11. Existence kořenových a rozkladových nadtěles

1. Najít iredubilní polynom stupně n nad $\mathbb{Z}_p[x]$, kde p je prvočíslo, nebývá pro $n \geq 4$ bez dalších teoretických poznatků snadné. Pro $n \leq 3$ to však nečiní problémy, neboť ireducibilita v těchto případech splývá s neexistencí kořene.

Nalezněte všechny monické ireducibilní polynomy stupně 2 a 3 v $\mathbb{Z}_3[x]$.

Rozhodněte, zda mezi ně patří polynom $x^2 + x + 1$ a rozhodněte, zda je tento polynom ireducibilní v $\mathbb{Z}_2[x]$.

2. Rozhodněte, zda polynomy $x^4 + 1$, $x^6 + 1$, $x^6 + x^3 + 2$ jsou v $\mathbb{Z}_3[x]$ ireducibilní.

3. Sestrojte tabulky binárních operací $T[y]_m$, je-li $T = \mathbb{Z}_2$ a $m = x^2 + 1$.

4. (Pokračování) Je okruh $\mathbb{Z}_2[y]_{x^2+1}$ tělesem? Kolik má v tomto okruhu polynom $x^2 + 1$ kořenů a které prvky to jsou (zde kořenem rozumíme každý prvek, který po dosazení dá nulovou hodnotu)?

5. To, že okruh $\mathbb{Z}_2[x]_{x^2+1}$ není tělesem, jsme mohli prohlásit okamžitě (bez studia tohoto okruhu). Proč?

6. Dokažte, že okruh $\mathbb{R}[x]_{x^2+1}$ je izomorfní s $\mathbb{C}$. ($\mathbb{R}$ a $\mathbb{C}$ jsou reálná a komplexní čísla).

7. Vytvořte tabulku sčítání a násobení v okruhu $\mathbb{Z}_3[y]_{y^2+1}$. Je to těleso? Nalezněte nějaký polynom ireducibilní nad tímto okruhem a nalezněte též rozklad polynomu $x^2 + 1$.

8. Buď $a \in \mathbb{Z}_p[y]$ ireducibilní polynom a ať $a = \sum a_i y^i$. Pro $j \in \mathbb{N}_0$ označme r_j ten prvek $\mathbb{Z}_p[y]_a$, který splňuje $r_j \equiv y^{p^j} \bmod a$. Dokažte, že r_j je kořenem polynomu $b \in \mathbb{Z}_p[y]_a[x]$, kde $b = \sum a_i x^i$.

Pomocí tohoto výsledku vysvětlete, proč $x^3 + x + 1$ má v $\mathbb{Z}_2[y]_{y^3+y+1}[x]$ rozklad $(x - y)(x - y^2)(x - (y^2 + y))$.

9. Dokažte, že polynom $a = x^6 + x^3 + 1 \in \mathbb{Z}_2[x]$ je ireducibilní.

Řešení

1. Ireducibilní v $\mathbb{Z}_3[x]$ jsou polynomy $x^2 + 1$, $x^2 + x + 2$, $x^2 + 2x + 2$, $x^3 + 2x + 2$, $x^3 + 2x + 1$, $x^3 + 2x + 2$, $x^3 + x^2 + 2$, $x^3 + x^2 + x + 2$, $x^3 + x^2 + 2x + 1$, $x^3 + 2x^2 + 1$, $x^3 + 2x^2 + x + 1$, $x^3 + 2x^2 + 2x + 2$, takže polynom $x^2 + x + 1$, který je v $\mathbb{Z}_2[x]$ ireducibilní, v $\mathbb{Z}_3[x]$ ireducibilní není.

2. Nejsou, neboť $x^4 + 1 = (x^2 + x + 2)(x^2 + 2x + 2)$, $x^6 + 1 = (x^2 + 1)^3$ a $x^6 + x^3 + 2 = (x^2 + x + 2)^3$. Poslední dva rozklady lze okamžitě ověřit, uvědomíme-li si, že $a \mapsto a^3$ je endomorfismus $\mathbb{Z}_3[x]$ (jde o tzv. Frobeniův endomorfismus).

3.

+	0	1	y	y+1
0	0	1	y	y+1
1	1	0	y+1	y
y	y	y+1	0	1
y+1	y+1	y	1	0

·	0	1	y	y+1
0	0	0	0	0
1	0	1	y	y+1
y	0	y	1	y+1
y+1	0	y+1	y+1	0

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

4. Není, neboť prvek $y+1$ není v daném okruhu invertibilní. Kořeny polynomu x^2+1 jsou prvky 1 a y.

5. Polynom $x^2+1 \in \mathbb{Z}_2[x]$ není ireducibilní, neboť $x^2+1=(x+1)^2$.

6. $(a+bx)\cdot(c+dx) = ac+bdx^2+(ad+bc)x \equiv (ac-bd)+(ad+bc)x \bmod (x^2+1)\mathbb{R}[x]$, neboť $x^2 \equiv -1 \bmod (x^2+1)\mathbb{R}[x]$. To je přímý důkaz. Tvrzení je však možno dokázat i bez podobného výpočtu, použijeme-li Tvrzení 12.4 a uvědomíme-li si, že $\mathbb{C} = \mathbb{R}[\mathrm{i}]$.

7. Polynom x^2+1 je v $\mathbb{Z}_3[x]$ ireducibilní, takže to těleso skutečně je. Tabulka sčítání je zcela zřejmá, následuje tabulka násobení.

·	0	1	2	y	y+1	y+2	2y	2y+1	2y+2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	y	y+1	y+2	2y	2y+1	2y+2
2	0	2	1	2y	2y+2	2y+1	y	y+2	y+1
y	0	y	2y	2	y+2	2y+2	1	y+1	2y+1
y+1	0	y+1	2y+2	y+2	2y	1	2y+1	2	y
y+2	0	y+2	2y+1	2y+2	1	y	y+1	2y	2
2y	0	2y	y	1	2y+1	y+1	2	2y+2	y+2
2y+1	0	2y+1	y+2	y+1	2	2y	2y+2	y	1
2y+2	0	2y+2	y+1	2y+1	y	2	y+2	1	2y

$x^2+1=(x-y)(x-2y)$, ireducibilní je například x^3+2x+1.

8. Vyhodnocením $b(y^{p^j})$ v $\mathbb{Z}_p[y]$ dostáváme $\sum a_i(y^{p^j})^i = \sum a_i^{p^j}(y^i)^{p^j} = \sum (a_i y^i)^{p^j}$ $= (\sum a_i y^i)^{p^j} = a^{p^j} \equiv 0 \bmod p$, neboť $z \mapsto z^{p^j}$ je endomorfismus okruhu $\mathbb{Z}_p[y]$ (je to j-tá mocnina Frobeniova endomorfismu).

V případě $\mathbb{Z}_2[y]_{y^3+y+1}$ obdržíme $r_0 = y$, $r_1 = y^2$ a $r_2 = y^2+y \equiv y^4 \bmod y^3+y+1$.

9. a nemá zjevně dělitele stupně 1. Jediný ireducibilní dělitel stupně 2 je x^2+x+1, ale $x^6+x^3+1 = (x^2+x+1)(x^4+x^3)+1$. Není-li a ireducibilní, musí být tedy součinem dvou ireducibilních polynomů b, c stupně 3, ať $b = \sum b_i x^i$ a $c = \sum c_i x^i$. Protože $b^2 = b_3x^6+b_2x^4+b_1x^2+b_0$, je $b \neq c$. Ovšem $b_3 = c_3 = 1$, a z ireducibility plyne $b_0 = c_0 = 1$. Dále $b_2 \neq c_2$ by vedlo na $a_5 = 1$, ovšem je $a_5 = 0$, takže $b_2 = c_2$. Je tedy $b_1 \neq c_1$, odkud dostáváme $b(1) = 0$ nebo $c(1) = 0$. Pak b nebo c není ireducibilní, což je ve sporu s naším předpokladem. Proto musí být a ireducibilní.