NI-MPI cvičení 9 handout 13. února 2025
Problémy, návrhy apod. hlaste v GitLabu.
Verze souboru: 2023-12-04 10:32.

Obsah

Co byste si měli z tohoto cvičení odnést:

- Jak poznat, jestli daná trojice „množina a dvě binární operace“ tvoří okruh nebo těleso.
- Jak počítat v tělesech, kde se násobí modulo ireducibilní polynom.

A co byste se měli doučit, pokud to ještě/už neumíte:

- Jak funguje rozšířený Euklidův algoritmus.
- Co je to ireducibilní polynom.

22 Okruhy a tělesa

Definice 22.1 — okruh (*ring*). Buďte M neprázdná množina a $+$ a $\cdot$ binární operace na této množině. Řekneme, že trojice $R = (M, +, \cdot)$ je okruh, pokud platí:

- $(M, +)$ je **abelovská grupa**,
- $(M, \cdot)$ je **monoid**,
- platí (levý a pravý) **distributivní zákon**:

$$(\forall a, b, c \in M)(a(b + c) = ab + ac \wedge (b + c)a = ba + ca).$$

Definice 22.2 — těleso (*field*). Okruh $T = (M, +, \cdot)$ se nazývá těleso, jestliže $(M \setminus \{0\}, \cdot)$ je abelovská grupa. Tuto grupu nazýváme multiplikativní grupou tělesa T.

Cvičení 22.1 Zjistěte, zda následující množina s operacemi obvyklého sčítání a násobení čísel tvoří okruh:

(a) Množina celých sudých čísel.

(b) Množina celých lichých čísel.

(c) Množina celých čísel.

(d) Množina nezáporných celých čísel.

(e) Množina racionálních čísel.

Cvičení 22.2

(a) Je množina matic $(\mathbb{R}^{n,n}, +, \cdot)$ se sčítáním po prvcích a maticovým násobením okruhem?

(b) Je tělesem? Pokud není, jakou podmnožinu jejího nosiče lze vzít, aby tělesem byla (při použití stejných

binárních operací)?

Cvičení 22.3 Uvažujme nějakou abelovskou grupu $G = (M, +)$ a množinu všech homomorfismů z G do G. Označme ji $\mathrm{End}(G)$ (takovému homomorfismu se říká endomorfismus). Zaveďme sčítání homomorfismů $f, g \in \mathrm{End}(G)$ takto:

$$\forall x \in G, (f+g)(x) = f(x) + g(x).$$

Je $(\mathrm{End}(G), +, \circ)$ okruhem? Je tělesem? Symbolem $\circ$ značíme skládání zobrazení jako v předchozích cvičeních. ■

23 Konečná tělesa řádu p^n

Jako další zajímavý studijní materiál je k dispozici ukázkový SageMath Jupyter notebook.

Pro hledání inverzních prvků v $\mathbb{Z}_n^\times$ se používá rozšířený Euklidův algoritmus. Již byste jej měli znát, ale pro jistotu si jej nyní připomeneme.

Základní cvičení 23.1 V tělese $\mathbb{Z}_{263}$ najděte multiplikativní inverzi k prvku 112.

Základní cvičení 23.2 Rozhodněte, zda je polynom $P(x)$ ireducibilní nad tělesem $\mathbb{Z}_5$, kde

(a) $P(x) = x^3 + 2x + 1$;

(b) $P(x) = x^2 + 2x + 2$;

■

Základní cvičení 23.3 Rozhodněte, zda je polynom $P(x)$ ireducibilní nad tělesem $\mathbb{Z}_3$, kde

(a) $P(x) = 2x^4 + x^3 + 2x + 1$;

(b) $P(x) = x^4 + x^3 + x + 2$;

(c) $P(x) = x^4 + x + 2$.

Cvičení 23.4 Sestavte Cayleyho tabulky pro obě operace pro těleso $GF(2^2)$, kde se násobí modulo x^2+x-1. Najděte neutrální prvky, generátory a inverzní prvek k $x+1$ a x.

Cvičení 23.5 Sestavte Cayleyho tabulku pro násobení pro těleso $GF(3^2)$, kde se násobí modulo x^2-x-1.

Cvičení 23.6 Najděte všechny ireducibilní polynomy z okruhu $\mathbb{Z}_2[x]$ stupně menšího než 5.

Základní cvičení 23.7 V tělese $GF(3^2)$, kde se násobí modulo ireducibilní polynom x^2+2x+2, najděte

(a) všechna y taková, aby $21(y+11)=01+y$,

(b) najděte všechny generátory multiplikativní grupy tohoto tělesa.

Cvičení 23.8 Uvažujme těleso $GF(2^3)$, kde se násobí modulo x^3+x+1.

(a) Definujte pojem ireducibilní polynom nad tělesem $\mathbb{Z}_2$.

(b) Najděte inverzní prvek k prvku 010.

(c) Vypočítejte

$$100\cdot(010)^{-1}+010\cdot 010$$

Cvičení 23.9 V tělese $GF(3^3)$ kde se násobí modulo x^3+2x+2 najděte

(a) inverzní prvek k prvku 011,

(b) vypočtěte $101\cdot 222$.

Cvičení 23.10 V tělese $GF(2^3)$, kde se násobí modulo x^3+x^2+1, najděte

(a) inverzní prvek k prvku 101,

(b) všechna y z tohoto tělesa splňující rovnici

$$101\cdot(100+y)=100\,.$$

Cvičení 23.11 Uvažujte těleso $GF(2^4)$, kde se počítá modulo polynom x^4+x^3+1.

(a) Najděte inverzi k prvku 1100.

(b) Vyřešte rovnici $(y+1010)(0101+1100)=0110$.

(c) Najděte všechna y z tohoto tělesa splňující rovnici

$$y^2+y+1010=0000\,.$$

Cvičení 23.12 Buď α tzv. zlatý řez, tedy kořen polynomu x^2-x-1. Označme $\mathbb{Z}_3(\alpha)=\{a\alpha+b \mid a,b\in\mathbb{Z}_3\}$ množinu, kde se sčítá po složkách modulo 3 (např. $(\alpha+2)+(2\alpha+2)=3\alpha+4=0\alpha+1=1$, v jiném zápisu $12+22=01$) a násobí klasicky (např. $(2\alpha+1)\cdot\alpha=2\alpha^2+\alpha=2(\alpha+1)+\alpha=3\alpha+2=2$). Je $\mathbb{Z}_3(\alpha)$ těleso? Jestli ano, najděte Cayleyho tabulku pro násobení. (Srovnejte s Příkladem 23.5) ∎

Cvičení 23.13 Nechť $v(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ je polynom z okruhu $\mathbb{Z}_p[x]$, kde p je prvočíslo a m je kladné celé číslo. Dokažte že platí

$$(v(x))^p = v(x^p),$$

tj. že umocnit polynom $v(x)$ na p je to samé, jako do něho dosadit jako argument x^p.
[Nápověda: lze dokázat pomocí Fermatovy věty a vhodně použité binomické věty]

Cvičení 23.14 V tělese $GF(3^3)$, kde se násobí modulo ireducibilní polynom $x^3 + 2x + 1$, najděte všechna y taková, aby $y^{107} = 111$.

Cvičení 23.15 Rozhodněte, jestli je polynom $4x^3 + 2x^2 + 4x + 2$ ireducibilní nad $\mathbb{Z}_5$.

Základní cvičení 23.16 Mějme těleso $GF(5^3)$, kde se násobí modulo ireducibilní polynom $x^3 + 3x + 3$.

(a) Nalezněte inverzní prvek vzhledem k násobení k prvku $x^2 + 2x$.

(b) Nalezněte všechna $y \in GF(5^3)$, která splňují $120 \cdot y^2 = 111$.

Cvičení 23.17 Mějme těleso $GF(5^3)$, kde se násobí modulo ireducibilní polynom $x^3 + 3x + 3$.

(a) Nalezněte inverzní prvek vzhledem k násobení k prvku $x^2 + 2x + 1$.

(b) Nalezněte všechna $y \in GF(5^3)$, která splňují $121 \cdot (y^2 + y + 1) = 101$.

Cvičení 23.18 Mějme dvě tělesa, , F a F', prvočíselného řádu p. Dokažte, že jsou tato tělesa izomorfní.

Cvičení 23.19 Mějme dvě tělesa, F a F', řádu 8. V F se násobí modulo x^3+x+1 a v F' modulo x^3+x^2+1. Nalezněte izomorfismus těchto dvou těles.

Řešení

Řešení Cvičení 22.1: (a) ani okruh (chybí neutrální prvek vůči násobení), (b) ani okruh, ani těleso, (c) okruh, ale ne těleso, (d) ani okruh (e) těleso.

Řešení Cvičení 22.2: Okruh ano, těleso ne. Ani podmínka regularity nestačí, neboť součet regulárních matic nemusí být regulární. Dokonce ani regulární diagonální nefungují.

Řešení Cvičení 23.1: jelikož $23 \cdot 263 + (-54) \cdot 112 = 1$, je $112 \cdot (-54) \equiv 1 \pmod{263}$ a tedy $112^{-1} = -54 \equiv 209 \pmod{263}$

Řešení Cvičení 23.3: (a) Protože $P(1) = 0$, má polynom kořen a není ireducibilní. (b)Snadno spočteme, že $P(0) = 2$, $P(1) = 2$, $P(2) = 1$. Proto $P(x)$ nemá kořen. Přesto není polynom $P(x)$ ireducibilní, neboť lze vyjádřit jako $P(x) = (x^2 + x + 2) \cdot (x^2 + 1)$. (c) $P(x)$ je ireducibilní.

Řešení Cvičení 23.4: Celkově tabulka pro operaci násobení vypadá takto:

·	01	10	11
01	01	10	11
10	10	11	01
11	11	01	10

Generátory jsou jak 10 tak 11.

Řešení Cvičení 23.5: Náznak řešení:

·	01	02	10	11	12	20	21	22
21	21	12	02	20	11	01	22	10

Využijte distributivního zákona! Např. víme-li, že $21 \cdot 01 = 21$ a $21 \cdot 10 = 02$, spočítáme $21 \cdot 12 = 21 \cdot (10 + 01 + 01) = 02 + 21 + 21 = 44 = 11$.

Řešení Cvičení 23.6: Polynomy stupně 1 jsou všechny ireducibilní, $x^2 + x + 1$ je jediný ireducibilní stupně 2, další ireducibilní jsou: $x^3 + x^2 + 1$, $x^3 + x + 1$, $x^4 + x + 1$, $x^4 + x^3 + 1$, $x^4 + x^3 + x^2 + x + 1$

Řešení Cvičení 23.7: (a) Jelikož x^2 se v této grupě rovná $x+1$ a $(2x+1)(x+1) = 2x^2+1 = 2x+2+1 = 2x$, můžeme rovnici pomocí distributivního zákona

$$21(y + 11) = 01 + y$$

přepsat do tvaru

$$21(y + 11) = 21y + 21 \cdot 11 = 21y + 20 = 01 + y.$$

K obou stranám rovnice přičteme $02y + 10$ a dostaneme

$$21y + 02y = 20y = 11.$$

Je třeba najít multiplikativní inverzi prvku 20. Pak po úpravě platí, že

$$y = 20^{-1} \cdot 11.$$

Inverzi k $20 = 2x$ najdeme buď pomocí rozšířeného Euklidova algoritmu, nebo si prostě všimneme, že

$$2x(2x + 1) = x^2 + 2x = x + 1 + 2x = 1.$$

Dostáváme tak

$$y = 21 \cdot 11 = 20\,,$$

jak jsme již spočítali výše.

(b) Z přednášky víme, že multiplikativní grupy těles $GF(p^k)$ jsou vždy cyklické. Jelikož v případě $GF(3^2)$ má multiplikativní grupa řád 8 (prvek 00 musíme vyhodit), má celkem $\varphi(8) = 4$ generátorů. Zkusme jeden z nich najít a vygenerovat pomocí něho všechny ostatní prvky. Začněme např. s prvkem $10 = x$ (prvky 01 a 02 jistě generátory nejsou). Při násobení využíváme toho, že v zadaném tělese je $x^2 = x + 1$:

$$x^2 = x + 1, x^3 = x^2 + x = 2x + 1, x^4 = 2x^2 + x = 2, x^5 = 2x, x^6 = 2x + 2, x^7 = x + 2, x^8 = 1,$$

a tedy 10 je generátor.

Dále použijeme větu, která říká, že umocníme-li generátor na všechny exponenty nesoudělné s řádem (pro řád 8 tedy čísla 1,3,5,7), dostaneme všechny generátory. Dle tohoto návodu dostáváme výsledek: všechny generátory jsou prvky 10, 21, 20 a 12.

Řešení Cvičení 23.8: (b) 101, (c) 110

Řešení Cvičení 23.9: (a) 120, (b) 1.

Řešení Cvičení 23.10: (a) 111, (b) 010

Řešení Cvičení 23.11: Označme polynom ze zadání $p(x) = x^4 + x^3 + 1$.

(a) Použitím jednoho kroku rozšířeného Euklidova algritmu dostáváme Bézoutovu rovnost ve tvaru

$$1 = p(x) - x \cdot (x^3 + x^2).$$

Inverzí k $x^3 + x^2$ je tedy x, v řeči koeficientů $(1100)^{-1} = 0010$.

(b) Přímočarými úpravami vyjádříme y jako

$$y = (1001)^{-1} \cdot 0110 - 1010. \tag{1}$$

Je třeba nalézt inverzi 1001, označme si $q(x) = x^3 + 1$ a použijme rozšířený Euklidův algoritmus

		podíl	zbytek
$p(x)$	$q(x)$	$x+1$	$x = p(x) - (x+1)q(x)$
$q(x)$	x	x^2	$1 = q(x) - x^2 \cdot x = (x^3 + x^2 + 1)q(x) - x^2 p(x)$

Tudíž hledanou inverzí je $(1001)^{-1} = 1101$. Dosazením do (1) dostáváme výsledek

$$y = 1101 \cdot 0110 - 1010 = 0101 - 1010 = 1111.$$

Součin 1101 a 0110 lze vypočítat vynásobením příslušných polynomů (nezapomeňte, že koeficienty se počítají modulo 2)

$$(x^3 + x^2 + 1) \cdot (x^2 + x) = x^5 + x^3 + x^2 + x$$

a vypočtením zbytku po dělení polynomem $p(x)$:

$$(x^5 + x^3 + x^2 + x) \pmod{p(x)} = x^2 + 1.$$

(c) Libovolné y z $GF(2^4)$ lze vyjádřit ve tvaru $y = abcd$, resp. $y(x) = ax^3 + bx^2 + cx + d$, kde $a, b, c, d \in \{0, 1\}$. Nejprve je potřeba vypočítat kvadrát y, čili nejprve vynásobit polynomy

$$\begin{aligned} y(x)^2 &= a^2x^6 + 2abx^5 + (b^2 + 2ac)x^4 + 2(ad + bc)x^3 + (c^2 + 2bd)x^2 + 2cdx + d^2 = \\ &= ax^6 + bx^4 + cx^2 + d. \end{aligned}$$

Zde jsme opět použili toho, že složky jsou dány modulo 2 a navíc $\alpha^2 = \alpha$ pro $\alpha \in \{0, 1\}$. Dále je nutné nalézt zbytek po dělení polynomem $x^4 + x^3 + 1$. Použitím standardního algoritmu dostáváme

$$ax^6 + bx^4 + cx^2 + d \pmod{x^4 + x^3 + 1} = -(a + b)x^3 + (c - a)x^2 + ax + d - a - b.$$

Tj. $y(x) \cdot y(x) = -(a + b)x^3 + (c - a)x^2 + ax + d - a - b$. Hledáme $a, b, c, d \in \{0, 1\}$ tak, aby

$$y(x)^2 + y(x) + x^3 + x = (1 - b)x^3 + (c - a + b)x^2 + (a + c + 1)x - a - b \stackrel{!}{=} 0.$$

Koeficienty jsme opět upravili modulo 2. Z prvního koeficientu jasně plyne, že $b = 1$. Takže potom $a = 1$ (absolutní člen) a $c = 0$ (lineární člen). Kvadratický člen je pak nulový $c - a + b = 0 - 1 + 1 = 0$. Na d jsme žádnou podmínku nezískali a může proto být libovolné. Shrnujeme, že řešením zadané rovnice jsou dvě

$$y_1 = 1100 \quad \text{a} \quad y_2 = 1101.$$

Řešení Cvičení 23.13: Budeme chtít využít binomické věty, která říká, že pro libovolná reálná čísla a a b (a klasické násobení a sčítání čísel) a nezáporné celé číslo n platí:

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

Abychom binomickou větu dokázali (a dávala smysl), potřebujeme vědět, že sčítání a násobení jsou asociativní a komutativní, to ale platí i pro okruh polynomů $\mathbb{Z}^p[x]$ a příslušné operace sčítání a násobení polynomů.

Pro dva polynomy $u(x)$ a $w(x)$ ze $\mathbb{Z}^p[x]$ tedy dostáváme

$$(u(x)+w(x))^p = \sum_{k=0}^{p} \binom{p}{k} (u(x))^{p-k}(w(x))^k.$$

Jelikož jsou koeficienty ze $\mathbb{Z}_p$, je $\binom{p}{k} = 0$ pro všechna k mimo $k = 0$ a $k = p$. Z toho dostáváme

$$(u(x)+w(x))^p = (u(x))^p + (w(x))^p.$$

Nyní využijeme tento fakt při výpočtu $(v(x))^p$, kde

$$v(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0.$$

Nejprve aplikujeme binomickou větu pro polynomy $u(x) = a_m x^m$ a $w(x) = a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$:

$$(v(x))^p = (u(x)+w(x))^p = (a_m)^p x^{pm} + \left(a_{m-1}x^{m-1} + \cdots + a_1 x + a_0\right)^p.$$

S využitím Malé Fermatovy věty máme $a_m^p = a_m$ (podobně i pro všechny ostatní koeficienty $a_i, i = m-1, m-2, \ldots, 0$ níže). S opětovným použitím binomické věty, tentokráte pro volbu $u(x) = a_{m-1}x^{m-1}$ a $w(x) = a_{m-2}x^{m-2} + \cdots + a_1 x + a_0$, dostáváme

$$(v(x))^p = (u(x)+w(x))^p = a_m x^{pm} + a_{m-1}x^{p(m-1)} + \left(a_{m-2}x^{m-2} + \cdots + a_1 x + a_0\right)^p.$$

Takto pokračujeme ještě $m-3$ krát a dostaneme

$$(v(x))^p = a_m x^{pm} + a_{m-1}x^{p(m-1)} + + \cdots + a_1 x^p + a_0 = v(x^p),$$

což bylo dokázati.

Řešení Cvičení 23.14: Multiplikativní grupa tělesa $GF(3^3)$ má řád 26, a tedy pro každý její prvek y platí, že y^{26} je neutrální prvek 001. Proto platí, že $y^{107} = (y^{26})^4 y^3 = y^3$, a příklad se tak zjednodušuje na řešení rovnice

$$y^3 = 111.$$

Označme $y = ax^2 + bx + c$, koeficienty a, b, c určíme z rovnice

$$(ax^2+bx+c)^3 = x^2 + x + 1.$$

S využitím příkladu 23.13 (pro $v(x) = ax^2 + bx + c$ a $p = 3$) máme

$$(ax^2+bx+c)^3 = ax^6 + bx^3 + c.$$

Spočítáme-li, že $x^3 = x + 2$ a $x^6 = (x^3)^2 = (x+2)^2 = x^2 + x + 1$ dostáváme rovnici

$$(ax^2+bx+c)^3 = ax^2 + (a+b)x + (a+2b+c) = x^2 + x + 1.$$

Z toho již plyne, že $a = 1$, $b = 0$ a $c = 0$ a jediným řešením je tedy $y = 100$.

Řešení Cvičení 23.15: Ověření ireducibility polynomu je v tomto případě jednoduché, neboť se jedná o polynom stupně tři. Pokud by polynom $p(x) = 4x^3 + 2x^2 + 4x + 2$ nebyl ireducibilní, musí být dělitelný polynomem stupně jedna, a tedy mít kořen buď 0, 1, 2, 3 nebo 4. Jelikož platí, že $p(2) = 0$, je polynom dělitelný např. $x + 3$, a není tedy ireducibilní. Skutečně:

$$4x^3 + 2x^2 + 4x + 2 = (x+3)(4x^2+4).$$

Řešení Cvičení 23.16: (a): 111, (b): 111 a -111.

ChangeLog

Verze	Datum	Autor	Log
1.1	14.10.2019	ŠS	Přidány příklady na izomorfismus těles.
1.0	14.10.19	ŠS	Výchozí verze.