Pole

Konečná pole existují pouze pro případ p^n prvků, kde p je prvočíslo a $n \in \mathbb{N}$ (např. existuje pole $\mathbb{F}_4 \to 4 = 2^2$, ale neexistuje konečné pole o šesti prvcích). V případě $n = 1$ se sčítá a násobí $mod\, p$. Je-li $n > 1$ je tomu jinak.

1. Příklad Nejjednodušší pole $\mathbb{F}_2$

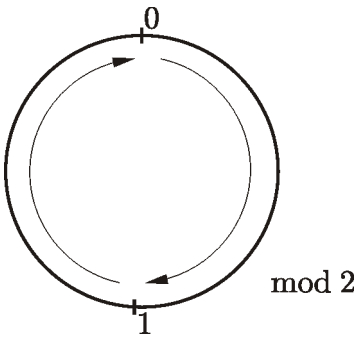
$p = 2, n = 1$ prvky: $0, 1$

Aditivní tabulka – sčítáme modulo 2

$+$	0	1
0	0	1
1	1	0

Multiplikativní tabulka – násobíme modulo 2 (viz Obrázek 1)

$\times$	0	1
0	0	0
1	0	1



Obrázek 1: Pole $\mathbb{F}_2$

2. Příklad Pole $\mathbb{F}_3$

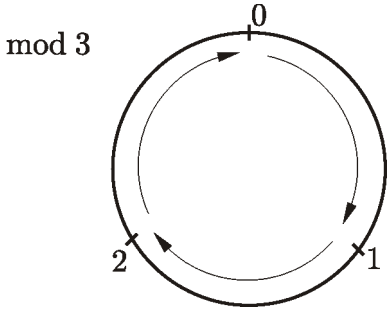
$p = 3, n = 1$ prvky: $0, 1, 2$

Aditivní tabulka – sčítáme modulo 3

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

Multiplikativní tabulka – násobíme modulo 3 (viz Obrázek 2)

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1



Obrázek 2: Pole $\mathbb{F}_3$

3. Příklad Pole $\mathbb{F}_5$

$p = 5, n = 1$ prvky: $0, 1, 2, 3, 4$

Aditivní tabulka – sčítáme modulo 5

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Multiplikativní tabulka – násobíme modulo 5

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

4. Poznámka Úloha o 36-ti důstojnících: Máme seřadit 36 důstojníků z šesti různých pluků a šesti různých hodností do čtverce tak, aby v jedné řadě ani v jednom sloupci nestáli 2 důstojnící ze stejného pluku nebo stejné hodnosti.

5. Situace pro $n > 1$: Prvky pole $\mathbb{F}_{p^n}$ vyjádříme jako polynomy v neurčité „x“ s koeficienty 0, 1, …, $p-1$ a stupně nejvýše $n-1$. Sčítání provedeme tak, že tyto polynomy sčítáme *modulo* p v každém stupni.

Pro násobení nejdříve vybereme tzv. **redukční polynom**, což je polynom stupně n (s koeficienty 0, 1, …, $p-1$), který není součinem polynomů stupňů nižších (tzn. je nerozložitelný). Dva prvky $\mathbb{F}_{p^n}$ nyní vynásobíme a odečítáme $x^i\ P_{red}$ (pro vhodné i) tak dlouho, až je výsledek stupně nejvýše $n-1$ (násobíme „*modulo* P_{red}“).

6. Příklad Pole $\mathbb{F}_4$ (viz Obrázek 3)

$p = 2, n = 2$ prvky:

0	1	2	3
0	1	x	$x+1$

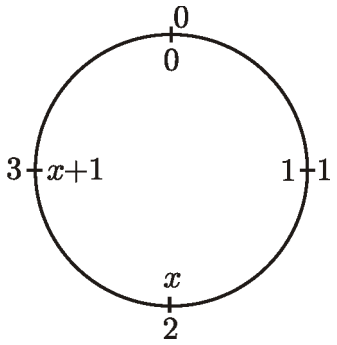
$+$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Vybereme redukční polynom z polynomů: $x^2,\ x^2+1,\ x^2+x,\ x^2+x+1$

$x \cdot x = x^2$

$x \cdot (x+1) = x^2 + x$

$(x+1) \cdot (x+1) = x^2 + \underbrace{2x}_{0} + 1 = x^2 + 1 \quad \Rightarrow P_{red} = x^2 + x + 1$



Obrázek 3: Pole $\mathbb{F}_4$

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

$2 \cdot 2: \quad x \cdot x = x^2, \quad x^2 - (x^2 + x + 1) = x + 1 \to 3$
$2 \cdot 3: \quad x \cdot (x + 1) = x^2 + x, \quad (x^2 + x) - (x^2 + x + 1) = 1 \to 1$
$3 \cdot 3: \quad (x + 1) \cdot (x + 1) = x^2 + 1, \quad (x^2 + 1) - (x^2 + x + 1) = x \to 2$

7. Cvičení Sestavte aditivní a multiplikativní tabulky polí $\mathbb{F}_8$ a $\mathbb{F}_9$.

$\mathbb{F}_8 : p = 2, n = 3$ prvky:

0	1	2	3	4	5	6	7
0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1

Pokud nalezneme více redukčních polynomů, libovolně si jeden zvolíme. Tento jev vede k izomorfismu polí se stejným počtem prvků. Např. můžeme vytvořit aditivní a multiplikativní tabulku pole $\mathbb{F}_8$ dvěma způsoby (má 2 redukční polynomy), tyto tabulky budou na první pohled odlišné, ovšem jsou *izomorfní*.

8. Definice Pole $\mathbb{F}$ a $\mathbb{G}$ jsou **izomorfní** $\Leftrightarrow \exists$ zobrazení $f : \mathbb{F} \to \mathbb{G}$ takové, že:

1. f je bijekce,
2. $f(x + y) = f(x) + f(y)$,
3. $f(x \cdot y) = f(x) \cdot f(y)$.

9. Poznámka Izomorfní pole jsou „stejná“, jen mohou mít různě pojmenované prvky (např. 3 v $\mathbb{F}$ je 7 v $\mathbb{G}$).

Děkujeme Lence Zavíralové za pečlivé vysázení poznámek z přednášky. Tento text zatím neprošel výraznějšími úpravami, proto přivítáme jakékoli upozornění na případné nepřesnosti. Připomínky adresujte na `hoderova@fme.vutbr.cz`