OKRUHY A POLE

Buď P množina, s
- binární operace na P, $(a,b) \mapsto a+b$, sčítání.
- binární operace na P, $(a,b) \mapsto a \cdot b$, násobení.
- dvěma prvky $0, 1$, $0 \neq 1$, nula a jednička.
- zobrazení $P \to P$, $a \mapsto -a$, prvek opačný

a navíc $\forall a,b,c \in P$ platí

1) $a+b = b+a$
2) $(a+b)+c = a+(b+c)$
3) $a+0 = a$
4) $a+(-a) = 0$
5) $a \cdot b = b \cdot a$
6) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
7) $a \cdot 1 = a$
8) $a \cdot (b+c) = a \cdot b + a \cdot c$

Potom P se nazývá OKRUH.

Př.: 1) $\mathbb{Z}$
2) $P[x]$

Okruh se zobrazením $P \setminus \{0\} \to P \setminus \{0\}$, $a \mapsto a^{-1}$, prvek a^{-1} se nazývá převrácená hodnota, takovým, že $\forall a \neq 0$ platí $a \cdot a^{-1} = 1$, se nazývá POLE.

Př.: 1) množina $\mathbb{R}$ reálných čísel, $\mathbb{C}$ komplexních čísel, $\mathbb{Q}$ racionálních čísel

2) $\{0,1\}$ s operacemi:

$+$	0	1
0	0	1
1	1	0

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

$-$	
0	0
1	1

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

Tvrzení Buď P pole. Pak $\forall a \in P$ platí

1) $a \cdot 0 = 0$
2) $a \cdot (-1) = -a$
3) $a \cdot (b - c) = a \cdot b - a \cdot c$

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

Tvrzení (Řešení jedné lineární rovnice o jedné neznámé)
Buď P pole, $a, b \in P$, $a \neq 0$. Pak existuje jediný prvek $\xi \in P$ tak, že

$$a\xi + b = 0$$

a to sice $\xi = -ba^{-1}$.

ξ se nazývá ŘEŠENÍ rovnice $ax + b = 0$.

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

$$\mathbb{Z}_m = \{0, 1, \dots, m-1\}$$

$$\mathbb{Z}_3 = \{0, 1, 2\}$$

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$-$	
0	0
1	2
2	1

$()^{-1}$	
0	nelze
1	1
2	2

$\mathbb{Z}_4$

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Buď P pole, $S \subseteq P$. Nechť $0, 1 \in S$,
$a, b \in S \Rightarrow a + b \in S$, $-a \in S$, $a \cdot b \in S$
a je-li $a \neq 0$, pak $a^{-1} \in S$.

Pak S se nazývá PODPOLE pole P.

Homomorfismy polí