Věta. *Nechť $R \subseteq R(\alpha)$ je jednoduché rozšíření těles, jeho stupeň označme $n = [R(\alpha) : R]$. Nechť $R \subseteq K$ je rozšíření těles. Pak existuje nejvýše n homomorfismů $\varphi : R(\alpha) \to K$ takových, že diagram*

$$\begin{array}{ccc} & R & \\ {\scriptstyle\subseteq}\swarrow & & \searrow{\scriptstyle\subseteq} \\ R(\alpha) & \xrightarrow{\ \varphi\ } & K \end{array} \tag{1}$$

komutuje, (tj. zúžení $\varphi|_R = \mathrm{id}_R$). Navíc platí, že každý takový homomorfismus φ je určen jednoznačně svou hodnotou $\varphi(\alpha)$, která je kořenem minimálního polynomu $f \in R[x]$ prvku $\alpha \in R(\alpha)$ nad R.

Důkaz. Zřejmě $\operatorname{st} f = n$, dále víme, že $R(\alpha) = R[\alpha] = \{g(\alpha); g \in R[x]\}$ (připomeňme, že $R(\alpha)$ je nejmenší těleso obsahující podmnožinu $R \cup \{\alpha\}$, kdežto $R[\alpha]$ je nejmenší okruh obsahující podmnožinu $R \cup \{\alpha\}$). Obecný prvek z $R[x]$ je tvaru $g = g_m x^m + \cdots + g_1 x + g_0$, kde $g_0, g_1, \ldots, g_m \in R$. Předpokládejme, že pro homomorfismus $\varphi : R(\alpha) \to K$ diagram (1) komutuje, a tedy $\varphi(g_i) = g_i$ pro každé i. Protože φ je homomorfismus, můžeme počítat

$$\begin{aligned} \varphi(g(\alpha)) &= \varphi(g_m \alpha^m + \cdots + g_1 \alpha + g_0) \\ &= \varphi(g_m) \cdot \varphi(\alpha)^m + \cdots + \varphi(g_1) \cdot \varphi(\alpha) + \varphi(g_0) \\ &= g_m \varphi(\alpha)^m + \cdots + g_1 \varphi(\alpha) + g_0 \\ &= g(\varphi(\alpha)). \end{aligned}$$

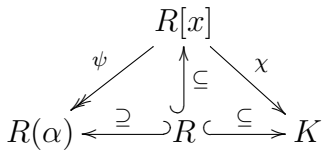
Předchozí výpočet znamená, že ze známe-li $\varphi(\alpha)$, jsme schopni určit $\varphi(g(\alpha))$ pro každé $g \in R[x]$. Speciálně pro $g = f$ dostáváme $0 = \varphi(0) = \varphi(f(\alpha)) = f(\varphi(\alpha))$, a tedy $\varphi(\alpha)$ je kořen f v K. V tělese K však nemůže mít polynom f více kořenů než $n = \operatorname{st} f$, proto ani homomorfismů φ, pro které komutuje diagram (1), není více než n.

Dodatek k větě. *Nechť $R \subseteq R(\alpha)$ je jednoduché rozšíření těles, jeho stupeň označme $n = [R(\alpha) : R]$. Nechť $R \subseteq K$ je rozšíření těles a f je minimální polynom prvku α nad R. Nechť $\beta \in K$ je kořen polynomu f. Pak existuje (a to jediný) homomorfismus $\varphi : R(\alpha) \to K$ splňující, že diagram* (1) *z předchozí věty komutuje a že $\varphi(\alpha) = \beta$.*

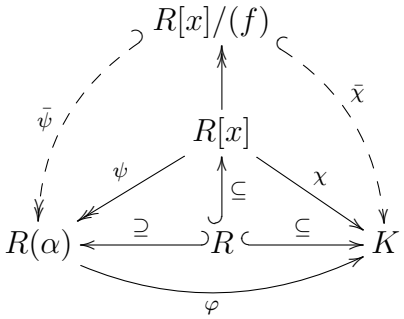
Důkaz. Nechť $\psi : R[x] \to R(\alpha)$ a $\chi : R[x] \to K$ jsou homomorfismy okruhů určené předpisy $\psi(g) = g(\alpha)$ a $\chi(g) = g(\beta)$ pro každé $g \in \mathbb{Z}[x]$. Protože obrazem

[1] Přednáška se nenachází ve skriptech profesora Rosického.

homomofismu ψ je $R[\alpha] = R(\alpha)$, je ψ surjektivní. Dostáváme komutativní diagram

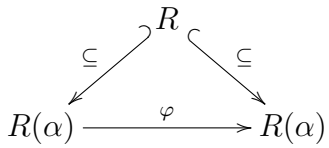


Protože f je minimální polynom prvků α i β nad R, platí $\ker\psi = \ker\chi = (f)$. Proto existují injektivní homomorfismy okruhů $\bar{\psi}$ a $\bar{\chi}$ tak, že následující diagram komutuje. Protože ψ surjektivní, je i $\bar{\psi}$ surjektivní, tedy je to izomorfismus. Stačí položit $\varphi = \bar{\chi} \circ \bar{\psi}^{-1}$.



Dodatek k větě je dokázán, stačí si uvědomit, že cesta diagramem z R doprava do K dává totéž jako cesta z R úplně nahoru a vpravo po $\bar{\chi} = \varphi \circ \bar{\psi}$, což dává totéž jako z R doleva a pak po φ.

Poznámka. Nechť $R \subseteq R(\alpha)$ je jednoduché rozšíření, $n = [R(\alpha) : R]$. Nechť homomorfismus $\varphi : R(\alpha) \to R(\alpha)$ je takový, že diagram



(2)

komutuje. Pak φ je bijekce (jinými slovy φ je automorfismus tělesa $R(\alpha)$ ponechávající na místě prvky tělesa R, tj. $\forall r \in R : \varphi(r) = R$), protože

- φ je injekce, neboť $R(\alpha)$ je těleso,
- φ je surjekce, neboť φ lze chápat jako lineární zobrazení vektorových prostorů $R(\alpha) \to R(\alpha)$ nad tělesem R konečné dimenze.

Pak množina všech automorfismů φ takových, že diagram (2) komutuje, tvoří grupu vzhledem ke skládání zobrazení. Tato grupa má podle výše uvedené věty nejvýše n prvků.

Aplikace na konečná tělesa

Nechť K je konečné těleso charakteristiky $\operatorname{char} K = p$. Pak $K = \mathbb{Z}_p(\alpha)$ pro vhodné $\alpha \in K$. Každý automorfismus $\varphi : K \to K$ splňuje $\varphi(r) = r$ pro každé $r \in \mathbb{Z}_p$, neboť je-li $r = \underbrace{1 + \cdots + 1 + 1}_{n}$, pak

$$\varphi(r) = \underbrace{\varphi(1) + \cdots + \varphi(1) + \varphi(1)}_{n} = \underbrace{1 + \cdots + 1 + 1}_{n} = r.$$

Definujme zobrazení $\psi : K \to K$ předpisem $\psi(u) = u^p$ pro každé $u \in K$. Protože umocňujeme v komutativním okruhu na prvočíselnou charakteristiku, pro každé $u, v \in K$ platí

$$\begin{aligned} \psi(u+v) &= (u+v)^p = u^p + v^p = \psi(u) + \psi(v), \\ \psi(uv) &= (uv)^p = u^p v^p = \psi(u)\psi(v), \\ \psi(1) &= 1^p = 1. \end{aligned}$$

A tedy ψ je homomorfismu okruhů, který je injektivní (K je těleso) i surjektivní (K je konečná množina). Proto $\psi \in \operatorname{Aut}(K)$, kde $\operatorname{Aut}(K)$ je grupa automorfismů tělesa K. Snadno dokážeme indukcí vzhledem ke $k \in \mathbb{N}$, že $\psi^k(u) = u^{p^k}$ pro každé $u \in K$. Skutečně, pro $k = 1$ jde o definici ψ. Jestliže rovnost platí pro nějaké $k \in \mathbb{N}$, pak

$$\psi^{k+1}(u) = (\psi \circ \psi^k)(u) = \psi(\psi^k(u)) = \psi(u^{p^k}) = (u^{p^k})^p = u^{p^{k+1}}.$$

Označme $n = [K : \mathbb{Z}_p]$, pak $|K| = p^n$. Výše jsme odvodili, že $|\operatorname{Aut}(K)| \leq n$. Určeme řád prvku ψ v grupě $(\operatorname{Aut}(K), \circ)$. Pro libovolné $k \in \mathbb{N}$ tedy platí následující ekvivalence:

$$\begin{aligned} \psi^k = \mathrm{id} \;&\Leftrightarrow\; \forall u \in K : u^{p^k} = u \\ &\Leftrightarrow\; \forall u \in K : u \text{ je kořen polynomu } x^{p^k} - x. \end{aligned}$$

Jestliže tedy pro nějaké $k \in \mathbb{N}$ platí $\psi^k = \mathrm{id}$, pak polynom $x^{p^k} - x$ stupně p^k má $|K| = p^n$ kořenů, a tedy $p^n \leq p^k$, odkud $n \leq k$.

Dostali jsme, že řád prvku ψ je alespoň n. Protože $|\operatorname{Aut}(K)| \leq n$, musí být řád prvku ψ roven n, a tedy platí, že $\operatorname{Aut}(K)$ je cyklická grupa generována ψ.

Označení. Nechť K je konečné těleso. Automorfismus $\psi : K \to K$ definovaný výše (tj. umocňování na charakteristiku) nazýváme Frobeniův automorfismus tělesa K.

Věta. *Nechť K je konečné těleso charakteristiky p. Nechť $\alpha \in K$ je takové, že $K = \mathbb{Z}_p(\alpha)$. Pak minimální polynom prvku α nad $\mathbb{Z}_p$ se rozkládá v $K[x]$ na*

lineární činitele, a to takto:

$$f = \prod_{i=0}^{n-1} (x - \alpha^{p^i}),$$

kde $n = [K : \mathbb{Z}_p]$*, tj.* $|K| = p^n$*.*

Důkaz. Protože $n = \operatorname{st} f$, stačí ověřit, že pro každé $i = 0, \ldots, n-1$ je α^{p^i} kořen f a že tyto kořeny jsou různé. Nechť ψ je Frobeniův automorfismus tělesa K. Víme, že $\mathrm{Aut}(K) = \langle\psi\rangle = \{\underbrace{\mathrm{id}, \psi, \psi^2, \ldots, \psi^{n-1}}_{\text{různé automorfismy}}\}$. Podle předchozích vět jsou α, $\psi(\alpha) = \alpha^p$, $\psi^2(\alpha) = \alpha^{p^2}$, …, $\psi^{n-1}(\alpha) = \alpha^{p^{n-1}}$ kořeny f, a to různé.

Normované ireducibilní polynomy nad $\mathbb{Z}_p$

Označení. Nechť p je prvočíslo, $d \in \mathbb{N}$. Označme $M_{p,d}$ (resp. $m_{p,d}$) součin (resp. počet) všech normovaných polynomů $f \in \mathbb{Z}_p[x]$ stupně d, které jsou ireducibilní nad $\mathbb{Z}_p$.

Příklad.

$$M_{2,2} = x^2 + x + 1; \quad m_{2,2} = 1,$$
$$M_{2,1} = (x+1) \cdot x; \quad m_{2,1} = 2.$$

Poznámka. Zřejmě $m_{p,n} \geq 1$ pro každé prvočíslo p a každé $n \in \mathbb{N}$. Vskutku, víme, že existuje těleso K mající p^n prvků, přitom $K = \mathbb{Z}_p(\alpha)$ pro vhodné α, přičemž minimální polynom prvku α nad $\mathbb{Z}_p$ má stupeň $[K : \mathbb{Z}_p] = n$.

Věta. *Pro každé prvočíslo* p *a každé* $n \in \mathbb{N}$ *platí*

$$\prod_{\substack{d \in \mathbb{N} \\ d|n}} M_{p,d} = x^{p^n} - x,$$

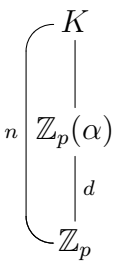
a tedy

$$\sum_{\substack{d \in \mathbb{N} \\ d|n}} d \cdot m_{p,d} = p^n.$$

Důkaz. Ukážeme, že z první rovnosti plyne druhá. Protože víme, že $M_{p,d}$ je součinem právě $m_{p,d}$ polynomů stupně d, platí $\operatorname{st} M_{p,d} = d \cdot m_{p,d}$, a tedy můžeme

počítat

$$\sum_{\substack{d\in\mathbb{N}\\ d|n}} d\cdot m_{p,d} = \sum_{\substack{d\in\mathbb{N}\\ d|n}} \operatorname{st} M_{p,d} = \operatorname{st} \prod_{\substack{d\in\mathbb{N}\\ d|n}} M_{p,d} = \operatorname{st}(x^{p^n}-x) = p^n.$$



Nechť těleso K má p^n prvků, víme, že $\prod_{\alpha\in K}(x-\alpha) = x^{p^n}-x$ (viz důkaz věty dokazující existenci tělesa o p^n prvcích jakožto rozkladového tělesa polynomu $x^{p^n}-x$). Proto libovolný normovaný ireducibilní polynom z $\mathbb{Z}_p[x]$, který je dělitelem polynomu $x^{p^n}-x$, se rozkládá na lineární činitele v $K[x]$, a má tedy všechny kořeny v K, a je tedy jejich minimálním polynomem. Pro libovolné $\alpha\in K$ označme f_α minimální polynom prvku $\alpha\in K$ nad $\mathbb{Z}_p$, pak $d = \operatorname{st} f_\alpha = [\mathbb{Z}_p(\alpha):\mathbb{Z}_p]$. Z multiplikativity stupně rozšíření plyne $d \mid n$. Dostali jsme, že každý normovaný ireducibilní polynom dělící $x^{p^n}-x$ je dělitelem polynomu $M_{p,d}$ pro vhodné $d\mid n$. Protože $x^{p^n}-x$ nemá násobné kořeny, plyne z jednoznačnosti rozkladu na ireducibilní činitele v $\mathbb{Z}_p[x]$, že

$$x^{p^n}-x \mid \prod_{\substack{d\in\mathbb{N}\\ d|n}} M_{p,d}.$$

Libovolný normovaný ireducibilní polynom $h\in\mathbb{Z}_p[x]$ stupně $d\mid n$ nám dává těleso $\mathbb{Z}_p[x]/(h)$ mající p^d prvků, přičemž $\beta = x+(h)$ je kořenem h. Protože každý prvek tělesa majícího p^d prvků je kořenem polynomu $x^{p^d}-x$, je β kořenem tohoto polynomu a proto minimální polynom h prvku β splňuje $h\mid x^{p^d}-x$. Využijeme známého vzorce

$$A-B \mid (A-B)(A^{m-1}+A^{m-2}B+\cdots+B^{m-1}) = A^m-B^m.$$

Z $d\mid n$ volbou $A=p^d$, $B=1$, $m=\frac{n}{d}$ dostáváme, že $p^d-1 \mid p^n-1$. Odtud zase volbou $A=x^{p^d-1}$, $B=1$, $m=\frac{p^n-1}{p^d-1}$ plyne $x^{p^d-1}-1 \mid x^{p^n-1}-1$. Proto $x^{p^d}-x = x\cdot(x^{p^d-1}-1) \mid x\cdot(x^{p^n-1}-1) = x^{p^n}-x$. Celkem tedy $h\mid x^{p^n}-x$. Opět využitím jednoznačnosti rozkladu na ireducibilní činitele v $\mathbb{Z}_p[x]$ dostáváme, že

$$\prod_{\substack{d\in\mathbb{N}\\ d|n}} M_{p,d} \mid x^{p^n}-x.$$

Oba polynomy jsou normované, proto z obou dělitelností plyne rovnost.