1 Polia

1.1. Ktoré z uvedených množín tvoria spolu s obvyklým sčitovaním a násobením pole?
a) $F = \{a + ib; a \in \mathbb{R}, b \in \mathbb{R}, b \geq 0\}$
b) $F = \{a + ib; a \in \mathbb{Q}, b \in \mathbb{Q}\}$
c) $F = \{a + ib; a \in \mathbb{Z}, b \in \mathbb{Z}\}$
d) $F = \{a + b\sqrt{5}; a \in \mathbb{Q}, b \in \mathbb{Q}\}$ (Hint: 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 $b = d$.)
e) $F = \{a + \sqrt{3}ib; a \in \mathbb{Q}, b \in \mathbb{Q}\}$
f) $F = \{a + \frac{b}{\sqrt{2}}; a, b, c \in \mathbb{Q}\}$
g*) $F = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}; a, b, c, d \in \mathbb{Q}\}$ (Hint: Možno pomôže prepísať si túto množinu do tvaru $F = \{a + b\sqrt{3}; a, b \in F'\}$, kde $F' = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$.)
h*) $F = \{a + b\sqrt{2} + c\sqrt{3}; a, b, c \in \mathbb{Q}\}$
i*) $F = \{a + b\sqrt[3]{5}; a \in \mathbb{Q}, b \in \mathbb{Q}\}$
j**) $F = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2; a, b, c \in \mathbb{Q}\}$ (Môže byť pre vás užitočný vzorec $u^3 + v^3 + w^3 - 3uvw = (u + v + w)(u^2 + v^2 + w^2 - uv - uw - vw) = \frac{1}{2}(u + v + w)((u - v)^2 + (v - w)^2 + (w - u)^2)$.) [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:

$$a + b = a + c \Rightarrow b = c$$
$$(a + b)(c + d) = ac + ad + bc + bd$$
$$-(-a) = a$$
$$-0 = 0$$
$$-(a + b) = (-a) + (-b)$$
$$(a - b)c = ac - bc$$
$$1 \neq 0$$
$$a \cdot a = 1 \Leftrightarrow a = 1 \vee a = -1$$
$$a^2 = b^2 \Leftrightarrow a = b \vee a = -b$$
$$a \cdot (b_1 + \ldots + b_n) = a \cdot b_1 + \ldots + a \cdot b_n$$

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
0	0	1
1	1	0

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

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

1.7. Zistite, či $(\mathbb{R}, +, *)$, kde + je obvyklé sčitovanie 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:
a) $(a, b) + (c, d) = (a + c, b + d)$ a $(a, b).(c, d) = (ac, bd)$,
b) $(a, b) + (c, d) = (a + c, b + d)$ a $(a, b).(c, d) = (ac - bd, ad + bc)$.
c) $(a, b) + (c, d) = (a + c, b + d)$ a $(a, b) \cdot (c, d) = (ac - bd, ad + bc - bd)$

[1] Táto 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 $u^3 + v^3 + w^3 - 3uvw = (u + v + w)(u^2 + v^2 + w^2 - uv - uw - vw)$ sa okrem manuálneho roznásobenia dá overiť aj použitím vhodného determinantu. O determinantoch sa budeme učiť na lineárnej algebre 1.

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

1.10*. 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])

2 Euklidov algoritmus

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

$$d=au+bv,$$

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, čí 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) $a=80$, $b=62$

[2] Malá Fermatova veta hovorí, že pre ľubovoľné prvočíslo 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 $\mathbb{Z}_p$.

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