Definice. *Nechť T je těleso. Libovolný podokruh R tělesa T takový, že R je těleso, nazýváme podtělesem tělesa T. Jinými slovy podokruh R tělesa T je podtělesem, jestliže $\forall a \in R, a \neq 0$ platí $a^{-1} \in R$. Říkáme též, že T je rozšířením tělesa R. Nebo také, že $R \subseteq T$ je rozšířením těles (v literatuře se hojně používá T/R je rozšířením těles).*

Věta. *Jsou-li R, T tělesa a $\varphi : R \to T$ homomorfismus okruhů, pak je φ injektivní.*

Důkaz. Nechť $\varphi : R \to T$ je homomorfismus okruhů, pak $\ker\varphi$ je ideál R a $1 \notin \ker\varphi$, vždyť $\varphi(1) = 1 \neq 0$, tj. $\ker\varphi \neq R$, proto $\ker\varphi$ je nulový ideál, jiné ideály už R nemá.

Věta. *Každé těleso charakteristiky $p \neq 0$ obsahuje podtěleso izomorfní s $\mathbb{Z}_p$.*
Každé těleso charakteristiky nula obsahuje podtěleso izomorfní s $\mathbb{Q}$.

Důkaz. Nechť R je těleso, char $R = 0$. Pak jediný homomorfismus okruhů $\varphi : \mathbb{Z} \to R$, určený předpisem $\varphi(m) = m1$ pro každé $m \in \mathbb{Z}$, je injektivní. Pak existuje homomorfismus okruhů $\mathbb{Q} \to R$ definovaný takto:

$$\begin{tikzcd}
\mathbb{Z} \arrow[rr, hook, "\varphi"] \arrow[dr, hook] & & R \ni \varphi(m)(\varphi(n))^{-1} \\
{\scriptstyle m,n\in\mathbb{Z},\ n\neq 0} & \mathbb{Q} \ni \frac{m}{n} \arrow[ur, hook] \arrow[ur, mapsto, shift right] &
\end{tikzcd}$$

Zřejmě předchozí diagram komutuje a podle předchozí věty je homomorfismus $\mathbb{Q} \to R$ injektivní.

Poznámka. Je-li R podtělesem tělesa T, pak můžeme aditivní grupu $(T, +)$ chápat jako vektorový prostor nad R (skalárním násobkem vektoru $t \in T$ skalárem $r \in R$ je součin $r \cdot t$ počítaný v tělese T, axiomy vektorového prostoru jsou splněny, protože v T platí distributivní zákony, násobení je asociativní a 1 je jednička). Pak máme definovánu dimenzi $\dim_R T \in \mathbb{N} \cup \{\infty\}$ (zřejmě tato dimenze nemůže být nula).

Definice. *Nechť $R \subseteq T$ je rozšířením těles. Stupněm $[T : R]$ tohoto rozšíření rozumíme dimenzi vektorového prostoru T nad tělesem R.*

Věta. *Nechť $R \subseteq S$, $S \subseteq T$ jsou rozšíření těles. Pak platí*

$$[T : R] = [T : S] \cdot [S : R],$$

kde užíváme konvence $n \cdot \infty = \infty \cdot n = \infty$ pro každé $n \in \mathbb{N} \cup \{\infty\}$.

Důkaz. Je-li $[S : R] = \infty$, pro každé $n \in \mathbb{N}$ v S existuje n lineárně nezávislých prvků nad R, protože $S \subseteq T$ jsou tyto prvky v T a platí $[T : R] = \infty$.

Je-li $[T : S] = \infty$, pro každé $n \in \mathbb{N}$ v T existuje n lineárně nezávislých prvků nad S. Ty jsou lineárně nezávislé i nad R, a proto $[T : R] = \infty$.

Nechť $n = [T : S]$, $m = [S : R] \in \mathbb{N}$. Nechť $\alpha_1, \ldots, \alpha_n$ je báze T nad S, $\beta_1, \ldots, \beta_m$ báze S nad R. Ukážeme, že $\alpha_i\beta_j$ $(1 \leq i \leq n, 1 \leq j \leq m)$ je bází T nad R. Nechť $\gamma \in T$ je libovolný. Pak existují $\delta_1, \ldots, \delta_n \in S$, že $\gamma = \sum_{i=1}^{n} \delta_i\alpha_i$. Existují tedy $\varepsilon_{ij} \in R$, že $\delta_i = \sum_{j=1}^{m} \varepsilon_{ij}\beta_j$ pro každé i. Dosazením

$$\gamma = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} \varepsilon_{ij}\beta_j \right) \alpha_i = \sum_{i=1}^{n} \sum_{j=1}^{m} \varepsilon_{ij}(\alpha_i\beta_j).$$

Tedy $\alpha_i\beta_j$ $(1 \leq i \leq n, 1 \leq j \leq m)$ je množina generátorů T nad R.

Je-li $\sum_{i=1}^{n} \sum_{j=1}^{m} \varepsilon_{ij}(\alpha_i\beta_j)$ pro nějaké $\varepsilon_{ij} \in R$ nulový vektor, pak z lineární nezávislosti $\alpha_1, \ldots, \alpha_n$ nad S dostaneme, že $\sum_{j=1}^{m} \varepsilon_{ij}\beta_j = 0$ pro každé $i = 1, \ldots, n$ a z lineární nezávislosti $\beta_1, \ldots, \beta_m$ nad R dostaneme, že $\varepsilon_{ij} = 0$ pro každé i, j. Tedy $\alpha_i\beta_j$ $(1 \leq i \leq n, 1 \leq j \leq m)$ je báze T nad R.

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