O primitivním prvku

Tvrzení 0.1. *Buď* $\mathbf{T}$ *těleso charakteristiky 0,* $\mathbf{T} \leq \mathbf{U}$ *rozšíření těles konečného stupně. Pak existuje* $\gamma \in \mathbf{U}$ *tak, že* $\mathbf{U} = \mathbf{T}(\gamma)$.

Důkaz. Indukcí dle n, kde $\mathbf{U} = \mathbf{T}(\gamma_1, \ldots, \gamma_n)$. Pro $n = 1$ je to triviální. K indukčnímu kroku předpokládejme, že $\mathbf{U} = \mathbf{T}(\alpha, \beta)$.

Označme $p, q \in T[x]$ minimální polynomy prvků α, resp. β, a $\mathbf{V}$ rozkladové nadtěleso polynomu pq. Dále ať $\{\alpha_i \in V;\, i = 1, 2, \ldots, \deg(p)\}$ a $\{\beta_j \in V;\, j = 1, 2, \ldots, \deg(q)\}$ jsou množiny všech kořenů polynomů p, resp. q. Jelikož je $\mathbf{T}$ nekonečné, lze zvolit $t \in T$ tak, aby $\alpha_i + t\beta_j$ byly vše po dvou různé prvky.

Položme $\gamma = \alpha + t\beta$ a zaveďme polynom $P = p(\gamma - tx) \in \mathbf{T}(\gamma)[x]$. Pro P platí, že $P(\beta) = p(\alpha) = 0$, a kdykoliv je $\beta_j \neq \beta$, pak $P(\beta_j) = p(\gamma - t\beta_j) \neq 0$, jelikož $\gamma - t\beta_j$ nemůže být žádné α_i (plyne přímo z definice t). Polynomy P a q mají tedy ve $\mathbf{V}$ právě jeden společný kořen, a sice β. Definujme H jako monický největší společný dělitel v $\mathbf{T}(\gamma)[x]$ polynomů P a q.

Jakožto dělitel q se H ve $\mathbf{V}$ rozkládá na (po dvou různé) lineární faktory. Ovšem každý kořen H musí být také kořenem P, takže nutně $H = x - \beta \in T(\gamma)[x]$. (Uvědomme si, že $H = 1$ by byl spor s platností Bézoutovy rovnosti ve $\mathbf{V}[x]$.) Máme tedy $\beta \in T(\gamma)$, z čehož již bezprostředně plyne i $\alpha \in T(\gamma)$. □