__def__: $f \in T[x]$ stupně ≥ 1

KOŘENOVÉ NADTĚLESO pro f nad T je libovolné $T(a)$ t.ž. $f(a) = 0$

ROZKLADOVÉ NADTĚLESO pro f nad T je libovolné $T(a_1, \dots, a_n)$ t.ž. $f \,\|\, (x-a_1) \cdots (x-a_n)$ v $T(a_1, \dots, a_n)[x]$

__def__: Buď $\underbrace{T}_{\text{těleso}} \leq \underbrace{U, V}_{\text{okruhy}}$, ~~[illegible]~~ pak $\varphi : U \to V$ se nazývá T-izomorfismus je-li to okruhový izomorfismus & $\varphi(t) = t \quad \forall t \in T$.

__Věta__: Buď $f \in T[x]$ stupně ≥ 1. Pak (1) je-li f ireducibilní, pak jsou každá dvě kořenová nadtělesa pro f nad T T-izomorfní

(2) každá dvě rozkladová nadt. pro f nad T jsou T-izom

__Lemma 1__: $T \leq U, V$ tělesa, $\varphi : U \to V$ T-izomorfismus, $f \in U[x]$ ireducibilní polynom.
Buď $U(a)$ kořenové pro f nad U, buď $V(b)$ kořenové pro $\varphi(f)$ nad V.
Pak $\exists \psi : U(a) \to V(b)$ T-izomorfismus t.ž. $\psi(a) = b$ & $\psi \restriction U = \varphi$.

__Lemma 2__: $T \leq U, V$ tělesa, $\varphi : U \to V$ T-izomorfismus, $f \in U[x]$ ~~[illegible]~~ stupně ≥ 1.
Buď $\bar{U}$ rozkladové pro f nad U, buď $\bar{V}$ rozkladové pro $\varphi(f)$ nad V.
Pak $\exists \psi : \bar{U} \to \bar{V}$ T-izomorfismus t.ž. $\psi \restriction U = \varphi$.

Lemma 1: Rozkladové nadtěleso polynomu $x^{p^k}-x$ nad $\mathbb{Z}_p$ má p^k prvků.

Lemma 2: T těleso, $|T| = p^k \Rightarrow T$ je rozkladové pro $x^{p^k}-x$ nad $\mathbb{Z}_p$

a v $T[x]$ platí $x^{p^k}-x = \prod_{a\in T}(x-a)$

Věta (klasifikace konečných těles):

(1) Konečné těleso velikosti n existuje $\Leftrightarrow n = p^k$ (p prvoč.).

(2) Konečná tělesa stejné velikosti jsou izomorfní.

Věta (reprezentace konečných těles):

Pro každé p prvočíslo, $k\in\mathbb{N}$ existuje $m\in\mathbb{Z}_p[\alpha]$ ireducibilní stupně k

& $\mathbb{F}_{p^k} \simeq \mathbb{Z}_p[\alpha]/(m)$.