Věta 3.3. *Nechť f je ireducibilní polynom nad $\mathbf{F}_q$ stupně m. Potom f má v $\mathbf{F}_{q^m}$ nějaký kořen α, prvky $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ jsou navzájem různé a tvoří množinu všech kořenů polynomu f.*

Důkaz. Kořenové rozšíření $\mathbf{F}_q$ určené polynomem f má q^m prvků a tedy se rovná $\mathbf{F}_{q^m}$. Je-li $\beta \in \mathbf{F}_{q^m}$ a $f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0$, pak $f(\beta)^q = (a_m x^m + \ldots + a_1 x + a_0)^q = a_m^q (\beta^m)^q + a_{m-1}^q (\beta^{m-1})^q + \ldots + a_1^q \beta^q + a_0^q = a_m (\beta^q)^m + a_{m-1}(\beta^q)^{m-1} + \ldots + a_1 \beta^q + a_0 = f(\beta^q)$. Je-li tedy $\alpha \in \mathbf{F}_{q^m}$ kořen polynomu $f(x)$, pak taky $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ jsou kořeny polynomu $f(x)$.

Zbývá ještě dokázat, že jsou navzájem různé. Nechť $\alpha^{q^i} = \alpha^{q^j}$ pro nějaké $0 \leq i < j \leq m-1$. Umocněním na q^{m-j} dostáváme $(\alpha^{q^i})^{q^{m-j}} = (\alpha^{q^j})^{q^{m-j}}$, tedy $\alpha^{q^{m-j+i}} = \alpha^{q^m} = \alpha$. Tedy α je kořenem polynomu $\alpha^{q^{m-j+i}} - \alpha$ a podle Lemma 3.2 platí $m | m-j+i$. Ovšem $m - j + i < m$, což je spor. □

Důsledek 3.4. *$\mathbf{F}_{q^m}$ je rozkladové rozšíření $\mathbf{F}_q$ určené libovolným ireducibilním polynomem $f \in \mathbf{F}_q[x]$.*

Důkaz. Polynom f se v $\mathbf{F}_{q^m}$ rozkládá na součin lineárních činitelů a tedy $\mathbf{F}_{q^m}$ obsahuje rozkladové rozšíření $\mathbf{F}_q$ určené polynomem f.

Naopak rozkladové rozšíření $\mathbf{F}_q$ určené polynomem f musí obsahovat kořenové rozšíření $\mathbf{F}_q$ určené polynomem f, které se rovná $\mathbf{F}_{q^m}$. Rozkladové rozšíření $\mathbf{F}_q$ určené polynomem f dostaneme jako $\mathbf{F}_q(\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}) = \mathbf{F}_q(\alpha) = \mathbf{F}_{q^m}$. □

Důsledek 3.5. *Rozkladová rozšíření $\mathbf{F}_q$ určená dvěma ireducibilními polynomy téhož stupně jsou izomorfní.*

Důkaz. Obě jsou izomorfní s $\mathbf{F}_{q^m}$. □

Definice. Jsou-li $\mathbf{F}_{q^m} \supseteq \mathbf{F}_q$ konečná tělesa a $\alpha \in \mathbf{F}_{q^m}$, pak prvky $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ se nazývají *konjugované* k α nad $\mathbf{F}_q$.

Je-li $\mathbf{F}_q$ prvotěleso tělesa $\mathbf{F}_{q^m}$, pak prvky $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ se nazývají *absolutně konjugované* k α nad $\mathbf{F}_q$.

Poznámka. Je-li $\alpha \in \mathbf{F}_{q^m}$, platí $\alpha^{q^m} - \alpha = 0$. Pak pro minimální polynom $f(x)$ prvku α nad $\mathbf{F}_q$ platí $f(x) | x^{q^m} - x$, tedy pro $\deg f = d$ platí $d | m$.

Pokud $d = m$, jsou prvky $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ navzájem různé. Je-li d je vlastní dělitel m, potom $\underbrace{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}}_{\text{navzájem různé}}, \alpha^{q^d} = \alpha, \alpha^{q^{d+1}} = \alpha^q, \ldots, \alpha^{q^{m-1}} = \alpha^{q^{d-1}}$,

tedy každý z navzájem různých prvků $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}$ se opakuje přesně $\frac{m}{d}$-krát.

Věta 3.6. *Prvky konjugované k $\alpha \in \mathbf{F}_{q^m}$ nad $\mathbf{F}_q$ mají stejný řád v multiplikativní grupě $\mathbf{F}_{q^m}$ tj. v grupě $\mathbf{F}_{q^m}^*$.*

Důkaz. Víme, že je-li $\mathbf{G}$ cyklická grupa řádu n a $a \in \mathbf{G}$ je její generátor, potom řád prvku a^k se rovná $\frac{n}{\mathrm{NSD}(n,k)}$. Grupa $\mathbf{F}_{q^m}^*$ je cyklická grupa řádu $q^m - 1$. Prvek α je generátor nějaké cyklické podgrupy $\mathbf{G}$ grupy $\mathbf{F}_{q^m}^*$ řádu $n | q^m - 1$. Tedy řád α^q se rovná $\frac{n}{\mathrm{NSD}(q,n)}$. Protože $\mathrm{NSD}(q, q^m - 1) = 1$ a $n | q^m - 1$, platí také $\mathrm{NSD}(q, n) = 1$. Řád α^q se proto rovná n. □

Důsledek 3.7. *Je-li $\alpha \in \mathbf{F}_{q^m}$ primitivní prvek $\mathbf{F}_{q^m}$, pak všechny prvky konjugované k α nad $\mathbf{F}_q$ jsou také primitivní prvky v $\mathbf{F}_{q^m}$ (tedy je-li $\alpha \in \mathbf{F}$ primitivní prvek $\mathbf{F}$, pak všechny prvky konjugované k α nad libovolným podtělesem $\mathbf{K} \subseteq \mathbf{F}$ jsou také primitivní prvky v $\mathbf{F}$).*

Příklad. Uvažujme těleso $\mathbf{F}_{16}$ a polynom $f(x) = x^4 + x + 1 \in \mathbf{F}_2[x]$. Vezměme kořen $\alpha \in \mathbf{F}_{16}$ polynomu $f(x)$. Pak prvky konjugované nad $\mathbf{F}_2$ jsou $\alpha, \alpha^2, \alpha^4 = \alpha + 1, \alpha^8 = (\alpha + 1)^2 = \alpha^2 + 1$. Prvky konjugované nad $\mathbf{F}_4$ jsou $\alpha, \alpha^4 = \alpha + 1$.

Definice. Automorfismus σ tělesa $\mathbf{F}_{q^m}$ se nazývá *automorfismus nad* $\mathbf{F}_q$, pokud platí $\sigma(\alpha) = \alpha$ pro libovolné $\alpha \in \mathbf{F}_q$.

Poznámka. Každý automorfismus $\mathbf{F}$ je automorfismus nad prvotělesem $\mathbf{F}$.

Věta 3.8. *Nechť $\mathbf{F}_{q^m}$ a $\mathbf{F}_q$ jsou tělesa, pak zobrazení σ_i pro $i = 0, 1, 2, \ldots, m-1$ definovaná předpisem $\sigma_i(\alpha) = \alpha^{q^i}$ pro $\alpha \in \mathbf{F}_{q^m}$ jsou navzájem různá a tvoří všechny automorfismy $\mathbf{F}_{q^m}$ nad $\mathbf{F}_q$.*

Důkaz. Pri libovolné $i = 0, 1, 2, \ldots, m-1$ platí $\sigma_i(\alpha\beta) = (\alpha\beta)^{q^i} = \alpha^{q^i}\beta^{q^i} = \sigma_i(\alpha)\sigma_i(\beta)$ a $\sigma_i(\alpha + \beta) = (\alpha + \beta)^{q^i} = \alpha^{q^i} + \beta^{q^i} = \sigma_i(\alpha) + \sigma_i(\beta)$. Dále $\sigma_i(\alpha) = 0$ právě tehdy, když $\alpha = 0$. Tedy σ_i je automorfismus $\mathbf{F}_{q^m}$. Je-li $\alpha \in \mathbf{F}_q$, potom $\sigma_i(\alpha) = \alpha^{q^i} = \alpha$. Tedy σ_i je automorfismus nad $\mathbf{F}_q$.

Nechť σ je libovolný automorfismus $\mathbf{F}_{q^m}$ nad $\mathbf{F}_q$, $\beta \in \mathbf{F}_{q^m}$ primitivní prvek tělesa $\mathbf{F}_{q^m}$ a $f(x)$ je minimální polynom β nad $\mathbf{F}_q$. POlynom $f(x)$ musí mít stupeň m. Označme $f(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_1x + a_0$. Platí $0 = \beta^m + a_{m-1}\beta^{m-1} + \ldots + a_1\beta + a_0$ a tedy také $0 = \sigma(0) = \sigma(\beta^m + a_{m-1}\beta^{m-1} + \ldots + a_1\beta + a_0) = \sigma(\beta^m) + \sigma(a_{m-1})\sigma(\beta^{m-1}) + \ldots + \sigma(a_1)\sigma(\beta) + \sigma(a_0) = \sigma(\beta^m) + a_{m-1}\sigma(\beta^{m-1}) + \ldots + a_1\sigma(\beta) + a_0 = f(\sigma(\beta))$. Platí $\sigma(\beta) = \beta^{q^i}$ pro nějaké $i = 0, 1, \ldots, m-1$. Pak $\sigma(\beta^k) = (\beta^k)^{q^i}$ pro libovolné $k = 1, \ldots, q^m - 1$, neboli $\sigma(\alpha) = \alpha^{q^i} = \sigma_i(\alpha)$ pro každé $0 \neq \alpha \in \mathbf{F}_{q^m}$ a rovněž pro $\alpha = 0$. □

Všimněte si, že platí:

$$\sigma = \sigma_1$$
$$\sigma \circ \sigma(\alpha) = \sigma(\alpha^q) = \alpha^{q^2} = \sigma_2$$
$$\sigma \circ \sigma \circ \sigma(\alpha) = \sigma_3$$

Důsledek 3.9. *Grupa automorfismů $\mathbf{F}_{q^m}$ nad $\mathbf{F}_q$ je cyklická grupa řádu m. Grupa automorfismů $\mathbf{F}_{p^k}$ je cyklická grupa řádu k.*