KONEČNÁ TĚLESA

JIŘÍ TŮMA

Obsah

1. Úvod

Definice. *Těleso* $\mathbf{F}$ je množina se dvěma operacemi $+$, $\cdot$, splňující axiomy:

- (A1) $a + (b + c) = (a + b) + c$ pro libovolné $a, b, c \in \mathbf{F}$
- (A2) $a + b = b + a$ pro libovolné $a, b \in \mathbf{F}$
- (A3) existuje $0 \in \mathbf{F}$ tak, že pro všechna $a \in \mathbf{F}$ platí $a + 0 = 0 + a = a$
- (A4) pro všechna $a \in \mathbf{F}$ existuje $-a \in \mathbf{F}$ tak, že platí $a + (-a) = (-a) + a = 0$
- (M1) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ pro všechna $a, b, c \in \mathbf{F}$
- (M2) $a \cdot b = b \cdot a$ pro všechna $a, b \in \mathbf{F}$
- (M3) existuje $1 \in \mathbf{F}$ tak, že pro všechna $a \in \mathbf{F}$ platí $1 \cdot a = a \cdot 1 = a$
- (M4) pro všechna $a \neq 0$ existuje $a^{-1} \in \mathbf{F}$ tak, že platí $a \cdot a^{-1} = a^{-1} \cdot a = 1$
- (D) $a \cdot (b + c) = a \cdot b + a \cdot c$ pro všechna $a, b, c \in \mathbf{F}$ (distributivita)
- (N) $0 \neq 1$ (netrivialita)

Je-li $\mathbf{F}$ konečná množina, pak $\mathbf{F}$ je konečné těleso.

V dalším textu postupně přejdeme od zápisu součinu dvou prvků $a, b \in \mathbf{F}$ ve tvaru $a \cdot b$ ke stručnému ab.

Příklad. Příkladem tělesa je $\mathbb{Z}_p$ s operacemi sčítání a násobení modulo p, kde p je prvočíslo a $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$.

Jediné ne zcela zřejmé je dokázat existenci inverzního prvku. Jak se inverzní prvky hledají? Nechť $p = 19997$ a mějme číslo 16. Pak hledáme prvek 16^{-1}.

Pomocí rozšířeného Eukleidova algoritmu najdeme celá čísla a, b tak, že $a \cdot 16 + b \cdot p = 1$. Nalezené číslo a ale nemusí patřit do $\mathbb{Z}_p$ a proto není obecně ještě inverzním prvkem k 16 v $\mathbb{Z}_p$. Najdeme proto dále nezáporný zbytek r při dělení čísla a číslem p. Číslo r je určené jednoznačně podmínkami $a = p \cdot q + r$ pro nějaké celé číslo q a $0 \leq r < p$. Dosazením $a = p \cdot q + r$ do rovnosti $a \cdot 16 + b \cdot p = 1$ pak dostaneme $r \cdot 16 + p \cdot (16 \cdot q + b) = 1$ a tedy $r \cdot 16 \equiv 1 \mod p$. Protože nyní už platí $r \in \mathbb{Z}_p$, je r hledaný inverz k 16.

Použitím Eukleidova algoritmu tedy dostáváme:

$$19997 = 1249 \cdot 16 + 13$$

$$16 = 1 \cdot 13 + 3$$

$$13 = 4 \cdot 3 + 1$$

Teď spočteme vyjádření čísel a a b. Z prvé rovnice dostáváme $13 = 19997 - 1249 \cdot 16$. Z druhé rovnice dostáváme $3 = 16 - 1 \cdot 13$ a po dosazení vyjádření z prvé rovnice dostáváme $3 = 16 - (19997 - 1249 \cdot 16) = 1250 \cdot 16 - 19997$. Z třetí rovnice dostáváme $1 = 13 - 4 \cdot 3$ a po dosazení vyjádření z prvé a druhé rovnice dostáváme $1 = (19997 - 1249 \cdot 16) - 4 \cdot (1250 \cdot 16 - 19997) = -6249 \cdot 16 + 5 \cdot 19997$.

Hledaným číslem je $-6249 + 19997 = 13748$. Inverz k číslu 16 v $\mathbb{Z}_{19997}$ je tedy číslo 13748.

Příklad. Nechť $p(x) = x^3 + x + 1 \in \mathbb{Z}[x]$. Platí, že množina všech polynomů s koeficienty v $\mathbb{Z}_2$ stupně rovného nebo menšího než 2 s operacemi sčítání a násobení modulo $x^3 + x + 1$ je těleso.

Vezměme polynom $(x + 1)$. Chceme najít polynom $(x + 1)^{-1}$ inverzní k $(x + 1)$. Budeme postupovat podobně jako v předchozím příkladě. Pomocí Eukleidova algoritmu najdeme polynomy $a(x), b(x) \in \mathbb{Z}_2[x]$ takové, aby platilo $a(x) \cdot (x + 1) + b(x) \cdot p(x) = 1$.

$$x^3 + x + 1 = (x + 1) \cdot (x^2 + x) + 1$$

Tedy $(x+1)^{-1} = x^2 + x$.

Tento postup funguje vždy, kdykoliv největší společný dělitel $p(x) \in \mathbf{F}[x]$ a libovolného nenulového polynomu z $\mathbf{F}[x]$ stupně menšího než je stupeň $p(x)$, je roven 1.

Postup neplatí například pro polynom $p(x) = x^3 + x = x \cdot (x^2 + 1)$.

Definice. Polynom $p(x) \in \mathbf{F}[x]$, kde $\mathbf{F}$ je těleso, se nazývá *ireducibilní* nad $\mathbf{F}$, pokud $\deg p(x) \geq 1$ a kdykoliv $p(x) = a(x).b(x)$ v $\mathbf{F}[x]$, pak buď $a(x)$ nebo $b(x)$ je konstanta.

Věta 1.1 (o existenci kořenového rozšíření tělesa $\mathbf{F}$ určeného ireducibilním polynomem $p(x) \in \mathbf{F}[x]$)**.** *Nechť $p(x) \in \mathbf{F}[x]$ je polynom stupně n ireducibilní nad $\mathbf{F}$. Pak množina všech polynomů z $\mathbf{F}[x]$ stupně menšího než n se sčítáním a násobením modulo n je těleso.*

Důkaz. Všechny vlastnosti tělesa jsou zřejmé, až na vlastnost (M4). Pro ověření vlastnosti (M4) potřebujeme předpoklad, že $p(x)$ je ireducibilní v $\mathbf{F}[x]$. Pro každý polynom $0 \neq f(x) \in \mathbf{F}[x]$ stupně menšího než n platí, že $\mathrm{NSD}(f(x), p(x)) = 1$, tedy existují polynomy $a(x), b(x) \in \mathbf{F}[x]$ takové, že $a(x)f(x) + b(x)p(x) = 1$. Po úpravě a vydělení polynomu $a(x)$ polynomem $p(x)$ se zbytkem dostáváme $a(x) = p(x)q(x) + r(x)$, kde $\deg r(x) < n$ a dosazení do rovnosti $a(x)f(x) + b(x)p(x) = 1$ dostaneme $r(x)f(x) + p(x)(f(x)q(x) + b(x)) = 1$. Polynom $r(x)$ je tedy inverzní polynom k $f(x)$. $\square$

Definice. Je-li $\mathbf{F}$ těleso, pak nejmenší přirozené číslo n, pro které platí $\underbrace{1+1+\ldots+1}_{n} = 0$, se nazývá *charakteristika* $\mathbf{F}$.

Pokud žádné takové n neexistuje, pak říkáme, že $\mathbf{F}$ má charakteristiku 0.

Poznámka (opakování)**.** Charakteristika libovolného tělesa je buď 0 nebo prvočíslo. Konečné těleso má vždy nenulovou charakteristiku.

Definice. Nejmenší podtěleso $\mathbf{K}$ tělesa $\mathbf{F}$ se nazývá *prvotěleso* tělesa $\mathbf{F}$.

Poznámka. Jak prvotěleso v tělese $\mathbf{F}$ vypadá, závisí na charakteristice $\mathbf{F}$.

(1) Je-li charakteristika $\mathbf{F}$ rovna prvočíslu $p \geq 2$, musí v prvotělese ležet prvky $0, 1, 1+1, 1+1+1, \ldots, \underbrace{1+1+\ldots+1}_{p-1}$, které jsou navzájem různé.

Značení:

$\underbrace{1+1+\ldots+1}_{k} = k.1$

$k.1 + l.1 = (k+l).1 = r.1$, kde r je zbytek po dělení $k+l$ prvočíslem p

$(k.1) \cdot (l.1) = (kl).1 = s.1$, kde s je zbytek po dělení $k+l$ prvočíslem p

Prvotěleso v $\mathbf{F}$ je izomorfní se $\mathbb{Z}_p$.

(2) Je-li charakteristika $\mathbf{F}$ rovna 0, pak prvotěleso v $\mathbf{F}$ je izomorfní s tělesem $\mathbb{Q}$.

2. Struktura konečných těles

Lemma 2.1. *Nechť* $\mathbf{F}$ *je konečné těleso a* $\mathbf{K}$ *je podtěleso* $\mathbf{F}$*, počet prvků* $\mathbf{K}$ *je* q*. Pak* $\mathbf{F}$ *má* q^m *prvků pro nějaké přirozené číslo* m*.*

Důkaz. Všimněme si, že $\mathbf{F}$ je vektorový prostor nad $\mathbf{K}$ (je třeba ověřit axiomy vektorového prostoru). Ten má konečnou dimenzi $m \geq 1$, neboť má pouze konečně mnoho prvků a tedy obsahuje konečnou generující množinu. Zvolíme bázi $b_1, \dots, b_m$ v $\mathbf{F}$. Potom každý prvek $x \in \mathbf{F}$ lze jednoznačně vyjádřit ve tvaru $x = a_1b_1 + a_2b_2 + \dots + a_mb_m$, kde $a_1, a_2, \dots, a_m \in \mathbf{K}$. Takových lineárních kombinací je právě q^m. □

Věta 2.2. *Každé konečné těleso má* p^k *prvků pro nějaké prvočíslo* p *a přirozené číslo* k*.*

Důkaz. Označme $\mathbf{K}$ prvotěleso v $\mathbf{F}$. Charakteristika $\mathbf{F}$ je p pro nějaké prvočíslo p, tedy $\mathbf{K}$ má p prvků. Zbytek plyne z Lemma 2.1. □

V dalším se budeme zabývat otázkou, zda pro každé prvočíslo p a přirozené číslo k existuje těleso s p^k prvky. Jestliže ano, kolik takových těles existuje?

Definice. Nechť $\mathbf{E}, \mathbf{F}$ jsou dvě tělesa. Pak vzájemně jednoznačné zobrazení $T : \mathbf{E} \to \mathbf{F}$ je *izomorfismus*, jestliže pro libovolné dva prvky $a, b \in \mathbf{E}$ platí:

$$T(a+b) = T(a) + T(b)$$

$$T(a \cdot b) = T(a) \cdot T(b)$$

Pokud pro nějaké těleso $\mathbf{K}$ platí $\mathbf{K} \subseteq \mathbf{E} \cap \mathbf{F}$, pak izomorfismus $T : \mathbf{E} \to \mathbf{F}$ se nazývá $\mathbf{K}$-*izomorfismus*, jestliže pro každé $a \in \mathbf{K}$ platí $\mathbf{T}(a) = a$.

Příklad. Nechť $\mathbf{F}$ je těleso charakteristiky $p > 0$ a $\mathbf{K}$ je prvotěleso $\mathbf{F}$. Pak zobrazení $T : \mathbb{Z}_p \to \mathbf{K}$ definované předpisem

$$T(k) = \underbrace{1 + 1 + \ldots + 1}_{k} = k \cdot 1$$

je izomorfismus. Je třeba ověřit podmínky z definice izomorfizmu.

Příklad. Nechť $\mathbf{K}$ je těleso a $p(x) \in \mathbf{K}[x]$ je ireducibilní polynom stupně n. Pak množina polynomů z $\mathbf{K}[x]$ stupně menšího než n s operacemi sčítání a násobení modulo $p(x)$ je opět těleso, jak jsme si připomněli v úvodu předchozí kapitoly. Označíme jej $\mathbf{E}$. Pro ty, co mají rádi ideály a faktorové okruhy (důkazy s nimi jsou jednodušší!) připomeňme, že $\mathbf{E} \simeq \mathbf{K}[x]/(p)$.

Nechť $p(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$, kde $a_i \in \mathbf{K}$. Prvky $\mathbf{E}$ jsou polynomy $x, x^3 - x + 1 + 1, \ldots$, mezi nimi jsou i konstanty $a \in \mathbf{K}$. S konstantami se v obou tělesech $\mathbf{K}$ a $\mathbf{E}$ počítá stejně. Tedy $\mathbf{K} \subseteq \mathbf{E}$ je podtěleso tělesa $\mathbf{E}$.

Polynom $p(x)$ nemá v $\mathbf{K}$ žádný kořen, pokud $n > 1$.

Poznámka. Nechť $f(x) \in \mathbf{K}[x]$ a $a \in \mathbf{K}$ je kořen $f(x)$. Potom $(x-a)|f(x)$.

Důkaz. Libovolný polynom $f(x)$ můžeme napsat ve tvaru $f(x) = q(x)\cdot(x-a)+r(x)$, kde $\deg r(x) < \deg(x-a) = 1$, takže $r(x)$ je konstantní polynom. Protože a je kořen $f(x)$, po dosazení do $f(x)$ dostáváme $0 = f(a) = q(a)\cdot(a-a)+r(a) = r(a)$. Protože je $r(x)$ konstantní polynom a $r(a) = 0$, platí $r(x) = 0$ a tedy $(x-a)|f(x)$. □

Příklad. Uvažujme polynom $p(z) = a_n z^n + \ldots + a_1 z + a_0 \in \mathbf{K}[z]$. Dosadíme-li $z = x \in \mathbf{E}$, pak je hodnota $p(x)$ nějaký prvek tělesa $\mathbf{E}$, konkrétně je to $p(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbf{E}$. Protože $p(x) \equiv 0 \mod p(x)$, platí $p(x) = 0 \in \mathbf{E}$. Polynom $p(z)$ má tedy v tělese $\mathbf{E}$ aspoň jeden kořen.

Definice. Nechť $\mathbf{K}$ je těleso a $p(x) \in \mathbf{K}[x]$ je polynom ireducibilní nad $\mathbf{K}$. Potom těleso $\mathbf{E} \supseteq \mathbf{K}$ se nazývá *kořenové rozšíření* $\mathbf{K}$ určené polynomem $p(x)$, jestliže v $\mathbf{E}$ existuje nějaký kořen θ polynomu $p(x)$ a každé podtěleso $\mathbf{E}$, které obsahuje současně $\mathbf{K}$ a θ, se rovná $\mathbf{E}$.

Věta 2.3 (O existenci a jednoznačnosti kořenového rozšíření tělesa $\mathbf{K}$ určeného ireducibilním polynomem $p(x) \in \mathbf{K}[x]$)**.** *Nechť $\mathbf{K}$ je těleso a $p(x) \in \mathbf{K}[x]$ je polynom ireducibilní nad $\mathbf{K}$. Potom existuje kořenové rozšíření $\mathbf{E}$ tělesa $\mathbf{K}$ určené polynomem $p(x)$. Kořenové rozšíření je určeno jednoznačně až na $\mathbf{K}$-izomorfismus.*

Důkaz. (1) Nejprve dokážeme existenci kořenového rozšíření. V předchozích příkladech jsme si ukázali, že těleso $\mathbf{E}$ obsahující všechny polynomy stupně menšího než je stupeň $p(x)$ s operacemi sčítání a násobení modulo $p(x)$ je těleso obsahující $\mathbf{K}$ jako podtěleso a ukázali jsme si, že v něm existuje aspoň jeden kořen polynomu $p(x)$. Nechť $f(x) = b_m x^m + \ldots + b_1 x + b_0 \in \mathbf{K}[x]$, přičemž m je menší než je stupeň $p(x)$. Pak takový polynom musí ležet v libovolném podtělese $\mathbf{E}$ obsahujícím x a $\mathbf{K}$.

(2) Zbývá dokázat jednoznačnost. Nechť $\mathbf{F} \supseteq \mathbf{K}$ je nějaké kořenové rozšíření $\mathbf{K}$ obsahující kořen θ polynomu $p(x)$. Definujme zobrazení $T : \mathbf{E} \to \mathbf{F}$ předpisem $T(f(x)) = f(\theta)$, kde $f(x) = b_m x^m + \ldots + b_1 x + b_0$ a $f(\theta) = b_m \theta^m + \ldots + b_1 \theta + b_0$.

Chceme dokázat, že T je $\mathbf{K}$-izomorfismus. Jestliže $a \in \mathbf{K}$, potom $T(a) = a$.

Dokážeme, že T je homomorfismus. Nechť $f(x), g(x) \in \mathbf{E}$ jsou libovolné dva polynomy, $f(x) = b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$ a $g(x) = c_{m-1}x^{m-1} + \ldots + c_1 x + c_0$. Potom platí platí

$$T(f(x)) = \sum_{i=0}^{m-1} b_i \theta^i, \qquad T(g(x)) = \sum_{i=0}^{m-1} c_i \theta^i,$$

$$\begin{aligned} T((f+g)(x)) &= \sum_{i=0}^{m-1} (b_i + c_i)\theta^i = \sum_{i=0}^{m-1} b_i \theta^i + \sum_{i=0}^{m-1} c_i \theta^i = \\ &= T(f(x)) + T(g(x)). \end{aligned}$$

Podobně (důkaz ale vyžaduje více počítání!)

$$T(fg(x)) = T(f(x)) \cdot T(g(x)).$$

Nyní dokážeme, že T je prosté zobrazení. Nechť $f(x), g(x) \in \mathbf{E}$ jsou navzájem různé polynomy z $\mathbf{E}$ takové, že $T(f(x)) = T(g(x))$. Pak $\sum_{i=0}^{m-1} b_i \theta^i = \sum_{i=0}^{m-1} c_i \theta^i$, t.j. $\sum_{i=0}^{m-1} (b_i - c_i)\theta^i = 0$. Takže θ je kořen polynomu $0 \neq g(x) = (b_{m-1} - c_{m-1})x^{m-1} + \ldots + (b_1 - c_1)x + (b_0 - c_0) \in \mathbf{K}[x]$, který musí mít stupeň aspoň 1. Prvek θ je ale také kořenem polynomu $p(x) \in \mathbf{K}[x]$. Tedy θ je kořen polynomu $d(x) := \mathrm{NSD}(g(x), p(x)) \in \mathbf{K}[x]$. Pak $d(x) | p(x)$ v $\mathbf{K}[x]$, přičemž $1 \leq \deg d(x) < \deg p(x)$. To je však spor s předpokladem, že $p(x)$ je ireducibilní v $\mathbf{K}[x]$.

Zbývá dokázat, že T je na $\mathbf{F}$. Im T je podtěleso $\mathbf{F}$ obsahující $\mathbf{K}$ a θ. Protože $\mathbf{F}$ je kořenové rozšíření $\mathbf{K}$ určené $p(x)$, platí Im $T = \mathbf{F}$.

Jsou-li nyní $\mathbf{F}, \mathbf{G}$ dvě kořenová rozšíření $\mathbf{K}$ určená polynomem $p(x)$, pak existují $\mathbf{K}$-izomorfismy $T : \mathbf{E} \to \mathbf{F}$ a $U : \mathbf{E} \to \mathbf{G}$. Potom $UT^{-1} : \mathbf{F} \to \mathbf{G}$ je $\mathbf{K}$-izomorfismus $\mathbf{F}$ a $\mathbf{G}$.

□

Poznámka. Jsou-li $\mathbf{F}$ a $\mathbf{G}$ dvě kořenová rozšíření tělesa $\mathbf{K}$ určená ireducibilním polynomem $p(x) \in \mathbf{K}[x]$ a označíme-li $\theta \in \mathbf{F}$ a $\sigma \in \mathbf{G}$ kořeny polynomu $p(x)$, pak $\mathbf{K}$-izomorfizmus $UT^{-1} : \mathbf{F} \to \mathbf{G}$ z posledního odstavce důkazu předchozí věty má vlastnost

$$UT^{-1}(\theta) = U(x) = \sigma$$

Lemma 2.4. *Nechť $\mathbf{F}$ je těleso charakteristiky $p > 0$. Pak pro libovolné $a, b \in \mathbf{F}$ a libovolné přirozené číslo $k > 0$ platí*

$$(a+b)^{p^k} = a^{p^k} + b^{p^k}$$

Důkaz. Důkaz provedeme indukcí dle k.

(1) Nechť $k = 1$. Podle binomické věty platí $(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \ldots + \binom{p}{p-1}ab^{p-1} + b^p$. Protože $p|\binom{p}{i}$ pro $i \in \{1, 2, \ldots, p-1\}$, platí v tělese $\mathbf{F}$, že $\binom{p}{i}.1 = 0$. Tedy také $\binom{p}{i}a^{p-i}b^i = 0$ v $\mathbf{F}$ a proto $(a+b)^p = a^p + b^p$.

(2) Předpokládejme platnost tvrzení pro $k-1$, tedy $(a+b)^{p^{k-1}} = a^{p^{k-1}} + b^{p^{k-1}}$. Potom platí $(a+b)^{p^k} = ((a+b)^{p^{k-1}})^p = (a^{p^{k-1}} + b^{p^{k-1}})^p = a^{p^k} + b^{p^k}$.

□

Lemma 2.5. *Nechť $\mathbf{F}$ je konečné těleso s q prvky. Potom pro každé $a \in \mathbf{F}$ platí $a^q = a$.*

Důkaz. Pro $a = 0$ lemma platí. Nechť $a \neq 0$, pak vezmeme multiplikativní grupu $\mathbf{F}$. Ta má $q-1$ prvků. Protože řád libovolného prvku konečné grupy je dělitelem počtu prvků této grupy, tak platí $a^{q-1} = 1$. □

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 $\mathbf{K}(\theta_1, \theta_2, \dots, \theta_m)$ nejmenší podtěleso tělesa $\mathbf{E}$ obsahující $\mathbf{K}$ a prvky $\theta_1, \theta_2, \dots, \theta_m \in \mathbf{E}$.

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 $\theta_1, \theta_2, \dots, \theta_m \in \mathbf{E}$ všechny kořeny polynomu $f(x)$, pak $\mathbf{K}(\theta_1, \theta_2, \dots, \theta_m) = \mathbf{E}$.

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 ireducibilni nad $\mathbf{E}$, právě když je polynom $T(p(x))$ ireducibilni 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* $\mathbf{K}$ *určené 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 $p_1, p_2, \dots, p_n$ 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 $f(x) = q_1 \cdot q_2 \cdots q_l$ 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 kterým 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 $\theta_1, \dots, \theta_k$, tj. $\mathbf{F} = \mathbf{K}(\theta_1, \dots, \theta_k)$. 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 $n - k > 0$ a 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 přirozené číslo n 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. □

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.*

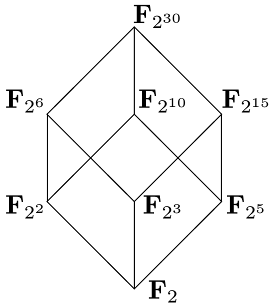
Pro každé $m|n$ existuje právě jedno podtěleso tělesa $\mathbf{F}_q$, které má p^m prvků.

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 $(p^{km} - 1) = (p^m - 1)(p^{(k-1)m} + p^{(k-2)m} + \cdots + p^m + 1)$. Pokud $a = b \cdot c$, pak $(x^{bc} - 1) = (x^b - 1)(x^{(c-1)b} + x^{(c-2)b} + \ldots + x^b + 1)$. 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 $h = q - 1 = p_1^{r_1} \cdot p_2^{r_2} \cdot \cdots \cdot p_k^{r_k}$. 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 $b = b_1 b_2 \cdots b_k$. Platí $b^h = 1$. Dále pro $i = 1, 2, \ldots, k$ 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 $g|f$.

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 $\mathbf{F}_r$. □

Věta 2.12. *Nechť $\mathbf{F}_q$ je konečné těleso a n je přirozené 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 $1 = \alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^k$ lineárně závislé a tedy existují prvky $a_0, a_1, \ldots, a_k \in \mathbf{F}_q$ takové, že $a_0 \cdot 1 + a_1 \cdot \alpha + a_2 \cdot \alpha^2 + \cdots + a_k \cdot \alpha^k = 0$. Tedy α je kořenem polynomu $f(x) = a_0 + a_1 x + \ldots + a_k x^k \in \mathbf{F}_q[x]$. Buď $g \in \mathbf{F}_q[x]$ minimální polynom prvku $\alpha \in \mathbf{F}_{q^m}$, 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 $\deg g = n$. □

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 $h \in \mathbf{F}_q[x]$, jehož kořenem je α. □

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. ($\Leftarrow$) 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 $m|n$.

($\Rightarrow$) 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 $\mathrm{NSD}(f(x), x^{q^n} - x) = f(x)$ (protože $f(x)$ je ireducibilní), platí $f(x)|(x^{q^n} - x)$. □

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 $\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{m-1}}$ 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 $f(x) = a_m x^m + a_{m-1}x^{m-1} + \dots + a_1 x + a_0$, pak $f(\beta)^q = (a_m\beta^m + \dots + a_1\beta + a_0)^q = a_m^q(\beta^m)^q + a_{m-1}^q(\beta^{m-1})^q + \dots + a_1^q\beta^q + a_0^q = a_m(\beta^q)^m + a_{m-1}(\beta^q)^{m-1} + \dots + a_1\beta^q + a_0 = f(\beta^q)$. Je-li tedy $\alpha \in \mathbf{F}_{q^m}$ kořen polynomu $f(x)$, pak taky $\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{m-1}}$ jsou kořeny polynomu $f(x)$.

Zbývá ješte 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 $0 < m-j+i < m$, 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 $\mathbf{F}_q(\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{m-1}}) = \mathbf{F}_q(\alpha) = \mathbf{F}_{q^m}$. □

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. $\square$

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. Pro 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 $\alpha = 0$. $\square$

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*.*

4. Stopy, normy a báze

Připomeňme si, že je-li $\mathbf{F}_{q^m} \supseteq \mathbf{F}_q$, tak všechny automorfismy $\mathbf{F}_{q^m}$ nad $\mathbf{F}_q$ jsou tvaru $\alpha \to \alpha^{q^i}$ pro $i = 0, 1, 2, \dots, m-1$ a libovolné $\alpha \in \mathbf{F}_{q^m}$.

V dalším bude často používat označení $\mathbf{F} = \mathbf{F}_{q^m}$ a $\mathbf{K} = \mathbf{F}_q$.

Definice. Nechť $\mathbf{F} = \mathbf{F}_{q^m}$, $\mathbf{K} = \mathbf{F}_q$ a $\alpha \in \mathbf{F}$. Pak definujeme prvek $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \dots + \alpha^{q^{m-1}}$ a nazýváme ho *stopa* α nad $\mathbf{K}$.

Je-li $\mathbf{K}$ prvotěleso v $\mathbf{F}$, potom zapisujeme $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha) = \mathrm{Tr}_{\mathbf{F}}(\alpha)$ a prvek $\mathrm{Tr}_{\mathbf{F}}(\alpha)$ nazýváme *absolutní stopa* $\alpha \in \mathbf{F}$.

Lemma 4.1. *Platí* $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha) \in \mathbf{K}$ *pro libovolné* $\alpha \in \mathbf{F}$.

Důkaz. Nechť $f(x) = x^d + a_{d-1}x^{d-1} + \dots + a_1 x + a_0 \in \mathbf{K}[x]$ je minimální polynom prvku $\alpha \in \mathbf{F}$ nad $\mathbf{K}$. Protože $f(x) | x^{q^m} - x$, platí $d|m$. Polynom $f(x)^{\frac{m}{d}} = g(x)$ se nazývá *charakteristický polynom* α nad $\mathbf{K}$. Kořeny $f(x)$ jsou $\alpha, \alpha^q, \alpha^{q^2}, \dots \alpha^{q^{d-1}}$ a všechny prvky konjugované k α nad $\mathbf{K}$ jsou právě všechny prvky kořeny polynomu $g(x) = x^m + b_{m-1}x^{m-1} + \dots + b_1 x + b_0 = (x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})\dots(x-\alpha^{q^{m-1}})$. Roznásobením pravé strany dostáváme

$$x^m + b_{m-1}x^{m-1} + \dots + b_1 x + b_0 = x^m + (-\alpha - \alpha^q - \dots - \alpha^{q-1}) \cdot x^{m-1} + \dots$$

Tedy $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha) = -b_{m-1} \in \mathbf{K}$. □

Poznámka. Tedy platí $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}} : \mathbf{F} \to \mathbf{K}$.

Věta 4.2 (O stopě)**.** *Nechť* $\mathbf{F} = \mathbf{F}_{q^m}$ *a* $\mathbf{K} = \mathbf{F}_q$. *Potom* $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}$ *má následující vlastnosti*

(1) $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha + \beta) = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha) + \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\beta)$ *pro všechny* $\alpha, \beta \in \mathbf{F}$
(2) $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(c \cdot \alpha) = c \cdot \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha)$ *pro všechna* $c \in \mathbf{K}$ *a* $\alpha \in \mathbf{F}$
(3) $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}} : \mathbf{F} \to \mathbf{K}$ *je lineární zobrazení na celé těleso* $\mathbf{K}$
(4) $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(a) = m \cdot a$ *pro všechna* $a \in \mathbf{K}$
(5) $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha^q) = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha)$ *pro všechna* $\alpha \in \mathbf{F}$

Důkaz.
(1) Platí $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha + \beta) = (\alpha + \beta) + (\alpha + \beta)^q + (\alpha + \beta)^{q^2} + \dots + (\alpha + \beta)^{q^{m-1}} = \alpha + \beta + \alpha^q + \beta^q + \alpha^{q^2} + \beta^{q^2} + \dots + \alpha^{q^{m-1}} + \beta^{q^{m-1}} = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha) + \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\beta)$.
(2) Platí $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(c \cdot \alpha) = c \cdot \alpha + (c \cdot \alpha)^q + \dots + (c \cdot \alpha)^{q^{m-1}} = c \cdot \alpha + c \cdot \alpha^q + c \cdot \alpha^{q^2} + \dots + c \cdot \alpha^{q^{m-1}} = c \cdot \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha)$, protože $c \in \mathbf{K} = \mathbf{F}_q$.
(3) Lineárnost zobrazení plyne z předchozích dvou bodů. Stačí tedy najít $\alpha \in \mathbf{F}$, pro které $0 \neq \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha) = \alpha + \alpha^q + \dots + \alpha^{q^{m-1}}$. Je-li $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha) = 0$, je α kořen rovnice $x + x^q + \dots + x^{q^{m-1}} \in \mathbf{K}[x]$. Takových je nejvýše $q^{m-1} < q^m$.
(4) Pro $a \in \mathbf{K}$ platí $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(a) = a + a^q + a^{q^2} + \dots + a^{q^{m-1}} = \underbrace{a + a + \dots + a}_{m\text{-krát}} = m \cdot a$
(5) Platí $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha^q) = \alpha^q + (\alpha^q)^q + \dots + (\alpha^q)^{q^{m-2}} + (\alpha^q)^{q^{m-1}} = \alpha^q + \alpha^{q^2} + \dots + \alpha^{q^{m-1}} + \alpha = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha)$

□

Věta 4.3. *Nechť* $\mathbf{F} = \mathbf{F}_{q^m} \supseteq \mathbf{F}_q = \mathbf{K}$. *Pak všechna lineární zobrazení z* $\mathbf{F}$ *do* $\mathbf{K}$ *jsou tvaru* $L_\beta(\alpha) = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha \cdot \beta)$ *pro* $\beta \in \mathbf{F}$.

Je-li $\beta \neq \gamma$, *pak* $L_\beta \neq L_\gamma$.

Důkaz. Nejprve dokážeme, že $L_\beta(\alpha)$ je lineární zobrazení. Platí $L_\beta(\alpha_1+\alpha_2) = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}((\alpha_1+\alpha_2)\beta) = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha_1\beta) + \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha_2\beta) = L_\beta(\alpha_1) + L_\beta(\alpha_2)$ pro všechny $\alpha_1, \alpha_2 \in \mathbf{F}$. Podobně $L_\beta(c\alpha) = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(c\alpha\beta) = c\cdot\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha\beta) = c\cdot L_\beta(\alpha)$.

Je-li $\beta \neq \gamma$, potom existuje prvek $\alpha \in \mathbf{F}$ takový, že $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}((\beta-\gamma)\alpha) \neq 0$ a tedy $L_\beta(\alpha) \neq L_\gamma(\alpha)$. Počet lineárních zobrazení z $\mathbf{F}$ do $\mathbf{K}$ je q^m, tedy stejný jako počet zobrazení L_β. □

Věta 4.4. *Nechť* $\mathbf{F} = \mathbf{F}_{q^m} \supseteq \mathbf{F}_q = \mathbf{K}$. *Potom pro* $\alpha \in \mathbf{F}$ *platí* $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha) = 0$ *právě tehdy, když* $\alpha = \beta^q - \beta$ *pro nějaké* $\beta \in \mathbf{F}$.

Důkaz. ($\Leftarrow$) Plyne z Věty 4.2 (5), protože $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha) = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\beta^q-\beta) = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\beta^q) - \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\beta) = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\beta) - \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\beta) = 0$.

($\Rightarrow$) Nechť $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha) = 0$. Vezmeme polynom $x^q - x - \alpha \in \mathbf{F}[x]$. Buď β kořen polynomu $x^q-x-\alpha$ v nějakém rozšíření $\mathbf{E} \supseteq \mathbf{F}$. Platí $\beta^q - \beta = \alpha$. Zbývá dokázat, že $\beta \in \mathbf{F}_{q^m}$. Platí $0 = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha) = \alpha+\alpha^q+\alpha^{q^2}+\ldots+\alpha^{q^{m-1}} = \beta^q-\beta+(\beta^q-\beta)^q+(\beta^q-\beta)^{q^2}+\ldots+(\beta^q-\beta)^{q^{m-1}} = (\beta^q-\beta)+(\beta^{q^2}-\beta^q)+(\beta^{q^3}-\beta^{q^2})+\ldots+(\beta^{q^m}-\beta^{q^{m-1}}) = \beta^{q^m}-\beta$. Tedy $\beta^{q^m}-\beta = 0$ a proto $\beta \in \mathbf{F}_{q^m}$. □

Věta 4.5 (O tranzitivitě stopy)**.** *Jsou-li* $\mathbf{K} = \mathbf{F}_q \subseteq \mathbf{F} = \mathbf{F}_{q^m} \subseteq \mathbf{E} = \mathbf{F}_{q^{m.n}}$ *konečná tělesa, pak* $\mathrm{Tr}_{\mathbf{E}/\mathbf{K}} = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}} \circ \mathrm{Tr}_{\mathbf{E}/\mathbf{F}}$.

Důkaz. Je-li $\alpha \in \mathbf{E}$, pak

$$\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\mathrm{Tr}_{\mathbf{E}/\mathbf{F}}(\alpha)) = \sum_{i=0}^{m-1}(\mathrm{Tr}_{\mathbf{E}/\mathbf{F}}(\alpha))^{q^i} = \sum_{i=0}^{m-1}(\sum_{j=0}^{n-1}(\alpha^{q^m})^j)^{q^i}$$

a dále

$$\sum_{i=0}^{m-1}(\sum_{j=0}^{n-1}(\alpha^{q^m})^j)^{q^i} \sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\alpha^{q^{mj+i}} = \sum_{k=0}^{mn-1}\alpha^{q^k} = \mathrm{Tr}_{\mathbf{E}/\mathbf{K}}(\alpha).$$

□

Definice. Nechť $\mathbf{F} = \mathbf{F}_{q^m} \supseteq \mathbf{F}_q = \mathbf{K}$. Pak prvek

$$\mathrm{N}_{\mathbf{F}/\mathbf{K}}(\alpha) = \alpha\cdot\alpha^q\cdot\alpha^{q^2}\cdot\ldots\cdot\alpha^{q^{m-1}} = \alpha^{\frac{q^m-1}{q-1}}$$

nazýváme *norma* $\alpha \in \mathbf{F}$ nad $\mathbf{K}$.

Poznámka. Pro všechna $\alpha \in \mathbf{F}$ je $\mathrm{N}_{\mathbf{F}/\mathbf{K}}(\alpha) \in \mathbf{K}$, neboť je až na znaménko rovna absolutnímu členu charakteristického polynomu prvku α nad $\mathbf{K}$ - viz důkaz Lemma 4.1.

Věta 4.6 (O normě)**.** *Pro funkci* $\mathrm{N}_{\mathbf{F}/\mathbf{K}}$ *platí*

(1) $\mathrm{N}_{\mathbf{F}/\mathbf{K}}(\alpha\cdot\beta) = \mathrm{N}_{\mathbf{F}/\mathbf{K}}(\alpha)\cdot\mathrm{N}_{\mathbf{F}/\mathbf{K}}(\beta)$ *pro všechna* $\alpha, \beta \in \mathbf{F}$
(2) $\mathrm{N}_{\mathbf{F}/\mathbf{K}}$ *je zobrazení z* $\mathbf{F}$ *na* $\mathbf{K}$ *a z* $\mathbf{F}^*$ *na* $\mathbf{K}^*$
(3) $\mathrm{N}_{\mathbf{F}/\mathbf{K}}(d) = d^m$ *pro všechna* $d \in \mathbf{K}$
(4) $\mathrm{N}_{\mathbf{F}/\mathbf{K}}(\alpha^q) = \mathrm{N}_{\mathbf{F}/\mathbf{K}}(\alpha)$ *pro všechna* $\alpha \in \mathbf{F}$

Důkaz.
(1) Platí $\mathrm{N}_{\mathbf{F}/\mathbf{K}}(\alpha\cdot\beta) = (\alpha\cdot\beta)\cdot(\alpha\cdot\beta)^q\cdot\ldots\cdot(\alpha\cdot\beta)^{q^{m-1}} = \alpha\cdot\alpha^q\cdot\ldots\cdot\alpha^{q^{m-1}}\cdot\beta\cdot\beta^q\cdot\ldots\cdot\beta^{q^{m-1}} = \mathrm{N}_{\mathbf{F}/\mathbf{K}}(\alpha)\cdot\mathrm{N}_{\mathbf{F}/\mathbf{K}}(\beta)$
(2) Podle (1) je $\mathrm{N}_{\mathbf{F}/\mathbf{K}} : \mathbf{F}^* \to \mathbf{K}^*$ homomorfismus grup. V jádru $\mathrm{N}_{\mathbf{F}/\mathbf{K}}$ jsou kořeny rovnice

$$x^{\frac{q^m-1}{q-1}} - 1 \in \mathbf{K}[x]$$

Buď d počet prvků (řád) jádra $\mathrm{N}_{\mathbf{F}/\mathbf{K}}$. Platí $d \leq (q^m-1)/(q-1)$ a současně $d|(q^m-1)$. Tedy Im $(\mathrm{N}_{\mathbf{F}/\mathbf{K}})$ má velikost $(q^m-1)/d \geq q-1$, což je řád $\mathbf{K}^*$.

(3) Platí $\mathrm{N}_{\mathbf{F}/\mathbf{K}}(d) = d \cdot d^q \cdot d^{q^2} \cdot \ldots \cdot d^{q^{m-1}} = \underbrace{d \cdot d \cdot \ldots \cdot d}_{m\text{-krát}} = d^m$

(4) Platí $\mathrm{N}_{\mathbf{F}/\mathbf{K}}(\alpha^q) = \alpha^q \cdot (\alpha^q)^q \cdot \ldots \cdot (\alpha^q)^{q^{m-2}} \cdot (\alpha^q)^{q^{m-1}} = \alpha^q \cdot \alpha^{q^2} \cdot \ldots \cdot \alpha^{q^{m-1}} \cdot \alpha = \mathrm{N}_{\mathbf{F}/\mathbf{K}}(\alpha)$

$\square$

Věta 4.7 (O tranzitivitě normy). *Jsou-li* $\mathbf{K} = \mathbf{F}_q \subseteq \mathbf{F} = \mathbf{F}_{q^m} \subseteq \mathbf{E} = \mathbf{F}_{q^{m.n}}$ *konečná tělesa, pak pro libovolné* $\alpha \in \mathbf{E}$ *platí* $\mathrm{N}_{\mathbf{E}/\mathbf{K}}(\alpha) = \mathrm{N}_{\mathbf{F}/\mathbf{K}}(\mathrm{N}_{\mathbf{E}/\mathbf{F}}(\alpha))$.

Důkaz. Z definice platí $\mathrm{N}_{\mathbf{E}/\mathbf{F}}(\alpha) = \alpha^{\frac{(q^m)^n-1}{q^m-1}}$. Pak platí

$$\mathrm{N}_{\mathbf{F}/\mathbf{K}}(\mathrm{N}_{\mathbf{E}/\mathbf{F}}(\alpha)) = (\mathrm{N}_{\mathbf{E}/\mathbf{F}}(\alpha))^{\frac{q^m-1}{q-1}} = (\alpha^{\frac{(q^m)^n-1}{q^m-1}})^{\frac{q^m-1}{q-1}} = \alpha^{\frac{q^{m.n}-1}{q-1}} = \mathrm{N}_{\mathbf{E}/\mathbf{K}}(\alpha).$$

$\square$

Je-li $\alpha_1, \ldots, \alpha_m$ báze $\mathbf{F} = \mathbf{F}_{q^m}$ nad $\mathbf{K} = \mathbf{F}_q$, potom libovolný prvek $\alpha \in \mathbf{F}_{q^m}$ můžeme vyjádřit jednoznačně ve tvaru

$$\alpha = c_1(\alpha) \cdot \alpha_1 + c_2(\alpha) \cdot \alpha_2 + \ldots + c_m(\alpha) \cdot \alpha_m$$

kde $c_i(\alpha) \in \mathbf{F}_q$ pro $i = 1, \ldots, m$.

Každé zobrazení $c_i(\alpha) : \mathbf{F}_{q^m} \to \mathbf{F}_q$ je lineární funkcionál. Pro každé $i = 1, \ldots, m$ existuje $\beta_i \in \mathbf{F}_{q^m}$ takové, že

$$c_i(\alpha) = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha\beta_i)$$

Je-li $\alpha = \alpha_j$, pak

$$c_i(\alpha_j) = \delta_{ij} = \begin{cases} 0, & i \neq j \\ 1, & i = j. \end{cases}$$

Tedy $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha_j\beta_i) = \delta_{ij}$.

Posloupnost $\beta_1, \ldots, \beta_m$ je lineárně nezávislá nad $\mathbf{F}_q$, neboť z rovnosti

$$d_1\beta_1 + \ldots + d_m\beta_m = 0$$

pro $d_1, \ldots, d_m \in \mathbf{F}_q$ plyne pro každé $j = 1, \ldots, m$

$$d_1\beta_1\alpha_j + \ldots + d_m\beta_m\alpha_j = 0,$$

$$\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(d_1\beta_1\alpha_j + \ldots + d_m\beta_m\alpha_j) = 0,$$

$$d_1\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\beta_1\alpha_j) + \ldots + d_m\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\beta_m\alpha_j) = 0$$

$$d_j \cdot 1 = 0.$$

Proto $\beta_1, \ldots, \beta_m$ je opět báze $\mathbf{F}_{q^m}$ nad $\mathbf{F}_q$.

Definice. Báze $\beta_1 \ldots, \beta_m$ se nazývá *duální báze* k bázi $\alpha_1, \ldots, \alpha_m$ v $\mathbf{F}_{q^m}$ nad $\mathbf{F}_q$.

Poznámka. Duální báze k bázi $\alpha_1, \ldots, \alpha_m$ je určena jednoznačně bází $\alpha_1, \ldots, \alpha_m$. To plyne ze vztahu $c_i(\alpha) = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha\beta_i)$. Proto duální báze k bázi $\beta_1, \ldots, \beta_m$ je původní báze $\alpha_1, \ldots, \alpha_m$.

Příklad. Nechť $\mathbf{F}_8 \supseteq \mathbf{F}_2$ je kořenové rozšíření $\mathbf{F}_2$ určené polynomem $f(x) = x^3 + x^2 + 1 \in \mathbf{F}_2[x]$. Buď $\alpha \in \mathbf{F}_8$ kořen $f(x)$. Uvažujme prvky $\alpha, \alpha^2, \alpha^3 = \alpha^2 + 1, \alpha^4 = \alpha(\alpha^2+1) = \alpha^3+\alpha = \alpha^2+\alpha+1, \alpha^5 = \alpha(\alpha^2+\alpha+1) = \alpha^3+\alpha^2+\alpha = \alpha^2+1+\alpha^2+\alpha = \alpha + 1, \alpha^6 = \alpha(\alpha + 1) = \alpha^2 + \alpha, \alpha^7 = 1$.

Prvky $\alpha, \alpha^2, \alpha^4$ tvoří bázi $\mathbf{F}_8$ nad $\mathbf{F}_2$. Ukážeme, že $\beta_1 = \alpha, \beta_2 = \alpha^2, \beta_3 = \alpha^2 + \alpha + 1$ je duální báze k $\alpha, \alpha^2, \alpha^2 + \alpha + 1$. Plyne to z následujících rovností.

$\mathrm{Tr}(\alpha_1\beta_1) = \mathrm{Tr}(\alpha\alpha) = \mathrm{Tr}(\alpha^2) = \alpha^2 + \alpha^4 + \alpha^8 = \alpha^2 + \alpha^2 + \alpha + 1 + \alpha = 1$.

$\mathrm{Tr}(\alpha_1\beta_2) = \mathrm{Tr}(\alpha\alpha^2) = \mathrm{Tr}(\alpha^3) = \alpha^3 + \alpha^6 + \alpha^{12} = \alpha^2 + 1 + \alpha^2 + \alpha + \alpha + 1 = 0$.

Analogicky dál.

Definice. Báze $\mathbf{F}_{q^m}$ nad $\mathbf{F}_q$ tvaru $\alpha, \alpha^q, \alpha^{q^2} \dots, \alpha^{q^{m-1}}$ pro nějaké $\alpha \in \mathbf{F}_{q^m}$ se nazývá *normální báze* $\mathbf{F}_{q^m}$ nad $\mathbf{F}_q$.

Věta 4.8. *Je-li* $\mathbf{F}_{q^m}$ *rozšíření* $\mathbf{F}_q$*, pak existuje v* $\mathbf{F}_{q^m}$ *nad* $\mathbf{F}_q$ *normální báze. Dokonce existuje normální báze tvořená primitivními prvky* $\mathbf{F}_{q^m}$*.*

Definice. Nechť $\mathbf{F} = \mathbf{F}_{q^m} \supseteq \mathbf{F}_q = \mathbf{K}$ a $\alpha_1, \dots, \alpha_m \in \mathbf{F}$. Označme

$$B = (\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha_i, \alpha_j))_{i,j}$$

Čili B je čtvercová matice řádu m, která má na místě (i,j) prvek $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha_i, \alpha_j)$. Pak $\Delta_{\mathbf{F}/\mathbf{K}}(\alpha_1, \dots, \alpha_m) = \det B$ se nazývá *diskriminant* $\alpha_1, \dots, \alpha_m$ nad $\mathbf{F}_q$.

Věta 4.9. *Prvky* $\alpha_1, \dots, \alpha_m \in \mathbf{F}$ *tvoří bázi* $\mathbf{F} = \mathbf{F}_{q^m}$ *nad* $\mathbf{K} = \mathbf{F}_q$ *právě tehdy, když* $\Delta_{\mathbf{F}/\mathbf{K}}(\alpha_1, \dots, \alpha_m) \neq 0$.

Důkaz. ($\Rightarrow$) Nechť $\alpha_1, \dots, \alpha_m$ je báze $\mathbf{F}$ nad $\mathbf{K}$. Ukážeme, že řádky matice B jsou lineárně nezávislé. Je-li $d_1 \cdot \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha_1\alpha_j) + d_2 \cdot \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha_2\alpha_j) + \dots + d_m \cdot \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha_m\alpha_j) = 0$ pro nějaké $d_1, \dots, d_m \in \mathbf{K}$ a každé $j = 1, \dots, m$, pak platí

$$\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}((d_1\alpha_1 + \dots + d_m\alpha_m) \cdot \alpha_j) = 0$$

pro $j = 1, \dots, m$. Označme si $\beta = d_1\alpha_1 + \dots + d_m\alpha_m$. Tedy $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\beta\alpha_j) = 0$ pro $j = 1, \dots, m$. Protože $\alpha_1, \dots, \alpha_m$ je báze $\mathbf{F}$ nad $\mathbf{K}$, plyne odtud $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\beta\alpha) = 0$ pro libovolné $\alpha \in \mathbf{F}_{q^m}$. Proto $\beta = 0$, neboli $d_1\alpha_1 + \dots + d_m\alpha_m = 0$. Protože $\alpha_1, \dots, \alpha_m$ je báze $\mathbf{F}$ nad $\mathbf{K}$, platí $d_1 = d_2 = \dots = d_m = 0$.

($\Leftarrow$) Nechť $\Delta_{\mathbf{F}/\mathbf{K}}(\alpha_1, \dots, \alpha_m) \neq 0$ a $c_1\alpha_1 + \dots + c_m\alpha_m = 0$ pro nějaké $c_1, \dots, c_m \in \mathbf{K}$. Pak platí $c_1\alpha_1\alpha_j + \dots + c_m\alpha_m\alpha_j = 0$ pro libovolné $j = 1, \dots, m$. Proto $0 = \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(c_1\alpha_1\alpha_j + \dots + c_m\alpha_m\alpha_j) = c_1 \cdot \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha_1\alpha_j) + \dots + c_m \cdot \mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha_m\alpha_j)$ pro $j = 1, \dots, m$. Tedy lineární kombinace řádků matice B s koeficienty $c_1, \dots, c_m$ se rovná 0. Protože $\det B = \Delta_{\mathbf{F}/\mathbf{K}}(\alpha_1, \dots, \alpha_m) \neq 0$, jsou řádky matice B lineárně nezávislé a proto $c_1 = \dots = c_m = 0$. Tedy $\alpha_1, \dots, \alpha_m$ jsou lineárně nezávislé nad $\mathbf{K}$ a tvoří bázi $\mathbf{F}$ nad $\mathbf{K}$. $\square$

Označme si nyní

$$A = \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_m \\ \alpha_1^q & \alpha_2^q & \dots & \alpha_m^q \\ \vdots & & & \\ \alpha_1^{q^{m-1}} & \alpha_2^{q^{m-1}} & \dots & \alpha_m^{q^{m-1}} \end{pmatrix} = (\alpha_j^{q^{i-1}})_{i,j}$$

Platí $\mathrm{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha_i\alpha_j) = \alpha_i\alpha_j + \alpha_i^q\alpha_j^q + \dots + \alpha_i^{q^{m-1}}\alpha_j^{q^{m-1}}$. Proto platí $A^T \cdot A = B$ a tedy $\det B = (\det A)^2$.

Důsledek 4.10. *Prvky* $\alpha_1, \dots, \alpha_m$ *tvoří bázi* $\mathbf{F}$ *nad* $\mathbf{K}$ *právě tehdy, když* $\det A \neq 0$.

5. Odmocniny z 1 a cyklotomické polynomy

Definice. Je-li $\mathbf{K}$ libovolné těleso, pak rozkladové rozšíření $\mathbf{K}$ určené polynomem $x^n-1 \in \mathbf{K}[x]$ se nazývá *n-té cyklotomické těleso* nad $\mathbf{K}$ a označuje se $\mathbf{K}^{(n)}$. Množina všech kořenů polynomu x^n-1 v $\mathbf{K}^{(n)}$ se označuje $\mathbf{E}^{(n)}$.

Věta 5.1. *Nechť $n>0$ a $\mathbf{K}$ je těleso charakteristiky p. Pak platí*

(1) *pokud $p \nmid n$, pak $\mathbf{E}^{(n)}$ je cyklická podgrupa řádu n multiplikativní grupy $(\mathbf{K}^{(n)})^*$ tělesa $\mathbf{K}^{(n)}$,*
(2) *pokud $p|n$ a $n=p^l m$, kde $p \nmid m$, pak $\mathbf{K}^{(n)}$ se rovná $\mathbf{K}^{(m)}$ a kořeny polynomu x^n-1 jsou prvky $\mathbf{E}^{(m)}$, každý s násobností p^l.*

Důkaz. (1) Platí, že x^n-1 a nx^n-1 nemají společný kořen v $\mathbf{K}[n]$, tedy jsou v $\mathbf{K}[x]$ nesoudělné a x^n-1 nemá žádný vícenásobný kořen. Tedy $\mathbf{E}^{(n)}$ obsahuje přesně n prvků.

Jsou-li $\xi,\mu \in \mathbf{E}^{(n)}$, pak $(\xi\mu)^n=\xi^n\mu^n=1$. Protože ξ je kořen x^n-1, platí $\xi^n=1$. Proto $(\xi^{-1})^n=1.(\xi^{-1})^n=\xi^n.(\xi^{-1})^n=1^n=1$. Tedy $\mathbf{E}^{(n)}$ je podgrupa $(\mathbf{K}^{(n)})^*$.

Nechť $n=p_1^{l_1}\cdot\ldots\cdot p_t^{l_t}$ rozklad na prvočinitele. Pak pro každé $i=0,\ldots,t$ existuje prvek $a_i \in \mathbf{E}^{(n)}$, pro který platí $a_i^{\frac{n}{p_i}} \neq 1$. Potom prvek $b_i=a_i^{\frac{n}{p_i^{l_i}}}$ má řád $p_i^{l_i}$ a $b_1,\ldots,b_t$ je generátor grupy $\mathbf{E}^{(n)}$.

(2) Platí $x^n-1=(x^m-1)^{p^l}$ v $\mathbf{K}[x]$, odkud už tvrzení snadno plyne.

$\square$

Definice. Nechť $\mathbf{K}$ je těleso charakteristiky p a nechť $p \nmid n$. Pak libovolný generátor $\mathbf{E}^{(n)}$ nazýváme *primitivní n-tá odmocnina z* 1indexprimitivní n-tá odmocnina z 1 nad $\mathbf{K}$.

Poznámka. Je-li ξ generátor $\mathbf{E}^{(n)}$, pak $\mathbf{E}^{(n)}=\{1,\xi,\xi^2,\ldots,\xi^{n-1}\}$. Platí, že ξ^s je také generátor $\mathbf{E}^{(n)}$ právě tehdy, když $\mathrm{NSD}(s,n)=1$. Tedy pokud $p=\operatorname{char}\mathbf{T}$ nedělí n, pak existuje $\varphi(n)$ primitivních n-tých odmocnin z 1 nad $\mathbf{K}$.

Definice. Nechť $\mathbf{K}$ je těleso charakteristiky p, $p \nmid n$ a ξ je primitivní n-tá odmocnina z 1. Pak polynom

$$Q_n(x)=\prod_{\substack{0\le s<n\\ \mathrm{NSD}(s,n)=1}}(x-\xi^s)$$

se nazývá *n-tý cyklotomický polynom* nad $\mathbf{K}$.

Poznámka. Polynom $Q_n(x)$ je nezávislý na výběru ξ, stupeň $Q_n(x)$ je $\varphi(n)$ a koeficienty leží v $\mathbf{K}^{(n)}$.

Věta 5.2. *Nechť $\mathbf{K}$ je těleso charakteristiky p, $n>0$ je celé číslo nesoudělné s p. Pak platí*

(1) $x^n-1=\prod_{d|n}Q_d(x)$
(2) *koeficienty $Q_n(x)$ leží v prvotělese tělesa $\mathbf{K}$. Je-li $p=0$, pak koeficienty $Q_n(x)$ jsou celá čísla.*

V $\mathbf{K}^{(n)}$ platí $x^n-1=\prod_{\xi\in\mathbf{E}^{(n)}}(x-\xi)$

Důkaz. (1) Libovolný prvek $\xi \in \mathbf{E}^{(n)}$ je primitivní d-tá odmocnina z 1 pro nějaké $d|n$. Je tomu tak proto, že každý prvek $\xi \in \mathbf{E}^{(n)}$ má řád d pro nějaké

$d|n$, platí tedy $\xi^d - 1 = 0$. Tedy ξ je d-tá odmocnina z 1 a je primitivní. Takže platí $x - \xi$ dělí $Q_d(x)$ a proto $x^n - 1 = \prod_{d|n} Q_d(x)$.

(2) Budeme postupovat indukcí dle n. Platí,že $Q_1(x) = x - 1$ má koeficienty v prvotělese tělesa $\mathbf{K}$. Nechť tvrzení platí pro všechna $d < n$. Pak z rovnosti $x^n - 1 = \prod_{d|n} Q_d(x)$ spočteme

$$Q_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d<n}} Q_d(x)}$$

Čitatel i jmenovatel zlomku mají koeficienty v prvotělese tělesa $\mathbf{K}$. Pomocí dělení polynomů se zbytkem dostaneme, že i $Q_n(x)$ má koeficienty v prvotělese tělesa $\mathbf{K}$.

V případě $p = 0$ jsou koeficienty $Q_1(x)$ celočíselné. Indukční předpoklad je, že koeficienty $Q_d(x)$ jsou celočíselné pro každé $d < n$. Z rovnosti

$$Q_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d<n}} Q_d(x)}$$

pak vyplývá pomocí indukčního předpokladu, že také koeficienty $Q_n(x)$ celočíselné, neboť každý polynom $Q_d(x)$ pro $d < n$ je monický a v procesu dělení se zbytkem jsou všechny koeficienty stále celočíselné.

□

Poznámka. Ve Věte 5.2 (1), je-li char $\mathbf{K} = 0$, pak je to rozklad na ireducibilní činitele, tj. všechny polynomy $Q_d(x)$ jsou ireducibilní nad $\mathbf{K}$. V tělese nenulové charakteristiky to tak být nemusí.

Příklad. Spočtěte $Q_r(x)$ pro r prvočíslo.

Podle Věty 5.2 (1) dostáváme $x^r - 1 = Q_1(x) \cdot Q_r(x)$. Víme, že $Q_1(x) = x - 1$. Tedy

$$Q_r(x) = \frac{x^r - 1}{x - 1} = x^{r-1} + x^{r-2} + \ldots + x + 1$$

Příklad. Spočtěte $Q_{r^k}(x)$ pro r prvočíslo a k nezáporné celé číslo.

Protože r je prvočíslo, všechny dělitele r^k jsou $r^0 = 1, r^1 = r, r^2, r^3, \ldots, r^{k-1}, r^k$. Podle Věty 5.2 (1) tedy platí

$$x^{r^k} - 1 = Q_1(x) \cdot Q_r(x) \cdot Q_{r^2}(x) \cdot \ldots \cdot Q_{r^{k-1}}(x) \cdot Q_{r^k}(x)$$

Všimněme si, že platí $x^{r^{k-1}} - 1 = Q_1(x) \cdot Q_r(x) \cdot Q_{r^2}(x) \cdot \ldots \cdot Q_{r^{k-1}}(x)$. Tedy

$$Q_{r^k}(x) = \frac{x^{r^k} - 1}{x^{r^{k-1}} - 1} = x^{(r-1).r^{k-1}} + x^{(r-2).r^{k-1}} + \ldots + x^{r^{k-1}} + 1$$

Věta 5.3. *n-té cyklotomické rozšíření tělesa $\mathbf{K}$ je jednoduchým algebraickým rozšířením tělesa $\mathbf{K}$ určeným vhodným ireducibilním polynomem z $\mathbf{K}[x]$.*

Nechť $\mathbf{K} = \mathbf{F}_q$ a $\mathrm{NSD}(q, n) = 1$. Potom se $Q_n(x)$ rozkládá na součin $\frac{\varphi(n)}{d}$ různých monických ireducibilních polynomů téhož stupně d, $\mathbf{K}^{(n)}$ je rozkladové rozšíření tělesa $\mathbf{K}$ určené libovolným ireducibilním faktorem Q_n v $\mathbf{K}[x]$ a $\dim_{\mathbf{K}} \mathbf{K}^{(n)} = d$, kde d je nejmenší kladné přirozené číslo takové, že $q^d \equiv 1 \bmod n$.

Důkaz. Pokud char $\mathbf{K} \nmid n$, vezměme primitivní n-tou odmocninu z 1 a označme ji ξ. Nejmenší podtěleso $\mathbf{K}^{(n)}$ obsahující $\mathbf{K}$ a ξ musí obsahovat všechny prvky $\{1, \xi, \xi^2 \ldots, \xi^{n-1}\}$. Ty jsou navzájem různé a tvoří všechny kořeny polynomu $x^n - 1$.

Tedy polynom $x^n - 1$ se rozkládá na součin lineárních činitelů nad nejmenším podtělesem tělesa $\mathbf{K}^{(n)}$ obsahujícím $\mathbf{K}$ a ξ. Protože $\mathbf{K}^{(n)}$ je rozkladové rozšíření $\mathbf{K}$ určené polynomem $x^n - 1$, platí, že $\mathbf{K}^{(n)}$ je nejmenší podtěleso $\mathbf{K}^{(n)}$ obsahující $\mathbf{K}$ a ξ. Vezměme minimální polynom prvku ξ nad $\mathbf{K}$ a označme jej f. Potom $\mathbf{K}^{(n)}$ je kořenovým rozšířením $\mathbf{K}$ určeným f.

Pokud $p = \operatorname{char} \mathbf{K} \,|\, n$, vezmeme rozklad $n = m \cdot p^l$, kde $p \nmid m$. Pak $\mathbf{K}^{(n)} = \mathbf{K}^{(m)}$, char $\mathbf{K} \nmid m$ a $\mathbf{K}^{(m)}$ je jednoduché algebraické rozšíření $\mathbf{K}$ určené vhodným polynomem podle předchozího odstavce.

Zbývá dokázat druhou část věty. Nechť $\mathbf{K} = \mathbf{F}_q$ a $\mathrm{NSD}(q, n) = 1$. Buď ξ primitivní n-tá odmocnina z 1. Prvek ξ leží v tělese $\mathbf{F}_{q^k}$ právě tehdy, když platí $\xi^{q^k - 1} = 1$, což je ekvivalentní $n | q^k - 1$, tedy $q^k \equiv 1 \bmod n$. Nechť d je nejmenší $k > 0$, pro které to platí. Pak platí $\xi \in \mathbf{F}_{q^d}$ a neleží v žádném vlastním podtělese $\mathbf{F}_{q^d}$. Tedy minimální polynom ξ nad $\mathbf{F}_q$ má stupeň d. Minimální polynom ξ nad $\mathbf{F}_q$ je ireducibilní nad $\mathbf{F}_q$. Protože to platí pro libovolnou primitivní n-tou odmocninu z 1 nad $\mathbf{F}_q$, rozkládá se $Q_n(x)$ na součin ireducibilních polynomů stupně d a těch je $\frac{\varphi(n)}{d}$. □

Příklad. Buď $\mathbf{K} = \mathbf{F}_{11}$. Spočtěte $Q_{12}(x)$. Dále spočtěte nejmenší d, pro které platí $11^d \equiv 1 \bmod 12$.

Podle Věty 5.2 platí

$$x^{12} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_6(x) \cdot Q_4(x) \cdot Q_{12}(x)$$

Z Věty 5.2 taktéž víme, že $Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_6(x) = x^6 - 1$ a $Q_4 = x^2 + 1$. Tedy $x^{12} - 1 = Q_1(x) \cdot Q_2(x) \cdot Q_3(x) \cdot Q_6(x) \cdot Q_4(x) \cdot Q_{12}(x) = (x^6 - 1)(x^2 + 1) \cdot Q_{12}(x) = (x^8 + x^6 - x^2 - 1) \cdot Q_{12}(x)$ a proto

$$Q_{12}(x) = \frac{x^{12} - 1}{x^8 + x^6 - x^2 - 1} = x^4 - x^2 + 1$$

Hledané d spočteme podle Věty 5.3. Platí $\mathrm{NSD}(11, 12) = 1$ a podle Věty 5.3 se $Q_{12}(x)$ rozkládá na součin $\frac{\varphi(12)}{d}$ různých monických polynomů téhož stupně d. Platí $Q_{12}(x) = x^4 - x^2 + 1 = (x^2 + 5x + 1)(x^2 - 5x + 1)$. Jelikož $Q_{12}(x)$ se rozkládá na 2 polynomy stupně 2, je $d = 2$. Platí taky $d = \frac{\varphi(12)}{2} = \frac{4}{2} = 2$. Tedy $\mathbf{F}_{11}^{(12)} = \mathbf{F}_{11^2}$.

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 použit 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 $\mathbf{F}_q = \{0, \xi, \xi^2, \dots, \xi^8\}$.

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 $f(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + x^n$, pak jeho doprovodná matice je matice

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

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

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 považovat 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 $h^q \equiv h \mod f$. 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 $h^q \equiv h \mod f$ 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 $h^q \equiv h \mod f$ a $0 < \deg h < \deg f$, je f-redukující.

Dále se budeme zabývat tím, jak hledat f-redukující polynomy. Použijeme čínskou větu o zbytcích.

Předpokládejme, že $f = f_1 \cdots f_k$ pro navzájem různé ireducibilní polynomy $f_1, \ldots, f_k$ a nechť $\deg f = n$. Zvolíme uspořádanou k-tici $(c_1, \ldots, c_k)$ prvků $\mathbf{F}_q$. Podle čínské věty o zbytcích existuje právě jeden polynom $h(x) \in \mathbf{F}_q[x]$ stupně menšího než n takový, že $h(x) \equiv c_i \mod f_i(x)$ pro všechna $i = 1, \ldots, k$. Pak $h^q(x) \equiv c_i^q = c_i \equiv h(x) \mod f_i(x)$ pro všechna $i = 1, \ldots, k$, tedy $f_i(x) | h^q(x) - h(x)$ pro všechna $i = 1, \ldots, k$. Protože jsou $f_1, \ldots, f_k$ po dvou nesoudělné, platí $f(x) = f_1(x) \cdots f_k(x) | h^q(x) - h(x)$.

Je-li $h(x)$ libovolný polynom stupně menšího než n, pak podle Věty 7.1 platí $f(x) = \prod_{c \in \mathbf{F}_q} \mathrm{NSD}(f(x), h(x) - c)$. Pro libovolné $i = 1, \ldots, k$ platí $f_i(x) | f(x) = \prod_{c \in \mathbf{F}_q} \mathrm{NSD}(f(x), h(x) - c)$. Protože $f_i(x)$ je ireducibilní v $\mathbf{F}_q[x]$, existuje $c_i \in \mathbf{F}_q$ takový, že $f_i(x) | \mathrm{NSD}(f(x), h(x) - c_i)$. Tedy $f_i(x) | h(x) - c_i$ a proto $h(x) \equiv c_i \mod f_i(x)$. Z jednoznačnosti existence takového polynomu $h(x)$ (t.j. stupně menšího než n a kongruentního s konstantou c_i modulo $f_i(x)$ pro $i = 1, \ldots, k$), která je dána čínskou větou o zbytcích, pak plyne, že počet polynomů $h(x)$, pro které platí $h^q(x) \equiv h(x) \mod f(x)$ a $\deg h < n$, je přesně q^k.

Jak tedy budeme postupovat? Předchozí odstavec a následující tvrzení nám dávají návod na algoritmus, který se nazývá *Berlekampův algoritmus*. Nejprve spočítáme $x^{jq} \bmod f(x)$ pro $j = 0, \dots, n-1$. Platí $x^{jq} \bmod f(x) = \sum_{i=0}^{n-1} b_{ij} x^i$, kde $b_{ij} \in \mathbf{F}_q$. Označme $B = (b_{ij})$ (čtvercová matice řádu n).

Lemma 7.2. *Polynom $h(x) = a_0 + a_1 x + \dots + a_{n-1} x^{n-1}$ je řešením rovnice $h^q(x) \equiv h(x) \bmod f(x)$ právě když platí*

$$B \cdot \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix},$$

neboli $(B - I) \cdot \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = 0.$

Důkaz. Platí $B \cdot \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix}$ právě tehdy, když $a_i = \sum_{j=0}^{n-1} b_{ij} \cdot a_j$ pro každé $i = 0, \dots, n-1$ (z násobení matic). To je právě tehdy, když $h(x) = \sum_{i=0}^{n-1} a_i x^i = \sum_{i=0}^{n-1} (\sum_{j=0}^{n-1} b_{ij} a_j) \cdot x^i = \sum_{j=0}^{n-1} a_j \sum_{i=0}^{n-1} b_{ij} x^i \equiv \sum_{j=0}^{n-1} a_j x^{jq} = \sum_{j=0}^{n-1} a_j^q x^{jq} = (\sum_{j=0}^{n-1} a_j x^j)^q = h^q(x) \bmod f(x)$ □

Stačí nám pak najít nějakou bázi nulového prostoru matice $(B - I)$. Jeden prvek je $(1, 0, \dots, 0)$, tomu odpovídá $h_1(x) = 1$. Doplníme ho do báze nulového prostoru a dostaneme tak další polynomy $h_2(x), \dots, h_k(x)$.

Lemma 7.3. *Jsou-li f_1, f_2 dva různé ireducibilní faktory $f(x)$, pak existuje polynom $h_j(x)$ pro $j = 2, \dots, k$ takový, že v součinu $\prod_{c \in \mathbf{F}_q} \mathrm{NSD}(f(x), h_j(x) - c)$ polynomy $f_1(x)$ a $f_2(x)$ dělí různé činitele.*

Důkaz. Platí, že $h_1(x) = 1$, tj. $h_1(x) \equiv 1 \bmod f_1(x)$ a také $h_1(x) \equiv \bmod f_2(x)$. Předpokládejme dále, že $h_j(x) \equiv c_{j1} \bmod f_1(x)$, $h_j(x) \equiv c_{j2} \bmod f_2(x)$ a $c_{j1} = c_{j2}$ pro každé $j = 2, \dots, k$. Pak libovolný polynom $h(x) \in \mathbf{F}_q[x]$ stupně menšího než n, pro který platí $h(x)^q \equiv h(x) \bmod f(x)$ lze vyjádřit jako lineární kombinaci

$$h(x) = \sum_{j=1}^{k} a_j h_j(x)$$

pro nějaké koeficienty $a_j \in \mathbf{F}_q$. Pak ale platí $h(x) \equiv \sum_{j=1}^{k} a_j c_{j1} \bmod f_1(x)$ a $h(x) \equiv \sum_{j=1}^{k} a_j c_{j2} \bmod f_2(x)$. Označíme-li $c = \sum_{j=1}^{k} a_j c_{j1} \in \mathbf{F}_q$ pak $h(x) \equiv c \bmod f_1(x)$ a $h(x) \equiv c \bmod f_2(x)$. To je ale ve sporu s tím, že podle čínské věty o zbytcích existuje polynom $h(x) \in \mathbf{F}_q[x]$ stupně menšího než n, pro který platí $h(x) \equiv 0 \bmod f_1(x)$, $h(x) \equiv 1 \bmod f_2(x)$ a $h(x)^q \equiv h(x) \bmod f(x)$. □

Příklad. Rozložte polynom $f(x) = x^8 + x^6 + x^4 + x^3 + 1 \in \mathbf{F}_2[x]$ pomocí Berlekampova algoritmu.

Řešení:

Máme $q = 2$ a $n = \deg f = 8$. Platí $f' = 8x^7 + 6x^5 + 4x^3 + 3x^2 = x^2$ a $\mathrm{NSD}(f, f') = 1$. Tedy $f(x)$ nemá vícenásobné činitele.

Spočteme x^{jq} pro $j = 0, \dots, n-1$.

$$\begin{aligned}
x^0 &\equiv 1 \bmod f(x)\\
x^2 &\equiv x^2 \bmod f(x)\\
x^4 &\equiv x^4 \bmod f(x)\\
x^6 &\equiv x^6 \bmod f(x)\\
x^8 &\equiv x^6 + x^4 + x^3 + 1 \bmod f(x)\\
x^{10} &\equiv x^6 + x^4 + x^3 + 1 + x^6 + x^5 + x^2 = x^5 + x^4 + x^3 + x^2 + 1 \bmod f(x)\\
x^{12} &\equiv x^7 + x^6 + x^5 + x^4 + x^2 \bmod f(x)\\
x^{14} &\equiv x^5 + x^4 + x^3 + x + 1 \bmod f(x)
\end{aligned}$$

Z toho dostáváme matici

$$B = \begin{pmatrix}
1 & 0 & 0 & 0 & 1 & 1 & 0 & 1\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1\\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 0\\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 1\\
0 & 0 & 1 & 0 & 1 & 1 & 1 & 1\\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1\\
0 & 0 & 0 & 1 & 1 & 0 & 1 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{pmatrix}$$

Dále spočteme

$$B - I = \begin{pmatrix}
0 & 0 & 0 & 0 & 1 & 1 & 0 & 1\\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 1\\
0 & 1 & 1 & 0 & 0 & 1 & 1 & 0\\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 1\\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 1\\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1\\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1
\end{pmatrix} \sim \begin{pmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 1\\
0 & 1 & 1 & 0 & 0 & 1 & 1 & 0\\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 1\\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 1\\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 1\\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1\\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1
\end{pmatrix} \sim$$

$$\sim \begin{pmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 1\\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 1\\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 1\\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 1\\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 1\\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1\\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix} \sim \begin{pmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 1\\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 1\\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 1\\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 1\\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

Báze nulového prostoru je tedy $(1, 0, 0, 0, 0, 0, 0, 0), (0, 1, 1, 0, 0, 1, 1, 1)$.

Tedy $h_2(x) = x + x^2 + x^5 + x^6 + x^7$. Platí $\mathrm{NSD}(f(x), h_2(x)) = x^6 + x^5 + x^4 + x + 1$ a $\mathrm{NSD}(f(x), h_2(x) - 1) = x^2 + x + 1$.

Příklad. Rozložte polynom $f(x) = x^4 + 1 \in \mathbf{F}_3[x]$ na ireducibilní činitele.

Řešení:

Máme $q = 3$ a $n = \deg f = 4$. Platí $f'(x) = x^3$ a $\mathrm{NSD}(f(x), f'(x)) = 1$. Tedy $f(x)$ nemá vícenásobné činitele.

Spočteme $x^{jq} \bmod f(x)$ pro $j = 0, \dots, n-1$.

$x^0 \equiv 1 \bmod f(x)$
$x^3 \equiv x^3 \bmod f(x)$
$x^6 \equiv 2x^2 \bmod f(x)$
$x^9 \equiv x \bmod f(x)$
Dostáváme tedy matici

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Gaussovou eliminací ji přivedeme do odstupňovaného tvaru:

$$B - I = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Báze nulového prostoru je např. $(1,0,0,0),(0,1,0,1)$. Dostáváme tedy $h_2(x) = x + x^3$. Platí $f(x) = \prod_{c \in \mathbf{F}_3} \mathrm{NSD}(f(x), h_2(x) - c)$, tedy spočteme
$c = 0$, pak $\mathrm{NSD}(x^4 + 1, x^3 + x) = 1$
$c = 1$, pak $\mathrm{NSD}(x^4 + 1, x^3 + x - 1) = x^2 + 2x + 2$
$c = 2$, pak $\mathrm{NSD}(x^4 + 1, x^3 + x - 2) = x^2 - 2x + 2$
a $f(x) = (x^2 + 2x + 2) \cdot (x^2 - 2x + 2)$.

Co však dělat, je-li $q >> n$? V tom případě bude $\mathrm{NSD}(f(x), h(x) - c) = 1$ pro většinu $c \in \mathbf{F}_q$. Budeme postupovat podobně jako předtím. Začneme Berlekampovým algoritmem a řešíme soustavu $(B - I)x = 0$, najdeme bázi $h_1(x) = 1, h_2(x), \ldots, h_k(x)$. Buď $h(x)$ jeden z těchto polynomů a $f(x) = \prod_{c \in \mathbf{F}_q} \mathrm{NSD}(f(x), h(x) - c)$. Označme $C = \{c \in \mathbf{F}_q; \mathrm{NSD}(f(x), h(x) - c) \neq 1\}$. Potom platí rovnost $f(x) = \prod_{c \in C} \mathrm{NSD}(f(x), h(x) - c)$. Odtud plyne, že $f(x) | \prod_{c \in C}(h(x) - c)$. Označme $G(y) = \prod_{c \in C}(y - c)$. Pak $f(x) | G(h(x))$.

Věta 7.4. *Mezi všemi polynomy $G(y) \in \mathbf{F}_q[y]$, pro které platí $f(x)|G(h(x))$, má monický polynom $G(y)$ nejmenší stupeň.*

Důkaz. Označme $\{0\} \neq J = \{g(y) \in \mathbf{F}_q[y]; f(x)|g(h(x))\} \subseteq \mathbf{F}_q[y]$. Snadno se ověří, že J je ideál v $\mathbf{F}_q[y]$. Jsou-li $g_1(y), g_2(y) \in J$, pak $f(x)|g_1(h(x))$, $f(x)|g_2(f(x))$ a tedy i $f(x)|(g_1 - g_2)(h(x))$. Je-li $k(y) \in \mathbf{F}_q[y]$, pak také $f(x)|k(h(x)) \cdot g_1(h(x))$.

Jelikož platí, že okruh $\mathbf{T}[x]$ je obor integrity hlavních ideálů pro libovolné těleso $\mathbf{T}$, je $\mathbf{F}_q[y]$ obor integrity hlavních ideálů. Proto existuje $G_0(y) \in J$ takový, že všechny polynomy v J jsou násobkem $G_0(y)$. $G_0(y)$ je monický polynom nejmenšího stupně v J. Speciálně $G_0(y)|G(y) = \prod_{c \in C}(y - c)$, tedy $G_0(y) = \prod_{c \in C_1}(y - c)$ pro nějaké $C_1 \subseteq C$. Protože $f(x)|G_0(h(x)) = \prod_{c \in C_1}(h(x) - c)$, platí $f(x) = \prod_{c \in C_1} \mathrm{NSD}(f(x), h(x) - c)$ a odtud plyne $C_1 = C$ a $G_0(y) = G(y)$. □

Jak tuto větu využít? Označme $m = |C|$. Pak $G(y) = \prod_{c \in C}(y - c) = \sum_{j=0}^{m} b_j y^j$ pro nějaké koeficienty $b_0, b_1, \ldots, b_{m-1}$ a $b_m = 1$. Dále platí $f(x)|G(h(x)) = \sum_{j=0}^{m} b_j h^j(x)$. Proto platí $0 \equiv G(h(x)) \bmod f(x) = (\sum_{j=0}^{m} b_j h^j(x)) \bmod f(x) = \sum_{j=0}^{m} b_j (h^j(x) \bmod f(x))$ a tedy platí $0 = \sum_{j=0}^{m} b_j (h^j(x) \bmod f(x))$.

Z vlastností $G(y)$ (přesněji řečeno z vlastnosti, že $G(y)$ je polynom nejmenšího stupně takový, že $f(x)|G(h(x)))$plyne, že posloupnost polynomů $1 = h^0(x) \bmod$

$f(x), h(x) = h^1(x) \bmod f(x), h^2(x) \bmod f(x), \dots, h^{m-1}(x) \bmod f(x)$ je lineárně nezávislá. Dále z rovnosti $f(x) = \prod_{c\in C} \mathrm{NSD}(f(x), h(x) - c)$ plyne, že $m \le k$, kde k je počet ireducibilních činitelů v rozkladu $f(x)$, protože počet činitelů na úpravě straně poslední rovnosti (každý z nich má stupeň aspoň 1) nemůže být větší než počet různých ireducibilních dělitelů polynomu $f(x)$.

Jak hledáme $G(y)$? Počítáme postupně $h^j(x) \bmod f(x)$ a první index j, pro který platí, že $h^j(x) \bmod f(x)$ je lineární kombinací $h^i(x) \bmod f(x)$ pro $i = 0, \dots, j-1$, se rovná m. Koeficienty této lineární kombinace jsou $b_0, b_1, \dots, b_{m-1}$. Tak dostaneme polynom $G(y)$, najdeme jeho kořeny C a pak dokončíme Berlekampův algoritmus. Berlekampův algoritmus s využitím polynomu $G(y)$ se nazývá *Zassenhausův algoritmus*.

Příklad. Rozložte polynom $f(x) = x^6 - 3x^5 + 5x^4 - 9x^3 - 5x^2 + 6x + 7 \in \mathbf{F}_{23}[x]$ pomocí Zassenhausenova algoritmu.

Řešení:

Máme $n = \deg f = 6$ a $q = 23$. Snadno spočteme, že platí $\mathrm{NSD}(f(x), f'(x)) = 1$.

Začneme počítat Berlekampovým algoritmem. Spočteme $x^{jq} \bmod f(x)$ pro $j = 0, \dots, n-1$. Dostáváme matici

$$B = \begin{pmatrix} 1 & 5 & -10 & 0 & 11 & -3 \\ 0 & 0 & 10 & 7 & 0 & 0 \\ 0 & -1 & 10 & 9 & -4 & -10 \\ 0 & 8 & 0 & -8 & 7 & 9 \\ 0 & -3 & 1 & 10 & 7 & 2 \\ 0 & -10 & -9 & -11 & 2 & -9 \end{pmatrix}$$

Matice $B-I$ má hodnost 3, báze nulového prostoru je např. $h_1 = (1,0,0,0,0,0)$, $h_2 = (0,4,2,1,0,0)$, $h_3 = (0,-2,9,0,1,1)$.

Nyní si vezměme např. $h(x) = h_2(x) = x^3 + 2x^2 + 4x$. Platí

$$\begin{aligned} h^0(x) &\equiv 1 \bmod f(x) \\ h^1(x) &\equiv x^3 + 2x^2 + 4x \bmod f(x) \\ h^2(x) &\equiv 7x^5 + 7x^4 + 2x^3 - 2x^2 - 6x - 7 \bmod f(x) \\ h^3(x) &\equiv -11x^5 - 11x^4 - x^3 - 9x^2 - 5x - 2 \bmod f(x) \end{aligned}$$

Platí $h^3(x) - 5h^2(x) + 11h(x) - 10 \equiv 0 \bmod f(x)$, takže $G(y) = y^3 - 5y^2 + 11y - 10$. Kořeny $G(y)$ jsou $-3, 2 - 6$.

Zbývá spočítat

$\mathrm{NSD}(f(x), x^3 + 2x^2 + 4x + 3) = x - 4$

$\mathrm{NSD}(f(x), x^3 + 2x^2 + 4x - 2) = x^2 - x + 7$

$\mathrm{NSD}(f(x), x^3 + 2x^2 + 4x - 6) = x^3 + 2x^2 + 4x - 6$

8. Výpočet kořenů polynomů nad konečnými tělesy

Buď $f(x) \in \mathbf{F}_q[x]$. Při hledání kořenů polynomu f, které leží v $\mathbf{F}_q$, napřed izolujeme tu část polynomu $f(x)$, která obsahuje lineární dělitele. To uděláme snadno, neboť víme, že každý prvek $a \in \mathbf{F}_q$ je kořenem polynomu $x^q - x \in \mathbf{F}_q[x]$. Každý lineární dělitel polynomu $f(x)$ tak dělí také polynom $x^q - x$ a tedy také $\mathrm{NSD}(f(x), x^q - x)$. Tento největší společný dělitel je tak součinem všech lineárních dělitelů polynomu $f(x)$.

Můžeme tedy od začátku předpokládat, že polynom $f(x) \in \mathbf{F}_q[x]$, jehož kořeny chceme najít, se nad $\mathbf{F}_q$ rozkládá na součin lineárních činitelů.

Budeme se zabývat pouze případem, kdy q se rovná nějakému prvočíslu p. Předpokládáme, že

$$f(x) = \prod_{i=1}^{n}(x - c_i),$$

kde $c_1, \dots, c_n$ jsou navzájem různé prvky $\mathbf{F}_p$. Je-li p malé číslo, pak lze najít kořeny $f(x)$ zkusmo dosazováním, neboli výpočtem hodnot $f(0), f(1), \dots, f(p-1)$.

Pro velké $p > 2$ použijeme následující metodu. Pro $b \in \mathbf{F}_p$ platí

$$f(x-b) = \prod_{i=1}^{n}(x - (b + c_i)) | x^p - x = x(x^{(p-1)/2} + 1)(x^{(p-1)/2} + 1).$$

Pokud je x dělitelem $f(x-b)$, platí $f(-b) = 0$ a našli jsme kořen $f(x)$.

Pokud x není dělitelem $f(x-b)$, platí $f(x) | (x^{(p-1)/2} + 1)(x^{(p-1)/2} + 1)$ a tedy

$$f(x-b) = \mathrm{NSD}(f(x-b), x^{(p-1)/2} + 1) \cdot \mathrm{NSD}(f(x), x^{(p-1)/2} - 1)$$

Dělí-li $f(x-b)$ jednoho z činitelů na pravé straně, pak platí buď $x^{(p-1)/2} \equiv 1 \bmod f(x-b)$ nebo $x^{(p-1)/2} \equiv -1 \bmod f(x-b)$. Pokud

$$x^{(p-1)/2} \not\equiv \pm 1 \bmod f(x-b)$$

pak rovnost $f(x-b) = \mathrm{NSD}(f(x-b), x^{(p-1)/2} + 1) \cdot \mathrm{NSD}(f(x), x^{(p-1)/2} - 1)$ dává netriviální rozklad $f(x-b)$. Dosadíme-li $x + b$ za x, dostaneme netriviální rozklad $f(x)$. V málo pravděpodobném případě, že $x^{(p-1)/2} \equiv \pm 1 \bmod f(x-b)$ prostě zkusíme jiné $b \in \mathbf{F}_p$. Tím dostáváme pravděpodobnostní algoritmus pro nalezení kořenů $f(x) \in \mathbf{F}_p[x]$. To, jak funguje, si ukážeme v následujícím příkladu.

Příklad. Najděte ty kořeny polynomu $f(x) = x^6 - 7x^5 + 3x^4 - 7x^3 + 4x^2 - x - 2 \in \mathbf{F}_{17}$, které leží v $\mathbf{F}_{17}$.
Řešení: Hledané kořeny polynomu $f(x)$ jsou právě kořeny polynomu $g(x) = \mathrm{NSD}(f(x), x^{17} - x)$. Eukleidovým algoritmem zjistíme, že $g(x) = x^4 + 6x^3 - 5x^2 + 7x - 2$. Při hledání kořenů $g(x)$ budeme postupovat způsobem uvedený před příkladem.

Napřed zvolíme $b = 0$. Přímým výpočtem zjistíme, že

$$x^{(p-1)/2} = x^8 \equiv 1 \bmod g(x)$$

takže tato volba b nedává netriviální rozklad $g(x)$. Zvolíme tedy $b = 1$. Pak $g(x-1) = x^4 + 2x^3 - 3x - 2$ a $x^{(p-1)/2} = x^8 \equiv -4x^3 - 7x^2 + 8x - 5 \bmod g(x-1)$, takže volba $b = 1$ nám dává netriviální faktorizaci $g(x-1)$. Platí

$$\mathrm{NSD}(g(x-1), x^8 + 1) = \mathrm{NSD}(x^4 + 2x^3 - 3x - 2, -4x^3 - 7x^2 + 8x - 4) = x^2 - 7x + 4$$

a

$$\mathrm{NSD}(g(x-1), x^8 - 1) = \mathrm{NSD}(x^4 + 2x^3 - 3x - 2, -4x^3 - 7x^2 + 8x - 6) = x^2 - 8x + 8$$

a tedy $g(x-1) = (x^2 - 7x + 4)(x^2 - 8x + 8)$, což vede k částečné faktorizaci

$$g(x) = (x^2 - 5x - 2)(x^2 - 6x + 1) = g_1(x)g_2(x)$$

Abychom rozložili $g_1(x)$ a $g_2(x)$, zkusíme $b = 2$. Platí $g_1(x-2) = x^2 + 8x - 5$ a $x^8 \equiv -8x + 2 \bmod g_1(x-2)$. Spočítáme

$$\mathrm{NSD}(g_1(x-2, x^8+1)) = \mathrm{NSD}(x^2 + 8x - 5, -8x + 3) = x + 6$$

a tedy $g_1(x-2) = (x+6)(x+2)$, a také $g_1(x) = (x+8)(x+4)$.

Pokud jde o $g_2(x)$, platí $g_2(x-2) = x^2 + 7x = x(x+7)$, čili -2 je kořen $g_2(x)$ a $g_2(x) = (x+2)(x-8)$. Zjistili jsme tak, že

$$g(x) = g_1(x)g_2(x) = (x+8)(x+4)(x+2)(x-8)$$

a kořeny $g(x)$ a tedy i $f(x)$ v $\mathbf{F}_{17}$ jsou $-8, -4, -2, 8$.

Pro hledání kořenů polynomů s koeficienty v konečných tělesech, která nemají prvočíselnou velikost, se používají jiné algoritmy.