13. Jednoznačnost kořenových a rozkladových nadtěles

(cvičení 1–6 na sebe navazují)

1. Buď p prvočíslo a $n, m \in \mathbb{N}$. Dokažte, že n dělí m právě když $p^n - 1$ dělí $p^m - 1$.

2. Buď p prvočíslo a $n, m \in \mathbb{N}$. Dokažte, že $n|m$ právě když $x^n - 1|x^m - 1$ v $\mathbb{Z}_p[x]$.

3. Ať $n, m \in \mathbb{N}$ a $n|m$. Pak pro každé prvočíslo $p \geq 2$ existuje vnoření $GF(p^n)$ do $GF(p^m)$.

4. Ať $n, m \in \mathbb{N}$ a ať p je prvočíslo. Lze-li $GF(p^n)$ vnořit do $GF(p^m)$, tak $n|m$.

5. Buď T konečné těleso řádu $q = p^n$, kde p je prvočíslo. Pak rozkladové nadtěleso polynomu $x^{q^k - 1} - 1 \in T[x]$ má q^k prvků.

6. Ukažte, že nad každým konečným tělesem T existuje nekonečně mnoho různých ireducibilních polynomů $a \in T[x]$.

7. Buď $U \subseteq T$ rozkladové nadtěleso polynomu $a \in T[x]$. Ať $\varphi \in \mathrm{Aut}(U)$ splňuje $\varphi(t) = t$ pro každé $t \in T$, a ať $\alpha \in T$ je kořen a. Ukažte, že $\varphi(a)$ je také kořen a.

8. Buď $U \supseteq T$ rozkladové nadtěleso monického ireducibilního polynomu $a \in T[x]$. Buďte $\alpha, \beta \in U$ dva kořeny polynomu a. Pak existuje automorfismus $\varphi \in \mathrm{Aut}(U)$ takový, že $\varphi(\alpha) = \beta$ a že $\varphi(t) = t$ pro každé $t \in T$.

Řešení

1. $m = nq \Rightarrow p^m - 1 = (p^n - 1)(1 + p^n + \cdots + p^{(q+1)n})$
$p^n - 1 | p^m - 1 \Rightarrow m = nq + r$, $0 \le r < n$, takže $p^m - 1 = p^{nq+r} - 1 = p^{nq+r} - p^r + p^r - 1 = p^r(p^{nq} - 1) + p^r - 1 = (p^n - 1)p^r(1 + p^n + \cdots + p^{(q-1)n}) + p^r - 1$. Jelikož $p^r - 1 < p^m - 1$, je $p^r - 1 = 0$, a tedy $r = 0$.

2. Ať $m = nq+r$, $0 \le r < q$ a ať $a = 1+x^n+\cdots+x^{(q-1)n}$. Platí $x^{nq}-1 = (x^n-1)a$, takže $x^m-1 = x^{nq+r}-x^r+x^r-1 = x^r(x^n-1)a+(x^r-1)$, takže $n|m \Leftrightarrow x^n-1|x^m-1$.

3. $GF(p^m)$ je rozkladové nadtěleso polynomu $x^{p^m-1} - 1$. Podle cvičení 2 a 1 platí $x^{p^n-1} - 1 | x^{p^m-1} - 1 \Leftrightarrow p^n - 1 | p^m - 1 \Leftrightarrow n|m$. Čili polynom $x^{p^n-1} - 1$ se v $GF(p^m)$ rozkládá na kořenové činitele, čili $GF(p^m)$ obsahuje rozkladové nadtěleso tohoto polynomu nad prvotělesem $P \simeq \mathbb{Z}_p$. Toto rozkladové nadtěleso je izomorfní $GF(p^n)$.

4. Předpokládejme $GF(p^n) \subseteq GF(p^m)$ a buď α primitivní prvek $GF(p^n)$ a β primitivní prvek $GF(p^m)$. Multiplikativní grupa $GF(p^m)$ má p^m-1 prvků, zatímco multiplikativní grupa $GF(p^n)$ má p^n-1 prvků. Podle Lagrangeovy věty p^n-1 dělí p^m-1, takže $n|m$ dle cvičení 1.

5. Protože $q^k = p^{kn}$ a n dělí kn, existuje podle cvičení 3 těleso U řádu q^k takové, že $U \supseteq T$. U je zjevně příslušným rozkladovým nadtělesem.

6. (Jeden z mnoha možných důkazů.) Ať m_α je minimální polynom prvku $\alpha \in T[\alpha]$, platí $[T[\alpha] : T] = \operatorname{st} m_\alpha$. Je-li ireducibilních polynomů konečně mnoho, je stupeň nadtěles, jež lze vyjádřit adjunkcí jediného prvku (například α), omezený. Podle předchozího cvičení však existují taková tělesa stupně k pro každé $k \in \mathbb{N}$.

7. Důkaz lze provést třemi různými způsoby, lišícími se mírou využití již dokázaných tvrzení. Je užitečné se seznámit se všemi řešeními.

A. Položme $S = T$, $V = U$, $f = \mathrm{id}_T$ a $g = \varphi$. Pak $f_x(a) = a$, takže $\varphi(\alpha) = g(\alpha)$ je kořen a podle 13.8.

B. Označme $\varphi(\alpha)$ jako β a ať $j_\alpha : T[x] \to U$, $j_\beta : T[x] \to U$ jsou dosazovací homomorfismy. Máme $\varphi_x(a) = a$, a podle 13.4 je $\varphi j_\alpha = j_\beta \varphi_x$. Dosadíme-li do této rovnice a, dostaneme $\varphi j_\alpha(a) = \varphi(ax) = \varphi(0) = 0 = a(\beta)$.

C. Ať $a = \sum a_i x^i$. Pak $\sum a_i \alpha^i = 0$ a použitím φ na obě strany rovnosti dostáváme $\varphi(\sum a_i\alpha^i) = \sum \varphi(a_i\alpha^i) = \sum a_i\varphi(\alpha^i) = \sum a_i\varphi(\alpha)^i = \sum a_i\beta^i = 0$, takže β je kořen a.

8. Protože a je ireducibilní, je $m_\alpha = m_\beta = a$. Podle 13.7 existuje izomorfismus $f : T[\alpha] = T[\beta]$ takový, že $f(\alpha) = \beta$ a $f(t) = t = \mathrm{id}_T(t)$ pro každé $t \in T$. Podle 13.8 (kde $T[\alpha]$ a $T[\beta]$ mají roli T a S, a $U = V$ je rozkladové nadtěleso jak nad $T[\alpha]$, tak nad $T[\beta]$) lze $f : T[\alpha] \to T[\beta]$ rozšířit na izomorfismus $g : U \to V$. Je tedy $g \in \Gamma(U|T)$ a $g(\alpha) = \beta$.