazenie.

8. Lineárne operátory

Definícia. Nech $(L,+,\cdot)$ a $(M,\oplus,\odot)$ sú lineárne priestory nad poľom K. Zobrazenie $T\colon L \to M$ sa nazýva lineárny operátor (lineárna transformácia), ak pre $\forall \mathbf{x}, \mathbf{y} \in L$, $\forall \alpha \in K$ platí
(LO1) $T(\mathbf{x}+\mathbf{y}) = (T\mathbf{x}) \oplus (T\mathbf{y})$,
(LO2) $T(\alpha\cdot\mathbf{x}) = \alpha \odot (T\mathbf{x})$.
Bijektívny lineárny operátor sa nazýva izomorfizmus.

Príklady lineárnych operátorov.
1. $T\mathbf{x} = \mathbf{0}$ (nulový operátor),
2. $T\mathbf{x} = \mathbf{x}$ (pre $L = M$ identický operátor)
3. Ak $\mathcal{B}$ je usporiadaná báza priestoru L, tak $T\mathbf{x} = [\mathbf{x}]_\mathcal{B}$ je izomorfizmus L na $K^{n\times 1}$.
4. $T\colon R^3 \to R^2$, $T(x_1,x_2,x_3) = (x_1, x_2+x_3)$ je lineárne
   $T(x_1,x_2,x_3) = (x_1^2, 0)$ nie je lineárne, lebo nesplňa LO1, napr. $T\,2(1,0,0) = (4,0) \neq 2T(1,0,0) = (2,0)$.

Veta. *Ak $T\colon L \to M$ je lineárny operátor, tak*
(1) $T\mathbf{0}_L = \mathbf{0}_M$,
(2) *Pre* $\forall\ \mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$; $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$
$T(\alpha_1\mathbf{x}_1 + \alpha_2\mathbf{x}_2 + \cdots + \alpha_n\mathbf{x}_n) = \alpha_1 T\mathbf{x}_1 + \alpha_2 T\mathbf{x}_2 + \alpha_n T\mathbf{x}_n$.

(2) $\implies$ Lineárny operátor $T\colon L \to M$ je jednoznačne určený svojimi hodnotami v prvkoch bázy priestoru L. Ak $\dim L < \infty$ aj $\dim M < \infty$, tak to umožní reprezentovať lineárny operátor pomocou matice.

Definícia. Nech $T\colon L \to M$ je lineárny operátor. Množina
$\operatorname{Ker} T = \{\mathbf{x} \in L\colon T\mathbf{x} = \mathbf{0}_M\} \subset L$ sa nazýva *jadro* lineárneho operátora T.
Obor hodnôt lineárneho operátora sa označuje $\operatorname{Ran} T = \{T\mathbf{x}\colon \mathbf{x} \in L\} \subset M$.

Veta. *Nech $T\ : L \to M$ je lineárny operátor. Potom platí:*

a) $\operatorname{Ker} T$ *je podpriestor priestoru L.*
b) $\operatorname{Ran} T$ *je podpriestor priestoru M.*
c) *Ak $\mathcal{B}$ je báza priestoru L, tak* $\operatorname{Ran} T = \operatorname{span}\{T\mathbf{b}\colon \mathbf{b} \in \mathcal{B}\}$, *preto* $\dim \operatorname{Ran} T \leq \dim L$.
d) *T je injektívny lineárny operátor vtedy a len vtedy, keď* $\operatorname{Ker} T = \{\mathbf{0}_L\}$.
e) *Ak* $\dim L = \dim M = n$, *tak T je injektívny vtedy a len vtedy keď je T surjektívny.*
f) *Ak* $\dim L = n$, *tak* $\dim \operatorname{Ker} T + \dim \operatorname{Ran} T = n$ *(„základná” veta lineárnej algebry)*
g) *Ak T je bijektívny lineárny operátor,*
tak aj k nemu inverzné zobrazenie T^{-1} je bijektívny lineárny operátor.

Maticová reprezentácia lineárneho operátora $T\colon K^n \to K^m$.

Najskôr pripomenieme označenie: Ak $A = (a_{ij})_{\substack{1\leq i\leq m\\ 1\leq j\leq n}} \in K^{m\times n}$ je matica s m riadkami a n stĺpcami a prvkami a_{ij} z poľa K, tak
jej riadky budeme označovať A_{i*}, $i = 1, 2, \ldots, m$ a stĺpce budeme označovať A_{*j}, $j = 1, 2, \ldots, n$.

Príkladom lineárneho operátora $T\colon K^{n\times 1} \to K^{m\times 1}$ je násobenie pevne zvolenou maticou $A \in K^{m\times n}$, presnejšie

$$\forall \mathbf{x} = (x_1, x_2, \ldots x_n)^\top\ T_A\mathbf{x} = A\mathbf{x} = x_1A_{*1} + x_2A_{*2} + \cdots + x_nA_{*n}\,.$$

Pre prvky štandardnej bázy $\mathcal{E} = \{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n\}$ priestoru $K^{n\times 1}$ tak dostaneme

$$T_A\mathbf{e}_1 = T_A\begin{pmatrix}1\\0\\\vdots\\0\\0\end{pmatrix} = A_{*1},\ T_A\mathbf{e}_2 = T_A\begin{pmatrix}0\\1\\\vdots\\0\\0\end{pmatrix} = A_{*2}, \ldots T_A\mathbf{e}_n = T_A\begin{pmatrix}0\\0\\\vdots\\0\\1\end{pmatrix} = A_{*n}\,.$$

Všimnime si ešte, že prvky usporiadanej bázy $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ sa ako lineárne kombinácie prvkov bázy $\mathcal{B}$ dajú (jednoznačne) vyjadriť ako

$$\begin{aligned}
\mathbf{b}_1 &= 1\cdot\mathbf{b}_1 + 0\cdot\mathbf{b}_2 + \cdots + 0\cdot\mathbf{b}_{n-1} + 0\cdot\mathbf{b}_n\,,\\
\mathbf{b}_2 &= 0\cdot\mathbf{b}_1 + 1\cdot\mathbf{b}_2 + \cdots + 0\cdot\mathbf{b}_{n-1} + 0\cdot\mathbf{b}_n\,,\\
&\vdots\\
\mathbf{b}_{n-1} &= 0\cdot\mathbf{b}_1 + 0\cdot\mathbf{b}_2 + \cdots + 1\cdot\mathbf{b}_{n-1} + 0\cdot\mathbf{b}_n\,,\\
\mathbf{b}_n &= 0\cdot\mathbf{b}_1 + 0\cdot\mathbf{b}_2 + \cdots + 0\cdot\mathbf{b}_{n-1} + 1\cdot\mathbf{b}_n\,,
\end{aligned}$$

a teda majú súradnice

$$[\mathbf{b}_1]_{\mathcal{B}} = \mathbf{e}_1,\ [\mathbf{b}_2]_{\mathcal{B}} = \mathbf{e}_2, \ldots, [\mathbf{b}_n]_{\mathcal{B}} = \mathbf{e}_n\,.$$

Definícia. Nech $\dim L = n$, $\dim M = m$, $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ je usporiadaná báza lineárneho priestoru L a $\mathcal{D}$ je usporiadaná báza lineárneho priestoru M. Matica $[T]_{\mathcal{BD}} = A \in K^{m\times n}$ sa nazýva matica lineárneho operátora $T\colon L \to M$ vzhľadom na bázy $\mathcal{B}$ a $\mathcal{D}$, ak $A_{*j} = [T\mathbf{b}_j]_{\mathcal{D}}$.

Ak $L = M$ a $\mathcal{B}$ je báza priestoru L, tak stručne píšeme $[T]_{\mathcal{B}}$ namiesto $[T]_{\mathcal{BB}}$.

Násobenie matíc a matica $[T]_{\mathcal{BD}}$ sú definované tak, aby platili nasledujúce dve vety:

Veta. *Nech $\mathcal{B}$ je usporiadaná báza lineárneho priestoru L a $\mathcal{D}$ je usporiadaná báza lineárneho priestoru M a $T\colon L \to M$ je lineárny operátor. Potom platí*

$$[T\mathbf{x}]_{\mathcal{D}} = [T]_{\mathcal{B}\mathcal{D}}[\mathbf{x}]_{\mathcal{B}} \qquad \forall\, \mathbf{x} \in L\,.$$

Dôkaz tejto (aj nasledujúcej) vety tu vynechám, ale odporúčam ho urobiť (priamym výpočtom) v prípade $\dim L = 3$, $\dim M = 2$, teda $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3\}$, $\mathcal{D} = \{\mathbf{d}_1, \mathbf{d}_2\}$.

Veta. *Nech $\mathcal{B}_1$, $\mathcal{B}_2$, $\mathcal{B}_3$ sú usporiadané bázy lineárnych priestorov L_1, L_2 a L_3; $T_1\colon L_1 \to L_2$, $T_2\colon L_2 \to L_3$ sú lineárne operátory a T_2T_1 znamená z nich zložený operátor, $T_2T_1\colon L_1 \to L_3$. Potom platí*

$$[T_2T_1]_{\mathcal{B}_1\mathcal{B}_3} = [T_2]_{\mathcal{B}_2\mathcal{B}_3}[T_1]_{\mathcal{B}_1\mathcal{B}_2}\,,$$

t.j. násobenie matíc zodpovedá skladaniu lineárnych operátorov.

Príklad. Nech $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3\}$, $\mathcal{D} = \{\mathbf{d}_1, \mathbf{d}_2, \mathbf{d}_3\}$ sú bázy lineárneho priestoru L, potom má identický operátor $I\colon L \to L$, $I\mathbf{x} = \mathbf{x}$ matice:

$$[I]_{\mathcal{B}} = [I]_{\mathcal{D}} = I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$
$$A = [I]_{\mathcal{B}\mathcal{D}}\,,\ A_{*1} = [\mathbf{b}_1]_{\mathcal{D}}\,,\ A_{*2} = [\mathbf{b}_2]_{\mathcal{D}}\,,\ A_{*3} = [\mathbf{b}_3]_{\mathcal{D}}\,;$$
$$B = [I]_{\mathcal{D}\mathcal{B}}\,,\ B_{*1} = [\mathbf{d}_1]_{\mathcal{B}}\,,\ B_{*2} = [\mathbf{d}_2]_{\mathcal{B}}\,,\ B_{*3} = [\mathbf{d}_3]_{\mathcal{B}}\,,$$

Ak $\mathcal{B}$ a $\mathcal{D}$ sú bázy konečnorozmerného lineárneho priestoru L, matica $[I]_{\mathcal{B}\mathcal{D}}$ sa nazýva matica prechodu od bázy $\mathcal{B}$ k báze $\mathcal{D}$. Súradnice $[\mathbf{x}]_{\mathcal{B}}$ vektora $\mathbf{x}$ vzhľadom na bázu $\mathcal{B}$ sa násobením maticou $[I]_{\mathcal{B}\mathcal{D}}$ zmenia na súradnice toho istého vektora vzhľadom na bázu $\mathcal{D}$. Ak $\mathcal{D}$ je štandardná báza priestoru $K^{n\times 1}$, tak stĺpce matice $[I]_{\mathcal{B}\mathcal{D}}$ sú priamo vektory $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$, ktoré tvoria bázu $\mathcal{B}$.

Ešte poznamenajme, že ak $P = [I]_{\mathcal{B}\mathcal{D}}$, tak $P^{-1} = [I]_{\mathcal{D}\mathcal{B}}$.

Príklad. $B = \{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3\}$, $D = \{\mathbf{d}_1, \mathbf{d}_2\}$ Napíšte matice $T_{\mathcal{E}_3\mathcal{E}_2}$ a T_{BD}, ak $T\colon R^3 \to R^2$,

$$T(x_1, x_2, x_3) = (x_2 + x_3\,,\ x_1 - x_2 + 2x_3)$$
$$\mathbf{b}_1 = (1, 0, -2)\,, \quad \mathbf{b}_2 = (1, 1, 0)\,, \quad \mathbf{b}_3 = (1, 0, 3)\,, \qquad \mathbf{d}_1 = (1\,,\,2)\,, \quad \mathbf{d}_2 = (2\,,\,1)\,.$$

Určte $\dim \operatorname{Ker} T, \dim \operatorname{Ran} T$

Riešenie. Stĺpce matice $[T]_{BD}$ sú $[T\mathbf{b}_1]_D$, $[T\mathbf{b}_2]_D$, $[T\mathbf{b}_3]_D$. Najprv teda vypočítame:

$$T\mathbf{b}_1 = T(1, 0, -2) = (-2, -3)\,,\ T\mathbf{b}_2 = T(1, 1, 0) = (1, 0)\,,\ T\mathbf{b}_3 = T(1, 0, 3) = (3, 7)$$

a hľadáme súradnice $[T\mathbf{b}_1]_D$, $[T\mathbf{b}_2]_D$, $[T\mathbf{b}_3]_D$:

$$\left(\begin{array}{cc|ccc} 1 & 2 & -2 & 1 & 3 \\ 2 & 1 & -3 & 0 & 7 \end{array}\right)_{R_2 - 2R_1} \sim \left(\begin{array}{cc|ccc} 1 & 2 & -2 & 1 & 3 \\ 0 & -3 & 1 & -2 & 1 \end{array}\right)_{R_2/-3} \sim \left(\begin{array}{cc|ccc} 1 & 2 & -2 & 1 & 3 \\ 0 & 1 & -1/3 & 2/3 & -1/3 \end{array}\right)_{R_1 - 2R_2}$$
$$\sim \left(\begin{array}{cc|ccc} 1 & 0 & -4/3 & -1/3 & 11/3 \\ 0 & 1 & -1/3 & 2/3 & -1/3 \end{array}\right), \quad [T]_{BD} = \begin{pmatrix} -4/3 & -1/3 & 11/3 \\ -1/3 & 2/3 & -1/3 \end{pmatrix}.$$

$T_{\mathcal{E}_2\mathcal{E}_3} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & -1 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & -1 & 2 \\ 0 & 1 & 1 \end{pmatrix}$ (má dva pivoty) $\implies \dim \operatorname{Ran} T = 2$,
$\dim \operatorname{Ker} T + \dim \operatorname{Ran} T = 3 \implies \dim \operatorname{Ker} T = 1$.

Zmena bázy sa dá použiť pri riešení sústavy lineárnych diferenciálnych rovníc:

Príklad*. Riešte sústavu diferenciálnych rovníc (neznáme sú funkcie $f_1, f_2\colon R \to R$)

$$\begin{aligned} f_1' &= f_1 - 3f_2\,, \\ f_2' &= -3f_1 + f_2 \end{aligned} \qquad \text{alebo pomocou matice} \quad \mathbf{f}' = \begin{pmatrix} f_1' \\ f_2' \end{pmatrix} = \begin{pmatrix} 1 & -3 \\ -3 & 1 \end{pmatrix} \begin{pmatrix} f_1 \\ f_2 \end{pmatrix}$$

Matica $A = \begin{pmatrix} 1 & -3 \\ -3 & 1 \end{pmatrix}$ je maticou oprátora $T\mathbf{x} = A\mathbf{x}$ vzhľadom na štandardnú bázu $\mathcal{E}$. Nájdime maticu toho istého operátora vzhľadom na bázu $\mathcal{B} = \{\mathbf{b}_1\mathbf{b}_2\}$, $\mathbf{b}_1 = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$, $\mathbf{b}_2 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$:

$$T_{\mathcal{B}} = I_{\mathcal{E}\mathcal{B}} T_{\mathcal{E}} \underbrace{I_{\mathcal{B}\mathcal{E}}}_{P} = P^{-1}AP$$

Vypočítame stĺpce matice $D = T_{\mathcal{B}}$:
$T\mathbf{b}_1 = A\mathbf{b}_1 = \begin{pmatrix} 1 & -3 \\ -3 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 4 \\ -4 \end{pmatrix} = 4\,\mathbf{b}_1$,
$T\mathbf{b}_2 = \begin{pmatrix} 1 & -3 \\ -3 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} -2 \\ -2 \end{pmatrix} = -2\,\mathbf{b}_2$
Odtiaľ dostávame $T_{\mathcal{B}} = D = \begin{pmatrix} 4 & 0 \\ 0 & -2 \end{pmatrix}$ a

$$D = P^{-1}AP \implies PDP^{-1} = A$$

a danú sústavu lineárnych diferenciálnych rovníc môžeme napísať

$$\mathbf{f}' = PDP^{-1}\mathbf{f} \implies P^{-1}\mathbf{f}' = DP^{-1}\mathbf{f}\,.$$

Teraz použijeme substitúciu $\mathbf{g} = P^{-1}\mathbf{f} = \begin{pmatrix} g_1 \\ g_2 \end{pmatrix}$ a riešime sústavu

$$\mathbf{g}' = \begin{pmatrix} g_1' \\ g_2' \end{pmatrix} = D\mathbf{g} \qquad \text{t.j.} \qquad \begin{aligned} g_1' &= 4g_1 \\ g_2' &= -2g_2 \end{aligned}$$

a riešime dve rovnice s jednou neznámou a riešením je každá dvojica funckií $g_1(x) = k_1e^{4x}$, $g_2(x) = k_2e^{-2x}$.

Riešenie pôvodnej sústavy je potom

$$\mathbf{g} = P^{-1}\mathbf{f} \implies \mathbf{f} = P\mathbf{g} = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} k_1e^{4x} \\ k_2e^{-4x} \end{pmatrix} = k_1e^{4x}\mathbf{b}_1 + k_2e^{-2x}\mathbf{b}_2\,.$$

Dá sa ukázať, že priestor všetkých riešení danej sústavy je dvojrozmerný a jeho báza je $\left\{e^{4x}\mathbf{b}_1,\, e^{-2x}\mathbf{b}_2\right\}$.