6. TEORIE POLÍ

Pole

$(A, +, 0, -, \cdot, 1, ^{-1})$ – je i komutativní těleso
je komutativní okruh s jednotkovým a inverzním prvkem kde nejsou dělitelé nuly:

$$\forall a, b \in A \setminus \{0\}: a \cdot b \neq 0$$
$$\forall a, b \in A: (a \cdot b = 0) \rightarrow (a = 0 \vee b = 0)$$
$$A \setminus \{0\} \neq \emptyset$$
$$0 \neq 1$$

$(A, +, 0, -)$ je komutativní (Abelovská) grupa
$(A \setminus \{0\}, \cdot, 1, ^{-1})$ je komutativní (Abelovská) grupa
$(A, \cdot, 1, ^{-1})$ je jen pologrupa, která je komutativní a má jednotkový a inverzní prvek

× není to ale grupa
– v grupě je každý prvek invertibilní a zde není 0 invertibilní jelikož $0^{-1} = \frac{1}{0} = NDEF$

– doplnění: pro okruh platí, že $(A, +, 0, -)$ je Abelovská grupa takže + je uzavřená binární operace nad A, + je asociativní i komutativní a 0 je nulový prvek (neutrální prvek vzhledem k +) a – je inverzní prvek a $\forall a \in A$ platí, že jsou invertibilní
+ $(A, \cdot)$ je pologrupa a tedy $\cdot$ je uzavřená operace na A a je asociativní

– pole je třeba $(\mathbb{Q}, +, \cdot)$ nebo $(\mathbb{R}, +, \cdot)$ a tedy zjednodušeně $\mathbb{Q}$ a $\mathbb{R}$

Podpole

– pokud omezíme nosnou množinu původního pole a nově vzniklé pole má stále vlastnosti pole tak je to podpole původního pole

Minimální pole

– nemá žádná jiná podpole než sebe sama (cokoli se odebere z nosné množiny tak už to nebude pole)
– každé ~~podp~~ pole má jedno minimální podpole (mimo jiné)

Scanned with CamScanner

Řád prvku

- řád prvku a v grupě G – značíme $O(a)$ nebo $ord(a)$ nebo $|a|$ je nejmenší přirozené číslo n že

$$a^n = e \quad \text{kde } e \text{ je neutrální prvek grupy } G$$

$$\underbrace{a \circ a \circ \ldots \circ a}_{n\text{-krát}} = e$$

- jestliže takové n neexistuje (nikdy to nedá e) tak je $ord(a) = \infty$

$(\mathbb{Z},+)$ má $\forall a \in \mathbb{Z}: ord(a) = \infty$

$(\mathbb{Z}_5,+)$ má $\forall a \in \mathbb{Z}: ord(a) = 5$

$ord(1) = 5 \quad \underbrace{1+1+1+1+1}_{5} = 5 = 0$ v $\mathbb{Z}_5$

$ord(4) = 5 \quad 4+4+4+4+4 = 20 = 0$ v $\mathbb{Z}_5$

Charakteristika okruhu

- okruh $(R,+,0,-,\cdot,1)$ má charakteristiku $char\,R$ danou dvěma způsoby:

1) $char\,R = \begin{cases} O(1) & \text{pokud } O(1) \in \mathbb{N} \\ 0 & \text{pokud } O(1) = \infty \end{cases}$ – kde se používá místo $\circ$ přímo ~~sčítání~~ sčítání

   - řád jednotkového prvku

2) $char\,R = \begin{cases} |\{n \cdot 1 \mid n \in \mathbb{Z}\}| & \text{pokud je ta konečná} \\ 0 & \text{jinak} \end{cases}$ – kardinalita množiny

   - velikost množiny (kardinalita) obsahující násobky prvků množiny jednotkovým prvkem

$char\,\mathbb{Z}_5 = 5$
$char\,\mathbb{Z}_{101} = 101$
$char\,\mathbb{Z} = 0$
$char\,\mathbb{Q} = 0$
$char\,\mathbb{R} = 0$

- prostě kolikrát musím sečíst jednotkový prvek abych dostal nulový prvek

- jestliže $char\,K = p$ kde K je pole a p je prvočíslo, pak $\mathbb{Z}_p$ je minimální podpole toho pole K (nebo je s ním minimálním izomorfní – takže to je prostě minimální podpole)

Scanned with CamScanner

Rozšíření pole

- pokud rozšíříme nosnou množinu a stále to bude pole
- dalo by se nazvat i nadpole
- pole L je rozšířením pole K takové že existuje podpole S pole L že $S \subseteq L$ a pak je definováno to rozšíření pole K jako
  $L = K(S) = \bigcap \{E \subseteq L \mid E$ je podpole pole L, které obsahuje $K \cup S\}$
- je-li S jednoprvkové $S = \{\alpha\}$ tak se jedná o jednoduché rozšíření pole K, tedy $K(S) = K(\alpha)$

Konečná pole (Galoisova pole)

- je pole, které má konečný počet prvků, značí se $GF(p^k)$ a počet prvků je p^k – např. $GF(3^2) = GF(9)$ a má tedy 9 prvků
- konečná (Galoisova) pole mají charakteristiku

$$\mathrm{char}\ GF(p^k) = p^k$$

- p je prvočíslo a $k \in N$ kde $k > 0$
- kdyby bylo $k = 0$ tak je $GF(p^0)$ a tedy $GF(1)$, což nejde, protože víme, že pole má nulový prvek 0 a jednotkový prvek 1 kde $0 \neq 1$ a tedy nejmenší GF je $GF(2)$ tedy $GF(2^1)$
- konečná tělesa jsou komutativní (konečná pole jsou komutativní)
- GF lze klasifikovat podle velikosti
  - $\Rightarrow$ pokud nalezneme dvě $GF(2)$ tělesa tak jsou izomorfní
    - pouze jedno je bijektivním zobrazením toho druhého
- minimální podpole pole $GF(p^k)$ je izomorfní se zbytkovou třídou Z_p — $GF(9)$ a Z_9
- jestliže máme konečné pole K a jeho podpole P, tak to K je vektorovým prostorem nad podpolem P
  - $\Rightarrow$ konečné pole je vektorovým prostorem nad svými podpoli
  - $\Rightarrow$ konečné pole má tedy danou bázi vektorového prostoru danou $\{1, \alpha, \dots, \alpha^{k-1}\}$ tedy $\{\alpha^0, \dots, \alpha^{k-1}\}$
    nebo i $\{\alpha^0, \dots, \alpha^m\}$ kde $n = [K:P]$, $n \in N$ je rozdíl velikosti pole a podpole – pro bin. čísla je lepší bázi psát jako $\{\alpha^{k-1}, \alpha^{k-2}, \dots, \alpha^0\}$

Tvorba konečného pole

- máme zadáno vytvořit konečné (Galoisovo) pole $GF(3^2)$ nebo taky $GF(9)$
- konečné pole sestavíme tak, že si vezmeme jeho minimální podpole
- víme, že jeho minimální podpole je izomorfní se zbytkovou třídou Z_3
- vezmeme tedy Z_3 a množinu všech polynomů nad Z_3 tedy

$\boxed{Z_3[x]}$

, kdyby nebyl ireducibilní tak to není konečné pole

- vyfaktorujeme-li $Z_3[x]$ nějakým ireducibilním polynomem $m(x) \in Z_3[x]$ který v $Z_3[x]$ nemá žádného dělitele a ani kořeny z Z_3 + musí být normalizovaný a primitivní

(tohle platí, protože je ireducibilní)

tak získáme faktorovou množinu, která bude nosnou množinou toho $GF(9)$

- ten ireducibilní polynom musí být normovaný polynom stupně k a taky primitivní
- pro Z_3 tedy $m(x) = x^2 - x - 1$ a pro Z_2 a $GF(8)$ třeba $x^3 + x + 1$, $GF(16)$ $x^4 + x + 1$
- pro polynomy $Z_p[x]$ platí že mají koeficienty a ze Z_p

$\Rightarrow$ jedná se tedy o kongruenci $Z_3[x]$ modulo $m(x)$ a výsledná množina $Z_3[x] \setminus m(x)$ ~~je~~ obsahuje množiny (třídy) kongruentních prvků vzhledem k modulo $m(x)$

- víme že $GF(3^2)$ musí mít 9 prvků
- 0 a 1 kde $0 \neq 1$ má každé pole – zbývá najít zbylých 7
- máme tedy $GF(3^2)$ a $m(x) = x^2 - x - 1$
- dosadíme-li $m(\alpha) = \alpha^2 - \alpha - 1$
- máme bázi vektorového prostoru $GF(9) = \{1, \alpha\}$
- položíme-li $m(\alpha) = 0$ máme přepisovací pravidlo pro α^2 tedy $\alpha^2 = \alpha + 1$
- všechny reprezentanty tříd zjistíme tak že tedy $\alpha^0, \alpha^1, \alpha^2, \alpha^3, \dots \alpha^{(p^k)-1}$ vymodulujeme $m(\alpha) = \alpha^2 - \alpha - 1$
- $\alpha^{(p^k)}$ musí dát zase 1 – polynom je primitivní ! platí $\alpha^{(p^k)} = 1$ a $\alpha^m \neq 1$ kde $n > 0 \wedge m < p^k$
- všechny prvky (reprezentanty tříd) můžeme vyjádřit vektorem zastoupení ~~už~~ jednotlivých prvků báze v daném reprezentantovi
- pro p a k a $GF(p^k)$ kde $p = 2$ dostáváme cyklické binární kódy na $\boxed{k}$ bitech $\Longrightarrow$ využití v kryptografii

Scanned with CamScanner

Př.: $GF(9) = GF(3^2)$

- minimální podpole je izomorfní se $\mathbb{Z}_3$
- polynom (ireducibilní, normovaný a primitivní) je $m(x) = x^2 - x - 1$
- tedy $m(\alpha) = \alpha^2 - \alpha - 1$
- tedy $m(\alpha) = 0 \;..\; \alpha^2 - \alpha - 1 = 0 \;..\; \alpha^2 = \alpha + 1$
- báze vektorového prostoru je $\{1, \alpha\}$ tedy $\{\alpha^0, \alpha^1\}$

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

— už je to cyklické

splníme $\alpha^{(p^k)} = 1$
a žádný jiný prvek α^m kde $m > 0 \wedge m < p^k$ není 1

→ tedy $\alpha^5 : \alpha^2 - \alpha - 1$
tak vyjde po dělení zbytek $5\alpha + 3$ ale jsme v $\mathbb{Z}_3$ takže $2\alpha + 0$ takže 2α **!**

- tedy $GF(9) = (\{0, 1, \alpha, 1+\alpha, 1+2\alpha, 2, 2\alpha, 2+2\alpha, 2+\alpha\}, +, \cdot)$

Př.: $GF(2^4) = GF(16)$ $\quad m(x) = x^4 + x + 1$

- výsledkem je Galoisovo pole vytvořené z $(m(x))$
- báze vektorového prostoru je $\{1, a, a^2, a^3\}$ tedy spíš $\{a^3, a^2, a, 1\}$
  ↳ z lin. čísel bázi zapisujeme sestupně tohle

	GP
	0000
$a^0 = 1$	0001
$a^1 = a$	0010
$a^2 = a^2$	0100
$a^3 = a^3$	1000
$a^4 = a + 1$	0011
$a^5 = a^2 + a$	0110
$a^6 = a^3 + a^2$	1100
$a^7 = a^3 + a + 1$	1011
$a^8 = a^2 + 1$	0101
$a^9 = a^3 + a$	1010
$a^{10} = a^2 + a + 1$	0111
$a^{11} = a^3 + a^2 + a$	1110
$a^{12} = a^3 + a^2 + a + 1$	1111
$a^{13} = a^3 + a^2 + 1$	1101
$a^{14} = a^3 + 1$	1001
$a^{15} = 1 = a^0$	0001

cykličnost

↳ cykličnost

- generuje to tedy cyklické kódy o k tedy 4 bitech ~~...~~ 16 jich je nulových a proto jsou cyklické
- tyto polynomy jsou reprezentanti tříd tedy třída $a^2 + a$ je $[a^2 + a]_{m(x)}$

Scanned with CamScanner