13. Jednoznačnost kořenových a rozkladových nadtěles

13.1 Lemma. *Ať $f : R \simeq S$ je izomorfismus okruhů a ať $I \subseteq R$ a $J \subseteq S$ jsou ideály takové, že $f(I) = J$. Potom zobrazení $a + I \mapsto f(a) + J$ je korektně definované a je to izomorfismus $R/I \simeq S/J$.*

Důkaz. $\mathrm{nat}_J\, f : R \to S/J$ je surjektivní homomorfismus, který zobrazuje prvek $a \in R$ na $f(a) + J$. Jeho jádrem je ideál I, a proto podle 1. věty o izomorfismu (7.10) je $a + I \mapsto f(a) + J$ izomorfismus R/I a S/J. $\square$

Je-li $f : R \to S$ homomorfismus okruhů, definujeme $f_x : R[x] \to S[x]$ tak, že pro $a = \sum a_i x^i \in R[x]$ je $f_x(a) = \sum f(a_i)x^i$. Všimněte si, že zobrazení f_x je rozšířením homomorfismu f.

13.2 Lemma. *$f_x : R[x] \to S[x]$ je okruhový homomorfismus.*

Důkaz. Ať $a = \sum a_i x^i$ a $b = \sum b_i x^i$ jsou polynomy z $R[x]$. Pak $f_x(a+b) = \sum f(a_i + b_i)x^i = \sum (f(a_i) + f(b_i))x^i = f_x(a) + f_x(b)$ a $f_x(a \cdot b) = \sum_k f(\sum_{i+j=k} a_i b_j)x^k = \sum_k (\sum_{i+j=k} f(a_i)f(b_j))x^k = f_x(a)f_x(b)$. Zbytek je zřejmý. $\square$

Okruh $R[x]$ je generován množinou $R \cup \{x\}$. Je-li A nějaký jiný okruh a h_1, h_2 jsou homomorfismy $R[x] \to A$, tak podle 3.3 musí být $h_1 = h_2$, pokud platí $h_1(x) = h_2(x)$ a pro každé $r \in R$ je $h_1(r) = h_2(r)$. Tohoto pozorování využijeme v obou následujících lemmatech.

13.3 Lemma. *Buďte $f : R \to S$ a $g : S \to T$ homomorfismy okruhů. Pak $(gf)_x = g_x f_x$.*

Důkaz. Platí $(gf)_x(x) = g_x(f_x(x))$ a pro $r \in R$ je $g_x f_x(r) = gf(r) = (gf)_x(r)$. $\square$

13.4 Důsledek. *Buď $f : R \simeq S$ izomorfismus okruhů. Pak $f_x : R[x] \to S[x]$ je rovněž izomorfismus.*

Důkaz. Podle 13.3 je $f_x(f^{-1})_x = (\mathrm{id}_S)_x = \mathrm{id}_{S[x]}$ a $(f^{-1})_x f_x = (\mathrm{id}_R)_x = \mathrm{id}_{R[x]}$. $\square$

13.5 Lemma. *Buď $f : R \to S$ homomorfismus okruhů a ať $\alpha \in R$. Pak $f j_\alpha = j_{f(\alpha)} f_x$.*

$$\begin{array}{ccc} R[x] & \xrightarrow{f_x} & S[x] \\ {\scriptstyle j_\alpha}\downarrow & & \downarrow{\scriptstyle j_{f(\alpha)}} \\ R & \xrightarrow{f} & S \end{array}$$

Důkaz. $f j_\alpha(r) = f(r) = j_{f(\alpha)}(f(r)) = j_{f(\alpha)} f_x(r)$ pro $r \in R$, a $f j_\alpha(x) = f(\alpha) = j_{f(\alpha)}(x) = j_{f(\alpha)} f_x(x)$. $\square$

13.6 Lemma. *Buď $f : T \simeq S$ izomorfismus komutativních těles a ať $I \subseteq T[x]$ a $J \subseteq S[x]$ jsou nenulové ideály, pro které platí $f_x(I) = J$. Jsou-li $a \in T[x]$ a $b \in S[x]$ ty (jednoznačně určené) monické polynomy, které splňují $I = aT[x]$ a $J = bS[x]$, tak platí $f_x(a) = b$.*

Důkaz. $bS[x] = J = f_x(I) = f_x(aT[x]) = f_x(a)f_x(T[x]) = f_x(a)S[x]$ a $f_x(a)$ je monický polynom. Víme (viz kapitola 10), že ideál J je generován právě jedním monickým polynomem. Proto se $f_x(a)$ musí rovnat b. $\square$

13.7 Tvrzení. *Buďte $T \subseteq U$ a $S \subseteq V$ komutativní tělesa, $f : T \simeq S$ izomorfismus a ať $\alpha \in U$ je prvek algebraický nad T a $\beta \in V$ prvek algebraický nad S. Izomorfismus $g : T[\alpha] \simeq S[\beta]$ splňující $g(\alpha) = \beta$ a $g(t) = f(t)$ pro všechna $t \in T$ existuje právě když $f_x(m_\alpha) = m_\beta$.*

Důkaz. Předpokládejme nejprve, že platí $f_x(m_\alpha) = m_\beta$. S využitím 12.3 a 13.1 sestrojíme řadu izomorfismů

$$T[\alpha] \simeq T[x]/m_\alpha T[x] \simeq S[x]/m_\beta S[x] \simeq S[\beta].$$

Oba krajní izomorfismy vyjadřují skutečnost, že každé kořenové nadtěleso algebraického prvku je strukturálně shodné s kvocientem podle hlavního ideálu příslušného minimálního polynomu (toto pozorování je obsahem Tvrzení 12.3). Prostřední izomorfismus je pak přímou aplikací 13.1, kde se říká, že izomorfismus okruhů (zde je to izomorfismus f_x) lze přenést na izomorfismus kvocientních okruhů, jestliže faktorizujeme přes ideály, které si v daném izomorfismu jednoznačně odpovídají (zde to jsou hlavní ideály generované polynomy a a b).

Proveďme nyní naznačený postup podrobně. Podle Tvrzení 12.3 jsou zobrazení $u : T[x]/m_\alpha T[x] \to T[\alpha]$ a $v : S[x]/m_\beta S[x] \to S[\beta]$, jež jsou definována vztahy $u(a+m_\alpha T[x]) = a(\alpha)$ a $v(b+m_\beta S[x]) = b(\beta)$, izomorfismy. Protože f_x je podle 13.4 izomorfismus $T[x]$ a $S[x]$ a protože podle předpokladu je $f_x(m_\alpha T[x]) = m_\beta S[x]$, dostáváme z 13.1 izomorfismus $w : T[x]/m_\alpha T[x] \simeq S[x]/m_\beta S[x]$, $w(a + m_\alpha T[x]) = f_x(a) + m_\beta S[x]$.

Jako vhodný kandidát se na místo hledaného izomorfismu g nabízí vwu^{-1}. Stačí ověřit, že je $vwu^{-1}(\alpha) = \beta$ a že $vwu^{-1}(t) = f(t)$ pro každé $t \in T$. Z definic izomorfismů v, w a u ale skutečně dostáváme $vwu^{-1}(t) = vw(t+m_\alpha T[x]) = v(f(t)+m_\beta S[x]) = f(t)$. Protože $x(\alpha) = \alpha$ a $x(\beta) = \beta$, tak $vwu^{-1}(\alpha) = vw(x + m_\alpha T[x]) = v(x + m_\beta S[x]) = \beta$, a lze tedy položit $g = vwu^{-1}$.

Nyní naopak předpokládejme, že existuje izomorfismus $g : T[\alpha] \simeq S[\beta]$, který je rozšířením $f : T \simeq S$, a splňuje $g(\alpha) = \beta$. Uvažme dosazovací homomorfismy $j_\alpha : T[\alpha][x] \to T[\alpha]$ a $j_\beta : S[\beta][x] \to S[\beta]$. Podle 13.5 je $j_\beta g_x = g j_\alpha$:

$$\begin{array}{ccc} T[x] \subseteq T[\alpha][x] & \xrightarrow{g_x} & S[\beta][x] \supseteq S[x] \\ {\scriptstyle j_\alpha}\big\downarrow & & \big\downarrow{\scriptstyle j_\beta} \\ T \ \subseteq \ T[\alpha] & \xrightarrow{g} & S[\beta] \ \supseteq \ S \end{array}$$

Pro $a \in T[x]$ je jistě $f_x(a) = g_x(a)$, neboť g je rozšířením f. Pro $a \in T[x]$ tedy platí $a \in m_\alpha T[x] \Leftrightarrow a(\alpha) = 0 \Leftrightarrow j_\alpha(a) = 0 \Leftrightarrow g j_\alpha(a) = 0 \Leftrightarrow j_\beta g_x(a) = 0 \Leftrightarrow (g_x(a))(\beta) = 0 \Leftrightarrow (f_x(a))(\beta) = 0 \Leftrightarrow f_x(a) \in m_\beta S[x]$. Polynom a tedy patří do ideálu $m_\alpha T[x]$ právě když $f_x(a)$ patří do ideálu $m_\beta S[x]$, takže $f_x(m_\alpha T[x]) = m_\beta S[x]$. Podle 13.6 je $f_x(m_\alpha)$ rovno m_β. $\square$

13.8 Věta. *Buď $f : T \simeq S$ izomorfismus komutativních těles, $a \in T[x]$, $\operatorname{st} a \geq 1$, a ať $U \supseteq T$ je rozkladové nadtěleso polynomu $a \in T[x]$, zatímco $V \supseteq S$ je rozkladové nadtěleso polynomu $b = f_x(a)$. Ať $\alpha_1, \ldots, \alpha_m$ jsou kořeny a v U a $\beta_1, \ldots, \beta_n$ kořeny b ve V. Pak $m = n$ a existuje permutace $\sigma \in S_n$ a izomorfismus $g : U \simeq V$ tak, že $g(t) = f(t)$ pro všechna $t \in T$ a $g(\alpha_i) = \beta_{\sigma(i)}$ pro $1 \leq i \leq n$.*

Důkaz. Ať $a = p_1^{k_1} \dots p_r^{k_r}$ je rozklad polynomu a na ireducibilní činitele v $T[x]$. Položme $q_i = f_x(p_i)$, $1 \leq i \leq k$. Pak $b = q_1^{k_1} \dots q_r^{k_r}$ je podle 13.4 rozklad na ireducibilní činitele v $S[x]$. Důkaz provedem indukcí podle $[U : T]$. Je-li $U = T$, lze kořeny uspořádat tak, že $p_i = x - \alpha_i$ a $q_i = x - \beta_i$, $1 \leq i \leq r$, takže stačí položit $g = f$. Ať je $[U : T] = j > 0$ a ať věta platí pro každý stupeň menší než j. Kořeny a polynomy jistě můžeme uspořádat tak, aby α_1 byl kořen p_1 a β_1 kořen q_1, a aby $\operatorname{st} p_1 = \operatorname{st} q_1 > 1$. Podle 13.8 existuje izomorfismus $h : T(\alpha_1) \to S(\beta_1)$ takový, že $h(\alpha_1) = \beta_1$ a $h(t) = f(t)$ pro každé $t \in T$. Protože $[U : T] = [U : T(\alpha_1)] \cdot [T(\alpha_1) : T] = [U : T(\alpha_1)] \cdot \operatorname{st} p_1$ (viz 12.1 a 12.3), je $[U : T(\alpha_1)] < j$. U je rozkladové nadtěleso polynomu $a \in T(\alpha_1)[x]$ a V je rozkladové nadtěleso polynomu $b \in S(\beta_1)[x]$. Podle indukčního předpokladu existuje izomorfismus $g : U \to V$, který má požadované vlastnosti a rozšiřuje h, a tím i f. $\square$

13.9 Věta. *Ať je $q \in \mathbb{N}$. Pak konečné komutativní těleso řádu q existuje právě když q je rovno p^n pro některé prvočíslo p a $n \in \mathbb{N}$. Libovolná dvě komutativní tělesa téhož řádu q jsou izomorfní.*

Důkaz. Ať pro $i = 1, 2$ jsou T_i komutativní tělesa řádu q a ať P_i jsou jejich prvotělesa. Podle 12.8 existuje prvočíslo p a $n \in \mathbb{N}$ takové, že je $P_i \simeq \mathbb{Z}_p$ a $q = p^n$. Podle 11.8 je T_i rozkladovým nadtělesem polynomu $x^{p^n} - x \in P_i[x]$, takže podle 13.8 plyne $T_1 \simeq T_2$ z $P_1 \simeq P_2$. $\square$

Těleso T řádu p^n se často značí $GF(p^n)$, kde GF je zkratka z 'Galois field'. Lze se dohodnout, že $GF(p)$ je rovno $\mathbb{Z}_p$. Ovšem pro $n > 1$ se už žádný kanonický tvar $GF(p^n)$ nezavádí. Podle 10.19 je multiplikativní grupa $GF(p^n)$ cyklická řádu $p^n - 1$. Proto má $\varphi(p^n - 1)$ generátorů. Každý z těchto generátorů se nazývá *primitivní prvek*.