Rozkladové pole

4. júna 2020

Rozkladové pole

Definícia

Nech F je pole, $f(x) \in F[x]$ je nekonštantný polynóm. Rozšírenie K poľa F nazývame *rozkladovým poľom polynómu* $f(x)$ *nad* F, ak existujú $c \in F$, $u_1, \ldots, u_n \in K$ také, že $L = F(u_1, \ldots, u_n)$ a f sa dá nad L rozložiť ako

$$f(x) = c(x - u_1)(x - u_2)\ldots(x - u_n).$$

Rozkladové pole

Veta

Nech F je pole, $f(x) \in F[x]$ a $\operatorname{st} f = n > 0$. Potom existuje rozšírenie K poľa F, ktoré je rozkladovým poľom polynómu $f(x)$.

Dôsledok

Ľubovoľné dve rozkladové polia polynómu $f(x)$ nad F sú izomorfné.

p^n-prvkové pole

Veta

Nech $q = p^n$, kde p je prvočíslo a $n > 0$ je prirodzené číslo. Potom existuje (až na izomorfizmus jediné) q-prvkové pole. Je to rozkladové pole polynómu $x^q - x$ nad $\mathbb{Z}_p$.

p^n-prvkové pole

Príklad

4-prvkové pole: $\mathbb{Z}_2[x]/(x^2+x+1)$

$$\begin{aligned} x^4 - x = x^4 + x &= x(x^3+1) \\ &= x(x+1)(x^2+x+1) \\ &= x(x+1)(x+u)(x+u+1) \end{aligned}$$

Korene sú práve všetky prvky poľa: 0, 1, u, $u+1$.

Izomorfizmus medzi rozšíreniami

Veta

Nech $\varphi\colon F \to F'$ je izomorfizmus polí. Nech $p(x)$ je ireducibilný polynóm nad F a $p'(x) \in F[x]$ je polynóm $\hat{\varphi}(p)$ (čiže polynóm, ktorý získame použitím izomorfizmu $\varphi\colon F \to F'$ na všetky koeficienty polynómu $f(x)$). Potom $p'(x)$ je tiež ireducibilný polynóm (nad F').
Nech u je koreň $p(x)$ (v nejakom nadpoli F) a v je koreň $p'(x)$ (v nejakom nadpoli F'). Potom existuje izomorfizmus

$$\sigma\colon F(u) \to F'(v),$$

ktorý zobrazí u na v a rozširuje φ, t.j. $\sigma(u) = v$ a $\sigma|_F = \varphi$.

Jednoznačnosť rozkladového poľa

Veta

Nech $\varphi\colon F \to F'$ je homomorfizmus polí, $f(x) \in F[x]$ a $f'(x) \in F'[x]$ je polynóm, ktorý získame z $f(x)$ aplikovaním φ na všetky koeficienty polynómu $f(x)$. (V označení z poznámky ?? to znamená $f'(x) = \hat{\varphi}(f(x))$.) Ak K je rozkladové pole polynómu $f(x)$ a L je rozkladové pole polynómu $f'(x)$, tak existuje izomorfizmus $\sigma\colon K \to L$, ktorý navyše rozširuje φ, t.j. $\sigma|_F = \varphi$.