Minimální polynom algebraického prvku

Věta. *Nechť $R \subseteq T$ je rozšířením těles, $c \in T$ algebraický prvek nad R. Pak c je kořenem právě jednoho normovaného ireducibilního polynomu $f \in R[x]$. Navíc platí*

1. *pro libovolný $h \in R[x]$ je $h(c) = 0$, právě když $f \mid h$ v $R[x]$,*
2. *$R(c) = R[c]$ v T,*
3. *$1, c, c^2, \ldots, c^{n-1}$, kde $n = \operatorname{st} f$, je bází vektorového prostoru $R[c]$ nad R,*
4. *stupeň rozšíření $[R(c) : R] = \operatorname{st} f$.*

Důkaz. Protože c je algebraický prvek nad R, můžeme mezi všemi normovanými polynomy z $R[x]$, jejichž je c kořenem, zvolit polynom co možná nejmenšího stupně a označit jej f. Označme $n = \operatorname{st} f$. Zřejmě $n > 0$. Kdyby $f = g \cdot h$ pro nějaké nekonstantní polynomy $g, h \in R[x]$, tak by bylo možné je zvolit oba normované a dostali bychom spor, protože $\operatorname{st} g < n$, $\operatorname{st} h < n$ a přitom c by byl kořenem alespoň jednoho z nich. Je tedy f ireducibilní.

Zvolme libovolný $h \in R[x]$ takový, že $h(c) = 0$. Vydělíme-li polynom h polynomem f se zbytkem, dostaneme polynomy $q, r \in R[x]$ takové, že $h = q \cdot f + r$, přičemž $\operatorname{st} r < n$. Protože $0 = h(c) = q(c) \cdot f(c) + r(c) = r(c)$, kdyby r nebyl nulový polynom, existoval by v $R[x]$ normovaný polynom stupně $\operatorname{st} r$ mající kořen c, což by byl spor s naší volbou polynomu f. Proto $f \mid h$ v $R[x]$. Protože opačná implikace je zřejmá, dokázali jsme bod 1.

Je jasné, že normovaný polynom s kořenem c splňující bod 1 je jediný (kdybychom měli takové polynomy dva, každý z nich by dělil toho druhého).

Podle věty o podokruzích generovaných množinou platí, že libovolný prvek $\alpha \in R[c]$ je tvaru $\alpha = h(c)$ pro nějaký polynom $h \in R[x]$. Dělením se zbytkem opět dostaneme polynomy $q, r \in R[x]$ takové, že $h = q \cdot f + r$, přičemž $\operatorname{st} r < n$. Opět $\alpha = h(c) = q(c) \cdot f(c) + r(c) = r(c)$. Proto $1, c, c^2, \ldots, c^{n-1}$ generují vektorový prostor $R[c]$ nad R; kdyby tyto vektory byly lineárně závislé, existoval by v $R[x]$ nenulový polynom stupně menšíno než n, který by měl c za kořen, a to by byl spor. Dokázali jsme bod 3.

Zbývá ukázat, že $R(c) = R[c]$, jinými slovy, že $R[c]$ je těleso.

Víme, že libovolný nenulový prvek $\alpha \in R[c]$ je tvaru $\alpha = h(c)$. Protože $h(c) = \alpha \neq 0$, tak $f \nmid h$, a protože f je ireducibilní, tak jsou f a h nesoudělné. Proto jejich největší společný dělitel 1 lze vyjádřit Bezoutovou rovností, tedy existují polynomy $a, b \in R[x]$ tak, že $1 = a \cdot f + b \cdot h$. Dosazením c odtud dostaneme

$$1 = a(c) \cdot f(c) + b(c) \cdot h(c) = b(c) \cdot h(c) = b(c) \cdot \alpha$$

Je tedy $b(c) \in R[c]$ inverzní prvek k prvku α v okruhu $R[c]$. Dokázali jsme bod 2, díky níž z bodu 3 plyne bod 4.

Definice. Polynom $f \in R[x]$ z předchozí věty nazýváme minimální polynom algebraického prvku $c \in T$ nad R.