Algebra — cvičení 7, řešení

1. (c, d, e) Ověřte, že je $F = \mathbb{Z}_3[\alpha]/(\alpha^2+1)$ těleso a spočítejte:

(c) $(\alpha+1)^{-1}$. V F máme $(\alpha-1)(\alpha+1) = \alpha^2-1 = \alpha^2+2 = 1$. Je tedy $(\alpha+1)^{-1} = \alpha-1 = \alpha+2$.

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

(e) $\alpha^{-1}\cdot(\alpha+2)$. Z (b) víme, že $\alpha^{-1} = -\alpha = 2\alpha$. Je proto $\alpha^{-1}\cdot(\alpha+2) = 2\alpha^2+\alpha = \alpha+1$.

4. Dokažte, že je těleso $T = \mathbb{Q}[\alpha]/(\alpha^3-2)$ izomorfní tělesu $\mathbb{Q}(\sqrt[3]{2})$. Definujeme zobrazení $\psi : T \to \mathbb{Q}[\sqrt[3]{2}]$ přirozeným vztahem $\psi(a\alpha^2+b\alpha+c) = a\sqrt[3]{4}+b\sqrt[3]{2}+c$. Abychom věděli, že se jedná o bijekci, stačí si uvědomit, že $(1, \sqrt[3]{2}, \sqrt[3]{4})$ tvoří bázi vektorového prostoru $\mathbb{Q}(\sqrt[3]{2})$ nad $\mathbb{Q}$. Na toto konto už jsme dříve příklad či dva dělali.

To, že $\psi(1) = 1$, je zřejmé. Stejně tak fakt, že $\psi(s+t) = \psi(s)+\psi(t)$ platí pro každé $t, s \in T$. Jediné, co musíme řádně ověřit, je rovnost $\psi(s\cdot t) = \psi(s)\psi(t)$ pro libovolná $t, s \in T$. Tady se teprve ukáže důležité, že v T počítáme modulo α^3-2, jehož kořenem je $\sqrt[3]{2}$, a ne třeba modulo $\alpha^3+2\alpha+2$. V oboru polynomů $\mathbb{Q}[\alpha]$ lze napsat $st = q(\alpha^3-2)+r$, kde $q, r \in \mathbb{Q}[\alpha]$ a $\deg r < 3$. V tělese T pak samozřejmě platí $s\cdot t = r$. Stačí proto ukázat, že $\psi(s)\psi(t) = r(\sqrt[3]{2})$. Z definice ovšem máme, že $\psi(s)\psi(t) = s(\sqrt[3]{2})t(\sqrt[3]{2}) = st(\sqrt[3]{2}) = q(\sqrt[3]{2})(\sqrt[3]{2}^3-2)+r(\sqrt[3]{2}) = r(\sqrt[3]{2})$. Zde jsme použili vlastnosti dosazovacího homomorfismu $d_{\sqrt[3]{2}} : \mathbb{Q}[\alpha] \to \mathbb{Q}[\sqrt[3]{2}]$.

5. (b), (c) Napište kořenová a rozkladová nadtělesa polynomů x^3-2x^2-2x-3 a x^n-1, kde $n \in \mathbb{N}$, nad tělesem $\mathbb{Q}$ obsažená v $\mathbb{C}$. Zadaný polynom třetího stupně má kořen 3, který najdeme zkusmo, s využitím kritéria racionálního kořene. Jedním z kořenových nadtěles je proto, dle definice, $\mathbb{Q}(3) = \mathbb{Q}$. Dále máme $x^3-2x^2-2x-3 = (x-3)(x^2+x+1)$, přičemž kořeny polynomu x^2+x+1 jsou dvě (komplexně sdružené) třetí odmocniny z jedné: je totiž $x^3-1 = (x-1)(x^2+x+1)$. Další kořenové nadtěleso je proto $\mathbb{Q}\big(\mathrm{e}^{\frac{2\pi i}{3}}\big) = \mathbb{Q}\big(\mathrm{e}^{\frac{4\pi i}{3}}\big)$, což je zároveň i rozkladové nadtěleso zadaného polynomu.

Nyní k příkladu x^n-1, který byl s hvězdičkou. Ten má za kořeny právě všechny komplexní $n$té odmocniny z jedné. Ty jsou všechny mocninami jedné z nich, konkrétně $\mathrm{e}^{\frac{2\pi i}{n}}$. Těleso $\mathbb{Q}\big(\mathrm{e}^{\frac{2\pi i}{n}}\big)$ je proto rozkladovým nadtělesem zadaného polynomu. Jeho kořenovými nadtělesy pak jsou $\mathbb{Q}\big(\mathrm{e}^{\frac{2\pi ik}{n}}\big)$, kde $k \in \mathbb{Z}_n$. Těžší je ovšem určit, která z nich se rovnají. S trochou znalosti řádů prvků v grupách lze vydedukovat, že $\mathbb{Q}\big(\mathrm{e}^{\frac{2\pi ik}{n}}\big) = \mathbb{Q}\big(\mathrm{e}^{\frac{2\pi il}{n}}\big)$, mají-li k, l stejný řád v grupě $(\mathbb{Z}_n; +, -, 0)$. Problém je, že neplatí opačná implikace, jak byste možná očekávali. Například $\mathbb{Q}\big(\mathrm{e}^{\frac{2\pi i}{6}}\big) = \mathbb{Q}\big(\mathrm{e}^{\frac{4\pi i}{6}}\big)$, neboť $\mathrm{e}^{\frac{2\pi i}{6}} = -\mathrm{e}^{\frac{8\pi i}{6}}$. Ukázat, že to je typově jediná výjimka, je nad rámec těchto cvičení. Bez důkazu tedy uveďme, že platí: $\mathbb{Q}\big(\mathrm{e}^{\frac{2\pi ik}{n}}\big) = \mathbb{Q}\big(\mathrm{e}^{\frac{2\pi il}{n}}\big)$ právě tehdy, když $\mathrm{ord}_{\mathbb{Z}_n} k = \mathrm{ord}_{\mathbb{Z}_n} l$ nebo jeden z řádů je lichý a druhý je jeho dvojnásobkem.

7. (b), (c) V tělese $\mathbb{Z}_5[\alpha]/(\alpha^3+\alpha+1)$ spočtěte

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

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

Při počítání budeme využívat, že v zadaném tělese platí $\alpha^3 = -\alpha-1$.

V případě (b) máme $(3\alpha^2+4\alpha+1)\cdot(2\alpha^2+4) = \alpha^4+3\alpha^3+4\alpha^2+\alpha+4 = -\alpha^2-\alpha-3\alpha-3+4\alpha^2+\alpha+4 = 3\alpha^2+2\alpha+1$.

V případě (c) spustíme rozšířený Eukleidův algoritmus, abychom v $\mathbb{Z}_5[\alpha]$ nalezli u, v taková, že $1 = u(\alpha^3 + \alpha + 1) + v(2\alpha^2 + 4)$. Dostaneme $v = 4\alpha^2 + 4\alpha + 1$, což je hledaný inverzní prvek.

8.

$+$	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

9. Buď $T = \mathbb{Z}_2[\alpha]/(\alpha^4 + \alpha^3 + 1)$. Najděte ireducibilní rozklad polynomu $x^3 - 1$ v $T[x]$. Máme $x^3 - 1 = (x - 1)(x^2 + x + 1)$. Musíme zjistit, zda lze nad T polynom $x^2 + x + 1$ dále rozložit.

Těleso T má 16 prvků. My hledáme takový, jehož třetí mocnina je rovna jedné a který je různý od jedné. To můžeme dělat zkoušením jednotlivých prvků. Jelikož je ale T těleso, víme již z přednášky, že $T^* = T \setminus \{0\}$ tvoří spolu s násobením grupu, tzv. multiplikativní grupu tělesa T. Ta má 15 prvků a každý z nich má nějaký řád. Později se na přednášce dovíte, že tento řád musí dělit počet prvků grupy, to jest číslo 15. I bez této znalosti ale můžeme ověřit, že $\alpha^{15} = 1$. Kandidáty na kořeny polynomu x^2+x+1 by proto mohly být prvky $\alpha^5 = \alpha^3+\alpha+1$ a $\alpha^{10} = \alpha^6+\alpha^2+1 = (\alpha^4+\alpha^2+\alpha)+\alpha^2+1 = \alpha^3+\alpha$. Zjistili jsme, že se jedná o prvky různé od jedné, a proto $x^3-1 = (x-1)(x-(\alpha^3+\alpha))(x-(\alpha^3+\alpha+1))$.

Příklad lze řešit i elementárně. Pokud v T existují dva kořeny polynomu $x^2 + x + 1$ různé od jedné, označme je t, s, pak je mezi nimi vztah $t+s = 1$, tj. $t = s+1$. To víme buď z příkladu 6, nebo z toho, že $x^2 + x + 1 = x^2 + (t + s)x + ts$, čili z Viètových vztahů. Buď bez újmy na obecnosti t kořen s nulovým absolutním členem. Pak je $t = a\alpha^3 + b\alpha^2 + c\alpha$ pro nějaká $a, b, c \in \mathbb{Z}_2$. Zároveň ale $t^2 + t + 1 = 0$, ekvivalentně $t^2 = t + 1$. Dosadíme:

$$\begin{aligned} t^2 &= a\alpha^6 + b\alpha^4 + c\alpha^2 = a(\alpha^3 + \alpha^2 + \alpha + 1) + b(\alpha^3 + 1) + c\alpha^2 = \\ &= (a + b)\alpha^3 + (a + c)\alpha^2 + a\alpha + (a + b) = a\alpha^3 + b\alpha^2 + c\alpha + 1. \end{aligned}$$

Porovnáním koeficientů dostaneme, že $a + b = a$, a tedy $b = 0$, a dále $a + c = b$, a tedy $a = c$. Zároveň $a + b = 1$, což dává $a = c = 1$ a $b = 0$. Hledané kořeny jsou proto $\alpha^3 + \alpha$ a $\alpha^3 + \alpha + 1$.

11. Ověřte, že je $T = \mathbb{Z}_2[\alpha]/(\alpha^3 + \alpha + 1)$ těleso a najděte v něm všechny kořeny polynomu $x^7 + 1$. O těleso se jedná, jelikož $\alpha^3 + \alpha + 1$ je ireducibilní v $\mathbb{Z}_2[\alpha]$; zřejmě tam nemá kořen a je stupně 3. Kořeny polynomu $x^7 + 1$ jsou právě všechny nenulové prvky zadaného 8prvkového tělesa T. To plyne opět z toho, že $T^* = T \setminus \{0\}$ tvoří s násobením sedmiprvkovou grupu a pro každý její prvek t proto musí platit $t^7 = 1$. (Buď je $t = 1$, nebo má t řád 7.)

12. Dokažte, že v tělese $T = \mathbb{Z}_3[\alpha]/(\alpha^2+1)$ najdete prvek u s vlastností, že každý nenulový prvek tělesa T lze napsat jako mocninu u. Napište ireducibilní rozklad polynomu $x^8 - 1$ v $T[x]$. Těleso T má 9 prvků. V 8prvkové grupě T^* hledáme prvek řádu 8. Nabízí se položit $u = \alpha$, ale $\alpha^4 = 1$, takže α má řád 4 (jelikož $\alpha, \alpha^2 = 2, \alpha^3 = 2\alpha$ jsou různé od 1).

Zkusme proto například $u = \alpha + 1$. V tom případě v T máme $u^2 = (\alpha+1)^2 = \alpha^2 + 2\alpha + 1 = 2\alpha$. Takže $u^3 = 2\alpha + 1$, $u^4 = \alpha^2 = 2$, $u^5 = 2\alpha + 2$, $u^6 = \alpha$, $u^7 = \alpha + 2$, $u^8 = 1$.

Hledaným rozkladem je potom $x^8 - 1 = \prod_{k=1}^{8}(x - u^k)$.

13. Dokažte, že existuje izomorfismus mezi okruhy $R = \mathbb{Z}_5[\alpha]/(\alpha^4 - 1)$ a $\mathbb{Z}_5^4$. Zadefinujeme zobrazení $\psi : R \to \mathbb{Z}_5^4$ vztahem

$$\psi(r) = (r \mod \alpha - 1, r \mod \alpha - 2, r \mod \alpha - 3, r \mod \alpha - 4).$$

Všimněte si, že polynom $\alpha^4 - 1 \in \mathbb{Z}_5[\alpha]$ má v $\mathbb{Z}_5$ kořeny $1, 2, 3, 4$. Jelikož jsou polynomy $\alpha - 1$, $\alpha - 2$, $\alpha - 3$, $\alpha - 4$ po dvou nesoudělené, víme z Čínské zbytkové věty, že ψ je bijekce (víme, že R má 5^4 prvků).

Podobně jako ve 4. příkladu je při ověřování toho, že ψ je okruhový homomorfismus, jediným netriviálním krokem ověřit slučitelnost s násobením, tj. že pro libovolné prvky $r, s \in R$ jest $\psi(r \cdot s) = \psi(r)\psi(s)$. To se dělá totožným způsobem; jen v tomto případě máme na pravé straně čtyři složky místo jedné.

14. Je následující polynom symetrický?

$$(x_1 + x_2 - x_3 - x_4)(x_1 - x_2 + x_3 - x_4)(x_1 - x_2 - x_3 + x_4)$$

Užijeme definici symetrického polynomu a fakt, že každou permutaci lze napsat jako složení transpozic prohazujících sousední prvky (jistě dobře znáte bubble sort). Stačí tedy ověřit, že se zadaný součin nezmění při transpozicích $(x_1\ x_2)$, $(x_2\ x_3)$ a $(x_3\ x_4)$. To se udělá snadno dosazením.

15. Vyjádřete následující symetrické polynomy jako součet součinů elementárních symetrických polynomů:

(a) $3x^2yz + 3xy^2z + 3xyz^2$,

(b) $x^3(y + z) + y^3(x + z) + z^3(x + y)$.

V případě (a) zřejmě máme $3x^2yz + 3xy^2z + 3xyz^2 = 3s_1s_3$. Případ (b) se nejsnáze vyřeší Gaussovým algoritmem popsaným v 11. kapitole skript doc. Stanovského. Dostaneme výsledek $s_1^2s_2 - s_1s_3 - 2s_2^2$.