

Věta 2.9 (O podtělesech konečných těles). *Nechť $\mathbf{F}_q$ je konečné těleso, $q = p^n$. Pak každé podtěleso tělesa $\mathbf{F}_q$ má p^m prvků pro nějaké m , které dělí n .*

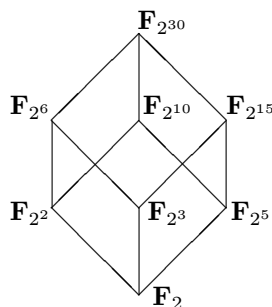
Pro každé $m|n$ existuje právě jedno podtěleso tělesa $\mathbf{F}_q$, které má p^m prvků.

Důkaz. Nejprve dokážeme první část věty. Je-li $\mathbf{G}$ podtěleso $\mathbf{F}_{p^n}$, má také charakteristiku p a tedy p^m prvků pro nějaké $m \leq n$. Navíc p^n musí být podle Lemma 2.1 mocninou p^m , čili $m|n$.

Zbývá dokázat druhou část věty. Těleso $\mathbf{F}_{p^n}$ je rozkladové rozšíření $\mathbf{F}_p$ určené polynomem $x^{p^n} - x \in \mathbf{F}_p[x]$. Ukážeme napřed, že z předpokladu $m|n$ plyne, že $(x^{p^m} - x)|(x^{p^n} - x)$, neboli $(x^{p^m-1} - 1)|(x^{p^n-1} - 1)$. Platí $(p^m - 1)|(p^n - 1)$, neboť z $n = k \cdot m$ plyne $(p^{km} - 1) = (p^m - 1)(p^{(k-1)m} + p^{(k-2)m} + \dots + p^m + 1)$. Pokud $a = b \cdot c$, pak $(x^{bc} - 1) = (x^b - 1)(x^{(c-1)b} + x^{(c-2)b} + \dots + x^b + 1)$. Tedy $(x^{p^m-1} - 1)|(x^{p^n-1} - 1)$ a tedy $(x^{p^m} - x)|(x^{p^n} - x)$. Každý kořen polynomu $x^{p^m} - x$ je proto také kořenem polynomu $x^{p^n} - x$ a leží tedy v $\mathbf{F}_{p^n}$. Tedy $x^{p^m} - x$ se nad $\mathbf{F}_{p^n}$ rozkládá na součin lineárních činitelů, proto $\mathbf{F}_{p^n}$ obsahuje rozkladové rozšíření $\mathbf{F}_p$ určené polynomem $x^{p^m} - x$, t.j. $\mathbf{F}_{p^m}$. Dvě různá podtělesa mohutnosti p^m by obsahovala dohromady více než p^m kořenů polynomu $x^{p^m} - x$, což nelze. $\square$

Příklad. Podtělesa $\mathbf{F}_{2^{30}}$ jsou $\mathbf{F}_2, \mathbf{F}_{2^2}, \mathbf{F}_{2^3}, \mathbf{F}_{2^5}, \mathbf{F}_{2^6}, \mathbf{F}_{2^{10}}, \mathbf{F}_{2^{15}}, \mathbf{F}_{2^{30}}$.

Pomocí Haaseova diagramu můžeme znázornit, jak jsou obsažena jedno v druhém.



Věta 2.10. *Multiplikativní grupa $\mathbf{F}_q^*$ konečného tělesa $\mathbf{F}_q$ je cyklická.*

Důkaz. Položme $h = q - 1 = p_1^{r_1} \cdot p_2^{r_2} \cdot \dots \cdot p_k^{r_k}$. Polynom $x^{h/p_i} - 1$ má v $\mathbf{F}_q$ nejvýše $\frac{h}{p_i} < h$ nenulových kořenů, proto existuje $0 \neq a_i \in \mathbf{F}_q$ (neboli $a_i \in \mathbf{F}_q^*$) takové, že $a_i^{h/p_i} \neq 1$. Položme $b_i = a_i^{h/p_i^{r_i}} \neq 1$. Spočteme řád b_i . Platí $b_i^{p_i^{r_i}} = a_i^h = 1$ (neboť řád a_i dělí počet prvků $\mathbf{F}_q^*$, t.j. $h = q - 1$). Protože $b_i^{p_i^{r_i-1}} = a_i^{h/p_i} \neq 1$, je řád b_i rovný $p_i^{r_i}$. Položme $b = b_1 b_2 \dots b_k$. Platí $b^h = 1$. Dále pro $i = 1, 2, \dots, k$ platí $b^{h/p_i} = \prod_{j=1}^k b_j^{h/p_i}$. Je-li $j \neq i$, tak $p_j^{r_j}$ dělí $\frac{h}{p_i}$ a tedy $b_j^{h/p_i} = 1$. Proto $b^{h/p_i} = b_i^{h/p_i} \neq 1$, neboť $p_i^{r_i} \nmid \frac{h}{p_i}$ a $p_i^{r_i}$ je řád b_i . Takže řád b je rovný h . $\square$

Definice. Libovolný generátor $\mathbf{F}_q^*$ se nazývá *primitivní prvek* $\mathbf{F}_q$.

Příklad. Kolik primitivních prvků má těleso $\mathbf{F}_q$? Tolik, kolik je čísel menších než $q - 1$ nesoudělných s $q - 1$, t.j. $\varphi(q - 1)$, kde φ je Eulerova funkce.

Připomeňme si, že jsou-li $\mathbf{F} \subseteq \mathbf{E}$ dvě tělesa a $\alpha \in \mathbf{E}$ je algebraický nad $\mathbf{F}$, pak monický polynom g z $\mathbf{F}[x]$ nejmenšího stupně, jehož kořenem je α , nazýváme *minimální polynom* prvku α . Pro polynom $f \in \mathbf{F}[x]$ platí, že $f(\alpha) = 0$ právě tehdy, když $q|f$.

Věta 2.11. *Nechť $\mathbf{F}_q \subseteq \mathbf{F}_r$ jsou konečné tělesa a α je primitivní prvek $\mathbf{F}_r$. Potom $\mathbf{F}_r = \mathbf{F}_q(\alpha)$.*

Důkaz. Jelikož $\mathbf{F}_q(\alpha)$ musí obsahovat 0 a všechny mocniny α , obsahuje taky všechny nenulové prvky $\mathbf{F}_r$. $\square$

Věta 2.12. *Nechť $\mathbf{F}_q$ je konečné těleso, $n > 0$ je celé číslo. Pak existuje ireducibilní polynom $f(x) \in \mathbf{F}_q[x]$ stupně n .*

Důkaz. Nechť α je primitivní prvek $\mathbf{F}_{q^n}$. Víme, že $\mathbf{F}_q \subseteq \mathbf{F}_{q^n}$. Prvek α je kořenem nějakého polynomu $f(x) \in \mathbf{F}_q[x]$. To plyne z toho, že $\mathbf{F}_{q^n}$ je vektorový prostor nad $\mathbf{F}_q$ a má nějakou konečnou dimenzi k (ve skutečnosti $k = n$). Proto jsou prvky $1 = \alpha^0, \alpha^1, \alpha^2, \dots, \alpha^k$ lineárně závislé a tedy existují prvky $a_0, a_1, \dots, a_k \in \mathbf{F}_q$ takové, že $a_0 \cdot 1 + a_1 \cdot \alpha + a_2 \cdot \alpha^2 + \dots + a_k \cdot \alpha^k = 0$. Tedy α je kořenem polynomu $f(x) = a_0 + a_1x + \dots + a_kx^k \in \mathbf{F}_q[x]$. Buď $g \in \mathbf{F}_q[x]$ minimální polynom prvku $\alpha \in \mathbf{F}_{q^n}$, tedy g je ireducibilní nad $\mathbf{F}_q$. Tedy $\mathbf{F}_{q^n}$ obsahuje kořenové rozšíření $\mathbf{F}_q$ určené polynomem $g(x)$. Protože $\mathbf{F}_{q^n} = \mathbf{F}_q(\alpha)$, je tím kořenovým rozšířením celé těleso $\mathbf{F}_{q^n}$. Odtud plyne, že $\deg g = n$. $\square$

3. KOŘENY IREDUCIBILNÍCH POLYNOMŮ

Lemma 3.1. *Nechť $f \in \mathbf{F}_q[x]$ je ireducibilní polynom nad $\mathbf{F}_q$ a $\mathbf{E} \supseteq \mathbf{F}_q$ je nějaké rozšíření obsahující kořen α polynomu f . Pak pro libovolný polynom $h \in \mathbf{F}_q[x]$ platí $h(\alpha) = 0$ právě tehdy, když $f|h$.*

Důkaz. Nechť a je vedoucí koeficient polynomu $f(x)$, pak $a^{-1}f(x)$ je monický polynom, jehož kořenem je α . Označme $g \in \mathbf{F}_q[x]$ minimální polynom prvku α . Potom $g(x)|a^{-1}f(x)$. Protože $f(x)$ je ireducibilní, platí $g(x) = a^{-1}f(x)$. Proto $f(x)$ dělí každý polynom $g \in \mathbf{F}_q[x]$, jehož kořenem je α . $\square$

Lemma 3.2 (O zamrzlém kýblu). *Nechť $f \in \mathbf{F}_q[x]$ je ireducibilní polynom stupně m . Potom platí $f(x)|(x^{q^n} - x)$ právě tehdy, když $m|n$.*

Důkaz. ($\Rightarrow$) Nechť $f(x)|(x^{q^n} - x)$. Buď $\mathbf{E}$ kořenové rozšíření $\mathbf{F}_q$ určené polynomem $f(x)$ a nechť v $\mathbf{E}$ leží kořen α polynomu $f(x)$. Proto je α také kořenem polynomu $x^{q^n} - x$. Tedy $\mathbf{F}_{q^n}$ (rozkladové rozšíření $\mathbf{F}_q$ určené polynomem $x^{q^n} - x$) obsahuje kořen α polynomu $f(x)$ a tedy i $\mathbf{F}_q(\alpha)$ (kořenové rozšíření $\mathbf{F}_q$ určené polynomem $f(x)$). Těleso $\mathbf{E} = \mathbf{F}_q(\alpha)$ má q^m prvků a je podtělesem $\mathbf{F}_{q^n}$, tedy $m|n$.

($\Leftarrow$) Nechť $m|n$. Pak $\mathbf{F}_{q^m}$ je podtělesem $\mathbf{F}_{q^n}$ a $\mathbf{F}_{q^m}$ je kořenové rozšíření $\mathbf{F}_q$ určené polynomem $f(x)$, tedy obsahuje kořen α polynomu $f(x)$. Proto $\alpha \in \mathbf{F}_{q^n}$ a platí $\alpha^{q^n} - \alpha = 0$, neboli α je kořen polynomu $x^{q^n} - x \in \mathbf{F}_q[x]$. Protože také $f(\alpha) = 0$ a $\text{NSD}(f(x), x^{q^n} - x) = f(x)$ (protože $f(x)$ je ireducibilní), platí $f(x)|(x^{q^n} - x)$. $\square$