MI-SPOL-2

Tělesa a okruhy: Základní definice a vlastnosti. Konečná tělesa. Okruhy polynomů, ireducibilní polynom.

M neprázdná množina, $+$ a $\cdot$ binární operace na této množině. Trojice $R = (M, +, \cdot)$ je **okruh**, pokud platí:

- $(M, +)$ je **abelovská grupa**
- $(M, \cdot)$ je **monoid**
- platí (levý a pravý) **distributivní zákon**:
  $(\forall a, b, c \in M)(a(b + c) = ab + ac \wedge (b + c)a = ba + ca)$

Buď $R = (M, +, \cdot)$ okruh.

- pokud $\cdot$ komutativní, je R **komutativní okruh**
- $(M, +)$ je **aditivní grupa** okruhu R
- $(M, \cdot)$ je **multiplikativní monoid** okruhu R
- neutrální prvek aditivní grupy je **nulový prvek** (0), neutrální prvek multiplikativního monoidu je **jednička**

Triviální okruh: $(\{0\}, +, \cdot)$ (pokud $0 \cdot 0 = 0$)
$(\mathbb{Z}, +, \cdot)$ je okruh, ale $(\mathbb{Z})N, +, \cdot)$ není

Nenulové prvky $a, b \in M$ z okruhu $(M, +, \cdot)$ jsou **dělitelé nuly**, právě když $a \cdot b = b \cdot a = 0$.
Obor integrity je komutativní okruh, ve kterém neexistují dělitelé nuly.

Navíc (MI-MKY):

- $J \subset R$ **ideál,** pokud:
  - J podokruh R
  - $\forall a \in J, \forall b \in R : a \cdot b \in J, b \cdot a \in J$
- **Faktorokruh okruhu R vůči ideálu J:** $R/J = (\{[a] | a \in R\}, +, \cdot)$
  - $[a]$: třída ekvivalence prvku a podle relace $\equiv \pmod J$
    - $[a] = a + J = \{a + r | r \in J\}$
  - $a \equiv b \pmod J$, pokud $a - b \in J$

Okruh $T = (M, +, \cdot)$ je **těleso**, pokud $(M \setminus \{0\}, \cdot)$ je **abelovská grupa**.

Okruh $(\mathbb{Z}, +, \cdot)$ není těleso, protože chybí inverze k násobení.
$(\mathbb{Q}, +, \cdot)$ je nejmenší číselné těleso
Nejmenší těleso je tzv. triviální těleso $(\{0, 1\}, +, \cdot)$, kde $+$ je XOR a $\cdot$ je AND (sčítání a násobení modulo 2)

Pokud pro $a, b \in T$ platí $ab = 0$, pak $a = 0$ nebo $b = 0$

- důkaz: multiplikativní grupa $(T \setminus \{0\}, \cdot)$ je uzavřená na násobení, takže ab nikdy není 0.
- Každé **těleso** je **obor integrity**

Zobrazení h z okruhu (tělesa) R_1 do okruhu (tělesa) R_2 je **homomorfismus**, pokud h je homomorfismem příslušných aditivních a multiplikativních grupoidů.
Pokud je h bijekce (prosté a na), jde o **izomorfismus**

Mějme okruh R a $a_i \in R, i = 0, 1, ..., n$. Formální výraz tvaru $P(x) = \sum_{i=0}^{n} a_i x^i$ je **polynom nad okruhem** R.

- a_i jsou koeficienty polynomu
- x je formální proměnná
- pokud existuje k t.ž. $a_k \neq 0$, je k stupeň polynomu
- $P(x) = 0$ je nulový polynom s nedefinovaným stupněm

Množina všech polynomů nad okruhem R spolu s operacemi sčítání polynomů a násobení polynomů tvoří **okruh polynomů nad okruhem** R a značí se $R[x]$

Lemma o dělení polynomů: Buď T těleso a $f(x), g(x) \in T[x]$ nenulové polynomy. Pak existují jednoznačně určené polynomy $q(x), r(x) \in T[x]$ t.ž. $f(x) = q(x)g(x) + r(x)$, kde $r(x)$ je buď nulový nebo má ostře menší stupeň než $g(x)$.

Polynom $h(x) \in T[x]$ je **největší společný dělitel polynomů** $f(x)$ **a** $g(x)$, jestliže:

- $h(x)$ dělí $f(x)$ a $g(x)$
- každý polynom dělící $f(x)$ a $g(x)$ dělí taky $h(x)$

Bézoutova rovnost pro polynomy: Buďte $f(x)$ a $g(x)$ nenulové polynomy nad tělesem T. Pak existují polynomy $u(x), v(x) \in T[x]$ takové, že $gcd(f(x), g(x)) = u(x)f(x) + v(x)g(x)$

$deg(f(x) \cdot g(x)) = deg(f(x)) + deg(g(x))$

Polynom $P(x) \in K[x]$ stupně alespoň 1 je **ireducibilní nad okruhem** K, jestliže pro každé dva polynomy $A(x), B(x) \in K[x]$ platí:
$A(x) \cdot B(x) = P(x) \Rightarrow deg(A(x)) = 0 \vee deg(B(x)) = 0$

Těleso s konečným počtem prvků je **konečné**.
Počet jeho prvků je **řád**.

Základní příklad konečného tělesa: $\mathbb{Z}_p = \{0, 1, ..., p-1\}$

- Aditivní grupa $\mathbb{Z}_p^+$:
  - řád p
  - generátor je každý nenulový prvek
- Multiplikativní grupa $\mathbb{Z}_p^\times$:
  - řád $p-1$ (neobsahuje 0)
  - cyklická (existuje generátor)
  - počet generátorů je $\varphi(p-1)$
  - grupa pouze pro p prvočíslo (jinak obsahuje dělitele 0)
  - pokud $k < p$ dělí $p-1$, pak v ní existuje podgrupa řádu k obsahující ty prvky, pro které $a^k = 1$

Řádem konečného tělesa musí být **mocnina prvočísla**, tedy číslo zapsatelné jako p^n, kde p je prvočíslo a n kladné celé číslo.

Všechna tělesa řádu p^n jsou navzájem **izomorfní**.

Těleso s p^n prvky je **Galoisovo těleso** $GF(p^n)$. Prvočíslo p je **charakteristika** tělesa.

- Aditivní grupa:
  - řád p^n
  - neutrální prvek 0
  - inverze k $b_1 b_2 ... b_n$ je (p-b_1)(p-b_2)...(p-b_n)
  - pro $n > 1$ není cyklická
- Multiplikativní grupa:
  - řád $p^n - 1$
  - neutrální prvek 1
  - inverzi ke každému prvku lze pomocí REA nalézt v poly čase
  - vždy cyklická