NI-MPI cvičení 9

Algebra IV

FIT ČVUT

Autoři: Karel Klouda, Tomáš Kalvoda, Jan Spěvák, Štěpán Starosta
Problémy, návrhy apod. hlaste v GitLabu.

Verze souboru: 2023-12-04 10:32.

Obsah

Poznámka

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**:

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

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

Poznámka

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

Poznámka

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.