1 Polia

Množina F s binárnymi operáciami $+$ a $\cdot$ tvorí pole, ak:

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

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

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

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

(Túto vlastnosť nazývame *distributívnosť*.)

Ekvivalentne môžeme túto definíciu prepísať pomocou takýchto podmienok:

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

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

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

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

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

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

(vii) existuje prvok $1 \in F$ taký, že $1 \neq 0$ a pre každé $a \in F$ sa $a \cdot 1 = a$,

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

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

Úloha 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) $F = \{a + b\sqrt{2}; a \in \mathbb{Q}, b \in \mathbb{Q}\}$
e) $F = \{a + b\sqrt{5}; a \in \mathbb{Q}, b \in \mathbb{Q}\}$
f) $F = \{a + \sqrt{3}ib; a \in \mathbb{Q}, b \in \mathbb{Q}\}$
g) $F = \{a + \frac{b}{\sqrt{2}}; a, b \in \mathbb{Q}\}$
h*) $F = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}; a, b, c, d \in \mathbb{Q}\}$ (Hint: Možno pomôže prepísať si túto množinu do tvaru $F = \{a + b\sqrt{3}; a, b \in F'\}$, kde $F' = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$.)
i*) $F = \{a + b\sqrt{2} + c\sqrt{3}; a, b, c \in \mathbb{Q}\}$
j*) $F = \{a + b\sqrt[3]{5}; a \in \mathbb{Q}, b \in \mathbb{Q}\}$

Pri úlohe o $F = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$ môže byť užitočné zamyslieť sa najprv nad tým, či vieme zdôvodniť, že pre $a, b \in \mathbb{Q}$ platí:

$$a + b\sqrt{2} = 0 \qquad \Leftrightarrow \qquad a = b = 0.$$

(Platilo by to aj bez predpokladu, že a, b sú racionálne?)

Tiež si môžeme uvedomiť, že potom pre $a, b, a', b' \in \mathbb{Q}$ už ľahko dostaneme

$$a + b\sqrt{2} = a' + b'\sqrt{2} \qquad \Leftrightarrow \qquad a = a' \wedge b = b'.$$

Úloha 1.2. Na $\mathbb{Q} \times \mathbb{Q}$ definujeme operácie + a · 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?

Úloha 1.3. V poli $\mathbb{Z}_5$ vyrátajte $2^{-1} \oplus 4$, $(-2) \oplus 4$, $2^{-1} \odot 3$ a $-4 \odot 3^{-1}$.

Úloha 1.4. V $\mathbb{Z}_5$ vyrátajte 2^3, $(2^{-1})^4$, $2 \odot (4^{-1})^3$, $(4 \odot 2^{-1})^3$, $(-1)^5 \odot (4 \odot 3^{-1})^2$.

Úloha 1.5. V ľubovoľnom poli F platí:

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

Úloha 1.6. 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 $(\mathbb{R}^+, \oplus, \odot)$? (Pričom $x \cdot y$ označuje obvyklé násobenie a x^y obvyklé umocňovanie.)

Úloha 1.7. Nech F je pole a $a \in F$. Definujeme zobrazenie $f_a \colon F \to F$ tak, že $f_a(b) = a+b$. Je f_a bijekcia? Ak áno, ako vyzerá zobrazenie f_a^{-1}? Čomu sa rovná $f_a \circ f_b$?

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

Úloha 1.8. Nech na množine $M = \{0,1\}$ sú operácie + a · dané tabuľkami

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	1	1

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

Úloha 1.9. Zistite, či $(\mathbb{R}, +, *)$, kde + je obvyklé sčitovanie reálnych čísel a pre každé $a, b \in \mathbb{R}$ $a * b = -2ab$, je pole.

Úloha 1.10*. Pre ktoré prvky a poľa $\mathbb{Z}_7$ má riešenie rovnica $x^2 = a$? Koľko je takých prvkov v poli $\mathbb{Z}_{109}$?

Úloha 1.11*. Dokážte, že:
a) V ľubovoľnom poli platí $(a+b)^m = a^m + \binom{m}{1} \times a^{m-1}b + \binom{m}{2} \times a^{m-2}b^2 + \ldots + \binom{m}{m-1} ab^{m-1} + b^m$. (Súčet na pravej strane sa zvykne označovať takto: $\sum_{k=0}^{m} \binom{m}{k} \times a^{m-k}b^k$.)
b) V poli $\mathbb{Z}_p$ platí: $(a \oplus b)^p = a^p \oplus b^p$.

Úloha 1.12*. Pomocou úlohy 1.11 dokážte matematickou indukciou vzhľadom na a, že v $\mathbb{Z}_p$ platí rovnosť $a^p = a$ (pre ľubovoľné $a \in \mathbb{Z}_p$). (Toto je vlastne iná formulácia malej Fermatovej vety.)

Úloha 1.13. Nech F je konečné pole a platí $|F| = n$. Ukážte, že potom pre každý prvok $a \in F \setminus \{0\}$ platí $a^{n-1} = 1$. (Týmto sme súčasne získali aj iné odvodenie malej Fermatovej vety.)

Úloha 1.14. 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
0	0	1	a	b
1		0		
a			0	
b				0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a				
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 $1 \cdot x = 1$ 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 Algebre 3 dozviete, že existujú aj iné konečné polia a aj to ako všetky také polia vyzerajú. Z toho, čo sa naučíte tam, sa štvorprkové pole bude dať dostať oveľa jednoduchšie – tu vlastne máme zadanú tabuľku sčitovania a násobenia, ale nevieme, prečo sme ich zobrali akurát takéto.)