6 Faktorizace pro začátečníky: sestroj si vlastní těleso

Řešení
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 $\mathbb{Z}_3[x]$.

Řešení. (a) Potřebujeme invertovat polynom x^3+x+1 modulo polynom x^4+x+1, což můžeme jistě provést pomocí Eukleidova algoritmu v oboru polynomů nad tělesem, neboť je polynom $x^4 + x + 1$ ireducibilní. Výpočet Bezoutových koeficientů si zapíšeme stejně jako v první sérii pro výpočet v oboru celých čísel a pro přehlednost přidáme i hodnotu podílu q_i (tedy $a_{i+1} = a_{i-1} - q_i q_i$):

a_i	u_i	v_i	q_i
$x^4 + x + 1$	1	0	
$x^3 + x + 1$	0	1	x
$x^2 + 1$	1	x	x
1	x	$x^2 + 1$	
0			

Protože

$$1 = x \cdot (x^4 + x + 1) + (x^2 + 1) \cdot (x^3 + x + 1),$$

je kongruence

$$(x^3 + x + 1)f \equiv 1 \pmod{x^4 + x + 1}$$

ekvivalentní kongruenci

$$f \equiv (x^2 + 1)(x^3 + x + 1)f \equiv (x^2 + 1) \pmod{x^4 + x + 1},$$

a proto dostáváme obecné řešení $(x^2 + 1) + s(x^4 + x + 1)$ pro libovolné $s \in \mathbb{Z}_2[x]$.

(b) Všimneme si, že $x^2 \equiv -1 \pmod{x^2 + 1}$ a upravíme $(2x + 1)f \equiv x^3 \equiv 2x \pmod{x^2 + 1}$ a poté co spočítáme, že

$$(2x + 1)(2x + 2) \equiv (-x + 1)(-x - 1) \equiv x^2 - 1 \equiv -1 - 1 \equiv 1 \pmod{x^2 + 1},$$

dostaneme

$$f \equiv (2x + 2)(2x + 1)f \equiv 2x(2x + 2) \equiv x^2 + x \equiv x + 2 \pmod{x^2 + 1},$$

což znamená, že $x + 2 + s(x^2 + 1)$ pro libovolné $s \in \mathbb{Z}_3[x]$ je obecné řešení této kongruence.

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

Řešení. (a) Budeme postupovat obdobně jako v 2. sérii při řešení soustav lineárních kongruencí na $\mathbb{Z}$. Obecné řešení druhé kongruence $f \equiv x \pmod{x^3+1}$ tvaru $x+s(x^3+1)$ pro $s \in \mathbb{Z}_5[x]$ dosadíme do první kongruence a ekvivalentně (tentokrát třeba bez explicitního využití Eukledova algoritmu) upravujeme

$$f \equiv x+s(x^3+1) \equiv x+s(-x+1) \equiv x+1 \pmod{x^2+1},$$

poté odečteme od obou stran kongruence x a dostaneme $s(-x+1) \equiv 1 \pmod{x^2+1}$. Protože $-(1+x)(1-x) = x^2-1 \equiv -2 \pmod{x^2+1}$, vidíme, že

$$-2s \equiv s(x^2-1) \equiv s(-x+1)(-x-1) \equiv (-x-1) \pmod{x^2+1},$$

proto $s \equiv 2(-x-1) \equiv (3x+3) \pmod{x^2+1}$. Jako řešení nejmenšího stupně dostáváme tudíž polynom $f = x+s(x^3+1) = x+(3x+3)(x^3+1) = 3x^4+3x^3+4x+3$.

(b) Můžeme buď úlohu převést na kongruence

$$f \equiv 1 \pmod{x}, \quad f \equiv 0 \pmod{x-1}, \quad f \equiv 2 \pmod{x-2}$$

a pak budeme postupovat obdobně jako v (a) nebo můžeme najít řešení $f = \frac{1}{2}(3x^2-5x+2)$ pomocí Lagrangeova interpolačního polynomu (viz důsledek 9.2 ve skriptech).

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

Řešení. Máme úplnou množinu zbytků modulo polynom stupně dva

$$\{p \in \mathbb{Z}_3[x] \mid \deg(p) < 2\} = \{0, 1, 2, x, x-1, x-2, 2x, 2x-1, 2x-2\},$$

odkud vidíme, že záleží pouze na stupni polynomu, nikoli na tom jak konkrétně daný polynom vypadá. Poznamenejme, že to v žádném případě neznamená, že počítání $\pmod{x^2+x+1}$ je to samé jako $\pmod{2x^2+1}$.

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

Řešení. (a) Protože jde o polynom stupně dva, který v $\mathbb{Z}_3$ nemá kořen, jedná se o ireducibilní polynom v oboru $\mathbb{Z}_3[x]$. Kořeny v tělese T má $\pm\alpha$.

(b) Z definice přímo plyne, že se jedná o komutativní okruh. Protože je polynom α^2+1 nad $\mathbb{Z}_3$ ireducibilní, tedy umíme pomocí Eukleidova algoritmu najít inverzní prvek ke každému nenulovému prvku úplné množiny zbytků, která má právě $|\mathbb{Z}_3|^2 = 9$ prvků.

(c) Veškeré výpočty v daném tělese provádíme podobně jako v 6.1 modulo polynom α^2+1, prvky tělesa jsou zbytky a místo kongruencí budeme všude psát rovnosti jako výsledky operací.

(i) Zde jen počítáme s koeficienty $(2\alpha+1)+(2\alpha+2)=\alpha$

(ii) Protože $\alpha^2=-1$, máme $\alpha^5=\alpha\cdot(\alpha^2)^2=\alpha\cdot(-1)^2=\alpha\cdot 1=\alpha$.

(iii) Všimli jsme si si, že $\alpha^2=-1$, proto $-\alpha\cdot\alpha-1$, proto $\alpha^{-1}=-\alpha=2\alpha$.

(iv) Tentokrát si povšimněme, že $(\alpha-1)(\alpha+1)=\alpha^2-1=-1-1=1$, tudíž $(\alpha+1)^{-1}=\alpha-1=\alpha+2$.

(v) $2\alpha\cdot(2\alpha+1)=\alpha^2-\alpha=-1-\alpha=2+2\alpha$.

(vi) Z (iii) dostáváme, že $\alpha^{-1}\cdot(\alpha+2)=-\alpha\cdot(\alpha-1)=-\alpha^2+\alpha=\alpha+1$

(d) Budeme upravovat, jak jsme byli zvyklí v lineární algebře, posloupností ekvivalentních řádkových úprav

$$\left(\begin{array}{cc|c}\alpha & 1 & \alpha+1\\ \alpha+1 & \alpha+1 & \alpha\end{array}\right)\sim\left(\begin{array}{cc|c}\alpha+1 & \alpha+1 & \alpha\\ \alpha & 1 & \alpha+1\end{array}\right)\sim\left(\begin{array}{cc|c}1 & \alpha & -1\\ \alpha & 1 & \alpha+1\end{array}\right)\sim$$

$$\sim\left(\begin{array}{cc|c}1 & \alpha & -1\\ 0 & 1-\alpha^2 & 2\alpha+1\end{array}\right)\sim\left(\begin{array}{cc|c}1 & \alpha & -1\\ 0 & -1 & -\alpha+1\end{array}\right)\sim\left(\begin{array}{cc|c}1 & 0 & \alpha\\ 0 & 1 & \alpha-1\end{array}\right),$$

kde jsme nejprve přehodily řádky upravili první řádek pomocí druhého, poté jsme vynulovali pozici pod prvním pivotem a po úpravě druhého řádky vynulovali i hodnotu nad druhým pivotem. Dostali jsme řešení $(\alpha,\alpha-1)=(\alpha,\alpha+2)$.

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.

Řešení. Už jsme zjistili, že oba polynomy m jsou ireducibilní v $\mathbb{Z}_2[\alpha]$, proto si v obou případech stačí vzít faktorový okruh $\mathbb{Z}_2[\alpha]/(m)$ modulo (a) $m=\alpha^2+\alpha+1$ (b) $m=\alpha^3+\alpha+1$. Všimneme-li si, že pro polynom m a jeho kořen α platí

$$0=0^2=m(\alpha)^2=m(\alpha^2)\ \text{ a }\ 0=0^2=m(\alpha^2)^2=m(\alpha^4).$$

Odtud vidíme, že s kořenem α dostáváme v případě

(a) další kořen $\alpha^2=\alpha+1$, a proto $x^2+x+1=(x+\alpha)(x+(\alpha+1))$ a v případě

(b) dva další kořeny α^2 a $\alpha^4=\alpha^2+\alpha$, které dávají rozklad na kořenové činitele

$$x^3+x+1=(x+\alpha)(x+(\alpha^2))(x+(\alpha^2+\alpha)).$$

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 $\alpha\cdot x+(\alpha+1)=\alpha^2$,

Řešení. Počítáme obdobně jako v 6.4, tedy upravujeme pomocí operací s polynomy v neznámé α modulo polynom $\alpha^3+\alpha+1$ a dostaneme:

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

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

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

(d) $x=\alpha^2+\alpha+1$.

Úloha 6.7. Napište tabulky operací čtyřprvkového tělesa.

Řešení. Prvky tělesa reprezentujeme standardně jako úplnou množinu zbytků, tedy polynomy nad $\mathbb{Z}_2$ modulo ireducibilní polynom $\alpha^2+\alpha+1$. Výpočty jsou zcela přímočaré:

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

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

Řešení. Stačí uvážit zobrazení $T[\alpha]/(\alpha-a)$ dané podmínkou $t\to t$, o němž je snadné ukázat, že je okruhovým izomorfismem.

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 $\mathbf{T}[x]$.

Řešení. Nejprve ověříme, že je polynom $\alpha^4+\alpha^3+1$ v oboru $\mathbb{Z}_2[\alpha]$ ireducibilní. Zřejmě nemá v $\mathbb{Z}_2$ kořen ani není druhou mocninou jediného ireducibilního polynomu $\alpha^2+\alpha+1$ stupně 2. Dále vidíme, že má polynom x^3+1 kořen 1, a proto $x^3+1=(x+1)(x^2+x+1)$, zbývá najít kořeny polynomu x^2+x+1, tedy prvky $\beta\in\mathbf{T}$ splňující $\beta^2=\beta+1$. Zkusmo najdeme dva kořeny $\alpha^3+\alpha$ a $\alpha^3+\alpha+1$ (víme, že součet i součin našich polynomů má být kongruentní 1), náš polynom se tedy rozkládá na součin kořenových činitelů

$$x^3+1=(x+1)(x+\alpha^3+\alpha+1)(x+\alpha^3+\alpha).$$

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

Řešení. Nejprve polynom rozložíme v $\mathbb{Z}_3[x]$

$$x^8-1=(x^4+1)(x^4-1)=(x^4+1)(x^2+1)(x^2-1)=(x^4+1)(x^2+1)(x+1)(x-1),$$

kde jsou poslední tři polynomy zjevně ireducibilní, protože kvadratický polynom x^2+1 nemá v $\mathbb{Z}_3$ kořen a lineární polynomy nad tělesem už nelze rozložit. Zároveň si všimneme, že díky ireducibilitě kvadratického polynomu je obor $T=\mathbb{Z}_3[\alpha]/(\alpha^2+1)$ tělesem. Nad ním je polynom $(x^2+1)=(x+\alpha)(x-\alpha)$ rozložitelný na lineární, tedy ireducibilní faktory.

Dále si můžeme všimnout, že $x^4+1=(x^2+x-1)(x^2-x-1)$ a že v tělese T máme:

$$(\alpha+1)+(2\alpha+1)=2,\quad(\alpha+1)\cdot(2\alpha+1)=-1,$$

$$(\alpha+2)+(2\alpha+2)=1,\quad(\alpha+2)\cdot(2\alpha+2)=-1,$$

a proto

$$x^2+x-1=(x+\alpha+2)(x+2\alpha+2)\ \text{ a }\ x^2-x-1=(x+\alpha+1)(x+2\alpha+1),$$

což jedna dává ireducibilní rozklad obou polynomů nad tělesem T a dále odtud vidíme, že jsou oba polynomy ireducibilní nad tělesem $\mathbb{Z}_3$. Spočítali jsme tedy oba ireducibilní rozklady

$$x^8 - 1 = (x^2 + x - 1)(x^2 - x - 1)(x^2 + 1)(x + 1)(x - 1) \in \mathbb{Z}_3[x],$$

$$x^8 - 1 = (x + \alpha + 2)(x + 2\alpha + 2)(x + \alpha + 1)(x + 2\alpha + 1)(x + \alpha)(x - \alpha)(x + 1)(x - 1) \in T[x].$$

Na závěr poznamenejme, že zjištění, že $x^8 - 1 = \prod_{\zeta \in T^*}(x - \zeta)$ není vůbec náhodné a brzy nám dá teorie grup účinnější prostředky, jak ho dostat.

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

Řešení. Spočítáme-li rozklad polynomu $\alpha^4+\alpha^3+\alpha+2 = (2+\alpha+\alpha^2)(1+\alpha^2)$, pak ani jeden z prvků rozkladu $2+\alpha+\alpha^2$ $1+\alpha^2$, protože v okruhu $\mathbb{Z}_3[\alpha]/(\alpha^4+\alpha^3+\alpha+2)$ platí, že $(2+\alpha+\alpha^2)(1+\alpha^2) = 0$, tedy se nejedná o obor.

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 $\mathbf{0} = (0, 0, 0, 0)$, $\mathbf{1} = (1, 1, 1, 1)$.

Řešení. Nejprve si uvědomíme, že polynom $x^4 - 1$ má nad $\mathbb{Z}_5$ čtyři kořeny $1, 2, 3, 4$, tj. je součinem $\prod_{a \in \mathbb{Z}_5^*}(x - a)$. Z Čínské věty o zbytcích pro polynomy plyne, že zobrazení

$$\rho(f) = (f(1), f(2), f(3), f(4))$$

je bijekce množin $\mathbb{Z}_5[\alpha]/(\alpha^4 - 1)$ a $\mathbb{Z}_5^4$. Zbývá si rozmyslet, že se dokonce jedná o okruhový izomorfismus, tedy že platí $\rho(0) = (0, 0, 0, 0)$, $\rho(1) = (1, 1, 1, 1)$ a pro všechna $a, b \in \mathbb{Z}_5[\alpha]/(\alpha^4 - 1)$

$$\rho(a \pm b) = (a(1) \pm b(1), a(2) \pm b(2), a(3) \pm b(3), a(4) \pm b(4)) = \rho(a) \pm \rho(b)$$

$$\rho(a \cdot b) = (a(1) \cdot b(1), a(2) \cdot b(2), a(3) \cdot b(3), a(4) \cdot b(4)) = \rho(a) \cdot \rho(b).$$

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

(a) $x^9 \pmod{x^2 + x + 1}$,

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

Řešení. (b) Stačí buď vydělit se zbytkem nebo využít pozorování $x^2 \equiv (x + 1) \pmod{x^2 + x + 1}$, abychom zjistili, že

$$x^9 \equiv x(x^2)^4 \equiv x(x + 1)^4 \equiv x(x^2 + 1)^2 \equiv x \cdot x^2 \equiv 1 \pmod{x^2 + x + 1}$$

$x^9 \pmod{x^2 + x + 1} = 1$

(b) Tentokrát využijeme snadného pozorování, že $x^4 \equiv x + 1 \pmod{x^4 + x + 1}$ a zápisu pomocí kongruencí:

$$x^{13} \equiv x(x^4)^3 \equiv x(x+1)^3 \equiv x^4 + x^3 + x^2 + x \equiv x + 1 + x^3 + x^2 + x \equiv x^3 + x^2 + 1 \pmod{x^4 + x + 1},$$

tedy $x^{13} \pmod{x^4 + x + 1} = x^3 + x^2 + 1$.

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

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

Řešení. Postupujeme jako v 6.2. První podmínku vyjádříme ve tvaru $f = (x+1) + s(x^2+1)$ pro $s \in \mathbb{Q}[x]$ tu dosadíme do druhé podmínky vyjádřené ve formě kongruence $f \equiv 3 \pmod{x}$:

$$f \equiv (x+1) + s(x^2+1) \equiv 1 + s \equiv 3 \pmod{x},$$

tedy $s \equiv 2 \pmod{x}$ a jediné řešení stupně stupně menšího než 3 je $f = (x+1) + 2(x^2+1) = 3 + x + 2x^2$.

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 $x^p - x$.

Řešení. Oba polynomy mají za za kořen každé $a \in \mathbb{Z}_p$ tedy i jejich rozdíl má tuto vlastnost. Ten má ale stupeň $< n$, takový však dle čínské věty o zbytcích existuje jen jeden, čirou náhodou je to právě 0.

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 $f \equiv g \pmod{x^p - x}$.

Řešení. To, že $f(a) = g(a)$ pro všechna $a \in \mathbb{Z}_p$ je ekvivalentní podmínce, že $(f-g)(a) = 0$, což nastává právě tehdy, když $x^p - x = \prod_{a \in \mathbb{Z}_p}(x-a)$ dělí $f - g$, tedy právě 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?

Řešení. Obor R není Gaussův podle Věty 6.3, neboť v něm existují nekonečné klesající posloupnosti vlastních dělitelů, například $\{2^{-n}x\}_{n \in \mathbb{N}}$. Vidíme, že $2 \cdot 2^{-n-1}x = 2^{-n}$, tedy 2^{-n-1} dělí 2^{-n} pro všechna $n > 1$, ale není s ním asociován.