Buď T těleso a $f \in T[x]$ stupně ≥ 1.

def.: Kořenové nadtěleso polynomu f nad T je libovolné těleso $T(a)$ t.ž. a je kořen f.

Rozkladové nadtěleso polynomu f nad T je libovolné těleso $T(a_1, \dots, a_n)$ t.ž. $f \parallel (x-a_1)\cdots(x-a_n)$ v $T(a_1,\dots,a_n)[x]$

def.: Buď $T \leq U, V$. Řekneme, že $\varphi: U \to V$ je T-izomorfismus, je-li to okruhový izomorfismus t.ž. $\varphi(t) = t$ $\forall t \in T$.

je to taky lineární zobrazení $U_T \to V_T$

Věta: (1) Každá dvě rozkladová nadtělesa polynomu f nad T jsou T-izomorfní.

(2) Je-li f ireducibilní, pak každá dvě kořenová nadtělesa polynomu f nad T jsou T-izomorfní.

Created by Notein

Def.: Kořenové nadtěleso polynomu f nad T je libovolné těleso $T(a)$ t.ž. a je kořen f.

Rozkladové nadtěleso polynomu f nad T je libovolné těleso $T(a_1,\dots,a_n)$ t.ž. $f \parallel (x-a_1)\cdots(x-a_n)$ v $T(a_1,\dots,a_n)[x]$

Věta: (1) Každá dvě rozkladová nadtělesa polynomu f nad T jsou T-izomorfní.

(2) Je-li f ireducibilní, pak
každá dvě kořenová nadtělesa polynomu f nad T jsou T-izomorfní.

Buď $T \leq U, V$, $\varphi: U \to V$ T-izomorfismus.

Definujeme $\tilde{\varphi}: U[x] \to V[x]$
$\sum u_i x^i \mapsto \sum \varphi(u_i) x^i$

- je to okruhový izomorfismus
- $f \mid g$ v $U[x] \iff \tilde{\varphi}(f) \mid \tilde{\varphi}(g)$ v $V[x]$
- f je ired. v $U[x] \iff \tilde{\varphi}(f)$ je ired. v $V[x]$

Lemma: Buď $f \in U[x]$ ireducibilní. Buď $U(a)$ kořenové nadtěleso pro f nad U,
$V(b)$ kořenové nadtěleso pro $\tilde{\varphi}(f)$ nad V.

Pak $\exists \psi: U(a) \to V(b)$ T-izomorfismus t.ž. $\psi(a) = b$ & $\psi|_U = \varphi$.

Lemma: Buď $f \in U[x]$ (lib.) stupně ≥ 1. Buď $\bar{U}$ rozkladové nadtěleso pro f nad U,
$\bar{V}$ rozkladové nadtěleso pro $\tilde{\varphi}(f)$ nad V.

Pak $\exists \psi: \bar{U} \to \bar{V}$ T-izomorfismus t.ž. $\psi|_U = \varphi$.

Created by Notein

Buď $T \subseteq U, V$, $\varphi: U \to V$ T-izomorfismus.

Definujeme $\tilde{\varphi}: U[x] \to V[x]$
$\sum u_i x^i \mapsto \sum \varphi(u_i) x^i$

$f \mid g$ v $U[x] \iff \tilde{\varphi}(f) \mid \tilde{\varphi}(g)$ v $V[x]$

f je ired. v $U[x] \iff \tilde{\varphi}(f)$ je ired. v $V[x]$

Lemma: Buď $f \in U[x]$ ireducibilní. Buď $U(a)$ rozšíření nadtělesa pro f nad U,
$V(b)$ rozšíření nadtělesa pro $\tilde{\varphi}(f)$ nad V.

Pak $\exists \psi: U(a) \to V(b)$ T-izomorfismus t.ž. $\psi(a) = b$ & $\psi|_U = \varphi$.

Lemma: Buď $f \in U[x]$ (lib.) stupně ≥ 1. Buď $\bar{U}$ rozkladové nadtělesa pro f nad U,
$\bar{V}$ rozkladové nadtělesa pro $\tilde{\varphi}(f)$ nad V.

Pak $\exists \psi: \bar{U} \to \bar{V}$ T-izomorfismus t.ž. $\psi|_U = \varphi$.

Created by Notein

Věta (KLASIFIKACE KONEČNÝCH TĚLES):

(1) Konečné těleso velikosti n existuje $\Leftrightarrow$ n je mocnina prvočísla.

(2) Jsou-li T_1, T_2 konečná tělesa t.ž. $|T_1| = |T_2|$, pak $T_1 \simeq T_2$.

Věta (REPREZENTACE KONEČNÝCH TĚLES):

Je-li $|T| = p^k$, pak $\exists f \in \mathbb{Z}_p[x]$ ireducibilní stupně k t.ž.

$$T \simeq \mathbb{Z}_p[\alpha] / (f(\alpha))$$

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

Lemma 2: Je-li $|T| = p^k$, pak T je rozkladové nadtěleso polynomu $x^{p^k} - x$ nad svým prvotělesem.

Navíc, v $T[x]$ platí

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

Created by Notein

Věta (KLASIFIKACE KONEČNÝCH TĚLES):

(1) Konečné těleso velikosti n existuje $\Leftrightarrow$ n je mocnina prvočísla.

(2) Jsou-li T_1, T_2 konečná tělesa t.ž. $|T_1| = |T_2|$, pak $T_1 \simeq T_2$.

Věta (REPREZENTACE KONEČNÝCH TĚLES):

Je-li $|T| = p^k$, pak $\exists f \in \mathbb{Z}_p[x]$ ireducibilní stupně k t.ž.

$$T \simeq \mathbb{Z}_p[\alpha] / (f(\alpha))$$

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

Lemma 2: Je-li $|T| = p^k$, pak T je rozkladové nadtěleso polynomu $x^{p^k} - x$ nad svým prvotělesem.

Navíc, v $T[x]$ platí

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

Created by Notein

Created by Notein