

Rozšírenia polí

Ak K je nadpole F , hovoríme, že K je rozšírenie F . V prípade, že K tvorí konečnorozmerný vektorový priestor nad F , hovoríme o konečnom rozšírení. V takomto prípade dimenziu tohoto vektorového priestoru označujeme $[K : F]$ a voláme stupeň rozšírenia.

Ak $F \subseteq L \subseteq K$ sú konečné rozšírenia, tak platí

$$[K : F] = [K : L] \cdot [L : F].$$

Algebraický prvok $u \in K$ je taký prvok, pre ktorý existuje polynóm $f(x) \in F[x]$ taký, že $f(u) = 0$ (t.j. u je koreňom F). Normovaný polynóm najmenšieho možného stupňa s touto vlastnosťou

Ak $F \cup \{u_1, \dots, u_k\} \subseteq K$, tak ako $F(u_1, \dots, u_k)$ označujeme najmenšie podpole K obsahujúce $F \cup \{u_1, \dots, u_k\}$. Platí, že $[F(u) : F]$ je rovné stupňu minimálneho polynómu prvku u .

1. Nech L je rozšírenie poľa F a $u \in L$. Dokážte, že ak $[F(u) : F] = 5$, tak $[F(u^2) : F] = 5$.
2. V poli $\mathbb{Q}(\sqrt[3]{2})$ nájdite inverzný prvok ku $1 - 2\sqrt[3]{2} + \sqrt[3]{4}$ (treba ho vyjadriť ako $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ pre vhodné $a, b, c \in \mathbb{Q}$.)
3. Nájdite izomorfizmus medzi poľami $\mathbb{Z}_3[x]/(x^2 + 1)$ a $\mathbb{Z}_3[x]/(x^2 + x + 2)$.
4. Nájdite minimálne polynómy týchto čísel nad $\mathbb{Q}$:
a) $\sqrt{2} + 1$; b) $2 - 3\sqrt{5}$; c) $\sqrt[3]{3} + \sqrt{3}$; d) $\sqrt{2} - \sqrt{3}$; e) $\sqrt[3]{2} + i$; f) $1 + \sqrt[3]{2} - \sqrt[3]{4}$;
g) $\frac{1}{2 - \sqrt[3]{2}} + \sqrt[3]{4}$; h) $\frac{3 + \sqrt{7}}{1 + 2\sqrt{7}}$.
5. Určite stupeň viacnásobného rozšírenia a nájdite bázu nad $\mathbb{Q}$:
a) $\mathbb{Q}(\sqrt{3}, \sqrt{5})$; b) $\mathbb{Q}(i, \sqrt{2})$; c) $\mathbb{Q}(\sqrt[3]{5}, \sqrt[3]{25})$; d) $\mathbb{Q}(1 + \sqrt{2}, 1 - \sqrt{8})$
6. Pomocou binomickej vety dokážte matematickou indukciou vzhľadom na a , že v $\mathbb{Z}_p$ platí rovnosť $a^p = a$ (pre ľubovoľné $a \in \mathbb{Z}_p$). (Toto je vlastne iná formulácia malej Fermatovej vety.)
7. Nech F je konečné pole a platí $|F| = n$. Ukážte, že potom pre každý prvok $a \in F \setminus \{0\}$ platí $a^{n-1} = 1$. (Tu je hint na odvodenie bez Lagrangeovej vety: Skúste využiť, že $a \mapsto ax$ je bijekcia $F \setminus \{0\} \rightarrow F \setminus \{0\}$; t.j. ak si označíme $F \setminus \{0\} = \{a_1, \dots, a_{n-1}\}$, tak máme aj rovnosť $F \setminus \{0\} = \{aa_1, \dots, aa_{n-1}\}$.)
8. Nech F je pole a $c \in F$. Označme $f(x) = x^n - 1$.
a) Ukážte, že ak c je koreň polynómu $f(x)$, tak
$$f(x) = (x - c)(x^{n-1} + cx^{n-2} + c^2x^{n-3} + \dots + c^{n-2}x + c^{n-1}).$$

b) Ukážte, že ak $f(x)$ má násobný koreň v F , tak F má konečnú charakteristiku a $\text{char}(F) \mid n$.

9. Ukážete s použitím predošlej úlohy, že polynóm

$$f(x) = x^{p^n} - x$$

v poli charakteristiky p nemá násobné korene.

10. Nech $\text{char}(F) = p$ (p je prvočíslo). Potom pre ľubovoľné $a, b \in F$ platí

$$\begin{aligned}(a + b)^p &= a^p + b^p \\ (ab)^p &= a^p b^p\end{aligned}$$

čiže zobrazenie $f: F \rightarrow F$, $f(x) = x^p$, je homomorfizmus. Ďalej pre ľubovoľné $n \in \mathbb{N}$ a $q = p^n$ máme

$$\begin{aligned}(a + b)^q &= a^q + b^q \\ (ab)^q &= a^q b^q\end{aligned}$$