Věta 5.4. *Konečné těleso* $\mathbf{F}_q$ *je* $(q-1)$*-ní cyklotomické rozšíření libovolného svého podtělesa.*

Důkaz. Polynom $x^q - 1 \in \mathbf{K}[x]$ pro libovolné podtěleso $\mathbf{K} \subset \mathbf{F}_q$ se v $\mathbf{F}_q$ rozkládá na součin lineárních činitelů a nemůže se rozkládat na součin lineárních činitelů nad libovolným menším podtělesem $\mathbf{F}_q$. □

Poznámka. $\mathbf{F}_q^*$ je cyklická grupa řádu $q-1$. Pro každého dělitele n čísla $q-1$ existuje cyklická podgrupa $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ grupy $\mathbf{F}_q^*$ řádu n. Prvky této grupy jsou n-té odmocniny z 1 nad každým podtělesem tělesa $\mathbf{F}_q$ a generátor α je primitivní n-tá odmocnina z 1 nad libovolným podtělesem tělesa $\mathbf{F}_q$.

Lemma 5.5. *Nechť* d *je dělitel čísla* n *a* $d < n$*. Potom* $Q_n(x)$ *dělí* $\frac{x^n-1}{x-1}$.

Důkaz. Platí $Q_n(x)$ dělí $x^n - 1 = (x^d - 1) \cdot \frac{x^n-1}{x^d-1}$. Je-li ξ primitivní n-tá odmocnina z 1, pak $x - \xi | Q_n(x)$ a současně $x - \xi$ nedělí $(x^d - 1)$. Tedy $x - \xi | \frac{x^n-1}{x^d-1}$. □

6. Reprezentace prvků konečných těles

Jak reprezentovat prvky konečného tělesa, které má $q = p^k$ prvků? V této kapitole uvedeme tři různé možnosti a budeme je pro názornost ilustrovat na tělese $\mathbf{F}_9 = \mathbf{F}_{3^2}$. Pak pro reprezentaci tělesa $\mathbf{F}_9$ můžeme použít následující metody.

Příklad 1: Nejprve nějak uhodneme ireducibilní polynom stupně 2 nad $\mathbf{F}_3[x]$. Je to např. $f(x) = x^2 + 1$. Vezmeme kořenové rozšíření $\mathbf{F}_3[x]$ určené polynomem $x^2 + 1$. Označme α nějaký kořen $x^2 + 1$ v $\mathbf{F}_q[x]$. Potom všechny prvky $\mathbf{F}_q(x)$ jsou $0, 1, 2, \alpha, \alpha + 1, \alpha + 2, 2\alpha, 2\alpha + 1, 2\alpha + 2$.

Nevýhoda: musíme nějak najít ireducibilní polynom stupně n v $\mathbf{F}_p[x]$, abychom uměli počítat v $\mathbf{F}_{p^n}$.

Příklad 2: těleso $\mathbf{F}_9$ je 8. cyklotomické rozšíření tělesa $\mathbf{F}_3$. Potřebujeme najít rozklad polynomu $Q_8(x) = x^4 + 1 = (x^2 + x + 2)(x^2 + 2x + 2)$ na ireducibilní činitele nad $\mathbf{F}_3$. Označme ξ primitivní 8. odmocninu z 1. Potom $\mathbf{F}_q = \{0, \xi, \xi^2, \ldots, \xi^8\}$.

Izomorfismus mezi řešením z předchozího příkladu je dán tím, že $\xi = \alpha + 1$, neboť pro α platí $\alpha^2 + 1 = 0$. Dále pak platí

$$\begin{array}{lll} \xi \sim \alpha + 1 & \xi^4 \sim 2 & \xi^7 \sim 2\alpha \\ \xi^2 \sim 2\alpha & \xi^5 \sim 2 + 2\alpha & \xi^8 \sim 1 \\ \xi^3 \sim 1 + 2\alpha & \xi^6 \sim \alpha & \end{array}$$

Nevýhoda: Je třeba rozložit $Q_{p^k-1}(x)$ na ireducibilní činitele nad $\mathbf{F}_p$.

Příklad 3: Tato metoda je založena na *doprovodné matici* polynomu (companion matrix). Nechť $f(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + x^n$, pak jeho doprovodná matice je matice

$$A = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & 0 & \ldots & 0 & -a_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \\ 0 & \ldots & 0 & 1 & 0 & -a_{n-2} \\ 0 & \ldots & 0 & 0 & 1 & -a_{n-1} \end{pmatrix}$$

Pokud je $f(x)$ monický ireducibilní polynom v $\mathbf{F}_p[x]$ a A je jeho doprovodná matice, pak platí $f(A) = a_0 \cdot I + a_1 \cdot A + a_2 \cdot A^2 + \ldots + a_{n-1} \cdot A^{n-1} + A^n = 0$.

Pro $f(x) = x^2 + 1 \in \mathbf{F}_3[x]$ je doprovodná matice $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \sim \alpha$. Platí $A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ a $A^0 = E \sim 1$. Tedy

$$f(A) = A^2 + I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 0,$$

čili A lze pova6ovat za kořen polynomu $x^2 + 1$

Platí $\alpha + 1 = A + I = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$.

Prvky tělesa $\mathbf{F}_9$ jsou potom matice $0, I, 2I, A, I + A, 2I + A, 2A, I + 2A, 2I + 2A$. Přímým výpočtem se potom můžeme přesvědčit, že např. $(2I + A)(I + 2A) = 2A$.

K polynomu $x^2 + x + 2 \in \mathbf{F}_3[x]$ je doprovodná matice $\begin{pmatrix} 0 & -2 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}$ v $\mathbf{F}_3$.

Tato matice je kořenem cyklotomického polynomu $Q_8(x) = (x^2 + x + 2)(x^2 + 2X + 2)$ a prvky tělesa $\mathbf{F}_9$ pak jsou matice $0, C, C^2, C^3, C^4, C^5, C^6, C^7, C^8$.

7. Faktorizace polynomů nad konečnými tělesy

V dalším uvažujme monický polynom $f(x)$ z $\mathbf{F}_q[x]$. Chceme najít rozklad $f(x) = f_1^{l_1}(x) \cdot f_2^{l_2}(x) \cdot \ldots \cdot f_k^{l_k}(x)$, kde $f_1, \ldots, f_k$ jsou ireducibilní a navzájem různé.

Na začátku spočteme $f'(x)$ a $\mathrm{NSD}(f(x), f'(x)) = d(x)$. Pak jestliže

(1) $d(x) = 1$, pak $l_1 = l_2 = \ldots = 1$,
(2) $d(x) = f(x)$, pak $f'(x) = 0$ (protože $\deg f'(x) < \deg f(x)$), tedy při derivování se všechny členy vynulovali. To nastane právě tehdy, když jediné monočleny s nenulovám koeficientem v $f(x)$ mají exponenty, které jsou násobkem p, kde $p = \mathrm{char}\ \mathbf{F}_q$. T.j. $f(x) = a_0 + a_1x^p + a_2x^{2p} + \ldots + a_{k-1}x^{(k-1)p} + x^{kp}$ a tedy $f(x) = g(x^p)$, kde $g(y) = a_0 + a_1y + \ldots + a_{k-1}y^{k-1} + y^k$,
(3) $\deg d(x) > 0$ a $\deg d(x) < n$, potom $f(x) = d(x) \cdot \frac{f(x)}{d(x)}$.

Věta 7.1. *Nechť $f \in \mathbf{F}_q[x]$ je monický polynom, $h \in \mathbf{F}_q[x]$ takový, že $h^q \equiv h \bmod f$. Pak platí*

$$f(x) = \prod_{c \in \mathbf{F}_q} \mathrm{NSD}(f(x), h(x) - c)$$

Důkaz. Pro všechna $c \in \mathbf{F}_q$ platí $\mathrm{NSD}(f(x), h(x) - c) | f(x)$. Pro různá $c \in \mathbf{F}_q$ jsou polynomy $h(x) - c$ nesoudělné, proto jsou po dvou nesoudělné i polynomy $\mathrm{NSD}(f(x), h(x) - c)$. Tedy $\prod_{c \in \mathbf{F}_q} NSD(f(x), h(x) - c) | f(x)$.

Naopak $f(x) | h^q(x) - h(x) = \prod_{c \in \mathbf{F}_q} h(x) - c$. Je-li $f_i(x)$ libovolný ireducibilní činitel $f(x)$, pak $f_i | h(x) - c$ pro nějaké $c \in \mathbf{F}_q$. Tedy $f_i(x)$ dělí $\mathrm{NSD}(f(x), h(x) - c)$ pro vhodné $c \in \mathbf{F}_q$. Proto $f(x) = f_1(x) \cdot f_2(x) \cdots f_k(x) | \prod_{c \in \mathbf{F}_q} \mathrm{NSD}(f(x), h(x) - c)$. □

Zajímají nás takové polynomy $h(x)$, pro které platí $h^q \equiv h \bmod f$ a rozklad $\prod_{c \in \mathbf{F}_q} \mathrm{NSD}(f(x), h(x) - c)$ je netriviální. Takovým polynomům h se říká *f-redukující.*

Snadno lze ověřit, že každý polynom $h(x) \in \mathbf{F}_q[x]$, pro který platí $h^q \equiv h \bmod f$ a $0 < \deg h < \deg f$, je f-redukující.