Středoškolská odborná činnost

Obor SOČ: 1. Matematika a statistika

Generování pseudonáhodné posloupnosti nad konečným tělesem pomocí Möbiovy funkce

Václav Zvoníček

Kraj: Jihomoravský

Brno 2020

Středoškolská odborná činnost

Obor SOČ: 1. Matematika a statistika

Generování pseudonáhodné posloupnosti nad konečným tělesem pomocí Möbiovy funkce

A Pseudorandom Sequence Generated over a Finite Field Using the Möbius Function

Autor:	Václav Zvoníček
Škola:	Gymnázium Brno, třída Kapitána Jaroše
Kraj:	Jihomoravský
Obor:	Matematika a statistika
Konzultant:	Mgr. Petr Pupík

Prohlášení

Prohlašuji, že jsem svou práci SOČ vypracoval samostatně a použil jsem pouze podklady (literaturu, projekty, SW atd.) uvedené v seznamu vloženém v práci SOČ.

Prohlašuji, že tištěná a elektronická verze soutěžní práce SOČ jsou shodné.

Nemám závažný důvod proti zpřístupňování této práce v souladu se zákonem § 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) v platném znění.

V _____ dne _____ podpis _____

Poděkování

Velice rád bych poděkoval Mgr. Petrovi Pupíkovi za jeho trpělivost při pomoci sepsat moji poslední středoškolskou odbornou práci, která mi jistě pomůže při následujícím studiu na univerzitě. Taktéž bych rád věnoval poděkování profesorovi RNDr. Radanovi Kučerovi, DSc. za velice užitečné připomínky k mé práci.

Abstrakt

Cílem této práce je vytvořit pseudonáhodnou posloupnost nad konečným tělesem pomocí Möbiovy funkce. U posloupností budou zkoumány jejich vlastnosti a testována náhodnost jejich členů. V teoretickém úvodu se nejprve seznámíme s Möbiovou funkcí, následovat bude teorie o tělesech zahrnující jejich základní vlastnosti nebo rozšíření těles až se dostaneme ke konečným tělesům. Kromě uvedené pseudonáhodné posloupnosti se v práci seznámíme i s jinými, například lineárním modulárním generátorem a posuvným registrem.

Ve vlastní části práce, po vygenerování několika pseudonahodných posloupností pomocí Möbiovy funkce, jsem došel k závěru, že je vhodné zvolit generování nad tělesem $\mathbb{F}_{3^n}$. Získáme tak posloupnost čísel -1,0,1, kde každé z těchto čísel je zastoupeno ve stejném počtu, navíc pomocí autokorelace jsem potvrdil nepravidelnost pořadí členů posloupnosti. Na konec práce jsem ještě dodal důkaz, že druhá polovina uvedené posloupnosti nad $\mathbb{F}_{3^n}$ je shodná s tou první až na znaménko členů.

Klíčová slova

konečné těleso, primitivní polynom, pseudonáhodná posloupnost, autokorelace

Abstract

The aim of this paper is to create a pseudorandom sequence over a finite field using the Möbius function. The sequences are then to be examined, their properties and mainly their randomness tested. The Möbius function is introduced in the theoretical preface along with the theory of algebraic fields in general and more specifically the theory of finite fields. The paper, apart from the aforementioned sequences, also touches upon subjects like linear congruential generators and shift registers.

In the main part of the paper, after generating a number of sequences using the Möbius function, I reach the conclusion, that it is preferable to generate sequences in fields of the form $\mathbb{F}_{3^n}$, thereby obtaining a sequence of the numbers -1,0,1, each of which appear in the same amounts. I also verify the sequences' randomness using autocorrelation and prove that the second half of any sequence in $\mathbb{F}_{3^n}$ is the same as the first, but for the sign of the terms.

Key words

finite field, primitive polynomial, pseudorandom sequence, autocorrelation

Obsah

Úvod

Konečná tělesa nás doprovází v mnoha situacích, ať už se jedná o matematiku nebo běžné každodenní záležitosti. Jistě nejznámější uplatnění konečných těles nalezneme u opravných kódů a dešifrování informací, například zpráva poslaná z vesmíru musí být poslaná tak, aby bylo její dešifrování na Zemi proveditelné. Kromě této aplikace jsou konečná tělesa užitečná také při generování pseudonáhodných posloupností, tj. posloupností, jejichž členy je náročné odhadnout. Řešit otázku náhodnosti představuje obtížný problém, kterým se nezabývá pouze matematika, ale také filosofie. V této práci se na problém náhodnosti budeme dívat z pohledu matematického, ukážeme si několik pseudonáhodných posloupností, ale především se budeme věnovat pseudonáhodné posloupnosti generované nad konečným tělesem pomocí Möbiovy funkce. Jedná se totiž o poměrně nový pohled na generování posloupnosti, jenž pochází z roku 2016. V této práci jsem vytvořil posloupnosti a zkoumal jejich vlastnosti, zejména jak jsou její členy náhodné.

Kapitola 1

Möbiova funkce

Představme si funkci f, jejíž předpis závisí na jiné funkci g, například tak, že se sčítají nebo násobí různé hodnoty g. Našim přáním je funkci g vyjádřit v závislosti na f, tedy vyjádřit jakousi *inverzní formuli*. V této kapitole se podíváme na *Möbiovu funkci* a s ní spojenou *Möbiovu inverzní formuli*, která nám řeší zmíněný problém pro jisté funkce. Porozumění Möbiově funkci bude navíc klíčové v jejím uplatnění jakožto generátoru pseudonáhodných posloupností, což je hlavním tématem kapitoly 6. Nejdříve si však představíme základní tvrzení související s Möbiovou funkcí a využijeme ji při určování hodnot Eulerovy funkce. Na konci kapitoly si ukážeme její alternativní výpočet.

1.1 Möbiova funkce

Definice 1.1.1. Möbiovu funkci $\mu : \mathbb{N} \mapsto \mathbb{Z}$ definujeme předpisem

$$\mu(n) = \begin{cases} 1 & \text{pro } n = 1, \\ 0 & \text{pokud } \exists d \in \mathbb{N}, d > 1 : d^2 | n, \\ (-1)^k & \text{jinak, kde } k \text{ je počet různých prvočísel v rozkladu čísla } n \text{ na prvočinitele.} \end{cases}$$

Z definice vyplývá, že klíčové v určení hodnoty Möbiovy funkce je znalost rozkladu, později uvidíme, že se nejedná o jediný možný postup. Uveďme si ještě pár příkladů.

Příklad 1.1.1.

1. $\mu(105) = -1$, neboť $105 = 3 \cdot 5 \cdot 7$.
2. Pro každé $n \in \mathbb{N}$ dělitelné 4 platí $\mu(n) = 0$, neboť $4 = 2^2$.

Začněme si nyní již uvádět některá tvrzení týkajících se Möbiovy funkce. Asi tím nejznámějším je to následující.

Tvrzení 1.1.1. *Nechť $g : \mathbb{N} \mapsto \mathbb{Z}$ je dána předpisem*

$$g(n) = \sum_{d|n} \mu(d).$$

Potom

$$g(n) = \begin{cases} 1 & \text{pokud } n = 1 \\ 0 & \text{pro } n > 1 \end{cases}$$

Důkaz. Případ $n = 1$ plyne přímo z definice. Uvažme proto $n > 1$. Rozložíme číslo n na prvočinitele jako $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$. Každý dělitel d čísla n lze tak napsat ve tvaru $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_m^{\beta_m}$, kde pro každé $1 \leq i \leq m$ platí $0 \leq \beta_i \leq \alpha_i$. Ve skutečnosti však všechny takové dělitele nebudeme potřebovat. Budou nás totiž zajímat pouze ty dělitelé větší jak 1, u nichž $\beta_i \leq 1$, tedy ty, jež nejsou dělitelný druhou mocninou přirozeného čísla větší jak 1. To je dáno tím, že v takovém případě by $\mu(n) = 0$ a přičtení 0 nezmění hodnotu $g(n)$.

Je ještě třeba rozlišit počet různých prvočísel v rozkladu daného dělitele. Dělitelů d obsahujících 0 prvočísel je 1, a to $d = 1$. Podobně dělitelů obsahujících jedno prvočíslo je m, dvě prvočísla $\binom{m}{2}$ a tak postupně až k děliteli rovnajícímu se číslu n. S využitím binomické věty můžeme psát, že

$$\begin{aligned} g(n) = \sum_{\beta_1,\beta_2,\ldots,\beta_m} p_1^{\beta_1} p_2^{\beta_2} \cdots p_m^{\beta_m} &= 1 + (-1) \cdot m + (-1)^2 \cdot \binom{m}{2} + \cdots + (-1)^m \\ &= \sum_{i=0}^{m} \binom{m}{m-i} \cdot (-1)^i = (1-1)^m = 0. \end{aligned}$$

□

V práci se dále vyskytnou pojmy *aritmetická funkce* a multiplikativní funkce, které jsou objasněny následujícími definicemi.

Definice 1.1.2. Funkci $f : \mathbb{N} \mapsto \mathbb{C}$ nazýváme aritmetická funkce.

Definice 1.1.3. Řekneme, že aritmetická funkce $f : \mathbb{N} \mapsto \mathbb{C}$ je multiplikativní, jestliže

1. $f(1) = 1$,
2. $\forall a, b \in \mathbb{N}, (a, b) = 1 : f(a \cdot b) = f(a) \cdot f(b)$.

Möbiova funkce disponuje oběma vlastnostmi výše zmíněných definic.

Tvrzení 1.1.2. *Möbiova funkce je multiplikativní.*

Důkaz. První podmínka multiplikativní funkce plyne přímo z definice. Stejně tak případ $a = b = 1$, kdy $\mu(ab) = 1 = \mu(1) \cdot \mu(1)$ je zřejmý.

Vyřešme nyní případ, kdy Möbiova funkce v ab nabývá 0. Využijme nesoudělnosti a, b a bez újmy na obecnosti předpokládejme, že existuje $d \in \mathbb{N}, d > 1$ takové, že $d^2|a$. Potom $\mu(a) = 0$, jistě zároveň $d^2|ab$. Z toho pak plyne, že $\mu(ab) = 0 = \mu(a) \cdot \mu(b)$.

Nakonec zbývá případ, kdy $a > 1$, $b > 1$ a zároveň $\mu(ab) \neq 0$, tedy že neexistuje $d \in \mathbb{N}$ splňující $d^2|a$ nebo $d^2|b$. Pro tuto situaci nechť číslo a má k různých prvočísel ve svém rozkladu na prvočinitele a číslo b má v rozkladu l různých prvočísel. Díky nesoudělnosti a, b pak

$$\mu(ab) = (-1)^{k+l} = (-1)^k \cdot (-1)^l = \mu(a) \cdot \mu(b).$$

□

1.2 Möbiova inverzní formule

V průběhu kapitoly jsme narazili na funkci ve tvaru

$$g(n) = \sum_{d|n} f(n),$$

konkrétně na případ, kdy $f(n) = \mu(n)$. V obecnějším případě f může být jakákoliv aritmetická funkce. Nabízí se otázka, zda můžeme funkci $f(n)$ zpětně vyjádřit pomocí $g(n)$. Pokud ano, mohli bychom v případě $f(n) = \mu(n)$ získat nový možný způsob výpočtu Möbiovy funkce. A skutečně, takové vyjádření pomocí funkce $g(n)$ existuje. Tvrzení dokazující existenci zmíněného vyjádření nazýváme *Möbiova inverzní formule.*

Tvrzení 1.2.1 (Möbiova inverzní formule)**.** *Nechť f, g jsou aritmetické funkce. Pokud*

$$g(n) = \sum_{d|n} f(d),$$

potom

$$f(n) = \sum_{d|n} \mu(d) \cdot g\left(\frac{n}{d}\right).$$

Důkaz.

$$\begin{aligned}\sum_{d|n} \mu(d) \cdot g\left(\frac{n}{d}\right) &= \sum_{d|n} \sum_{e|\frac{n}{d}} \mu(d) \cdot f(e) \\ &= \sum_{e|n} \left(\sum_{d|\frac{n}{e}} \mu(d) \right) \cdot f(e).\end{aligned}$$

V úpravě výrazu jsme využili toho, že sčítáme přes všechny uspořádané dvojice (d, e) přirozených čísel, jejichž součin je dělitelem čísla n.

Nyní je nám součet v závorce povědomý, neboť podle tvrzení 1.1.1 je roven 0 pro všechna $d \neq n$, pro totiž $d = n$ je roven 1. Dostáváme tak, že

$$\sum_{d|n} \mu(d) \cdot g\left(\frac{n}{d}\right) = f(n)$$

□

Po seznámení se s Möbiovou inverzní formulí můžeme konečně využít Möbiovu funkci k dokázání výpočtu hodnoty Eulerovy funkce. Připomeňme si ještě její definici.

Definice 1.2.1. Nechť $n \in \mathbb{N}$. Hodnota Eulerovy funkce $\varphi : \mathbb{N} \mapsto \mathbb{N}$ v n nám udává počet čísel m takových, že $1 \leq m \leq n$ a $(n, m) = 1$.

Definice nám jednoduše říká, že hodnota $\varphi(n)$ odpovídá počtu přirozených čísel nesoudělných s n, která jsou menší nebo rovna n.

Příklad 1.2.1.

1. $\varphi(6) = 2$ (čísla $1, 5$ jsou nesoudělná s 6).
2. $\varphi(p) = p - 1$, kde $p \in \mathbb{N}$ je prvočíslo.

Jak ale přímo spočítat hodnotu $\varphi(n)$ pro libovolné n? K určení budeme potřebovat znalost rozkladu n na prvočinitele. Následující tvrzení nám ukazuje, jak hodnotu $\varphi(n)$ zjistit. Předtím si uvedeme pomocné lemma.

Lemma 1.2.1. *Pro každé $n \in \mathbb{N}$ platí*

$$\sum_{d|n} \varphi(d) = n.$$

Důkaz. Pro libovolné $n \in \mathbb{N}$ uvažme množinu $R = \{\frac{k}{n} \mid 1 \leq k \leq n\}$. Zlomky v R si upravme do základního tvaru, kdy čitatel bude nesoudělný se jmenovatelem. Potom pro každého dělitele d čísla n nalezneme zlomek, v jehož jmenovateli bude d. Kolik takových zlomků ale je? Zapišme si n jako $n = kd$, kde d je náš hledaný dělitel ve jmenovateli. Pak počet zlomků takových, které mají d ve jmenovateli, odpovídá počtu čísel ve tvaru kl, kde $1 \leq l \leq d$ a zároveň $(d, l) = 1$, což je přesně $\varphi(d)$. Pokud projdeme přes všechny dělitele čísla n, získáme každý zlomek z R *právě jednou*, a proto

$$\sum_{d|n} \varphi(d) = n.$$

□

Tvrzení 1.2.2. *Nechť $n \in \mathbb{N}$ a $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$. Potom*

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_m}\right).$$

Důkaz. Z lemma 1.2.1 víme, že platí

$$\sum_{d|n} \varphi(d) = n.$$

Nyní použijeme Möbiovu inverzní formuli. Ve formuli budeme uvažovat jen dělitele $d|n$, které nejsou dělitelné druhou mocninou přirozeného čísla. Položíme-li $g(n) = n$, potom

$$\varphi(n) = \sum_{\substack{d|n \\ \nexists r \in \mathbb{N}: r>1, r^2|d}} \mu(d)\frac{n}{d} = n + (-1) \cdot \sum_{i=1}^{m} \frac{n}{p_i} + (-1)^2 \cdot \sum_{i<j} \frac{n}{p_i p_j} + \cdots + (-1)^m \cdot \frac{n}{p_1 p_2 \cdots p_m}.$$

Po vhodném vytýkání nakonec obdržíme

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_m}\right).$$

□

Příklad 1.2.2. Pomocí právě dokázaného vzorce vidíme, že:

$$\varphi(6) = 6 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 2.$$

Čtenáři se může jevit zvláštní počítat hodnoty Eulerovy funkce jakožto součin n a několika *racionálních čísel*, přestože se pohybujeme v přirozených číslech. Vztah 1.2.2 lze přepsat na tvar

$$\begin{aligned}\varphi(n) &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_m}\right) \\ &= \prod_{i=1}^{m} p_i^{\alpha_i - 1} \cdot (p_i - 1).\end{aligned}$$

1.3 Alternativní výpočet hodnot Möbiovy funkce

Mějme konečnou cyklickou grupu $G = \langle e^{\frac{2\pi i}{n}} \rangle$, grupu n-tých komplexních odmocnin 1. Dále nechť $f(n)$ je součet všech prvků G takových, že jejich řád je roven n. Není obtížné ukázat, že g^i je řádu n právě tehdy, když $(i, n) = 1$.

Pro $n = 1$ obdržíme triviálně $f(n) = 1$. Mějme tak $n \geq 2$. Z lemma 1.2.1 plyne, že součet všech $f(d)$ pro $d|n$ je roven součtu $\sum_{d|n} \varphi(d) = n$ různých prvků grupy G. To znamená, že součet všech $f(d)$ pro všechny dělitele čísla n je roven součtu všech prvků G. Takže

$$g(n) = \sum_{d|n} f(d) = \sum_{k=1}^{n-1} e^{\frac{2\pi ik}{n}} = \frac{1 - \left(e^{\frac{2\pi i}{n}}\right)^n}{1 - e^{\frac{2\pi i}{n}}} = 0.$$

Všimněme si, že definice funkce $g(n)$ nám dává možnost aplikovat Möbiovu inverzní formuli. Vezmeme-li v potaz, že $g(n) = 1$ pro $n = 1$ a $g(n) = 0$ pro $n > 1$, potom pro libovolné $n \in \mathbb{N}$ platí, že

$$\sum_{d|n} \mu(d) \cdot g\left(\frac{n}{d}\right) = \mu(n).$$

Dostáváme zajímavé tvrzení, k němuž došli pánové G. H. Hardy a E. M. Wright.

Tvrzení 1.3.1 (G. H. Hardy a E. M. Wright)**.** *Pro libovolné $n \in \mathbb{N}$ platí*

$$\mu(n) = \sum_{\substack{1 \leq k \leq n \\ (k,n)=1}} e^{\frac{2ik\pi}{n}}.$$

K určení hodnoty $\mu(n)$ tak není potřeba znát rozklad n, lze také použít zmíněný součet. Ukažme si důkaz tvrzení 1.1.1 pomocí definice 1.3.1. Stačí si pouze povšimnout, s využitím lemmatu 1.2.1, že

$$\sum_{d|n} \mu(d) = \sum_{d|n} \sum_{\substack{1 \leq k \leq n \\ (k,n)=1}} e^{\frac{2ik\pi}{n}} = \sum_{j=1}^{n} e^{\frac{2ij\pi}{n}} = 0,$$

jelikož součet všech komplexních odmocnin 1 je roven 0.

Kapitola 2

Tělesa

Tělesa představují v matematice důležitou algebraickou strukturu. Mezi takové známé příklady patří množiny $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ společně s operacemi sčítání a násobení. Zmíněná tělesa jsou příklady nekonečných těles. Často nad tělesy uvažujeme nějaké polynomy a nacházíme jejich kořeny. Všechna tělesa ovšem nemají nekonečný počet prvků. O takových tělesech říkáme, že jsou *konečná*. Nejintuitivnější ukázkou konečných těles je těleso $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, množina $\{0, 1, \ldots, p-1\}$ s klasickými operacemi sčítání a násobení zbytkových tříd modulo prvočíslo p.

Předmětem této kapitoly však budou obecně tělesa a povíme si také něco o jejich rozšířeních jako třeba o jednoduchých nebo algebraických rozšířeních. Konečným tělesům se budeme věnovat až v příští kapitole.

2.1 Základní vlastnosti těles

Definice 2.1.1. Množina F spolu s binárními operacemi $+, \cdot$, pro kterou platí, že

1. $(F, +)$ tvoří komutativní aditivní grupu s neutrálním prvkem 0,
2. $(F^*, \cdot)$ tvoří komutativní multiplikativní grupu, kde $F^* = F \setminus \{0\}$,
3. $\forall a, b, c \in F : a \cdot (b + c) = (b + c) \cdot a = ab + ac$,

se nazývá těleso. Pokud je množina F konečná, potom o tělese $(F, +, \cdot)$ říkáme, že je konečné.

Příklad 2.1.1.

1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ jsou tělesa s nekonečným počtem prvků.
2. $\mathbb{Z}/p\mathbb{Z}$, kde $p \in \mathbb{N}$ je prvočíslo, je konečné těleso obsahující p prvků.

3. $\mathbb{Z}$ netvoří s klasickými operacemi $(+, \cdot)$ těleso, neboť neexistuje inverzní prvek pro $n \in \mathbb{Z} \setminus \{-1, 1\}$ vzhledem k násobení.

Definice 2.1.2. Nechť $(F, +, \cdot)$ je těleso a buď $(K, +, \cdot)$ jeho podmnožina, kde operace sčítání a násobení v K jsou zúženími operací na F. Pak řekneme, že K je podtěleso F, jestliže K je také těleso.

Příklad 2.1.2.

1. $\mathbb{R}$ je podtělesem $\mathbb{C}$ a $\mathbb{Q}$ je podtělesem $\mathbb{R}$.

2. Množina $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ tvoří s klasickými operacemi $(+, \cdot)$ těleso, $\mathbb{Q}$ je zřejmě jeho podtělesem. V následující kapitole uvidíme, že libovolná množina $\mathbb{Q}(\sqrt{D})$, kde $D \in \mathbb{Q}$, ale $\sqrt{D} \notin \mathbb{Q}$, s klasickými operacemi je těleso.

Takovou základní vlastností tělesa a jeho libovolného podtělesa je charakteristika tělesa, která je vysvětlena v následující definici.

Definice 2.1.3. Charakteristikou tělesa F rozumíme nejmenší přirozené číslo n, pro které platí, že

$$n \cdot 1_F = \underbrace{1_F + 1_F + \cdots + 1_F}_{n} = 0,$$

kde 1_F je neutrální prvek grupy $(F^*, \cdot)$. Pokud takové přirozené n neexistuje, říkáme, že charakteristika tělesa F je rovna 0.

Tvrzení 2.1.1. *Každé těleso má buď charakteristiku rovnu* 0*, nebo prvočíslu.*

Důkaz. Předpokládejme, že F má přirozenou charakteristiku a předpokládejme pro spor, že je rovna $n = kl$, kde $k, l \in \mathbb{N}$ a $k, l > 1$. Potom

$$\underbrace{1 + 1 + \cdots + 1}_{n} = \underbrace{(1 + 1 + \cdots + 1)}_{k} \cdot \underbrace{(1 + 1 + \cdots + 1)}_{l} = 0.$$

Protože těleso je oborem integrity, alespoň jedna závorka musí být rovna 0, což je spor vzhledem k minimalitě n. □

Příklad 2.1.3.

1. Tělesa $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ mají charakteristiku 0.

2. Těleso $\mathbb{Z}/p\mathbb{Z}$, kde p je prvočíslo, má charakteristiku p.

Vybaveni znalostí charakteristiky tělesa si můžeme detailněji povědět o speciálním případu podtělesa, a to o takzvaném *prvotělesu*, které bude velice důležité v příštích kapitolách.

Definice 2.1.4. Nechť F je těleso a K je jeho podtěleso. Řekneme, že K je prvotělesem, jesliže pro každé podtěleso E tělesa F platí $K \subseteq E$.

Definice nám vlastně říká, že prvotěleso je nejmenší podtěleso vzhledem k inkluzi. Než se dostaneme k hlavnímu tvrzení týkajícího se prvotělesa, je nutné si dokázat, že všechna tělesa obsahují své prvotěleso.

Tvrzení 2.1.2. *Každé těleso obsahuje své prvotěleso.*

Důkaz. Nechť F je těleso. Uvažme množinový průnik všech podtěles F. Není obtížné ukázat, že průnik (nekonečného) systému těles je opět těleso. Navíc, protože uvažujeme průnik všech podtěles, získané podtěleso je jistě minimální vzhledem k inkluzi. □

Jak takové prvotěleso vlastně vypadá? Ačkoliv je definice prvotělesa poměrně obecná, všechna tělesa obsahují ve skutečnosti pouze dva typy prvotěles v závislosti na jejich charakteristice.

Tvrzení 2.1.3. *Nechť F je těleso a buď P jeho prvotěleso.*

1. *Pokud charakteristika F je rovna 0, potom P je izomorfní s $\mathbb{Q}$.*
2. *Pokud charakteristika F je rovna prvočíslu p, potom P je izomorfní s tělesem $\mathbb{F}_p$, tělesem mající p prvků.*

Důkaz.

1. Protože $1 \in P$, potom $n \cdot 1 \in P$ pro $n \in \mathbb{Z}$ jsou různé prvky, jelikož charakteristika F je 0. To znamená, že okruh $\{n \cdot 1 \mid n \in \mathbb{Z}\}$ je izomorfní s $\mathbb{Z}$. Zřejmě pak okruh

$$Q_F = \left\{ \frac{n \cdot 1}{m \cdot 1} \mid n, m \in \mathbb{Z} \ \wedge \ m \neq 0 \right\}$$

   je izomorfní s $\mathbb{Q}$, takže Q_F je dokonce těleso. Z konstrukce tělesa Q_F plyne $Q_F \subseteq P$. Zároveň ale P je nejmenší podtěleso, takže $P \subseteq Q_F$, což dohromady dává, že $P = Q_F \cong \mathbb{Q}$.

2. Vezměme si těleso $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ mající prvočíselný počet prvků. Uvažme zobrazení $\phi : \mathbb{F}_p \mapsto F$ definované předpisem $\phi(n) \mapsto n \cdot 1$, kde $n \in \{0, 1, \ldots, p-1\}$. Dané zobrazení je pak homomorfismus, neboť

$$\phi(a+b) = (a+b) \cdot 1 = a \cdot 1 + b \cdot 1 = \phi(a) + \phi(b)$$
$$\phi(ab) = ab \cdot 1 = (a \cdot 1)(b \cdot 1) = \phi(a) \cdot \phi(b).$$

   Zřejmě je dané zobrazení surjektivní. Ukážeme si, že je také injektivní, a tudíž bijektivní.

   Nechť $a, b \in F$, potom $\phi(a) = \phi(b)$ implikuje, že $\phi(a-b) = 0$. Položme $c = a - b$. Pak

$$\phi(1) = \phi(c \cdot c^{-1}) = \phi(c) \cdot \phi(c^{-1}) = 0,$$

což je spor, neboť 1 je neutrální prvek $\mathbb{F}_p$, a vždy platí, že homomorfismus zobrazuje neutrální prvek na neutrální prvek. Námi zvolené zobrazení je tedy bijektivní a je homomorfismus, a tudíž představuje izomorfismus. Je ještě potřeba zjistit, na jakou množinu prvky zobrazujeme.

Pro prvotěleso vždy platí $P \subseteq \operatorname{Im}\phi$. Zároveň $n \cdot 1 \in \operatorname{Im}\phi$ pro každé $n \in \{0, 1, \ldots, p-1\}$, takže $P = \operatorname{Im}\phi$, což jsme chtěli dokázat.

□

2.2 Konstrukce tělesa

Od popisu tělesa přejděme k jeho konstrukci. Nejčastěji konstruujeme tělesa pomocí okruhů, a to těmito dvěma postupy:

- Konstrukce *podílového těleso* pomocí oboru integrity.
- Konstrukce *faktorokruhu* pomocí oboru hlavních ideálů.

My se v této práci zaměříme na druhý způsob konstrukce, neboť má velkého využití při konstrukci konečných těles. Kdy nám ale tato konstrukce skutečně poskytne těleso?

Tvrzení 2.2.1. *Nechť R je obor hlavních ideálů a I jeho ideál. Potom faktorokruh R/I je těleso právě tehdy, když $I = \langle p \rangle$, kde $p \in I$ je ireducibilní prvek.*

Místo ideálu generovaném ireducibilním prvkem bychom mohli uvážit dokonce tzv. *maximální ideál*. Důkaz se opírá o věty o izomorfismu okruhů. Nebudeme se jím zde zabývat, čtenář jej může nalézt v [2].

Nejznámějším příkladem takto konstruovaného tělesa je jistě $\mathbb{Z}/p\mathbb{Z}$, obsahující zbytkové třídy modulo prvočíslo p. A právě kongruence je klíčová při používání uvedeného tělesa. Ukážeme si totiž, že pomocí výše uvedené konstrukce můžeme vytvářet tělesa, ve kterých se sčítá a násobí jako u kongruencí.

Ve výše zmíněném tvrzení se odkazujeme na ireducibilní prvky ideálu. Zaměříme se na ireducibilní polynomy. Ireducibilní polynom stupně většího než 1 nemá kořen v tělese, nad kterým je ireducibilní. U reálných čísel víme, že polynom s reálnými koeficienty má kořen v $\mathbb{C}$. Existuje ale vždy těleso, v kterém má polynom kořen?

Tvrzení 2.2.2. *Nechť F je těleso a nechť $f \in F[x]$ je ireducibilní polynom nad F. Potom existuje těleso K obsahující podtěleso izomorfní s F, v němž má f kořen.*

Důkaz. Ukážeme, že faktorokruh $K = F[x]/\langle f \rangle$ je naším požadovaným tělesem. Protože $F[x]$ je okruh polynomů nad tělesem, jedná se o obor hlavních ideálů. Navíc f je ireducibilním polynomem, takže ideál $\langle f \rangle$ je generovaný ireducibilním prvkem, a tudíž K je těleso.

Dále dokážeme existenci podtělesa $\overline{F}$ izomorfního s F. Vezměme si zobrazení $\varphi : F \mapsto \overline{F}$ definované předpisem $\varphi(a) \mapsto a + \langle f \rangle$. Zřejmě je zobrazení φ surjektivní, stačí dokázat, že je injektivní; předpokládejme $a + \langle f \rangle = b + \langle f \rangle$ a chceme ukázat, že pak $a = b$. Náš předpoklad přímo implikuje, že $b - a \in \langle f \rangle$, tedy $b - a$ je dělitelné f. Ovšem $a, b \in F$, a proto se jedná o polynomy stupně 0, avšak polynom dělitelný f má stupeň alespoň $\deg f \geq 1$, z čehož plyne, že nutně $b - a = 0$ neboli $a = b$. Tímto je dokázáno, že $\overline{F} \subseteq K$.

Zbývá ukázat existenci prvku $\theta \in K$ takového, že $f(\theta) = 0$. Předpokládejme, že $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, kde $a_i \in F$. Stačí zvolit $\theta = x + \langle f \rangle \in K$, přičemž nesmíme zapomenout, že při dosazování θ do f počítáme v K:

$$\begin{aligned} f(x + \langle f \rangle) &= (a_n + \langle f \rangle)(x + \langle f \rangle)^n + (a_{n-1} + \langle f \rangle)(x + \langle f \rangle)^{n-1} + \cdots + (a_0 + \langle f \rangle) \\ &= (a_n x^n + \langle f \rangle) + (a_{n-1}x^{n-1} + \langle f \rangle) + \cdots + (a_0 + \langle f \rangle) \\ &= f + \langle f \rangle = \langle f \rangle. \end{aligned}$$

Nulovým prvkem v K je prvek $\langle f \rangle$. Tímto je důkaz hotov. □

Prozkoumejme chování tělesa K. Vezměme si dva libovolné prvky $g + \langle f \rangle, h + \langle f \rangle$ a zjistěme, kdy jsou si rovny. Pokud totiž $g + \langle f \rangle = h + \langle f \rangle$, pak $g - h \in \langle f \rangle$, takže rozdíl $g - h$ je *dělitelný* f. Toto pozorování nám připomíná chování faktorokruhu $\mathbb{Z}/p\mathbb{Z}$. Ukažme si, že skutečně můžeme libovolný prvek K určit jednoznačně pomocí zbytku po dělení polynomem f.

Hledáme polynom $r \in F[x]$ s vlastností $0 \leq \deg r < \deg f$. Existence takového polynomu je splněna díky faktu, že $F[x]$ je euklidovským oborem, tedy že můžeme použít Euklidův algoritmus pro nějaký polynom $g \in F[x]$, abychom nalezli zbytek po dělení g polynomem f.

Zbývá dokázat jednoznačnost takového r. Nechť $r_1, r_2 \in F[x]$ a $0 \leq r_1 \leq r_2 < \deg f$, potom rovnost $r_1 + \langle f \rangle = r_2 + \langle f \rangle$ implikuje $r_2 - r_1 \in \langle f \rangle$, takže rozdíl $r_2 - r_1$ je dělitelný f. Nicméně, vlastnost $r_1, r_2 < \deg f$ vyžaduje rovnost $r_2 - r_1 = 0$, neboli $r_1 = r_2$. Tímto jsme dokázali jednoznačnost reprezentantů prvků tělesa K.

Máme-li tedy libovolný polynom $g \in F[x]$ a pokud θ je kořen polynomu f v K, potom

$$g + \langle f \rangle = r + \langle f \rangle = r(\theta),$$

kde r je zbytek po dělení g polynomem f, což také můžeme značit jako $r \equiv g \pmod f$ a $\theta = x + \langle f \rangle$.

Důsledek 2.2.1. *Každý prvek g tělesa $K = F[x]/\langle f \rangle$, kde F je těleso, $f \in F[x]$ ireducibilní polynom a $\deg f = n$, lze jednoznačně zapsat pomocí kořenu $\theta \in K$ polynomu f jako*

$$g = a_{n-1}\theta^{n-1} + a_{n-2}\theta^{n-2} + \cdots + a_0,$$

kde $\theta = x + \langle f \rangle$, $a_1, a_2, \ldots, a_{n-1} \in \overline{F}$.

Správně bychom měli členy $a_0, a_1, \ldots, a_{n-1}$ zapsat jako třídy $a_0 + \langle f \rangle, a_1 + \langle f \rangle, \ldots, a_{n-1} + \langle f \rangle$. Protože ovšem existuje izomorfní těleso $\overline{F} \subseteq K$, není třeba počítat se třídami.

Příklad 2.2.1. Podívejme se, jak se počítá ve faktorokruhu $K = \mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$. Protože $x^2 + x + 1 \in \mathbb{Z}_2[x]$ je ireducibilní, K je těleso. Existuje tedy prvek $\theta \in K$, jenž je kořenem $x^2 + x + 1$. Podle důsledku 2.2.1 jsou prvky tělesa K prvky množiny $\{0, 1, \theta, \theta + 1\}$.

Sčítání prvků K je jednoduché, neboť charakteristika tělesa K je 2. Pro násobení dostaneme postupně $\theta^2 = -(\theta + 1) = \theta + 1$ a $\theta \cdot (\theta + 1) = \theta + 1 + \theta = 1$. Můžeme tedy sestavit tabulku pro operace.

$+$	0	1	θ	$\theta+1$
0	0	1	θ	$\theta+1$
1	1	0	$\theta+1$	θ
θ	θ	$\theta+1$	0	1
$\theta+1$	$\theta+1$	θ	1	0

$\cdot$	1	θ	$\theta+1$
1	1	θ	$\theta+1$
θ	θ	$\theta+1$	1
$\theta+1$	$\theta+1$	1	θ

Získané těleso má 4 prvky.

Poznámka. Obecně pokud bychom měli těleso s q prvky a ireducibilní polynom n-tého stupně, získané těleso by mělo q^n prvků; každý prvek lze zapsat jako $a_{n-1}\theta^{n-1} + a_{n-2}\theta^{n-2} + \cdots + a_0$, kde za a_i pro $0 \leq i \leq n-1$ máme q možností, celkem tak q^n prvků.

Ze *základového* tělesa jsme získali *rozšířené těleso*. Nakousli jsme tím další kapitolu související s tělesy, a to rozšíření těles.

Kapitola 3

Rozšíření těles

Samotná definice rozšíření těles se ve své podstatě neliší od definice podtělesa. V průběhu práce uvidíme, že ačkoliv definice rozšíření je takřka shodná s definicí podtělesa, bude vhodnější v některých případech hovořit o vztahu rozšíření tělesa než o vztahu podtěleso tělesa. V těchto případech budeme hovořit o tělesu jako vektorovém prostoru.

3.1 Těleso jako vektorový prostor

Definice 3.1.1. Řekneme, že F je rozšířením tělesa K, jestliže $K \subseteq F$ a zároveň F je tělesem. Zde operace na K jsou zúženími operací na F.

Tvrzení 3.1.1. *Nechť F je těleso a $K \subseteq F$ jeho podtěleso. Potom F je rozšíření tělesa K. Dané rozšíření značíme $F : K$.*

Proč je ale výhodné hovořit o rozšíření tělesa, když můžeme stejnou vlastnost popsat pomocí podtělesa? Odpověď na tuto otázku tkví v pojetí $F : K$ jako *vektorového prostoru* F nad K.

Tvrzení 3.1.2. *Nechť $F : K$ je rozšíření tělesa $(K, +, \cdot)$. Potom $(F, +, \cdot)$ je vektorovým prostorem nad K.*

Důkaz. Musíme ověřit všechny axiomy vektorového prostoru. Vyjdeme z definice tělesa. Z ní přímo plyne, že $(F, +)$ je komutativní grupa.

U násobení je důkaz následující:

1. V tělese K je neutrální prvek 1 splňující $1 \cdot \alpha = a$ pro každé $\alpha \in F$.
2. Pro všechna $a, b \in K$ a $\alpha \in F$ platí $(a \cdot b) \cdot \alpha = a \cdot (\alpha \cdot b)$.
3. Pro všechna $a, b \in K$ a $\alpha \in F$ platí $(a + b) \cdot \alpha = a \cdot \alpha + b \cdot \alpha$.

4. Pro všechna $a \in K$ a $\alpha, \beta \in F$ platí $a \cdot (\alpha + \beta) = a \cdot \alpha + a \cdot \beta$.

□

U vektorových prostorů nad tělesy je pro nás klíčové označení dimenze daného vektorového prostoru, na které se budeme v práci často odvolávat.

Definice 3.1.2. Dimenzi vektorového prostoru F nad K říkáme stupeň rozšíření $F : K$. Značíme jej $[F : K]$.

Příklad 3.1.1.

1. $[\mathbb{C} : \mathbb{R}] = 2$, neboť $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$, kde $\{1, i\}$ je báze.
2. $[\mathbb{R} : \mathbb{Q}]$ je nekonečný.

Mějme tělesa $K \subseteq F \subseteq L$. Představme si situaci, kdy známe stupně $[L : F]$ a $[F : K]$ a chceme z této znalosti odvodit $[L : K]$. Intuitivně si lze představit, že bychom mohli uvážit bázi $\alpha_i\beta_j$, kde $1 \leq i \leq [L : F]$, $1 \leq j \leq [F : K]$. Následující tvrzení nám naši hypotézu potvrzuje.

Tvrzení 3.1.3. *Nechť K, F, L jsou tělesa a $K \subseteq F \subseteq L$. Potom*

$$[L : K] = [L : F][F : K].$$

Důkaz. Nejprve předpokládejme, že stupně $[L : F], [F : K]$ jsou konečné. Nechť $n = [L : F]$ a $m = [F : K]$. Dále nechť je $\alpha_1, \alpha_2, \ldots, \alpha_n$ báze $L : F$ a $\beta_1, \beta_2, \ldots, \beta_m$ báze $F : K$. Libovolný prvek $x \in L$ lze jednoznačně vyjádřit lineární kombinací

$$x = \sum_{i=1}^{n} a_i\alpha_i,$$

kde $a_i \in F$. Každé takové a_i lze zároveň vyjádřit jednoznačně lineární kombinací

$$a_i = \sum_{j=1}^{m} b_{ij}\beta_j,$$

kde $b_{ij} \in K$. Ukážeme, že $\alpha_i\beta_j$ pro $1 \leq i \leq n$, $1 \leq j \leq m$ tvoří bázi $L : K$. Zřejmě každý prvek L lze vyjádřit jejich lineární kombinací nad K. Zbývá dokázat, že jsou tyto prvky lineárně nezávislé.

Předpokládejme spor. Hledejme $c_{ij} \in K$, $1 \leq i \leq n$, $1 \leq j \leq m$, kde alespoň jedno je nenulové, splňující

$$\sum_{i=1}^{n}\sum_{j=1}^{m} c_{ij} \cdot \alpha_i\beta_j = 0$$

Výraz na levě straně mírně upravíme pomocí předchozího vyjádření a_i na tvar:

$$\sum_{j=1}^{n} a_i \alpha_i = 0,$$

kde ovšem α_i pro $1 \leq i \leq n$ jsou lineárně nezávislé nad F, a proto musí platit $a_i = 0$. Prvky a_i můžeme zase napsat pomocí báze $\beta_1, \beta_2, \ldots, \beta_m$, což bude opět implikovat, že skaláry takové reprezentace a_i budou opět nulové, a proto dostáváme $c_{ij} = 0$ pro $1 \leq i \leq n$ a $1 \leq j \leq m$.

Zbývá vyřešit případ, kdy stupeň rozšíření je nekonečný. Pokud $[F : K]$ je nekonečný, potom F obsahuje nekonečně mnoho lineárně nezávislých prvků nad K, a tak i L obsahuje nekonečně mnoho lineárně nezávislých prvků nad K, a tudíž i $[L : F]$ obsahuje nekonečně mnoho lineárně nezávislých prvků nad F. Obdobně postupujeme pro ostatní stupně $[L : F]$ a $[L : K]$. □

Uvedené tvrzení tedy lze aplikovat i na nekonečné stupně, čehož můžeme využít při důkazu nekonečnosti ostatních stupňů. U konečných těles se setkáme pouze s *konečnými rozšířeními*, tj. rozšířeními s bází.

Základní povědomí o tělesu jako vektorovém prostoru nám nyní bude nápomocné při zkoumání prvního rozšíření, a sice *algebraického rozšíření*.

3.2 Algebraické rozšíření

Mějme rozšíření $L : K$. Bude nás nyní zajímat, co znamená, když $\alpha \in L$ je algebraické nad K.

Definice 3.2.1. Nechť $L : K$ je rozšíření. O prvku $\alpha \in L$ řekneme, že je algebraický nad K, jestliže existuje nekonstantní polynom $f(x) \in K[x]$, pro který je α jeho kořenem.

Definice 3.2.2. Nechť $L : K$ je rozšíření. Pokud každý prvek L je algebraický nad K, pak $L : K$ se nazývá algebraické rozšíření.

Nyní si vezměme množinu všech polynomů nad tělesem K, které mají jako kořen nějaký algebraický prvek α z tělesa L. Symbolicky tuto množinu označme I_α, pak

$$I_\alpha = \{f(x) \mid f(x) \in K[x] \wedge f(\alpha) = 0\}$$

Není náhodou, že je množina nazvána, jako by by byla ideálem $K[x]$, protože jím vskutku je. Tento fakt lze snadno ověřit. Pro další zkoumání I_α si ještě dokážeme jednu důležitou vlastnost ideálů.

Tvrzení 3.2.1. *Každý ideál $I_\alpha = \{f(x) \mid f(x) \in K[x] \wedge f(\alpha) = 0\}$ je generovaný jednoznačně určeným normovaným polynomem $m \in I_\alpha$.*

Důkaz. Pro $I_\alpha = \{0\}$, pak je I_α generované 0. Pro netriviální I_α si vezměme normovaný[1] polynom nejnižšího stupně a označme jej $m \in I_\alpha$. Z vlastnosti ideálu plyne, že pro libovolné $f \in K[x]$ platí $mf \in I_\alpha$, takže $\langle m \rangle \subseteq I_\alpha$. Pokud se nám podaří ukázat, že $I_\alpha \subseteq \langle m \rangle$, pak jsme hotovi.

[1] Nekonstantní polynom $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ je normovaný, jestliže $a_n = 1$.

Vezměme si libovolný polynom $f \in I_\alpha$. Tento polynom si můžeme vyjádřit pomocí m jako $f = gm + r$, kde $g, r \in K[x]$ a $\deg r < \deg m$. Potom ovšem $r = f - gm \in I_\alpha$ díky uzavřenosti I_α na sčítání. To je ale ve sporu s předpokladem, že m je polynom nejmenšího stupně v I_α. Musí proto platit pouze případ, kdy $r = 0$, neboli že $f = gm \in I_\alpha$, tedy $I_\alpha \subseteq \langle m \rangle$.

Zbývá ukázat jednoznačnost m. Nechť $n \in I_\alpha$ je jiný normovaný polynom generující ideál I. Potom existují $f, g \in I_\alpha$ tak, že $m = fn$ a $n = gm$. Po dosazení obdržíme rovnost $m = fn = fgm$. Protože m je normovaný polynom, potom nutně $fg = 1$. Ovšem polynomy f, g si mohou být sami inverzní, právě když jsou konstantními polynomy, ale n, m jsou normované, takže nutně $f = g = 1$, tedy $m = n$, čímž je dokázána jednoznačnost polynomu m. □

Vraťme se k našemu ideálu I_α. Podle tvrzení 3.2 existuje jednoznačně určený polynom m_α generující I_α, jenž nese své jméno.

Definice 3.2.3. Nechť $L : K$ je rozšíření a buď $\alpha \in L$ algebraický prvek nad K. Potom polynom m_α, splňující $\langle m_\alpha \rangle = I_\alpha = \{f(x) \mid f(x) \in K[x] \wedge f(\alpha) = 0\}$ se nazývá minimální polynom α. Stupeň polynomu m_α se nazývá stupeň α nad K.

Zaměřme se právě na minimální polynom m_α nějakého algebraického prvku $\alpha \in L$ nad tělesem K. V důkazu tvrzení 3.2 byl generátor zvolen, jako normovaný polynom, takže m_α je jistě normovaný. Můžeme také nahlédnout, že každý prvek ideálu$\langle m_\alpha \rangle$ je dělitelný m_α, což nám nabízí tvrdit, že m_α je ireducibilní. Uvedená a jiná tvrzení týkající se minimálního polynomu nyní dokážeme.

Tvrzení 3.2.2. *Nechť $\alpha \in L$ je algebraický nad K a nechť m_α je jeho minimální polynom stupně $n \in \mathbb{N}$. Potom*

1. $\forall f \in K[x] : f(\alpha) = 0 \Leftrightarrow m_\alpha | f$.
2. *m_α je ireducibilní polynom nad K.*
3. *Polynom m_α je normovaný polynom nejmenšího stupně mající α jako kořen.*

Důkaz.

1. Víme, že $\langle m_\alpha \rangle$ generuje ideál I_α. To znamená, že libovolný polynom $f \in \langle m_\alpha \rangle$ právě tehdy, když $m_\alpha | f$, takže $f(\alpha) = 0$ právě tehdy, když f je dělitelný m_α.
2. Předpokládejme spor, tedy že $\exists f, g \in K[x] : m_\alpha = gf$ a $0 < \deg f \leq \deg g < \deg m_\alpha$. Potom $m_\alpha(\alpha) = g(\alpha)f(\alpha) = 0$. Protože $K[x]$ je obor integrity, pak $g(\alpha) = 0$ nebo $f(\alpha) = 0$, ale to bylo znamenalo, že $f \in \langle m_\alpha \rangle$ nebo $g \in \langle m_\alpha \rangle$, takže by podle předchozího tvrzení platilo, že $m_\alpha | f$ nebo $m_\alpha | g$. To je však nemožné, neboť $\deg m_\alpha > \deg g \geq \deg f$.

3. Opět řešme sporem a buď $f \in K[x]$ polynom mající nižší stupeň než m_α a $f(\alpha) = 0$. Vydělíme-li polynom m_α polynomem f, dostaneme $m_\alpha = fg + r$, kde $f, r \in K[x]$ a $0 \leq \deg r < \deg f$. Máme pak, že $m_\alpha(\alpha) = f(\alpha)g(\alpha) + r(\alpha) = 0$, ale $f(\alpha) = 0$, takže nutně $r(\alpha) = 0$, což je ve sporu s předpokladem, že $\deg f$ je minimální možný.

□

Naším cílem bude nyní propojit povědomí o algebraických rozšířeních s popisem tělesa jako vektorového prostoru. Pro tento popis si ještě zavedeme pár pojmů, které lze shrnout pod následující sekci.

3.3 Rozšíření generovaná konečným počtem prvků

Generování rozšíření pomocí jistého počtu prvků je analogické ke generování okruhu pomocí konečného počtu prvků.

Definice 3.3.1. Nejmenší rozšíření tělesa K obsahující prvky $\alpha_1, \alpha_2, \ldots, \alpha_n$ značíme $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Definice 3.3.2. Nechť K je těleso. Řekneme, že rozšíření L tělesa K je generované konečným počtem prvků, jestliže existují prvky $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$ takové, že $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Definice 3.3.3. Jednoduchým rozšířením tělesa K nazýváme takové rozšíření L, že existuje prvek $\alpha \in L$ splňující $L = K(\alpha)$.

Příklad 3.3.1.

1. Těleso $\mathbb{C}$ je jednoduché rozšíření $\mathbb{R}$ generované prvkem $i \in \mathbb{C}$.
2. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ je rozšíření $\mathbb{Q}$ generované $\sqrt{2}$ a $\sqrt{3}$. Časem uvidíme, že skutečně je $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ generované oběma prvky.

Omezíme se v této sekci na generování pomocí algebraických prvků. Uvidíme, že dostaneme jistá kritéria, kdy jsou nějaké rozšíření konečného stupně, čímž dostaneme naše kýžené propojení výše diskutovaných sekcí.

Tvrzení 3.3.1. *Každé konečné rozšíření $L : K$ je algebraické.*

Důkaz. Označíme-li $[L : K] = n$, pak báze má n prvků. Z definice báze plyne, že pro libovolný prvek $\alpha \in L$ platí, že prvky $1, \alpha, \alpha^2, \ldots, \alpha^n$ jsou lineárně závislé, jelikož jich je $n + 1$. To znamená, že existují prvky $c_0, c_1, \ldots, c_n \in K$, které nejsou všechny nulové, splňující

$$c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_n\alpha^n = 0.$$

To znamená, že pro libovolný prvek $\alpha \in L$ existuje polynom nad K mající α za kořen a to je přesně definice algebraického prvku. □

Poznámka. Musíme být opatrní na směr implikace, protože ne každé algebraické rozšíření je konečné, například těleso komplexních čísel algebraických nad $\mathbb{Q}$ není konečné algebraické rozšíření.

Příklad 3.3.2. $[\mathbb{C} : \mathbb{R}] = 2$ implikuje, že pro každé komplexní číslo existuje polynom nad $\mathbb{R}$, jehož je kořenem.

3.3.1 Jednoduché rozšíření

Dosud jsme si pouze objasnili, že rozšíření $L : K$ si lze vyložit jako vektorový prostor L nad K. To je stále příliš obecné pojetí na představu, jak se v takovém rozšíření počítá. V případě konečně generovaného rozšíření ovšem obdržíme zajímavý případ, který bude snáze představitelnější. Pomůžeme si právě minimálním polynomem. Začneme s jednoduchým rozšířením. Mějme nějaký algebraický prvek $\alpha \in L$ nad K a jednoduché rozšíření K určené α. Protože α je novým prvkem v tělese K, je otázkou, jakých hodnot budou vlastně polynomy nad K v α nabývat.

Uvažme zobrazení $\varphi : K[x] \mapsto K(\alpha)$, které určuje hodnoty libovolného polynomu nad K v α, takže $\varphi(f(x)) = f(\alpha)$, kde $f(x) \in K[x]$. Ukážeme, že dané zobrazení je homomorfismus. Nechť f, g jsou polynomy nad K. Potom díky tomu, že polynomy nad tělesem tvoří okruh, máme

$$\begin{aligned}\varphi(f+g) &= (f+g)(\alpha) = f(\alpha) + g(\alpha) = \varphi(f) + \varphi(g)\\ \varphi(f \cdot g) &= (fg)(\alpha) = f(\alpha)g(\alpha) = \varphi(f)\varphi(g).\end{aligned}$$

Podívejme se na vlastnosti tohoto zobrazení. Pokud si určíme jádro φ, obdržíme

$$\operatorname{Ker}\varphi = \{f(x) \mid f(x) \in K[x] \ \wedge \ f(\alpha) = 0\},$$

což je ale přesně definice ideálu I_α, jehož generátorem je m_α. Podle první věty o izomorfismu okruhů víme, že $K[x]/\langle m_\alpha\rangle \cong \operatorname{Im}\varphi$, tudíž $\operatorname{Im}\varphi$ je tělesem, navíc zřejmě $\operatorname{Im}\varphi \subseteq K(\alpha)$ a zároveň $\alpha \in \operatorname{Im}\varphi$, ale $K(\alpha)$ je nejmenším tělesem obsahující α, takže dohromady dostáváme, že $K(\alpha) = \operatorname{Im}\varphi$.

Tvrzení 3.3.2. *Nechť α je algebraický nad K a nechť $K(\alpha)$ je rozšíření tělesa K. Potom*

$$K(\alpha) \cong K[x]/\langle m_\alpha\rangle,$$

kde $m_\alpha \in K[x]$ je minimální polynom α.

Vidíme, že dva pohledy ukazují totéž: můžeme se dívat se na prvky jednoduchého rozšíření jako na zbytkové třídy ve tvaru $f + \langle m_\alpha\rangle$, kde $f \in K[x]$ je polynom, anebo jako na hodnotu polynomu s koeficienty z K v α, přičemž α je kořenem polynomu m_α.

Všimněme si, že úplně stejně jsme mohli reprezentovat prvky rozšíření tělesa K, které obsahovalo kořen polynomu $f(x) \in K[x]$ ireducibilního nad K. Navíc protože $f(x)$ je ireducibilní, stačí jej vynásobit inverzním prvkem vedoucího členu a dostáváme minimální polynom tohoto kořenu. Toto pozorování nám nabízí nové tvrzení.

Důsledek 3.3.1. *Nechť K je těleso, nad kterým je polynom $f(x) \in K[x]$ ireducibilní, a nechť α je jeho kořen v nějakém rozšíření tělesa K. Potom $K(\alpha)$ je rozšířením K obsahující α, jehož prvky lze reprezentovat jako lineární kombinaci $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$, kde n je stupeň $f(x)$.*

Ke stejnému závěru jsme došli již v předchozí kapitole.

Jelikož si $K(\alpha)$ můžeme představit jako polynomy po dělení polynomem v α ze zbytkem, vyvstává okamžitě otázka, jak je to s bází a dimenzí $K(\alpha)$

Tvrzení 3.3.3. *Nechť $K(\alpha) : K$ je rozšíření určené algebraickým prvkem α nad K. Označíme-li $n = deg\ m_\alpha$, potom*

1. $[K(\alpha) : K] = n$,
2. *množina prvků $\mathcal{B} = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ tvoří bázi $K(\alpha)$ nad K.*

Důkaz. Dokážeme, že $\mathcal{B}$ generuje $K(\alpha)$ a zároveň je lineárně nezávislá. Z předchozího tvrzení víme, že $\operatorname{Im}\varphi = K(\alpha)$, takže pro libovolný prvek $\beta \in K(\alpha)$ existuje vzor $f(x)$ tak, že $\beta = f(\alpha)$. Jak bylo řečeno, prvky $K(\alpha)$ lze reprezentovat jako polynomy nad K stupně nejvýše $n-1$, takže $\deg f(x) < n$.

Podívejme se nyní na lineární nezávislost. Předpokládejme, že $\mathcal{B}$ je lineárně nezávislá množina nad K, takže existují koeficienty $c_0, c_1, \ldots, c_{n-1} \in K$, ne všechny nulové, splňující rovnost

$$c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1} = 0$$

Protože existuje $c_i \neq 0 \in K, 0 \leq i < n$, potom existuje polynom nižšího stupně jak m_α mající α za kořen. To je ale spor, navíc protože je m_α ireducibilní, je m_α nesoudělný s každým netriviálním polynomem nižšího stupně, ale podle tvrzení 3.2.2 je m_α dělitelný. Nutně tak musí platit, že $c_i = 0$ pro všechna $0 \leq i < n$. □

Příklad 3.3.3.

1. Vezměme si $\mathbb{Q}(\sqrt{3})$. Minimální polynom $\sqrt{3}$ nad $\mathbb{Q}$ je $x^2 - 3$, jelikož $\sqrt{3}$ je iracionální. Podle 3.3.2 lze těleso $\mathbb{Q}(\sqrt{3})$ lze reprezentovat jako $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$.
2. Pokud $D \in \mathbb{Q}$, kde $\sqrt{D} \notin \mathbb{Q}$, pak $\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\}$. Pokud by $\sqrt{D} \in \mathbb{Q}$, pak $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}$. Takové rozšíření se nazývá *kvadratické rozšíření.*
3. Obecně pokud L je konečné rozšíření tělesa K, přičemž $[L : K] = 2$ a $\alpha \in L \setminus K$, pak rozšíření $K(\alpha)$ se nazývá kvadratické.

Pomocí tvrzení 3.3.3 můžeme také formulovat a dokázat nutnou a dostatečnou podmínku pro to, aby prvek α byl algebraický nad nějakým tělesem.

Tvrzení 3.3.4. *Prvek α je algebraický nad K právě tehdy, když rozšíření $K(\alpha) : K$ je konečné.*

Důkaz. Implikaci zprava doleva jsme dokázali u tvrzení 3.3.1. Pro důkazu druhé implikace máme, že α je algebraický nad K, takže podle tvrzení 3.3.3 platí $[K(\alpha) : K] = n$, kde $n \in \mathbb{N}$ je stupeň α nad K. □

3.3.2 Těleso generované více prvky

Od jednoduchého rozšíření se přesuneme k rozšířením generovaným více prvky. Příkladem takového rozšíření je již dříve uvedené rozšíření $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Nejprve určíme jeho stupeň rozšíření nad $\mathbb{Q}$. Snadno náhledneme, že $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ s minimálními polynomy $x^2 - 2$ a $x^2 - 3$, respektive. Dostáváme tak, že $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})]$. Hodilo by se nám tedy určit stupeň $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})]$. Abychom tento stupeň určili, uděláme si malou odbočku k tomu, jak chápat generování pomocí více prvků.

Tvrzení 3.3.5. *Nechť $K(\alpha, \beta)$ je rozšíření K generované prvky α, β a $(K(\alpha))(\beta)$ jednoduché rozšíření tělesa $K(\alpha)$ určené β. Potom $K(\alpha, \beta) = (K(\alpha))(\beta)$.*

Důkaz. Vidíme, že zřejmě $\alpha, \beta \in (K(\alpha))(\beta)$, takže $(K(\alpha))(\beta)$ je těleso obsahující prvky α, β, tudíž z definice $K(\alpha)$ plyne $K(\alpha, \beta) \subseteq (K(\alpha))(\beta)$. Podobně vidíme, že $K(\alpha) \subseteq (K(\alpha))(\beta)$, a protože $(K(\alpha))(\beta)$ je nejmenší těleso obsahující $K(\alpha)$ a β, dostáváme, že $(K(\alpha))(\beta) \subseteq K(\alpha, \beta)$. □

Dejme si nyní za cíl určit stupeň rozšíření tělesa generovaného konečným počtem algebraických prvků. Mějme konečně generované rozšíření $L = K(\alpha_1, \alpha_2, \ldots, \alpha_m)$, kde prvky $\alpha_1, \alpha_2, \ldots, \alpha_m$ jsou algebraické nad K, jejichž stupně nad K jsou postupně $n_1, n_2, \ldots, n_m$. Z předchozího tvrzení víme, že

$$K(\alpha_1, \alpha_2, \ldots, \alpha_m) = (K(\alpha_1, \alpha_2, \ldots, \alpha_{m-1}))(\alpha_m).$$

Stejně z výše uvedeného tvrzení plyne, že

$$(K(\alpha_1, \alpha_2, \ldots, \alpha_{m-1}))(\alpha_m). = (K(\alpha_1, \alpha_2, \ldots, \alpha_{m-2})(\alpha_{m-1}))(\alpha_m)$$

Díky tomuto postupu bude schopni odhadnout stupeň rozšíření $[L : K]$. Dosud jsme viděli, že stupeň jednoduchého rozšíření $K(\alpha_1) : K$ je určen minimálním polynomem α_1. Stejně tak se můžeme dívat nad stupeň rozšíření $K(\alpha_1, \alpha_2) : K(\alpha_1)$, protože stupeň $[K(\alpha_1, \alpha_2) : K(\alpha_1)]$ je roven stupni $[(K(\alpha_1)(\alpha_2) : K(\alpha_1)]$, který je roven stupni minimálního polynomu α_2 nad $K(\alpha_1)$. Co kdybychom ale uvážili rozšíření $[K(\alpha_1, \alpha_2) : K]$?

Využijeme tvrzení 3.1.3 k zodpovězení této otázky. Zřejmě $K \subseteq K(\alpha_1) \subseteq K(\alpha_1, \alpha_2) = (K(\alpha_1))(\alpha_2)$, takže nám toto tvrzení říká, že

$$[K(\alpha_1, \alpha_2) : K] = [K(\alpha_1, \alpha_2) : K(\alpha_1)] \cdot [K(\alpha_1) : K]$$

Víme, že $[K(\alpha_1) : K] = n_1$ a $[K(\alpha_1, \alpha_2) : K] = [(K(\alpha_1))(\alpha_2) : K(\alpha_1)] \leq n_2$, protože $[K(\alpha_2) : K] = n_2$ a přidáním prvku do tělesa můžeme pouze snížit stupeň rozšíření. Kombinací těchto poznatků dostaneme, že

$$[K(\alpha_1, \alpha_2) : K] = [K(\alpha_1, \alpha_2) : K(\alpha_1)] \cdot [K(\alpha_1) : K] \leq n_1 \cdot n_2.$$

Stejným postupem nakonec dojdeme k tomu, že

$$[K(\alpha_1, \alpha_2, \ldots, \alpha_m) : K] \leq n_1 n_2 \cdots n_m$$

Díky poslednímu poznatku můžeme formulovat nutnou a dostatečnou podmínku pro to, aby rozšíření $L : K$ bylo konečné.

Tvrzení 3.3.6. *Rozšíření L tělesa K je konečné právě tehdy, když je L generované konečným počtem algebraických prvků nad K.*

Důkaz. Pokud $L : K$ je konečné rozšíření, čili $[L : K] = n \in \mathbb{N}$, pak existuje báze $\beta_1, \beta_2, \ldots, \beta_n \in L$ generující L. Uvažme jednoduchá rozšíření $K(\beta_1), K(\beta_2), \ldots, K(\beta_n)$. Potom pro libovolné z těchto rozšíření $K(\beta_i)$ platí, že $[L : K] = [L : K(\beta_i)] \cdot [K(\beta_i) : K]$, a protože $L : K$ je konečné, musí nutně $K(\beta_i) : K$ být konečné, což implikuje, že $\beta_1, \beta_2, \ldots, \beta_n$ jsou algebraické nad K.

Dále vidíme, že $K(\beta_1, \beta_2, \ldots, \beta_n) \subseteq L$ a jelikož každý prvek L lze jednoznačně vyjádřit pomocí báze, pak inkluzí obdržíme, že $L = K(\beta_1, \beta_2, \ldots, \beta_n)$, tedy že L je generované konečným počtem algebraických prvků.

K důkazu druhé implikace položme $L = K(\alpha_1, \alpha_2, \ldots, \alpha_m)$, kde α_i pro $1 \leq i \leq m$ jsou algebraické prvky nad K, jejichž stupně nazvěme n_i pro $1 \leq i \leq m$. Před chvílí jsme ukázali, že $[K(\alpha_1, \alpha_2, \ldots, \alpha_m) : K] \leq n_1 n_2 \cdots n_m$, tudíž rozšíření $K(\alpha_1, \alpha_2, \ldots, \alpha_m)$ je konečné nad K.

□

Vraťme se k našemu příkladu o rozšíření $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Z předchozího tvrzení víme, že $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] \leq 4$ a zároveň víme, že $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$, z čehož dostáváme, že je dané rozšíření rovno 2, nebo 4.

Aby bylo rovno 2, musela by $\sqrt{3}$ ležet v $\mathbb{Q}(\sqrt{2})$. Předpokládejme tedy, že existují $a, b \in \mathbb{Q}$ tak, aby $a + b\sqrt{2} = \sqrt{3}$. Zjevně $b \neq 0$, protože $a \in \mathbb{Q}$ ale $\sqrt{3}$ je iracionální. Obdobně $a \neq 0$, pak by nutně pro b ve tvaru $b = \frac{p}{q}$, kde $p, q \in \mathbb{Z}$, $(p, q) = 1$ a $q \neq 0$, platilo

$$\frac{p}{q} \cdot \sqrt{2} = \sqrt{3} \quad \Rightarrow \quad 2p^2 = 3q^2,$$

z čehož bychom dostali, že $2|q$, tedy $4|q^2$. Potom ovšem $4|2p^2$, takže $2|p$, ale to je ve sporu s předpokladem $(p, q) = 1$.

Předpokládejme tak, že $ab \neq 0$. Po umocnění obou stran dostáváme, že

$$a^2 + 2\sqrt{2}ab + 2b^2 = 3$$
$$\sqrt{2} = \frac{3 - a^2 - 2b^2}{2ab} \in \mathbb{Q}$$

Ovšem $\sqrt{2} \notin \mathbb{Q}$, takže $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, tudíž nutně dostáváme, že $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.

3.4 Rozkladové těleso

Posledním rozšířením, kterému věnujeme pozornost, je tzv. *rozkladové těleso*. Prvně se však seznámíme s rozšířením, které nám bude povědomější, a to *kořenovým rozšířením*.

Definice 3.4.1. Nechť K je těleso a $f(x) \in K[x]$. Řekneme, že těleso L je kořenovým rozšířením K určeným polynomem $f(x)$, jestliže

1. $K \subseteq L$,
2. $\exists \alpha \in L : \alpha$ je kořen $f(x)$,
3. $L = K(\alpha)$.

Příklad 3.4.1. Kořenová rozšíření určené polynomem $x^4 - x^2 - 2 \in \mathbb{Q}$ jsou $\mathbb{Q}(i)$ a $\mathbb{Q}(\sqrt{2})$, protože $x^4 - x^2 - 2 = (x^2 + 1)(x^2 - 2)$.

Definice nám vlastně říká, že kořenové rozšíření určené nějakým polynomem nad libovolným tělesem je minimální těleso vzhledem k inkluzi takové, že obsahuje jeho kořen. Podobná věta však zazněla při hledání tělesa majícího alespoň jeden kořen polynomu, který byl nad jistým tělesem ireducibilní. Ukážeme si, že jsme tehdy ve skutečnosti měli co do činění s kořenovým rozšířením.

Tvrzení 3.4.1. *Nechť K je těleso a $f(x) \in K[x]$ polynom nad K. Potom existuje kořenové rozšíření tělesa K určené $f(x)$, které v případě, že f je ireducibilní nad K, je jednoznačně určené až na izomorfismus.*

Důkaz. Dokážeme si zde pouze existenční část, jednoznačnost je dokázána například v [8]. Označme L hledané kořenové rozšíření. Pokud $f(x)$ má kořen v K, potom zřejmě $L = K$. Předpokládejme tedy, že f je ireducibilní nad K. Potom $K[x]/\langle f \rangle$ je těleso obsahující alespoň jeden kořen α a zároveň je toto těleso izomorfní s jednoduchým rozšířením $K(\alpha)$, takže $L = K[\alpha]/\langle f \rangle$. □

Příklad 3.4.2.

1. Kořenové rozšíření určené polynomem $x^2 - 2$ je $\mathbb{Q}(\sqrt{2})$.
2. Uvážíme-li polynom $f(x) = x^2 + 2x + 2 \in \mathbb{Z}_3[x]$, pak $f(x)$ je zřejmě ireducibilní nad $\mathbb{Z}_3$. Jeho kořenové rozšíření je $\mathbb{Z}_3[\alpha]/\langle \alpha^2 + 2\alpha + 2 \rangle$.

Pro další pokračování v práci nebude nicméně tak důležité kořenové rozšíření jako *rozkladové rozšíření*. Na rozdíl od kořenového rozšíření ovšem nebude požadavek, aby obsahoval kořen polynomu, ale dokonce, aby obsahoval všechny kořeny.

Definice 3.4.2. Nechť K je těleso a $f(x) \in K[x]$ polynom stupně $n \in \mathbb{N}$. Řekneme, že L je rozkladovým rozšířením určeným polynomem $f(x)$, jestliže

1. $\exists \alpha_1, \alpha_2, \ldots, \alpha_n \in L$ tak že $f(x) = a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$, kde $a_n \in K$ je vedoucí koeficient $f(x)$,
2. $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Rozkladové rozšíření daného polynom nám umožní rozklad daného polynomu na součin lineárních mnohočlenů. Příkladem známého rozkladového rozšíření jsou komplexní čísla s libovolným reálným polynomem mající alespoň jeden nereálný kořen. Podobně jako u kořenového rozšíření existuje pro libovolný polynom rozkladové rozšíření.

Tvrzení 3.4.2. *Nechť K je těleso a $f(x) \in K[x]$ polynom nad K. Potom existuje rozkladové rozšíření určené polynomem $f(x)$ a toto rozšíření je v případě, že f je ireducibilní nad K, jednoznačně určeno až na izomorfismus.*

Důkaz. Důkaz existenční části provedeme pomocí indukce vzhledem k rozdílu stupně polynomu a počtu ireducibilních polynomů v rozkladu $f(x)$ nad K, nazvěme jej n. Aby totiž polynom $f(x)$ byl rozložitelný nad nějakým tělesem na pouze lineární polynomy, musí být $n = 0$. Pro $n = 0$ lze polynom rozložit na součin lineárních polynomů nad K, v tomto případě je rozkladovým rozšířením přímo K.

Předpokládejme, že pro dané $n = k$ tvrzení platí a uvažme, že pro polynom $f(x)$ platí $n = k + 1$. V rozkladu $f(x)$ je alespoň jeden polynom alespoň stupně 2, který je ireducibilní nad K. Vezměme si kořenové rozšíření L tělesa K určené libovolným takovým ireducibilním polynomem, které jistě existuje podle předchozího tvrzení. Pro polynom $f(x)$ nad L platí jistě, že $n < k+1$, a tak můžeme užít indukčního předpokladu pro $n = k$. Díky tomu, že kořenové rozšíření je minimální těleso, nad kterým existuje kořen daného polynomu, máme zaručeno, že získané rozkladové rozšíření je minimální.

Druhá část důkazu je k nalezení v [8]. □

Příklad 3.4.3.

1. Mějme polynom x^2-2, pak kořeny jsou $\pm\sqrt{2}$, tudíž $\mathbb{Q}(\sqrt{2})$ je jeho kořenovým i rozkladovým rozšířením.
2. Ne vždy je kořenové rozšíření shodné s rozkladovým rozšířením. Typickým příkladem je rozkladové rozšíření určené polynomem $x^3-2=0$. Polynom lze rozložit na tvar $(x-\sqrt[3]{2})(x^2+\sqrt[3]{2}x+\sqrt[3]{4})$, snadno si poté ověříme, že kořeny daného polynomu jsou

$$x_1 = \sqrt[3]{2}, \quad x_2 = \sqrt[3]{2}\left(\frac{-1-i\sqrt{3}}{2}\right), \quad x_3 = \sqrt[3]{2}\left(\frac{-1+i\sqrt{3}}{2}\right).$$

   Letmým pohledem můžeme odhadnout, že daným rozkladovým tělesem je $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$, jistě totiž dokážeme vyjádřit všechny zmíněné kořeny pomocí $\sqrt[3]{2}, i\sqrt{3}$ a $\mathbb{Q}$. Dokázat bychom to mohli tím, že bychom nalezli stupeň rozšíření $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}$, což by se dokazovalo obdobně jako při hledání stupně rozšíření $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$.

   Kořenovým rozšířením určeným tímto polynomem je však těleso $\mathbb{Q}(x_1) \cong \mathbb{Q}(x_2)$.

Kapitola 4

Konečná tělesa

4.1 Základní vlastnosti konečných tělesech

V této sekci se zaměříme na fundamentální tvrzení, jež budou potřebná v pokračování o konečných tělesech, týkající se zejména rozkladu polynomů nad konečnými tělesy.

V teorii těles jsme se setkali s pojmem *charakteristika tělesa*. Jak víme, charakteristika těles může být rovna buď 0 nebo nějakému prvočíslu p. Konečná tělesa mají vždy prvočíselnou charakteristiku. Prvočíselná charakteristika p také znamená, že je prvotěleso libovolného konečného tělesa izomorfní s $\mathbb{F}_p$, tělesem majícím prvočíselný počet prvků roven p. Těleso $\mathbb{F}_p$ je tak jednoznačné až na izomorfismus, a tak můžeme s $\mathbb{F}_p$ pracovat jako s $\mathbb{Z}_p$.

S charakteristikou tělesa dále souvisí *Frobeniovo zobrazení*. Jak uvidíme, toto zobrazení má klíčové vlastnosti v následujících kapitolách. Začněme jeho definicí.

Definice 4.1.1. Pro libovolné těleso F charakteristiky $p > 0$ definujme Frobeniovo zobrazení jako zobrazení $\varphi : F \mapsto F$ s předpisem $\varphi(a) = a^p$.

Právě definované zobrazení je navíc homomorfismus pro nenulovou charakteristiku tělesa.

Tvrzení 4.1.1. *Nechť F je těleso charakteristiky p. Potom pro libovolné dva prvky $a, b \in \mathbb{F}_q$ a libovolné $n \in \mathbb{N}$ platí*

$$\begin{aligned}(a+b)^{p^n} &= a^{p^n} + b^{p^n}\\ (ab)^{p^n} &= a^{p^n} b^{p^n}.\end{aligned}$$

Důkaz. Dokážeme-li, že $(a+b)^p = a^p + b^p$, potom jsme dokázali, že $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ (stačí místo a, b napsat $a^{p^{n-1}}, b^{p^{n-1}}$, respektive, a takto můžeme pokračovat, až se dostaneme k první mocnině p). Rozšiřme výraz pomocí binomické věty:

$$(a+b)^p = \binom{p}{0}a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \cdots + \binom{p}{p}b^p.$$

Nyní si již stačí povšimnout, že $\binom{p}{k}$ pro $1 \leq k < p$ je dělitelné p; hodnotu $\binom{p}{k}$ si můžeme rozepsat jako

$$\frac{p!}{k!(p-k)!} = \frac{p(p-1)\cdots(p-k+1)}{k!},$$

pak v rozkladu tohoto výrazu na prvočinitele se bude jistě vyskytovat pro takto ohraničené k prvočíslo p, jelikož k i $p-k$ jsou menší jak p. Protože uvažujeme Frobeniovo zobrazení u tělesa s nenulovou charakteristikou, každý člen dělitelný p je roven 0 a dostáváme tak, že

$$(a+b)^p = \binom{p}{0}a^p + \binom{p}{p}b^p = a^p + b^p.$$

Druhá část tvrzení pro násobení je zřejmá, jelikož stačí levou stranu pouze rozepsat a díky komutativitě násobení upravit na kýžený tvar. □

Obdobně jako při zkoumání zobrazení tělesa $K[x]/\langle f\rangle$ na $K(\alpha)$ v předchozí kapitole se podívejme také u Frobeniova zobrazení na jeho jádro $\operatorname{Ker}\varphi$. K tomu budeme potřebovat jedno pomocné tvrzení.

Tvrzení 4.1.2. *Pokud F je těleso, pak jeho jedinými ideály jsou $\{0\}$ a samotné F.*

Důkaz. Buď $I \subseteq F$ ideál tělesa F. Předpokládejme, že $I \neq \{0\}$. Vezměme si nenulový prvek $a \in I$. Potom $1 = a \cdot a^{-1} \in I$, takže každý prvek $x \in F$ leží v I, jelikož $x \cdot 1 \in I$. □

Důsledek 4.1.1. *Frobeniovo zobrazení nad konečným tělesem F je izomorfismus.*

Důkaz. Označme $\varphi : F \mapsto F$ Frobeniovo zobrazení. Již víme, že φ je homomorfismem, zbývá dokázat, že je dané zobrazení injektivní a surjektivní. Jádro $\operatorname{Ker}\varphi$ je ideálem F a z předchozího tvrzení tak dostáváme, že

$$\operatorname{Ker}\varphi = \{a \mid \varphi(a) = 0\} = \{0\},$$

neboť například $\varphi(1) = 1$, takže nemůže platit, že $\operatorname{Ker}\varphi = F$.

Frobeniovo zobrazení je zřejmě surjektivní, neboť se jedná o injektivní zobrazení z konečné množiny do konečné množiny stejné kardinality. □

Přesuňme se k hledání vlastností jednotlivých grup tělesa. Konkrétně k tomu, jak dané prvky grup *generovat* pomocí jejich prvku.

Není příliš překvapivé, že ne vždy dokážeme aditivní grupu vygenerovat z jediného prvku, tedy ne vždy je cyklická. Takovým protipříkladem může být libovolný prvek tělesa $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$, kde zjevně nedokážeme vygenerovat prvky pomocí opakovaného sčítání jednoho prvku. Co však může být překvapivé je fakt, že multiplikativní grupa libovolného konečného tělesa lze vygenerovat pomocí alespoň jednoho prvku. Před dalším pokračováním si přesněji definujeme pojem generátor grupy.

Definice 4.1.2. Prvek g konečné grupy G je primitivním prvkem G, jestliže jeho řád je roven $|G|$.

S generováním grupy a následujícím tvrzení souvisí následující dvě lemmata.

Lemma 4.1.1. *Nechť $G = \langle a \rangle$ je cyklická grupa řádu n. Potom*

1. *a^k generuje cyklickou grupu řádu $\frac{n}{(n,k)}$.*
2. *Pro libovolné $d|n$ obsahuje grupa G právě $\varphi(d)$ prvků řádu d.*

Důkaz.

1. $a^k = 1$ právě když $n|k$. Hledáme tedy nejmenší přirozené číslo m splňující $a^{mk} = 1$. Musí proto platit, že $n|mk$. Pokud bychom položili $m = n$, jistě by n dělilo mk. Jakým největším přirozeným číslem můžeme vydělit n tak, aby $n|mk$? Odpověď je: číslem odpovídající největší společné části v rozkladu čísel n, k na prvočinitele. To ale přesně odpovídá největšímu společnému děliteli (n, k), takže $m = \frac{n}{(n,k)}$.
2. Protože $d|n$, existuje přirozené k takové, že $n = kd$. Z předchozího lemma víme, že prvek $a^i \in \langle a \rangle$ má řád d, jestliže $(n, i) = k$. Protože $n = kd$, lze největší společný dělitel přepsat na $(kd, i) = k$, ale protože na pravé straně se nachází k, lze největšího společného dělitele upravit na tvar $(d, i) = 1$. Hledáme všechna $i \in \mathbb{N}$ splňující $(d, i) = 1$, to je ale ekvivalentní s definicí Eulerovy funkce v d, čili hledaný počet je roven $\varphi(d)$.

□

A pojďme již k samotnému tvrzení.

Tvrzení 4.1.3. *Grupa $\mathbb{F}_q^*$ konečného tělesa $\mathbb{F}_q$ s q prvky je cyklická.*

Důkaz. Pokud dokážeme existenci primitivního prvku v $\mathbb{F}_q^*$, budeme hotovi. Grupa $\mathbb{F}_q^*$ obsahuje nejvýše jednu podgrupu libovolného řádu d; uvážíme-li totiž polynom $x^d - 1 \in \mathbb{F}_q[x]$, hledání jeho kořenů je ekvivalentní s hledáním řešení rovnice $x^d = 1$, jejíž jedním řešením je prvek $a \in \mathbb{F}_q^*$ řádu d. Ovšem potom libovolný prvek g grupy $\langle a \rangle$ splňuje $g^d = 1$. Protože $\langle a \rangle$ obsahuje d prvků, tvoří prvky této cyklické grupy všechny kořeny polynomu $x^d - 1$. Z toho plyne, že existuje nanejvýše jedna podgrupa $\mathbb{F}_q^*$ řádu d.

Z Lagrangeovy věty však víme, že řád d nemůže být libovolný, ale musí být dělitelem řádu $|\mathbb{F}_q^*| = q-1$. Proto můžeme uvažovat pouze ty podgrupy řádu $d|(q-1)$. Podle předchozího lemma existuje v každé cyklické podgrupě řádu d právě $\varphi(d)$ prvků řádu d. Každý prvek grupy $\mathbb{F}_q^*$ musí mít konečný řád, takže jejich sjednocením dostáváme, že

$$\sum_{d|(q-1)} \varphi(d) \leq q - 1.$$

Z první kapitoly ale víme, že

$$\sum_{d|(q-1)} \varphi(d) = q - 1,$$

což nám říká, že sjednocením všech těchto podgrup dostaneme celou grupu $\mathbb{F}_q^*$. Nás ovšem zajímá konkrétní případ, kdy $d = q - 1$, jelikož $\varphi(q-1) \geq 1$, tudíž existuje v $\mathbb{F}_q^*$ primitivní prvek. □

Jak je to s počtem prvků konečného tělesa? Na rozdíl od grup, které mohou mít libovolný počet prvků, se u těles setkáme s jistým omezením, které je způsobeno komplikovanější strukturou, než můžeme vidět u grup. K zodpovězení této otázky nám pomůže pojetí tělesa jako vektorového prostoru nad jeho podtělesem.

Tvrzení 4.1.4. *Každé konečné těleso má p^n prvků, kde $p \in \mathbb{N}$ je prvočíslo a $n \in \mathbb{N}$.*

Důkaz. Nazvěme naše konečné těleso $\mathbb{F}_q$. Jak již bylo naznačeno, pojmeme $\mathbb{F}_q$ jako vektorový prostor nad $\mathbb{F}_p$. Pak libovolný prvek $a \in \mathbb{F}_q$ lze jednoznačně vyjádřit ve formě $a = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n$, kde $n = [\mathbb{F}_q : \mathbb{F}_p]$ a $c_i \in \mathbb{F}_p$ pro $1 \leq i \leq n$. Bázi máme předem určenou, a tak všechny prvky generujeme různou volbou $c_1, c_2, \ldots, c_n$. Za každý takovýto koeficient můžeme dosadit $|\,\mathbb{F}_p\,| = p$ různých prvků, celkem tak získáme p^n prvků. □

Důkaz tvrzení nám dokonce říká konkrétně, že počet prvků libovolného konečného tělesa je roven p^n, kde p je *charakteristika* $\mathbb{F}_q$ a n dimenze $[\mathbb{F}_q : \mathbb{F}_p]$. Ihned se dále nabízí otázka, zda pro každé prvočíslo p a libovolné $n \in \mathbb{N}$ existuje konečné těleso. K zodpovězení této otázky jsme se ve skutečnosti velice přiblížili při konstrukci tělesa $K[x]/\langle f \rangle$; zvolíme-li totiž $K = \mathbb{Z}_p$ a pokud $\deg f = n$, potom získáme těleso s p^n prvky.

4.2 Existence konečného tělesa

Problém při konstrukci konečného tělesa jako $\mathbb{Z}_p[x]/\langle f \rangle$ spočívá v tom, že nevíme, zda existuje ireducibilní polynom $f \in \mathbb{Z}_p[x]$ libovolného stupně $n \in \mathbb{N}$. V průběhu této sekce si ukážeme, že opravdu existuje konečné těleso, jenž je libovolnou přirozenou mocninou prvočísla. Tato sekce bude zejména využívat polynomu $x^q - x \in \mathbb{F}_p[x]$, který, jak nám následující lemma napovídá, je propojen s konečnými tělesy.

Lemma 4.2.1. *Nechť $\mathbb{F}_q$ je těleso s q prvky. Potom pro každý prvek $\alpha \in \mathbb{F}_q$ platí $\alpha^q - \alpha = 0$.*

Důkaz. Jistě má každý prvek $\alpha \in \mathbb{F}^*{}_q$ konečný řád, jinak by $\mathbb{F}_q$ nebylo konečné. Z Lagrangeovy věty dostáváme, že řád každého prvku dělí řád $|\mathbb{F}^*{}_q| = q - 1$, takže jistě $\alpha^{q-1} = 1$. To znamená, že každý prvek $\alpha \in \mathbb{F}_q^*$ je kořenem polynomu $x^{q-1} - 1$. Abychom zahrnuli i $0 \in \mathbb{F}_q$, stačí upravit polynom na tvar $x^q - x$, a tudíž $\alpha^q - \alpha = 0$ pro všechny prvky $\mathbb{F}_q$. □

Dejme si nyní za cíl nalézt rozkladové těleso určené polynomem $x^q - x \in \mathbb{F}_p$, kde $q = p^n$ je přirozená mocnina prvočísla. Potřebujeme tento polynom rozložit na součin lineárních polynomů. Následující lemma nám rovnou na tuto otázku odpovídá.

Lemma 4.2.2. *Nechť $\mathbb{F}_q$ je konečné těleso s q prvky a $f(x) = x^q - x \in \mathbb{F}_p[x]$. Potom se polynom $f(x)$ rozkládá nad $\mathbb{F}_q$ následovně:*

$$x^q - x = \prod_{a \in \mathbb{F}_q} (x - a).$$

Důkaz. Z předchozího lemma víme, že pro každé $a \in \mathbb{F}_q$ je kořenem $x^q - x$. Polynom $x^q - x$ může mít však nejvýše q kořenů, a protože všechny prvky $\mathbb{F}_q$ jsou kořeny daného polynomu, žádné jiné neexistují nad $\mathbb{F}_q$. Protože navíc je polynom $x^q - x$ normovaný, pak zřejmě $\prod_{a \in \mathbb{F}_q}(x-a) = x^q - x$. □

Příklad 4.2.1. Mějme těleso $\mathbb{F}_4 = \mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$ a označme $\alpha = x + \langle x^2 + x + 1\rangle$. Potom podle předchozího tvrzení je rozklad $x^4 - x \in \mathbb{Z}_2[x]$ následující

$$x^4 - x = x(x-1)(x-\alpha)(x-\alpha^2).$$

Polynom $x^q - x \in \mathbb{F}_p[x]$ lze tedy rozložit na součin lineárních polynomů nad $\mathbb{F}_q$. Kandidátem pro hledané rozkladové rozšíření je tak těleso $\mathbb{F}_q$ s q prvky. Musíme ještě ověřit minimalitu $\mathbb{F}_q$ vzhledem k inkluzi. Ukážeme si, že rozkladové rozšíření zmíněného polynomu se skládá pouze z kořenů daného polynomu. Dosud jsme nevyužili předpokladu, že $q = p^n$ je přirozená mocnina prvočísla, kvůli následujícímu tvrzení však pochopíme, proč jsme tento požadavek zahrnuli.

Tvrzení 4.2.1. *Nechť $q = p^n$, kde p je prvočíslo a $n \in \mathbb{N}$. Rozkladové rozšíření polynomu $f(x) = x^q - x \in \mathbb{F}_p[x]$ je $\mathbb{F}_q$, konečné těleso s q prvky.*

Důkaz. Nechť K je rozkladové rozšíření určené polynomem $x^q - x \in \mathbb{F}_p[x]$. Potřebujeme ukázat, že $F = \{\alpha \in K \mid \alpha^q = \alpha\}$ je rovno K a že má q prvků. Uvážíme-li derivaci polynomu $f(x) \in \mathbb{F}_p$, obdržíme polynom $f' = qx^{x-1} - 1$. Protože však $q = p^n$, dostáváme, že $f' = 0 - 1 = -1$, a protože tím pádem f a f' jsou nesoudělné polynomy, tak f nemá násobný kořen, a tudíž $|F| = q$.

Inkluze $F \subseteq K$ je zřejmá, k ověření $K \subseteq F$ je potřeba ukázat, že F je těleso. To provedeme například tak, že ukážeme, že F je podtělesem K.

1. (F je komutativní grupa vzhledem ke sčítání) Vezměme si $a, b \in F$, potom $(a-b)^q - (a-b) = (a-b)^{p^n} - (a-b) = a^{p^n} - b^{p^n} - (a-b) = a - b - (a-b) = 0$, kde jsme využili lemma 4.2.1.
2. ($F \setminus \{0\}$ je komutativní grupa vzhledem ke násobení) Vezměme si $a, b \in F$, potom $(ab^{-1})^q - ab^{-1} = (ab^{-1})^{p^n} - ab^{-1} = a^{p^n}b^{-p^n} - ab^{-1} = ab^{-1} - ab^{-1} = 0$.

Rozkladové rozšíření je nejmenší těleso, jenž obsahuje všechny kořeny polynomu, a proto $K \subseteq F$, jelikož F je těleso. Dostáváme tak, že $F = K$. □

Kromě toho, že jsme si splnili cíl nalézt rozkladové rozšíření $x^{p^n} - x$, jsme se také dopracovali k zodpovězení otázky existence konečného tělesa.

Důsledek 4.2.1. *Pro libovolné prvočíslo p a přirozené číslo n existuje konečné těleso s p^n prvků. Konečné těleso s p^n prvky je určeno jednoznačně až na izomorfismus.*

Důkaz. Vezměme s polynom $x^{p^n} - x \in \mathbb{F}_p$, potom jeho rozkladovým tělesem je konečné těleso s p^n prvků. Druhá část tvrzení plyne z faktu, že rozkladové těleso je určené jednoznačně až na izomorfismus. □

Díky důsledku 4.2.1 je značení konečného tělesa s q prvky jako $\mathbb{F}_q$ jednoznačné až na izomorfismus. V dalším pokračování práce tak budeme rozumět symbolem $\mathbb{F}_q$ konečné těleso s q prvky, přičemž jeho charakteristika p je vystižena tím, mocnina jakého prvočísla p je počet prvků q. Prvotěleso konečného tělesa $\mathbb{F}_q$, kde $q = p^n$, budeme značit obvyklým způsobem jako $\mathbb{F}_p$.

Příklad 4.2.2. Uvažme tělesa $\mathbb{Z}_3[x]/\langle x^2 + 1\rangle$ a $\mathbb{Z}_3[x]/\langle x^2 + x + 2\rangle$. Obě tělesa mají $3^2 = 9$ prvků a podle 4.2.1 jsou izomorfní. Počítání v obou tělesech je tak totožné vzhledem k izomorfismu a obě tělesa shrnujeme pod značení $\mathbb{F}_9$.

Když už nyní víme, jak to je s počtem prvků konečného tělesa a jak konečná tělesa vypadají, nabízí se vyřešit problém, jak vypadají podtělesa konečného tělesa.

Tvrzení 4.2.2. *Nechť p je prvočíslo, $n \in \mathbb{N}$ a $\mathbb{F}_{p^n}$ konečné těleso s p^n prvky. Potom každé podtěleso tělesa $\mathbb{F}_{p^n}$ má p^m prvků pro $m \in \mathbb{N}$ takové, že $m|n$. Navíc pro každé $m|n$ existuje právě jedno konečné podtěleso s tělesa $\mathbb{F}_{p^n}$ s p^m prvky.*

Důkaz. Těleso $\mathbb{F}_{p^n}$ má charakteristiku p, a tudíž i jeho libovolné podtěleso musí mít tutéž charakteristiku. Nechť $\mathbb{F}_q$ je podtěleso tělesa $\mathbb{F}_{p^n}$. Podtěleso $\mathbb{F}_q$ je konečné, a proto musí mít p^m prvků pro nějaké $m \in \mathbb{N}$. Zbývá ukázat, že $m|n$. K tomu postačí uvažovat těleso $\mathbb{F}_{p^n}$ jako vektorový prostor nad $\mathbb{F}_q$. Každé konečné těleso s p^n prvky má své prvotěleso $\mathbb{F}_p$, čímž dostáváme inkluzi $\mathbb{F}_p \subseteq \mathbb{F}_q \subseteq \mathbb{F}_{p^n}$ a můžeme použít tvrzení 3.1.3, díky němuž dostaneme, že $n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_q][\mathbb{F}_q : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_q] \cdot m$, takže $m|n$.

Nechť nyní $m|n$ pro $m \in \mathbb{N}$. Pro druhou část tvrzení si vezměme polynomy $x^{p^n} - x$ a $x^{p^m} - x$ nad $\mathbb{F}_p$. Rozkladová tělesa polynomů $x^{p^n} - x, x^{p^m} - x$ nad $\mathbb{F}_p$ jsou tělesa $\mathbb{F}_{p^n}, \mathbb{F}_{p^m}$, respektive. Pokud ukážeme, že $(p^m - 1)|(p^n - 1)$ a že i $(x^{p^m} - x)|(x^{p^n} - 1)$, potom je dokázána inkluze $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$.

Díky předpokladu $m|n$ existuje $d \in \mathbb{N}$ splňující $n = md$. Potom

$$p^n - 1 = p^{md} - 1 = (p^m)^d - 1 = (p^m - 1)(p^{md-1} + p^{md-2} + \cdots + 1) \quad \Rightarrow \quad (p^m - 1)|(p^n - 1).$$

Obdobně potom existuje $r \in \mathbb{N}$ splňující $p^n - 1 = r(p^m - 1)$ a dostáváme, že

$$x^{p^n-1} - 1 = x^{r(p^m-1)} - 1 = (x^{p^m-1})^r - 1 = (x^{p^m-1} - 1)(x^{r(p^m-1)-1} + p^{r(p^m-1)-2} + \cdots + 1),$$

a proto $(x^{p^n} - x)|(x^{p^m} - x)$, takže existuje právě jedno podtěleso tělesa $\mathbb{F}_{p^n}$ s p^m prvky. Pokud by existovalo ještě jiné podtěleso s p^m prvky, pak by polynom $x^{p^m} - x$ měl více než p^m kořenů, což není možné. □

Dostáváme se postupně mimo jiné také k důkazu, který jsme potřebovali, abychom věděli, že vždy existuje ireducibilní polynom nad konečným tělesem $\mathbb{F}_q$ libovolného stupně, což také dokazuje, že vždy jsme schopni sestrojit konečné těleso jako $\mathbb{F}_q[x]/\langle f\rangle$, kde $f \in \mathbb{F}_q[x]$ je ireducibilní polynom.

Tvrzení 4.2.3. *Pro každé $m \in \mathbb{N}$ existuje ireducibilní polynom nad $\mathbb{F}_{p^n}$.*

Důkaz. Vezměme si konečné těleso $\mathbb{F}_{q^m}$, kde $q = p^n$, jehož existence je zaručena tvrzením 4.2.1. Rozšíření $\mathbb{F}_{q^m} : \mathbb{F}_q$ má stupeň m, takže je konečné, a tedy i algebraické. Pokud označíme $\alpha \in \mathbb{F}_{q^m}$ primitivní prvek multiplikativní grupy tělesa $\mathbb{F}_{q^m}$, potom zřejmě $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$, tudíž minimální polynom α nad $\mathbb{F}_q$ je ireducibilní polynom stupně $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$. □

4.3 Kořeny ireducibilních polynomů a primitivní polynomy

Jak nám předchozí tvrzení 4.2.3 říká, máme garantováno, že nad libovolným konečným tělesem existuje ireducibilní polynom libovolného stupně. V poslední sekci této kapitoly si řekneme, jak vypadají kořeny ireducibilního polynomu nad konečným tělesem a také se podíváme na primitivní polynomy.

Vraťme se k našemu polynomu $x^{p^n} - x \in \mathbb{F}_p[x]$. Ireducibilní polynomy totiž dokážeme najít i v rozkladu tohoto polynomu, jak nám říká následující tvrzení.

Tvrzení 4.3.1. *Nechť $\mathbb{F}_{p^n}$ je konečné těleso a $f \in \mathbb{F}_p[x]$ ireducibilní polynom nad $\mathbb{F}_p$ stupně $m \in \mathbb{N}$. Pak $f|(x^{p^n} - x)$ právě tehdy, když $m|n$.*

Důkaz. Předpokládejme, že $f|(x^{p^n} - x)$ a nechť F je kořenové rozšíření určené f nad $\mathbb{F}_p$. Potom z podmínky $f|(x^{p^n} - x)$ víme, že existuje polynom g nad nějakým rozšířením $\mathbb{F}_p$ takový, že $x^q - x = gf$. Označíme-li $\alpha \in F$ kořen f, pak díky tomu vidíme, že $\alpha^{p^n} - \alpha = g(\alpha)f(\alpha) = 0$, tudíž $\alpha \in \mathbb{F}_{p^n}$. Ovšem stupeň rozšíření $[\mathbb{F}_p(\alpha) : \mathbb{F}_p]$ je roven m, protože polynom $a^{-1}f$, kde $a \in \mathbb{F}_{p^n}$ je vedoucí koeficient f, je minimální polynom α stupně m. Zřejmě také $\mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^n}$, čímž dostáváme, že $n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_p(\alpha)][\mathbb{F}_p(\alpha) : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_p(\alpha)]m$, a proto $m|n$.

Naopak nyní předpokládejme, že $m|n$. Opět si vezměme kořenové rozšíření F určené f nad $\mathbb{F}_p$ a nechť $\alpha \in F$ je kořen f. Pak, jak jsme si již zdůvodnili v předchozím části důkazu, platí $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = m$. Jelikož $|\,\mathbb{F}_p\,| = p$, má těleso $\mathbb{F}_p(\alpha)$ právě p^m prvků. Navíc $m|n$, a proto je $\mathbb{F}_p(\alpha)$ podtělesem $\mathbb{F}_{p^n}$. Důsledkem tohoto faktu je, že $\alpha \in \mathbb{F}_{p^n}$, jelikož $\alpha \in \mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$. □

V průběhu důkazu tvrzení 4.3.1 jsme narazili na kořenové rozšíření ireducibilního polynomu stupně $m \in \mathbb{N}$ nad konečným tělesem $\mathbb{F}_{p^n}$. Zjistili jsme , že jeho kořenovým rozšířením je podtěleso $\mathbb{F}_{p^m}$ tělesa $\mathbb{F}_{p^n}$. Následující tvrzení uvedený poznatek ještě zesílí.

Tvrzení 4.3.2. *Rozkladovým rozšířením určeným ireducibilním polynomem f nad $\mathbb{F}_p$, jehož stupeň je roven $m \in \mathbb{N}$, je těleso $\mathbb{F}_{p^m}$. Označíme-li navíc $\alpha \in \mathbb{F}_{p^m}$, pak prvky $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{m-1}}$ jsou kořeny f.*

Důkaz. Jako v důkazu tvrzení 4.3.1 buď F kořenové rozšíření určené f nad $\mathbb{F}_p$ a $\alpha \in F$ kořen f. Pak $\mathbb{F}_p \subseteq \mathbb{F}_p(\alpha)$ a $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = \deg f = m$, takže $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^m}$. Nyní ukažme, že každý prvek α^{p^i} pro $0 \leq i \leq p^m - 1$ je také kořenem f. Položme $f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0$, kde $a_i \in \mathbb{F}_p$ pro $0 \leq i \leq m$, Dosaďme do polynomu obecně α^{p^i}:

$$\begin{aligned} f(\alpha^{p^i}) &= a_m\alpha^{mp^i} + a_{m-1}\alpha^{(m-1)p^i} + \cdots + a_1\alpha^{p^i} + a_0 \\ &= (a_m\alpha^m + a_{m-1}\alpha^{m-1} + a_1\alpha + a_0)^{p^i} \\ &= (f(\alpha))^{p^i} = 0, \end{aligned}$$

přičemž jsme vyžili faktu, že Frobeniovo zobrazení je homomorfismus. Tím jsme dokázali, že F je i rozkladovým rozšířením. U druhé části řešení nám však zbývá dokázat, že jsme nalezli všech m kořenů, tedy že všechny tyto kořeny jsou různé.

Zvolme $0 \leq i < j < m$ a předpokládejme, že $\alpha^{p^i} = \alpha^{p^j}$. Potom však

$$\alpha^{p^{i-j}} - \alpha = 0.$$

Opět můžeme využít Frobeniova zobrazení, abychom získali tvar

$$\begin{aligned} (\alpha^{p^{i-j}} - \alpha)^{p^m} &= 0 \\ \alpha^{p^{m+i-j}} - \alpha &= 0. \end{aligned}$$

Z vlastností minimálního polynomu α nad $\mathbb{F}_p$ navíc platí, že $f | x^{m+i-j} - x$; $a_m^{-1}f$ je minimální polynom α a platí, že každý polynom nad $\mathbb{F}_p$ mající α za kořen musí být dělitelný $a_m^{-1}f$, a tedy i f. Důkaz nám tak zkompletuje tvrzení 4.3.1, jelikož podle něj musí platit, že $m|n$, ale zjevně m nedělí $m + i - j$, protože $m + i - j < m$. □

Poznámka. Tvrzení 4.3.2 lze také interpretovat tak, že pokud $\alpha \in \mathbb{F}_{p^m}$ je kořenem polynomu f, pak pokud opakovaně aplikujeme Frobeniovo zobrazení φ nad $\mathbb{F}_{p^m}$ na α, $\varphi(\alpha)$ a tak dále, dostaneme všechny zmíněné kořeny.

Na konci kapitoly ještě zmíníme speciální případ ireducibilního polynomu nad konečným tělesem, který bude hrát klíčovou roli při generování pseudonáhodné posloupnosti pomocí Möbiovy funkce. Máme tím na mysli *primitivní polynom*.

Definice 4.3.1. Řekneme, že polynom nad $\mathbb{F}_p$ je primitivní, jestliže je minimálním polynomem primitivního prvku grupy $\mathbb{F}_{p^n}^*$.

Příklad 4.3.1. Mějme čtyřprvkové těleso $\mathbb{F}_4$. Jeho prvky, jak jsme si již řekli dříve, můžeme napsat jako $0, 1, \alpha, \alpha + 1$, kde α je kořenem polynomu $x^2 + x + 1 \in \mathbb{Z}_2[x]$. Generátorem tohoto tělesa je α a $\alpha + 1$, jelikož

$$\begin{aligned} \alpha^1 &= (\alpha + 1)^2 = \alpha \\ \alpha^2 &= \alpha + 1 \\ \alpha^3 &= (\alpha + 1)^3 = 1. \end{aligned}$$

Zároveň $x^2 + x + 1$ je minimální polynom α nad $\mathbb{Z}_2$, takže je také primitivním polynomem.

Tvrzení 4.3.3. *Počet primitivních polynomů nad konečným tělesem $\mathbb{F}_p$ stupně n je roven*

$$\frac{\varphi(p^n-1)}{n}.$$

Důkaz. Vezměme si těleso $\mathbb{F}_{p^n}$ a označme α primitivní prvek multiplikativní grupy $\mathbb{F}^*_{p^n}$. Každý prvek α^i pro $1 \leq i \leq p^n - 1$ je primitivním prvkem, pokud $(i, p^n - 1) = 1$ a jedná se o všechny primitivní prvky $\mathbb{F}^*_{p^n}$. Máme tak celkem $\varphi(p^n - 1)$ primitivních prvků.

Nechť dále je $f(x)$ primitivní polynom nad $\mathbb{F}_p$ nějakého z těchto prvků. Tento polynom má n kořenů v $\mathbb{F}_{p^n}$ podle tvrzení 4.3.2 a tyto kořeny jsou získány pomocí Frobeniova zobrazení. Protože je ale Frobeniovo zobrazení automorfismus, kořeny minimálních polynomů všech primitivních prvků se opakují, takže minimální polynomy mají více primitivních prvků za kořen. Pokud $\alpha \in \mathbb{F}_{p^n}$ je primitivní prvek, pak podle tvrzení 4.3.2 mají prvky α^{p^i} pro $1 \leq i \leq n$ stejné minimální polynomy. Celkově tak získáváme, že primitivních polynomů je

$$\frac{\varphi(p^n-1)}{n}.$$

□

Kapitola 5

Pseudonáhodné posloupnosti

Jak už nám název napovídá, budeme mít v této kapitole co dotčení s posloupnostmi. My se zde zaměříme na posloupnosti pseudonáhodné, což jsou ty, které se "jeví"jako náhodné - nedokážeme snadno předpovědět, jaké číslo bude na daném místě v posloupnosti. Ačkoliv ke zkoumání pseudonáhodných posloupností se využívá statistiky, nebudeme zabíhat do podrobných detailů. V kapitole si hlavně ukážeme některé pseudonáhodné posloupnosti a řekneme si, co nás u nich bude zajímat. Nakonec si povíme, jaké mají využití.

5.1 Úvod do pseudonáhodných posloupností

Abychom pochopili, jak taková pseudonáhodná posloupnost vypadá, začneme její konstrukcí. Mějme nějakou neprázdnou *konečnou* množinu $S \subseteq \mathbb{N}_0$. Pomocí této množiny budeme konstruovat pseudonáhodnou posloupnost následovně: vezmeme si funkci $f : S \mapsto S$ a $g : S \mapsto V$ a *počáteční hodnotu* $s_0 \in S$. Pak posloupnost definovaná podle předpisu

$$v_n = g(s_n),$$

kde

$$s_n = f(s_{n-1}),$$

tvoří *pseudonáhodnou posloupnost.* Množinu S chápeme jako *vstupní hodnoty* pro posloupnost, zatímco množinu V jako výstupní množinu.

U pseudonáhodných posloupností nás bude zajímat její *perioda.*

Definice 5.1.1. Nechť $\{a_i\}_{i=0}^{\infty}$ je posloupnost. Nejmenší číslo $p \in \mathbb{N}$ splňující $a_i = a_{i+p}$ pro všechna $i \in \mathbb{N}_0$ nazýváme perioda posloupnosti.

Příklad 5.1.1.

1. Posloupnost $\{(-1)^i\}_{i=0}^{\infty}$ má periodu $p = 2$.
2. Posloupnost $\{i^2 \pmod 3\}_{i=0}$, posloupnost zbytků druhých mocnin přirozených čísel po dělení 3, má periodu $p = 4$, jelikož první členy vypadají následovně: **0, 1, 1, 0**, 0, 1, 1, 0.

5.2 Příklady pseudonáhodných posloupností

5.2.1 Lineární kongruentní generátor

Ukažme si definici pseudonáhodné posloupnosti na konkrétních příkladech. Podívejme se na posloupnost $f : \mathbb{N}_0 \mapsto \mathbb{Z}_m$ danou předpisem

$$s_n = f(s_{n-1}) = as_{n-1} + b \pmod{m}$$

kde $a, m \in \mathbb{N}$ a $b \in \mathbb{N}_0$. Protože je posloupnost definována rekurentně, musíme ještě určit počáteční prvek s_0, v našem případě nechť $s_0 = 1$. Jedná se o posloupnost generovanou lineární funkcí nad přirozenými čísly modulo přirozené číslo. Zvolme nyní například $a = 2, b = 1$ a $m = 9$. Pak získáme postupně hodnoty

$$\begin{aligned} s_1 &= f(1) = 3 \\ s_2 &= f(3) = 7 \\ s_3 &= f(7) = 6 \\ s_4 &= f(6) = 4 \\ s_5 &= f(4) = 0 \\ s_6 &= f(0) = 1 \\ s_7 &= f(1) = 3 \end{aligned}$$

Vidíme, že perioda uvedené posloupnosti je $p = 6$, neboť $s_1 = s_7$, a protože se jedná o kongruenci, platí i $s_i = s_{i+6}$ pro všechna $i \in \mathbb{N}$.

Dále bychom mohli zvolit výstupní funkci $g : \mathbb{N} \mapsto \langle 0, 1\rangle$ definovanou předpisem

$$g(s_{n-1}) = \frac{f(s_{n-1})}{m},$$

čímž máme zaručeno, že jsou její hodnoty v intervalu $\langle 0, 1\rangle$, protože $f(n) < m$ pro všechna $n \in \mathbb{N}_0$.

Ve zvoleném případě daná posloupnost neobsahuje všechny zbytkové třídy modulo m. Všimněme si však, že pokud $(a, m) = 1$ a $b = 0$, bude daná posloupnost obsahovat každou zbytkovou třídu modulo m; pokud totiž $x_1, x_2 \in \mathbb{N}_0$ a $x_1 \neq x_2$, pak kongruence $ax_1 \equiv ax_2 \pmod{m}$ je ekvivalentní s $a(x_1 - x_2) \equiv 0 \pmod{m}$, ale $(a, m) = 1$, tedy nutně $x_1 \equiv x_2 \pmod{m}$.

Co se týče periody, je obecně obtížné ji určit pro takto zvolenou pseudonáhodnou posloupnost. Je však zřejmé, že její maximální hodnota je m; pokud by m nebyla, pak by v posloupnosti existovalo $m + 1$ zbytkových tříd, což není možné. Pro konkrétní případ, kdy $(a, m) = 1$ a $b = 0$ je perioda maximální, tedy rovna m.

5.2.2 Kvadratický kongruentní generátor

Postupujme analogicky při konstrukci kvadratického generátoru. Zvolme $f : \mathbb{N}_0 \mapsto \mathbb{Z}_m$ s předpisem

$$s_n = f(s_{n-1}) = as_{n-1}^2 + bs_{n-1} + c \pmod{m},$$

kde $a, b, c \in \mathbb{N}_0$, $a \neq 0$ a $m \in \mathbb{N}$. Obdobně jako v předchozím případě získáme pseudonáhodnou posloupnost s jistou periodou, kterou je opět obtížné předpovědět. Uvedená posloupnost má kromě využití, které je zmíněné na konci kapitoly, uplatnění při hledání netriviálních dělitelů přirozených čísel, tj. dělitelů různých od samotného zkoumaného čísla a jedničky, u Pollardovy ρ metody.

5.2.3 Posuvný registr

Generování pseudonáhodné posloupnosti pomocí tzv. posuvného registru se liší od těch předchozích tím, že generuje posloupnost jedniček a nul. Využívá primitivních polynomů, s nimiž jsme se seznámili na konci 4. kapitoly.

Začneme konkrétním případem. Zvolme si primitivní polynom $f(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$ a zvolme počáteční člen posloupnosti jako $s_0 = a_2a_1a_0$, kde $a_0, a_1, a_2 \in \mathbb{Z}_2$, a umístíme jej do tzv. registru ilustrovaném jako jednořádková tabulka. Další člen posloupnosti získáme tak, že určíme $a_3 = a_1 + a_0 \pmod 2$ a obsah registru posuneme doprava, tak že v něm bude posloupnost $a_3a_2a_1$. Další člen pak určíme jako $a_4 = a_2 + a_1 \pmod 2$, posuneme obsah registru doprava a takto můžeme pokračovat dále. Získáme tedy rekurentní vztah $a_{i+3} = a_{i+1} + a_i \pmod 2$ pro $i \in \mathbb{N}_0$.

Všimněme si, že v rekurentním vztahu odpovídá a_{i+3} vedoucímu koeficientu $f(x)$ a že je vypočten, jako součet členů posloupnosti nad pozicích i, kde a_i je nenulový koeficient $f(x)$. Tabulka níže ukazuje obsah registru pro počáteční stav $s_0 = 100$, kde nový řádek odpovídá následujícímu stavu registru.

1	0	0
0	1	0
1	0	1
1	1	0
1	1	1
0	1	1
0	0	1
1	0	0

Tabulka 5.1: Obsah registru při generování pomocí primitivního polynomu $f(x) = x^3 + x + 1$.

Celý postup lze zobecnit pro libovolný primitivní polynom nad $\mathbb{Z}_2$ stupně $m \in \mathbb{N}$, přičemž budeme postupovat naprosto totožně: sečteme členy posloupnosti na pozicích, kde primitivní polynom má nenulové koeficienty, a posuneme obsah registru doprava. Z tohoto postupu také pramení název posuvný registr.

V našem případě byla perioda posloupnosti stavů registrů rovna 7. Pokud bychom zvolili jiný počáteční stav, byla by periody opět 7. Obecně pak lze dokázat, že právě díky primitivnímu polynomu stupně $n \in \mathbb{N}$ takto vygenerujeme posloupnosti stavů registru s periodou $2^n - 1$, což je maximální možná, neboť máme n polí registru, do kterých připadne jednička, nebo nula a počáteční stav již máme zvolen.

Co je ale tou pseudonáhodnou posloupností? Z tabulky stavů registru si můžeme vybrat libovolný sloupec a považovat ji za pseudonáhodnou posloupnost délky 2^n-1. Co se týče uplatnění posuvného registru nalezneme jej například v obvodech, kde se používá při sériových vstupech a paralelních výstupech.

5.3 Autokorelace

Budeme zde nyní hovořit o *autokorelaci*, jenž bude práci provázet následující kapitolu a bude využívána ke zkoumání náhodnosti jednotlivých posloupnosti. Existují samozřejmě sofistikovanější testy k testování náhodnosti, ale jak již bylo naznačeno v úvodu kapitoly, složitější statistické metody jsou nad rámec této práce.

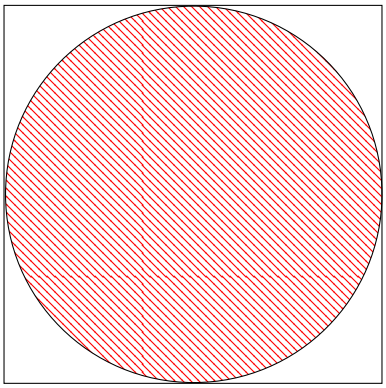
Mějme posloupnost $A = \{a_i\}_{i=0}^{\infty}, B = \{b_j\}_{j=0}^{\infty}$ obě s periodou p. Hodnota tzv. *korelace* posloupností A, B určuje, jak moc jsou na sobě *závislé* dané posloupnosti. Závislostí zde jednoduše rozumíme míru toho, jak dokážeme jednu posloupnost vyjádřit pomocí druhé. Autokorelací pak chápeme korelaci posloupnosti A se sebou sama. Jednoduše řečeno nám autokorelace popisuje, jak je posloupnost A závislá na posloupnosti A_x, kde $A = \{a_{i+x}\}_{i=0}^{\infty}$ pro nějaké $x \in \mathbb{N}_0$, tedy na posloupnosti, která je posunuta vzhledem k původní posloupnosti A. Právě autokorelace nám dokáže povědět, jak jsou hodnoty pseudonáhodné posloupnosti na sobě závislé. Přesný výpočet autokorelace závisí na zvolené posloupnosti, takže se k němu vrátíme až v následující kapitole.

5.4 Využití pseudonáhodných posloupností

Úkolem pseudonáhodných posloupností je generovat tak náhodnou posloupnost, jak je to možné. Nabízí se tak, že mají uplatnění v různých telekomunikacích, šifrovacích algoritmech nebo dalších zabezpečovacích konceptech. Uvažme například lineární kongruentní generátor. Výpočet jeho jednotlivých hodnot je rychlý a zabírá málo paměti. Ovšem velikost jednotlivých členů posloupností se od sebe příliš neliší. Problémy lineárního kongruentního generátoru jsou malé, ale složité natolik, že jejich zkoumání se nebudeme zabývat dále.

Zřejmě nejznámějším využití generátoru pseudonáhodných čísel objevíme u *metody Monte Carlo*. Metoda Monte Carlo využívá právě pseudonáhodných čísel k řešení matematických problémů, které je jinak obtížné řešit. Jedná se tak o numerickou metodu využívající náhodnosti. Takovým klasickým příkladem je určení hodnoty π pomocí generátoru pseudonáhodných čísel.

Nechť je dán kruh vepsaný do čtverce o straně 1 jako na obrázku 5.1. Příklad zní následovně: jaká je pravděpodobnost, že náhodně zvolený bod ve čtverci je uvnitř kruhu? K zodpovězení této otázky je potřeba určit poměr obsahu kruhu a obsahu čtverce. Ten je roven $\frac{\pi}{4}$. Pokud bychom



Obrázek 5.1

tedy použili Monte Carlo metody k určení náhodných bodů ve čtverci, pak bychom se s použitím dostatečně mnoho bodů blížili k hodnotě $\frac{\pi}{4}$. Po vynásobení výsledku čtyřmi obdržíme hodnotu π.

Kapitola 6

Pseudonáhodná posloupnost generovaná Möbiovou funkcí

Často se generují tzv. *binární pseudonáhodné posloupnosti*, tj. pseudonáhodné posloupnosti tvořené nulami a jedničkami. S jednou takovou posloupností jsme se seznámili v předchozí kapitole. V závěrečné kapitole této práce se budu věnovat poměrně novému přístupu ke generování pseudonáhodné posloupnosti. Navíc tato posloupnost nebude generována nad $\mathbb{Z}_2$, jak tomu obvykle bývá, ale nad libovolným konečným tělesem s lichou charakteristikou. Výsledný tvar posloupnosti je poté získán aplikováním Möbiovy funkce, s níž jsme se seznámili hned na začátku práce. K veškerým výpočtům jsem použil matematický software SageMath 8.6. a k tvorbě grafů Python verze 3.8.

6.1 Algoritmus generování

Mějme konečné těleso $\mathbb{F}_{p^n}$ a uvažme libovolný primitivní polynom nad $\mathbb{F}_p$. Metoda generování pseudonáhodné posloupnosti, kterou budeme zkoumat v této kapitole, je založena na tom, že pomocí primitivního polynomu dokážeme vygenerovat všechny nenulové prvky tělesa $\mathbb{F}_{p^n}$.

Tvrzení 6.1.1. *Nechť $\mathbb{F}_{p^n}$ je konečné těleso a f polynom nad $\mathbb{F}_p$. Potom f je primitivním polynomem právě tehdy, když*

$$x^{p^n-1} \equiv 1 \ (mod\ f(x))$$
$$x^i \not\equiv 1 \ (mod\ f(x)) \ pro\ 1 \leq i < p^n - 1.$$

Důkaz. Primitivní polynom je minimální polynom $\alpha \in \mathbb{F}_{p^n}$ nad $\mathbb{F}_p$. Tuto definici lze ekvivalentně formulovat tak, že minimální polynom f generuje celé těleso $\mathbb{F}_{p^n}$, tedy že nejmenší $k \in \mathbb{N}$ splňující $x^k \equiv 1 \pmod{f(x)}$ je $n = p^n - 1$ a zároveň tak $x^i \equiv 1 \pmod{f(x)}$ pro všechna $1 \leq i < p^n - 1$.

□

Poslední aparát, který potřebujeme k porozumění generování pseudonáhodné posloupnosti pomocí Möbiovy funkce, je transformace prvku z tělesa $\mathbb{F}_{p^n}$ do jeho prvotělesa $\mathbb{F}_p$. Budeme využívat následujícího tvrzení.

Tvrzení 6.1.2. *Nechť $\mathbb{F}_{p^n}$ je konečné těleso a $\mathbb{F}_p$ jeho prvotěleso. Pro libovolný prvek $X \in \mathbb{F}_{p^n}$ potom platí, že*

$$\sum_{i=0}^{n-1} X^{p^i} \in \mathbb{F}_p\,.$$

Důkaz. Klíčové v důkazu je pozorování, že pro libovolné $X \in \mathbb{F}_{p^n}$ platí implikace: pokud $X^p = X$, potom $X \in \mathbb{F}_p$. Rozkladovým rozšířením $\mathbb{F}_p$ určeným polynomem $x^p - x$ je totiž samo $\mathbb{F}_p$. To znamená, pokud $X \in \mathbb{F}_{p^n}$ a $X^p - X = 0$, pak $X \in \mathbb{F}_p$.

Dosaďme tedy součet do polynomu $x^p - x$:

$$\left(\sum_{i=0}^{n-1} X^{p^i}\right)^p - \sum_{i=0}^{n-1} X^{p^i} = \sum_{i=1}^{n} X^{p^i} - \sum_{j=0}^{n-1} X^{p^j} = X^{p^n} - X = 0.$$

Využili jsme toho, že Frobeniovo zobrazení je homomorfismus a také toho, že $X^{p^n} = X$ pro každé $X \in \mathbb{F}_{p^n}$. Tím jsme dokázali, že uvedený součet je prvkem $\mathbb{F}_p$. □

Definice 6.1.1. Zobrazení $\mathrm{Tr} : \mathbb{F}_{p^n} \mapsto \mathbb{F}_p$ dané předpisem

$$\mathrm{Tr}(X) = \sum_{i=0}^{n-1} X^{p^i}$$

říkáme stopa.

Uvažujme nyní $\mathbb{F}_{p^n}$ jako vektorový prostor nad $\mathbb{F}_p$. Stopa $\mathrm{Tr} : \mathbb{F}_{p^n} \mapsto \mathbb{F}_p$ je lineárním zobrazením, neboť pro libovolné prvky $a, b \in \mathbb{F}_{p^n}$ a $c \in \mathbb{F}_p$ plyne z vlastností Frobeniova zobrazení:

$$\mathrm{Tr}(a+b) = \sum_{i=0}^{n-1} (a+b)^{p^i} = \sum_{i=0}^{n-1} a^{p^i} + \sum_{i=0}^{n-1} b^{p^i} = \mathrm{Tr}(a) + \mathrm{Tr}(b)$$

$$\mathrm{Tr}(c \cdot a) = \sum_{i=0}^{n-1} (c \cdot a)^{p^i} = c^{p^i} \sum_{i=0}^{n-1} a^{p^i} = c \cdot \mathrm{Tr}(a).$$

Obraz lineárního zobrazení $\mathrm{Tr} : \mathbb{F}_{p^n} \mapsto \mathbb{F}_p$ je podprostor $\mathbb{F}_p$. Protože $\mathbb{F}_p$ je vektorový prostor nad $\mathbb{F}_p$ dimenze 1, musí platit buď $\mathrm{Im}\,\mathrm{Tr} = \mathbb{F}_p$, nebo $\mathrm{Im}\,\mathrm{Tr} = \{0\}$. Tvrzení níže nás přesvědčí, že platí první varianta.

Tvrzení 6.1.3. *Stopa $Tr : \mathbb{F}_{p^n} \mapsto \mathbb{F}_p$ je surjektivní zobrazení.*

Důkaz. Obraz Tr je buď $\{0\}$, nebo $\mathbb{F}_p$. Ukažme sporem, že Im Tr nemůže být $\{0\}$. Označme $\alpha \in \mathbb{F}_{p^n}$ primitivní prvek multiplikativní grupy a uvažme Vandermondovu matici M s tímto prvkem:

$$M = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha & \alpha^p & \cdots & \alpha^{p^{n-1}} \\ \alpha^2 & \alpha^{2p} & \cdots & \alpha^{2p^{n-1}} \\ \vdots & & & \\ \alpha^{n-1} & \alpha^{(n-1)p} & \cdots & \alpha^{(n-1)p^{n-1}} \end{pmatrix}.$$

Pomocí řádkových úprav lze matici M upravit na nulovou, jelikož předpokládáme, že stopa libovolného prvku $\mathbb{F}_{p^n}$ je nulová, z čehož dostáváme, že $\det M = 0$. Avšak pro determinant matice M také platí

$$\det M = \prod_{0 \le i < j \le n-1} (\alpha^{p^j} - \alpha^{p^i}).$$

Prvek α je řádu $p^n - 1$, a tak prvky $\alpha^{p^i}, \alpha^{p^j}$, kde $0 \le i < j \le n-1$, jsou různé, takže součin jednotlivých rozdílů je nenulový. To znamená, že $\det M \neq 0$, ale to je spor. □

Nakonec je nutná ještě poznámka ohledně modifikace Möbiovy funkce.

Definice 6.1.2. Möbiovu funkci $\mu : \mathbb{F}_p \mapsto \mathbb{Z}$ definujeme předpisem

$$\mu(n) = \begin{cases} 1 & \text{pro } n = 1, \\ 0 & \text{pokud } n = 0 \text{ nebo } \exists d \in \mathbb{N}, d > 1 : d^2 | n, \\ (-1)^k & \text{jinak, kde } k \text{ je počet různých prvočísel v rozkladu čísla } n \text{ na prvočinitele.} \end{cases}$$

V definici se chováme k prvkům $\mathbb{F}_p$ jako prvkům $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ a uvažujeme rozklad a dělitele právě těchto reprezentantů zbytkových tříd v $\mathbb{Z}_p$.

Jsme připraveni na to si představit generování pseudonáhodné posloupnosti nad konečnými tělesy pomocí Möbiovy funkce.

Algoritmus: Generování pseudonáhodné posloupnosti Möbiovou funkcí nad konečným tělesem

- **Vstup:** prvočíslo $p > 2$, přirozené číslo n.
- **Výstup:** pseudonáhodná posloupnost prvků množiny $\{-1, 0, 1\}$ délky $p^n - 1$.

1: Zvolme primitivní polynom konečného tělesa $\mathbb{F}_{p^n}$ nad $\mathbb{F}_p$. Nazvěme jej $f(x)$.
2: Označme α primitivní prvek tělesa $\mathbb{F}_p[x]/\langle f(x) \rangle$, tělesa $\mathbb{F}_{p^n}$, a spočtěme $X_i = \alpha^i$ pro $0 \le i < p^n - 1$.
3: Pro každý prvek $X_i \in \mathbb{F}_{p^n}$, $0 \le i < p^n - 1$, určíme hodnotu $x_i = \mathrm{Tr}(X_i) \in \mathbb{F}_p$.
4: Určíme i-tý prvek posloupnosti jako $s_i = \mu(x_i)$ pro $0 \le i < p^n - 1$.
5: Získali jsme posloupnost $\mathcal{S} = \{s_i\}$.

Ukažme si postup na konkrétním příkladu. Zvolme $p = 3$ a $n = 2$. Primitivním polynomem tělesa $\mathbb{F}_{3^2}$ nad $\mathbb{Z}_3$ je například polynom $f(x) = x^2 + x + 2$. Veškeré hodnoty konstrukce pseudonáhodné posloupnosti pak shrnuje tabulka níže.

1	2	α	2α	$\alpha+1$	$\alpha+2$	$2\alpha+1$	$2\alpha+2$
-1	1	-1	1	1	0	0	-1

Tabulka výše nám podává informace o tom, jaké hodnoty jsou pro jednotlivé prvky generovány. Ve správném pořadí, tj. pořadím, ve kterém jsou prvky tělesa postupně generovány pomocí primitivního polynomu pak dostáváme posloupnost

$$-1 \mid -1 \mid 0 \mid -1 \mid 1 \mid 1 \mid 0 \mid 1$$

6.2 Vlastnosti uvedené posloupnosti

Uvedená posloupnost má maximální periodu, a sice $p^n - 1$, pokud si zvolíme těleso $\mathbb{F}_{p^n}$. Vyšší periodu již mít nemůže; kdyby měla, bylo by v posloupnosti p^n prvků, neboť nad daným tělesem je hodnota prvku pro konkrétní primitivní polynom jednoznačně určena. Ovšem těleso $\mathbb{F}_{p^n}$ má právě $p^n - 1$ nenulových prvků, spor.

V takto generované posloupnosti závisí na volbě tělesa. Nevolíme těleso charakteristiky 2, jelikož nad tímto tělesem se v posloupnosti nebude vyskytovat -1, protože $\mu(0) = 0$ a $\mu(1) = 1$. Úkolem pseudonáhodné posloupnosti je generovat posloupnost, která se jeví jako co možná nejnáhodnější. Avšak ne všechna tělesa jsou vhodná, pokud uvažujeme jednoduché požadavky jako třeba rovnost *četností* jednotlivých členů posloupnosti. Vytvořil jsem tak tabulku 6.2, která zachycuje četnost jednotlivých členů posloupnosti pro různá tělesa a jeden zvolený primitivní polynom pro každé těleso.

Základové těleso	Stupeň rozšíření											
$\mathbb{F}_p$	2			3			4			5		
	-1	0	1	-1	0	1	-1	0	1	-1	0	1
$\mathbb{F}_3$	3	2	3	9	8	9	27	26	27	81	80	81
$\mathbb{F}_5$	10	9	5	50	49	25	250	249	1250	1249	625	81
$\mathbb{F}_7$	21	13	14	147	97	98	1029	685	686	7203	4801	4802
$\mathbb{F}_{11}$	44	43	33	484	483	363	5324	5323	3993	58564	58563	43923

Tabulka 6.1: Počet jednotlivých členů posloupnosti generované pomocí Möbiovy funkce nad konečnými tělesy. Řádek se základovým tělesem $\mathbb{F}_p$ a stupněm rozšíření n odpovídá tělesu $\mathbb{F}_{p^n}$.

Poznámka. Podotkněme, že četnost členů není ovlivněna primitivním polynomem, jelikož ten pouze ovlivňuje pořadí členů posloupnosti.

Povšiml jsem si, že pouze u tělesa s prvotělesem $\mathbb{F}_3$ je všech členů posloupnosti takřka stejný počet. Pokud se tedy budeme dívat na posloupnost jako celou, pak jedině základové těleso $\mathbb{F}_3$ vyhovuje podmínce, aby byly počty členů stejné. V tabulce je ovšem uvedeno pouze několik těles, a proto jsem uvedené rozhodl zjistit, zda platí pro libovolné těleso $\mathbb{F}_{3^n}$. Následujícím tvrzením s důkazem dokládá moji hypotézu.

Tvrzení 6.2.1. *Pokud je těleso $\mathbb{F}_{p^n}$ charakteristiky $p \neq 3$, potom posloupnost generovaná nad konečným tělesem $\mathbb{F}_{p^n}$ pomocí Möbiovy funkce není náhodná.*

Důkaz. Předpokládejme, že $p > 3$. Dokážeme, že pravděpodobnost nabývání hodnoty 0 je vyšší než $\frac{1}{3}$. Podíváme se tedy na pravděpodobnost, že náhodně zvolené přirozené číslo není dělitelné druhou mocninou žádného prvočísla.

Nechť $p_1, p_2, \ldots, p_k$ jsou všechna různá prvočísla menší než zvolená charakteristika $p > 3$. Pravděpodobnost, že číslo není dělitelné p_1^2, je rovna $1 - \frac{1}{p_1^2}$, a protože jsou prvočísla navzájem nesoudělná, pak pro $p \to \infty$ platí

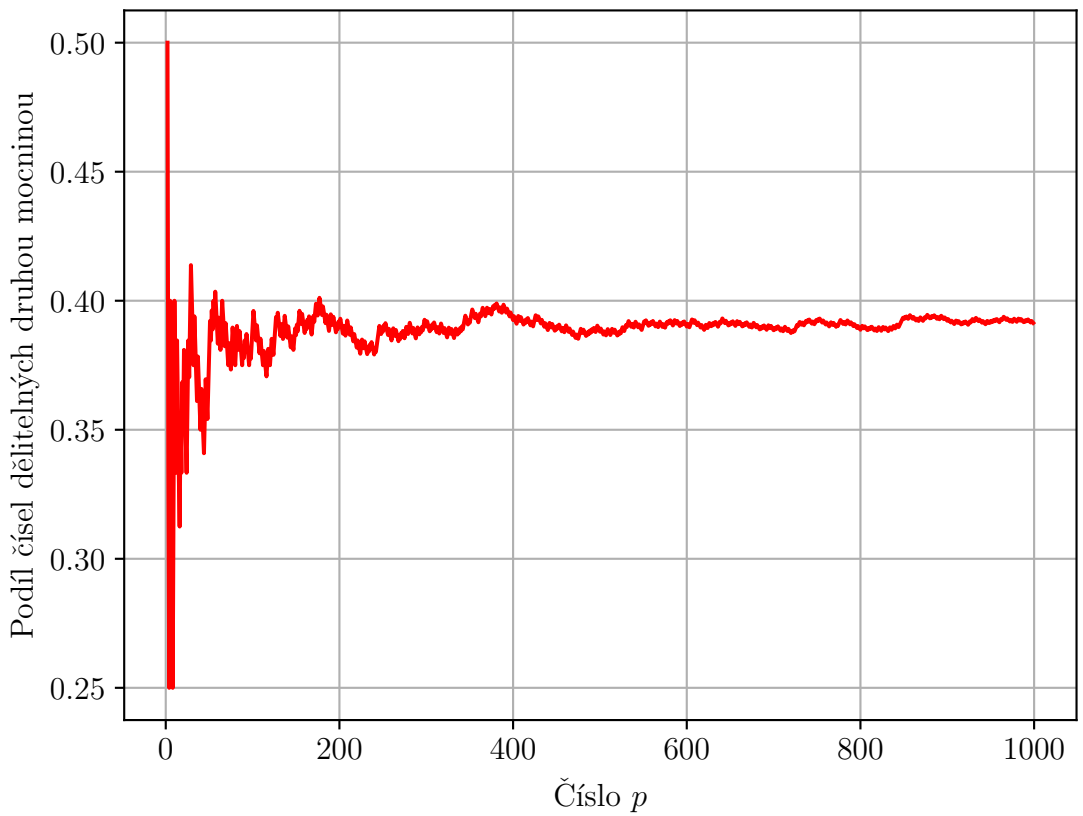
$$\lim_{p\to\infty} P(p) = \prod_{i=1}^{\infty}\left(1 - \frac{1}{p_i^2}\right) = \prod_{i=1}^{\infty}\left(\frac{1}{1 - p_i^{-2}}\right)^{-1} = \frac{1}{\prod_{i=1}^{\infty}\frac{1}{1-p_i^{-2}}} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2},$$

kde jsme využili Eulerova tvaru zeta funkce. Pro naši hledanou pravděpodobnost pak platí

$$\lim_{p\to\infty}(1 - P(p)) > 1 - \frac{6}{9} = \frac{1}{3}.$$

Tedy pro dostatečně velké p tvrzení platí. Stačí tak projít jen konečný počet prvočísel, abychom se přesvědčili, že tvrzení platí pro libovolné $p > 3$. Pro některá čísla, jako třeba 7, nefunguje argument přes počet nul v posloupnosti, přesto však tvrzení platí, protože počet -1 je 3, jedničky jsou tři, ale nuly jsou dvě. Podobně můžeme argumentovat pro ostatní čísla. Graf 6.1 na další straně dokládá uvedenou limitu. □

Jak takové tvrzení interpretovat? Říká nám, že vyšší prvočísla jako charakteristiku není vhodné volit, neboť bude narušena náhodnost členů posloupnosti. Pro zvýšení periody posloupnosti se tak nabízí říct, že bude dostatečné zvýšit stupeň rozšíření. I toto řešení však není úplně vhodné, jak se můžeme přesvědčit z tabulky na předchozí straně. Pro těleso s charakteristikou $p = 3$ však hypotéza, že zvyšování stupně rozšíření přispívá k délce posloupnosti a zároveň neovlivňuje četnost, vypadá nadějně. Nejprve ukážu, že uvedená pseudonáhodná posloupnost bude mít vždy takřka totožný počet (lišící se pouze o jeden člen) jednotlivých členů, pokud zvolíme těleso $\mathbb{F}_{3^n}$.



Obrázek 6.1: Graf vyjadřující podíl počtu čísel, která jsou menší jak číslo p a jsou dělitelné druhou mocninou přirozeného čísla, a čísla p. Vidíme že pro čísla $p < 100$ není příliš očividné, že tvrzení platí, pro větší čísla se drží pravděpodobnost nad $\frac{1}{3}$.

Tvrzení 6.2.2. *Jádro stopy* $Tr : \mathbb{F}_{p^n} \mapsto \mathbb{F}_p$ *obsahuje* p^{n-1} *prvků.*

Důkaz. Vezměme si libovolné dva prvky $a, b \in \mathbb{F}_{p^n}$ a předpokládejme, že $\mathrm{Tr}(a) = \mathrm{Tr}(b)$. Potom díky tomu, že stopa Tr je lineární zobrazení, platí

$$\mathrm{Tr}(a - b) = \mathrm{Tr}(a) + \mathrm{Tr}(-b) = \mathrm{Tr}(b) - \mathrm{Tr}(b) = 0,$$

a proto $\alpha = a - b \in \mathrm{Ker}\,\mathrm{Tr}$. Zafixujeme-li si $b \in \mathbb{F}_{p^n}$, potom množina

$$H = \{\alpha + b \mid \alpha \in \mathrm{Ker}\,\mathrm{Tr}\}$$

obsahuje stejný počet prvků jako $\mathrm{Ker}\,\mathrm{Tr}$, protože rovnost $\alpha_1 + b = \alpha_2 + b$ implikuje $\alpha_1 = \alpha_2$. Ovšem jádro $\mathrm{Ker}\,\mathrm{Tr}$ je podgrupa aditivní grupy tělesa $\mathbb{F}_{p^n}$. Z Lagrangeovy věty, první věty o izomorfismus grup a díky faktu, že Tr je surjekce, platí

$$|\,\mathrm{Ker}\,\mathrm{Tr}\,| = \frac{|\,\mathbb{F}_{p^n}\,|}{|\,\mathrm{Im}\,\mathrm{Tr}\,|} = \frac{|\,\mathbb{F}_{p^n}\,|}{|\,\mathbb{F}_p\,|} = p^{n-1}.$$

□

Tvrzení 6.2.3. *Na každý prvek $\mathbb{F}_p$ se aplikováním stopy $Tr : \mathbb{F}_{p^n} \mapsto \mathbb{F}_p$ zobrazí právě p^{n-1} prvků.*

Důkaz. Z izomorfismu $\mathbb{F}_{p^n} / \operatorname{Ker} \mathrm{Tr} \cong \mathbb{F}_p$ vidíme, že v rozkladu tělesa $\mathbb{F}_{p^n}$ pomocí jádra $\operatorname{Ker} \mathrm{Tr}$ na třídy vznikne právě p různých tříd a každá tato třída musí mít totožný počet prvků, tedy p^{n-1}. □

Dostáváme se tak k důležitému důsledku.

Důsledek 6.2.1. *Na každý prvek tělesa $\mathbb{F}_3$ se pomocí stopy $Tr : \mathbb{F}_{3^n} \mapsto \mathbb{F}_3$ zobrazí z tělesa $\mathbb{F}_{3^n}$ právě 3^{n-1} prvků.*

Pokud tedy zvolíme těleso $\mathbb{F}_{3^n}$, tak na prvky $1, 2 \in \mathbb{F}_3$ se zobrazí 3^{n-1} prvků, na prvek 0 se zobrazí 3^{n-1}, neboť nezobrazujeme nulový prvek tělesa $\mathbb{F}_{3^n}$. Ovšem $\mu(1) = 1, \mu(2) = -1$ a $\mu(0)0$, je naše pozorování teoreticky dokázáno, protože na $-1, 1$ se zobrazí 3^{n-1} prvků a na nulu $3^{n-1} - 1$ prvků.

Pro bližší zkoumání generování nad $\mathbb{F}_{3^n}$ jsem proto využil znalostí z předchozí kapitoly a aplikoval autokorelaci.

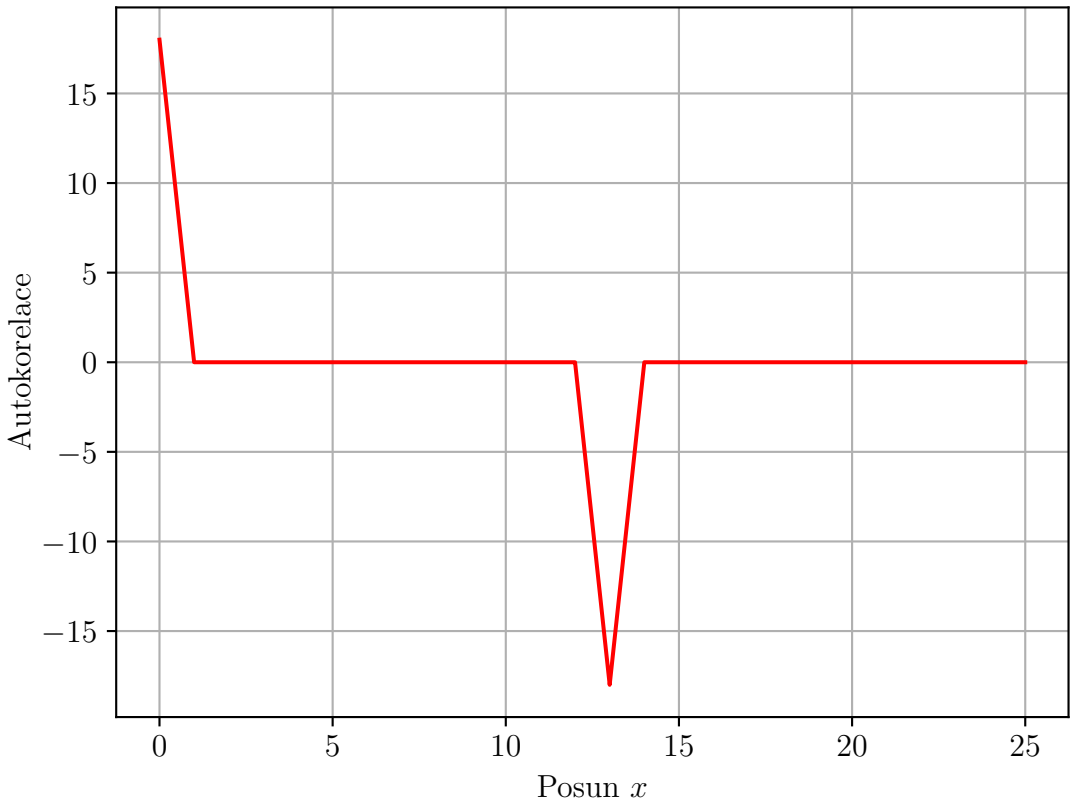
6.3 Autokorelace

Během zkoumání autokorelace jsem se zaměřil na závislost hodnoty autokorelace na stupni rozšíření tělesa $\mathbb{F}_3$. Nejprve si uvedeme, jak autokorelaci zjistíme. Máme-li posloupnost $\mathcal{S} = \{s_i\}$ délky L, potom pro výpočet autokorelace budeme využívat následujícího vztahu:

$$\mathcal{R}_{\mathcal{S}}(x) = \sum_{i=0}^{L-1} s_i s_{i+x},$$

kde $x \in \mathbb{N}_0$ vyjadřuje posun, tj. autokorelace s posunem x znamená, že porovnáváme nezávislost původní posloupnosti a posunuté posloupnosti $\mathcal{S}_x = \{s_{i+x}\}$.

Volbou tělesa $\mathbb{F}_{3^3}$ a primitivního polynomu $f(x) = x^3 + x^2 + 2x + 1$ obdržíme graf 6.2, který můžeme vidět na následující straně. Z grafu můžeme číst, že prvky podposloupnosti $\mathcal{S}_1 = \{s_i\}$ pro $0 \leq i \leq 12$ jsou nezávisle generované, jelikož autokorelace pro ni nabývá hodnoty 0. To znamená, že členy podposloupnosti $\mathcal{S}_i$ jsou originálně generované, a nedokážeme odhadnout člena podposloupnosti $\mathcal{S}_1$ v závislosti na jejím předchozím členu. Situace se změní pro posun $x = 13$, kdy členové posloupnosti $\mathcal{S}$ jsou od 13. členu závislé na předchozí podposloupnosti $\mathcal{S}_1$, a lze je tak lépe odhadnout. Nakonec pro podposloupnost $\mathcal{S}_2 = \{s_j\}$ pro $14 \leq j \leq 26$, dostáváme totožný výsledek jako pro podposloupnost $\mathcal{S}_1$.



Obrázek 6.2: Graf závislosti autokorelace na posunu vzhledem k původní posloupnosti.

Dostáváme se k otázce, zda grafy autokorelací pro libovolné těleso $\mathbb{F}_{3^n}$ vypadají podobně jako graf pro těleso $\mathbb{F}_{3^3}$. Můžeme se však přesvědčit z tabulky 6.3 na následující straně, že pro tělesa $\mathbb{F}_{3^n}$ pro $n < 10$ je charakter grafu závislosti autokorelace na posunu shodný s tím pro $\mathbb{F}_{3^3}$.

Pro posun $x = 0$ je vždy autokorelace nezáporná, neboť dostaneme, že

$$\mathcal{R}(0) = \sum_{i=0}^{L-1} s_i^2 \geq 0.$$

Z tabulky jsem však vypozoroval zajímavé pravidlo: pro posun x je autokorelace záporná *právě v polovině* periody. Záporná autokorelace zde znamená, že závislost je opačná, než kdyby byla kladná. Opačnou závislostí zde rozumíme, že se liší znaménkem jednotlivých členů. Vzpomeňme si na naši posloupnost, kterou jsme vygenerovali na začátku kapitoly:

$$-1 \mid -1 \mid 0 \mid -1 \mid 1 \mid 1 \mid 0 \mid 1$$

Těleso	Hodnota autokorelace		
	0	< 0	0
$\mathbb{F}_{3^2}$	$0 \leq i \leq 3$	$i = 4$	$5 \leq i \leq 8$
$\mathbb{F}_{3^3}$	$0 \leq i \leq 12$	$i = 13$	$14 \leq i \leq 26$
$\mathbb{F}_{3^4}$	$0 \leq i \leq 39$	$i = 40$	$41 \leq i \leq 80$
$\mathbb{F}_{3^5}$	$0 \leq i \leq 120$	$i = 121$	$122 \leq i \leq 242$
$\mathbb{F}_{3^6}$	$0 \leq i \leq 363$	$i = 364$	$365 \leq i \leq 728$
$\mathbb{F}_{3^7}$	$0 \leq i \leq 1092$	$i = 1093$	$1094 \leq i \leq 2186$
$\mathbb{F}_{3^8}$	$0 \leq i \leq 3279$	$i = 3280$	$3281 \leq i \leq 6560$

Tabulka 6.2: Tabulka ukazuje indexy členů posloupností, pro které je autokorelace rovna 0 a pro které je záporná.

Z ní pak snadno vypozorujeme, že druhá polovina posloupnosti je totožná s tou první až na znaménko. Toto pozorování mě vedlo k zobecnění pro libovolné těleso $\mathbb{F}_{3^n}$.

Tvrzení 6.3.1. *Nechť $\mathcal{S} = \{s_i\}$ je posloupnost vygenerovaná pomocí Möbiovy funkce nad tělesem $\mathbb{F}_{3^n}$, kde $n \in \mathbb{N}$. Označíme-li $L = 3^n - 1$ délku posloupnosti $\mathcal{S}$, potom $s_k = -s_{k+\frac{L}{2}}$ pro všechna $k \in \mathbb{N}_0$.*

Důkaz. Nejprve dokážeme, že pro libovolný primitivní prvek multiplikativní grupy tělesa $\mathbb{F}_{p^n}$ s charakteristikou $p > 2$ platí $\alpha + \alpha^{\frac{p^n+1}{2}} = 0$. Mějme polynom $x^2 - 1 \in \mathbb{F}_p[x]$. Tento polynom má právě dva kořeny v tělese $\mathbb{F}_{p^n}$, a to 1 a -1. Všimněme si, že

$$\left(\alpha^{\frac{p^n-1}{2}}\right)^2 - 1 = \alpha^{p^n-1} - 1 = 1 - 1 = 0.$$

Protože ale $\alpha^{\frac{p^n-1}{2}} \neq 1$, jelikož α je primitivní prvek, nutně tak $\alpha^{\frac{p^n-1}{2}} = -1$, čímž dostáváme, že

$$\alpha + \alpha^{\frac{p^n+1}{2}} = \alpha(1 + \alpha^{\frac{p^n-1}{2}}) = 0.$$

Pro libovolné $k \in \mathbb{N}$ obdobně dojdeme k rovnosti

$$\alpha^k + \alpha^{k+\frac{p^n-1}{2}} = \alpha^k(1 + \alpha^{\frac{p^n-1}{2}}) = 0.$$

Dosaďme nyní α^k do $\mathrm{Tr}(X)$ a upravme využitím předchozího poznatku:

$$\mathrm{Tr}(\alpha^k) = \sum_{i=0}^{L-1} (\alpha^k)^{p^i} = \sum_{i=0}^{L-1} (-\alpha^{k+\frac{p^n-1}{2}})^{p^i}.$$

V našem případě $p = 3$, a protože p je liché, pak $\mathrm{Tr}(\alpha^k) = -\mathrm{Tr}(\alpha^{k+\frac{p^a-1}{2}})$. Zároveň jedinými prvky $\mathbb{F}_3$ jsou $0, 1, 2$, pro něž platí

$$\mu(0) = 0$$
$$\mu(1) = 1$$
$$\mu(2) = -1.$$

Z toho dostáváme, že mohou nastat tyto varianty:

$$s_k = \mu(\mathrm{Tr}(\alpha^k)) = 0 \quad \Rightarrow \quad s_{k+\frac{L}{2}}\, \mu(\mathrm{Tr}(\alpha^{k+\frac{p^n-1}{2}})) = 0$$

nebo

$$s_k = \mu(\mathrm{Tr}(\alpha^k)) = \pm 1 \quad \Rightarrow \quad s_{k+\frac{L}{2}} = \mu(\mathrm{Tr}(\alpha^{k+\frac{p^n-1}{2}})) = \mp 1,$$

což jsme přesně chtěli ukázat □

Důsledkem tohoto tvrzení a předchozího pozorování je, že takto vygenerovaná pseudonáhodná posloupnost má první polovinu členů originálně zvolenou, kdežto druhou polovinu získáme pouhou záměnou znamének.

6.4 Využití

Získaná pseudonáhodná posloupnost může mít uplatnění například v kryptografii, kde využíváme náhodnosti k zabezpečení informace tak, aby nebylo možné ji rozluštit. Jestliže například používáme kódovací algoritmus, kde potřebujeme nějaký těžce odhadnutelný klíč, můžeme využít právě pseudonáhodných posloupností. Závisí však na kvalitě algoritmu, který pokud je odhalen, pak již lze informaci snadno dekódovat. Tento přístup se liší od klasického zabezpečovacího algoritmu RSA, v němž znalost algoritmu nezaručí rozluštění zprávy. Uvedená posloupnost je tak bezpečná do té doby, než je odhalen algoritmus, pak totiž pro krátké takové posloupnosti není obtížné vyzkoušet několik málo těles a primitivních polynomů, kterých pro malá tělesa není moc. Bezpečnost uvedené posloupnosti můžeme zvýšit právě zvýšením počtu prvků použitého tělesa.

Závěr

Zjistil jsem, že těleso $\mathbb{F}_{3^n}$ mi vždy poskytne díky uvedenému algoritmu posloupnost, která má stejnou četnost jednotlivých členů, což byl jeden z mých požadavků. Tento požadavek lze opodstatnit tak, že bylo mým cílem získat posloupnost, u které, když se budu ptát, jaké hodnoty nabývá libovolný člen takové posloupnosti, mám pravděpodobnost $\frac{1}{3}$, že to uhodnu. Existují i jiné pohledy na požadavky, například aby získána posloupnost byla náhodnou permutací $-1, 0, 1$.

Co se týče náhodnosti členů posloupnosti při volbě tělesa $\mathbb{F}_{3^n}$, narazil jsem díky autokorelaci na zajímavý fakt, že libovolná taková posloupnost nad $\mathbb{F}_{3^n}$ bude od poloviny totožná až na znaménko. Autokorelace pro dvě poloviny této posloupnosti však byla nulová, čímž jsem došel k závěru, že členy první poloviny posloupnosti jsou na sobě nezávislé a taktéž členy druhé poloviny jsou na sobě nezávislé, ale pouze jedna z polovin posloupnosti je originální.

Literatura

[1] PUPÍK, Petr. Ireducibilní polynomy nad konečnými tělesy [online]. Brno, 2007 [cit. 2020-02-03]. Dostupné z: https://is.muni.cz/th/vr5nq/bakalarka.pdf. Bakalářská práce. Masarykova univerzita.

[2] J. CAMERON, Peter. Introduction to Algebra. Second Edition. Oxford: Oxford University Press, 2008. ISBN 978-0-19-852793-0.

[3] HUCZYNSKA, Sophie. Finite Fields [online]. 2013 [cit. 2020-01-28]. Dostupné z: http://www.math.rwth-aachen.de/~Max.Neunhoeffer/Teaching/ff2013/ff2013.pdf

[4] AKHTER, Fatema a Yasuyuki NOGAMI. Pseudo Random Sequence over Finite Field using Möbius Function. In: IWCI [online]. Dhaka, Bangladesh, 2016, s. 69-73 [cit. 2020-01-28]. ISBN 978-1-5090-5769-6/16/. Dostupné z: https://ieeexplore.ieee.org/document/7860341

[5] MACWILLIAMS, F. Jessie a Neil J. A. SLOANE. Pseudo-Random Sequences and Arrays [online]. In: . IEEE, s. 1715-1729 [cit. 2020-01-28]. Dostupné z: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.477.8455&rep=rep1&type=pdf

[6] DUMMIT, David S. a Richard M. FOOTE. Abstract Algera. Third Edition. USA: John Wiley, 2004. ISBN 0-471-43334-9.

[7] TŮMA, Jiří. Konečná tělesa [online]. [cit. 2020-01-29]. Dostupné z: http://www.karlin.mff.cuni.cz/~barto/student/SkriptaKonTelPuvodni.pdf.Skripta.

[8] SKOUFRANIS, Paul. Determinant Of The Vandermonde Matrix [online]. In: . 2012, 1 - 3 [cit. 2020-02-21]. Dostupné z: http://math.uga.edu/~pete/Skoufranis12.pdf