Matematický ústav Slezské univerzity v Opavě
Učební texty k přednášce ALGEBRA I, zimní semestr 2000/2001
Michal Marvan

3. Pole

Množina **Q** všech racionálních čísel, množina **R** všech reálných čísel a množina **C** všech komplexních čísel, vybavené čtyřmi základními aritmetickými operacemi – sčítáním, odečítáním, násobením a dělením –, jsou příklady jedné a téže abstraktní algebraické struktury, zvané pole.

Definice. *Pole* je množina, řekněme P, spolu s
a) binární operací $P \times P \to P$, $(a, b) \mapsto a + b$; nazývá se *sčítání*;
b) binární operací $P \times P \to P$, $(a, b) \mapsto a \cdot b$; nazývá se *násobení*;
c) dvěma vybranými prvky $0 \neq 1 \in P$; nazývají se *nula* a *jednička*;
d) zobrazením $P \to P$, $a \mapsto -a$; prvek $-a$ se nazývá *opačný* k prvku a;
e) zobrazením $P \setminus \{0\} \to P \setminus \{0\}$, $a \mapsto a^{-1}$; prvek a^{-1} se nazývá *převrácená hodnota* k prvku a;

přičemž je požadováno, aby pro libovolné prvky $a, b, c \in P$ platilo

(1) $a + b = b + a$,   (5) $a \cdot b = b \cdot a$,

(2) $a + (b + c) = (a + b) + c$,   (6) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$,

(3) $a + 0 = a$,   (7) $a \cdot 1 = a$,

(4) $a + (-a) = 0$,   (8) $a \neq 0 \quad \Rightarrow \quad a \cdot a^{-1} = 1$,

(9) $a \cdot (b + c) = a \cdot b + a \cdot c$.

Podmínky (1)–(9) z definice pole nazýváme *axiomy pole*. Axiomy (1)–(4) znamenají, že $(P, +, 0, -)$ je komutativní grupa. Axiom (9) říká, že násobení je *distributivní* vzhledem ke sčítání. Axiomy (5)–(8) říkají, že $(P, \cdot, 1)$ je monoid, v němž jsou všechny nenulové prvky invertibilní.

Příklady. 1) Pole **R** reálných čísel (definice je podána v přednášce z matematické analýzy), pole **C** komplexních čísel a pole **Q** čísel racionálních.

2) Dvouprvkové pole $(\{0, 1\}, +, 0, -, \cdot, 1)$ s operacemi

$+$	0	1
0	0	1
1	1	0

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

$-$	
0	1
1	0

$(\,)^{-1}$	
0	neex.
1	1

(ověřte, že se jedná o pole). V každém počítači jsou realizovány operace „+“ (XOR), „·“ (AND) a „−“ (NOT). Pozoruhodný je fakt, že vztah $1 + 1 = 0$ není ve sporu s axiomy pole (protože jsme právě uvedli příklad struktury, ve které platí všechny axiomy polei vztah $1 + 1 = 0$ současně).

Tvrzení. *Buď P pole. Pak pro každý prvek $a \in P$ platí:*
(i) $a \cdot 0 = 0$;
(ii) $a \cdot (-1) = -a$;
(iii) $a \cdot (b - c) = a \cdot b - a \cdot c$.

Důkaz. (i) Počítejme: $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$. Přičteme-li k oběma stranám rovnosti prvek $-(a \cdot 0)$, obdržíme požadovaný výsledek.

(ii) S použitím právě dokázaného výsledku máme $0 = a \cdot 0 = a \cdot (1 + (-1)) = a \cdot 1 + a \cdot (-1) = a + a \cdot (-1)$. Přičteme-li k oběma stranám získané rovnosti prvek $-a$, obdržíme hledaný výsledek.

(iii) Cvičení.

Tvrzení. *Buď P pole. Nechť prvky $a, b \in P$ splňují rovnost $a \cdot b = 0$. Pak $a = 0$ nebo $b = 0$.*

Důkaz. Jestliže $b = 0$, pak jsme hotovi. Jestliže $b \neq 0$, pak vynásobením obou stran rovnosti $a \cdot b = 0$ prvkem b^{-1} získáme rovnost $a = 0$.

Cvičení. Dokažte rovnosti

1) $(-1) \cdot (-1) = 1$,

2) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$.

Tvrzení. *Je-li P pole, pak $P^* := P \setminus \{ 0 \}$ je grupa vzhledem k binární operaci „$\cdot$“.*

Důkaz. Nejprve dokážeme sporem, že pro $a, b \in P^*$ máme $a \cdot b \in P^*$. Je-li totiž naopak $a \cdot b \notin P^*$, pak vzhledem k tomu, že $a \cdot b \in P$, zbývá jediná možnost: $a \cdot b = 0$. Pak ovšem $a = 0$ nebo $b = 0$ podle předchozího tvrzení, což je spor. Množina P^* je tedy uzavřená vzhledem k operaci „$\cdot$“. Zbytek tvrzení pak plyne z toho, že prvek $1 \in P^*$ je neutrálním prvkem, a že každý nenulový prvek je invertibilní.

Tvrzení (Řešení jedné lineární rovnice o jedné neznámé). *Buď P pole, buďte a, b prvky z P. Je-li $b \neq 0$, pak existuje jediný prvek $\xi \in P$ takový, že*

$$a\xi + b = 0,$$

a sice prvek $\xi = -ba^{-1}$ a nazývá se řešení *rovnice $ax + b = 0$.*

Důkaz. Je-li $\xi \in P$ řešení rovnice $ax + b = 0$, pak platí rovnost $a\xi + b = 0$. Přičteme-li k oběma stranám prvek $-b$, získáme rovnost $a\xi = b$. Po vynásobení prvkem a^{-1} získáme $\xi = -ba^{-1}$. Tím je současně dokázána jednoznačnost řešení (každý prvek ξ, který je řešením naší rovnice, je roven $-ba^{-1}$).

Zbývá ověřit, že $\xi = -ba^{-1}$ je vždy řešením: $a\xi + b = a \cdot (-ba^{-1}) + b = aa^{-1}(-b) + b = -b + b = 0$.

Prvek $b \cdot a^{-1}$ se značí b/a a nazývá se podíl prvků b a a.

Tvrzení. *Množina $\mathbf{Z}_m$, $m > 1$, zbytkových tříd modulo m tvoří pole právě tehdy, když m je prvočíslo.*

Důkaz. Distributivní zákon (9) z definice pole není těžké ověřit. Zbývá ukázat, že multiplikativní monoid $\mathbf{Z}_m^*$, $m > 1$, je grupa právě tehdy, když m je prvočíslo.

Je-li m číslo složené, pak $m = rs$ pro nějaká čísla $r, s \in \mathbf{N}$, $1 < r < m$, $1 < s < m$, načež $[r]_m \cdot [s]_m = [rs]_m = [m]_m = [0]_m$. Vidíme, že $[r]_m \neq [0]_m$ i $[s]_m \neq [0]_m$ jsou nenulové prvky s nulovým součinem, což je spor.

Naopak, buď p prvočíslo. Ukažme, že $\mathbf{Z}_p^*$ je multiplikativní grupa. Ke každé nenulové zbytkové třídě $[a]_p \neq [0]_p$ najdeme třídu inverzní. Zaveďme pomocné zobrazení $\ell_a : \mathbf{Z}_p \to \mathbf{Z}_p$, $[i]_p \mapsto [ai]_p = [a]_p[i]_p$. Toto zobrazení je homomorfismus aditivních grup (cvičení). Označme $K_a = \{ z \mid \ell_a(z) = 0 \}$. Nechť $[b]_p \in K_a$, čili $[0]_p = \ell_a([b]_p) = [ab]_p$, to jest, ab je násobkem p. Protože p je prvočíslo, musí být buď a násobkem p nebo b násobkem p (což snadno vyplývá ze známé věty o existenci a jednoznačnosti rozkladu celých čísel na prvočinitele), a tedy $[a]_p = [0]_p$ nebo $[b]_p = [0]_p$. První možnost je však vyloučena předpokladem $[a]_p \neq [0]_p$, takže nutně $[b]_p = [0]_p$. Vidíme, že K_a obsahuje jen nulovou třídu $0 = [0]_p$.

Zobrazení ℓ_a je injektivní. Skutečně, kdyby existovaly dvě třídy z_1, z_2 takové, že $\ell_a(z_1) = \ell_a(z_2)$, pak by bylo $\ell_a(z_1 - z_2) = 0$ (cvičení), načež $z_1 - z_2 \in K_a$, takže $z_1 - z_2 = 0$ a $z_1 = z_2$. Protože ℓ_a zobrazuje p-prvkovou množinu do p-prvkové množiny a je injektivní, je rovněž surjektivní. Speciálně, prvek $[1]_p \in \mathbf{Z}_p$ má vzor, označme jej $[x]_p$. Pak $[1]_p = \ell_a([x]_p) = [a]_p[x]_p$. Tudíž, $[x]_p$ je inverzní prvek k $[a]_p$.

Předchozí důkaz neobsahuje praktický návod, jak inverzní prvky hledat. Získání použitelných postupů je předmětem následujících cvičení.

Cvičení. 1. Dokažte, že existují právě dva prvky $[a]_p$ grupy $\mathbf{Z}_p^*$ splňující $[a]_p = [a]_p^{-1}$, a sice $[1]_p$ a $[-1]_p = [p-1]_p$.
Návod: Řešte rovnici $\zeta^2 = 1$, tj. $(\zeta + 1)(\zeta - 1) = 0$ v $\mathbf{Z}_p^*$.

2. Ukažte, že pro $a = 2, \dots, p-2$ platí $[a]_p^{-1} = [2]_p \cdots [a-1]_p[a+1]_p \cdots [p-2]_p$ (součin všech tříd $[2]_p, \dots, [p-2]_p$ s vynecháním samotné třídy $[a]_p$.

Cvičení. Dokažte, že pro každé $[a]_p \in \mathbf{Z}_p^*$ platí $[a]_p^{-1} = [a]_p^{p-2}$.
Návod: Ukažte, že platí $\{[1]_p, \dots, [p-1]_p\} = \{[a]_p[1]_p, \dots, [a]_p[p-1]_p\}$. Porovnejte součin $[1]_p \cdots [p-1]_p$ všech prvků grupy $\mathbf{Z}_p$ se součinem $([a]_p[1]_p) \cdots ([a]_p[p-1]_p)$.

Poznamenejme ještě bez důkazu, že konečné pole o n prvcích existuje pro každé $n \in \mathbf{N}$ tvaru $n = p^k$, kde p je prvočíslo a $k \in \mathbf{N}$.

Definice. Buď P pole, buď $S \subseteq P$ podmnožina množiny P. Nechť jsou splněny následující podmínky: $0, 1 \in S$; je-li $a, b \in S$, pak $a + b \in S$, $-a \in S$ a $ab \in S$; je-li navíc $a \neq 0$, pak $a^{-1} \in S$. Potom řekneme, že S je *uzavřená* podmnožina. Podobně jako v předešlých případech algebraických struktur se množina S stává polem vzhledem k operacím omezeným na S. Nazývá se *podpole* pole P.

Příklady. 1. Pole $\mathbf{Q}$ je podpolem v poli $\mathbf{R}$ i $\mathbf{C}$. Pole $\mathbf{R}$ je podpolem v poli $\mathbf{C}$.

2. Naopak, množina $\mathbf{Z} \subset \mathbf{Q}$ není uzavřená a nedává podpole, protože v $\mathbf{Z}$ leží prvek 2, ale neleží tam prvek $2^{-1} = \frac{1}{2}$.

3. Pole $\{0, 1\}$ není podpolem v poli $\mathbf{Q}$, protože $1 + 1 = 0$ v prvním případě a $1 + 1 = 2 \neq 0$ v druhém případě.

Definice. Podpole v poli $\mathbf{C}$ se nazývá *číselné pole.*

Definice. Buďte P, Q pole, buď $f : P \to Q$ zobrazení. Nechť pro každé $a, b \in P$ platí $f(a + b) = f(a) + f(b)$, $f(-a) = -f(a)$, $f(0) = 0$, $f(a \cdot b) = f(a) \cdot f(b)$, $f(1) = 1$ a je-li navíc $a \neq 0$, pak i $f(a^{-1}) = f(a)^{-1}$. Pak se f nazývá *homomorfismus* polí. Je-li navíc bijektivní, nazývá se *izomorfismus* polí. Pole, mezi nimiž existuje izomorfismus se nazývají *izomorfní*.

Příklad. Dvouprvkové pole $\{0, 1\}$ je izomorfní s polem $\mathbf{Z}_2$. Izomorfismem je zobrazení $0 \mapsto [0]_2$, $1 \mapsto [1]_2$.

Příklad. Buď P pole, buď $m \in P$ prvek takový, že neexistuje $s \in P$ tak, aby $s^2 = s \cdot s = m$, tj. nechť prvek m nemá v poli P druhou odmocninu. Zkonstruujme nové pole S tak, že P bude podpole v S a prvek m bude mít druhou odmocninu v S.

Položme $S = P \times P$. Na množině S zavedeme algebraické operace formulemi

$$\begin{aligned}
&(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2),\\
&(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2 + m b_1 + b_2, a_1 b_2 + b_1 a_2),\\
&0 = (0, 0),\\
&1 = (1, 0),\\
&-(a, b) = (-a, -b),\\
&(a, b)^{-1} = \left(\frac{a}{a^2 - mb^2}, \frac{-b}{a^2 - mb^2}\right) \qquad \text{pro } (a, b) \neq (0, 0).
\end{aligned}$$

a ukažme, že množina S s uvedenými operacemi je pole.

Nejdříve je třeba ukázat, že prvek $(a, b)^{-1}$ skutečně existuje pro každý prvek $(a, b) \in S$ různý od nulového prvku, tj. $(a, b) \neq (0, 0)$. Kritickým místem je jmenovatel $a^2 - mb^2$, který musí být nenulový (v poli P). Důkaz veďme sporem, tj. připusťme, že $a^2 - mb^2 = 0$. Rozeznávejme dva případy:

1. Jestliže $b = 0$, pak $a^2 = mb^2 = 0$, a tedy i $a = 0$ (zdůvodněte proč), načež $(a, b) = (0, 0)$, což ovšem bylo v předpokladech vyloučeno, takže tento případ nenastává.

2. Jestliže naopak $b \neq 0$, pak můžeme prvkem b dělit a vypočíst $m = a^2/b^2 = (a/b)^2$. Ale pak je prvek $s = a/b \in P$ druhou odmocninou prvku m, což je opět ve sporu s předpoklady.

Tento spor ukazuje, že $a^2 \neq mb^2$, tj. $a^2 - mb^2 \neq 0$, což se mělo dokázat.

Ověření axiomů (1)–(9) je jednoduché cvičení.

Pole P, striktně vzato, není podpole v S, protože množina P není podmnožina v S. Je ale možné množinu P ztotožnit s podmnožinou $\{(p, 0) \mid p \in P\}$ množiny S, která takovým podpolem je.

Předchozí příklad má zajímavá použití. Je-li $P = \mathbf{R}$ a $m = -1$, pak m nemá odmocninu v $\mathbf{R}$. Pole S pak je pole komplexních čísel (vlastně jde o známou konstrukci komplexních čísel). Skutečně, ztotožníme-li dvojici $(a, b) \in S$ s komplexním číslem $a + bi$, přejdou operace zavedené na S v obvyklé operace nad komplexními čísly (ověřte podrobně).

Je-li $P = \mathbf{Q}$ a $m = 2$, pak m nemá odmocninu v $\mathbf{Q}$. Pole S pak je pole všech reálných čísel tvaru $a + b\sqrt{2}$, s obvyklými operacemi nad reálnými čísly (ověřte podrobně).

Problém k řešení. Buďte P, Q pole, buď $f : P \to Q$ zobrazení.

1. Nechť pro každé $a, b \in P$ platí $f(a + b) = f(a) + f(b)$, $f(a \cdot b) = f(a) \cdot f(b)$, $f(1) \neq 0$. Pak f je homomorfismus polí.

2. Je-li f homomorfismus polí, pak je injektivní.

Dokažte.