12. Algebraické prvky a minimální polynomy

V celé této kapitole ‘těleso’ znamená ‘komutativní těleso’.

Jestliže $U \supseteq T$ jsou komutativní tělesa, tak U můžeme chápat jako vektorový prostor nad T (sčítání ve vektorovém prostoru je shodné se sčítáním v U, je–li $t \in T$ a $u \in U$, tak skalární násobení $t \cdot u$ definujeme jako součin $t \cdot u$ v tělese U). Dimenze $\dim_T U$ vektorového prostoru U se značí $[U : T]$ a nazývá se *stupeň* tělesa U (nad T). Je–li $[U : T] < \infty$, řekneme, že U je *rozšíření konečného stupně*.

Jako příklad můžeme uvést komplexní a reálná čísla. Je zřejmé, že $\mathbb{C}$ jako reálný vektorový prostor má dimenzi 2 (máme-li zvolit jeho bázi, tak nejpřirozenější je vybrat čísla 1 a i). Poznamenejme, že $\mathbb{C}$ je jak kořenové, tak rozkladové nadtěleso polynomu $x^2 + 1 \in \mathbb{R}[x]$.

12.1 Lemma. *Buď $T \subseteq U \subseteq V$ do sebe vřazená tělesa. Potom $[V : T] = [V : U] \cdot [U : T]$.*

Důkaz. Ať A je báze U nad T a B je báze V nad U. Stačí ukázat, že $C = \{ab;\, a \in A,\, b \in B\}$ je báze V nad T. Je-li $v \in V$, existují $u_b \in U$, že $v = \sum_{b \in B} u_b b$, a protože každé u_b lze zapsat jako $\sum_{a \in A} t_{a,b} a$, kde $t_{a,b} \in T$, tak $v = \sum t_{a,b} ab$. Naopak, ať $\sum t_{a,b} ab = 0$, kde $a \in A$, $b \in B$ a $t_{a,b} \in T$. Pak $\sum_{b \in B} (\sum_{a \in A} t_{a,b} a) b = 0$, takže pro každé $b \in B$ je $\sum_{a \in A} t_{a,b} a = 0$, a tedy $t_{a,b} = 0$ pro všechna $a \in A$, $b \in B$. $\square$

12.2 Lemma. *Ať $S \supseteq R$ jsou komutativní okruhy a α ať je prvek S. Pak okruh $R[\alpha]$ je roven okruhu $\operatorname{Im} j_\alpha = \{a(\alpha);\, a \in R[x]\}$.*

Důkaz. $\{a(\alpha);\, a \in R[x]\} = \operatorname{Im} j_\alpha$ je podokruh S, a proto $R[\alpha] \subseteq S$. Pro $a = \sum a_i x^i \in R[x]$ je $a(\alpha) = \sum a_i \alpha^i$ jistě prvek $R[\alpha]$. $\square$

Prvek $\alpha \in U$ se nazývá *algebraický* (nad T), jestliže $a(\alpha) = 0$ pro nějaké $a \in T[x]$, $a \neq 0$. Pokud takový polynom a neexistuje, nazýváme α *transcendentní* (nad T).

12.3 Tvrzení. *Nechť $T \subseteq U$ jsou tělesa a ať $\alpha \in U$ je prvek algebraický nad T. Pak existuje jediný monický polynom $m \in T[x]$ takový, že pro všechna $a \in T[x]$ je $a(\alpha) = 0$ právě když m dělí a. Polynom m je ireducibilní a hlavní ideál $mT[x]$ je jádrem dosazovacího homomorfismu $j_\alpha : T[x] \to U$. Zobrazení $a + mT[x] \mapsto a(\alpha)$ je izomorfismus okruhů $T[x]/mT[x]$ a $T[\alpha]$. Oba tyto okruhy jsou tělesa a platí $T[\alpha] = T(\alpha)$.*

Důkaz. Pro $a \in T[x]$ platí $a(\alpha) = 0$ právě když je $j_\alpha(a) = 0$. Jádro homomorfismu j_α je vlastní ideál, a z kapitoly 10 víme, že každý vlastní ideál lze jednoznačným způsobem vyjádřit jako hlavní ideál generovaný monickým polynomem.

Ať m dělí pq, kde $p, q \in T[x]$ jsou polynomy. Pak $0 = m(\alpha) = p(\alpha)q(\alpha)$, takže je $p(\alpha) = 0$ nebo $q(\alpha) = 0$. Čili m dělí p nebo q, takže vidíme, že m je prvočinitel, a tedy ireducibilní polynom.

Podle 12.2 je $\operatorname{Im} j_\alpha$ rovno $T[\alpha]$, takže j_α je surjektivní homomorfismus $T[x]$ na $T[\alpha]$. Podle první věty o izomorfismu 7.10 je zobrazení $a + mT[x] \mapsto a(\alpha)$ izomorfismem okruhů $T[x]/mT[x]$ a $T[\alpha]$. Protože $mT[x]$ je maximální ideál (viz 10.12), tak je okruh $T[x]/mT[x]$ tělesem (viz 7.14), a proto je i okruh $T[\alpha]$ těleso. Protože $T(\alpha)$ je nejmenší podtěleso U, které obsahuje $T[\alpha]$, musí být $T(\alpha) = T[\alpha]$. $\square$

Polynom m z Tvrzení 12.3 se nazývá *minimální polynom* prvku α (nad T) a značí se m_α.

12.4 Tvrzení. *Buď $\alpha \in U \supseteq T$. Pak α je algebraický nad T právě když $[T(\alpha) : T] < \infty$. Je-li α algebraický nad T, tak $T(\alpha) = T[\alpha]$ a $[T[\alpha] : T] = \operatorname{st} m_\alpha$.*

Důkaz. Ať $[T(\alpha) : T] = n$. Je-li $n < \infty$, jsou $1, \alpha, \dots, \alpha^n$ prvky nad T lineárně závislé, takže existují $c_0, c_1, \dots, c_n$ prvky T takové, že $\sum c_i \alpha^i = 0$ a $c_j \neq 0$ pro alespoň jedno $0 \le j \le n$. Tudíž $c(\alpha) = 0$ pro $0 \neq c = \sum c_i x^i$, takže α je algebraický nad T.

Naopak, ať $\alpha \in U$ je algebraický nad T a $s = \operatorname{st} m_\alpha$. Ukážeme, že $1, \alpha, \dots, \alpha^{s-1}$ tvoří bázi $T[\alpha] = T(\alpha)$. Je-li $c \in T[x]$, $\operatorname{st} c \le s - 1$, tak $c(\alpha) = 0$ jedině pro $c = 0$. Proto jsou $1, \alpha, \dots, \alpha^{s-1}$ lineárně nezávislé. Je-li $\beta \in T[\alpha]$, tak existuje $b \in T[x]$, že $\beta = b(\alpha)$. Ovšem $b = m_\alpha q + r$, kde $q, r \in T[x]$, $r = \sum r_i x^i$ a $\operatorname{st} r < \operatorname{st} m_\alpha = s$, takže $\beta = b(\alpha) = r(\alpha) = \sum_{1 \le i \le s-1} r_i \alpha^i$. $\square$

Ať $T \subseteq U$ jsou tělesa. U nazveme *algebraickým rozšířením* T, jestliže každý prvek $\beta \in U$ je algebraický nad T.

12.5 Důsledek. *Každé rozšíření konečného stupně U tělesa T je algebraické rozšíření.*

Důkaz. Buď $\beta \in U$. Podle 12.1 je $[U : T] = [U : T(\beta)] \cdot [T(\beta) : T]$, takže $[T(\beta) : T]$ je konečné číslo. Podle 12.4 je β algebraický prvek. $\square$

12.6 Tvrzení. *Ať $T \subseteq U$ jsou tělesa a $\alpha_1, \dots, \alpha_n \in U$ jsou algebraické nad T. Potom $V = T(\alpha_1, \dots, \alpha_n)$ je konečné algebraické rozšíření T a $V = T[\alpha_1, \dots, \alpha_n]$.*

Důkaz. Položme $T_0 = T$ a $T_i = T[\alpha_1, \dots, \alpha_i]$, $1 \le i \le n$. Indukcí ukážeme, že T_i je těleso a že pro $i \ge 1$ je $[T_i : T_{i-1}]$ konečné. Pro $i = 0$ není co dokazovat, ať $0 \le i \le n-1$. Pak $T_{i+1} = T_i[\alpha_{i+1}]$, přičemž α_{i+1} je algebraický nad $T_i \supseteq T$. Podle 12.3 je T_{i+1} těleso a podle 12.4 je $[T_{i+1} : T_i]$ konečné.

Tudíž $V = T_n$, V je rozšíření konečného stupně, a to je podle 12.5 algebraické. $\square$

12.7 Důsledek. *Ať $U \supseteq T$ je rozkladové nadtěleso polynom $a \in T[x]$ a ať $\alpha_1, \dots, \alpha_n \in U$ jsou všechny kořeny a. Pak $U = T[\alpha_1, \dots, \alpha_n]$.*

Na závěr této kapitoly ještě zmíníme, jak lze dosažené výsledky využít pro konečná tělesa.

12.8 Lemma. *Buď T konečné těleso, a ať p je jeho charakteristika. Pak je $p > 0$ prvočíslo a $|T| = p^n$ pro nějaké $n \in \mathbb{N}$.*

Důkaz. T je vektorový prostor nad prvotělesem P. Protože P je konečné, je $P \simeq \mathbb{Z}_p$. T je nad P dimenze $[T : P]$, takže $|T| = |P|^{[T:P]}$. $\square$

Podle 10.19 je multiplikativní grupa T^* každého konečného tělesa T cyklická. Má-li těleso $q = p^n$ prvků, tak T^* je řádu $q - 1 = p^n - 1$, takže cyklická grupa T^* má $\varphi(p^n - 1)$ generátorů. Je zvykem každý takový generátor nazývat *primitivní prvek* tělesa T. Je-li $P \simeq \mathbb{Z}_p$, tak $T = P[\xi]$ jistě platí pro každý primitivní prvek ξ. Podle 12.4 tudíž dostáváme:

12.9 Tvrzení. *Ať T je konečné těleso řádu p^n a P jeho prvotěleso. Ať ξ je nějaký primitivní prvek tělesa T. Pak je $P \simeq \mathbb{Z}_p$ a $\operatorname{st} m_\xi = n$.*

Z 12.3 nyní okamžitě plyne:

12.10 Důsledek. *Pro každé $n \in \mathbb{N}$ a pro každé prvočíslo p existuje ireducibilní polynom $a \in \mathbb{Z}_p[x]$, který je stupně n.*

Podle 12.10 je tedy vždy možné sestrojit těleso řádu p^n ve tvaru $\mathbb{Z}_p[x]_a$ (viz kapitola 11). V následující kapitole dokážeme, že libovolná dvě tělesa řádu p^n jsou izomorfní. To znamená, že ze strukturálního hlediska nezáleží na konkrétní volbě ireducibilního polynomu a.

Možná, že si někdo položí otázku po vztahu polynomu $x^{p^n} - x \in \mathbb{Z}_p[x]$ a ireducibilních polynomů stupně n. K tomu lze například uvést, že $x^{p^n} - x$ je roven součinu všech ireducibilních polynomů stupňů $m \leq n$, přičemž každý z těchto polynomů se v rozkladu polynomu $x^{p^n} - x$ vyskytuje právě jednou. Toto tvrzení ovšem leží mimo rámec výkladu, a dokazovat ho nebudeme.