6. Teorie polí (minimální pole, rozšíření pole, konečná pole a jejich konstrukce).

Minimální pole

Pole (K,+, 0,−, ·, 1) se nazývá **minimální**, pokud nemá žádná jiná podpole než sebe sama.

Každé pole má vždy jediné podpole, které je minimální.

Buď (R,+, 0,−, ·, 1) okruh s jednotkovým prvkem. Potom se definuje vztahem

$$\operatorname{char} R := \begin{cases} |\{n \cdot 1 \mid n \in \mathbb{Z}\}|, & \text{pokud se jedná o konečnou kardinalitu,} \\ 0 & \text{jinak.} \end{cases}$$

charakteristika okruhu R (formálně: charR).
Buď o(1) řad prvku 1 v abelovské grupě (R,+). Potom platí

$$\operatorname{char} R = \begin{cases} o(1), & \text{pokud } o(1) \in \mathbb{N}, \\ 0, & \text{pokud } o(1) = \infty. \end{cases}$$

Příklad:

1. Pro okruh zbytkových tříd ($\mathbb{Z}$n,+, 0,−, ·, 1) platí char$\mathbb{Z}$n = n (n ∈ $\mathbb{N}$0).
2. char $\mathbb{Z}$ = char $\mathbb{Q}$ = char $\mathbb{R}$ = char $\mathbb{C}$ = 0.

Buď (K,+, 0,−, ·, 1) pole takové, že char K ∈ $\mathbb{P}$ (char K je prvočíslo). Potom {n · 1 | n ∈ $\mathbb{Z}$} je minimální podpole pole K. V tomto případě tedy platí: minimální podpole pole K je izomorfní se $\mathbb{Z}_m$, kde m = char K.

Každé minimální pole je izomorfní se $\mathbb{Z}_p$ (p ∈ $\mathbb{P}$) nebo $\mathbb{Q}$.

Rozšíření pole

Je-li L nadpole pole K, potom je L také vektorovým prostorem nad K s operacemi

a + b . . . součet v L (a, b ∈ L),
λa . . . součin v L (a ∈ L, λ ∈ K).

Existuje proto báze vektorového prostoru L nad K. Vztahem $\dim_K L$ =: [L : K] definujeme tzv. **stupeň rozšíření** L **pole** K. Je-li [L : K] < ∞, pak se L nazývá **konečné rozšíření** pole K.

Buď L nadpole pole K a α ∈ L. α se nazývá **algebraický prvek** nad K :⇔∃f(x) ∈ K[x] \ {0} : f(α) = 0. α se nazývá **transcendentní prvek** nad K :⇔ ∄f(x) ∈ K[x] \ {0} : f(α) = 0.
Příklad:

1. √2 je algebraický prvek nad $\mathbb{Q}$ (f(x) = x^2 − 2, L = $\mathbb{R}$).
2. i je algebraický prvek nad $\mathbb{R}$ (f(x) = x^2 + 1, L = $\mathbb{C}$).
3. e, π jsou transcendentní prvky nad $\mathbb{Q}$ (bez důkazu).

Je-li L nadpole pole K a S ⊆ L, pak definujeme rozšíření K(S) pole K takto:

K(S) :=∩{E ⊆ L | E je podpole pole L, které obsahuje K ∪ S}.

Je-li $S = \{u_1, \ldots, u_r\}$ konečné, pak píšeme $K(S) =: K(u_1, \ldots, u_r)$. Je-li speciálně $S = \{\alpha\}$ jednoprvkové, pak píšeme $K(S) =: K(\alpha)$ („jednoduché rozšíření“ pole K).

Konečná pole

Buď K konečné pole. Potom platí charK = p ∈ P a minimální podpole P pole K je izomorfní se Zp. Protože K je vektorový prostor nad podpolem P, existuje báze {a1, . . . , an} vektorového prostoru K nad P ([K : P] = n ∈ N). Proto platí K = {λ1a1 + ... + λnan | λi ∈ P} a |K| = pn, neboť každý koeficient λi lze zvolit |P| = p způsoby.

Při určování konečného pole K takového, že $|K| = p^n$ ($p \in P$, $n \in N$), tj. při sestavování tabulek jeho operací, lze postupovat následujícícm způsobem:

1. Za minimální podpole pole K se vezme $\mathbb{Z}_p$.
2. Určí se normovaný ireducibilní polynom $q(x) \in \mathbb{Z}_p[x]$, kde grad q(x) = n (konečným počtem kroků).
3. Zkonstruuje se $\mathbb{Z}_p[x] / (q(x))$, což je hledané pole K.

Platí, že α := x + (q(x)) je (po vnoření Zp) kořenem polynomu q(x). Toto α však nemusí být vždy primitivním prvkem K. α je primitivní prvek ⇔ $\alpha^r \neq 1$ pro $0 < r < |K|-1 = p^n - 1$ ⇔ α není kořenem $x^r - 1$ pro $0 < r < p^n - 1$ ⇔ $q(x) \nmid x^r - 1$ pro $0 < r < p^n - 1$.
Ireducibilní polynomy q(x) s touto vlastností se nazývají primitivní polynomy.
Příklad:
Určení $GF(9) = GF(3^2)$: Vezmeme $\mathbb{Z}_3 = \{0, 1, 2\}$ za minimální pole. Polynom $x^2 - x - 1 \in \mathbb{Z}_3[x]$ je ireducibilní, protože nemá v $\mathbb{Z}_3$ žádný kořen. Proto máme $\mathbb{Z}_3[x]/(x^2 - x - 1) \cong \mathbb{Z}_3(\alpha) = GF(9)$, přičemž platí $\alpha^2 = \alpha + 1$. Platí $[GF(9) : \mathbb{Z}_3] = 2$ a tím je zadaná báze $\{1, \alpha\}$. Spočítáme nyní v bázi $\{1, \alpha\}$ prvky $GF(9)$ i s jejich souřadnicemi v bázi:

Prvky	Vyjádřenívsouřadnicích
0	$(0,0)$
$\alpha^0 = 1$	$(1,0)$
$\alpha^1 = \alpha$	$(0,1)$
$\alpha^2 = 1 + \alpha$	$(1,1)$
$\alpha^3 = 1 + 2\alpha$	$(1,2)$
$\alpha^4 = 2$	$(2,0)$
$\alpha^5 = 2\alpha$	$(0,2)$
$\alpha^6 = 2 + 2\alpha$	$(2,2)$
$\alpha^7 = 2 + \alpha$	$(2,1)$
$\alpha^8 = 1$	$(1,0)$

Praktický postup:

1. Zvolíme normovaný ireducibilní polynom $q(x) \in \mathbb{Z}_p[x]$ stupně n. Nechť např. $q(x) = x_n - a_{n-1}x_{n-1} - \ldots - a_1x - a_0$, kde $a_i \in \mathbb{Z}_p$.
2. Položíme q(α) = 0 a uvažujeme bázi $\{1, \alpha, \ldots, \alpha_{n-1}\}$ vektorového prostoru $GF(p_n)$ nad $\mathbb{Z}_p$. Spočítáme použitím q(α) = 0 (tj. $\alpha_n = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha_{n-1}$) mocniny α. Platí-li $\alpha^{(p\hat{}n)-1} = 1$ (tj., $\alpha^j \neq 1$ pro $1 \leq j < p^n - 1$), je zvolený polynom q(x) primitivní. Jinak učiníme další pokus s novým polynomem q(x).