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

Okruh: $R = (M, +, \cdot)$

pokud: $(M, +)$ je Abelovská grupa (aditivní grupa okruhu)

$(M, \cdot)$ je pologrupa * (multiplikativní pologrupa okruhu)

platí levý a pravý distributivní zákon $a(b+c) = ab + ac$

=> nějaký prvek v $(M, +)$ (třeba nula)

[triviální okruh: $(\{0\}, +, \cdot)$] - neutrální prvek $(M, +)$ = nulový prvek → označíme ho 0 - násobení 0 musí být 0

nenulové prvky $a, b \in M$ takové, že $a \cdot b = 0$ → dělitelé nuly

$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

Obor Integrity: komutativní okruh bez dělitelů nuly

násobení je komutativní

Těleso: okruh, jehož $(M - \{0\}, \cdot)$ je grupa

nenulové dělitele nulou

triviální těleso $(\{0,1\}, +, \cdot)$ - nejmenší (operace jako XOR, AND)

každé (komutativní) těleso je obor integrity

Homomorfismus & Izomorfismus

- fungují pro jednotlivé grupy zvlášť (aditivní & multiplikativní)

$(\mathbb{Q}, +, \cdot)$ - nejmenší číselné těleso

* každý prvek má své inverzní - neplatí komutativita

$P(x) \in K[x]$ stupeň ≥ 1 ireducibilní $\Leftrightarrow \forall A(x), B(x) \in K[x]$

$A(x) \cdot B(x) = P(x) \Rightarrow$ stupeň $A(x) = 0 \vee$ stupeň $B(x) = 0$

Konečná tělesa: konečný počet prvků — každý nenulový prvek generuje

základní příklad $\mathbb{Z}_p$ .... $(M, +)$ - řád p

$(M, \cdot)$ - řád $p-1$ (není prvočíslo)

$(M, \cdot)$ je vždy cyklická, $\varphi(p-1)$ generátorů

obecně: $\mathbb{Z}_n^\times$ je cyklická pokud $n = 2, 4, p^k, 2p^k$ $p \neq 2$

- řád konečného tělesa je vždy p^n (charakteristika)

$GF(p^n)$

$P(x) \in K[x]$ ← okruh polynomů

ireducibilní polynom: $P(x) = A(x) \cdot B(x) \Rightarrow$ stupeň $A(x) = 0 \vee B(x) = 0$

→ chovají se podobně jako prvočísla

(K je okruh → $K[x]$ komutativní okruh polynomů nad okruhem K)

$GF(m^n)$

- sčítání definujeme po složkách modulo m
- násobení modulujeme vzorcem ireducibilním polynomem

- aditivní grupa tělesa $GF(p^n)$
  - má řád p^n
  - nenulových prvků 0^n
  - není cyklická
- multiplikativní grupa
  - má řád p^{n-1}
  - nenulových prvků 0^{n-1}
  - je vždycky cyklická

těleso p^n pro konkrétní n

$n = 1 \rightarrow (\mathbb{Z}_p, +, \cdot)$

$n > 1 \rightarrow$ množina polynomů okruhu $\mathbb{Z}_p[x]$

(stupně nejvýše $n-1$)

→ sčítání po složkách modulo p

→ násobení v okruhu $\mathbb{Z}_p[x]$ mod vzorový ired. pol. stupně n

operace nad GF (m^n)

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i + b_i) x^i$$

$$\left(\sum_{i=0}^{n} a_i x^i\right) \cdot \left(\sum_{i=0}^{m} b_i x^i\right) = \sum_{i=0}^{n+m} \left(\sum_{j+k=i} a_j b_k\right) x^i$$