6 Faktorizace pro začátečníky: sestroj si vlastní těleso

Řešení
verze ze dne 27. března 2025.

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.

Úlohy, které bychom určitě měli umět řešit:

Úloha 6.1. Najděte všechny polynomy f 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. 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 (mod x^2+x+1) je to samé jako (mod $2x^2+1$).

Úloha 6.3. 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, určete, kolik má prvků a jakou má charakteristiku.

(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, umíme pomocí Eukleidova algoritmu najít inverzní prvek ke každému nenulovému prvku úplné množiny zbytků, tedy jde o těleso. Úplná množina zbytků má v tomto případě právě $|\mathbb{Z}_3|^2 = 9$ prvků, jelikož ji tvoří všechny polynomy stupně max. 1. Charakteristika tělesa je 3, jelikož v něm platí $1+1+1=0$.

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

Úloha 6.4. 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

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

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

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

Úloha 6.5. Napište všechna kořenová a rozkladová nadtělesa nad tělesem $\mathbb{Q}$ obsažená v $\mathbb{C}$ následujících polynomů z $\mathbb{Q}[x]$:

(a) $x^2 - 2$,

(b) $x^3 - 2x^2 - 2x - 3$.

Řešení. (a) Polynom $x^2 - 2$ má dva reálné kořeny $\pm\sqrt{2}$, o kvadratických rozšířeních tělesa racionálních čísel víme, že tvoří těleso, tudíž máme jediné kořenové nadtěleso $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(-\sqrt{2})$, které je zároveň i rozkladovým nadtělesem $\mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$ polynomu $x^2 - 2$ nad tělesem $\mathbb{Q}$.

(b) Nejprve si všimneme, že má polynom $x^3 - 2x^2 - 2x - 3$ racionální kořen 3 (už umíme zjistit, že v úvahu připadají pouze hodnoty ± 1, ± 3, a ty zkusíme dosadit). To znamená, že triviální rozšíření $\mathbb{Q}(3) = \mathbb{Q}$ je kořenovým nadtělesem tohoto polynomu. Dále standardním postupem spočítáme kořeny polynomu

$$\frac{x^3 - 2x^2 - 2x - 3}{x - 3} = x^2 + x + 1 = \left(x + \frac{1}{2} - \frac{i\sqrt{3}}{2}\right)\left(x + \frac{1}{2} + \frac{i\sqrt{3}}{2}\right),$$

odkud dostáváme druhé možné kořenové nadtěleso $\mathbb{Q}(-\frac{1}{2} + \frac{i\sqrt{3}}{2}) = \mathbb{Q}(-\frac{1}{2} - \frac{i\sqrt{3}}{2}) = \mathbb{Q}(i\sqrt{3})$. Toto těleso je zřejmě i rozkladovým nadtělesem polynomu $x^3 - 2x^2 - 2x - 3$, neboť se zde rozkládá na kořenové činitele

$$x^3 - 2x^2 - 2x - 3 = (x - 3)\left(x + \frac{1}{2} - \frac{i\sqrt{3}}{2}\right)\left(x + \frac{1}{2} + \frac{i\sqrt{3}}{2}\right).$$

Úloha 6.6. Uvnitř tělesa $T = \mathbb{Z}_2[\alpha]/(\alpha^4+\alpha+1)$ nalezněte kořenové nadtěleso polynomu $x^2+x+1 \in \mathbb{Z}_2[x]$.

Řešení. V podstatě chceme v T najít kořen(y) onoho polynomu. Jelikož T má charakteristiku 2, můžeme ekvivalentně hledat řešení β rovnice $x^2 = x + 1$; kromě toho mocnění mnohočlenu na druhou probíhá v charakteristice 2 „člen po členu“ (smíšené členy jsou díky výskytu 2 rovny nule).

Předně si všimněme, že z Viètových vztahů bude součet řešení rovnice roven 1, tím pádem můžeme BÚNO hledat řešení β, jehož abs. člen je nulový (a druhé řešení se bude lišit jen v onom abs. členu).

Pokud si dále spočteme $(\alpha^3)^2 = \alpha^3 + \alpha^2$, vidíme, že β musí nutně obsahovat α^2, aby mělo β^2 nenulový abs. člen (stejně jako má $\beta + 1$). Jelikož ovšem $(\alpha^2)^2 = \alpha + 1$, je v β^2 nutně přítomen lineární člen α, tím pádem musí být i v β. Ze zbývajících dvou možností $\alpha^2 + \alpha$ a $\alpha^3 + \alpha^2 + \alpha$ snadno potvrdíme první a vyloučíme druhou.

Máme tedy $\beta = \alpha^2+\alpha$, druhé řešení rovnice je tedy $\alpha^2+\alpha+1$. Hledané kořenové nadtěleso je $\mathbb{Z}_2(\alpha^2+\alpha) \leq T$, které je zřejmě stejné jako $\mathbb{Z}_2(\alpha^2+\alpha+1)$. Toto těleso je i rozkladové a zadaný polynom se v něm rozkládá jako

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

Úloha 6.7. Dokažte, že jsou izomorfní páry těles

(a) $\mathbb{Q}[\alpha]/(\alpha^3-2)$ a $\mathbb{Q}(\sqrt[3]{2})$,

(b) $\mathbb{Q}[\alpha]/(\alpha^2-3)$ a $\mathbb{Q}(\sqrt{3})$,

(c) $\mathbb{R}[\alpha]/(\alpha^2+\alpha+2)$ a $\mathbb{C}$.

Řešení. Ve všech úlohách zkonstruujeme dosvědčující izomorfismus.

(a) Nejprve poznamenejme, že kubický polynom x^3-2 nemá racionální kořeny, proto je ireducibilní, a poté definujme zobrazení $\Omega\colon \mathbb{Q}[\alpha]/(\alpha^3-2) \to \mathbb{Q}[\sqrt[3]{2}]$ předpisem

$$\Omega(a\alpha^2+b\alpha+c) = a\sqrt[3]{4}+b\sqrt[3]{2}+c.$$

Přímo z definice vidíme, že se jedná o dobře definované lineární zobrazení nad tělesem $\mathbb{Q}$ na celé $\mathbb{Q}[\sqrt[3]{2}]$. Ukážeme, že jde o prosté zobrazení. Jestliže je $r \in \mathbb{Q}[x]$ polynom stupně menšího než 3, jehož kořenem je $\sqrt[3]{2}$, pak i pro $s = \mathrm{NSD}_{\mathbb{Q}[x]}(r, x^3-2)$ platí, že je $\sqrt[3]{2}$ jeho kořenem. Protože je $\deg(r) < 3$ a x^3-2 ireducibilní, musí nutně $r=0$. Proto pokud pro $a,b,c \in \mathbb{Q}$

$$a(\sqrt[3]{2})^2 + b\sqrt[3]{2} + c = 0,$$

dostáváme, že $a=b=c=0$. Tedy Ω má triviální jádro a jedná se o prosté zobrazení. Už jsme si všimli, že je Ω lineární, tedy slučitelné se sčítáním, a musíme ověřit pro všechna $r,s \in \mathbb{Q}[\alpha]$ stupně nejvýše 2 a takové $t(\alpha) = (r(\alpha)s(\alpha)) \pmod{\alpha^3-2}$, že $r(\sqrt[3]{2}) \cdot s(\sqrt[3]{2}) = t(\sqrt[3]{2})$. Protože existuje $q \in \mathbb{Q}[\alpha]$ splňující $t = rs - q(\alpha^3-2)$, dostáváme, že

$$t(\sqrt[3]{2}) = r(\sqrt[3]{2})s(\sqrt[3]{2}) - q(\sqrt[3]{2})((\sqrt[3]{2})^3-2) = r(\sqrt[3]{2}) \cdot s(\sqrt[3]{2}),$$

tedy zobrazení Ω je okruhový izomorfismus. Zbývá si všimnout, že obor $\mathbb{Q}[\sqrt[3]{2}]$ je izomorfní obraz tělesa, tedy opět těleso, což znamená, že $\mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}(\sqrt[3]{2})$ a Ω představuje dosvědčující izomorfismus těles $\mathbb{Q}[\alpha]/(\alpha^3-2)$ a $\mathbb{Q}(\sqrt[3]{2})$

(b) Opět si s pomocí Eisensteinova kritéria a tvrzení o ireducibilitě primitivních polynomů i nad podílovým tělesem všimneme, že je polynom x^2-3 v oboru $\mathbb{Q}[x]$ ireducibilní a postupujeme stejně jako v (a). Definujeme lineární zobrazení $\Omega\colon \mathbb{Q}[\alpha]/(\alpha^2-3) \to \mathbb{Q}[\sqrt{3}] = \mathbb{Q}(\sqrt{3})$ předpisem

$$\Omega(a\alpha+b) = a\sqrt{2}+b,$$

o němž stejný argument jako v (a) ukáže, že se jedná o okruhový izomorfismus.

(c) Vidíme, že polynom x^2+x+2 má komplexní kořeny $\frac{1\pm i\sqrt{7}}{2}$, tudíž je v $\mathbb{R}[x]$ nerozložitelný a opět můžeme definovat zjevně lineární zobrazení $\Omega\colon \mathbb{R}[\alpha]/(\alpha^2+\alpha+2) \to \mathbb{C}$, tentokrát například podmínkou $\Omega(a\alpha+b) = a\frac{1+i\sqrt{7}}{2} + b$. Protože se zjevně jedná o prosté lineární zobrazení mezi reálnými vektorovými prostory dimenze 2, jde o bijekci, u níž stejně jako v (a) a (b) nahlédneme slučitelnost s operacemi.

A teď něco na zaplašení smutku a rozšíření obzorů:

Úloha 6.8. 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 6.3, 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 6.9. 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 6.10. 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 6.11. Položme $T=\mathbb{Z}_2[\alpha]/(\alpha^4+\alpha^3+1)$. Přesvědčte se, že jde o těleso, a najděte ireducibilní rozklad polynomu x^3+1 v $T[x]$.

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 6.12. 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

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

což jednak dává ireducibilní rozklad obou polynomů nad tělesem T a dále odtud vidíme, že jsou oba kvadratické 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 6.13. Je-li $m \in \mathbb{Q}[x]$ ireducibilní polynom a $\beta \in \mathbb{C}$ jeho komplexní kořen, dokažte, že jsou tělesa $\mathbb{Q}[\alpha]/(m(\alpha))$ a $\mathbb{Q}(\beta)$ izomorfní.

Řešení. Obdobně jako v 6.7 sestrojíme izomorfismus $\Omega : \mathbb{Q}[\alpha]/(m(\alpha)) \to \mathbb{Q}[\beta]$ předpisem

$$\Omega(f(\alpha)) = f(\beta) \quad \forall\, f \in \mathbb{Q}[x],\ \deg(f) < \deg(m),$$

o němž se stejným postupem ukáže, že je izomorfismem. Protože je $\mathbb{Q}[\beta]$ izomorfním obrazem tělesa, jedná se rovněž o těleso, tedy máme zkonstruovaný izomorfismus $\mathbb{Q}[\alpha]/(m(\alpha)) \cong \mathbb{Q}[\beta] = \mathbb{Q}(\beta)$.

Úloha 6.14. 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 $2+\alpha+\alpha^2$, $1+\alpha^2$ nemá inverz, protože v okruhu $\mathbb{Z}_3[\alpha]/(\alpha^4+\alpha^3+\alpha+2)$ platí, že $(2+\alpha+\alpha^2)(1+\alpha^2) = 0$; takovíto „dělitelé nuly“ ovšem nemohou být nikdy invertibilní (v situaci $ab = 0$ pro a invertibilní dostáváme přenásobením $a^{-1}\ b = 0$).

Úloha 6.15. Najděte v $\mathbb{Z}_2[x]$ modulo dané polynomy zbytky co nejnižších stupňů:

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

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

Řešení. (a) 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 6.16. 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.