Věta 2.6. *Nechť* $\mathbf{F}$ *je konečné těleso s* q *prvky a* $\mathbf{K}$ *je jeho podtěleso. Potom pro polynom* $x^q - x \in \mathbf{K}[x]$ *platí v* $\mathbf{F}[x]$

$$x^q - x = \prod_{a \in \mathbf{F}} (x - a)$$

Důkaz. Podle Lemma 2.5 platí pro každý prvek $a \in \mathbf{F}$, že $a^q = a$, tedy $a^q - a = 0$. Z toho plyne, že každý prvek $a \in \mathbf{F}$ je kořenem polynomu $x^q - x$, proto platí $(x-a)|(x^q - x)$. Protože polynomy $x - a$ jsou pro různá $a \in \mathbf{F}$ po dvou nesoudělné, platí taky $\prod_{a \in \mathbf{F}}(x - a)|(x^q - x)$.

Zbývá ještě dokázat rovnost polynomů. Oba polynomy mají stupeň q (protože $\mathbf{F}$ má q prvků) a vedoucí člen obou polynomů je x^q. Protože $\prod_{a \in \mathbf{F}}(x-a)|(x^q - x)$, oba polynomy se rovnají. □

Před následující definicí si ještě zavedeme nové označení. Je-li $\mathbf{E}$ rozšíření tělesa $\mathbf{K}$ a $\theta \in \mathbf{E}$, pak nejmenší podtěleso tělesa $\mathbf{E}$ obsahující (tj. průnik všech podtěles tělesa $\mathbf{E}$ obsahujících) podtěleso $\mathbf{K}$ a prvek θ budeme označovat $\mathbf{K}(\theta)$. Druhou podmínku z definice kořenového rozšíření tělesa $\mathbf{K}$ určeného ireducibilním polynomem $p(x) \in \mathbf{K}[x]$ (že libovolné podtěleso $\mathbf{E}$ obsahující $\mathbf{K}$ a θ se rovná $\mathbf{E}$) pak můžeme zapsat stručně jako $\mathbf{K}(\theta) = \mathbf{E}$. Podobně označíme $\mathbf{K}(\theta_1, \theta_2, \ldots, \theta_m)$ nejmenší podtěleso tělesa $\mathbf{E}$ obsahující $\mathbf{K}$ a prvky $\theta_1, \theta_2, \ldots, \theta_m \in \mathbf{E}$.

Definice. Nechť $\mathbf{K}$ je těleso, $f(x) \in \mathbf{K}[x]$. Pak rozšíření $\mathbf{E}$ tělesa $\mathbf{K}$ nazýváme *rozkladové rozšíření* tělesa $\mathbf{K}$ určené polynomem $f(x)$, pokud se polynom $f(x)$ rozkládá v $\mathbf{E}[x]$ na součin lineárních polynomů a současně těleso $\mathbf{E}$ je nejmenší podtěleso $\mathbf{E}$ (vzhledem k inkluzi) obsahující $\mathbf{K}$, nad kterým se $f(x)$ rozkládá na součin lineárních činitelů. Jinak řečeno, pokud jsou $\theta_1, \theta_2, \ldots, \theta_m \in \mathbf{E}$ všechny kořeny polynomu $f(x)$, pak $\mathbf{K}(\theta_1, \theta_2, \ldots, \theta_m) = \mathbf{E}$.

Je-li $T : \mathbf{E} \to \mathbf{F}$ izomorfizmus těles $\mathbf{E}$ a $\mathbf{F}$, pak jej můžeme přirozeně rozšířit do izomorfizmu $T : \mathbf{E}[x] \to \mathbf{F}[x]$ oborů integrity polynomů jedné proměnné nad oběma tělesy pomocí předpisu

$$T(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0) = T(a_n)x^n + T(a_{n-1})x^{n-1} + \cdots + T(a_1)x + T(a_0).$$

Je samozřejmě třeba ověřit, že takto definované zobrazení $T : \mathbf{E}[x] \to \mathbf{F}[x]$ je skutečně izomorfizmus. Speciálně, polynom $p(x) \in \mathbf{E}[x]$ je izomorfní nad $\mathbf{E}$, právě když je polynom $T(p(x))$ izomorfní nad $\mathbf{F}$.

Věta 2.7 (O existenci a jednoznačnosti rozkladového rozšíření)**.** *Pro každé těleso* $\mathbf{K}$ *a každý polynom* $f(x) \in \mathbf{K}[x]$ *stupně aspoň* 1 *existuje rozkladové rozšíření tělesa* $\mathbf{K}$ *určená polynomem* $f(x)$*.*

Každá dvě rozkladová rozšíření tělesa $\mathbf{K}$ *určená polynomem* $f(x)$ *jsou* $\mathbf{K}$*-izomorfní.*

Důkaz. (1) Nejprve dokážeme existenci. Nechť $\deg f = n$ a $f(x) = p_1 \cdot p_2 \cdots p_k$ je rozklad polynomu $f(x)$ na součin polynomů ireducibilních v $\mathbf{K}[x]$. Budeme postupovat indukcí podle $n-k$. Je-li $n-k = 0$, jsou všechny polynomy $p_1, p_2, \ldots, p_n$ lineární a těleso $\mathbf{K}$ je rozkladové rozšíření $\mathbf{K}$ určené polynomem $f(x)$.

Nechť $n - k > 0$. Pak aspoň jeden z činitelů $p_i(x)$ má stupeň aspoň 2. Nechť to je $p_1(x)$. Označme $\mathbf{G}$ kořenové rozšíření tělesa $\mathbf{K}$ určené polynomem $p_1(x)$. V $\mathbf{G}[x]$ se $p_1(x)$ rozkládá na součin aspoň dvou ireducibilních polynomů. Vezměme rozklad $f(x) = q_1 \cdot q_2 \cdots g_l$ na součin ireducibilních polynomů v $\mathbf{G}[x]$. Platí $l > k$, tedy $n - l < n - k$.

Nyní zformulujeme indukční předpoklad: pro každé rozšíření $\mathbf{G}$ tělesa $\mathbf{K}$ takové, že $f(x) = q_1 \cdot q_2 \cdots q_l$ v $\mathbf{G}[x]$ a $n - l < n - k$, existuje rozkladové rozšíření $\mathbf{E}$ tělesa $\mathbf{G}$ určené $f(x)$.

Tedy podle indukčního předpokladu existuje rozkladové rozšíření $\mathbf{E}$ tělesa $\mathbf{G}$ určené polynomem $f(x)$. Těleso $\mathbf{E}$ je tedy rozšířením tělesa $\mathbf{K}$, nad kterýmm se polynom $f(x)$ rozkládá na součin lineárních činitelů. Nyní ještě musíme ověřit podmínku minimality, aby to bylo také rozkladové rozšíření tělesa $\mathbf{K}$ určené polynomem $f(x)$. Nad tělesem $\mathbf{E}$ se polynom $f(x)$ rozkládá na součin lineárních činitelů $f(x) = a(x-\theta_1)\cdots(x-\theta_k)$. Označme $\mathbf{F}$ nejmenší podtěleso tělesa $\mathbf{E}$ obsahující $\mathbf{K}$ a $\theta_1, \ldots, \theta_k$, tj. $\mathbf{F} = \mathbf{K}(\theta_1, \ldots, \theta_k)$. Pak $\mathbf{F}$ splňuje oba požadavky na rozkladové rozšíření $\mathbf{K}$ určené polynomem $f(x)$.

(2) Zbývá dokázat jednoznačnost. Ve skutečnosti dokážeme silnější tvrzení v podobě:

Jsou-li $\mathbf{G}$ a $\mathbf{H}$ rozšíření téhož tělesa $\mathbf{K}$, zobrazení $T : \mathbf{G} \to \mathbf{H}$ je $\mathbf{K}$-izomorfizmus a $f(x) \in \mathbf{G}[x]$, pak jsou $\mathbf{K}$-izomorfní také rozkladové rozšíření $\mathbf{G}$ určené polynomem $f(x)$ a rozkladové rozšíření $\mathbf{H}$ určené polynomem $T(f(x))$.

Také v tomto případě budeme předpokládat, že $\deg f = n$ a že $f = p_1 \cdot p_2 \cdots p_k$ je rozklad polynomu $f(x)$ na součin polynomů ireducibilních v $\mathbf{G}[x]$ a budeme postupovat indukcí podle $n-k$. Protože rozšířené zobrazení $T : \mathbf{G}[x] \to \mathbf{H}[x]$ je izomorfizmus, je také $T(f) = T(p_1)T(p_2)\cdots T(p_k)$ rozklad na součin polynomů ireducibilních v $\mathbf{H}[x]$. Označme $\mathbf{E}$ rozkladové rozšíření $\mathbf{G}$ určené polynomem $f(x)$ a $\mathbf{F}$ rozkladové rozšíření $\mathbf{H}$ určené polynomem $T(f(x))$.

Je-li $n - k = 0$, pak je $\mathbf{E} = \mathbf{G}$, $\mathbf{F} = \mathbf{H}$ a $T : \mathbf{G} \to \mathbf{H}$ je $\mathbf{K}$-izomorfizmus.

Nechť $n - k > 0$. Nechť $\deg p_1 > 1$. Potom polynom $p_1(x)$ má v $\mathbf{E}$ nějaký kořen α a v $\mathbf{F}$ má nějaký kořen β. Pak $\mathbf{E}(\alpha)$ je kořenové rozšíření tělesa $\mathbf{G}$ určené polynomem $p_1(x)$ a $\mathbf{F}(\beta)$ je kořenové rozšíření tělesa $\mathbf{H}$ určené polynomem $T(p_1)$. Podle věty o existenci a jednoznačnosti kořenového rozšíření existuje $\mathbf{K}$-izomorfizmus $U : \mathbf{G}[\alpha] \to \mathbf{H}[\beta]$. Větu o existenci a jednoznačnosti kořenového rozšíření jsme sice nedokázali v té obecnosti, v jaké jsme ji právě použili, ale původní formulaci a důkaz lze snadno zobecnit do potřebného tvaru.

Je-li $f = q_1 q_2 \cdots q_l$ rozklad na polynomy ireducibilní nad $\mathbf{G}[x]$, pak platí $l > k$ a tedy $n - l < n - k$.

Nyní zformulujeme indukční předpoklad. Pro libovolná dvě $\mathbf{K}$-izomorfní rozšíření $\mathbf{E}', \mathbf{F}'$ tělesa $\mathbf{K}$, izomorfizmus $\mathbf{T} : \mathbf{E}' \to \mathbf{F}'$ a libovolný polynom $f(x) \in \mathbf{E}'[x]$, který se nad $\mathbf{E}'$ rozkládá na více ireducibilních polynomů než nad $\mathbf{E}$, jsou rozkladová rozšíření $\mathbf{F}'$ určené f a $\mathbf{G}'$ určené $\mathbf{T}(f)$ $\mathbf{K}$-izomorfní.

Podle indukčního předpokladu použitého na tělesa $\mathbf{E}' = \mathbf{G}(\alpha)$, a $\mathbf{F}' = \mathbf{H}(\beta)$, na izomorfizmus $U : \mathbf{E}' \to \mathbf{F}'$ a na polynom $f(x)$ tedy existuje $\mathbf{K}$-izomorfismus $\mathbf{F}$ a $\mathbf{G}$.

□

Věta 2.8 (O existenci a jednoznačnosti konečných těles)**.** *Pro každé prvočíslo p a celé číslo $n > 0$ existuje těleso s $q = p^n$ prvky.*

Libovolná dvě tělesa s p^n prvky jsou izomorfní (a jsou izomorfní rozkladovému rozšíření tělesa $\mathbb{Z}_p$ určeného polynomem $x^q - x \in \mathbb{Z}_p[x]$).

Důkaz. Nejprve dokážeme existenci takového tělesa. Buď $\mathbf{F}$ rozkladové rozšíření $\mathbb{Z}_p$ určené polynomem $x^q - x \in \mathbb{Z}_p[x]$. Polynom $f(x) := x^q - x$ nemá v $\mathbf{F}$ vícenásobný kořen, protože $(x^q - x)' = q.x^{q-1} - 1 = -1$, tedy $\mathrm{NSD}(f, f') = 1$ a proto f nemůže mít v $\mathbf{F}$ vícenásobný kořen. Tedy $x^q - x$ má v $\mathbf{F}$ přesně $q = p^n$ kořenů. Označme $\mathbf{G} = \{a \in \mathbf{F} : a^q - a = 0\}$. Ukážeme, že $\mathbf{G}$ je podtěleso $\mathbf{F}$. Platí $0, 1 \in \mathbf{G}$ a pro všechny $a, b \in \mathbf{G}$ platí $(a.b)^q = a^q.b^q = a.b$ a $(a + b)^{p^k} = a^{p^k} + b^{p^k} = a + b$. Tedy $\mathbf{G}$ je podtěleso $\mathbf{F}$, které obsahuje $\mathbb{Z}_p$ a nad kterým se $x^q - x$ rozkládá na součin lineárních činitelů. Protože $\mathbf{F}$ je rozkladové rozšíření tělesa $\mathbb{Z}_p$ určené polynomem $x^q - x$, platí $\mathbf{F} = \mathbf{G}$ a $\mathbf{F}$ má tedy q prvků.

Zbývá dokázat jednoznačnost. Nechť $\mathbf{E}$ je těleso s $q = p^n$ prvky. Pak podle Věty 2.6 platí $x^q - x = \prod_{a \in \mathbf{F}}(x - a)$. Tedy $\mathbf{E}$ je rozkladové rozšíření $\mathbb{Z}_p$ určené polynomem $x^q - x \in \mathbb{Z}_p$. Podle Věty 2.7 jsou libovolná dvě rozkladová rozšíření tělesa $\mathbb{Z}_p$ určená polynomem $x^q - x$ izomorfní. □