12. Algebraické prvky a minimální polynomy

1. Buď $R(+,\cdot,-,\mathbf{0},\mathbf{1})$ komutativní okruh, $G \subseteq R$ množina jeho generátorů a I podgrupa $R(+,-,\mathbf{0})$. Ukažte:

(i) $\{a \in R;\ aI \subseteq I\}$ je podokruh R.
(ii) Je-li $gI \subseteq I$ pro každé $g \in G$, je I ideál R.
(iii) Je-li $J \subseteq R[x]$ podgrupa $R[x](+,-,\mathbf{0})$ taková, že $ra \in J$ a $xa \in J$ pro každé $a \in J$, $r \in R$, je J ideál v $R[x]$.

2. Buď T komutativní těleso. Definujme $I = \{\sum a_i x^i \in T[x];\ \sum a_i = 0\}$. Dokažte, že I je ideál. Najděte monický polynom $m \in T[x]$ takový, že $I = mT[x]$. Zjistěte, zda je m určen jednoznačně.

3. Z teorie množin víme (a je to snadné dokázat), že množina všech konečných posloupností tvořených prvky dané nekonečné množiny A má stejnou mohutnost jako A. Buď T nekonečné těleso a U jeho algebraické rozšíření. Ukažte, že U má stejnou mohutnost jako T.

4. Buď T konečné těleso a U jeho algebraické rozšíření. Ukažte, že mohutnost U je buď konečná, nebo nekonečná spočetná.

5. Buď $T \subseteq U \subseteq V$ do sebe vřazená tělesa. Ať V je algebraické nad U a U je algebraické nad T. Ukažte, že V je algebraické nad T.

6. Buď T těleso. Ukažte, že existuje jeho algebraické rozšíření U takové, že každé $a \in T[x]$, $\operatorname{st} a \geq 1$, se rozkládá v U na kořenové činitele.

7. (pokračování) Ukažte, že ke každému tělesu T existuje jeho algebraické rozšíření $U \supseteq T$, které je algebraicky uzavřené (tj. každý polynom $a \in U[x]$, $\operatorname{st} a \geq 1$, se rozkládá v U na kořenové činitele).

8. Buď U rozšíření tělesa T. Položme $V = \{\alpha \in U;\ \alpha \text{ je algebraické nad } T\}$. Ukažte, že V je podtěleso U.

9. Buď $U \subseteq T$ rozšíření těles a ať $\alpha \in U$ je transcendentní nad T. Najděte izomorfismus $T[x]$ a $T[\alpha] \subseteq U$.

10. Buď $T \subseteq U$ rozšíření těles. Ať $\alpha \in U$, $\alpha \neq 0$, a ať $a = m_\alpha$ je jeho minimální polynom stupně n. Vyjádřete $m_{\alpha^{-1}}$ pomocí koeficientů polynomu a.

11. Určete $[\mathbb{C} : \mathbb{R}]$ a $[\mathbb{R} : \mathbb{Q}]$. Srovnejte $[\mathbb{C} : \mathbb{R}]$ a $|\mathbb{C} : \mathbb{R}|$, kde $|\mathbb{C} : \mathbb{R}|$ značí index Abelovy grupy $\mathbb{R}(+,-,0)$ v $\mathbb{C}(+,-,0)$ (viz kapitola 6).

Řešení

1. (i) Je-li $aI \subseteq I$ a $bI \subseteq I$, je $(a+b)I \subseteq aI + bI \subseteq I$ a $abI \subseteq aI \subseteq I$. (ii) Podokruh dle (i) obsahuje G, a tedy je roven R. (iii) Použij (ii) na $R[x]$.

2. I je zjevně podgrupa $T[x]$. Je-li $a \in I$, tak $xa \in I$ a $ra \in I$ pro každé $r \in T$. Podle cvičení 2(iii) je tedy I ideál. (Důkaz, že I je ideál, lze samozřejmě provést i přímo.) $m = x - 1$. Polynom m je samozřejmě určen jednoznačně (viz kapitola 10).

3. Víme, že $T[x]$ je stejně mohutné jako U. Zobrazení $\alpha \to m_\alpha$ je zobrazením U do $T[\alpha]$, které sice není prosté, avšak každá z ekvivalenčních tříd jádra tohoto zobrazení je konečná.

5. Buď $\alpha \in V$ a ať $m = [U(\alpha) : U]$. Buď $a = \sum a_i x^i \in U[x]$ monický polynom stupně $m$takový, že $a(\alpha) = 0$ (a je tedy minimální polynom prvku α nad U). Pak $a_0, \dots, a_m \in U$ jsou algebraické nad T a těleso $U' = T[a_1, \dots, a_m]$ má nad T konečný stupeň. Pak $a \in U'[x]$ a $[U'(\alpha) : T] < \infty$ podle 12.1. Proto je α algebraický nad T.

6. Označme $\mathcal{U}$ množinu všech algebraických rozšíření tělesa T (zde je potřeba jisté opatrnosti z hlediska teorie množin, neboť $\mathcal{U}$ je vlastně třída a ne množina. Poučený čtenář si však s užitím cvičení 2 a 3 jistě s tímto problémem poradí, nepoučený ať $\mathcal{U}$ považuje za množinu.) Uspořádejme $\mathcal{U}$ tak, aby bylo $U_1 \leq U_2$ právě když U_1 je podtělesem U_2. Je-li I lineárně uspořádaná neprázdná množina, kde pro každé $i \in I$ je definováno $U_i \in \mathcal{U}$, přičemž $U_i \leq U_j$ kdykoliv $i, j \in I$ a $i \leq j$, tak $\cup_{i \in I} U_i$ opět patří do $\mathcal{U}$. Proto podle Zornova lemmatu obsahuje $\mathcal{U}$ maximální prvek, řekněme U. Ať $a \in T[x]$ je polynom, který se v U nerozkládá na lineární činitele. Pak existuje $V \supseteq U$, jež je rozkladovým polynomem $a \in U[x]$. Ale podle cvičení 5 je V algebraickým rozšířením T. To je spor s maximalitou U.

7. Položme $T_0 = T$ a definujme T_{i+1} jako algebraické rozšíření T_i takové, že každé $a \in T_i[x]$, st $a \geq 1$, se v T_{i+1} rozkládá na kořenové činitele. To je možné podle předchozího cvičení. Stačí pak položit $U = \cup T_i$.

8. Ať $\alpha, \beta \in V$. Pak $T[\alpha, \beta]$ je podle 12.6 algebraické rozšíření konečného stupně. Protože $\alpha + \beta$, $\alpha \cdot \beta$, α^{-1}, $-\alpha$ patří do $T[\alpha, \beta]$, jsou tyto prvky algebraické.

9. Uvažte dosazovací homomorfismus $j_\alpha : T[x] \to U$. Podle 12.2 je $\operatorname{Im} j_\alpha = T[\alpha]$ a $a \in \operatorname{Ker} j_\alpha \Leftrightarrow \alpha$ je kořen a, takže pro α transcendentní je $\operatorname{Ker} j_\alpha = \{0\}$.

10. $\sum a_i \alpha^i = 0 \Leftrightarrow \sum a_i \alpha^{i-n} = 0$, takže $m_{\alpha^{-1}} = \frac{1}{a_n} \sum_{0 \leq i \leq n} a_{n-i} x^i$.

11. $[\mathbb{C} : \mathbb{R}] = 2$, zatímco $[\mathbb{R} : \mathbb{Q}]$ a $|\mathbb{C} : \mathbb{R}|$ mají mohutnost kontinua (tj. mohutnost rovnou mohutnosti $\mathbb{R}$).