

1 POLIA Q, R, C, Z_p

Definícia. Poľom K nazývame neprázdnu množinu, ktorá obsahuje dva (osobitné) prvky $0, 1 \in K$, ak sú na K definované operácie

$+: K \times K \rightarrow K$ (sčítanie),

$\cdot: K \times K \rightarrow K$ (násobenie),

pre ktoré platí: $\forall a, b, c \in K$

K1 $a + b = b + a$ (komutatívnosť sčítania)

K2 $(a + b) + c = (a + b) + c$ (asociatívnosť sčítania)

K3 $a + 0 = a$ (0 je neutrálny prvok vzhľadom na sčítanie)

K4 $\forall a \in K \exists b \in K: a + b = 0$ ($b = -a$, opačný prvok vzhľadom na sčítanie)

K5 $a \cdot b = b \cdot a$ (komutatívnosť násobenia)

K6 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (asociatívnosť násobenia)

K7 $a \cdot (b + c) = a \cdot b + a \cdot c$ (distributívnosť)

K8 $1 \cdot a = a$

K9 $\forall a \neq 0 \exists b \in K: a \cdot b = 1$ ($b = a^{-1}$ je inverzný prvok k prvku a)

K10 $0 \neq 1$

Lahko 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

Zopakujeme stručne vlastnosti komplexných čísel. Množinu všetkých reálnych čísel budem označovať R , imaginárnu jednotku i (i je riešenie rovnice $x^2 + 1 = 0$, t.j. platí $i^2 = -1$). Potom množinu všetkých komplexných čísel skonštruujeme tak, že k reálnym číslam pridáme všetky výsledky násobení a sčítaní reálnych čísel a čísla i :

$$C = \{x + iy : x, y \in R\}. \quad x = \operatorname{Re} z \text{ je reálna a } y = \operatorname{Im} z \text{ imaginárna časť čísla } z = x + iy.$$

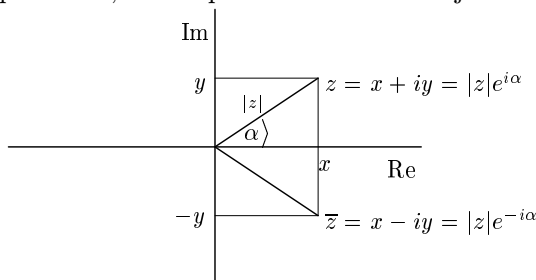
Aritmetické operácie v C ($\bar{z} = x - iy$ sa nazýva číslo komplexne združené k $z = x + iy$):

$$\text{sčítanie: } (x_1 + iy_1) + (x_2 + iy_2) = (x_1 + x_2) + i(y_1 + y_2),$$

$$\text{násobenie: } (x_1 + iy_1)(x_2 + iy_2) = (x_1x_2 - y_1y_2) + i(x_1y_2 + y_1x_2)$$

$$\text{delenie: } \frac{x_1 + iy_1}{x_2 + iy_2} = \frac{x_1 + iy_1}{x_2 + iy_2} \frac{x_2 - iy_2}{x_2 - iy_2} = \frac{x_1x_2 + y_1y_2}{x_2^2 + y_2^2} + i \frac{y_1x_2 - x_1y_2}{x_2^2 + y_2^2}, \quad (x_2 + iy_2 \neq 0)$$

Pripomeňme, že komplexné čísla znázorňujeme v Gaussovej rovine:



$|z| = \sqrt{x^2 + y^2}$ sa nazýva absolútna hodnota a orientovaný uhol α sa nazýva argument komplexného čísla $z = x + iy$ (argument čísla $c = 0$ nie je definovaný).
 $e^{i\alpha} = \cos \alpha + i \sin \alpha$

Základné vlastnosti komplexných čísel zhrnieme v nasledujúcich tvrdeniach:

Moivreova veta:

Pre všetky $r_1, r_2 > 0$, $\alpha_1, \alpha_2 \in R$ platí: $r_1 e^{i\alpha_1} \cdot r_2 e^{i\alpha_2} = r_1 r_2 e^{i(\alpha_1 + \alpha_2)}$ (absolútne hodnoty sa násobia; argumenty sčítajú).

vlastnosti absolútnej hodnoty Pre $\forall z_1, z_2 \in C$ platí:

$$(1) |z_1 + z_2| \leq |z_1| + |z_2| \text{ (trojuholníková nerovnosť),}$$

$$(2) |z_1 z_2| = |z_1| |z_2|$$

vlastnosti komplexne združených čísel Pre $\forall z, z_1, z_2 \in C$ platí:

$$(3) \overline{(z_1 + z_2)} = \overline{z_1} + \overline{z_2}$$

$$(4) \overline{(z_1 z_2)} = \overline{z_1} \overline{z_2}$$

$$(5) z\overline{z} = |z|^2.$$

$$(6) \operatorname{Re} z = \frac{1}{2}(z + \overline{z}), \operatorname{Im} z = \frac{1}{2i}(z - \overline{z}) = \frac{i}{2}(\overline{z} - z)$$

Zopakujeme ešte, ako sa rieši binomická rovnica: $z^n = c$, $n \in \mathbb{N}$, $c \in \mathbb{C}$, $c \neq 0$:

Pravú stranu napíšeme v goniometrickom tvare $c = |c|e^{i\alpha}$ a použijeme Moivreovu vetu:

$$z^n = |c|e^{i\alpha}$$

$$z^n = |c|e^{i(\alpha+2k\pi)}$$

$$z_k = \sqrt[n]{|c|}e^{i\left(\frac{\alpha}{n}+k\frac{2k\pi}{n}\right)}, k = 0, 1, 2, \dots, n-1$$

Úlohy.

1. Dokážte vlastnosti (1)–(6)

2. Riešte binomické rovnice:

$$(a) z^4 = -4, \quad (b) z^6 = -8, \quad (c) z^4 = -2 + 2\sqrt{3}.$$

Korene vyjadrite v algebraickom aj goniometrickom tvare a znázornite.

3. číslo c vyjadrite v algebraickom a v goniometrickom tvare

$$(a) c = i^{4k+m}, k \in \mathbb{Z}, m = 0, 1, 2, 3. \quad (b) c = \left(\frac{1+i}{1-i}\right)^{2007},$$

POLIA Z_p

Najprv pripomeniem (z predmetu Diskretna matematika), že celé čísla majú nasledujúcu vlastnosť (delenie so zvyškom):

Ak $n \in \mathbb{Z}$, $m \in \mathbb{N}$, tak $\exists! a \in \mathbb{Z}$, $r \in \{0, 1, \dots, m-1\}$, 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 $a, b \in \mathbb{Z}$ sú kongruentné modulo m ($a \equiv b \pmod{m}$), ak dostaneme po ich delení číslom m rovnaký zvyšok, t.j

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

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 $a \in \{0, 1, 2, 3, 4, 5\}$, pre ktoré $2a \equiv 1 \pmod{6}$.

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

1. reflexívnosť: $k \equiv k \pmod{m}$, $\forall k \in \mathbb{Z}$,

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 $k_1, k_2; \ell_1, \ell_2 \in \mathbb{Z}$:

$$\left. \begin{array}{l} k_1 \equiv k_2 \pmod{m} \\ \ell_1 \equiv \ell_2 \pmod{m} \end{array} \right\} \implies \begin{array}{l} k_1 + k_2 \equiv \ell_1 + \ell_2 \pmod{m}, \\ k_1 k_2 \equiv \ell_1 \ell_2 \pmod{m}. \end{array}$$

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

$$\begin{aligned} k_1 \ell_1 - k_2 \ell_2 &= k_1 \ell_1 - k_2 \ell_1 + k_2 \ell_1 - k_2 \ell_2 \\ &= (k_1 - k_2) \ell_1 + k_2 (\ell_1 - \ell_2) \\ k_1 &\equiv k_2 \pmod{m} \\ \ell_1 &\equiv \ell_2 \pmod{m} \end{aligned} \implies m | k_1 \ell_1 - k_2 \ell_2 \implies k_1 \ell_1 \equiv k_2 \ell_2 \pmod{m}.$$

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

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

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

Veta. Z_n vtedy a len vtedy keď je n prvočíslo.

3. VLASTNOSTI POLYNÓMOV S KOMPLEXNÝMI KOEFICIENTAMI A S KOEFICIENTAMI V POLI Z_p

V M1 sme polynómom nazývali funkciu $f: C \rightarrow C$ tvaru $f(z) = c_n z^n + c_{n-1} z^{n-1} + \dots + c_1 z + c_0$, kde $c_0, c_1, \dots, c_n, c_n \neq 0$ sú dané komplexné čísla (koeficienty polynómu f). Potom sme (napr. na rozklad racionálnej funkcie na parciálne zlomky) používali fakt, že koeficienty sú určené jednoznačne. To nie je pravda pre polynómy s koeficientami v poliach Z_p .

Príklad. Vzťahy $f(x) = x^2 + x + 1$ a $g(x) = x^3 + x^2 + 1$ určujú tú istú funkciu $h: Z_2 \rightarrow Z_2$, t.j. $h(0) = f(0) = g(0) = 1$, $h(1) = f(1) = g(1) = 1$

Takže definovať polynóm nad poľom K (t.j. s koeficientami z K) pomocou funkcie $K \rightarrow K$ nie je možné. Preto zavedieme polynóm ako formálny výraz

$$f(x) = c_0 + c_1 x + \dots + c_n x^n, c_0, c_1, \dots, c_n \in K,$$

pričom násobenie, sčítanie, odčítanie aj delenie je definované formálne rovnako ako pre polynómy s komplexnými koeficientami. Ak $n \neq 0$, tak hovoríme, že f má *stupeň* n . Množinu všetkých polynómov nad poľom K , budeme označovať $P(K)$. $(P(K); +, \cdot)$ má všetky vlastnosti poľa okrem K9 (existencia inverzného prvku), pričom *jednotkový prvok* je polynóm $e(x) = 1$, *nulový prvok* polynóm, ktorý má všetky koeficienty nulové.

Každý polynóm z $P(K)$ určuje funkciu $K \rightarrow K$ (ale rôzne polynómy môžu určovať tú istú funkciu). Preto budeme rovnako ako pre $f \in P(C)$ označovať $f(k)$ hodnotu polynómu f v bode $k \in K$, *koreň* polynómu je $k \in K$, pre ktoré $f(k) = 0$.

Pole komplexných čísel je algebraicky uzavreté, t.j. platí v ňom

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

Veta. Ak $f(z)$ je polynóm nad C a je dané $c \in C$, tak zvyšok po delení $f(z) : (z - c)$ je číslo $f(c)$; špeciálne, ak c je koreň polynómu f , tak sa dá deliť $f(z) : (z - c)$ bezo zvyšku.

Dôkaz. Delením dostaneme podiel $g(z)$ a zvyšok je polynóm $r(z)$, st $r < \text{st}(z - c) = 1$. Teda $r(z) = r$ je konštanta a $f(z) = (z - c)(g(z) + r) \implies f(c) = (c - c)g(c) + r = r$.

Výpočet koeficientov polynómu g (podielu) a hodnoty zvyšku, t.j. $f(c)$ sa dá urobiť pomocou Hornerovj schémy.

Z predchádzajúcej vety vyplýva pre polynómy nad C (aj nad každým algebraicky uzavretým poľom)

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

$$a_n z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0 = a_n (z - c_1)^{k_1} (z - c_2)^{k_2} \dots (z - c_m)^{k_m}, \text{ kde } k_1 + k_2 + \dots + k_m = n,$$

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

Definícia.

1. Nech K je pole a $m \geq 0$ je celé číslo. Prvok $c \in K$ je koreň násobnosti m polynómu $f \in P(K)$, ak existuje polynóm $g \in P(K)$, pre ktorý

$$f(x) = g(x)(x - c)^m, \quad g(c) \neq 0.$$

2. Polynóm $f \in P(K)$ sa nazýva *ireducibilný*, ak sa nedá vyjadriť ako súčin $f(x) = f_1(x)f_2(x)$ polynómov stupňa ≥ 1 .

3. $f_1 \in P(K)$ je deliteľom $f \in P(K)$ (označenie $f_1 | f$), ak existuje $f_2 \in P(K)$ také, že $f(x) = f_1(x)f_2(x)$.

4. Polynóm $g \in P(K)$ je m -násobný ireducibilný deliteľ polynómu $f \in P(K)$, ak

$$g^m | f, \quad g \text{ je ireducibilný a } g^{m+1} \text{ nie je deliteľom polynómu } f.$$

Úlohy.

2.1a. Napíšte zvyšok po delení $(z^{10} - z^5 + 1) : (z + i)$

2.1b. Napíšte rozklad nad C polynómov $f_1(z) = z^6 + 1$, $f_2(z) = z^6 - 1$, $f_3(z) = z^2 + z + 1$, $f_4(z) = 2z^2 + 2z + 1$.

Popíšeme algoritmus na určenie najväčšieho spoločného deliteľa dvoch polynómov f_1, f_2 ($\gcd(f_1, f_2)$). Je založený na nasledujúcom jednoduchom tvrdení:

Ak f, g, p, r sú polynómy a platí $f(z) = g(z)p(z) + r(z)$, tak $\gcd(f, g) = \gcd(g, r)$. Stačí si uvedomiť, že

$$\left. \begin{aligned} g(z) &= d(z)g_1(z), \\ r(z) &= d(z)r_1(z) \end{aligned} \right\} \implies f(z) = d(z)g_1(z)p(z) + d(z)r_1(z) = d(z)[g_1(z)p(z) + r_1(z)],$$

teda každý spoločný deliteľ d polynómov g, r je deliteľom všetkých troch polynómov f, g, r . Podobne, ak d je deliteľom f aj g , tak je aj deliteľom polynómu $r(z) = f(z) - g(z)p(z)$.

Euklidov Algoritmus.

Vstupom je dvojica nekonštatných polynómov $f_1(z), f_2(z)$; môžeme predpokladať, že $\text{st } f_1 \geq \text{st } f_2$.

Delením $f_1(z) : f_2(z)$ dostaneme podiel $p(z)$ a zvyšok $f_3(z)$

$f_1(z) = p_1(z)f_2(z) + f_3(z)$, $\text{st } f_3 < \text{st } f_2$. Ak $f_3(z) = 0$, tak $\text{gcd}(f_1, f_2) = f_2$ a skončíme. V opačnom prípade $\text{gcd}(f_1, f_2) = \text{gcd}(f_2, f_3)$ a opakujeme to isté s novými dvojicami polynómov $[(f_2, f_3); (f_3, f_4); \dots]$

Pretože $\text{st } f_1 > \text{st } f_2 > \text{st } f_3 \dots$, po $k \leq n = \text{st } f_2$ krokoch dostaneme nulový polynóm $f_{k+2} = 0$, $f_{k+1} \neq 0$. Posledný nenulový zvyšok je $f_{k+1} = \text{gcd}(f_1, f_2)$.

Nasledujúce tvrdenie sa dá jednoducho dokázať pomocou Euklidovho algoritmu. Využijeme ho neskoršie pri jednej zo základných úloh lineárnej algebry — konštrukcii Jordanovho tvaru matice.

Veta. *Nech $f(z), g(z)$ sú polynómy, potom existujú polynómy $a(z), b(z)$ také, že $\text{gcd}(f, g) = a(z)f(z) + b(z)g(z)$.*

Polia a vektorové (lineárne) priestory.

Príkladom nekonečných polí je pole všetkých racionálnych čísel Q , reálnych čísel R , komplexných čísel C .

Množinu $Z_n = \{0, 1, \dots, n-1\}$ všetkých zvyškov po delení prirodzeného čísla číslom n spolu s operáciami $\oplus, \odot$: $a \oplus b = c \iff n \mid [c - (a + b)]$; $a \odot b = c \iff n \mid [c - (a \cdot b)]$ spĺňa vlastnosti 1–8 a 10. Ku každému nenulovému prvku však nemusí existovať inverzný. Je známe, že Z_n je pole práve vtedy, keď je n prvočíslo. Pripomeňme ešte označenie: Ak a, b sú prirodzené čísla, ktoré po delení číslom n dávajú rovnaký zvyšok (teda $n \mid (a - b)$), tak píšeme $a \equiv b \pmod n$. Z_n môžeme stotožniť s rozkladom množiny Z všetkých celých čísel na zvyškové triedy:

$$[0] = \{n \cdot k : k \in Z\}, [1] = \{n \cdot k + 1 : k \in Z\}, \dots, [n-1] = \{n \cdot k + (n-1) : k \in Z\}$$

$$Z = \bigcup_{k=0}^{n-1} [k], \quad \text{pričom zrejme } a, b \in [k] \implies a \equiv b \pmod n$$

Tento rozklad sa označuje $Z/(n)$. Podobná konštrukcia sa používa na rozširovanie polí.

Definícia. Pole K sa nazýva algebraicky uzavreté ak má každý polynóm $f \in P(K)$ stupňa apoň 1 koreň v poli K .

Napríklad pole komplexných čísel je algebraicky uzavreté rozšírenie poľa reálnych čísel: $x^2 + 1$ je v poli R ireducibilný (nemá koreň). Označíme $P(R)$ množinu všetkých polynómov s reálnymi koeficientami. Pole komplexných čísel môžeme potom stotožniť s množinou tried rozkladu $P(R)$ podľa ekvivalencie

$$f(x) \equiv g(x) \pmod{(x^2 + 1)} \iff x^2 + 1 \text{ je deliteľom } f(x) - g(x) \quad \text{t.j. } C \cong P(R)/(x^2 + 1)$$

$x^2 + 1 \equiv 0 \pmod{(x^2 + 1)} \implies x^2 \equiv -1 \pmod{(x^2 + 1)}$. Keď označíme triedu $[x] = i$ dostaneme $[x]^2 = -1$. Komplexné čísla sa teda dajú stotožniť s množinou zvyškov po delení polynómov s reálnymi koeficientami polynómom $x^2 + 1$, teda s množinou $P_1(R)$ všetkých reálnych polynómov najviac prvého stupňa.

Príklad. Polynóm $f(x) = x^2 + x + 1$ je ireducibilný polynóm nad Z_2 . Popíšte pole $P(Z_2)/(x^2 + x + 1)$

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

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

Pre toto pole napíšte tabuľku násobenia a sčítania.

Viacnásobné ireducibilné delitele polynómu.

Euklidov algoritmus sa dá použiť na zistenie, či má daný polynóm nad poľom K viac ako jednonásobný ireducibilný deliteľ:

Najprv definujeme „algebraickú“ **deriváciu polynómu**:

$$(c_n x^n + c_{n-1} x^{n-1} + \dots + c_1 x + c_0)' = n c_n x^{n-1} + (n-1) c_{n-1} x^{n-2} + \dots + c_1.$$

Ľahko sa dá ukázať, že platí pre $\forall f, g \in P(k), m \in N$

$$[f(x)g(x)]' = f'(x)g(x) + f(x)g'(x), \quad [f(x)^m]' = m[f(x)]^{m-1}f'(x).$$

Veta. *Polynóm $f(x)$ má aspoň dvojnásobný ireducibilný deliteľ vtedy a len vtedy, ak $\text{gcd}(f, f')$ je polynóm stupňa aspoň jeden.*

Dôkaz. Predpokladajme, že $g(x)$ je aspoň dvojnásobný ireducibilný deliteľ polynómu f , t.j. existuje polynóm $h(x)$, pre ktorý $a \ f(x) = [g(x)]^2 h(x)$. Potom $f'(x) = 2[g(x)]g'(x)h(x) + [g(x)]^2 h'(x) = g(x)[2g'(x)h(x) + g(x)h'(x)]$, takže $g \mid \text{gcd}(f, f')$.

Ak $g(x)$ je ireducibilný deliteľ polynómu f , t.j. $f = gh$, tak $f' = g'h + gh'$. Ak je g aj deliteľom f' , tak $g \mid (g'h)$. Pretože g je ireducibilný a delí súčin $g \mid (g'h)$ vieme, že je buď deliteľom polynómu g' alebo h . Prvá možnosť nenastane, lebo stupeň g' je menší ako stupeň polynómu g . Teda $g \mid h \implies g^2 \mid f$.

Podobne sa dá dokázať

Veta. Nech K je pole a $k > 1$ je prirodzené číslo. Polynom $f(x) \in P(K)$ je deliteľný k -tou mocninou ireducibilného polynómu $g(x)$ vtedy a len vtedy keď $g^{k-1} \mid \gcd(f, f')$.

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) $z^3 - 2z^2 + 2z - 1$, (e) $z^3 + 8i$, (f) $z^3 - 8i$
- 2.2 $f_1, f_2 \in P(C)$. Napíšte $\gcd(f_1(z), f_2(z))$ v tvare $a_1(z)f_1 + a_2(z)f_2(z)$ a nájdite (najmenší spol. násobok) $\text{lcm}(f_1(z), f_2(z))$ pre
 (a) $f_1(z) = z^3 - z^2 + 2$, $f_2(z) = z^4 + z^3 + z^2 - 1$;
 (b) $f_1(z) = 2z^4 + z^3 + z^2 - 2$, $f_2(z) = z^3 + 2z^2 + 3z + 2$;
 (c) $f_1(z) = z^4 + (1 - i)z^3 + (-2 - 2i)z^2 + (2i - 1)z + i$, $f_2(z) = z^3 + (2 - i)z^2 + (2 - 2i)z - 2i$;
 (d) $f_1(z) = z^4 + z^3 + 2z^2 + 1$, $f_2(z) = z^3 - 2z^2 + z - 2$.
- 2.4 Zistite, či má daný polynóm $f \in P(C)$ koreň násobnosti väčšej ako 1.
 (a) $f(z) = 4z^3 - 8z^2 - 11z - 3$, (b) $f(z) = z^3 - 2z^2 + 3z - 3$, (c) $f(z) = z^4 - 2iz^3 - 2iz - 1$.
- 2.5 Pre každý polynóm z cvičenia 2.4 napíšte polynóm, ktorý má tie isté korene, ale všetky sú násobnosti 1.
- 2.6 Dokážte tvrdenia o derivácii súčtu a súčinu polynómov nad poľom K :
 $[f(x) + g(x)]' = f'(x) + g'(x)$, $[f(x)g(x)]' = f'(x)g(x) + f(x)g'(x)$
 Pozor! Nemôžete použiť vety o limitách.
- 2.7 Zistite, či sa v (kanonickom) rozklade polynómu $f(x)$ nad poľom K nachádza aspoň druhá mocnica ireducibilného polynómu.
 a) $f(x) = x^5 + x^4 + x^3 + x^2 + x + 1$, $K = Z_2$,
 b) $f(x) = x^5 + x^4 + x^3 + x^2 + x + 1$, $K = Z_3$, (c) $f(x) = x^5 + x^4 + 2x^2 + 2$, $K = Z_3$.

Lineárne priestory.

Definícia. Trojica $(L, \oplus, \odot)$ sa nazýva lineárny (vektorový) priestor nad poľom $(K, +, \cdot)$, ak L je neprázdna množina (vektorov) a $\oplus: L \times L \rightarrow L$; $\odot: K \times L \rightarrow L$ 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) $(\alpha + \beta) \odot x = (\alpha \odot x) \oplus (\beta \odot x)$
 (L7) $(\alpha\beta) \odot x = \alpha \odot (\beta \odot x)$
 (L8) $1 \odot x = x$

Príkladmi lineárnych priestorov nad R sú priestory funkcií $f: A \rightarrow R$ s obvyklými operáciami sčítania funkcií a násobenia funkcie reálnym číslom. Rovnako aj množina všetkých funkcií $f: A \rightarrow K$ je lineárny 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. 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

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

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
 $x = \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n \in L$ 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 $\text{span } M$.
- c. Konečná podmnožina vektorov $\{x_1, x_2, \dots, x_n\} \subset L$ sa nazýva *lineárne nezávislá*, ak

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

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) $\text{span } B = L$,
- 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 $M = \text{span } A$.

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 $f: R \rightarrow R$ 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 $M = \{(x_1, x_2, x_3, x_4) \in C^4: x_1 - x_2 = 2x_3 - x_4 = 0\}$.

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

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

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

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

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

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

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

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

tak by platilo

$$\mathbf{x} - \mathbf{x} = (x_1 \mathbf{b}_1 + x_2 \mathbf{b}_2 + \dots + x_n \mathbf{b}_n) - (y_1 \mathbf{b}_1 + y_2 \mathbf{b}_2 + \dots + y_n \mathbf{b}_n) = (x_1 - y_1) \mathbf{b}_1 + (x_2 - y_2) \mathbf{b}_2 + \dots + (x_n - y_n) \mathbf{b}_n = \mathbf{0}$$

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

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

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

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

Stĺpce matice sústavy tvoria prvky bázy $\mathcal{B}$, roširená 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 $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\}$ je jeho usporiadaná báza. Zobrazenie $\varphi: L \rightarrow K^{n \times 1}$, $\varphi(\mathbf{x}) = [\mathbf{x}]_{\mathcal{B}}$ 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.

LINEÁRNE OPERÁTORY

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

$$(LO1) \quad T(\mathbf{x} + \mathbf{y}) = (T\mathbf{x}) \oplus (T\mathbf{y}),$$

$$(LO2) \quad T(\alpha \cdot \mathbf{x}) = \alpha \odot (T\mathbf{x}).$$

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. $T: R^3 \rightarrow R^2$, $T(x_1, x_2, x_3) = (x_1, x_2 + x_3)$ je lineárne
 $T(x_1, x_2, x_3) = (x_1^2, 0)$ nie je lineárne, lebo nesplňa LO1, napr. $T2(1, 0, 0) = (4, 0) \neq 2T(1, 0, 0) = (2, 0)$.

Veta. Ak $T: L \rightarrow M$ je lineárny operátor, tak

- 1) $T\mathbf{0}_L = \mathbf{0}_M$,
- 2) Pre $\forall \mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n; \alpha_1, \alpha_2, \dots, \alpha_n \in K$
 $T(\alpha_1 \mathbf{x}_1 + \alpha_2 \mathbf{x}_2 + \dots + \alpha_n \mathbf{x}_n) = \alpha_1 T\mathbf{x}_1 + \alpha_2 T\mathbf{x}_2 + \dots + \alpha_n T\mathbf{x}_n$.

(2) $\implies$ Lineárny operátor $T: L \rightarrow M$ 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 $T: L \rightarrow M$ je lineárny operátor. Množina $\text{Ker } T = \{\mathbf{x} \in L: T\mathbf{x} = \mathbf{0}_M\} \subset L$ sa nazýva jadro lineárneho operátora T .

Obor hodnôt lineárneho operátora sa označuje $\text{Ran } T = \{T\mathbf{x}: \mathbf{x} \in L\} \subset M$.

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

- a) $\text{Ker } T$ je podpriestor priestoru L .
- b) $\text{Ran } T$ je podpriestor priestoru M .
- c) Ak $\mathcal{B}$ je báza priestoru L , tak $\text{Ran } T = \text{span}\{T\mathbf{b}: \mathbf{b} \in \mathcal{B}\}$, preto $\dim \text{Ran } T \leq \dim L$.
- d) T je injektívny lineárny operátor vtedy a len vtedy, keď $\text{Ker } T = \{\mathbf{0}_L\}$.
- 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 $\dim \text{Ker } T + \dim \text{Ran } T = n$ („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 $T: K^m \rightarrow K^n$.

Najskôr zavedieme 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*} , $i = 1, 2, \dots, m$ a stĺpce budeme označovať A_{*j} , $j = 1, 2, \dots, n$.

Definícia. Nech $\dim L = n$, $\dim M = m$, $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\}$ je usporiadaná báza lineárneho priestoru L a $\mathcal{D}$ je usporiadaná báza lineárneho priestoru M . Matica $[T]_{\mathcal{B}\mathcal{D}} = A \in K^{m \times n}$ sa nazýva matica lineárneho operátora $T: L \rightarrow M$, 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 $[T]_{\mathcal{B}\mathcal{B}}$.

Násobenie matíc a matca $[T]_{\mathcal{B}\mathcal{D}}$ 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 $T: L \rightarrow M$ je lineárny operátor. Potom platí

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

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 ; $T_1: L_1 \rightarrow L_2, T_2: L_2 \rightarrow L_3$ sú lineárne operátory a T_2T_1 znamená z nich zložený operátor, $T_2T_1: L_1 \rightarrow L_3$. 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 $I: L \rightarrow L$, $I\mathbf{x} = \mathbf{x}$ matice:

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

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 $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n$, ktoré tvoria bázu $\mathcal{B}$.

Príklad. $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3\}$, $\mathcal{D} = \{\mathbf{d}_1, \mathbf{d}_2\}$ Napíšte maticu $[T]_{BD}$, ak $T: R^3 \rightarrow R^2$,

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

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

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

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

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