**Algebrou proti koronaviru VII**

(cvičení cihlovou barvou jsme udělali na cvičení, a tak je můžete vynechat)

## Faktorokruhy a kořenová/rozkladová nadtělesa

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

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

   (b) $x^{13} \pmod{x^4+x+1}$ [$x^3+x^2+1$]

2. Pracujme nad $\mathbb{Z}_3$.

   (a) Ověřte, že je polynom $p(\alpha)=\alpha^2+1$ ireducibilní. [nemá kořen]

   (b) Okruh $\mathbb{Z}_3[\alpha]/(\alpha^2+1)$ je pak těleso. Kolikaprvkové? [devítiprvkové]

   (c) Spočítejte

   $(2\alpha+1)+(2\alpha+2)$ [$\alpha$] $(\alpha)^5$ [$\alpha$] $\alpha^{-1}$[$2\alpha$] $(\alpha+1)^{-1}$[$\alpha+2$] $2\alpha\cdot(2\alpha+1)$ [$2\alpha+2$] $\alpha^{-1}\cdot(\alpha+2)$ [$\alpha+1$]

   (d) Vyřešte soustavu lineárních rovnic s maticí: $\left(\begin{array}{cc|c} \alpha & 1 & \alpha+1 \\ \alpha+1 & \alpha+1 & \alpha \end{array}\right)$ [$[\alpha;\alpha+2]$]

3. Napište všechna kořenová a rozkladová nadtělesa následujících polynomů z $\mathbb{Q}[x]$:

   (a) $x^2-2$ [kořenová: $\mathbb{Q}(\sqrt{2})=\mathbb{Q}(-\sqrt{2})$, rozkladové: $\mathbb{Q}(\sqrt{2},-\sqrt{2})=\mathbb{Q}(\sqrt{2})$]

   (b) $x^3-2x^2-2x-3$ [kořenová: $\mathbb{Q}(3)=\mathbb{Q}$, $\mathbb{Q}(-\frac{1}{2}+\frac{i\sqrt{3}}{2})=\mathbb{Q}(-\frac{1}{2}-\frac{i\sqrt{3}}{2})$, rozkladové: $\mathbb{Q}(-\frac{1}{2}+\frac{i\sqrt{3}}{2},-\frac{1}{2}-\frac{i\sqrt{3}}{2},3)=\mathbb{Q}(-\frac{1}{2}+\frac{i\sqrt{3}}{2})$]

   nad tělesem $\mathbb{Q}$ obsažená v $\mathbb{C}$.

4. Popište rozkladové nadtěleso polynomu $x^2+x+1$ nad $\mathbb{Z}_2$ a rozložte v něm daný polynom na lineární členy. [$\mathbf{T}\simeq\mathbb{Z}_2[\alpha]/(\alpha^2+\alpha+1)$, $x^2+x+1=(x+(\alpha+1))(x+\alpha)$]

5. 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 $\mathbf{T}[x]$. [Polynom zde má 3 kořeny: 1, $\alpha^3+\alpha$ a $\alpha^3+\alpha+1$, tedy se rozkládá na součin kořenových činitelů.]

6. V okruhu $\mathbb{Z}_3[\alpha]/(\alpha^4+\alpha^3+\alpha+2)$ najděte prvek, který nemá (multiplikativní) invers. [např. $\alpha^4+\alpha^3+\alpha+2=(2+\alpha+\alpha^2)(1+\alpha^2)$]

*A pro odvážné několik zábavných a zcela dobrovolných příkladů navíc:*

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

(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) řešení lineární rovnice $\alpha\cdot x+(\alpha+1)=\alpha^2$ [$\alpha^2+\alpha+1$]

8.* Napište tabulky operací čtyřprvkového tělesa. [prvky tělesa reprezentujeme jako polynomy nad $\mathbb{Z}_2$ modulo ireducibilní polynom $\alpha^2+\alpha+1$

| $+$ | $0$ | $1$ | $\alpha$ | $\alpha+1$ |
|---|---|---|---|---|
| $0$ | $0$ | $1$ | $\alpha$ | $\alpha+1$ |
| $1$ | $1$ | $0$ | $\alpha+1$ | $\alpha$ |
| $\alpha$ | $\alpha$ | $\alpha+1$ | $0$ | $1$ |
| $\alpha+1$ | $\alpha+1$ | $\alpha$ | $1$ | $0$ |

| $\times$ | $0$ | $1$ | $\alpha$ | $\alpha+1$ |
|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $\alpha$ | $\alpha+1$ |
| $\alpha$ | $0$ | $\alpha$ | $\alpha+1$ | $1$ |
| $\alpha+1$ | $0$ | $\alpha+1$ | $1$ | $\alpha$ |

]

9.* Buď $T=\mathbb{Z}_2[\alpha]/(\alpha^4+\alpha^3+1)$. Najděte ireducibilní rozklad polynomu $x^3-1$ v $T[x]$. [$x^3+1=(x+1)(x+\alpha^3+\alpha+1)(x+\alpha^3+\alpha)$]

10.* Dokažte, že jsou okruhy (ve skutečnosti dokonce tělesa) $\mathbb{Q}[\alpha]/(\alpha^3-2)$ a $\mathbb{Q}(\sqrt[3]{2})$ izomorfní (ideálně zkonstruujte dosvědčující izomorfismus). [$a\alpha^2+b\alpha+c\mapsto a\sqrt[3]{4}+b\sqrt[3]{2}+c$]

11.* Ověřte, že je $\mathbb{Z}_2[\alpha]/(\alpha^3+\alpha+1)$ těleso a najděte v něm všechny kořeny polynomu $x^7+1$. [kořenem je každý invertibilní prvek (lze si všimnout, že $x^7+1=(x+1)(x^6+\ldots+1)$, přičemž kořenem druhého z činitelů je číslo $t$ právě tehdy, splňuje-li $t^6+\ldots+t+1=0$, což je ekvivalentní $t(t^5+\ldots+1)=1$, tedy s každým kořenem je i jeho invers kořenem a úvaha funguje i naopak)]

12.* Najděte v tělese $T=\mathbb{Z}_3[\alpha]/(\alpha^2+1)$ prvek $u$ s vlastností, že každý nenulový prvek tělesa $T$ lze napsat jako mocninu $u$. [např. $\alpha+2$]

13.* Napište ireducibilní rozklad polynomu $x^8-1$ v $T[x]$, kde $T$ je těleso z předchozího příkladu. [$x^8-1=(x^4+1)(x^4-1)=(x+1)(x^3+2x^2+2x+1)(x^2+1)(x^2-1)=(x+1)(x^3+2x^2+2x+1)(x^2+1)(x+1)(x-1)$; kořeny druhého činitele jsou $\alpha+2,\alpha+1,2\alpha+1$, kořeny třetího (přímo z definice tohoto tělesa) $\alpha,2\alpha$]

14.* Dokažte, že existuje izomorfismus mezi okruhy $\mathbb{Z}_5[\alpha]/(\alpha^4-1)$ a $\mathbb{Z}_5^4$. [použijme ČVZ pro polynomy a fakt, že polynom $x^4-1$ má nad $\mathbb{Z}_5$ čtyři kořeny $1,2,3,4$, tj. je součinem $\prod_{a\in\mathbb{Z}_5^*}(x-a)$]

15.* Je následující polynom symetrický?

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

[ano; stačí si rozmyslet, že libovolná transpozice dvou proměnných výsledný polynom nezmění (jen převede jeden činitelze zadání na druhý), tudíž ani žádná obecná permutace]

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

(a) $3x^2yz+3xy^2z+3xyz^2$ [v obou případech postupujme podle Gaussova algoritmu; $3s_1s_3$]

(b) $x^3(y+z)+y^3(x+z)+z^3(x+y)$. [$s_1^2s_2-2s_2^2-s_1s_3$]