Cvičné příklady z Konečných těles

Tělesa, polynomy, homomorfismy těles, prvotěleso

1. Najděte všechny ireducibilní polynomy stupně 1, 2, 3, 4 nad $\mathbb{Z}_2$

   Řešení: $\{x, x+1, x^2+x+1, x^3+x+1, x^3+x^2+1, x^4+x+1, x^4+x^3+1, x^4+x^3+x^2+x+1\}$

   Komentář: *polynomy stupně 1 jsou ireducibilní všechny (oba), polynomy vyšších stupňů musí mít nenulový absolutní člen (jinak lze vytknout x), tyto kandidáty zkouším dělit ireducibilními polynomy nižších stupňů (každý neireducibilní lze rozložit na součin ireducibilních)*

2. Spočtěte α^{40} v tělese $\mathbb{Z}_2[\alpha] / (\alpha^6 + \alpha^5 + 1)$

   Řešení: $\alpha^3 + \alpha^2 + \alpha$

   Komentář: $\alpha^{40} = \left(\left(\alpha^{10}\right)^2\right)^2$

3. Ukažte, že polynom $f(x) = x^3 + x + 1$ má v tělese $\mathbb{Z}_2[\alpha]/(f(\alpha))$ kořeny $\alpha, \alpha^2, \alpha^2 + \alpha$

   Komentář: *Buď dosadím a spočítám, že* $f(\alpha) = f(\alpha^2) = f(\alpha^2 + \alpha) = 0$. *Nebo spočítám* $g(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^2+\alpha)$, *pokud jsou to všechny kořeny, pak* $g(x) = f(x)$, jinak $g(x) \mid f(x)$.

4. Najděte všechny kořeny polynomu $f(x) = x^3+2x+1$ v tělese $\mathbb{Z}_3[\alpha]/(f(\alpha))$

   Řešení: $\{\alpha, \alpha+1, \alpha+2\}$

   Komentář: $x^3+2x+1 = 0 \Rightarrow f(\alpha) = 0 \Rightarrow \alpha$ *je kořen* $\Rightarrow f(x) : (x-\alpha) = x^2 + \alpha x + (2+\alpha^2) \Rightarrow$ *hledám kořeny* $x^2 + \alpha x + (2+\alpha^2)$. *Lze zkusit použít klasický vzorec pro výpočet kořenů kvadratické rovnice, pokud najde kořeny, vše je OK, pokud nelze spočítat, neznamená, že kořeny nemám (tady lze použít). Variantou je rozložit polynom podle Vietových vzorců a pokusit se dopočítat. Hrubá síla: zkoušet polynom dělit všemi možnostmi, které připadají v úvahu, a čekat, kdy se podaří vydělit beze zbytku. Možnosti* $= \{x-1, x-2, x-\alpha, x-2\alpha, x-(\alpha+1), x-(\alpha+2), x-(2\alpha+1), x-(2\alpha+2)\}$

   Elegantní řešení: α *je kořen, dle V.3.7. jsou další kořeny* $\alpha^3 = \alpha + 2$ *a* $\alpha^9 = \alpha + 1$.

Charakterizace konečných těles

1. Tvrzení o vícenásobných kořenech a derivaci:

   (a) Buď K těleso a $()' : K[x] \to K[x]$ zobrazení def. vztahem $\left(\sum_{i=0}^{n} a_i x^i\right)' = \sum_{i=1}^{n} i a_i x^{i-1}$ Potom $()'$ je endomorfismus $K[x]$ jakožto vektorového prostoru nad K. (Dokažte)

   Komentář: *Ověřit sčítání a násobení skalárem.*

   (b) Dokažte, že platí $(fg)' = f'g + fg'$ *(Nápověda: indukce + a))*

(c) Dokažte, že $a \in K$ je vícenásobným kořenem polynomu $f(x) \in K[x]$ $\left((x-a)^2 / f(x)\right)$ právě tehdy, když a je kořenem polynomu $f'(x)$.

Řešení: (obecné a asi ale jen částečné) *a kořenem* $f(x) \Rightarrow f(x) = (x-a)^n g(x) \Rightarrow f'(x) = n(x-a)^{n-1}g(x) + (x-a)^n g'(x) = (x-a)^{n-1}(ng(x) + (x-a)g'(x))$. *Pro* $n \geq 2$ *je a vícenásobným kořenem* $f(x)$ *a také kořenem* $f'(x)$.

2. Které podtěleso tělesa komplexních čísel je rozkladovým nadtělesem polynomu $x^3 - 5 \in \mathbb{Q}[x]$

   Řešení: *Vždy funguje použít kořen a primitivní odmocninu z 1* $\Rightarrow \mathbb{Q}\left[\sqrt[3]{5}, e^{\frac{2\pi i}{3}}\right] = G$ *Lze také vydělit kořenem* $\sqrt[3]{5}$ *a poté spočítat klasickým vzorcem kořeny* $\Rightarrow \mathbb{Q}\left[\sqrt[3]{5}, \sqrt{3}i\right] = H$, *obě rošíření jsou stejná, protože je to rovnost dvou vektorových prostorů nad* $\mathbb{Q}$ ($dim_{\mathbb{Q}}G = dim_{\mathbb{Q}}H = 6$).

Struktura konečných těles

1. Určete výčtem prvků podtěleso F_4 tělesa $\mathbb{Z}_2[\alpha] / \left(\alpha^4 + \alpha + 1\right)$

   Řešení: *Zadané těleso je* F_{16} . *Z důkazu věty 3.1 se dá vyčíst, že* F_{16} *obsahuje* F_4 *a to můžeme najít jako rozkladové rozšíření* $\mathbb{Z}_2$ *určené polynomem* $x^4 - x$. *Jenže* $x^4 - x = x(x-1)(x^2+x+1)$ *takže to rozkladové rozšíření by mělo odpovídat* $\mathbb{Z}_2[\alpha] / \left(\alpha^2 + \alpha + 1\right)$, *to je* $\{0, 1, \alpha, \alpha+1\}$

2. Ukažte, že α není primitivní prvek tělesa $F = \mathbb{Z}_3[\alpha] / \left(\alpha^2 + 1\right)$. Jaký je řád α ? Najděte v F nějaký primitivní prvek.

   Řešení: α *má řád 4* $\Rightarrow \alpha$ *není primitivní,* $\langle\alpha+1\rangle = \langle\alpha+2\rangle = \langle 2\alpha+1\rangle = \langle 2\alpha+2\rangle = \{1, 2, \alpha, 2\alpha, \alpha+1, \alpha+2, 2\alpha+1, 2\alpha+2\}$

3. Najděte minimální polynom prvku $\alpha^3+\alpha^2$ nad tělesem $\mathbb{Z}_2[\alpha] / \left(\alpha^4 + \alpha + 1\right)$.

   Řešení: *Zadané těleso prvek* $\alpha^3 + \alpha^2$ *obsahuje* $\Rightarrow$ *primitivní polynom je* $(x - \alpha^3 + \alpha^2)$.

   Pokud budeme uvažovat primitivní polynom nad tělesem $\mathbb{Z}_2 \Rightarrow$ *přes konjugované prvky*: $\beta = \alpha^3 + \alpha^2, \beta^2 = \alpha^3 + \alpha^2 + \alpha + 1, \beta^4 = \alpha^3 + \alpha, \beta^8 = \alpha^3 \Rightarrow m(x) = (x + \alpha^3 + \alpha^2)(x + \alpha^3 + \alpha^2 + \alpha + 1)(x + \alpha^3 + \alpha)(x + \alpha^3) = x^4 + x^3 + x^2 + x + 1$.

   Komentář: *Známe už 3 varianty hledání minimálního polynomu: 1) obecné koeficienty (musím vědět, jakého stupně má polynom být); 2) mocniny bázových prvků a jejich lineární kombinace (musím mít konečné rozšíření); 3) konjugované prvky (když znám jeden kořen polynomu)*

4. Zvolte si nějakou reprezentaci tělesa F_4 a najděte nad F_4 všechny ireducibilní polynomu stupně 1 a 2.

   Řešení: *Vybrala jsem si jako reprezentaci* F_4 *stejnou jako v prvním příkladě, tedy* $\{0, 1, \alpha, \alpha+1\}$ *a ireducibilní polynomy stupně 1 by měly být snad všechny, tedy* $x, x+1, x+\alpha, x+\alpha+1$. *Reducibilní polynomy stupně dva jsou součinem dvou ireducibilních stupně 1* $\Rightarrow$ *ty vyloučím a zbydou ireducibilní*: $x^2 + x + \alpha, x^2 + x + \alpha + 1, x^2 + \alpha x + 1, x^2 + \alpha x + \alpha, x^2 + (\alpha+1)x + 1, x^2 + (\alpha+1)x + \alpha$.

5. Reprezentujte maticemi prvky tělesa F_9 s využitím polynomu $f(x) = x^2 + x + 2 \in F_3[x]$. Ukažte, že α je primitivním prvkem tělesa $F_3[\alpha]/(f(\alpha))$ **(POZOR byla chyba v zadání!)**

   Řešení: *Tady jsem jen opsala ten postup, co dělal Šaroch na přednášce, takže to asi moc nepomůže...* $f(x) = x^2 + x + 2 \in F_3[x]$ *má doprovodnou matici* $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathrm{A}$ *a pak* F_9 *můžeme reprezentovat (podle nějaké věty) jako* $\{0, I, 2I, A, A+I, A+2I, 2A, 2A+I, 2A+2I\}$. *Postupným umocňováním* α *lze ukázat, že má řád 8.*

   Z konzultace mám poznámku: ověřit, že α^2, α^4 *se nerovnají 1 (dokonce* $\alpha^4 = -1$ *)* $\Rightarrow \alpha$ *generuje vše (já osobně nechápu, pokud někdo dodá jakékoliv vysvětlení, ráda ho sem přidám)*

6. (z konzultace) Najděte nějaký kořen polynomu $f(x) = x^4 + x + 1$ v tělese $\mathbb{Z}_2[\alpha] / \left(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1\right)$.

   Komentář: *Kdo si poctivě psal, co Šaroch říkal a dodá kompletní řešení? :-)*

Odmocniny z jedné a cyklotomické polynomy

1. Rozložte polynom $Q_{15}(x) \in F_2[x]$ na ireducibilní činitele. *(Nápověda: použít V.4.3.)*

   Řešení: $\left(x^4 + x^3 + 1\right)\left(x^4 + x + 1\right)$

   Komentář: $Q_{15}(x) = \frac{x^{15}-1}{Q_1(x)Q_3(x)Q_5(x)} = x^8 + x^7 + x^5 + x^4 + x^3 + x + 1$, V.4.3. $\Rightarrow d = 4 \Rightarrow Q_{15}(x)$ *se rozkládá na 2 ireducibilní polynomy stupně 4; ty dopočítám porovnáním koeficientů*

2. Označme $Q_n(x)$ n-tý cyklotomický polynom nad Q a $R_n(x)$ n-tý cyklotomický polynom nad tělesem K charakteristiky $p \nmid n$. Dokažte, že koeficienty $R_n(x)$ jsou stejné jako koeficienty $Q_n(x)$ mod p.

   Komentář: *Využila bych V.4.2. 2), ale do detailů se pouštět nebudu :-)*

3. Najděte primitivní deváté odmocniny z 1 v $\mathbb{Z}_{19}$.

   Řešení: $4, 5, 6, 9, 16, 17$

   Komentář: *Bude jich právě* $\varphi(9) = 6$ *a jsou to kořeny* $Q_9(x) = x^6 + x^3 + 1$ *v* $\mathbb{Z}_{19}$ *(rozkládá se dle V.4.3. na šest ireducibilních polynomů stupně 1); spočítala jsem to porovnáním koeficientů, ale musela jsem to narvat Mathematice... (Jen tak btw. řešením jsou právě všechny generátory* $\mathbb{Z}_{19}*$*, to asi nebude úplně náhoda...)*

4. Nechť K je libovolné těleso, $n > 1$. Dokažte, že polynom $x^{n-1} + x^{n-2} + ... + x + 1$ je rozložitelný kdykoliv je n složené číslo.

5. Najděte nejmenší prvočíslo p takové, že $x^{22} + x^{21} + ... + x + 1$ je ireducibilní nad F_p.

6. Dokažte následující vlastnosti cyklotomických polynomů (nad tělesem, kde existují):

(a) $Q_{mp}(x) = \frac{Q_m(x^p)}{Q_m(x)}$, kde p je prvočíslo, $p \nmid m$.

(b) $Q_{mp}(x) = Q_m(x^p)$, kde p je prvočíslo, $p \mid m$.

(c) $Q_{mp^k}(x) = Q_{mp}(x^{p^{k-1}})$, kde p je prvočíslo, $m, k \in \mathbb{N}$.

(d) $Q_{2n}(x) = Q_n(-x)$, kde $n \geq 3$ liché.

(e) $Q_n(0) = 1$, kde $n \geq 2$.

(f) $Q_n(x^{-1})x^{\varphi(n)} = Q_n(x)$, kde $n \geq 2$.

(g) $Q_n(1) = \begin{cases} 0 & n = 1 \\ p & n \text{ mocnina prvočísla} \\ 1 & \text{jinak} \end{cases}$

(h) $Q_n(-1) = \begin{cases} 0 & n = 2 \\ -2 & n = 1 \\ p & n \text{ dvojnásobek mocniny prvočísla} \\ 1 & \text{jinak} \end{cases}$

Möbiova inverzní formule

1. Dokažte, že $\mu(mn) = \mu(m)\mu(n)$, pokud $NSD(m, n) = 1$.
2. Dokažte pro libovolné $n \in \mathbb{N}$ rovnost $\sum_{d|n} \frac{\mu(d)}{d} = \frac{\varphi(n)}{n}$, kde φ je Eulerova funkce *(Nápověda: Zkusit použít MIF).*
3. Dokažte, že $\sum_{d|n} \mu(d)\varphi(d) = 0$ pro všechna $n \in \mathbb{N}$.
4. Dokažte, že $PMIP_{q,n} \leq \frac{1}{n}(q^n - q)$ (horní odhad $PMIP_{q,n}$) a $PMIP_{q,n} \geq \frac{1}{n}q^n - \frac{q}{n(q-1)}(q^{\frac{n}{2}} - 1)$ (horní odhad $PMIP_{q,n}$).
5. Vypočtěte $Q_{30}(x)$.

   Řešení: $x^8 + x^7 - x^5 - x^4 - x^3 + x + 1$

   Komentář: *dle vzorce odvozeného pomocí Möbiovy inverzní formule* $Q_{30}(x) = \frac{(x^2-1)(x^3-1)(x^5-1)(x^{30}-1)}{(x-1)(x^6-1)(x^{10}-1)(x^{15}-1)} = x^8 + x^7 - x^5 - x^4 - x^3 + x + 1$ *(jak ten zlomek spočítat ručně?)*

Nápověda: Poslední úlohu z předchozí série zkusit dokázat pomocí Möbiovy funkce.

Faktorizace polynomů nad konečným tělesem

1. Nechť $f(x)$ je polynom nad tělesem F_{p^m} takový, že $f'(x) = 0$. Dokažte, že existuje $g(x) \in F_{p^m}[x]$ tak, že $f(x) = (g(x))^p$.
2. $f(x) = x^8 + 2x^6 + x^5 + 2x^3 + x^2 + 2 \in \mathbb{Z}_3[x]$. Nalezněte ireducibilní rozklad $f(x)$.
3. $f(x) = x^8 + x^6 + x^4 + x^3 + 1 \in \mathbb{Z}_2[x]$. Nalezněte ireducibilní rozklad $f(x)$.
4. Ukažte, že polynom $x^4 + 1$ je ireducibilní nad $\mathbb{Q}$, ale rozkládá se nad každým konečným tělesem.