

1 Polia

- 1.1. Ktoré z uvedených množín tvoria spolu s obvyklým sčítaním a násobením pole?
- $F = \{a + ib; a \in \mathbb{R}, b \in \mathbb{R}, b \geq 0\}$
 - $F = \{a + ib; a \in \mathbb{Q}, b \in \mathbb{Q}\}$
 - $F = \{a + ib; a \in \mathbb{Z}, b \in \mathbb{Z}\}$
 - $F = \{a + b\sqrt{2}; a \in \mathbb{Q}, b \in \mathbb{Q}\}$ (Poznámka: Môže byť užitočné najprv overiť, že pre $a, b, c, d \in \mathbb{Q}$ platí $a + b\sqrt{2} = c + d\sqrt{2}$ p.v.k. $a = c$ a $b = d$. Hint: Kedy platí $a + b\sqrt{2} = 0$ pre racionálne čísla a, b ?)
 - $F = \{a + b\sqrt{5}; a \in \mathbb{Q}, b \in \mathbb{Q}\}$ (Poznámka: Môže byť užitočné najprv overiť, že pre $a, b, c, d \in \mathbb{Q}$ platí $a + b\sqrt{5} = c + d\sqrt{5}$ p.v.k. $a = c$ a $b = d$.)
 - $F = \{a + \sqrt{3}ib; a \in \mathbb{Q}, b \in \mathbb{Q}\}$
 - $F = \{a + \frac{b}{\sqrt{2}}; a, b, c \in \mathbb{Q}\}$
 - $F = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}; a, b, c, d \in \mathbb{Q}\}$ (Hint: Možno pomôže prepísať si túto množinu do tvaru $F = \{a + b\sqrt{3}; a, b \in F'\}$, kde $F' = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$.)
 - $F = \{a + b\sqrt{2} + c\sqrt{3}; a, b, c \in \mathbb{Q}\}$
 - $F = \{a + b\sqrt[3]{5}; a \in \mathbb{Q}, b \in \mathbb{Q}\}$
 - $F = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2; a, b, c \in \mathbb{Q}\}$ (Môže byť pre vás užitočný vzorec $u^3 + v^3 + w^3 - 3uvw = (u + v + w)(u^2 + v^2 + w^2 - uv - vw - vw) = \frac{1}{2}(u + v + w)((u - v)^2 + (v - w)^2 + (w - u)^2)$.)¹
- 1.2. V poli \mathbb{Z}_5 vyrátajte $2^{-1} + 4$, $(-2) + 4$, $2^{-1} + 3$ a $-4 \odot 3^{-1}$.
- 1.3. Napíšte tabuľku násobenia pre \mathbb{Z}_4 a \mathbb{Z}_6 . Viete nejako zdôvodniť, že \mathbb{Z}_4 resp. \mathbb{Z}_6 nie sú polia?
- 1.4. V ľubovoľnom poli F platí:

$$\begin{aligned}
 a + b = a + c &\Rightarrow b = c \\
 (a + b)(c + d) &= ac + ad + bc + bd \\
 -(-a) &= a \\
 -0 &= 0 \\
 -(a + b) &= (-a) + (-b) \\
 (a - b)c &= ac - bc \\
 1 &\neq 0 \\
 a \cdot a = 1 &\Leftrightarrow a = 1 \vee a = -1 \\
 a^2 = b^2 &\Leftrightarrow a = b \vee a = -b \\
 a \cdot (b_1 + \dots + b_n) &= a \cdot b_1 + \dots + a \cdot b_n
 \end{aligned}$$

- 1.5. Na množine \mathbb{R}^+ všetkých kladných reálnych čísel zadefinujme operácie \oplus a \odot tak, že $x \oplus y = x \cdot y$ a $x \odot y = x^y$. Ktoré z axióm poľa spĺňa $(\mathbb{R}^+, \oplus, \odot)$?
- 1.6. Nech na množine $M = \{0, 1\}$ sú operácie $+$ a \cdot dané tabuľkami
- | | | | | | |
|-----|---|---|---------|---|---|
| $+$ | 0 | 1 | \cdot | 0 | 1 |
| 0 | 0 | 1 | 0 | 0 | 0 |
| 1 | 1 | 0 | 1 | 1 | 1 |
- Ukážte, že $(M, +)$ a $(M \setminus \{0\}, \cdot)$ sú komutatívne grupy a že platí distributívny zákon $(a + b)c = ac + bc$. Je $(M, +, \cdot)$ pole?
- 1.7. Zistite, či $(\mathbb{R}, +, *)$, kde $+$ je obvyklé sčítanie reálnych čísel a pre každé $a, b \in \mathbb{R}$ $a * b = -2ab$, je pole.
- 1.8. Na $\mathbb{R} \times \mathbb{R}$ definujeme operácie $+$ a \cdot takto:

¹Táto úloha je naozaj dosť náročná. Snáď je aspoň trochu zaujímavé vedieť, že sa dá vyriešiť pomerne jednoducho, keď už budete mať nejaké vedomosti o báze a dimenzii vektorových priestorov. Podobnými poľami sa budete zaoberať neskôr v druhom ročníku na algebre. Tiež prezradím, že rovnosť $u^3 + v^3 + w^3 - 3uvw = (u + v + w)(u^2 + v^2 + w^2 - uv - vw - vw)$ sa okrem manuálneho roznásobenia dá overiť aj použitím vhodného determinantu. O determinantoch sa budeme učiť na lineárnej algebre 1.

- a) $(a, b) + (c, d) = (a + c, b + d)$ a $(a, b) \cdot (c, d) = (ac, bd)$,
 b) $(a, b) + (c, d) = (a + c, b + d)$ a $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$.
 c) $(a, b) + (c, d) = (a + c, b + d)$ a $(a, b) \cdot (c, d) = (ac - bd, ad + bc - bd)$
 d) $(a, b) + (c, d) = (a + c, b + d)$ a $(a, b) \cdot (c, d) = (bd - ac, ad + bc)$

Je potom $(\mathbb{R} \times \mathbb{R}, +, \cdot)$ pole?

- 1.9. Na $\mathbb{Q} \times \mathbb{Q}$ definujeme operácie $+$ a \cdot takto:

- a) $(a, b) + (c, d) = (a + c, b + d)$ a $(a, b) \cdot (c, d) = (ac + 3bd, ad + bc)$,
 b) $(a, b) + (c, d) = (a + c, b + d)$ a $(a, b) \cdot (c, d) = (ac + 2bd, ad + bc)$.
 c) $(a, b) + (c, d) = (a + c, b + d)$ a $(a, b) \cdot (c, d) = (ac - 5bd, ad + bc)$.

Je potom $(\mathbb{R} \times \mathbb{R}, +, \cdot)$ pole?

- 1.10. Pre ktoré prvky a poľa \mathbb{Z}_7 má riešenie rovnica $x^2 = a$? Koľko je takých prvkov v poli \mathbb{Z}_{109} ?
- 1.11. Pre dané a a p vypočítajte hodnotu a^p a a^{p-1} v \mathbb{Z}_p . (Malá Fermatova veta hovorí, že by vám malo vyjsť $a^p = a$, v tejto úlohe si to môžete vyskúšať na konkrétnych číslach.)
- a) $a = 2, p = 17$;
 b) $a = 6, p = 17$;
 c) $a = 3, p = 29$;
 d) $a = 5, p = 13$;
 e) $a = 3, p = 13$;
 f) $a = 2, p = 13$

- 1.12*. Nech F je konečné pole a platí $|F| = n$. Ukážte, že potom pre každý prvok $a \in F \setminus \{0\}$ platí $a^{n-1} = 1$. (V staršej sade úloh máme súvisiace tvrdenie pre konečné grupy. Týmto sme dostali aj jedno možné odvodenie malej Fermatovej vety.²)

- 1.13. Majme štvorprvkovú množinu $F = \{0, 1, a, b\}$ a binárne operácie $+$, \cdot na tejto množine. Ak viete, že $(F, +, \cdot)$ je pole, tak doplňte zvyšok zadaných tabuliek:

$+$	0	1	a	b	\cdot	0	1	a	b
0	0	1	a	b	0	0	0	0	0
1		0			1	0	1	a	b
a			0		a			a	
b				0	b				b

T.j. v tabuľkách máme zadané, že $0 + x = x$ a $x + x = 0$ pre všetky $x \in F$. A tiež to, že $0 \cdot x = 0$ a $1 \cdot x = x$ pre všetky $x \in F$.

Zdôvodnite, prečo váš výsledok je jediná možnosť, ako sa tieto tabuľky dajú doplniť. (To, či na konci naozaj vyšlo pole, overovať nemusíte.)

Poznámka. Jeden z dôvodov, prečo som pridal takýto príklad, je ukázať, že existuje aj štvorprvkové pole. (Z konečných polí ste sa zatiaľ stretli s poľami, ktoré majú prvočíselný počet prvkov. Neskôr sa na Algebra 3 dozvieme, že existujú aj iné konečné polia a aj to ako všetky také polia vyzerajú. Z toho, čo sa naučíte tam, sa štvorprvkové pole bude dať dostať oveľa jednoduchšie – tu vlastne máme zadanú tabuľku sčítovania a násobenia, ale nevieme, prečo sme ich zobrali akurát takéto.)

2 Euklidov algoritmus

Na cvičeniach si zvykneme ukázať aj rozšírený Euklidov algoritmus, t.j. ako sa dajú nájsť pre dané $a, b \in \mathbb{Z}$ čísla $u, v \in \mathbb{Z}$ také, že platí

$$d = au + bv,$$

²Malá Fermatova veta hovorí, že pre ľubovoľné prvočíсло p a ľubovoľné $a \in \mathbb{Z}$ platí $a^p \equiv a \pmod{p}$. Resp. dá sa vyjadriť aj tak, že ak $p \nmid a$, tak $a^{p-1} \equiv 1 \pmod{p}$; čo je vlastne toto tvrdenie aplikované na \mathbb{Z}_p .

kde $d = \gcd(a, b)$ je najväčší spoločný deliteľ čísel a, b . Existenciu takýchto čísel ste využili v dôkaze, že \mathbb{Z}_p je pole pre každé prvočíslo p . Tento algoritmus by sa pri väčšom p dal využiť aj na výpočet inverzného prvku v poli \mathbb{Z}_p . Stretnete sa s ním aj neskôr – okrem iného sa analogicky dá postupnosť aj pri výpočte najväčšieho spoločného deliteľa dvoch polynómov.³

1. Overte, či p je prvočíslo. Ak je to prvočíslo, nájdite x^{-1} v poli \mathbb{Z}_p .
 - a) $p = 103, x = 41$
 - b) $p = 107, x = 32$
 - c) $p = 109, x = 61$
 - d) $p = 71, x = 31$
 - e) $p = 97, x = 18$
2. Pre dané čísla $a, b \in \mathbb{Z}$ vypočítajte $d = \gcd(a, b)$ a nájdite čísla $u, v \in \mathbb{Z}$, pre ktoré platí $au + bv = d$.
 - a) $a = 24, b = 17$
 - b) $a = 172, b = 20$
 - c) $a = 60, b = 17$
 - d) $a = 100, b = 23$
 - e) $a = 29, b = 19$
 - f) $a = 80, b = 62$

³Nejaké ukážky výpočtu môžete nájsť na fóre: <https://msleziak.com/forum/viewtopic.php?t=298>.