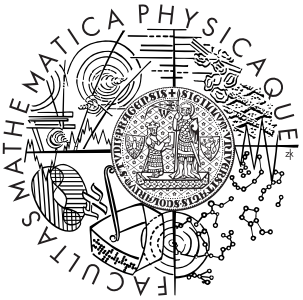
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Jiří Sýkora

Ireducibilní polynomy nad konečnými tělesy

Katedra algebry

Vedoucí bakalářské práce: Mgr. Libor Barto, Ph.D.

Studijní program: Matematika, Obecná matematika

2010

Děkuji vedoucímu této práce Mgr. Liboru Bartovi, Ph.D. za jeho užitečné rady a trpělivost.

Prohlašuji, že jsem svou bakalářskou práci napsal samostatně a výhradně s použitím citovaných pramenů. Souhlasím se zapůjčováním práce a jejím zveřejňováním.

V Praze dne 2. srpna 2010 Jiří Sýkora

Obsah

Název práce: Ireducibilní polynomy nad konečnými tělesy
Autor: Jiří Sýkora
Katedra (ústav): Katedra algebry
Vedoucí bakalářské práce: Mgr. Libor Barto, Ph.D.
e-mail vedoucího: Libor.Barto@mff.cuni.cz

Abstrakt: V předložené práci studujeme polynomy nad konečnými tělesy. Zaměřujeme se především na ireducibilní polynomy, jejich vlastnosti a metody konstrukce. Nejprve zavádíme pojmy jako řád polynomu, primitivní polynom, trojčlen či cyklotomický polynom a uvádíme je do souvislosti s ireducibilními polynomy. Kromě základních vět dokazujeme cvičení, která popisují složitější chování těchto objektů. Dále využíváme Möbiovu inverzní formuli a její důsledky, což nám například umožní odhadnout počet ireducibilních polynomů. Nakonec se zabýváme konstrukcí ireducibilních polynomů pomocí faktorizace i jiných metod a také ukazujeme, jak je možno sestrojit primitivní polynomy. Tyto metody demonstrujeme na cvičeních. Podáváme také přehled publikovaných algoritmů pro konstrukci ireducibilních polynomů.

Klíčová slova: ireducibilní polynom, konečné těleso, primitivní polynom

Title: Irreducible polynomials over finite fields
Author: Jiří Sýkora
Department: Department of Algebra
Supervisor: Mgr. Libor Barto, Ph.D.
Supervisor's e-mail address: Libor.Barto@mff.cuni.cz

Abstract: In this paper we study polynomials over finite fields. We focus especially on irreducible polynomials, their properties and methods of construction. First, we introduce terms like order of a polynomial, primitive polynomial, trinomial or cyclotomic polynomial and their relations to irreducible polynomials. In addition to the presented basic theorems we proof exercises that describe more complex behaviour of these terms. Next, we use Möbius inversion formula and its corollaries, which enables us, for example, to estimate the number of irreducible polynomials. Finally, we concentrate on the construction of irreducible polynomials using the factorization of cyclotomic polynomials and other methods. We also show, how to construct primitive polynomials. We demonstrate these methods on exercises. We aslo present some published algorithms for finding irreducible polynomials.

Keywords: irreducible polynomial, finite field, primitive polynomial

Kapitola 1

Úvod

1.1 Několik slov úvodem

Tato práce se, jak už sám název napovídá, zabývá ireducibilními polynomy nad konečnými tělesy. Vychází z knihy [1], především její třetí kapitoly, odkud je převzata většina teorie. Věty a tvrzení uvádíme bez důkazu, pro jejich možné dohledání je vždy v závorce uvedeno číslo odpovídajícího tvrzení v [1], případně několika tvrzení jejichž spojením naše věta vznikla. Naším cílem je ukázat některé vlastnosti polynomů nad konečnými tělesy. Prezentujeme pojmy jako řád polynomu, primitivní polynom, trojčlen či cyklotomický polynom a ukazujeme jejich souvislost s ireducibilními polynomy. Kromě definic a vět převzatých z [1] obsahuje tato práce cvičení z téže knihy. Jsou dvojího druhu, některá jsou početní, jejich řešení ilustruje metody a postupy popsané ve větách, zbylá naopak rozšiřují teorii. Důkazy a řešení těchto cvičení tvoří významnou část naší práce. Ke konci se pak dostáváme k tématu konstrukce ireducibilních polynomů nad konečnými tělesy, uvádíme některé metody a jejich použití demonstrujeme na cvičeních. Protože výklad teorie konečných těles by zabral příliš místa a není rozhodně cílem této práce, předpokládáme u čtenáře znalost alespoň na úrovni základního kurzu algebry. Tedy očekáváme, že zná definici tělesa, ví, pro jaká q existují q-prvková tělesa, že konečná tělesa se stejným počtem prvků jsou izomorfní, dají se reprezentovat pomocí polynomů a podobně.

V následující kapitole zavedeme pojem řádu polynomu, ukážeme si, jak je možno ho spočítat a jaké má vlastnosti. Dále zavedeme cyklotomické polynomy a ukážeme jejich vztah s řádem. Poté definujeme primitivní polynomy a uvedeme je do souvislosti s předchozími dvěma pojmy. Také se věnujeme Möbiově inverzní formuli, pomocí níž odvodíme některé zajímavé vzorce, které nám umožní odhadnout počet ireducibilních polynomů daného stupně, sestrojit cyklotomické polynomy atd. Na závěr kapitoly se zabýváme trojčleny a jejich nerozložitelností. Třetí kapitola je věnována konstrukci ireducibilních polynomů. Nejprve ukážeme metodu založenou na faktorizaci cyklotomických polynomů, poté vyslovíme dvě věty, které nám umožní konstruovat ireducibilní polynomy z ireducibilních polynomů nižšího stupně. Dále ukážeme, jak zkonstruovat minimální polynom daného prvku. Závěr je věnován přehledu některých algoritmů pro konstrukci ireducibilních polynomů a jejich složitosti.

Kapitola 2

Teoretický základ

2.1 Řád polynomu a cyklotomické polynomy

Důležitým pojmem při zkoumání polynomů nad konečnými tělesy je řád polynomu.

1. Definice. Buď f nenulový polynom nad $\mathbb{F}_q$. Pokud $f(0) \neq 0$, definujeme *řád polynomu* f jako nejmenší k přirozené, že $f(x)$ dělí $x^k - 1$. V opačném případě platí $f(x) = x^l g(x)$, kde $l \in \mathbb{N}, g \in \mathbb{F}_q[x], g(0) \neq 0$. Pak řád polynomu f definujeme jako řád g. Řád f značíme $\mathrm{ord}(f)$.

2. Poznámka. [LN 3.1] Předchozí definice je korektní, protože pro každý polynom $f \in \mathbb{F}_q[x], f(0) \neq 0$ stupně $m \geq 1$ platí, že existuje přirozené číslo $k \leq q^m - 1$, pro něž $f(x)$ dělí $x^k - 1$.

Na několika následujících stránkách uvedeme základní vlastnosti řádu polynomu a také ukážeme, jak je možné řád polynomu spočítat. Nejprve je dobré si uvědomit elementární vlastnost řádu polynomu, která připomíná řád prvku.

3. Lemma. [LN 3.6] *Pro přirozené číslo k a polynom $f \in \mathbb{F}_q[x], f(0) \neq 0$ platí: f dělí $x^k - 1$, právě když $\mathrm{ord}(f)$ dělí k.*

Dále si všimneme, jaký význam má řád pro ireducibilní polynomy.

4. Tvrzení. [LN 3.3] *Řád ireducibilního polynomu f stupně m nad tělesem $\mathbb{F}_q$, který splňuje $f(0) \neq 0$, je roven řádu jeho libovolného kořene v grupě $\mathbb{F}_{q^m}^*$.*

5. Důsledek. [LN 3.4] *Řád ireducibilního polynomu f stupně m nad tělesem $\mathbb{F}_q$ dělí $q^m - 1$.*

Pro reducibilní polynomy toto tvrzení ani jeho důsledek nemusí platit, ale řád reducibilního polynomu dokážeme spočítat z řádů jeho ireducibilních faktorů. To nám ukáží následující tvrzení.

6. Tvrzení. [LN 3.9] *Pokud $f \in \mathbb{F}_q[x]$ je součinem po dvou nesoudělných polynomů nad $\mathbb{F}_q$, pak řád f je roven nejmenšímu společnému násobku jejich řádů.*

7. Tvrzení. [LN 3.8] *Označme p charakteristiku tělesa $\mathbb{F}_q$. Nechť g je ireducibilní polynom nad $\mathbb{F}_q$ řádu k splňující $g(0) \neq 0$ a buď $f = g^m, m \in \mathbb{N}$. Pak* $\mathrm{ord}(f) = kp^l$, *kde $l \in \mathbb{N} \cup \{0\}$ je nejmenší takové, že $p^l \geq m$.*

Z těchto dvou tvrzení bezprostředně vyplývá následující věta pro určení řádu polynomu.

8. Věta. [LN 3.11] *Označme p charakteristiku tělesa $\mathbb{F}_q$. Buď f polynom kladného stupně nad $\mathbb{F}_q$ splňující $f(0) \neq 0$. Buď $f = ag_1^{m_1} \cdots g_n^{m_n}$, $a \in \mathbb{F}_q, m_1, \ldots, m_n \in \mathbb{N}$ rozklad f na součin monických ireducibilních polynomů. Pak* $\mathrm{ord}(f) = kp^l$, *kde k je rovno nejmenšímu společnému násobku čísel* $\mathrm{ord}(g_1), \ldots, \mathrm{ord}(g_n)$ *a $l \in \mathbb{N} \cup \{0\}$ je nejmenší takové, že $p^l \geq \max(m_1, \ldots, m_n)$.*

S pomocí těchto tvrzení vyřešíme a dokážeme několik cvičení, která ilustrují popsané metody, případně popisují další vlastnosti řádu. Nejprve ukážeme použití Věty 8.

3.1 *Určete řád polynomu $(x^2 + x + 1)^5(x^3 + x + 1)$ nad $\mathbb{F}_2$.*

Řešení: Označme $g(x) = (x^2 + x + 1), h(x) = (x^3 + x + 1)$. Snadno se ověří, že g, h jsou ireducibilní polynomy nad $\mathbb{F}_2$. Z Důsledku 5 plyne, že $\mathrm{ord}(g(x))$ dělí $2^2 - 1 = 3$. Je evidentní, že $\mathrm{ord}(g(x)) \geq 3$, tudíž $\mathrm{ord}(g(x)) = 3$. Obdobně $\mathrm{ord}(h(x))$ dělí $2^3 - 1 = 7$ a $\mathrm{ord}(h(x)) > 1$, takže $\mathrm{ord}(h(x)) = 7$. Z Věty 8 dostáváme $\mathrm{ord}(f) = kp^l$, kde $k = 21, p = 2, l = 3$. Tedy $\mathrm{ord}(f) = 21 \cdot 8 = 168$.

Dále se zaměříme na jiné možnosti jak určit řád polynomu, jedná se o speciální případy, kdy všechny kořeny polynomu jsou jednoduché nebo je polynom ireducibilní a podobně.

3.5 *Buď $f \in \mathbb{F}_q[x]$ polynom stupně $m \geq 1$ splňující $f(0) \neq 0$ a předpokládejme, že kořeny $\alpha_1, ..., \alpha_m$ polynomu f v rozkladovém nadtělese polynomu f nad $\mathbb{F}_q$ jsou všechny jednoduché. Dokažte, že* $\mathrm{ord}(f)$ *je roven nejmenšímu přirozenému číslu e takovému, že $\alpha_i^e = 1$ pro všechna $1 \leq i \leq m$.*

Důkaz: Nechť $\mathbb{F}$ je rozkladové nadtěleso polynomu f nad $\mathbb{F}_q$. Pak v $\mathbb{F}[x]$ platí $f(x) = a(x-\alpha_1)\cdots(x-\alpha_m)$. Označme $f_i(x) = x-\alpha_i, h_i(x) = x^{e_i}-1, i = 1, \ldots, m$, kde e_i je nejmenší přirozené číslo takové, že $\alpha_i^{e_i} = 1$. Polynomy f_i jsou ireducibilní, stupně 1. Protože $h_i(\alpha_i) = 0, f_i(\alpha_i) = 0$, platí $f_i \mid h_i$. Zřejmě, pokud $f_i(x) \mid x^k - 1$ pro nějaké k přirozené, pak $\alpha_i^k - 1 = 0$, odkud plyne $k \geq e_i$. Tedy $\mathrm{ord}(f_i) = e_i$. Dle Tvrzení 6 je $\mathrm{ord}(f)$ roven nejmenšímu společnému násobku čísel e_i, kterým je zřejmě číslo e. Toto platí pokud f bereme jako polynom v $\mathbb{F}[x]$. Ovšem, protože $x^e - 1 \in \mathbb{F}_q[x]$, dělí f polynom $x^e - 1$ i nad $\mathbb{F}_q$. Z toho plyne $\mathrm{ord}(f) = e$.

Z předchozího cvičení vyplývá Tvrzení 4, protože kořeny ireducibilních polynomů jsou jednoduché a mají stejný řád. V následujících cvičeních se vyskytují cyklotomické polynomy, proto uvedeme jejich definici a některé základní vlastnosti.

9. Definice. Buď $\mathbb{F}$ těleso charakteristiky p a nechť n je přirozené číslo, $p \nmid n$. Pak definujeme *n-tý cyklotomický polynom* jako

$$Q_n(x) = \prod_{\xi} (x - \xi),$$

kde násobení probíhá přes všechny primitivní n-té odmocniny z jedné. Tento součin probíhá v rozkladovém nadtělese $\mathbb{F}$ určeném polynomem $x^n - 1$, v němž existují primitivní n-té odmocniny z jedné.

10. Poznámka. Je zřejmé, že Q_n je možno ekvivalentně definovat jako

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

kde ξ je libovolná primitivní n-tá odmocnina z jedné.

11. Věta. [LN 2.45, 2.47] (Vlastnosti cyklotomických polynomů) *Buď $\mathbb{F}$ těleso charakteristiky p a nechť n je přirozené číslo, $p \nmid n$. Potom platí:*

(1) $x^n - 1 = \prod_{d|n} Q_d(x)$;
(2) *koeficienty $Q_n(x)$ leží v prvotělese tělesa $\mathbb{F}$. Pokud je $p = 0$, pak jsou koeficienty $Q_n(x)$ celá čísla;*
(3) *pokud $\mathbb{F} = \mathbb{F}_q$, kde $q = p^k$ pro nějaké k přirozené, potom se polynom Q_n rozkládá na součin $\varphi(n)/d$ různých monických ireducibilních polynomů nad $\mathbb{F}$, jejichž stupeň je d. Přitom φ je Eulerova funkce a d je multiplikativní řád q modulo n, tj. nejmenší přirozené číslo s takové, že $q^s \equiv 1 \bmod n$.*

Nyní můžeme dokázat dvě tvrzení o řádu týkající se cyklotomických polynomů.

3.6 *Dokažte, že $\mathrm{ord}(Q_e) = e$ pro všechna e, pro něž je cyklotomický polynom $Q_e \in \mathbb{F}_q[x]$ definován.*

Důkaz: Dle definice je $Q_e = (x - \xi_1) \cdots (x - \xi_{\varphi(e)})$, kde $\xi_1, \ldots, \xi_{\varphi(e)}$ jsou všechny primitivní e-té odmocniny z jedné. Kořeny Q_e jsou jednoduché, a tedy můžeme použít cvičení 3.5. Z něj vyplývá, že $\mathrm{ord}(Q_e) = e$.

3.7 *Nechť f je ireducibilní polynom nad $\mathbb{F}_q$ splňující $f(0) \neq 0$. Pro $e \in \mathbb{N}$ nesoudělné s q dokažte, že $\mathrm{ord}(f) = e$, právě když f dělí cyklotomický polynom Q_e.*

Důkaz: Nechť $\mathrm{ord}(f) = e$. Dle Věty 11 je

$$x^e - 1 = \prod_{d|e} Q_d(x).$$

Taktéž dle Věty 11 se každý z cyklotomických polynomů Q_d rozkládá v součin různých monických ireducibilních polynomů. Můžeme tedy psát

$$x^e - 1 = g_{d_1,1}(x) \cdots g_{d_1,k_1}(x) \cdots g_{d_l,k_l}(x),$$

kde ireducibilní polynomy $g_{d_i,j}, j = 1, \ldots, k_j$ tvoří rozklad polynomu Q_{d_i}. Protože je f ireducibilní a dělí $x^e - 1$, je $f = a g_{d_i,j}$ pro nějaká i, j a $a \in \mathbb{F}_q$. Tedy $f \mid Q_{d_i}$. Z toho, že $Q_{d_i} \mid x^{d_i} - 1$ a $\mathrm{ord}(f) = e$, plyne $d_i = e$.

Nechť naopak f dělí Q_e. Pak $f = ag$, kde $a \in \mathbb{F}_q$ a g je nějaký monický ireducibilní polynom z rozkladu Q_e. Pak f splňuje podmínky cvičení 3.5 a jeho kořeny jsou primitivní e-té odmocniny z jedné, z čehož dostáváme $\mathrm{ord}(f) = e$.

Pomocí těchto tvrzení můžeme odvodit další vlastnosti řádu.

3.9 *Buď $\mathbb{F}_q$ konečné těleso charakteristiky p a buď $f \in \mathbb{F}_q[x]$ polynom kladného stupně splňující $f(0) \neq 0$. Dokažte, že* $\mathrm{ord}(f(x^p)) = p{\cdot}\mathrm{ord}(f(x))$.

Důkaz: Označme $e = \mathrm{ord}(f(x))$ a $k = \mathrm{ord}(f(x^p))$. Pak $f(x)$ dělí $x^e - 1$, tedy $x^e - 1 = f(x)g(x)$ pro nějaký polynom $g \in \mathbb{F}_q[x]$. Zjevně $x^{pe} - 1 = f(x^p)g(x^p)$, a tedy dle Lemmatu 3 k dělí pe; pro spor předpokládejme $k < pe$. Buď K rozkladové nadtěleso polynomu f nad $\mathbb{F}_q$. Pak $f(x) = a(x-\alpha_1)^{b_1} \cdots (x-\alpha_m)^{b_m}$, kde a je vedoucí koeficient f, $\alpha_1, ..., \alpha_m \in K$ jsou kořeny f. Protože i K má charakteristiku p, je zobrazení $\varphi : \alpha \to \alpha^p$ (tzv. Frobeniův) automorfismus K. Pak i zobrazení φ^{-1} je automorfismus K, tudíž

$$f(x^p) = a(x^p-\alpha_1)^{b_1} \cdots (x^p-\alpha_m)^{b_m} = a(x-\varphi^{-1}(\alpha_1))^{pb_1} \cdots (x-\varphi^{-1}(\alpha_m))^{pb_m}.$$

Protože $f(x^p)$ dělí $x^k - 1$, musí mít $x^k - 1$ alespoň jeden vícenásobný kořen. Ovšem pro k, které není dělitelné p, má $x^k - 1$ jen jednoduché kořeny, protože polynom $x^k - 1$ a jeho formální derivace kx^{k-1} nemají žádné společné kořeny. Nutně tedy $k = pl$, pro nějaké $l \in \mathbb{N}, l < e$. Víme, že existuje nekonstantní polynom $h \in \mathbb{F}_q[x]$ takový, že $x^{pl} - 1 = f(x^p)h(x)$. Pokud si uvědomíme, jak se provádí dělení polynomů, snadno nahlédneme, že platí $h(x) = \bar{h}(x^p)$ pro vhodný polynom $\bar{h} \in \mathbb{F}_q[x]$. Tedy $x^{pl} - 1 = f(x^p)\bar{h}(x^p)$, z čehož plyne $x^l - 1 = f(x)\bar{h}(x)$. Z této rovnosti dostáváme $\mathrm{ord}(f(x)) \leq l < e$, což je spor.

3.10 *Buď f ireducibilní polynom v $\mathbb{F}_q[x]$ splňující $f(0) \neq 0$ a ord$(f) = e$ a buď r prvočíslo, které nedělí q. Dokažte: (i) pokud r dělí e, pak každý ireducibilní faktor polynomu $f(x^r)$ v $\mathbb{F}_q[x]$ má řád er; (ii) pokud r nedělí e, pak jeden ireducibilní faktor polynomu $f(x^r)$ v $\mathbb{F}_q[x]$ má řád e a ostatní faktory mají řád er.*

Důkaz: Označme m stupeň polynomu f a p charakteristiku tělesa $\mathbb{F}_q$. Pak dle Důsledku 5 platí $e \mid q^m - 1$, z čehož plyne, že čísla e a q jsou nesoudělná. Tedy z cvičení 3.7 dostáváme $f \mid Q_e$. Tudíž v rozkladovém nadtělese K polynomu f platí $f(x) = a(x-\xi_1)\cdots(x-\xi_m)$, kde $a \in \mathbb{F}_q$ a $\xi_1, \ldots, \xi_m$ jsou primitivní e-té odmocniny z jedné. Pak $f(x^r) = a(x^r-\xi_1)\cdots(x^r-\xi_m)$. Protože i K má charakteristiku p a čísla r, p jsou nesoudělná, mají polynomy $(x^r - \xi_i)$ jen jednoduché kořeny pro $i = 1, \ldots, m$. Tedy zjevně můžeme psát (v rozkladovém nadtělese $f(x^r)$)

$$f(x^r) = a(x-\xi_{1,1})\cdots(x-\xi_{1,r})\cdots(x-\xi_{m,1})\cdots(x-\xi_{m,r}),$$

kde $\xi_{i,j}^r = \xi_i$.

(i) V případě $r \mid e$ stačí dokázat, že prvky $\xi_{i,j}$ jsou primitivní re-té odmocniny z jedné. Pak totiž každý ireducibilní faktor $f(x^r)$ dělí Q_{re}, a tedy (dle cvičení 3.7) má řád re. Víme $\xi_{i,j}^{re} = (\xi_{i,j}^r)^e = \xi_i^e = 1$. Buď k řád prvku $\xi_{i,j}$ a pro spor předpokládejme $k < re$. Pak nutně $k \mid re$. Máme tři možnosti. (a) $k \mid e, k < e$. Pak $\xi_i^k = (\xi_{i,j}^r)^k = (\xi_{i,j}^k)^r = 1^r = 1$, což je spor, protože ξ_i je primitivní e-tá odmocnina z jedné. (b) $k = e = rl$ pro nějaké $l < e$, poněvadž $r \mid e$. Pak $\xi_i^l = (\xi_{i,j}^r)^l = \xi_{i,j}^{rl} = \xi_{i,j}^k = 1$, což je opět spor. (c) $k = rl', l' \mid e, l' < e$. Pak $\xi_i^{l'} = \xi_{i,j}^{rl'} = 1$ a opět dostaneme spor. Tedy $k = re$ a jsme hotovi.

(ii) Nechť $r \nmid e$. Označme $\mathcal{M}$ množinu všech primitivních e-tých odmocnin z jedné a definujme na $\mathcal{M}$ zobrazení φ předpisem $\varphi(\xi) = \xi^r$. Pak je určitě φ zobrazení z $\mathcal{M}$ do $\mathcal{M}$. Ukažme, že je prosté. Nechť $\xi_1^r = \xi_2^r$. Protože r, e jsou nesoudělná, existuje s takové, že $sr \equiv 1 \bmod e$. Pak $\xi_1 = \xi_1^1 = \xi_1^{sr} = (\xi_1^r)^s = (\xi_2^r)^s = \xi_2^{sr} = \xi_2^1 = \xi_2$. Tudíž máme, že φ je prosté, a tedy, protože $\mathcal{M}$ je konečná, je surjektivní. Proto pro každé $i, 1 \leq i \leq m$ existuje právě jedno j, že $\xi_{i,j}$ je primitivní e-tá odmocnina z jedné, označme $\xi_i' = \xi_{i,j}$. Pro $j' \neq j$ má $\xi_{i,j'}$ řád re, což se ukáže obdobně jako v případech (a) a (c) z bodu (i). Buď $g'(x) = (x - \xi_1') \cdots (x - \xi_m')$ a označme h ireducibilní faktor $f(x^r)$ v $\mathbb{F}_q[x]$, který má za kořen ξ_1' Dle Tvrzení 4 je $\mathrm{ord}(h) = e$. Tedy dle cvičení 3.7 $h \mid Q_e$. Z Věty 11 plyne, že $\deg(h) = \deg(f) = m$. A z Tvrzení 4 dostáváme, že všechny kořeny h mají řád e. Tudíž platí $h(x) = bg'(x)$, kde $b \in \mathbb{F}_q$. Tedy právě jeden ireducibilní faktor polynomu $f(x^r)$ má řád e a ostatní mají řád re.

3.11 *Odvoďte z cvičení* 3.10, *že, pokud* $f \in \mathbb{F}_q[x]$ *je polynom kladného stupně splňující* $f(0) \neq 0$ *a* r *je prvočíslo, které nedělí* q, *pak platí* $\mathrm{ord}(f(x^r)) = r{\cdot}\mathrm{ord}(f(x))$.

Důkaz: Z důkazu cvičení 3.10 víme, že kořeny polynomu f jsou jednoduché, tedy $f(x^r) = g_1(x) \cdots g_n(x)$, kde g_i jsou ireducibilní takové, že $g_i \neq g_j$ pro $i \neq j$. Pak dle Tvrzení 6 je řád $f(x^r)$ roven nejmenšímu společnému násobku řádů polynomů $g_1, \ldots, g_n$, který je podle cvičení 3.10 roven $r{\cdot}\mathrm{ord}(f(x))$.

2.2 Primitivní polynomy

Dalším důležitým pojmem, kterým se budeme zabývat, je primitivní polynom.

12. Definice. Polynom stupně m z $\mathbb{F}_q[x]$ nazveme *primitivním polynomem* nad $\mathbb{F}_q$, pokud je minimálním polynomem nad $\mathbb{F}_q$ primitivního prvku tělesa $\mathbb{F}_{q^m}$.

Následující věta uvádí do souvislosti pojem primitivního polynomu a řád polynomu. Víme, že polynom nad $\mathbb{F}_q$ stupně m má řád menší nebo roven $q^m - 1$. Pro primitivní polynomy platí rovnost.

13. Věta. [LN 3.16] *Polynom* $f \in \mathbb{F}_q[x]$ *stupně* m *je primitivní nad* $\mathbb{F}_q$, *právě když* f *je monický,* $f(0) \neq 0$ *a* $ord(f) = q^m - 1$.

Následující cvičení ukazují několik základních vlatností primitivních polynomů a ukazují, jak ověřit, zda je zadaný polynom primitivní.

3.16 *Ukažte, že* $x^6 + x^5 + x^2 + x + 1$ *je primitivní polynom nad* $\mathbb{F}_2$.

Důkaz: Označme zadaný polynom $f(x)$. Zjevně je f monický a $f(0) \neq 0$. Dle Věty 13 stačí ukázat, že $\mathrm{ord}(f) = 2^6 - 1 = 63$. Protože ireducibilní polynomy $x + 1, x^2 + x + 1, x^3 + x + 1, x^3 + x^2 + 1$ nedělí f, je f ireducibilní. Z Důsledku 5 plyne $\mathrm{ord}(f) \mid 63$. Řád polynomu je určitě větší nebo roven jeho stupni a pro polynomy $x^7 - 1, x^9 - 1, x^{21} - 1$ snadno ověříme, že je f nedělí. Tedy $\mathrm{ord}(f) = 63$ a f je primitivní.

3.19 *Buď $f \in \mathbb{F}_q[x]$ monický stupně $m \geq 1$. Dokažte, že f je primitivní nad $\mathbb{F}_q$, právě když f je ireducibilní faktor nad $\mathbb{F}_q$ cyklotomického polynomu $Q_d \in \mathbb{F}_q[x]$, kde $d = q^m - 1$.*

Důkaz: Nechť f je primitivní nad $\mathbb{F}_q$. Pak dle Věty 13 je f monický, $f(0) \neq 0$ a $\mathrm{ord}(f) = q^m - 1 = d$. Tedy $f(x) \mid x^d - 1$. Z Věty 11 víme, že

$$x^d - 1 = \prod_{e|d} Q_e(x).$$

Protože f je ireducibilní, je f ireducibilní faktor některého z polynomů Q_e. Buď to Q_k. Víme, že $k \mid d$. Pokud $k < d$, pak $f(x) \mid x^k - 1$, protože

$$x^k - 1 = \prod_{l|k} Q_l(x).$$

Tedy jsme došli ke sporu, tudíž f je ireducibilní faktor Q_d.

Buď naopak f ireducibilní faktor Q_d. Nechť je α kořen f. Pak je α primitivní $(q^m - 1)$-tá odmocnina z jedné, tedy α je primitivní prvek tělesa $\mathbb{F}_{q^m}$. Polynom f je monický a ireducibilní, tudíž je minimálním polynomem prvku α, a tedy se jedná o primitivní polynom.

3.20 *Určete počet primitivních polynomů stupně m nad $\mathbb{F}_q$.*

Řešení: Z cvičení 3.19 plyne, že stačí určit počet ireducibilních faktorů polynomu Q_d, kde $d = q^m - 1$. Označme ho k. Protože čísla q, d jsou nesoudělná, platí dle Věty 11 $k = \varphi(d)/m = \varphi(q^m - 1)/m$.

2.3 Möbiova inverzní formule a její důsledky

Dále se budeme zaobírat Möbiovou inverzní formulí, což je užitečný nástroj pro určení počtu ireducibilních polynomů, sestrojování cyklotomických polynomů a podobně.

14. Definice. *Möbiova funkce* je zobrazení $\mathbb{N} \to \{-1, 0, 1\}$ definované předpisem

$$\mu(n) = \begin{cases} 1 & \text{pokud n=1} \\ (-1)^k & \text{pokud n je součinem k různých prvočísel} \\ 0 & \text{pokud n je dělitelné čtvercem nějakého prvočísla} \end{cases}$$

15. Věta. [LN 3.24] (Möbiova inverzní formule) *Buď $G = (G, +)$ komutativní grupa a $h, H : \mathbb{N} \to G$ zobrazení. Pak*

$$H(n) = \sum_{d|n} h(d) \quad \textit{pro všechna } n \in \mathbb{N},$$

právě když

$$h(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) H(d) = \sum_{d|n} \mu(d) H\left(\frac{n}{d}\right) \quad \textit{pro všechna } n \in \mathbb{N}.$$

16. Poznámka. [LN 3.24] Pro multiplikativně zapsanou grupu G zřejmě dostáváme:

$$H(n) = \prod_{d|n} h(d) \quad \textit{pro všechna } n \in \mathbb{N},$$

právě když

$$h(n) = \prod_{d|n} H(d)^{\mu\left(\frac{n}{d}\right)} = \prod_{d|n} H\left(\frac{n}{d}\right)^{\mu(d)} \quad \textit{pro všechna } n \in \mathbb{N}.$$

Abychom mohli z Möbiovy inverzní formule odvodit některé vzorce týkající se ireducibilních polynomů, potřebujeme následující lemma.

17. Lemma. [LN 3.20] *Pro každé konečné těleso $\mathbb{F}_q$ a přirozené číslo n platí, že polynom $x^{q^n} - x$ je roven součinu všech monických ireducibilních polynomů nad $\mathbb{F}_q$, jejichž stupeň dělí n.*

Označme $N_q(n)$ počet monických ireducibilních polynomů v $\mathbb{F}_q[x]$ stupně n. Porovnáním stupňů polynomů v Lemmatu 17 dostáváme

$$q^n = \sum_{d|n} d \cdot N_q(d).$$

Použitím Möbiovy inverzní formule pro grupu celých čísel a funkce $H(n) = q^n$, $h(n) = n \cdot N_q(n)$ dostaneme

$$n \cdot N_q(n) = \sum_{d|n} \mu(d) q^{\frac{n}{d}},$$

z čehož plyne následující tvrzení.

18. Tvrzení. [LN 3.25] *Buď $N_q(n)$ jako výše. Pak platí*

$$N_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{\frac{n}{d}}.$$

Obdobným způsobem odvodíme z Lemmatu 17 i toto tvrzení.

19. Tvrzení. [LN 3.29] *Označme $I(q, n; x)$ součin všech monických ireducibilních polynomů v $\mathbb{F}_q[x]$ stupně n. Pak platí*

$$I(q, n; x) = \prod_{d|n} \left(x^{q^d} - x\right)^{\mu\left(\frac{n}{d}\right)}.$$

Möbiovu inverzní formuli můžeme použít i na vztah z části (1) Věty 11 a odvodíme tak tvrzení pro výpočet cyklotomických polynomů.

20. Tvrzení. [LN 3.27] *Pro těleso $\mathbb{F}$ charakteristiky p a přirozené číslo n takové, že $p \nmid n$, platí*

$$Q_n(x) = \prod_{d|n} \left(x^d - 1\right)^{\mu\left(\frac{n}{d}\right)}.$$

Existuje i jiný způsob jak vyjádřit $I(q,n;x)$ pomocí cyklotomických polynomů.

21. Tvrzení. [LN 3.31] *Pro $n > 1$ platí*

$$I(q,n;x) = \prod_m Q_m(x),$$

kde m je dělitel $q^n - 1$ takový, že n je multiplikativní řád q modulo m.

S pomocí těchto tvrzení můžeme dokázat vztah mezi počtem monických ireducibilních polynomů a primitivních polynomů.

3.21 *Pokud $m \in \mathbb{N}$ není prvočíslo, dokažte, že ne každý monický ireducibilní polynom nad $\mathbb{F}_q$ stupně m je primitivním polynomem nad $\mathbb{F}_q$.*

Důkaz: Zjevně pro $m = 1$ je polynom $f(x) = x$ monický ireducibilní, ale není primitivní, protože 0 není primitivním prvkem $\mathbb{F}_q$.

Omezme se tedy na případ $m > 1$. Pak $m = m_1 m_2$, kde $m_1 > 1, m_2 > 1$ jsou dvě, ne nutně různá, přirozená čísla. Pak platí

$$(q^m - 1) = (q^{m_2} - 1) \cdot \left(q^{(m_1-1)m_2} + q^{(m_1-2)m_2} + \cdots + q^{m_2} + 1\right),$$

z čehož plyne, že $(q^m - 1)$ není prvočíslo. Buď $I(q,m;x)$ jako v Tvrzení 21. Pak platí

$$I(q,m;x) = \prod_k Q_k(x),$$

kde součin probíhá přes všechna kladná k taková, že $k \mid q^m - 1$ a m je multiplikativní řád q modulo k, tj. m je nejmenší přirozené číslo, pro které platí $q^m \equiv 1 \mod k$.

Dle cvičení 3.19 víme, že primitivní polynomy stupně m jsou právě ireducibilní faktory polynomu Q_n, kde $n = q^m - 1$. Protože $n \mid q^m - 1$ a m je multiplikativní řád q modulo n, dostáváme

$$I(q,m;x) = Q_n(x) \cdot \prod_k Q_k(x),$$

kde k je jako výše a navíc $k \neq n$. Aby mohl být každý monický ireducibilní polynom stupně m primitivní, muselo by platit $I(q,m;x) = Q_n(x)$. Nám tedy stačí ukázat, že existuje $K < n, K \mid n$ takové, že m je multiplikativní řád q modulo K.

Při důkazu budeme postupovat sporem. Označme k největší vlastní dělitel čísla n. Ten existuje, protože n je složené. Předpokládejme, že existuje $s < m$, které je multiplikativním řádem q modulo k. Platí tedy $q^s - 1 = tk$ pro nějaké $t \in \mathbb{N}$. Protože zřejmě $q^m \equiv 1 \mod k$, musí s dělit m. Poněvadž $s \mid m$, máme $(q^s - 1) \mid (q^m - 1)$. Tudíž $n = (q^m - 1) = a(q^s - 1)$ pro nějaké $a \in \mathbb{N}$. Pak dostáváme $n = atk$. Zjevně $a > 1$, neboť $(q^s - 1) < n$, a také $tk \geq k$. Tedy tk je vlastní dělitel a z maximality k plyne $t = 1$ a $q^s - 1 = k$. Označme $l = m/s$. Platí $kk' = n$, kde k' je nejmenší vlastní dělitel čísla n. Z toho plyne rovnost

$$k' = \frac{n}{k} = \frac{q^m - 1}{q^s - 1} = \frac{q^{ls} - 1}{q^s - 1} = \left(q^{(l-1)s} + \ldots + q^s + 1\right).$$

Protože $l > 1$, máme $k' \geq q^s + 1 > q^s - 1 = k$. Ovšem to je spor a jsme hotovi.

3.22 *Pokud m je prvočíslo, dokažte, že všechny monické ireducibilní polynomy nad $\mathbb{F}_q$ stupně m jsou primitivní nad $\mathbb{F}_q$, právě když $q = 2$ a $2^m - 1$ je prvočíslo.*

Důkaz: Pokud $q = 2$ a $2^m - 1$ je prvočíslo, je dle cvičení 3.20 počet primitivních polynomů nad $\mathbb{F}_q$ stupně m roven $\varphi(q^m - 1)/m = (q^m - 2)/m = (q^m - q)/m$. Počet monických ireducibilních polynomů stupně m je podle Tvrzení 18

$$\frac{1}{m}\sum_{d|m}\mu(d)q^{\frac{m}{d}} = \frac{1}{m}(q^m - q).$$

Tedy každý monický ireducibilní polynom stupně m je primitivní.

Pokud naopak $q \neq 2$, nastávají dvě možnosti. (i) q je liché. Pak $q^m - 1$ je sudé a různé od dvou, tedy není prvočíslo. (ii) $q = 2^k, k > 1$. Potom $q^m - 1 = 2^{km} - 1$, což není prvočíslo (je dělitelné např. $2^k - 1$). Stačí tedy dokázat, že, pokud $q^m - 1$ není prvočíslo, pak ne každý monický ireducibilní polynom stupně m je primitivní. K tomu nám stačí ukázat, že existuje $K < n, K \mid n$ takové, že m je multiplikativní řád q modulo K. To uděláme stejně jako v důkazu cvičení 3.21.

Z Tvrzení 18 odvodíme odhady pro počet monických ireducibilních polynomů daného stupně. Zjevně platí

$$N_q(n) \geq \frac{1}{n}(q^n - q^{n-1} - \cdots - q) = \frac{1}{n}\left(q^n - \frac{q^n - q}{q - 1}\right) > 0.$$

Tedy umíme dokázát, že pro každé konečné těleso a pro každé n přirozené existuje monický ireducibilní polynom stupně n. Ovšem pro $N_q(n)$ lze odvodit i přesnější odhady, jak si ukážeme v následujících dvou cvičeních.

3.26 *Dokažte, že $N_q(n) \leq (1/n)(q^n - q)$, přičemž rovnost nastává, právě když je n prvočíslo.*

Důkaz: Tvrzení 18 říká

$$N_q(n) = \frac{1}{n}\sum_{d|n}\mu(d)q^{\frac{n}{d}}.$$

Pro $n = 1$ dostáváme $N_q(n) = q$, zatímco na pravé straně nerovnosti nám vyjde 0. Nerovnost $q \leq 0$ samozřejmě neplatí, tudíž tvrzení neplatí pro $n = 1$. Dokažme, že platí pro $n \geq 2$. Pokud je n prvočíslo, platí $N_q(n) = (1/n)(q^n - q)$.

Nechť n není prvočíslo. Pokud je n mocnina prvočísla, tj. $n = p^k, k \geq 2$, pak $N_q(n) = (1/n)\left(q^n - q^{(n/p)}\right) < (1/n)(q^n - q)$. Buď tedy $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ prvočíselný rozklad n, kde $m \geq 2$, $p_1, \ldots, p_m$ jsou navzájem různá prvočísla, pro něž platí $p_1 < p_2 < \ldots < p_m$. Označme $r = n/p_1$. Potom r je zjevně největší vlastní dělitel n, a tudíž

$$N_q(n) \leq \frac{1}{n}\left(q^n - q^r + q^{r-1} + \ldots + q - q^{\frac{n}{p_2}}\right) = \frac{1}{n}\left(q^n - q^{\frac{n}{p_2}} + \frac{q^r - q}{q - 1} - q^r\right).$$

Teď už jen stačí si uvědomit, že $q^n - q^{n/p_2} < q^n - q$ a $(q^r - q)/(q - 1) - q^r < 0$ a dostáváme $N_q(n) < (1/n)(q^n - q)$.

3.27 *Dokažte, že*

$$N_q(n) \geq \frac{1}{n}q^n - \frac{q}{n(q-1)}\left(q^{\frac{n}{2}} - 1\right).$$

Důkaz: Stejně jako v předchozím příkladu použijeme Tvrzení 18. Máme

$$N_q(n) = \frac{1}{n}\sum_{d|n}\mu(d)q^{\frac{n}{d}}.$$

Nejprve vyřešme případ $n = 1$. Pak $N_q(n) = q$ a nerovnost zřejmě platí. Buď $n \geq 2$. Označme p nejmenší prvočíslo, které dělí n. Zřejmě $p \geq 2$. Dále buď $r = n/p$. Pak

$$\begin{aligned} N_q(n) &\geq \frac{1}{n}(q^n - q^r - q^{r-1} - \ldots - q) = \frac{1}{n}\left(q^n - \frac{q^r - q}{q-1}\right) \\ &= \frac{1}{n}q^n - \frac{q}{n(q-1)}(q^r - 1) \geq \frac{1}{n}q^n - \frac{q}{n(q-1)}\left(q^{\frac{n}{2}} - 1\right). \end{aligned}$$

Na následujícím příkladu ukážeme výpočet cyklotomických polynomů pomocí Tvrzení 20.

3.34 *Spočítejte cyklotomické polynomy Q_{12} a Q_{30} s využitím explicitního vzorce z Tvrzení 20.*

Řešení: Tvrzení 20 říká, že pro těleso K charakteristiky p a $n \in \mathbb{N}$ nesoudělné s p platí

$$Q_n(x) = \prod_{d|n}(x^d - 1)^{\mu(\frac{n}{d})}.$$

Tedy

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

a

$$\begin{aligned} Q_{30} &= \frac{(x^2-1)(x^3-1)(x^5-1)(x^{30}-1)}{(x-1)(x^6-1)(x^{10}-1)(x^{15}-1)} = \frac{(x+1)(x^{15}+1)}{(x^3+1)(x^5+1)} = \\ &= x^8 + x^7 - x^5 - x^4 - x^3 + x + 1 \end{aligned}$$

2.4 Trojčleny

V této části se budeme zabývat trojčleny a jejich ireducibilitou. Zatímco normálně se trojčlenem rozumí libovolný polynom skládající se ze tří monomů, naše definice je poněkud specifická.

22. Definice. Pro účely této kapitoly rozumíme *trojčlenem* polynom skládající se ze tří monomů, přičemž jedním z nich je konstantní člen.

Nyní se zaměřme na nerozložitelnost některých trojčlenů.

23. Tvrzení. [LN 3.78] *Buď $a \in \mathbb{F}_q$ a označme p charakteristiku $\mathbb{F}_q$. Pak je trojčlen $x^p - x - a$ ireducibilní v $\mathbb{F}_q[x]$, právě když nemá v $\mathbb{F}_q$ žádný kořen.*

Než zformulujeme důsledek tohoto tvrzení musíme zavést pojem stopy polynomu.

24. Definice. Pro $\alpha \in F = \mathbb{F}_{q^m}$ a $K = \mathbb{F}_q$, definujeme *stopu* $\mathrm{Tr}_{F/K}(\alpha)$ prvku α nad K předpisem $\mathrm{Tr}_{F/K}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}$. Pokud je K prvotěleso tělesa F, pak se $\mathrm{Tr}_{F/K}(\alpha)$ nazývá *absolutní stopa* prvku α a značí se $\mathrm{Tr}_F(\alpha)$.

25. Důsledek. [LN 3.79] *Buďte a, p jako v Tvrzení 23. Pak je trojčlen $x^p - x - a$ ireducibilní v $\mathbb{F}_q[x]$, právě když $\mathrm{Tr}_{\mathbb{F}_q}(a) \neq 0$.*

Nyní můžeme dokázat několik cvičení, která se týkají ireducibility trojčlenů.

3.83 *Pro nenulový prvek b prvotělesa $\mathbb{F}_p$ dokažte, že trojčlen $x^p - x - b$ je ireducibilní v $\mathbb{F}_{p^n}[x]$, právě když n není dělitelné p.*

Důkaz: Dle Důsledku 25 je zadaný polynom ireducibilní, právě když $\mathrm{Tr}_{\mathbb{F}_{p^n}}(b) \neq 0$. Dle definice je $\mathrm{Tr}_{\mathbb{F}_{p^n}}(b) = b + b^p + \cdots + b^{p^{n-1}}$. Protože $b \in \mathbb{F}_p$, je $b^p = b$, a tedy i $b^{p^k} = b$ pro libovolné k přirozené. Tudíž $\mathrm{Tr}_{\mathbb{F}_{p^n}}(b) = n \cdot b$, kde výrazem $n \cdot b$ rozumíme součet n prvků b. Zřejmě platí, že $n \cdot b = 0$ (chápáno v $\mathbb{F}_p$), právě když $p \mid n \cdot b$ (chápáno v $\mathbb{Z}$). Poněvadž $b \neq 0$, je $\mathrm{NSD}_{\mathbb{Z}}(p, b) = 1$, z čehož plyne, že $p \mid n \cdot b$, právě když $p \mid n$, čímž je tvrzení dokázáno.

3.84 *Dokažte, že každý polynom tvaru $x^q - ax - b \in \mathbb{F}_q[x]$, kde $a \neq 1$, má kořen v $\mathbb{F}_q$.*

Důkaz: Hledáme řešení rovnice $x^q - ax - b = 0$ v $\mathbb{F}_q$. Máme

$$x^q - ax - b = x(x^{q-1} - a) - b.$$

Buď $\alpha = b/(1-a) \in \mathbb{F}_q$. Protože $a \neq 1$, výraz má smysl, a z nenulovosti b plyne $\alpha \neq 0$. Dosazením α do polynomu dostaneme

$$\frac{b}{1-a}(\alpha^{q-1} - a) - b = \frac{b}{1-a}(1-a) - b = b - b = 0.$$

První rovnost platí, poněvadž pro každý nenulový prvek $\beta \in \mathbb{F}_q$ je $\beta^{q-1} = 1$.

26. Poznámka. Označme polynom z předchozího cvičení f. Pro $a \neq 1$ má f kořen v $\mathbb{F}_q$, tudíž není ireducibilní v $\mathbb{F}_q[x]$. Pro $b = 0$ je $f(x) = x(x^{q-1} - a)$, tedy ani v tomto případě není f ireducibilní v $\mathbb{F}_q[x]$. Nechť $a = 1, b \neq 0$. Pak pro každé $\alpha \in \mathbb{F}_q$ dostáváme

$$f(\alpha) = \alpha^q - \alpha - b = \alpha - \alpha - b = -b \neq 0.$$

Polynom f nemá v $\mathbb{F}_q$ kořen, tudíž může být ireducibilní, ale nemusí. Jeho nerozložitelnost je nutné ověřit nějakým jiným způsobem.

Kapitola 3

Konstrukce ireducibilních polynomů

3.1 Ireducibilní polynomy

Nyní obrátíme pozornost ke konstrukci ireducibilních polynomů. Jednou z možných metod je využití cyklotomických polynomů. Uvědomíme si, že následující cvičení je triviálním důsledkem Věty 11.

3.36 *Dokažte, že cyklotomický polynom Q_n, kde NSD$(n, q) = 1$, je ireducibilní nad $\mathbb{F}_q$,* právě když multiplikativní řád q modulo n je $\varphi(n)$.

Pomocí této vlastnosti dokážeme reducibilitu polynomu Q_{15}.

3.38 *Dokažte, že Q_{15} je reducibilní nad libovolným konečným tělesem, nad nímž je definován.*

Důkaz: Dle cvičení 3.36 stačí ukázat, že multiplikativní řád q modulo 15 je menší než $\varphi(15)$, pro libovolné q nesoudělné s 15. Platí $\varphi(15) = 8$. Dokažme, že pro q nesoudělné s 15 je $q^4 \equiv 1 \bmod 15$. Ovšem $q^4 = \left(q^{\varphi(3)}\right)^2$ a protože NSD$(q, 3) = 1$, Eulerova věta dává $q^4 \equiv 1 \bmod 3$. Obdobně $q^4 = q^{\varphi(5)}$, a tedy $q^4 \equiv 1 \bmod 5$. Pak platí $q^4 \equiv 1 \bmod 15$ a jsme hotovi.

Následující cvičení poskytuje návod jak konstruovat ireducibilní polynomy.

3.42 *Pokud $e \geq 2$, NSD$(e, q) = 1$ a m je multiplikativní řád q modulo e, dokažte, že součin všech monických ireducibilních polynomů v $\mathbb{F}_q[x]$ stupně m a řádu e je roven cyklotomickému polynomu Q_e nad $\mathbb{F}_q$.*

Důkaz: Z Věty 11 víme, že Q_e se rozkládá na součin monických ireducibilních polynomů stupně m. Protože zřejmě nula není primitivní e-tou odmocninou z jedné, platí, že nula není kořenem žádného z těchto polynomů. Pak ale z cvičení 3.7 dostáváme, že řád těchto polynomů je e. Nechť naopak f je monický ireducibilní polynom stupně m a řádu e. Protože $e > 1$ je $f(0) \neq 0$ a z cvičení 3.7 plyne, že f dělí Q_e, tedy je jeho monickým ireducibilním faktorem.

V případě, kdy chceme zkonstruovat ireducibilní polynom stupně m nad tělesem $\mathbb{F}_q$, nám stačí najít přirozené číslo $e \geq 2$ takové, že m je multiplikativní

řád q modulo e, a hledané polynomy dostaneme faktorizací polynomu Q_e, který sestrojíme podle Tvrzení 20. Takto vzniklé polynomy jsou monické, ireducibilní a mají řád e. Speciálně pro e zvolené jako $q^m - 1$ dostaneme primitivní polynomy nad $\mathbb{F}_q$ stupně m.

Jiná metoda konstrukce ireducibilních polynomů je založena na následujících dvou větách.

27. Věta. [LN 3.35] *Nechť $f_1(x), f_2(x), \ldots, f_N(x)$ jsou všechny různé monické ireducibilní polynomy v $\mathbb{F}_q[x]$ stupně m a řádu e a buď $t \geq 2$ přirozené číslo, jehož prvočíselné faktory dělí e, ale ne $(q^m - 1)/e$. Předpokládejme také, že $q^m \equiv 1 \bmod 4$, pokud $t \equiv 0 \bmod 4$. Pak $f_1(x^t), f_2(x^t), \ldots, f_N(x^t)$ jsou všechny různé monické ireducibilní polynomy v $\mathbb{F}_q[x]$ stupně mt a řádu et.*

28. Věta. [LN 3.37] *Nechť $f_1(x), f_2(x), \ldots, f_N(x)$ jsou všechny různé monické ireducibilní polynomy v $\mathbb{F}_q[x]$ lichého stupně m a řádu e. Buď $q = 2^a u - 1$, $t = 2^b v - 1$, kde $a, b \geq 2$ a u a v jsou lichá a všechny prvočíselné faktory čísla t dělí e, ale ne $(q^m - 1)/e$. Buď k menší z čísel a a b. Potom se každý z polynomů $f_j(x^t)$ rozkládá na součin 2^{k-1} monických ireducibilních polynomů $g_{ij}(x)$ v $\mathbb{F}_q[x]$ stupně $mt2^{1-k}$. Tyto polynomy $g_{ij}(x)$, kterých je $2^{k-1}N$, jsou všechny různé monické ireducibilní polynomy v $\mathbb{F}_q[x]$ stupně $mt2^{1-k}$ a řádu et.*

Použití těchto vět ukážeme na následujících příkladech.

3.48 *Najděte všechny ireducibilní polynomy v $\mathbb{F}_2[x]$ stupně 6 a řádu 21 a potom všechny ireducibilní polynomy v $\mathbb{F}_2[x]$ stupně 294 a řádu 1029.*

Řešení: Dle cvičení 3.7 jsou ireducibilní polynomy v $\mathbb{F}_2[x]$ stupně 6 a řádu 21 ireducibilními faktory cyklotomického polynomu $Q_{21}(x)$. Z Tvrzení 20 máme

$$\begin{aligned} Q_{21}(x) &= \frac{(x^{21}-1)(x-1)}{(x^3-1)(x^7-1)} = \frac{x^{14}+x^7+1}{x^2+x+1} = \\ &= x^{12}+x^{11}+x^9+x^8+x^6+x^4+x^3+x+1. \end{aligned}$$

Tento polynom rozložíme na součin dvou ireducibilních polynomů stupně 6. Vyjde

$$x^{12}+x^{11}+x^9+x^8+x^6+x^4+x^3+x+1 = (x^6+x^4+x^2+x+1)(x^6+x^5+x^4+x^2+1).$$

Pro získání polynomů stupně 294 a řádu 1029 použijeme Větu 27, kde $m = 6$, $e = 21$, $t = 49 = 7^2$. Platí, že 7 dělí 21 a 7 nedělí $(2^6-1)/21 = 3$, tedy předpoklady věty jsou splněny. Protože $mt = 294, et = 1029$ dostáváme, že všechny ireducubilní polynomy v $\mathbb{F}_2[x]$ stupně 294 a řádu 1029 jsou $x^{294} + x^{196} + x^{98} + x^{49} + 1$ a $x^{294} + x^{245} + x^{196} + x^{98} + 1$.

3.49 *Najděte všechny monické ireducibilní polynomy v $\mathbb{F}_3[x]$ stupně 3 a řádu 26 a potom všechny monické ireducibilní polynomy v $\mathbb{F}_2[x]$ stupně 6 a řádu 104.*

Řešení: Podobně jako v minulém cvičení nalezneme hledané polynomy faktorizací cyklotomického polynomu $Q_{26}(x)$. Použitím Tvrzení 20 a jednoduchými úpravami dostaneme $Q_{26}(x) = x^{12} - x^{11} + x^{10} - x^9 + x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$.

Tento polynom se nad $\mathbb{F}_3$ rozkládá v součin čtyř ireducibilních polynomů stupně tři. Konkrétně $Q_{26}(x) = (x^3-x+1)(x^3+x^2-x+1)(x^3-x^2+1)(x^3-x^2+x+1)$.

Pro získání polynomů stupně 6 a řádu 104 použijeme Větu 28, kde $m = 3$, $e = 26, a = b = 2, u = v = 1, t = 4 = 2^2, k = 2$. Protože 2 dělí 26 a nedělí $(3^3-1)/26 = 1$, jsou předpoklady věty splněny a hledané polynomy stupně 6 dostaneme rozkladem polynomů $x^{12}-x^4+1, x^{12}+x^8-x^4+1, x^{12}-x^8+1, x^{12}-x^8+x^4+1$. Tedy jsou to polynomy $x^6+x^5-x^4-x^3-1, x^6-x^5-x^4+x^3-1, x^6+x^5-x^4+x^3+x^2-x-1, x^6-x^5-x^4-x^3+x^2+x-1, x^6+x^3+x^2-x-1, x^6-x^3+x^2+x-1, x^6+x^5-x^4-x^3+x^2-x-1, x^6-x^5-x^4+x^3+x^2+x-1$.

Větu 27 lze použít ke konstrukci ireducibilních polynomů určitého stupně poměrně jednoduchým způsobem například takto. Když chceme zkonstruovat ireducibilní polynom stupně k nad tělesem $\mathbb{F}_q$, najdeme si nějaký rozklad čísla $k = tl$. Pokud ireducibilní faktory t dělí $q^l - 1$, stačí nám najít primitivní polynom f stupně l a hledaným polynomem je $f(x^t)$. To platí, protože řád f je $q^l - 1$, a tedy podmínky Věty 27 jsou splněny. Speciálně pro případ $t \equiv 0 \bmod 4$ musíme ověřit platnost podmínky $q^l \equiv 1 \bmod 4$. Stačí nám tedy sestrojit primitivní polynom stupně l. K tomu můžeme použít faktorizaci cyklotomického polynomu, jak bylo vysvětleno výše, nebo jinou metodu, kterou zmíníme později.

Samozřejmě, někdy je tato metoda výhodná a někdy je její přínos malý. Zjevně, pokud chceme sestrojit ireducibilní polynom prvočíselného stupně, tak nám nepomůže. I v některých jiných případech je její užitek nepříliš velký, dosáhneme třeba pouze toho, že t je rovno dvěma, tedy hledáme primitivní polynom poloviční stupně. V případě tělesa $\mathbb{F}_5$ a $k = 49$, pak také není možno tuto metodu použít. Naopak pro těleso $\mathbb{F}_3$ a $k = 160$ nám stačí najít primitivní polynom stupně 4. Platí totiž $160 = 4 \cdot 40$, 40 dělí $3^4 - 1 = 80$, a $3^4 \equiv 1 \bmod 4$. Najdeme tedy primitivní polynom x^4+x+2 a z něj vytvoříme ireducibilní polynom $x^{160}+x^{40}+2$.

Uveďme větu, jež popisuje, jak se chovají ireducibilní polynomy nad rozšířeními těles.

29. Věta. [LN 3.46] *Buď f ireducibilní polynom nad $\mathbb{F}_q$ stupně n. Pro libovolné k přirozené platí, že f se nad $\mathbb{F}_{q^k}$ rozkládá na součin d ireducibilních polynomů stejného stupně n/d, kde $d = NSD(n, k)$.*

30. Důsledek. [LN 3.47] *Ireducibilní polynom nad $\mathbb{F}_q$ stupně n je ireducibilní i nad $\mathbb{F}_{q^k}$, právě když n a k jsou nesoudělná.*

3.2 Minimální a primitivní polynomy

Nyní se zaměříme na hledání minimálních polynomů prvků tělesa. Buď θ takový prvek tělesa $\mathbb{F}_{q^m}$, že $\{1, \theta, \ldots, \theta^{m-1}\}$ tvoří bázi $\mathbb{F}_{q^m}$ nad $\mathbb{F}_q$. Pokud chceme najít minimální polynom f prvku $\beta \in \mathbb{F}_{q^m}$ nad $\mathbb{F}_q$, vyjádříme mocniny $1, \beta, \beta^2, \ldots, \beta^m$ pomocí této báze. Tedy

$$\beta^i = \sum_{j=0}^{m-1} b_{ij}\theta^j \quad \text{pro } 0 \le i \le m.$$

Nechť $f(x) = a_m x^m + \cdots + a_1 x + a_0$. Pak z podmínky $f(\beta) = 0$ dostáváme

$$\sum_{i=0}^{m} a_i b_{ij} = 0 \quad \text{pro } 0 \le j \le m-1.$$

Máme tedy homogenní soustavu m lineárních rovnic o $m+1$ neznámých. Buď $A = (a_{ij})$ matice typu $m \times (m+1)$ taková, že $a_{ij} = b_{j+1,i+1}$. Zjevně se jedná o matici jejíž i-tý sloupec je tvořen zápisem β^{i-1} v dané bázi. Taktéž je zřejmé, že jde o matici naší soustavy. Označme h hodnost matice A. Pak prostor řešení dané soustavy má dimenzi $d = m + 1 - h$. Protože $1 \le h \le m$, platí $1 \le d \le m$. Můžeme tedy položit $a_m = a_{m-1} = \cdots = a_{m-d+2} = 0$ a $a_{m-d+1} = 1$. Ostatní koeficienty polynomu dopočítáme ze soustavy.

Ilustrujme tuto metodu na následujícím cvičení.

3.55 *Buď $\theta \in \mathbb{F}_{64}$ kořen ireducibilního polynomu $x^6 + x + 1$ v $\mathbb{F}_2[x]$. Najděte minimální polynom prvku $\beta = 1 + \theta^2 + \theta^3$ nad $\mathbb{F}_2$.*

Řešení: Napišme si nejprve mocniny β vyjádřené v bázi $1, \theta, \theta^2, \ldots, \theta^5$. Máme

$$\begin{aligned}
\beta^0 &= 1 \\
\beta^1 &= 1 + \theta^2 + \theta^3 \\
\beta^2 &= \theta + \theta^4 \\
\beta^3 &= 1 + \theta + \theta^2 + \theta^3 \\
\beta^4 &= \theta^3 \\
\beta^5 &= 1 + \theta + \theta^3 + \theta^5 \\
\beta^6 &= \theta + \theta^2 + \theta^4.
\end{aligned}$$

Matice A je tedy dána

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

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

Hodnost matice je $h = 6$ a $d = 6 + 1 - 6 = 1$. Zvolme tedy $a_6 = 1$ a dopočtěme ostatní koeficienty. Vyjde $a_5 = 0, a_4 = 1, a_3 = 0, a_2 = 1, a_1 = 1, a_0 = 1$. Minimální polynom β nad $\mathbb{F}_2$ je tedy $x^6 + x^4 + x^2 + x + 1$.

Jiná metoda hledání minimálních polynomů je založena na následující větě.

31. Věta. [LN 3.33] *Buď $\alpha \in \mathbb{F}_{q^m}$. Nechť g je minimální polynom prvku α nad $\mathbb{F}_q$, který má stupeň d. Pak kořeny g jsou prvky $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$, a g je minimální polynom všech těchto prvků nad $\mathbb{F}_q$.*

Z Věty 31 plyne, že pro nalezení minimálního polynomu f prvku $\beta \in \mathbb{F}_{q^m}$ nad $\mathbb{F}_q$ stačí spočítat mocniny $\beta, \beta^q, \ldots, \beta^{q^{d-1}}$, kde d je nejmenší přirozené číslo takové, že $\beta^{q^d} = \beta$. Potom $f(x) = (x-\beta)(x-\beta^q)\cdots(x-\beta^{q^{d-1}})$.

Nakonec si řekneme něco o konstrukci primitivních polynomů. Jednou z možností je faktorizace vhodného cyklotomického polynomu, jak vyplývá ze cvičení 3.42. Druhým způsobem je nalezení primitivního prvku vhodného tělesa a konstrukce jeho minimálního polynomu. Přesněji, pokud chceme sestrojit primitivní polynom stupně m nad $\mathbb{F}_q$, najdeme primitivní prvek tělesa $\mathbb{F}_{q^m}$ a sestrojíme jeho minimální polynom některou z uvedených metod. Prvek $\mathbb{F}_{q^m}$ je primitivní, právě když má v grupě $\mathbb{F}_{q^m}^*$ řád $q^m - 1$. Nechť je $q^m - 1 = k_1 \cdots k_l$ rozklad na součin po dvou nesoudělných přirozených čísel. Pro každé $1 \leq i \leq l$ nalezneme prvek $\alpha_i \in \mathbb{F}_{q^m}^*$ řádu k_i. Poté $\alpha = \alpha_1 \cdots \alpha_l$ má řád $q^m - 1$. Tudíž je α primitivní prvek a sestrojením jeho minimálního polynomu dostaneme požadovaný primitivní polynom.

3.3 Algoritmy pro konstrukci ireducibilních polynomů

Na závěr si řekněme něco o publikovaných algoritmech pro konstrukci ireducibilních polynomů nad konečnými tělesy. V současnosti není znám žádný deterministický polynomiální algoritmus pro sestrojení ireducibilního polynomu stupně n nad tělesem $\mathbb{F}_q$. Polynomiálním algoritmem se zde rozumí algoritmus jehož počet operací je omezen polynomem v n a $\log q$. Existují tedy dva přístupy, některé práce se zabývají nalezením rychlého deterministického algoritmu, ostatní se naopak zaměřují na nalezení co nejrychlejšího pravděpodobnostního algoritmu, který může využívat náhodných bitů. Například v [2] ukázali autoři existenci deterministického polynomiálního algoritmu pro nalezení ireducibilního polynomu daného stupně nad $\mathbb{F}_p$ za předpokladu platnosti rozšířené Riemannovy hypotézy. V [3] představil Victor Shoup několik deterministických algoritmů pro tělesa $\mathbb{F}_p$. Jeden z nich například převádí problém konstrukce ireducibilního polynomu na problém faktorizace polynomů, k čemuž využívá cyklotomické polynomy. Následná faktorizace se poté provede vylepšeným Berlekampovým algoritmem. Celkově algoritmus potřebuje $O(p^{1/2+\varepsilon}n^{3+\varepsilon} + (\log p)^2 n^{4+\varepsilon})$ operací v $\mathbb{F}_p$. Jak Shoup zmiňuje, v praxi se často používají tělesa, kde p je malé, a tudíž i algoritmus se složitostí $p^{1/2}$, tedy exponenciální v $\log p$, není špatný.

Jedna z možných nedeterministických metod je následující. Vezmeme nějaký náhodný monický polynom daného stupně a otestujeme, zdali je ireducibilní. Pokud je, tak jsme hotovi, jinak postup zopakujeme. Z cvičení 3.26 a 3.27 vyplývá, že náhodný monický polynom stupně n je ireducibilní s pravděpodobností přibližně $1/n$. Důležitou částí takovéhoto postupu je ověřování nerozložitelnosti polynomu. Zásadní tedy je mít efektivní test ireducibility. Příklady takovýchto testů je možné nalézt například v [4]. Tato práce pojednává i o algoritmu pro nalezení ireducibilního polynomu, který pracuje se složitostí $O((n^2 \log n + n \log q) \cdot \log n \operatorname{loglog} n)$

operací v $\mathbb{F}_q$. V [5] autoři zmiňují, že všechny známé algoritmy využívající prvočíselné testy mají složitost alespoň kvadratickou v n a zdá se být složité toto zlepšit. Oni sami ukazují postup založený na izogenii eliptických křivek. Jejich algoritmus má složitost $n^{1+o(1)} \cdot (\log q)^{5+o(1)}$. V tomto zápisu představuje $o(1)$ u n funkci, jež konverguje k nule pro n jdoucí do nekonečna, a obdobně $o(1)$ u $\log q$ je funkce konvergující k nule pro q jdoucí do nekonečna.

Literatura

[1] Lidl R., Niederreiter H. (1997): *Introduction to finite fields and their applications*. Second Edition. Cambridge : Cambridge University Press.

[2] Adleman L. M., Lenstra H. W. (1986): Finding irreducible polynomials over finite fields. *Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing, 28-30 May 1986, Berkeley, California, USA*, 350-355.

[3] Shoup V. (1990): New algorithms for finding irreducible polynomials over finite fields. *Mathematics of Computation* **54**, 435-447.

[4] Shoup V. (1994): Fast construction of irreducible polynomials over finite fields. *Journal of Symbolic Computation* **17**, 371-391.

[5] Couveignes J.-M., Lercier R. (2009): Fast construction of irreducible polynomials over finite fields. *arXiv.org e-Print archive* [online]. Ithaca (NY) : Cornell University Library, update date 2009-09-11 [cit. 2010-07-23]. Dostupný z WWW: `http://arxiv.org/PS_cache/arxiv/pdf/0905/0905.1642v2.pdf`.