Cvičení 8 – soustavy polynomiálních rovnic

25. listopadu 2025

Příklad 1. Najděte všechny polynomy f splňující kongruence:

a) $(x^3 + x + 1)f \equiv 1 \bmod x^4 + x + 1$ v $\mathbb{Z}_2[x]$,

b) $(2x + 1)f \equiv x^3 \bmod x^2 + 1$ v $\mathbb{Z}_3[x]$.

Příklad 2. Najděte polynom f nejmenšího stupně v příslušném oboru a procházející následující body:

a) $f \in \mathbb{Z}_7[x], f(0) = 1, f(2) = 5, f(5) = 1$,

b) $f \in \mathbb{Z}_5[x], f(0) = 0, f(1) = 2, f(2) = 0$,

c) $f \in \mathbb{Q}[x], f(0) = 1, f(1) = 0, f(2) = 2$.

Příklad 3. Vypište všechny zbytky (mod $x^2 + x + 1$) v $\mathbb{Z}_3[x]$. Bude se lišit, pokud budeme uvažovat zbytky (mod $2x^2 + 1$)?

Příklad 4. Určete Cayleyho tabulku okruhů $T = \mathbb{Z}_2[\alpha]/(\alpha^2 + \alpha + 1)$ a $S = \mathbb{Z}_2[\alpha]/(\alpha^3 + 1)$ pro sčítání a násobení. Na základě toho rozhodněte, zda se jedná o tělesa.

Příklad 5. Označme okruh $T = \mathbb{Z}_3[\alpha]/(\alpha^2 + 1)$.

a) Ukažte, že polynom $x^2 + 1 \in \mathbb{Z}_3[x]$ je ireducibilní a určete jeho kořeny,

b) rozmyslete si, proč je T těleso, a určete počet jeho prvků.

c) Spočtěte: $(2\alpha + 1) + (2\alpha + 2)$, α^5, α^{-1}, $2\alpha(\alpha + 2)^{-1}$,

d) vyřešte následující soustavu: $\left(\begin{array}{cc|c} \alpha & 1 & \alpha + 1 \\ \alpha + 1 & \alpha + 1 & \alpha \end{array}\right)$.

Příklad 6. Buď T těleso a $a \in T$. Ukažte, že $T[\alpha]/(\alpha - a) \cong T$.

Příklad 7. Buď $T = \mathbb{Z}_2[\alpha]/(\alpha^4 + \alpha^3 + 1)$. Najděte ireducibilní rozklad polynomu $x^3 + 1 \in T[x]$.

Příklad 8. Ukažte, že okruh $\mathbb{Z}_3[\alpha]/(\alpha^4 + \alpha^3 + \alpha + 2)$ není těleso tím, že naleznete prvek, který není invertibilní.

Příklad 9. Napište ireducibilní rozklad polynomu $x^8 - 1$ v oborech $\mathbb{Z}_3[x]$ a $T[x]$, kde $T = \mathbb{Z}_3[\alpha]/(\alpha^2 + 1)$.

Příklad 10. Ukažte, že $\mathbb{Q}[\omega] \cong \mathbb{Q}[\alpha]/(\alpha^2 + \alpha + 1)$.

Příklad 11. Buď p prvočíslo a $f, g \in \mathbb{Z}_p[x]$ polynomy. Pak ukažte, že příslušná polynomiální zobrazení na $\mathbb{Z}_p$ jsou identická právě, když $f \equiv g \bmod x^p - x$.

Příklad 12. Buď $R = \{f \in \mathbb{Q}[x] : f(0) \in \mathbb{Z}\}$. Pak R je podokruh $\mathbb{Q}[x]$. Ukažte, že pro libovolné $f, g \in R$ platí, že existuje NSD(f, g,). Proč přesto není R Gaussovým oborem?

Domácí úkol. Mějme polynom $x^6 + x + 1$. Najděte jeho ireducibilní rozklad nad tělesy $\mathbb{Z}_2$ a $T = \mathbb{Z}_2[\alpha]/(\alpha^2 + \alpha + 1)$.