6 Faktorizace pro začátečníky: sestroj si vlastní těleso

Zadání
Cvičení 27. a 28. března, verze ze dne 27. března 2024.

Cíle cvičení: Tentokrát se naučíme něco opravdu fantastického: slepovat ze starých polynomů zbrusu nová tělesa. Přitom si vyzkoušíme, že jsou plně funkční a že nad nimi můžeme provozovat všechny kejkle lineární algebry! Nejprve se ovšem rozcvičíme počítáním polynomiálních kongruencí a polynomiální verze Čínské věty o zbytcích.

Úlohy, které bychom určitě měli umět řešit:

Úloha 6.1. Najděte všechny polynomy $f \in \mathbb{Z}_2[x]$ splňující kongruence:

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

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

Úloha 6.2. Najděte polynom f nejmenšího možného stupně splňující

(a) $f \in \mathbb{Z}_5[x]$, $f \equiv x+1 \pmod{x^2+1}$ a $f \equiv x \pmod{x^3+1}$,

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

Úloha 6.3. Napište úplnou množinu zbytků $\pmod{x^2+x+1}$ v $\mathbb{Z}_3[x]$. Bude se lišit, pokud budeme uvažovat zbytky $\pmod{2x^2+1}$?

Úloha 6.4. Označme okruh $T = \mathbb{Z}_3[\alpha]/(\alpha^2+1)$.

(a) Dokažte, že je polynom x^2+1 nad $\mathbb{Z}_3$ ireducibilní. Co jsou jeho kořeny v T?

(b) Vysvětlete, proč je T je těleso, a určete, kolik má prvků.

(c) Spočítejte v tělese T
(i) $(2\alpha+1)+(2\alpha+2)$, (ii) α^5, (iii) α^{-1},
(iv) $(\alpha+1)^{-1}$, (v) $2\alpha\cdot(2\alpha+1)$, (vi) $\alpha^{-1}\cdot(\alpha+2)$.

(d) Vyřešte soustavu lineárních rovnic s maticí: $\left(\begin{array}{cc|c} \alpha & 1 & \alpha+1 \\ \alpha+1 & \alpha+1 & \alpha \end{array}\right)$.

Úloha 6.5. Zkonstruujte kořenové nadtěleso polynomů (a) x^2+x+1 (b) x^3+x+1 nad $\mathbb{Z}_2$. Uvědomte si, že jsou obě tělesa dokonce rozkladová a polynomy nad nimi rozložte na lineární členy.

A teď něco na zaplašení smutku a rozšíření obzorů:

Úloha 6.6. V tělese $\mathbb{Z}_5[\alpha]/(\alpha^3+\alpha+1)$ spočtěte

(a) $(3\alpha^2+4\alpha+1)+(2\alpha^2+4)$,

(b) $(3\alpha^2+4\alpha+1)\cdot(2\alpha^2+4)$,

(c) $(2\alpha^2+4)^{-1}$,

(d) řešení lineární rovnice $\alpha \cdot x + (\alpha+1) = \alpha^2$,

Úloha 6.7. Napište tabulky operací čtyřprvkového tělesa.

Úloha 6.8. Buď T těleso a $a \in T$. Dokažte, že je těleso $T[\alpha]/(\alpha - a)$ izomorfní tělesu T.

Úloha 6.9. Položme $\mathbf{T} = \mathbb{Z}_2[\alpha]/(\alpha^4+\alpha^3+1)$. Přesvědčte se, že jde o těleso, a najděte ireducibilní rozklad polynomu x^3+1 v $\mathbf{T}[x]$.

Úloha 6.10. Napište ireducibilní rozklad polynomu x^8-1 v oborech $\mathbb{Z}_3[x]$ a $T[x]$, kde $T = \mathbb{Z}_3[\alpha]/(\alpha^2+1)$.

Úloha 6.11. V okruhu $\mathbb{Z}_3[\alpha]/(\alpha^4+\alpha^3+\alpha+2)$ najděte prvek, k němuž neexistuje (multiplikativní) inverzní prvek.

Úloha 6.12. Najděte izomorfismus mezi okruhy $\mathbb{Z}_5[\alpha]/(\alpha^4-1)$ a $(\mathbb{Z}_5^4, +, -, \cdot, \mathbf{0}, \mathbf{1})$ s operacemi definovanými po složkách a $\mathbf{0} = (0,0,0,0)$, $\mathbf{1} = (1,1,1,1)$.

Úloha 6.13. Najděte v $\mathbb{Z}_2[x]$ modulo dané polynomy zbytky co nejnižších stupňů:

(a) $x^9 \mod x^2+x+1$,

(b) $x^{13} \mod x^4+x+1$.

Úloha 6.14. Najděte všechny polynomy $f \in \mathbb{Q}[x]$ stupně menšího než 3 splňující

$$f \equiv x+1 \pmod{x^2+1}, \qquad f(0) = 3.$$

Úloha 6.15. Buď p prvočíslo. S pomocí čínské věty o zbytcích pro polynomy ukažte, že polynom $\prod_{a\in\mathbb{Z}_p}(x-a) \in \mathbb{Z}_p[x]$ je roven polynomu $x^p - x$.

Úloha 6.16. Buď p prvočíslo a buďte $f, g \in \mathbb{Z}_p[x]$ polynomy. Ukažte, že příslušná polynomiální zobrazení na $\mathbb{Z}_p$ jsou identická právě tehdy, když $f \equiv g \pmod{x^p - x}$.

Úloha 6.17.* Buď $R = \{f \in \mathbb{Q}[x];\ f(0) \in \mathbb{Z}\}$. Pak je R podokruh oboru $\mathbb{Q}[x]$. Dokažte, že pro libovolné $f, g \in R$ existuje $\mathrm{NSD}(f,g)$. Proč není přesto R Gaussovým oborem?