Věta. *Nechť $R \subseteq T$ je rozšíření těles, $a \in T$ prvek algebraický nad R. Nechť $f \in R[x]$ je minimální polynom prvku a nad R. Pak platí*

$$R(a) = R[a] = \{g(a) \mid g \in R[x]\} = \{g(a) \mid g \in R[x],\, \operatorname{st} g < \operatorname{st} f\}. \tag{1}$$

Navíc stupeň rozšíření $[R(a) : R] = \operatorname{st} f$.

Důkaz. Nechť $\varphi : R[x] \to T$ je homomorfismus okruhů určený předpisem $\varphi(g) = g(a)$ pro každé $g \in R[x]$. Následující diagram komutuje:

$$\begin{tikzcd}
R \arrow[r, hook, "\subseteq"] \arrow[d, hook, "\subseteq"'] & T \\
R[x] \arrow[ur, "\varphi"'] &
\end{tikzcd}$$

Zřejmě obraz $\varphi(R[x]) = \{g(a) \mid g \in R[x]\})$ je podokruh tělesa T obsahující $R \cup \{a\}$. Naopak každý podokruh tělesa T obsahující $R \cup \{a\}$ obsahuje $g(a)$ pro každé $g \in R[x]$. Je tedy $\varphi(R[x]) = R[a]$ a náš diagram můžeme upravit do tvaru

$$\begin{tikzcd}
R \arrow[r, hook, "\subseteq"] \arrow[d, hook, "\subseteq"'] & R[a] \arrow[r, hook, "\subseteq"] & T \\
R[x] \arrow[ur, two heads, "\tilde{\varphi}"] \arrow[urr, "\varphi"'] & &
\end{tikzcd}$$

Podle věty o minimálním polynomu platí, že každý polynom $g \in R[x]$, který má kořen a, je dělitený polynomem f v $R[x]$. Proto jádro

$$\ker \tilde{\varphi} = \ker \varphi = \{g \in R[x] \mid g(a) = 0\} = (f),$$

kde (f) je hlavní ideál generovaný polynomem f. Proto

$$\begin{tikzcd}
R \arrow[r, hook, "\subseteq"] \arrow[d, hook, "\subseteq"'] & R[a] \\
R[x] \arrow[ur, two heads, "\tilde{\varphi}"] \arrow[r, two heads, "\pi"'] & R[x]/(f) \arrow[u, hook, two heads]
\end{tikzcd} \tag{2}$$

Protože $R[x]/(f) \cong R[a]$, což je je podokruh tělesa T, a tedy obor integrity, je (f) prvoideál okruhu $R[x]$. Protože R je těleso, znamená to, že (f) je maximální ideál okruhu $R[x]$ (a také že f je ireducibilní nad R, což už víme). Proto $R[x]/(f) \cong R[a]$ je těleso, a tedy nejmenší podtěleso tělesa T obsahující $R \cup \{a\}$. Dostali jsme $R(a) = R[a]$.

[1]Pouze část přednášky, která se nenachází ve skriptech profesora Rosického.

Označme $n = \operatorname{st} f$. Pro každý polynom $g \in R[x]$ existují polynomy $q, r \in R[x]$ tak, že $g = q \cdot f + r$, $\operatorname{st} r < n$. Přitom $g(a) = q(a) \cdot f(a) + r(a) = r(a)$. Dokázali jsme (1).

Je-li $r = r_{n-1}x^{n-1} + \cdots + r_1 x + r_0 \in R[x]$, pak

$$r(a) = r_{n-1}a^{n-1} + \cdots + r_1 a + r_0,$$

a tedy $R[a]$ jakožto vektorový prostor nad R má systém generátorů

$$1, a, a^2, \ldots, a^{n-1}. \tag{3}$$

Kdyby vektory (3) byly lineárně závislé nad R, existovaly by $r_0, r_1, \ldots, r_{n-1} \in R$, ne všechny nulové, tak, že $\sum_{i=0}^{n-1} r_i a^i = 0$, odkud

$$r = r_{n-1}x^{n-1} + \cdots + r_1 x + r_0 \in R[x]$$

by byl nenulový polynom s kořenem a splňující $\operatorname{st} r < n = \operatorname{st} f$, spor. Jsou tedy (3) lineárně nezávislé nad R, odkud $[R(a) : R] = \operatorname{st} f$.

Poznámka. Nechť $R \subseteq T$ je rozšíření těles, $a \in T$ prvek transcendentní nad R. Pak stejným postupem ukážeme, že $R[a] \cong R[x]$, což není těleso, a tedy $R[a] \neq R(a)$. V tomto případě je $R(a)$ podílové těleso okruhu $R[a]$, tedy

$$R(a) \cong \{\tfrac{h}{g} \mid h, g \in R[x],\ g \neq 0\}$$

s obvyklými operacemi sčítání a násobení zlomků.

Definice. Nechť $R \subseteq T$ je rozšíření těles. Řekneme, že toto rozšíření je

- *jednoduché*, existuje-li $a \in T$, který je algebraický nad R, takový, že $T = R(a)$;
- *konečné*, je-li $[T : R] < \infty$;
- *algebraické*, je-li každý prvek $t \in T$ algebraický nad R.

Věta. *Každé jednoduché rozšíření těles je konečné. Každé konečné rozšíření těles je algebraické.*

Důkaz. (i) Je-li $T = R(a)$ pro $a \in T$, který je algebraický nad R, pak podle předchozí věty je $[T : R] = [R(a) : R] = \operatorname{st} f$, kde $f \in R[x]$ je minimální polynom prvku a nad R.

(ii) Je-li $R \subseteq T$ konečné rozšíření těles, pak $[T : R] = m$ je přirozené číslo. Pro libovolný prvek $t \in T$ jsou prvky $1, t, t^2, \ldots, t^m$ lineárně závislé nad

R, neboť je jich více než $\dim_R T = m$. Existují tedy $r_0, r_1, \ldots, r_m \in R$, ne všechny nulové, tak, že $\sum_{i=0}^m r_i t^i = 0$, odkud $r = r_m x^m + \cdots + r_1 x + r_0 \in R[x]$ je nenulový polynom s kořenem t, a tedy t je algebraický nad R.

Věta. *Nechť $R \subseteq T$ je rozšíření těles. Pak platí: $R \subseteq T$ je jednoduché rozšíření, právě když existuje polynom $f \in R[x]$, který je ireducibilní nad R, a izomorfismus okruhů $\varphi : T \to R[x]/(f)$ tak, že následující diagram komutuje*

$$\begin{tikzcd} R \arrow[r, hook, "\subseteq"] \arrow[d, hook, "\subseteq"'] & R[x] \arrow[d, "\pi"] \\ T \arrow[r, hook, two heads, "\varphi"'] & R[x]/(f) \end{tikzcd}$$

Důkaz. Předpokládejme, že takové f a φ existují a označme $a = \varphi^{-1}(\alpha)$, kde $\alpha = \pi(x) = x + (f)$. Ukážeme, že a je algebraický nad R a že $T = R(a)$. Nechť $f = f_n x^n + \cdots + f_1 x + f_0$, kde $f_0, f_1, \ldots, f_n \in R$, $f_n \neq 0$. Pro libovolné $r \in R$ jsme ztotožnili prvek r s jeho obrazem $\pi(r) = r + (f)$. Z komutativity diagramu pak plyne rovnost $\varphi(r) = \pi(r) = r + (f) = r$.

Protože $\alpha = \varphi(a)$, pro libovolný polynom $g = g_m x^m + \cdots + g_1 x + g_0 \in R[x]$ platí

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

Tuto hodnotu $g(\alpha) \in R[x]/(f)$ můžeme dále upravit

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

Speciálně pro $g = f$ dostaneme $f(\alpha) = f + (f) = 0 + (f)$, což je nula v tělese $R[x]/(f)$. Proto $\alpha \in R[x]/(f)$ je kořenem polynomu f. Protože φ je injektivní, z $\varphi(f(a)) = f(\alpha) = \varphi(0)$ plyne, že $f(a) = 0$ a že a je algebraický nad R.

Pro libovolný $t \in T$ platí $\varphi(t) = g + (f)$ pro vhodný $g \in R[x]$. Pak z výše vypočteného

$$\varphi(t) = g + (f) = g(\alpha) = \varphi(g(a)),$$

a tedy $t = g(a)$, vždyť φ je injektivní. Proto $T = R(a)$.

Naopak, předpokládejme, že $T = R(a)$. Podle (1) platí $T = R[a]$ a překreslením diagramu (2) dostaneme potřebné, vždyť inverzní zobrazení k izomorfismu okruhů je izomorfismus okruhů.

Poznámka. Předchozí věta je ve skriptech nepřesně formulovaná (jde o větu 11.12 na straně 114). V jejím důkaze sice chyba není, ale nedokazuje se zde přesně to, co je ve znění věty.

Věta. *Nechť $R \subseteq T$ je rozšíření těles. Označme A množinu všech prvků $t \in T$, které jsou algebraické nad R. Pak A je podtěleso tělesa T obsahující těleso R.*

Důkaz. Zřejmě $R \subseteq A$, neboť každý $r \in R$ je kořenem nenulového polynomu $x - r \in R[x]$. Musíme dokázat, že pro každé $\alpha, \beta \in A$ platí $-\alpha, \alpha + \beta, \alpha \cdot \beta \in A$, a pokud $\alpha \neq 0$, tak také $\alpha^{-1} \in A$. Protože α je algebraický nad R, platí $[R(\alpha) : R] < \infty$. Zřejmě $(R(\alpha))(\beta)$ je nejmenší podtěleso tělesa T obsahující $(R(\alpha)) \cup \{\beta\}$, a tedy nejmenší podtěleso tělesa T obsahující $R \cup \{\alpha, \beta\}$. Proto $(R(\alpha))(\beta) = R(\alpha, \beta)$. Protože β je algebraický nad R, je také algebraický nad $R(\alpha)$ a platí $[R(\alpha, \beta) : R(\alpha)] < \infty$. Dohromady $[R(\alpha, \beta) : R] = [R(\alpha, \beta) : R(\alpha)] \cdot [R(\alpha) : R] < \infty$. Protože každé konečné rozšíření těles je algebraické, platí, že $-\alpha, \alpha + \beta, \alpha \cdot \beta \in R(\alpha, \beta)$, a pokud $\alpha \neq 0$, tak také $\alpha^{-1} \in R(\alpha, \beta)$ jsou algebraické prvky nad R.

Příklad. Aplikujme předchozí větu na rozšíření $\mathbb{Q} \subseteq \mathbb{C}$. Pak A je těleso všech algebraických čísel. Proto je $\mathbb{Q} \subseteq A$ algebraické rozšíření. Není však konečné. Kdyby totiž $[A : \mathbb{Q}] = m \in \mathbb{N}$, pak bychom z $\sqrt[m+1]{2} \in A$ a $[\mathbb{Q}(\sqrt[m+1]{2}) : \mathbb{Q}] = m + 1$ dostali spor $m + 1 \mid m$. (Rovnost $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$ pro libovolné $n \in \mathbb{N}$ plyne z toho, že polynom $x^n - 2$ je ireducibilní nad $\mathbb{Q}$ podle Eisensteinova kriteria.)