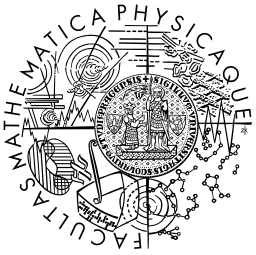

MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Eliška Červenková

Řetězové zlomky v tělese p-adických čísel

Katedra algebry

Vedoucí bakalářské práce: doc. Mgr. Pavel Příhoda, Ph.D.

Studijní program: Matematika

Studijní obor: Obecná matematika

Praha 2023

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů. Tato práce nebyla využita k získání jiného nebo stejného titulu.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ....

Podpis autora

Ráda bych zde poděkovala vedoucímu bakalářské práce doc. Mgr. Pavlu Příhodovi, Ph.D. za ochotu, trpělivost, dále za čas věnovaný konzultacím a za cenné rady při psaní této práce.

Název práce: Řetězové zlomky v tělese p-adických čísel

Autor: Eliška Červenková

Katedra: Katedra algebry

Vedoucí bakalářské práce: doc. Mgr. Pavel Příhoda, Ph.D., Katedra algebry

Abstrakt: Tato práce se věnuje Rubanovu a Browkinovu rozvoji p-adických čísel do řetězového zlomku a jejich vlastnostem. Nejprve je zaveden pojem p-adických čísel a sepsaná potřebná teorie. Následně je definován řetězový zlomek a jsou odvozeny podmínky konvergence v reálných a p-adických číslech. Dále je v textu popsán Rubanův rozvoj do řetězového zlomku a práce se zabývá jeho konečností. Součástí je popis algoritmu, díky kterému lze o konečnosti rozhodnout. Odvozen je i maximální počet kroků v tomto algoritmu. Pro Rubanův rozvoj dále platí, že je-li nekonečný, pak je periodický. V textu je periodicita včetně jejích vlastností blíže popsána. Práce se pak věnuje Browkinovu rozvoji do řetězového zlomku včetně důkazu, že tento rozvoj je pro racionální čísla konečný. Obsahem jsou i příklady ilustrující popsané vlastnosti obou rozvojů.

Klíčová slova: p-adická čísla, řetězové zlomky, Rubanův rozvoj do řetězového zlomku, Browkinův rozvoj do řetězového zlomku

Title: Continued fractions in local fields

Author: Eliška Červenková

Department: Department of algebra

Supervisor: doc. Mgr. Pavel Příhoda, Ph.D., Department of algebra

Abstract: The theses concerns the topic of p-adic Ruban and Browkin continued frations and their properties. To begin with, the concept of p-adic numbers is introduced and the necessary theory is shown. Next, continued fractions are defined and their convergence in both real and p-adic numbers is analyzed. Following this, the theses examines Ruban continued fractions and presents an algorithm for determining whether the expansion is terminating, along with a derivation of the maximum number of algorithmic steps required. It also holds that if Ruban expansion is not terminating, then it is periodic. A detailed description of the periodicity, including its properties, is provided. Then the focus is shifted to Browkin continued fractions. It holds that every rational number has a finite Browkin continued fraction. This claim is subsequently proven. The theses concludes with examples that demonstrate the properties of both Ruban and Browkin continued fractions.

Keywords: p-adic numbers, continued fractions, Ruban continued fractions, Browkin continued fractions

Obsah

Úvod

Řetězové zlomky jsou jedním ze základních nástrojů Teorie čísel. V reálných číslech mají mnoho zajímavých vlastností, například jsou konečné právě tehdy, když reprezentují racionální čísla, nebo díky nim získáme dobré racionální aproximace reálných čísel. Pro definici řetězových zlomků je zásadní celá část, která je v reálných číslech kanonicky definována. V p-adických číslech tomu tak není. Existují různé definice, které uvádí například K. Mahler, T. Schneider, J. Browkin nebo A. A. Ruban. My budeme používat definici A. A. Rubana, která je nejblíže té v reálných číslech. Ruban, stejně jako mnoho jiných matematiků, se snažil řetězové zlomky analogicky zavést v tělese p-adických čísel. Jeho rozvoj je s rozvojem v reálných číslech téměř totožný, avšak veškeré vlastnosti zachovány nejsou.

V této práci se na některé rozvoje p-adických čísel zaměříme. Zajímat nás bude primárně výše zmíněný Rubanův algoritmus, jehož vlastnosti popíšeme podrobněji. V závěru jej porovnáme s algoritmem J. Browkina.

V první kapitole se podíváme na p-adická čísla obecně a odvodíme je takovým způsobem, ze kterého budou více patrné důležité vlastnosti, které později využijeme. Zavedeme pro ně také p-adický rozvoj, normu a valuaci. Více formální odvození a definici p-adických čísel lze pak nalézt například v Bakerově článku (Baker).

Druhá kapitola se věnuje řetězovým zlomkům. Pomocí rekurentních polynomů dále definujeme konvergenty a popíšeme jejich vlastnosti. Následně se zaměříme na konvergenci řetězových zlomků jak v p-adických, tak v reálných číslech.

Třetí kapitola se věnuje Rubanovu rozvoji p-adických čísel do řetězového zlomku a jeho vlastnostem. V úvodu je definována p-adická celá část, která je k zavedení Rubanova rozvoje nezbytná. Hlavním výsledkem této kapitoly je pak rozpracování důkazu věty z článku Capuano, Veneziana a Zanniera (Capuano, Veneziano a Zannier (2019)) týkající se konečnosti a periodicity Rubanova rozvoje. V konečnosti je tento rozvoj odlišný od řetězových zlomků v reálných číslech. Zároveň je zde představen konkrétní algoritmus a ukázán maximální počet jeho kroků, které jsou k rozhodnutí o konečnosti třeba. Kvůli tomuto důkazu ještě navíc zavedeme tzv. logaritmickou a multiplikativní výšku. O této teorii lze nalézt více informací v knize Bombieriho (Bombieri (2007 - 2006)).

Ve čtvrté kapitole popíšeme rozvoj Browkinův. Ten na první pohled vypadá téměř totožně jako rozvoj Rubanův, navíc má mnoho stejných vlastností. Zásadně se však liší v konečnosti. Představíme podrobný důkaz věty z článku Browkina (Browkin (1978)), která říká, že každé racionální číslo má Browkinův rozvoj konečný.

Poslední kapitola obsahuje konkrétní příklady, které ilustrují vlastnosti Rubanova a Browkinova rozvoje dokázané v této práci.

1. p-adická čísla

Buď p prvočíslo a $R = \Pi_{i=1}^{\infty}\mathbb{Z}/p^i\mathbb{Z}$ komutativní okruh. Pro $i \geq 2$ můžeme mezi $\mathbb{Z}/p^i\mathbb{Z}$ a $\mathbb{Z}/p^{i-1}\mathbb{Z}$ definovat zobrazení π_i:

$$z + p^i\mathbb{Z} \mapsto z + p^{i-1}\mathbb{Z}.$$

Dále definujeme *okruh p-adických celých čísel* $\hat{\mathbb{Z}}_p$ jakožto podokruh R následovně

$$\hat{\mathbb{Z}}_p \coloneqq \{(x_1, x_2, \dots) \in R \mid x_i \in \mathbb{Z}/p^i\mathbb{Z},\ \pi_{i+1}(x_{i+1}) = x_i\ \forall i \in \mathbb{N}\}.$$

Označme S množinu reprezentantů rozkladových tříd $\mathbb{Z}/p\mathbb{Z}$. Speciálně se zaměříme na dva případy:

(I) $S = \{0, 1, \dots, p-1\}$. S touto množinou se v literatuře setkáváme standardně. Ve svých studiích při rozvoji p-adických čísel do řetězových zlomků s těmito reprezentaty pracoval například A. A. Ruban (Ruban (1970)).

(II) $S = \{-\frac{p-1}{2}, -\frac{p-1}{2}+1, \dots, \frac{p-1}{2}-1, \frac{p-1}{2}\}$ pro p liché. Tuto množinu ve svém článku používal J. Browkin (Browkin (1978)).

Vezměme libovolný prvek $(y_1 + p\mathbb{Z}, y_2 + p^2\mathbb{Z}, \dots) \in \hat{\mathbb{Z}}_p$. Zřejmě $y_1 + p\mathbb{Z} = s_0 + p\mathbb{Z}$ pro $s_0 \in S$. Dále $y_2 + p^2\mathbb{Z} = y_2' + p^2\mathbb{Z}$ pro $y_2' \in \mathbb{Z}/p^2\mathbb{Z}$ tvaru $s_0' + s_1 p$, kde $s_0', s_1 \in S$. Jelikož platí $\pi_2(y_2' + p^2\mathbb{Z}) = y_1 + p\mathbb{Z} = s_0 + p\mathbb{Z}$, tak $y_2' = s_0 + s_1 p$ pro $s_0, s_1 \in S$. Celkem dostáváme $y_2 + p^2\mathbb{Z} = s_0 + s_1 p + p^2\mathbb{Z}$. Postupnou iterací tohoto výpočtu dostáváme, že pro každý prvek $(y_1 + p\mathbb{Z}, y_2 + p^2\mathbb{Z}, \dots) \in \hat{\mathbb{Z}}_p$ platí $y_i + p^{i+1}\mathbb{Z} = \sum_{j=0}^{i} s_j p^j + p^{i+1}\mathbb{Z}$ pro $s_j \in S$. Libovolný prvek $\hat{\mathbb{Z}}_p$ tak můžeme vyjádřit jako $(s_0 + p\mathbb{Z}, s_0 + s_1 p + p^2\mathbb{Z}, \dots)$, kde $s_i \in S$ pro $i \geq 0$. Všimněme si, že daný prvek $(y_1 + p\mathbb{Z}, y_2 + p^2\mathbb{Z}, \dots) \in \hat{\mathbb{Z}}_p$ je určen posloupností prvků $s_i \in S$.

Definice 1. *Buď $s_0, s_1, \dots$ posloupnost prvků S. Pak $\sum_{i=0}^{\infty} s_i p^i$ označuje prvek $(s_0 + p\mathbb{Z}, s_0 + s_1 p + p^2\mathbb{Z}, \dots, s_0 + s_1 p + \dots + s_i p^i + p^{i+1}\mathbb{Z}, \dots) \in \hat{\mathbb{Z}}_p$.*

Lemma 2. *Pro každé $x \in \hat{\mathbb{Z}}_p$ platí, že vyjádření x ve tvaru $\sum_{i=0}^{\infty} s_i p^i$ je jednoznačné.*

Důkaz: Předpokládejme, že platí $x = \sum_{i=0}^{\infty} s_i p^i = \sum_{i=0}^{\infty} \tilde{s}_i p^i$, kde alespoň pro jedno i platí $s_i \neq \tilde{s}_i$. Nejmenší takové i označíme j. Pro $(j+1)$-tou složku prvku x tak platí

$$\begin{aligned}
s_0 + s_1 p + \dots + s_j p^j + p^{j+1}\mathbb{Z} &= \tilde{s}_0 + \tilde{s}_1 p + \dots + \tilde{s}_j p^j + p^{j+1}\mathbb{Z} \\
s_0 + s_1 p + \dots + s_j p^j + p^{j+1}\mathbb{Z} &= s_0 + s_1 p + \dots + s_{j-1} p^{j-1} + \tilde{s}_j p^j + p^{j+1}\mathbb{Z} \\
s_j p^j + p^{j+1}\mathbb{Z} &= \tilde{s}_j p^j + p^{j+1}\mathbb{Z} \\
(s_j - \tilde{s}_j) p^j &\in p^{j+1}\mathbb{Z}.
\end{aligned}$$

Jelikož $s_j, \tilde{s}_j \in S$, nemůže nastat $s_j \neq \tilde{s}_j$. Dostáváme spor a tedy platí $s_i = \tilde{s}_i$ pro všechna $i \geq 0$ a vyjádření je tudíž jednoznačné.

□

Pro $m > 0$ ještě zavedeme značení

$$\sum_{i=m}^{\infty} s_i p^i = (0 + p\mathbb{Z}, \dots, 0 + p^m\mathbb{Z}, s_m p^m + p^{m+1}\mathbb{Z}, s_m p^m + s_{m+1}p^{m+1} + p^{m+2}\mathbb{Z}, \dots), \tag{1.1}$$

které odpovídá tomu, že $s_i = 0$ pro všechna $0 \leq i \leq m-1$.

Definujeme dále zobrazení Φ :

$$\begin{aligned} \Phi : \mathbb{Z} &\to \hat{\mathbb{Z}}_p \\ z &\mapsto (z + p\mathbb{Z}, z + p^2\mathbb{Z}, \dots). \end{aligned}$$

Jedná se o okruhový homomorfismus. Pokud $z \in \operatorname{Ker}\Phi$, pak $z + p^i\mathbb{Z} = 0 + p^i\mathbb{Z}$ pro všechna $i \geq 0$. Zřejmě $0 \in \operatorname{Ker}\Phi$. Pro libovolné $u \in \mathbb{Z}$ takové, že $u \neq 0$, platí, že existuje nejmenší k takové, že $p^k > u$. Pak pro všechna $i \geq k$ dostáváme $u + p^i\mathbb{Z} \neq 0 + p^i\mathbb{Z}$, a proto $u \notin \operatorname{Ker}\Phi$. Z toho plyne, že $\operatorname{Ker}\Phi = 0$ a zobrazení Φ je prosté.

Abychom výpočty v $\hat{\mathbb{Z}}_p$ mohli provádět s mnohočleny v $\mathbb{Z}$, ztotožníme z a $\Phi(z)$. Nejprve si uvědomme, že

$$\begin{aligned} &\Phi(s_i) = (s_i + p\mathbb{Z}, s_i + p^2\mathbb{Z}, \dots), \\ &\Phi(p) = (p + p\mathbb{Z}, p + p^2\mathbb{Z}, \dots) = (0 + p\mathbb{Z}, p + p^2\mathbb{Z}, \dots), \\ &\Phi(p)^i = \Phi(p^i) = (p^i + p\mathbb{Z}, \dots) = (0 + p\mathbb{Z}, \dots, 0 + p^i\mathbb{Z}, p^i + p^{i+1}\mathbb{Z}, \dots) \text{ pro i>1.} \end{aligned}$$

Jelikož je Φ homomorfismus, tak pro konečné součty platí

$$\Phi\left(\sum_{i=0}^{k} s_i p^i\right) = \sum_{i=0}^{k} \Phi(s_i p^i) = \sum_{i=0}^{k} \Phi(s_i)\Phi(p)^i = \sum_{i=0}^{\infty} s_i p^i,$$

kde $s_i = 0$ pro $i > k$.

Nechť nyní $z \in \mathbb{Z}$. Postupně můžeme spočítat

$$\begin{aligned} z &= z_1 \cdot p + s_0 \\ z_1 &= z_2 \cdot p + s_1 \\ &\vdots \\ z_{k-1} &= z_k \cdot p + s_k \\ &\vdots \end{aligned} \tag{1.2}$$

kde $s_i \in S$ pro všechna $i \geq 0$. Z toho plyne, že $z = s_0 + p(s_1 + p(\dots))$, a proto z můžeme vyjádřit ve tvaru $z = s_0 + s_1 p + s_2 p^2 + \dots$ pro $s_i \in S$ pro všechna $i \geq 0$. Dostáváme tak

$$z = \sum_{i=0}^{\infty} s_i p^i, \tag{1.3}$$

což budeme označovat jako *p-adický rozvoj* čísla z. Můžeme si všimnout, že je-li p-adický rozvoj konečný (tedy existuje $k \in \mathbb{N}$ takové, že $s_j = 0$ pro všechna $j > k$), pak jsou j-té složky prvku $z = \sum_{i=0}^{\infty} s_i p^i$ rovny $z + p^j\mathbb{Z}$ pro všechna $j > k$. Všimněme si také, že takovýto rozvoj je jednoznačně určen posloupností prvků $s_i \in S$.

Poznámka: Ne každé celé číslo lze vyjádřit ve tvaru $\sum_{i=0}^{k} s_i p^i$ pro $k \geq 0$. Například pro volbu $S = \{0, 1, \ldots, p-1\}$ platí $\sum_{i=0}^{k} s_i p^i \geq 0$, tudíž pro záporná celá čísla požadovaný tvar neexistuje.

Dále můžeme ověřit

$$\begin{aligned} p^j \sum_{i=0}^{\infty} s_i p^i &= (0 + p\mathbb{Z}, \ldots, 0 + p^j\mathbb{Z}, p^j + p^{j+1}\mathbb{Z}, p^{j+2}\mathbb{Z}, \ldots)(s_0 + p\mathbb{Z}, \ldots) = \\ &= (0 + p\mathbb{Z}, (s_0 + s_1 p)0 + p^2\mathbb{Z}, \ldots, (s_0 + s_1 p + \cdots + s_i p^i)p^j + p^{i+1}\mathbb{Z}, \ldots)) = \\ &= (0 + p\mathbb{Z}, \ldots, s_0 p^j + s_1 p^{j+1} + \cdots + s_i p^{i+j} + p^{i+j+1}\mathbb{Z}, \ldots)) = \sum_{i=0}^{\infty} s_i p^{i+j}. \end{aligned}$$

Na $\hat{\mathbb{Z}}_p$ definujeme p-adickou valuaci:

Definice 3. *Nechť $x \in \hat{\mathbb{Z}}_p$ s p-adickým rozvojem $\sum_{i=0}^{\infty} s_i p^i$. Definujeme zobrazení $v_p : \hat{\mathbb{Z}}_p \to \mathbb{N}_0 \cup \{\infty\}$ následovně*

$$v_p(x) = \begin{cases} \min\{i \mid s_i \neq 0\}, & \text{pro } x \neq 0, \\ \infty, & \text{pro } x = 0. \end{cases}$$

Toto zobrazení nazveme p-adickou valuací na $\hat{\mathbb{Z}}_p$.

Poznámka: Pro pozdější práci s p-adickou valuací ještě upřesníme: buď $n \in \mathbb{N}_0$, pak

$$\begin{aligned} \infty + \infty &= \infty, \\ \infty + n &= \infty, \\ \infty - n &= \infty, \\ n^{-\infty} &= 0. \end{aligned}$$

Buď nyní $x = (x_1, x_2, \ldots) \in \hat{\mathbb{Z}}_p$ s p-adickým rozvojem $\sum_{i=0}^{\infty} s_i p^i$ takové, že $s_0 \notin p\mathbb{Z}$. Pak pro všechna $j \geq 1$ je prvek $x_j = \sum_{i=0}^{j} s_i p^i + p^{j+1}\mathbb{Z}$ invertibilní v $\mathbb{Z}/p^{j+1}\mathbb{Z}$. Tedy existuje $x_j^{-1} \in \mathbb{Z}/p^{j+1}\mathbb{Z}$ takové, že $x_j^{-1} x_j = 1 + p^{j+1}\mathbb{Z}$. Inverzní prvek k x je pak tvaru $x^{-1} = (x_1^{-1}, x_2^{-1}, \ldots) \in \hat{\mathbb{Z}}_p$.

Poznámka: Libovolný nenulový prvek $x \in \hat{\mathbb{Z}}_p$ s p-adickým rozvojem $\sum_{i=0}^{\infty} s_i p^i$ můžeme vyjádřit jako $p^k x'$, kde $k = v_p(x)$. Pak navíc pro $x' = \sum_{i=0}^{\infty} s'_i p^i$ platí $s'_0 \notin p\mathbb{Z}$ a tudíž x' má inverz x'^{-1}.

Lemma 4 (Baker, str. 16)**.** *Nechť x,y $\in \hat{\mathbb{Z}}_p$. Pak má p-adická valuace následující vlastnosti:*

(i) $v_p(x) = \infty$, *právě když* $x = 0$,

(ii) $v_p(xy) = v_p(x) + v_p(y)$,

(iii) $v_p(x + y) \geq min\{v_p(x), v_p(y)\}$, *přičemž rovnost platí, pokud* $v_p(x) \neq v_p(y)$.

Důkaz:

(*i*) Plyne z definice.

(*ii*) Nejprve nechť $x = 0$ nebo $y = 0$. Bez újmy na obecnosti nechť $x = 0$. Pak

$$v_p(xy) = v_p(0) = \infty,$$
$$v_p(x) + v_p(y) = v_p(0) + v_p(y) = \infty,$$

a lemma tudíž platí. Buďte nyní $x, y \neq 0$, $x = p^k x'$ a $y = p^l y'$ pro $k, l \in \mathbb{N}_0$, $x', y' \in \hat{\mathbb{Z}}_p$ invertibilní. Dostáváme

$$v_p(xy) = v_p(p^{k+l} x' y') = k + l = v_p(p^k x') + v_p(p^l y') = v_p(x) + v_p(y).$$

(*iii*) Nejprve nechť $x = 0$ nebo $y = 0$. Bez újmy na obecnosti nechť $x = 0$. Pak

$$v_p(x + y) = v_p(0 + y) = v_p(y),$$
$$min\{v_p(x), v_p(y)\} = min\{v_p(0), v_p(y)\} = v_p(y),$$

a lemma platí. Buďte nyní $x, y \neq 0$, $x = p^k x'$ a $y = p^l y'$ pro $k, l \in \mathbb{N}_0$, x', y' invertibilní. Bez újmy na obecnosti nechť $v_p(x) = k \geq l = v_p(y)$. Dostáváme

$$v_p(x + y) = v_p(p^k x' + p^l y') = v_p(p^l(p^{k-l} x' + y')) \geq l = min\{v_p(x), v_p(y)\}.$$

Zřejmě pokud $v_p(x) = k > l = v_p(y)$, platí $v_p(x + y) = min\{v_p(x), v_p(y)\}$.

□

Lemma 5. *$\hat{\mathbb{Z}}_p$ je obor integrity.*

Důkaz: Předpokládejme, že existují u,$v \in \hat{\mathbb{Z}}_p$, $u, v \neq 0$ takové, že $u \cdot v = 0$. Můžeme je tedy vyjádřit jako $u = p^k u'$ a $v = p^l v'$ pro $k, l \in \mathbb{N}_0$ a $u', v' \in \hat{\mathbb{Z}}_p$ invertibilní. Pak

$$\begin{aligned} u \cdot v &= 0 \\ p^k u' p^l v' &= 0 \\ p^k u' u'^{-1} p^l v' v'^{-1} &= 0 \cdot u'^{-1} v'^{-1} \\ p^{k+l} &= 0 \end{aligned}$$

což je spor.

□

Vezměme nyní podílové těleso $\hat{\mathbb{Z}}_p$ a označme jej $\mathbb{Q}_p$:

$$\mathbb{Q}_p = \left\{ \frac{u}{v} \;\middle|\; u,v \in \hat{\mathbb{Z}}_p, v \neq 0 \right\}.$$

Budeme jej nazývat *těleso p-adických čísel*. Libovolné $q \in \mathbb{Q}_p$, $q \neq 0$ můžeme s využitím poznámky před lemmatem 5 rozepsat ve tvaru:

$$q = \frac{u}{v} = \frac{p^k u'}{p^l v'} = p^{k-l} u' v'^{-1} = p^m w,$$

kde $w \in \hat{\mathbb{Z}}_p$ invertibilní a $m \in \mathbb{Z}$.

Lemma 6. *Každý prvek $q \in \mathbb{Q}_p$, $q \neq 0$ lze zapsat jednoznačně ve tvaru $\sum_{i=m}^{\infty} s_i p^i$, kde $m \in \mathbb{Z}, s_i \in S$ pro všechna $i \geq m$ a $s_m \notin p\mathbb{Z}$.*

Důkaz: Předpokládejme, že platí $q = p^{m_1} w_1 = p^{m_2} w_2$ pro $m_1, m_2 \in \mathbb{Z}$, $w_1, w_2 \in \hat{\mathbb{Z}}_p$ invertibilní. Bez újmy na obecnosti nechť $m_1 \geq m_2$. Pak

$$\begin{aligned} p^{m_1} w_1 &= p^{m_2} w_2 \\ p^{m_1 - m_2} &= w_1^{-1} w_2 \end{aligned}$$

a jelikož prvek $w_1^{-1} w_2$ je invertibilní v $\hat{\mathbb{Z}}_p$, je nutně invertibilní v $\hat{\mathbb{Z}}_p$ i $p^{m_1 - m_2}$, což implikuje, že $m_1 = m_2$. Z rovnosti $p^{m_1} w_1 = p^{m_2} w_2$ pak plyne, že $w_1 = w_2$ a vyjádření $q = \sum_{i=m}^{\infty} s_i p^i$ je jednoznačné.

□

Vyjádření $q = \sum_{i=m}^{\infty} s_i p^i$ představuje p-adický rozvoj čísla $q \in \mathbb{Q}_p$. Pro $m \geq 0$ se jedná o prvek $\hat{\mathbb{Z}}_p \subset \mathbb{Q}_p$ (viz (1.1)). Pokud $m < 0$, pak

$$\sum_{i=m}^{\infty} s_i p^i = \frac{\sum_{i=0}^{\infty} s_{i-m} p^i}{p^{-m}} \in \mathbb{Q}_p.$$

Alternativně tak můžeme těleso p-adických čísel vyjádřit jako

$$\mathbb{Q}_p = \left\{ \sum_{i=m}^{\infty} s_i p^i \mid m \in \mathbb{Z}, s_i \in S \right\}.$$

Pokud $q = \sum_{i=m}^{\infty} s_i p^i$, budeme pro jednoznačnost zápisu předpokládat, že $s_m \notin p\mathbb{Z}$.

Na $\mathbb{Q}_p$ také definujeme p-adickou valuaci:

Definice 7. *Buď $q \in \mathbb{Q}_p$ takové, že $q = \frac{u}{v}$ pro $u, v \in \hat{\mathbb{Z}}_p$, $v \neq 0$. Pak*

$$v_p\left(\frac{u}{v}\right) = v_p(u) - v_p(v).$$

Pokud pro $u_1, u_2, v_1, v_2 \in \hat{\mathbb{Z}}_p$ takové, že $v_1, v_2 \neq 0$, platí $\frac{u_1}{v_1} = \frac{u_2}{v_2}$, tedy $u_1 v_2 = u_2 v_1$, pak z lemmatu 4 plyne

$$\begin{aligned} v_p(u_1 v_2) &= v_p(u_2 v_1) \\ v_p(u_1) + v_p(v_2) &= v_p(u_2) + v_p(v_1) \\ v_p(u_1) - v_p(v_1) &= v_p(u_2) - v_p(v_2) \\ v_p\left(\frac{u_1}{v_1}\right) &= v_p\left(\frac{u_2}{v_2}\right). \end{aligned}$$

Definice je tedy korektní.
Následuje několik lemmat a definic, které využijeme v následujících kapitolách. Více informací včetně důkazů lze nalézt v práci Bakera (Baker, str. 15-27).

Definice 8. *Buď R komutativní okruh. Nechť $N : R \to \mathbb{R}^+$ je zobrazení splňující následující vlastnosti:*

(i) $N(x) = 0$ právě tehdy, když $x = 0$, $x \in R$,

(*ii*) $N(xy) = N(x)N(y)$ *pro všechna* $x,y \in R$,

(*iii*) $N(x+y) \leq N(x) + N(y)$ *pro všechna* $x,y \in R$.

Pak N nazveme normou. *Můžeme-li podmínku* (*iii*) *nahradit podmínkou silnější*

(*iii'*) $N(x+y) \leq \max\{N(x), N(y)\}$ *pro všechna* $x,y \in R$,

nazýváme takovou normu nearchimédovskou.

Definice 9. *Nechť* $x \in \mathbb{Q}_p$. *Pak*

$$|x|_p = \begin{cases} p^{-v_p(x)} & \text{pro } x \neq 0, \\ p^{-\infty} = 0 & \text{pro } x = 0 \end{cases}$$

nazveme p-adickou normou.

Lemma 10 (Baker, str. 16)**.** *Funkce* $|\ |_p : \mathbb{Q}_p \to \mathbb{R}^+$ *má následující vlastnosti:*

(*i*) $|x|_p = 0$ *právě tehdy, když* $x = 0$,

(*ii*) $|xy|_p = |x|_p|y|_p$ *pro všechna* $x,y \in \mathbb{Q}_p$,

(*iii*) $|x+y|_p \leq max\{|x|_p,|y|_p\}$ *pro všechna* $x,y \in \mathbb{Q}_p$, *přičemž rovnost platí, pokud* $|x|_p \neq |y|_p$.

Definice 11. *Buď R okruh s normou N. Řekneme, že posloupnost* (a_i) *má limitu* $a \in R$, *pokud pro všechna* $\epsilon > 0$ *existuje* $n_0 \in \mathbb{N}$ *takové, že pro všechna* $n > n_0$ *platí* $N(a - a_n) < \epsilon$.

Definice 12. *Buďte* $a_i \in R$. *Řekneme, že posloupnost* (a_i) *je* cauchyovská vzhledem k N, *pokud pro všechna* $\epsilon > 0$ *existuje* $n_0 \in \mathbb{N}$ *takové, že pro všechna* $m, n > n_0$ *platí* $N(a_m - a_n) < \epsilon$.

Definice 13. *Okruh R s normou N nazveme* úplným vzhledem k normě N, *pokud má každá cauchyovská posloupnost limitu.*

Lemma 14. $\mathbb{Q}_p$ *je úplný vzhledem k* $|\ |_p$.

Z definic 11 a 12 mj. plyne, že každá konvergentní posloupnost je cauchyovská. Spolu s definicí 13 a lemmatem 14 dostáváme, že v $\mathbb{Q}_p$ každá posloupnost konverguje právě tehdy, když je cauchyovská.

V práci Bakera (Baker, str. 15-27) lze nalézt ještě jiný způsob zavedení p-adických čísel.

2. Řetězové zlomky

2.1 Definice a základní vlastnosti

V této kapitole budeme pracovat s tělesem $\mathbb{F}$ charakteristiky 0 a zavedeme pojem řetězového zlomku. Definujeme také posloupnosti polynomů, které v následujcích kapitolách využijeme k rozhodnutí o konečnosti rozvojů do řetězových zlomků.

Definice 15. *Buď $\mathbb{F}$ těleso charakteristiky 0. Pro $n \in \mathbb{N}_0$ definujeme* konečný řetězový zlomek délky n+1 *jako posloupnost $a_0, a_1, \ldots, a_n \in \mathbb{F}$ takovou, že výraz*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}$$

je definovaný. Hodnotu konečného řetězového zlomku *budeme značit $[a_0, \ldots, a_n]$ a definujeme ji jako*

$$[a_0, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}.$$

Poznámka: Můžeme si všimnout, že platí $[a_0, a_1, \ldots, a_n] = a_0 + \dfrac{1}{[a_1, a_2, \ldots, a_n]}$.

Definice 16. *Rekurentně definujeme celočíselné polynomy P_n a Q_n v proměnných $x_1, \ldots, x_n$:*

$$\begin{aligned}
&P_{-1} \coloneqq 0,\\
&P_0 \coloneqq 1,\\
&P_1 \coloneqq x_1,\\
&P_{n+1}(x_1, \ldots, x_{n+1}) \coloneqq x_{n+1}P_n(x_1, \ldots, x_n) + P_{n-1}(x_1, \ldots, x_{n-1}),\\
&Q_{-1} \coloneqq 1,\\
&Q_0 \coloneqq 0,\\
&Q_1 \coloneqq 1,\\
&Q_{n+1}(x_2, \ldots, x_{n+1}) \coloneqq x_{n+1}Q_n(x_2, \ldots, x_n) + Q_{n-1}(x_2, \ldots, x_{n-1}).
\end{aligned}$$

Poznámka: Můžeme si všimnout, že $P_n(x_1, \ldots, x_n) = Q_{n+1}(x_1, \ldots, x_n)$. Tyto polynomy splňují mnoho důležitých vlastností, ty nejpodstatnější si dokážeme.

Lemma 17. *Nechť P_n a Q_n jsou definovány jako v definici 16. Označme $M_{x_i} = \begin{pmatrix} x_i & 1 \\ 1 & 0 \end{pmatrix}$. Pak pro všechna $n \geq 1$ platí:*

(*i*) $\begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix} = M_{x_1} \cdot \ldots \cdot M_{x_n}$,

(*ii*) $P_n = \begin{pmatrix} 1 & 0 \end{pmatrix} \cdot M_{x_1} \cdot \ldots \cdot M_{x_n} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$,
$Q_n = \begin{pmatrix} 0 & 1 \end{pmatrix} \cdot M_{x_1} \cdot \ldots \cdot M_{x_n} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$,

(*iii*) $P_n Q_{n-1} - P_{n-1} Q_n = (-1)^n$.

(*iv*) $P_n(x_1, \ldots, x_n) = P_n(x_n, \ldots, x_1)$,
$Q_n(x_2, \ldots, x_n) = Q_n(x_n, \ldots, x_2)$.

Důkaz:

(*i*) Důkaz provedeme indukcí. Pro $n = 1$ dostaneme

$$\begin{pmatrix} P_1 & P_0 \\ Q_1 & Q_0 \end{pmatrix} = \begin{pmatrix} x_1 & 1 \\ 1 & 0 \end{pmatrix} = M_{x_1}.$$

Pro $n + 1 \geq 2$ pak platí

$$M_{x_1} \cdot \ldots \cdot M_{x_{n+1}} = \begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix} \cdot \begin{pmatrix} x_{n+1} & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} x_{n+1}P_n + P_{n-1} & P_n \\ x_{n+1}Q_n + Q_{n-1} & Q_n \end{pmatrix} = \\ = \begin{pmatrix} P_{n+1} & P_n \\ Q_{n+1} & Q_n \end{pmatrix}.$$

(*ii*) Pro $n = 1$ plyne rovnost přímým výpočtem z (*i*). Pro $n \geq 2$ dostaneme

$$P_n = \begin{pmatrix} 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \end{pmatrix} \cdot M_{x_1} \cdot \ldots \cdot M_{x_n} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$
$$Q_n = \begin{pmatrix} 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \end{pmatrix} \cdot M_{x_1} \cdot \ldots \cdot M_{x_n} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

(*iii*) $P_n Q_{n-1} - P_{n-1} Q_n = \det \begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix} = \det(M_{x_1} \cdot \ldots \cdot M_{x_n}) =$
$= \det(M_{x_1}) \cdot \ldots \cdot \det(M_{x_n}) = (-1) \cdot \ldots \cdot (-1) = (-1)^n.$

(*iv*) Levou stranu rovnosti můžeme jakožto matici 1×1 transponovat a dostaneme

$$(P_n(x_1, \ldots, x_n)) = (P_n(x_1, \ldots, x_n))^T = \left[\begin{pmatrix} 1 & 0 \end{pmatrix} \cdot M_{x_1} \cdot \ldots \cdot M_{x_n} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right]^T = \\ = \begin{pmatrix} 1 \\ 0 \end{pmatrix}^T \cdot M_{x_n}^T \cdot \ldots \cdot M_{x_1}^T \cdot \begin{pmatrix} 1 & 0 \end{pmatrix}^T = \begin{pmatrix} 1 & 0 \end{pmatrix} \cdot M_{x_n} \cdot \ldots \cdot M_{x_1} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \\ = P_n(x_n, \ldots, x_1).$$

Pro Q_0 platí rovnost triviálně, pro $n \geq 1$ pak dostáváme

$$Q_n(x_2, \ldots, x_n) = P_{n-1}(x_2, \ldots, x_n) = P_{n-1}(x_n, \ldots, x_2) = Q_n(x_n, \ldots, x_2).$$

□

Lemma 18. *Nechť P_n a Q_n jsou definovány jako v definici 16 a $a_0, a_1, a_2, \ldots \in \mathbb{Q}_p$ takové, že $v_p(a_i) < 0$ pro všechna $i \geq 0$. Pak pro $n \geq 1$ platí*

$$v_p(P_n(a_0, \ldots, a_{n-1})) = \sum_{i=0}^{n-1} v_p(a_i),$$
$$v_p(Q_{n+1}(a_0, \ldots, a_{n-1})) = \sum_{i=0}^{n-1} v_p(a_i).$$

Důkaz: Důkaz provedeme indukcí. Pro $n = 0$ máme

$$\begin{aligned}
&v_p(P_1(a_0)) = v_p(a_0),\\
&v_p(P_2(a_0, a_1)) = v_p(a_1P_1(a_0) + P_0) = min\{v_p(a_1P_1(a_0)), v_p(P_0)\} =\\
&= min\{v_p(a_1) + v_p(P_1(a_0)), 0\} = min\{v_p(a_1) + v_p(a_0), 0\} = v_p(a_1) + v_p(a_0).
\end{aligned}$$

Předpokládejme, že rovnost platí pro $n \geq 2$. Pro $n + 1$ pak dostáváme

$$\begin{aligned}
&v_p(P_{n+1}(a_0, \ldots, a_n)) = v_p(a_nP_n(a_0, \ldots, a_{n-1}) + P_{n-1}(a_0, \ldots, a_{n-2})) =\\
&= min\left\{v_p(a_nP_n(a_0, \ldots, a_{n-1})), v_p(P_{n-1}(a_0, \ldots, a_{n-2}))\right\} =\\
&= min\left\{v_p(a_n) + v_p(P_n(a_0, \ldots, a_{n-1})), \sum_{i=0}^{n-2} v_p(a_i)\right\} =\\
&= min\left\{v_p(a_n) + \sum_{i=0}^{n-1} v_p(a_i), \sum_{i=0}^{n-2} v_p(a_i)\right\} =\\
&= min\left\{\sum_{i=0}^{n} v_p(a_i), \sum_{i=0}^{n-2} v_p(a_i)\right\} = \sum_{i=0}^{n} v_p(a_i).
\end{aligned}$$

Jelikož platí $P_n(x_1, \ldots, x_n) = Q_{n+1}(x_1, \ldots, x_n)$, je rovnost pro $Q_{n+1}(a_0, \ldots, a_{n-1})$ zřejmá.

□

Poznámka:

(*i*) Posloupnost $a_0, a_1, \ldots, a_n \in \mathbb{R}$ taková, že $a_i \in \mathbb{R}^+$ pro $1 \leq i \leq n$, je řetězový zlomek v $\mathbb{R}$, protože $[a_1, a_2, \ldots, a_{n-1}] > 0$ pro všechna $n \geq 2$.

(*ii*) Posloupnost $a_0, a_1, \ldots, a_n \in \mathbb{Q}_p$ taková, že $v_p(a_i)$ pro $1 \leq i \leq n$, je řetězový zlomek v $\mathbb{Q}_p$.

Lemma 19. *Nechť pro $n \geq 1$ je posloupnost $a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}$ řetězový zlomek a P_n a Q_n jsou definovány jako v definici 16. Pak $Q_n(a_1, a_2, \ldots, a_{n-1}) \neq 0$ a platí*

$$[a_0, a_1, \ldots, a_{n-1}] = \frac{P_n(a_0, a_1, \ldots, a_{n-1})}{Q_n(a_1, a_2, \ldots, a_{n-1})}.$$

Důkaz: Důkaz provedeme indukcí podle délky řetězového zlomku n. Pro $n = 1$ dostáváme

$$[a_0] = \frac{P_1(a_0)}{Q_1} = \frac{a_0}{1} = a_0.$$

Předpokládejme nyní, že lemma platí pro $n \geq 2$. S využitím vlastnosti (iv) z lematu 17 pro $n + 1$ dostáváme

$$\begin{aligned}
&[a_0, a_1, a_2, \ldots, a_n] = a_0 + \frac{1}{[a_1, a_2, \ldots, a_n]} = a_0 + \frac{1}{\frac{P_n(a_1,\ldots,a_n)}{Q_n(a_2,\ldots,a_n)}} = \\
&= \frac{a_0 P_n(a_1, \ldots, a_n) + Q_n(a_2, \ldots, a_n)}{P_n(a_1, a_2, \ldots, a_n)} = \frac{a_0 P_n(a_n, \ldots, a_1) + Q_n(a_n, \ldots, a_2)}{P_n(a_1, a_2, \ldots, a_n)} = \\
&= \frac{a_0 P_n(a_n, \ldots, a_1) + P_{n-1}(a_n, \ldots, a_2)}{Q_{n+1}(a_1, a_2, \ldots, a_n)} = \frac{P_{n+1}(a_n, \ldots, a_0)}{Q_{n+1}(a_1, a_2, \ldots, a_n)} = \\
&= \frac{P_{n+1}(a_0, \ldots, a_n)}{Q_{n+1}(a_1, a_2, \ldots, a_n)}.
\end{aligned}$$

Z indukčního předpokladu $[a_1, a_2, \ldots, a_n] = \frac{P_n(a_1,\ldots,a_n)}{Q_n(a_2,\ldots,a_n)}$ a $Q_n(a_2, \ldots, a_n) \neq 0$. Navíc $\frac{P_n(a_1,\ldots,a_n)}{Q_n(a_2,\ldots,a_n)} \neq 0$, jelikož předpokládáme, že $a_0, a_1, a_2, \ldots, a_n$ je řetězový zlomek. Výpočet je proto korektní.

□

2.2 Konvergence v $\mathbb{Q}_p$ a $\mathbb{R}$

V této části se místo obecného tělesa $\mathbb{F}$ s charakteristikou 0 specificky zaměříme na řetězové zlomky v $\mathbb{Q}_p$ a $\mathbb{R}$. Zavedeme pojem konvergence a ukážeme několik podmínek, při jejichž splnění řetězové zlomky konvergují. Tato sekce podrobněji rozvádí důkazy lemmat z článku Capuano a kol. (Capuano a kol. (2019), str. 1855-1856).

Definice 20. Nekonečný řetězový zlomek *definujeme jako nekonečnou posloupnost* $a_0, a_1, \ldots \in \mathbb{F}$*, pro kterou platí, že pro všechna* $n \geq 0$ *je* $a_0, a_1, \ldots, a_n$ *konečný řetězový zlomek.*

Definice 21. *Buď* $a_0, a_1, \ldots \in \mathbb{F}$ *nekonečný řetězový zlomek a nechť* P_n, Q_n *jsou definovány stejně jako v definici 16. Budte*

$$\begin{aligned}
p_n &\coloneqq P_n(a_0, a_1, \ldots, a_{n-1}), \\
q_n &\coloneqq Q_n(a_1, a_2, \ldots, a_{n-1}).
\end{aligned}$$

Pro $n \geq 1$ *definujeme* n-té konvergenty tohoto nekonečného řetězového zlomku *jako* $\frac{p_n}{q_n}$.

Definice 22. *Buď* $\mathbb{F}$ *těleso s normou* N*,* $a_0, a_1, \ldots \in \mathbb{F}$ *nekonečný řetězový zlomek a* p_n, q_n *definované jako v definici 21. Řekneme, že* řetězový zlomek konverguje v $\mathbb{F}$*, pokud posloupnost n-tých konvergentů* $\frac{p_n}{q_n}$ *má limitu vzhledem k* N.

Lemma 23 (Capuano a kol., 2019, str. 1855)**.** *Buď $a_0, a_1, \ldots \in \mathbb{Q}_p$ nekonečný řetězový zlomek takový, že $v_p(a_i) < 0$ pro $i \geq 1$. Pak tento řetězový zlomek v $\mathbb{Q}_p$ konverguje.*

Důkaz: Nejprve odvodíme pomocnou nerovnost. Buď $n \geq 2$. Pak z lemmat 17 a 18 máme

$$v_p\left(\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}\right) = v_p\left(\frac{(-1)^n}{q_n q_{n-1}}\right) = -v_p(q_n q_{n-1}) = -v_p(q_n) - v_p(q_{n-1}) =$$
$$= -\sum_{i=1}^{n-1} v_p(a_i) - \sum_{i=1}^{n-2} v_p(a_i) \geq (n-1) + (n-2) = 2n-3,$$

z čehož pro $n, n' \in \mathbb{N}$ takové, že $n < n'$, zároveň vyplývá

$$v_p\left(\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}\right) < v_p\left(\frac{p_{n'}}{q_{n'}} - \frac{p_{n'-1}}{q_{n'-1}}\right).$$

Nechť nyní $\epsilon > 0$ a $n \leq m$ pro $n, m \in \mathbb{N}$. Pak platí

$$\left|\frac{p_m}{q_m} - \frac{p_n}{q_n}\right|_p = \left|\left(\frac{p_m}{q_m} - \frac{p_{m-1}}{q_{m-1}}\right) + \left(\frac{p_{m-1}}{q_{m-1}} - \frac{p_{m-2}}{q_{m-2}}\right) + \ldots + \left(\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right)\right|_p =$$
$$= p^{-v_p\left(\left(\frac{p_m}{q_m} - \frac{p_{m-1}}{q_{m-1}}\right) + \left(\frac{p_{m-1}}{q_{m-1}} - \frac{p_{m-2}}{q_{m-2}}\right) + \ldots + \left(\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right)\right)} =$$
$$= p^{-\min\limits_{0 \leq i \leq (m-n-1)} \left\{v_p\left(\frac{p_{m-i}}{q_{m-i}} - \frac{p_{m-i-1}}{q_{m-i-1}}\right)\right\}} \leq p^{-v_p\left(\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right)} \leq p^{-(2(n+1)-3)} = p^{-(2n-1)},$$

a tedy pro n takové, že $p^{-(2n-1)} \leq \epsilon$, dostaneme

$$\left|\frac{p_m}{q_m} - \frac{p_n}{q_n}\right|_p \leq \epsilon,$$

tedy posloupnost $\{\frac{p_n}{q_n}\}$ je cauchyovská v $\mathbb{Q}_p$, a proto má v $\mathbb{Q}_p$ limitu.

□

Lemma 24 (Capuano a kol., 2019, str. 1856)**.** *Buď $a_0, a_1, \ldots \in \mathbb{R}$ nekonečný řetězový zlomek takový, že $a_i \in \mathbb{R}^+$ pro $i \geq 1$, a $\frac{p_n}{q_n}$ jsou jeho konvergenty. Pak je v $\mathbb{R}$ posloupnost $\{\frac{p_n}{q_n}\}$ pro sudá n klesající a pro lichá n rostoucí. Navíc každý sudý člen této posloupnosti je menší než člen s lichým indexem.*

Důkaz: Přímo z definice q_n plyne pro všechna $n \geq 1$, že $q_{n+2} \geq q_n > 0$. Dále platí:

$$\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{p_n q_{n-2} - p_{n-2} q_n}{q_n q_{n-2}} = \frac{(a_{n-1}p_{n-1} + p_{n-2})q_{n-2}}{q_n q_{n-2}} -$$
$$- \frac{p_{n-2}(a_{n-1}q_{n-1} + q_{n-2})}{q_n q_{n-2}} = \frac{a_{n-1}(p_{n-1}q_{n-2} - p_{n-2}q_{n-1})}{q_n q_{n-2}} =$$
$$= \frac{a_{n-1}(-1)^{n-1}}{q_n q_{n-2}} = \begin{cases} \dfrac{a_{n-1}}{q_n q_{n-2}} > 0, & \text{pro } n \text{ liché,} \\ \dfrac{-a_{n-1}}{q_n q_{n-2}} < 0, & \text{pro } n \text{ sudé,} \end{cases}$$

a tedy posloupnost $\{\frac{p_n}{q_n}\}$ je pro n sudá klesající a pro n lichá rostoucí. Zároveň z lemmatu 17 části (iii) máme

$$\frac{p_{2k}}{q_{2k}} - \frac{p_{2k-1}}{q_{2k-1}} = \frac{(-1)^{2k}}{q_{2k}q_{2k-1}} = \frac{1}{q_{2k}q_{2k-1}} > 0.$$

Tedy každý sudý člen posloupnosti $\{\frac{p_n}{q_n}\}$ je větší než libovolný člen s lichým indexem. Z toho také plyne, že $\frac{p_n}{q_n}$ jsou omezené.

□

Věta 25 (Capuano a kol., 2019, str. 1856)**.** *Buď $a_0, a_1, \ldots \in \mathbb{R}$ nekonečný řetězový zlomek takový, že pro všechna $i \in \mathbb{N}$ $a_i \in \mathbb{R}^+$. Pak tento řetězový zlomek konverguje v $\mathbb{R}$, právě když $\sum_{i=1}^{\infty} a_i = \infty$, což platí právě tehdy, když q_n jsou neomezené.*

Důkaz: Z lemmatu 24 plyne, že podposloupnost $\{\frac{p_n}{q_n}\}$ pro n sudá je klesající a zdola omezená, tudíž má konečnou limitu v $\mathbb{R}$. Obdobně podposloupnost pro n lichá je rostoucí a shora omezená, tudíž má také konečnou limitu v $\mathbb{R}$. Označme

$$\lim_{k\to\infty} \frac{p_{2k}}{q_{2k}} = A,$$

$$\lim_{k\to\infty} \frac{p_{2k-1}}{q_{2k-1}} = B.$$

Z definice vyplývá, že pro $\epsilon > 0$ existuje k_B takové, že pro všechna $k > k_B$ platí $\left|\frac{p_{2k-1}}{q_{2k-1}} - B\right| < \frac{\epsilon}{2}$. Předpokládejme nyní, že

$$\lim_{k\to\infty} q_{2k}q_{2k-1} = \infty, \text{ ekvivalentně } \lim_{k\to\infty} \frac{1}{q_{2k}q_{2k-1}} = 0.$$

Tedy pro $\epsilon > 0$ existuje l_0 takové, že pro všechna $k > l_0$, platí $\frac{1}{q_{2k}q_{2k-1}} < \frac{\epsilon}{2}$. Pak pro všechna $k > \max\{k_B, l_0\}$ platí

$$\left|\frac{p_{2k}}{q_{2k}} - B\right| = \left|\frac{p_{2k}}{q_{2k}} - \frac{p_{2k-1}}{q_{2k-1}} + \frac{p_{2k-1}}{q_{2k-1}} - B\right| \leq \left|\frac{p_{2k}}{q_{2k}} - \frac{p_{2k-1}}{q_{2k-1}}\right| + \left|\frac{p_{2k-1}}{q_{2k-1}} - B\right| \leq$$
$$\leq \frac{1}{q_{2k}q_{2k-1}} + \frac{\epsilon}{2} < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon,$$

z čehož plyne, že

$$\lim_{k\to\infty} \frac{p_{2k}}{q_{2k}} = B.$$

Z jednoznačnosti limity dostáváme, že $A = B$. Vybraná podposloupnost sudých členů konverguje ke stejné limitě jako vybraná podposloupnost lichých členů, tudíž konverguje i původní posloupnost.

Tedy dokázali jsme, že řetězový zlomek konverguje, pokud $\lim_{k\to\infty} q_n q_{n-1} = \infty$. Pro $n \geq 1$ označme $\tau_n \coloneqq q_n q_{n-1}$. Z definice 16 můžeme odvodit rekurentní vztah:

$$q_{n+1} = a_n q_n + q_{n-1}$$
$$q_n q_{n+1} = a_n q_n^2 + q_n q_{n-1}$$
$$\tau_{n+1} = a_n q_n^2 + \tau_n.$$

Z této rovnosti dále můžeme odvodit:

$$\tau_{n+1} = a_n q_n^2 + a_{n-1} q_{n-1}^2 + \cdots + a_2 q_2^2 + a_1 q_1^2.$$

Nyní opět využijeme vlastnosti $q_{n+2} \geq q_n$ společně s tím, že $q_1 = 1$ a $q_2 = a_1 > 0$. Označme $t = \min\{1, a_1\} > 0$. τ_n pak můžeme odhadnout

$$\tau_{n+1} > a_n t^2 + a_{n-1} t^2 + \cdots + a_2 t^2 + a_1 t^2 = t^2 \sum_{i=1}^{n} a_i.$$

Z této nerovnosti plyne, že když $\sum_{i=1}^{n} a_i$ diverguje, řetězový zlomek v $\mathbb{R}$ konverguje. Současně při divergenci $\sum_{i=1}^{n} a_i$ dostáváme, že $\tau_n \to \infty$, což implikuje neomezenost q_n.
Pro druhou část důkazu potřebujeme pro $n \geq 2$ nejprve dokázat následující odhad

$$q_n \leq (a_{n-1} + 1)(a_{n-2} + 1) \cdot \ldots \cdot (a_1 + 1),$$

což provedeme indukcí. Pro $n = 2$ máme $q_2 = a_1 \leq a_1 + 1$. Nechť nyní nerovnost platí pro $n \geq 3$. Pro $n + 1$ dostáváme

$$\begin{aligned} q_{n+1} &= a_n q_n + q_{n-1} \leq a_n (a_{n-1} + 1) \cdot \ldots \cdot (a_1 + 1) + (a_{n-2} + 1) \cdot \ldots \cdot (a_1 + 1) \leq \\ &\leq a_n (a_{n-1} + 1) \cdot \ldots \cdot (a_1 + 1) + (a_{n-1} + 1)(a_{n-2} + 1) \cdot \ldots \cdot (a_1 + 1) = \\ &= (a_n + 1)(a_{n-1} + 1) \cdot \ldots \cdot (a_1 + 1), \end{aligned}$$

jelikož $(a_{n-1} + 1) \geq 1$. Za využití nerovnosti $x + 1 \leq e^x$ můžeme odhad ještě upravit:

$$q_n \leq (a_{n-1} + 1)(a_{n-2} + 1) \cdot \ldots \cdot (a_1 + 1) \leq e^{a_{n-1}} e^{a_{n-2}} \cdot \ldots \cdot e^{a_1} = e^{\sum_{i=1}^{n-1} a_i}.$$

Tedy pokud $\sum_{i=1}^{n} a_i$ konverguje, jsou q_n omezené. Nechť $q_n < K$ pro všechna $n > 0$ pro $K \in \mathbb{R}^+$. Pak dostaneme

$$\left| \frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} \right| = \frac{1}{q_n q_{n-1}} > \frac{1}{K^2},$$

z čehož vyplývá, že posloupnost $\{\frac{p_n}{q_n}\}$ není cauchyovská a řetězový zlomek proto nekonverguje.

□

3. Rubanův rozvoj do řetězového zlomku

3.1 Definice a základní vlastnosti

V celé této kapitole budeme počítat s p-adickým rozvojem čísla $\alpha \in \mathbb{Q}_p$ ve tvaru $\sum_{i=m}^{\infty} s_i p^i$ pro $m \in \mathbb{Z}$, $s_i \in \{0, 1, \ldots, p-1\}$ a $s_m \neq 0$. Pro zavedení Rubanova rozvoje do řetězového zlomku potřebujeme nejprve pro p-adická čísla definovat p-adickou celou část. Opět rozvedeme důkazy některých lemmat z článku Capuano a kol. (Capuano a kol. (2019), str. 1855-1856).

Definice 26. *Nechť $\alpha \in \mathbb{Q}_p$, $\alpha \neq 0$ a jeho p-adický rozvoj je tvaru $\sum_{i=m}^{\infty} s_i p^i$ pro $m \in \mathbb{Z}$, $s_m \neq 0$. Pak* p-adickou celou část *čísla α značíme $\lfloor \alpha \rfloor_p$ a definujeme jako*

$$\lfloor \alpha \rfloor_p = \begin{cases} \sum_{i=m}^{0} s_i p^i & \text{pro } m \leq 0, \\ 0 & \text{pro } m > 0. \end{cases}$$

Dále definujeme $\lfloor 0 \rfloor_p = 0$.

Tato p-adická celá část splňuje několik důležitých vlastností.

Tvrzení 27. *Nechť $\alpha \in \mathbb{Q}_p$. Pak platí*

(i) $\lfloor \alpha \rfloor_p \in \mathbb{Z}[\frac{1}{p}]$, $|\alpha - \lfloor \alpha \rfloor_p|_p < 1$ *a* $0 \leq \lfloor \alpha \rfloor_p < p$,

(ii) nechť $\beta \in \mathbb{Z}[\frac{1}{p}]$ splňuje vlastnosti z (i), pak $\beta = \lfloor \alpha \rfloor_p$.

Důkaz:

(i) Pro $\alpha = 0$ platí $\lfloor \alpha \rfloor_p = 0$ a vlastnosti jsou splněny. Nechť nyní $\alpha \neq 0$ a $\sum_{i=m}^{\infty} s_i p^i$ je jeho p-adický rozvoj takový, že $s_m \neq 0$. Pro $m > 0$ platí $\lfloor \alpha \rfloor_p = 0$ a vlastnosti jsou splněny. Buď $m \leq 0$. Zřejmě $\lfloor \alpha \rfloor_p = \sum_{i=m}^{0} s_i p^i \in \mathbb{Z}[\frac{1}{p}]$. Jelikož $s_i \in \{0, 1, \ldots, p-1\}$, tak $v_p(s_i) \in \{0, \infty\}$, a proto

$$\left| \alpha - \sum_{i=m}^{0} s_i p^i \right|_p = \left| \sum_{i=1}^{\infty} s_i p^i \right|_p = p^{-v_p\left(\sum_{i=1}^{\infty} s_i p^i\right)} \leq p^{-\left(\min\limits_{1 \leq i \leq \infty} \{v_p(s_i) + v_p(p^i)\}\right)} =$$

$$= \begin{cases} p^{-\left(\min\limits_{1 \leq i \leq \infty} \{i | s_i \neq 0\}\right)} \leq p^{-1} < 1, & \text{pokud existuje } s_i \neq 0 \text{ pro } i \geq 0, \\ p^{-\infty} = 0 < 1, & \text{pokud pro všechna } i \geq 0 \text{ platí } s_i = 0. \end{cases}$$

Dále pak

$$0 \leq \sum_{i=m}^{0} s_i p^i \leq \sum_{i=m}^{0} (p-1) p^i = (p-1) \sum_{j=0}^{-m} p^{-j} = (p-1) \frac{p^m (p^{-m+1} - 1)}{p-1} =$$

$$= \frac{p^{-m+1} - 1}{p^{-m}} = p - p^m < p.$$

(*ii*) Platí

$$0 \leq |\lfloor\alpha\rfloor_p - \beta|_p = |\lfloor\alpha\rfloor_p - \alpha + \alpha - \beta|_p \leq$$
$$\leq \max\{|\lfloor\alpha\rfloor_p - \alpha|_p, |\beta - \alpha|_p\} < 1.$$

A tedy dostáváme

$$p^{-v_p(\lfloor\alpha\rfloor_p - \beta)} < 1 \implies v_p(\lfloor\alpha\rfloor_p - \beta) > 0.$$

Avšak $\lfloor\alpha\rfloor_p, \beta \in \mathbb{Z}[\frac{1}{p}]$, a proto také $\lfloor\alpha\rfloor_p - \beta \in \mathbb{Z}[\frac{1}{p}]$. Pro spor předpokládejme, že $\lfloor\alpha\rfloor_p \neq \beta$, tudíž $\lfloor\alpha\rfloor_p - \beta$ můžeme vyjádřit ve tvaru $\frac{\varkappa}{p^k}$ pro $k \in \mathbb{Z}$ a $\varkappa \in \mathbb{Z}$ takové, že $p \nmid \varkappa$. Z tohoto zápisu je také zřejmé, že $v_p(\lfloor\alpha\rfloor_p - \beta) = -k$. Podle předchozího výpočtu ale víme, že $k < 0$. Z toho plyne $\lfloor\alpha\rfloor_p - \beta \in p\mathbb{Z}$. Jenže $0 \leq \lfloor\alpha\rfloor_p, \beta < p$, tudíž i $|\lfloor\alpha\rfloor_p - \beta| < p$. Celkem dostáváme $\lfloor\alpha\rfloor_p - \beta = 0$, což je spor s předpokladem. Musí tedy platit

$$\lfloor\alpha\rfloor_p = \beta.$$

□

Z definice navíc přímočaře plyne, že $v_p(\lfloor\alpha\rfloor_p) = m$. Nyní už můžeme definovat Rubanův rozvoj do řetězového zlomku.

Definice 28. *Nechť $\alpha \in \mathbb{Q}_p$. Položme*

$$\alpha_0 \coloneqq \alpha, \qquad a_0 \coloneqq \lfloor\alpha_0\rfloor_p, \qquad r_0 \coloneqq \alpha_0 - a_0.$$

Předpokládejme, že jsou definována α_n, a_n a r_n. V případě $r_n \neq 0$ definujeme

$$\alpha_{n+1} \coloneqq \frac{1}{r_n}, \qquad a_{n+1} \coloneqq \lfloor\alpha_{n+1}\rfloor_p, \qquad r_{n+1} \coloneqq \alpha_{n+1} - a_{n+1},$$

ze kterých získáme řetězový zlomek $a_0, a_1, \ldots$, který budeme nazývat Rubanův rozvoj čísla α do řetězového zlomku. *V případě $r_n = 0$ nejsou pro $i \geq n+1$ členy α_i ani a_i definovány, Rubanův rozvoj čísla α do řetězového zlomku je konečný a platí $\alpha = [a_0, a_1, \ldots, a_n]$.*
Pro všechna $n \in \mathbb{N}$, pro která je α_n definováno, zavedeme značení $e_n \coloneqq -v_p(\alpha_n)$.

Definice 29. *Nechť $\alpha \in \mathbb{Q}_p$. Rubanův rozvoj čísla α do řetězového zlomku $a_0, a_1, \ldots$ nazveme* periodický, *pokud existují $k_0, l \geq 0$ takové, že pro všechna $k \geq k_0$ platí $a_k = a_{k+l}$. Nejmenší takové l pak nazýváme* délkou periody.

Dokážeme několik vlastností Rubanova rozvoje do řetězového zlomku, které ve svém článku bez důkazu uvádí Capuano a kol. (Capuano a kol. (2019), str. 1854).

Lemma 30 (Capuano a kol., 2019, str. 1854)**.** *Buď $\alpha \in \mathbb{Q}_p$ a a_n jako v definici 28. Pro $n > 0$ splňuje a_n následující vlastnosti:*

(*i*) $e_n > 0$,

(*ii*) $|a_n|_p = p^{e_n}$,

(*iii*) $0 < a_n \leq p - p^{-e_n} < p$.

Důkaz:

(*i*) Jelikož $n \geq 1$, tak z tvrzení 27 platí

$$\begin{aligned} |\alpha_{n-1} - \lfloor \alpha_{n-1} \rfloor_p|_p &< 1 \\ |\alpha_{n-1} - a_{n-1}|_p &< 1 \\ |r_{n-1}|_p &< 1 \\ p^{-v_p(r_{n-1})} < 1 &\iff v_p\left(\frac{1}{\alpha_n}\right) > 0 \\ v_p(1) - v_p(\alpha_n) &> 0 \\ e_n &> 0 \end{aligned}$$

(*ii*) Z definice 28 plyne $|a_n|_p = p^{-v_p(a_n)} = p^{-v_p(\lfloor \alpha_n \rfloor_p)}$ a zároveň $p^{e_n} = p^{-v_p(\alpha_n)}$. Tedy pro důkaz $|a_n|_p = p^{e_n}$ potřebujeme ověřit, že $v_p(\alpha_n) = v_p(\lfloor \alpha_n \rfloor_p)$. Buď $\sum_{i=m}^{\infty} s_i p^i$ p-adický rozvoj α. Jelikož z části (*i*) víme, že $v_p(\alpha_n) < 0$ pro všechna $n \geq 1$, pak nutně $m < 0$. Z definic 3 a 26 dostaneme

$$\begin{aligned} v_p(\alpha) &= v_p\left(\sum_{i=m}^{\infty} s_i p^i\right) = m, \\ v_p(\lfloor \alpha \rfloor_p) &= v_p\left(\sum_{i=m}^{0} s_i p^i\right) = m, \end{aligned}$$

A tedy $v_p(\alpha) = v_p(\lfloor \alpha \rfloor_p)$.

(*iii*) Z (*i*) a (*ii*) víme, že $v_p(\alpha_n) = v_p(a_n) < 0$. V důkazu tvrzení 27 jsme pro $m = v_p(\lfloor \alpha_n \rfloor_p) < 0$ odvodili

$$0 \leq \lfloor \alpha_n \rfloor_p = \sum_{i=m}^{0} s_i p^i \leq p - p^m.$$

A jelikož přímo z definice 28 plyne, že $a_n \neq 0$ pro $n \geq 1$, a platí $a_n = \lfloor \alpha_n \rfloor_p$, dostáváme požadované nerovnosti.

□

Pokud $|\alpha|_p < 1$, pak $v_p(\alpha) > 0$ a pro $a_0 = \lfloor \alpha \rfloor_p$ platí $|\alpha - \lfloor \alpha \rfloor_p|_p < 1$, a tedy $v_p(\alpha - \lfloor \alpha \rfloor_p) = \min\{v_p(\alpha), v_p(\lfloor \alpha \rfloor_p)\} > 0$. Zároveň ale víme, že

$$\begin{aligned} &v_p(\alpha) > 0, \\ &v_p(\lfloor \alpha \rfloor_p) \begin{cases} = \infty & \text{pro } \lfloor \alpha \rfloor_p = 0, \\ \leq 0 & \text{pro } \lfloor \alpha \rfloor_p \neq 0, \end{cases} \end{aligned}$$

protože $\lfloor \alpha \rfloor_p \in [0, p)$. Tedy dostáváme $a_0 = \lfloor \alpha \rfloor_p = 0$. Dále pro $\alpha_1 = \frac{1}{\alpha}$ máme

$$|\alpha_1|_p = \left|\frac{1}{\alpha}\right|_p = p^{-v_p(\frac{1}{\alpha})} = p^{-(v_p(1) - v_p(\alpha))} = p^{v_p(\alpha)} \geq 1.$$

Z toho plyne, že až na případné posunutí indexů n o 1 můžeme předpokládat $|\alpha|_p \geq 1$, a tedy $a_0 \neq 0$.

Co se týče konvergentů Rubanova rozvoje do řetězového zlomku, tak splňují několik klíčových vlastností. Z definice plyne, že se jedná o nezáporná racionální čísla. Jsou-li v základním tvaru, jejich jmenovatel je mocninou p. Pro $n \geq 1$ navíc $q_n > 0$, díky čemuž jsou n-té konvergenty dobře definované. V následujících lemmatech dokážeme ještě některé jejich další vlastnosti.

Lemma 31 (Capuano a kol., 2019, str. 1854)**.** *Buď $\alpha \in \mathbb{Q}_p$, a_i a α_i definované jako v definici 28 a p_i, q_i jako v definici 21. Pak pro všechna $n \geq 0$, pro která jsou α_n definována, jsou splněny následující rovnosti:*

$$(i)\ \ \alpha = \frac{\alpha_n p_n + p_{n-1}}{\alpha_n q_n + q_{n-1}},$$

$$(ii)\ \ \varphi_n \coloneqq p_n - \alpha q_n = \frac{(-1)^n}{\alpha_n q_n + q_{n-1}}.$$

Důkaz:

$$(i)\ \ \alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{\alpha_n}}}} = \frac{P_{n+1}(a_0, \ldots, a_{n-1}, \alpha_n)}{Q_{n+1}(a_1, \ldots, a_{n-1}, \alpha_n)} =$$

$$= \frac{\alpha_n P_n(a_0, \ldots, a_{n-1}) + P_{n-1}(a_0, \ldots, a_{n-2})}{\alpha_n Q_n(a_1, \ldots, a_{n-1}) + Q_{n-1}(a_1, \ldots, a_{n-2})} = \frac{\alpha_n p_n + p_{n-1}}{\alpha_n q_n + q_{n-1}}.$$

Z lemmatu 30 víme, že $a_i > 0$ pro všechna $i > 0$, a tedy všechny výrazy ve výpočtu jsou dobře definované.

$$(ii)\ \ \varphi_n = p_n - \frac{\alpha_n p_n + p_{n-1}}{\alpha_n q_n + q_{n-1}} q_n = \frac{\alpha_n q_n p_n + q_{n-1} p_n - \alpha_n p_n q_n - p_{n-1} q_n}{\alpha_n q_n + q_{n-1}} =$$

$$= \frac{q_{n-1} p_n - p_{n-1} q_n}{\alpha_n q_n + q_{n-1}} = \frac{(-1)^n}{\alpha_n q_n + q_{n-1}}.$$

□

Z (i) můžeme ještě odvodit

$$\begin{aligned} \alpha &= \frac{\alpha_n p_n + p_{n-1}}{\alpha_n q_n + q_{n-1}} \\ \alpha\alpha_n q_n + \alpha q_{n-1} &= \alpha_n p_n + p_{n-1} \\ \alpha_n(\alpha q_n - p_n) &= p_{n-1} - \alpha q_{n-1} \\ \alpha_n &= \frac{p_{n-1} - \alpha q_{n-1}}{\alpha q_n - p_n} = -\frac{\varphi_{n-1}}{\varphi_n}. \end{aligned} \tag{3.1}$$

3.2 Konečnost Rubanova rozvoje do řetězového zlomku

V této podkapitole se budeme zabývat otázkou, za jakých podmínek je Rubanův rozvoj do řetězového zlomku konečný. Nejprve odvodíme několik nerovností

a odhadů, které později využijeme. Tyto odhady jsou popsány v článku Capuano a kol. (Capuano a kol. (2019), str. 1857).

Buď $a \in \mathbb{R}$, $a > 0$. Označme následující matice a vektory

$$B(a) \coloneqq \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}, \qquad \vec{p_n} \coloneqq \begin{pmatrix} p_n \\ p_{n-1} \end{pmatrix}, \qquad \vec{q_n} \coloneqq \begin{pmatrix} q_n \\ q_{n-1} \end{pmatrix}.$$

Spočteme vlastní čísla matice $B(a)$: $\det(B(a) - xI) = x^2 - ax - 1$, tedy vlastní čísla λ_1, λ_2 jsou kořeny rovnice $x^2 - ax - 1 = 0$. Dostáváme

$$\lambda_{1,2} = \frac{a \pm \sqrt{a^2+4}}{2}.$$

Označíme $\lambda(a)$ maximální vlastní číslo matice $B(a)$. Pro $\lambda_1 = \frac{a+\sqrt{a^2+4}}{2}$ platí

$$\lambda_1 > \frac{a+\sqrt{4}}{2} = 1 + \frac{a}{2},$$

zatímco pro $\lambda_2 = \frac{a-\sqrt{a^2+4}}{2}$ máme

$$\lambda_2 = \frac{a-\sqrt{a^2+4}}{2} < 0.$$

Proto dostáváme $\lambda(a) = \frac{a+\sqrt{a^2+4}}{2}$. Tato vlastní čísla nám poslouží k hornímu odhadu p_n a q_n.

Lemma 32 (Capuano a kol., 2019, str. 1857)**.** *Buď $\alpha \in \mathbb{Q}_p$, $a_0, a_1, \ldots, e_0, e_1, \ldots$ definované jako v definici 28 a p_n, q_n definované jako v definici 21. Nechť platí $a_i > 0$ pro všechna $i \geq 0$. Pak pro $n > 1$ platí*

$$p_n \leq \lambda(a_{n-1}) \cdot \ldots \cdot \lambda(a_0) \qquad a \qquad q_n \leq \lambda(a_{n-1}) \cdot \ldots \cdot \lambda(a_1).$$

Je-li rozvoj konečný délky l, pak platí tytéž rovnosti pro $1 < n \leq l$.

Důkaz: Pro všechna $m \geq 0$ máme $\vec{p}_{m+1} = B(a_m)\vec{p}_m$. Postupnou iterací získáme

$$\vec{p}_{m+1} = B(a_m) \cdot B(a_{m-1}) \cdot \ldots \cdot B(a_0)\vec{p}_0.$$

Jelikož jsou $B(a_i)$ symetrické reálné, a tudíž normální, matice, existují dle Schurovy věty matice Q unitární a D diagonální takové, že jsou-li λ_i vlastní čísla matice $B(a_i)$, pak

$$B(a_i) = \overline{Q}^T D Q, \qquad \text{kde } D = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}.$$

Postupnými úpravami a substitucí $\vec{y} = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = Q\vec{x}$ dostaneme pro libovolné $\vec{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{R}^2$:

$$\|B(a_i)\vec{x}\|^2 = (B(a_i)\vec{x})^T B(a_i)\vec{x} = \vec{\overline{x}}^T \overline{B(a_i)}^T B(a_i)\vec{x} = \vec{\overline{x}}^T \left(\overline{\overline{Q}^T D Q}\right)^T \overline{Q}^T D Q\vec{x} =$$

$$= \vec{\overline{x}}^T \overline{Q}^T \overline{D}^T Q \overline{Q}^T D Q\vec{x} = \vec{\overline{x}}^T \overline{Q}^T D^2 Q\vec{x} = \vec{\overline{y}}^T D^2 \vec{y} = \sum_{i=1}^{2} |\lambda_i|^2 |y_i|^2 \leq \lambda(a_i)^2 \sum_{i=1}^{2} |y_i|^2 =$$

$$= \lambda(a_i)^2 \|Q\vec{x}\|^2 = \lambda(a_i)^2 \|x\|^2,$$

z čehož plyne

$$\|B(a_i)\vec{x}\| \leq \lambda(a_i)\|\vec{x}\|,$$

kde $\|\vec{x}\|$ značí eukleidovskou délku. Za využití iterace a faktu, že $p_0 = 1$ a $p_{-1} = 0$, dostaneme

$$p_n \leq \sqrt{p_n^2 + p_{n-1}^2} = \|\vec{p}_n\| \leq \lambda(a_{n-1}) \cdot \ldots \cdot \lambda(a_0)\|\vec{p}_0\|.$$

Pro q_n je důkaz analogický.

□

Ještě budeme potřebovat odhadnout α_n, k tomu však musíme zavést logaritmickou a multiplikativní výšku. Podrobné odvození a více informací o této teorii lze nalézt v knize Bombieriho (Bombieri (2007 - 2006)).

Definice 33. *Buď $\alpha = \frac{u}{v}$ pro $u, v \in \mathbb{Z}$ takové, že $v \neq 0$ a $gcd(u, v) = 1$.* Logaritmickou výšku $h(\alpha)$ *definujeme následovně:*

$$h(\alpha) = \log \max\{|u|, |v|\}.$$

Dále definujeme multiplikativní výšku $H(\alpha)$ *jako*

$$H(\alpha) = e^{h(\alpha)}.$$

Poznámka: V definici i dále v textu pracujeme s logaritmem o základu e.

Pro logaritmickou výšku dokážeme jednu důležitou nerovnost.

Lemma 34. *Buďte $\alpha, \beta \in \mathbb{Q}$. Pro logaritmickou výšku platí*

$$h(\alpha + \beta) \leq h(\alpha) + h(\beta) + \log 2.$$

Důkaz: Nechť $\alpha = \frac{a}{b}$ pro $a, b \in \mathbb{Z}$ takové, že $gcd(a, b) = 1$, $b \neq 0$ a $\beta = \frac{c}{d}$ pro $c, d \in \mathbb{Z}$ takové, že $d \neq 0$ a $gcd(c, d) = 1$. Pak dostáváme

$$\begin{aligned} h(\alpha + \beta) = h\left(\frac{a}{b} + \frac{c}{d}\right) = h\left(\frac{ad + cb}{bd}\right) \leq \log \max\{|ad + cb|, |bd|\} \leq \\ \leq \log \max\{|ad| + |cb|, |bd|\} \end{aligned}$$

Opět rozlišíme dva případy

$$\begin{aligned} (i)\ |a| \geq |b| \implies |bd|, |ad| + |cb| \leq |ad| + |ca| = |a|(|d| + |c|) \leq \\ \leq 2|a| \max\{|c|,|d|\} = 2 \max\{|a|,|b|\} \cdot \max\{|c|,|d|\}, \end{aligned}$$

$$\begin{aligned} (ii)\ |a| \leq |b| \implies |bd|, |ad| + |cb| \leq |bd| + |cb| = |b|(|d| + |c|) \leq \\ \leq 2|b| \max\{|c|,|d|\} = 2 \max\{|a|,|b|\} \cdot \max\{|c|,|d|\}. \end{aligned}$$

Odtud plyne, že $\max\{|ad|+|cb|,|bd|\} \leq 2\max\{|a|,|b|\}\cdot\max\{|c|,|d|\}$. A tedy

$$\begin{aligned}&\log\max\{|ad|+|cb|,|bd|\} \leq \log(2\max\{|a|,|b|\}\cdot\max\{|c|,|d|\}) = \\ &= \log 2 + \log\max\{|a|,|b|\} + \log\max\{|c|,|d|\} = \log 2 + h\left(\frac{a}{b}\right) + \left(\frac{c}{d}\right) = \\ &= h(\alpha) + h(\beta) + \log 2.\end{aligned}$$

□

V následujícím lemmatu odvodíme primárně kvůli zjednodušení značení dvě nerovnosti.

Lemma 35. *Buď $a_0, a_1, \ldots \in \mathbb{Q}_p$ nekonečný řetězový zlomek. Buďte p_n, q_n definované stejně jako v definici 21. Pak pro $n \geq 1$ platí*

$$-v_p(p_n) = e_0 + \cdots + e_{n-1}, \qquad -v_p(q_n) = e_1 + \cdots + e_{n-1}.$$

Důkaz: Z lemmatu 30 víme, že $v_p(a_i) < 0$ pro $i \geq 1$. Dále z lemmatu 18 dostaneme

$$\begin{aligned}-v_p(p_n) &= -v_p(P_n(a_0,\ldots,a_{n-1})) = -\sum_{i=0}^{n-1} v_p(a_i) = e_0 + \ldots + e_{n-1},\\ -v_p(q_n) &= -v_p(Q_n(a_1,\ldots,a_{n-1})) = -\sum_{i=1}^{n-1} v_p(a_i) = e_1 + \ldots + e_{n-1}.\end{aligned}$$

□

Poznámka: Pro $e_0, e_1, \ldots e_{n-1}$ definované v 28 zavedeme pro $n \geq 1$ značení $s_n \coloneqq e_0 + \ldots + e_{n-1}$ a pro $n = 0$ dodefinujeme $s_0 \coloneqq 0$.

Nyní už můžeme odhadnout logaritmickou výšku α_n.

Lemma 36 (Capuano a kol., 2019, str. 1857)**.** *Buď $\alpha \in \mathbb{Q}$ takové, že $v_p(\alpha) \leq 0$, a α_n definované stejně jako v definici 28. Pak pro všechna $n \geq 0$, pro která je α_n definováno, platí následující nerovnosti*

(*i*) $h(\alpha_n) \leq h(\alpha) + s_n \log p + n\log(2p)$,

(*ii*) $h(\alpha_n) \leq 2^n(h(\alpha) + \log(2p)) - \log(2p)$.

Důkaz:

(*i*) Pro $n = 0$ platí $h(\alpha_0) = h(\alpha)$ a nerovnost je splněna. Pro $n \geq 1$ nejprve odhadneme $h(a_n)$. Z tvrzení 27 víme, že $a_n \in \mathbb{Z}[\frac{1}{p}]$. Tedy pro $k \in \mathbb{N}$ takové, že $p \nmid k$, je a_n tvaru $\frac{k}{p^{e_n}}$, kde $e_n > 0$. Navíc $0 < a_n < p$, a proto $k < p^{e_n+1}$. Dostáváme

$$\begin{aligned}h(a_n) = h\left(\frac{k}{p^{e_n}}\right) &\leq \log\max\{|k|,|p^{e_n}|\} < \log\max\{|p^{e_n+1}|,|p^{e_n}|\} = \\ &= \log(p^{e_n+1}) = (e_n+1)\log p.\end{aligned} \tag{3.2}$$

Dále z definice 28 máme $\frac{1}{\alpha_{n+1}} = \alpha_n - a_n$. Pak s využitím odhadu v (3.2) dostaneme

$$\begin{aligned} h(\alpha_{n+1}) = h\left(\frac{1}{\alpha_{n+1}}\right) = h(\alpha_n - a_n) \leq h(\alpha_n) + h(a_n) + \log 2 \leq \\ \leq h(\alpha_n) + (e_n + 1)\log p + \log 2. \end{aligned} \tag{3.3}$$

Nyní budeme pokračovat indukcí. Pro $n = 1$ máme z (3.3)

$$\begin{aligned} h(\alpha_1) \leq h(\alpha_0) + (e_0 + 1)\log p + \log 2 = h(\alpha) + e_0 \log p + \log p + \log 2 = \\ = h(\alpha) + s_1 \log p + \log(2p). \end{aligned}$$

Nechť dále nerovnost platí pro $n \geq 2$. Z nerovnosti (3.3) pro $n+1$ dostáváme

$$\begin{aligned} h(\alpha_{n+1}) &\leq h(\alpha_n) + (e_n + 1)\log p + \log 2 \leq \\ &\leq h(\alpha) + s_n \log p + n \log(2p) + (e_n + 1)\log p + \log 2 = \\ &= h(\alpha) + (s_n + e_n)\log p + n\log(2p) + \log 2 + \log p = \\ &= h(\alpha) + (s_{n+1})\log p + (n+1)\log(2p). \end{aligned}$$

(*ii*) Pro $n = 0$ platí $h(\alpha_0) = h(\alpha)$ a nerovnost je splněna. Pro $n \geq 1$ nejprve odhadneme $h(\alpha_n)$. Jelikož platí, že $e_n = -v_p(\alpha_n) \geq 0$, vyjádříme α_n ve tvaru $\frac{m}{p^{e_n}}$, kde $p \nmid m$, a dostaneme

$$h(\alpha_n) = h\left(\frac{m}{p^{e_n}}\right) = \log \max\{|m|, |p^{e_n}|\} \geq \log(p^{e_n}) = e_n \log p. \tag{3.4}$$

Zároveň s využitím nerovnosti v (3.2) můžeme odhadnout

$$\begin{aligned} h(\alpha_{n+1}) = h\left(\frac{1}{\alpha_{n+1}}\right) = h(\alpha_n - a_n) \leq h(\alpha_n) + h(a_n) + \log 2 < \\ < h(\alpha_n) + (e_n + 1)\log p + \log 2 = h(\alpha_n) + e_n \log p + \log 2p \leq \\ \leq 2h(\alpha_n) + \log(2p). \end{aligned} \tag{3.5}$$

Dále budeme postupovat indukcí. Pro $n = 1$ máme z (i)

$$h(\alpha_1) \leq h(\alpha) + s_1 \log p + \log(2p) = h(\alpha) + e_0 \log p + \log(2p).$$

Z předpokladu víme, že $e_0 \geq 0$. V případě $e_0 = 0$ plyne přímo z definice 33 $h(\alpha_0) = h(\alpha) \geq 1 > 0 = e_0 \log p$. Pokud $e_0 > 0$, pak můžeme využít přímo nerovnost (3.4). Dostaneme

$$h(\alpha_1) \leq h(\alpha) + h(\alpha_0) + \log(2p) = 2(h(\alpha) + \log(2p)) - \log(2p).$$

Nechť dále nerovnost platí pro $n \geq 2$. Z nerovnosti (3.5) pro $n+1$ dostáváme

$$\begin{aligned} h(\alpha_{n+1}) &\leq 2h(\alpha_n) + \log(2p) \leq \\ &\leq 2(2^n(h(\alpha) + \log(2p)) - \log(2p)) + \log(2p) = \\ &= 2^{n+1}(h(\alpha) + \log(2p)) - 2\log(2p) + \log(2p) = \\ &= 2^{n+1}(h(\alpha) + \log(2p)) - \log(2p). \end{aligned}$$

□

Nyní už můžeme dokázat hlavní větu této podkapitoly. Zde rozepsaný důkaz kopíruje postup v článku Capuano a kol. (Capuano a kol. (2019), str. 1859-1861).

Věta 37 (Capuano, Veneziano a Zannier, 2019, str. 1852)**.** *Buď p prvočíslo a $\alpha \in \mathbb{Q}$, $\alpha \geq 0$. Pak platí*

(*i*) *Rubanův rozvoj čísla α do řetězového zlomku $a_0, a_1, \ldots$ je konečný právě tehdy, když pro všechna $i \geq 0$ platí $\alpha_i \geq 0$; zda toto nastane lze rozhodnout algoritmicky v konečném počtu kroků.*

(*ii*) *Pokud je Rubanův rozvoj čísla α do řetězového zlomku $a_0, a_1, \ldots$ nekonečný, pak je periodický s délkou periody 1 a všechny členy periody jsou rovny $p - p^{-1}$. Předperiodickou část lze navíc spočítat efektivně.*

Poznámka: Z (*i*) je zřejmé, že pro $\alpha \in \mathbb{Q}_p$, $\alpha < 0$ je Rubanův rozvoj do řetězového zlomku vždy nekonečný, jelikož $\alpha_0 = \alpha < 0$.

Důkaz:

(*i*) Během důkazu popíšeme i požadovaný algoritmus. Ten spočívá v tom, že spočteme dostatečně mnoho α_i a zjistíme, zda jsou nezáporné.
Předpokládejme, že jsme spočetli již $a_0, \ldots, a_{n+1}$, $\alpha_0, \ldots, \alpha_{n+1}$ a $\frac{p_0}{q_0}, \ldots, \frac{p_{n+1}}{q_{n+1}}$ pro $n = 2k \geq 2$. Pokud bylo některé ze spočtených α_i záporné, pak se algoritmus zastaví. Bez újmy na obecnosti nechť $\alpha_{n+1} < 0$. Jelikož $a_{n+1} \in (0,p]$, pak $r_{n+1} = \alpha_{n+1} - a_{n+1} < 0$, a tudíž $\alpha_{n+2} = \frac{1}{r_{n+1}} < 0$. Tedy vyskytne-li se při výpočtu záporné α_{k_0}, pak pro všechna $k > k_0$ platí $\alpha_k < 0$ a řetězový zlomek není konečný. Navíc pokud k_0 bylo nejmenší takové, že $\alpha_i < 0$, pak $\alpha_0, \ldots, \alpha_{k_0-1} \geq 0$.

Nyní předpokládejme, že $\alpha_0, \ldots, \alpha_{2k} \geq 0$.

Z lemmatu 31 části (*ii*) dostaneme

$$\frac{p_{2k}}{q_{2k}} - \alpha = \frac{p_{2k} - \alpha q_{2k}}{q_{2k}} = \frac{\frac{(-1)^{2k}}{\alpha_{2k} q_{2k} + q_{2k-1}}}{q_{2k}} > 0,$$

tedy $\alpha \leq \frac{p_{2k}}{q_{2k}}$ a připomeňme $q_{2k-1} \geq q_1 = 1$. Z lemmatu 31 (*ii*) dále můžeme odvodit

$$0 \leq \varphi_{2k} = p_{2k} - \alpha q_{2k} = \frac{1}{\alpha_{2k} q_{2k} + q_{2k-1}} \leq \frac{1}{q_{2k-1}} \leq 1.$$

Protože předpokládáme, že $\alpha \in \mathbb{Q}$, vyjádřeme α jako $\frac{a}{b}$ pro $b = b_0 p^{e_0}$, kde $b, b_0 \in \mathbb{N}^+$ a $p \nmid b_0, a$. Pak dostaneme

$$\begin{aligned}
&v_p(b_0 \varphi_{2k}) = v_p(b_0) + v_p(\varphi_{2k}) = 0 + v_p(\varphi_{2k}) = v_p(p_n - \alpha q_n) = \\
&= v_p\left(\frac{(-1)^n}{\alpha_n q_n - q_{n-1}}\right) = -\min\{v_p(\alpha_n q_n), v_p(q_{n-1})\} = \\
&= -\min\{(v_p(\alpha_n) + v_p(q_n)), v_p(q_{n-1})\} = \\
&= -\min\{(v_p(a_n) + v_p(q_n)), v_p(q_{n-1})\} = \\
&= -\min\{(v_p(a_n q_n)), v_p(q_{n-1})\} = -v_p(a_n q_n + q_{n-1}) = -v_p(q_{n+1}) = \\
&= s_{n+1} - e_0 \geq n.
\end{aligned} \tag{3.6}$$

Navíc víme, že p_i a q_i jsou racionální čísla, která v základním tvaru mají jmenovatele mocninu p. Jelikož z lemmatu 35 máme $v_p(p_i) = -s_i$ a $v_p(q_i) = e_0 - s_i$, můžeme pak p_{2k} a q_{2k} zapsat ve tvaru

$$p_{2k} = \frac{f}{p^{s_{2k}}}, \qquad q_{2k} = \frac{g}{p^{s_{2k}-e_0}},$$

kde f,$g \in \mathbb{Z}$ takové, že $p \nmid f$,g. Pro výraz $b_0\varphi_{2k}$ platí

$$b_0\varphi_{2k} = b_0(p_{2k} - \alpha q_{2k}) = b_0\left(\frac{f}{p^{s_{2k}}} - \frac{a}{b_0 p^{e_0}}\frac{g}{p^{s_{2k}-e_0}}\right) = \frac{f \cdot b_0}{p^{s_{2k}}} - \frac{a \cdot g}{p^{s_{2k}}}$$

a tedy $b_0\left(p_{2k} - \alpha q_{2k}\right) \in \mathbb{Z}[\frac{1}{p}]$.

Pokud $p^{s_{2k+1}} > p^{e_0}b_0 = b$, pak

$$\mathbb{Z} \ni \frac{b_0\varphi_{2k}}{p^{s_{2k+1}-e_0}} = \frac{b_0 p^{e_0}}{p^{s_{2k+1}}}\varphi_{2k} < 1,$$

a tedy nutně $0 = \varphi_{2k} = p_{2k} - \alpha q_{2k}$. Podle lemmatu 19 dostáváme

$$\alpha = \frac{p_{2k}}{q_{2k-1}} = [a_0, \ldots, a_{2k-1}] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{2k-1}}}}.$$

Zároveň však z definice 28 plyne

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots\, a_{2k-2} + \cfrac{1}{\alpha_{2k-1}}}},$$

tudíž $\alpha_{2k-1} = a_{2k-1}$, $r_{2k-1} = \alpha_{2k-1} - a_{2k-1} = 0$ a řetězový zlomek čísla α je konečný.

Rozhodující kritérium je $p^{s_{2k+1}} > b$, což je ekvivalentní podmínce $s_{2k+1} > \frac{\log b}{\log p}$. Navíc $s_{2k+1} = e_0 + \ldots + e_{2k} \geq 2k + 1$, kde $2k + 1$ odpovídá počtu α_i, která potřebujeme spočítat, neboli odpovídá počtu kroků n v algoritmu. V krajním případě $s_{2k+1} = 2k + 1 = n$, a tedy algoritmus se zastaví v okamžik, kdy $n > \frac{\log b}{\log p}$. Tento odhad platí pouze za předpokladu, že algoritmus vykoná alespoň 2 kroky (podmínka $n \geq 2$). Závěr: k rozhodnutí, zda je Rubanův rozvoj čísla α do řetězového zlomku konečný, stačí v algoritmu udělat $\max\{\lceil\frac{\log b}{\log p}\rceil$,2$\}$ kroků.

(*ii*) Můžeme předpokládat, že $v_p(\alpha) < 0$, jelikož pro případ $v_p(\alpha) \geq 0$ můžeme α nahradit α_1, pro které již platí $-v_p(\alpha_1) = e_1 > 0$. Vyjádříme α ve tvaru $\alpha = \frac{d}{bp^{e_0}}$ pro b,$d \in \mathbb{Z}$ takové, že $gcd(b,d) = 1$, $b > 0$ a $p \nmid b$,d. Stejně jako v (*i*) uvažujme čísla $b\varphi_n = b(p_n - \alpha q_n)$.

Jelikož $p_n, q_n \in \mathbb{Z}[\frac{1}{p}]$ a $b \in \mathbb{Z}$, pak platí

$$b\varphi_n = b(p_n - \alpha q_n) = b\left(p_n - \frac{d}{bp^{e_0}}q_n\right) = bp_n - \frac{d}{p^{e_0}}q_n \in \mathbb{Z}[\tfrac{1}{p}].$$

Navíc $p \nmid b$ a podle (3.6) $v_p(\varphi_n) = s_{n+1} - e_0 \geq n$. Můžeme $b\varphi_n$ vyjádřit ve tvaru $\beta_n p^{s_{n+1}-e_0}$ pro $\beta_n \in \mathbb{Z}$, $\beta_n \neq 0$, jelikož Rubanův rozvoj do řetězového zlomku není konečný.

Nyní využijeme odhadu z lemmatu 32:

$$\begin{aligned}
&|p_n - \alpha q_n| \leq |p_n| + |\alpha||q_n| \leq \\
&\leq |\lambda(a_{n-1}) \cdot \ldots \cdot \lambda(a_0)| + |\alpha||\lambda(a_{n-1}) \cdot \ldots \cdot \lambda(a_1)| = \\
&= (|\lambda(a_0)| + |\alpha|)|\lambda(a_{n-1}) \cdot \ldots \cdot \lambda(a_1)|.
\end{aligned}$$

Pro a_i dále z lemmatu 30 platí

$$\begin{aligned}
a_i &\leq p - p^{-e_i} \leq p^{e_i} - p^{-e_i} \\
a_i^2 + 4 &\leq (p^{e_i} - p^{-e_i})^2 + 4 \\
a_i^2 + 4 &\leq (p^{e_i} + p^{-e_i})^2 \\
\sqrt{a_i^2 + 4} &\leq p^{e_i} + p^{-e_i} \\
\frac{a_i + \sqrt{a_i^2 + 4}}{2} &\leq \frac{a_i + p^{e_i} + p^{-e_i}}{2} \\
\frac{a_i + \sqrt{a_i^2 + 4}}{2} &\leq \frac{p^{e_i} - p^{-e_i} + p^{e_i} + p^{-e_i}}{2} \\
\frac{a_i + \sqrt{a_i^2 + 4}}{2} &\leq \frac{2p^{e_i}}{2} \\
\lambda(a_i) &\leq p^{e_i}.
\end{aligned} \tag{3.7}$$

Jelikož $0 < a_i \leq p - p^{-e_i}$, tak rovnost v (3.7) může nastat pouze v případě $e_i = 1$, tedy pro $a_i = p - p^{-1}$.

Ještě využijeme nerovnosti odvozené v lemmatu 36. Dostaneme

$$H(\alpha) = H\left(\frac{d}{bp^{e_0}}\right) = e^{\log \max\{|d|,|bp^{e_0}|\}} = \max\{|d|,|bp^{e_0}|\}.$$

Tedy platí $|bp^{e_0}| \leq H(\alpha)$ a $|b\alpha| = \frac{|d|}{p^{e_0}} \leq |d| \leq H(\alpha)$ a celkem dostáváme odhad

$$b(p^{e_0} + |\alpha|) \leq 2H(\alpha).$$

Nyní můžeme odhadnout $|\beta_n|$ nezávisle na n:

$$\begin{aligned}
1 \leq |\beta_n| &= \left|\frac{b(p_n - \alpha q_n)}{p^{s_{n+1}-e_0}}\right| \leq b(|\lambda(a_0)| + |\alpha|)p^{-(e_1+\cdots+e_n)} \prod_{i=1}^{n-1} \lambda(a_i) = \\
&= b(|\lambda(a_0)| + |\alpha|)p^{-e_n} \prod_{i=1}^{n-1} \frac{\lambda(a_i)}{p^{e_i}} \leq b(|\lambda(p^{e_0})| + |\alpha|)\frac{1}{p^{e_n}} \prod_{i=1}^{n-1} \frac{p^{e_i}}{p^{e_i}} \leq \\
&\leq 2H(\alpha)\frac{1}{p} = \frac{2H(\alpha)}{p}.
\end{aligned}$$

Jelikož $\beta_n \in \mathbb{Z}$, tak $|\beta_n|$ patří do konečné množiny s kardinalitou nejvýše $\frac{2H(\alpha)}{p}$.

Nyní odhadneme $\lambda(a_i)p^{-1}$. Rozlišíme dva případy:

(a) pro $e_i = 1$ a $a_i \neq p - p^{-1}$:
a_i je tvaru $\frac{r}{p}$ pro $p \nmid r$ a $a_i < p - p^{-1} = \frac{p^2-1}{p} \implies a_i \leq \frac{p^2-2}{p} = p - 2p^{-1}$.
Pak

$$\lambda(a_i)p^{-1} \leq \lambda(p - 2p^{-1})p^{-1} \leq \frac{p - 2p^{-1} + \sqrt{(p - 2p^{-1})^2 + 4}}{2p} =$$
$$= \frac{p - 2p^{-1} + \sqrt{p^2 + 4p^{-2}}}{2p} = \frac{p^2 - 2 + \sqrt{p^4 + 4}}{2p^2} \leq$$
$$\leq \frac{2p^2 - 4 + 2\sqrt{p^4 + 4}}{4p^2} \leq \frac{2p^2 - 4 + 2\sqrt{p^4 + p^2 + \frac{1}{4}}}{4p^2} \leq$$
$$\leq \frac{2p^2 - 4 + 2(p^2 + \frac{1}{2})}{4p^2} = \frac{4p^2 - 3}{4p^2} = 1 - \frac{3}{4p^2}.$$

(b) pro $e_i \geq 2$:

$$\lambda(a_i)p^{-e_i} \leq \lambda(p)p^{-e_i} = \frac{(p + \sqrt{p^2 + 4})}{2}p^{-e_i} \leq \frac{(p + \sqrt{p^2 + p^2})}{2p^{e_i}} \leq$$
$$\leq \frac{(1 + \sqrt{2})p}{2p^{e_i}} \leq \left(\frac{(1 + \sqrt{2})}{2p}\right)^{e_i - 1} \leq \left(\frac{(1 + \sqrt{2})}{4}\right)^{e_i - 1}.$$

Zřejmě $\frac{(1+\sqrt{2})}{4} < 1$ a $e_i - 1 \geq \frac{e_i}{2}$. Navíc platí

$$p^2 > \frac{3}{4\left(1 - \sqrt{\frac{1+\sqrt{2}}{4}}\right)} \implies \left(\frac{1 + \sqrt{2}}{4}\right)^{\frac{1}{2}} < 1 - \frac{3}{4p^2},$$

díky čemuž můžeme dokončit odhad:

$$\lambda(a_i)p^{-e_i} \leq \left(\frac{(1 + \sqrt{2})}{4}\right)^{e_i - 1} \leq \left(\frac{(1 + \sqrt{2})}{4}\right)^{\frac{e_i}{2}} \leq \left(1 - \frac{3}{4p^2}\right)^{e_i}.$$

Celkem dostáváme, že pro $a_i \neq p - p^{-1}$ platí $\lambda(a_i)p^{-e_i} \leq \left(1 - \frac{3}{4p^2}\right)^{e_i}$.
Označme ještě

$$\sigma_n = \sum_{\substack{1 \leq i \leq n-1 \\ a_i \neq p - p^{-1}}} e_i.$$

Pak

$$1 \leq b(|\lambda(a_0)| + |\alpha|)p^{-e_n} \prod_{i=1}^{n-1} \frac{\lambda(a_i)}{p^{e_i}} \leq b(|\lambda(a_0)| + |\alpha|)p^{-1} \prod_{i=1}^{n-1} \left(1 - \frac{3}{4p^2}\right)^{e_i} =$$
$$= b(|\lambda(a_0)| + |\alpha|)p^{-1} \left(1 - \frac{3}{4p^2}\right)^{\sigma_n} \leq \frac{2H(\alpha)}{p} \left(1 - \frac{3}{4p^2}\right)^{\sigma_n}.$$

Vidíme, že nezávisle na n je σ_n omezeno, což znamená, že jen konečně mnoho a_n není rovno $p - p^{-1}$. Tedy existuje $n_0 \in \mathbb{N}$ takové, že pro všechna $n > n_0$ je $a_n = p - p^{-1}$ a řetězový zlomek je tak periodický.

Z rovnosti (3.1) vezměme nyní v úvahu

$$\alpha_n = -\frac{\varphi_{n-1}}{\varphi_n} = -\frac{\frac{\beta_{n-1}p^{s_n-e_0}}{b}}{\frac{\beta_n p^{s_{n+1}-e_0}}{b}} = -\frac{\beta_{n-1}}{\beta_n p^{e_n}}.$$

Ukázali jsme, že všechna $|\beta_n|$ náleží konečné množině s kardinalitou nejvýše $\frac{2H(\alpha)}{p}$. Přesněji jsme určili, že $|\beta_n| \leq \frac{2H(\alpha)}{p^{e_n}}$. Tedy $|p^{e_n}\beta_n|$ náleží konečné množině s kardinalitou nejvýše $\frac{2H(\alpha)}{p^{e_n}}p^{e_n} = 2H(\alpha)$. Celkově dostáváme, že $|\alpha_n| \leq \frac{2H(\alpha)}{p}2H(\alpha) = \frac{4H(\alpha)^2}{p}$ a α_n náleží konečné množině s kardinalitou nejvýše $2\frac{4H(\alpha)^2}{p} = \frac{8H(\alpha)^2}{p}$. To znamená, že existují $i < j \leq \frac{8H(\alpha)^2}{p} + 1$ takové, že $\alpha_i = \alpha_j$ a pro všechna $k > i$ už platí $a_i = a_k = p - p^{-1}$.

Pro tento výpočet jsme předpokládali, že $e_0 > 0$, přičemž pokud by to náhodou neplatilo, dosadili jsme $\alpha_0 = \alpha_1$. V tomto případě by samozřejmě došlo k prodloužení předperiodické části o 1. V odhadu bychom pak ještě museli nahradit $H(\alpha)$ za $H(\alpha_1)$. Jelikož v tomto případě $e_0 < 0$, z lemmatu 36 části (ii) odvodíme

$$H(\alpha_1) \leq H(\alpha)p^{e_0}2p \leq H(\alpha)2p.$$

Závěr: pokud je Rubanův rozvoj do řetězového zlomku nekonečný, délka předperiodické části je maximálně $32pH(\alpha)^2$.

□

Poznámka: Tvrzení platí i pro $\alpha = 0$, protože pak $\alpha_0 = a_0 = r_0 = 0$ a Rubanův rozvoj do řetězového zlomku je tak konečný.

4. Browkinův rozvoj do řetězového zlomku

4.1 Definice a základní vlastnosti

Browkinův rozvoj do řetězového zlomku je velmi podobný rozvoji Rubanovu. V této kapitole budeme vycházet z článku Browkina (Browkin (1978)). Nechť p je prvočíslo takové, že $p \geq 3$. Při zavedení p-adických čísel jsme ukázali, že každé $q \in \mathbb{Q}_p$ lze zapsat ve tvaru

$$q = \sum_{i=m}^{\infty} s_i p^i$$

pro nějaké $m \in \mathbb{Z}$ a $s_i \in \mathbb{Z}/p\mathbb{Z}$. Na rozdíl od předchozí kapitoly budeme ovšem nyní pro p uvažovat $s_i \in \{-\frac{p-1}{2}, \ldots, \frac{p-1}{2}\}$. Opět zavedeme p-adickou celou část, která, ač je definovaná stejně jako pro Rubanův rozvoj, má odlišné vlastnosti. Budeme ji tedy i odlišně značit.

Definice 38. *Nechť $\alpha \in \mathbb{Q}_p$ a jeho p-adický rozvoj je tvaru $\sum_{i=m}^{\infty} s_i p^i$ pro $m \in \mathbb{Z}$, $s_m \neq 0$. Pak* p-adickou celou část *čísla α značíme $\langle \alpha \rangle_p$ a definujeme jako*

$$\langle \alpha \rangle_p = \begin{cases} \sum_{i=m}^{0} s_i p^i & \text{pro } m \leq 0, \\ 0 & \text{pro } m > 0. \end{cases}$$

Dále definujeme $\langle 0 \rangle_p = 0$.

Tvrzení 39. *Nechť $\alpha \in \mathbb{Q}_p$. Pak*

(*i*) $\langle \alpha \rangle_p \in \mathbb{Z}[\frac{1}{p}]$, $|\langle \alpha \rangle_p| < \frac{p}{2}$ *a* $|\alpha - \langle \alpha \rangle_p|_p < 1$,

(*ii*) *nechť $\beta \in \mathbb{Z}_p$ splňuje vlastnosti z (i), pak $\beta = \langle \alpha \rangle_p$.*

Důkaz:

(*i*) Pro $\alpha = 0$ platí $\langle \alpha \rangle_p = 0$ a vlastnosti jsou splněny. Nechť nyní $\alpha \neq 0$ a $\sum_{i=m}^{\infty} s_i p^i$ je jeho p-adický rozvoj takový, že $s_m \neq 0$. Pro $m > 0$ platí $\langle \alpha \rangle_p = 0$ a vlastnosti jsou splněny. Buď $m \leq 0$. Zřejmě $\langle \alpha \rangle_p = \sum_{i=m}^{0} s_i p^i \in \mathbb{Z}[\frac{1}{p}]$. Jelikož $s_i \in \{0, 1, \ldots, p-1\}$, tak $v_p(s_i) \in \{0, \infty\}$, a proto

$$\left| \alpha - \sum_{i=m}^{0} s_i p^i \right|_p = \left| \sum_{i=1}^{\infty} s_i p^i \right|_p = p^{-v_p\left(\sum_{i=1}^{\infty} s_i p^i\right)} \leq p^{-\left(\min\limits_{1 \leq i \leq \infty} \{v_p(s_i) + v_p(p^i)\}\right)} =$$

$$= \begin{cases} p^{-\left(\min\limits_{1 \leq i \leq \infty} \{i | s_i \neq 0\}\right)} \leq p^{-1} < 1, & \text{pokud existuje } s_i \neq 0 \text{ pro } i \geq 0, \\ p^{-\infty} = 0 < 1, & \text{pokud pro všechna } i \geq 0 \text{ platí } s_i = 0. \end{cases}$$

Dále

$$|\langle\alpha\rangle_p| = \left|\sum_{i=m}^{0} s_i p^i\right| \leq \frac{1}{2}(p-1)\sum_{i=m}^{0} p^i = \frac{1}{2}(p-1)p^{-m}\sum_{j=0}^{m} p^j =$$
$$= \frac{1}{2}(p-1)p^{-m}\frac{p^{m+1}-1}{p-1} = \frac{1}{2}\frac{p^{m+1}-1}{p^m} < \frac{p}{2}.$$

(*ii*) Důkaz je stejný jako v tvrzení 27 části (*ii*).

□

Browkinův rozvoj do řetězového zlomku je pak definován analogicky jako rozvoj Rubanův:

Definice 40. *Buď $\alpha \in \mathbb{Q}_p$ a položme*

$$\alpha_0 \coloneqq \alpha, \qquad b_0 \coloneqq \langle\alpha_0\rangle_p, \qquad r_0 = \alpha_0 - b_0.$$

Předpokládejme, že jsou definována α_n, b_n a r_n. V případě $r_n \neq 0$ definujeme

$$\alpha_{n+1} \coloneqq \frac{1}{r_n}, \qquad b_n \coloneqq \langle\alpha_n\rangle_p., \qquad r_{n+1} \coloneqq \alpha_{n+1} - b_{n+1},$$

ze kterých získáme řetězový zlomek $b_0, b_1, \ldots,$ který budeme nazývat Browkinův rozvoj čísla α do řetězového zlomku. *V případě $r_n = 0$ již nejsou pro $i \geq n+1$ členy α_i ani b_i definovány, Browkinův rozvoj čísla α do řetězového zlomku je konečný a platí $\alpha = [b_0, b_1, \ldots, b_n]$.*

Můžeme si všimnout, že platí $v_p(\alpha_n - \langle\alpha_n\rangle_p) = v_p(\sum_{i=1}^{\infty} s_i p^i) > 0$, a tedy opět $v_p(\alpha_{n+1}) = -v_p(\alpha_n - \langle\alpha_n\rangle_p) < 0$ pro $n > 0$. Dále

$$\begin{aligned} v_p(b_{n+1}) &= v_p(\alpha_{n+1} + (\langle\alpha_{n+1}\rangle_p - \alpha_{n+1})) = \\ &= \min\{v_p(\alpha_{n+1}), v_p(\langle\alpha_{n+1}\rangle_p - \alpha_{n+1})\} = v_p(\alpha_{n+1}), \end{aligned} \tag{4.1}$$

jelikož $v_p(\alpha_{n+1}) < 0$, zatímco $v_p(\langle\alpha_{n+1}\rangle_p - \alpha_{n+1}) > 0$. Tato nerovnost platí pro $n > 0$. V případě b_0 může nastat:

$$v_p(b_0) = v_p(\langle\alpha\rangle_p) = \begin{cases} v_p(\alpha_0) & \text{pro } v_p(\alpha) \leq 0, \\ v_p(0) & \text{pro } v_p(\alpha) > 0, \end{cases}$$

což mj. znamená, že $b_0 = 0$ nebo $v_p(b_0) = v_p(\alpha_0) \leq 0$.

Připomeňme ještě definici konvergentů $\frac{p_n}{q_n}$:

$$p_n \coloneqq P_n(b_0, b_1, \ldots, b_{n-1}),$$
$$q_n \coloneqq Q_n(b_1, b_2, \ldots, b_{n-1}).$$

Podle lemmat 17 a 19 platí

$$[b_0, b_1, \ldots, b_n] = \frac{p_n}{q_n} \qquad \text{a} \qquad \frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^n}{q_n q_{n-1}}.$$

Podle lemmatu 18 navíc máme, že $v_p(q_n) = v_p(b_1) + v_p(b_2) + \cdots + v_p(b_{n-1})$ pro $n \geq 1$.

4.2 Konečnost Browkinova rozvoje do řetězového zlomku

V této části dokážeme hlavní rozdíl mezi rozvojem Browkinovým a Rubanovým; Browkinův rozvoj racionálního čísla do řetězového zlomku je totiž vždy konečný. Podrobně rozvedeme důkaz tohoto tvrzení z Browkinova článku (Browkin (1978)).Pokud je Browkinův rozvoj čísla $\alpha \notin \mathbb{Q}$ do řetězového zlomku nekonečný, pak posloupnost $\frac{p_n}{q_n}$ konverguje v $\mathbb{Q}_p$ k α, což je tvrzení z téhož článku (str. 7-8).

Věta 41 (Browkin, 1978, str.73)**.** *Buď $\alpha \in \mathbb{Q}$. Pak je Browkinův rozvoj do řetězového zlomku konečný.*

Důkaz: Buďte α_n a b_n definované jako v definici 40. Pro $n \geq 1$ máme $\alpha_n = b_n + \alpha_{n+1}^{-1}$. Víme, že $b_n = \langle \alpha_n \rangle_p \in \mathbb{Z}[\frac{1}{p}] \subseteq \mathbb{Q}$, tedy můžeme b_n vyjádřit ve tvaru $\frac{d_n}{p^{-v_p(b_n)}}$ pro $d_n \in \mathbb{Z}$ a $v_p(b_n) < 0$. Navíc z tvrzení 39 máme odhad $|b_n| \leq \frac{p}{2}$. Pak

$$\begin{aligned} |b_n| &\leq \frac{p}{2} \\ \left|\frac{d_n}{p^{-v_p(b_n)}}\right| &\leq \frac{p}{2} \\ |d_n| = |b_n| \cdot |p^{-v_p(b_n)}| &\leq \frac{1}{2} \cdot p \cdot p^{-v_p(b_n)} = \frac{p^{-v_p(b_n)+1}}{2}. \end{aligned} \tag{4.2}$$

Jelikož $\alpha_0 = \alpha \in \mathbb{Q}$ a $b_0 = \langle \alpha_0 \rangle_p \in \mathbb{Z}[\frac{1}{p}]$, tak $\alpha_1 = \frac{1}{\alpha_0 - \langle \alpha \rangle_p} \in \mathbb{Q}$. Indukcí tedy můžeme odvodit, že všechna definovaná α_n jsou racionální. V (4.1) jsme ukázali, že $v_p(b_n) = v_p(\alpha_n)$, proto můžeme α_n vyjádřit ve tvaru

$$\alpha_n = \frac{\gamma_n}{p^{-v_p(b_n)}\beta_n},$$

kde $\beta_n, \gamma_n \in \mathbb{Z}$, $\gcd(\beta_n, \gamma_n)$=1 a $p \nmid \beta_n, \gamma_n$. Obdobně

$$\alpha_{n+1} = \frac{\gamma_{n+1}}{p^{-v_p(b_{n+1})}\beta_{n+1}},$$

kde $-v_p(b_{n+1}) \geq 1$, $\gamma_{n+1}, \beta_{n+1} \in \mathbb{Z}$, $\gcd(\gamma_{n+1}, \beta_{n+1})$=1 a $p \nmid \gamma_{n+1}, \beta_{n+1}$.

Z těchto dvou vyjádření můžeme dále odvodit

$$\frac{\gamma_{n+1}}{p^{-v_p(b_{n+1})}\beta_{n+1}} = \alpha_{n+1} = \frac{1}{\alpha_n - b_n} = \frac{1}{\frac{\gamma_n}{p^{-v_p(b_n)}\beta_n} - \frac{d_n}{p^{-v_p(b_n)}}} = \frac{p^{-v_p(b_n)}\beta_n}{\gamma_n - d_n\beta_n},$$

z čehož dostáváme

$$\gamma_{n+1}(\gamma_n - d_n\beta_n) = p^{-v_p(b_n)-v_p(b_{n+1})}\beta_n\beta_{n+1}. \tag{4.3}$$

Víme, že $\gcd(\gamma_{n+1}, \beta_{n+1})$=1, $\gcd(p^{-v_p(b_n)-v_p(b_{n+1})}, \gamma_{n+1})$=1 a z rovnosti (4.3) navíc $\gamma_{n+1} \mid p^{-v_p(b_n)-v_p(b_{n+1})}\beta_n\beta_{n+1}$. Nutně tedy platí, že $\gamma_{n+1} \mid \beta_n$.

Obdobnou úvahu provedeme pro β_n. Z rovnosti v (4.3) víme, že $\beta_n \mid (\gamma_{n+1}\gamma_n - \gamma_{n+1}d_n\beta_n)$. Jelikož však zároveň $\beta_n \mid -d_n\beta_n\gamma_{n+1}$, tak musí platit $\beta_n \mid \gamma_{n+1}\gamma_n$. Avšak $\gcd(\beta_n, \gamma_n)=1$, což implikuje $\beta_n \mid \gamma_{n+1}$.

Dohromady dostáváme $\beta_n||\gamma_{n+1}$, a tedy $\beta_n = \pm\gamma_{n+1}$. Tento poznatek společně s nerovnostmi v tvrzení 39 a (4.2) a rovností v (4.3) použijeme k odhadu β_{n+1}:

$$|\beta_{n+1}| = |p^{v_p(b_n)+v_p(b_{n+1})}(\gamma_n - d_n\beta_n)| \leq |p^{v_p(b_n)+v_p(b_{n+1})}|(|\gamma_n| + |d_n||\beta_n|) \leq$$
$$\leq p^{v_p(b_n)+v_p(b_{n+1})}(|\gamma_n| + \frac{p^{-v_p(b_n)+1}}{2}|\beta_n|) = p^{v_p(b_n)+v_p(b_{n+1})}|\gamma_n| + \frac{p^{v_p(b_{n+1})+1}}{2}|\beta_n| <$$
$$< \frac{1}{2}|\gamma_n| + \frac{1}{2}|\beta_n|.$$

Celkem můžeme odhadnout

$$|\gamma_{n+1}| + 2|\beta_{n+1}| < |\beta_n| + (|\beta_n| + |\gamma_n|) = |\gamma_n| + 2|\beta_n|.$$

Jelikož posloupnost $(|\gamma_n| + 2|\beta_n|)$ se skládá z přirozených čísel a je klesající, musí být konečná. To znamená, že je definováno pouze konečně mnoho α_n a Browkinův rozvoj do řetězového zlomku je tak konečný.

□

5. Příklady

Buď p=5.

Příklad 1. $\alpha = \frac{281}{116}$
Ukážeme, jak spočítat Rubanův rozvoj do řetězového zlomku. Nejprve potřebujeme najít p-adický rozvoj čísla $\frac{281}{116}$. Postupovat budeme jako v případě (1.2). Tedy chceme vyjádřit α ve tvaru $z_1 \cdot 5 + s_0$, kde $s_0 \in S$, tedy v případě Rubanova rozvoje $s_0 \in \{0,1,2,3,4\}$. Spočteme

$$\begin{aligned} &\frac{281}{116} \mod 5 = 1 \\ &\frac{281}{116} - 1 = \frac{165}{116} = 5 \cdot \frac{33}{116}. \end{aligned}$$

Analogicky pokračujeme dále, stejný výpočet provedeme pro $\frac{33}{116}$:

$$\begin{aligned} &\frac{33}{116} \mod 5 = 3 \\ &\frac{33}{116} - 3 = -\frac{315}{116} = 5 \cdot \left(-\frac{63}{116}\right). \end{aligned}$$

Celkově pak dostáváme

$$\frac{281}{116} = 1 + 5 \cdot \frac{33}{116} = 1 + 5 \cdot \left(3 + 5 \cdot \left(-\frac{63}{116}\right)\right)$$

a p-adický rozvoj je tvaru

$$\frac{281}{116} = 1 + 3 \cdot 5 + \dots.$$

Dále už p-adický rozvoj není třeba počítat. K dalšímu výpočtu jsou nutné jen koeficienty u členů 5^k pro $k \leq 0$.
Určíme a_0, r_0 a α_1:

$$\begin{aligned} a_0 &= \left\lfloor \frac{281}{116} \right\rfloor_5 = \sum_{i=0}^{0} s_i 5^i = 1, \\ r_0 &= \alpha_0 - a_0 = \frac{281}{116} - 1 = \frac{165}{116}, \\ \alpha_1 &= \frac{1}{r_0} = \frac{116}{165}. \end{aligned}$$

Nyní opět potřebujeme p-adický rozvoj čísla α_1. Postupujeme stejně jako u α_0:

$$\begin{aligned} &\frac{116}{165} = \frac{1}{5} \cdot \frac{116}{33} \\ &\frac{116}{33} \mod 5 = 2 \\ &\frac{116}{33} - 2 = 5 \cdot \frac{10}{33} = 25 \cdot \frac{2}{33}. \end{aligned}$$

Stejný výpočet provedeme pro $\frac{2}{33}$:

$$\begin{aligned}\frac{2}{33} \mod 5 &= 4\\ \frac{2}{33} - 4 = -\frac{130}{33} &= 5 \cdot \left(-\frac{26}{33}\right).\end{aligned}$$

Celkem dostáváme

$$\frac{116}{165} = \frac{1}{5} \cdot \left(2 + 25 \cdot \frac{2}{33}\right) = \frac{1}{5}\left(2 + 25 \cdot \left(4 + 5 \cdot \left(-\frac{26}{33}\right)\right)\right)$$

a p-adický rozvoj je tvaru

$$\frac{116}{165} = 2 \cdot 5^{-1} + 4 \cdot 5 + \dots.$$

Pak můžeme určit a_1, r_1 a α_2:

$$\begin{aligned}a_1 &= \left\lfloor \frac{116}{165} \right\rfloor_5 = \sum_{i=-1}^{0} s_i 5^i = 2 \cdot 5^{-1},\\ r_1 &= \alpha_1 - a_1 = \frac{116}{165} - \frac{2}{5} = \frac{10}{33},\\ \alpha_2 &= \frac{1}{r_2} = \frac{33}{10}.\end{aligned}$$

Určíme p-adický rozvoj α_2:

$$\frac{33}{10} = 4 \cdot 5^{-1} + 3 \cdot 5 + \dots.$$

Můžeme spočítat a_2, r_2 a α_3:

$$\begin{aligned}a_2 &= \left\lfloor \frac{33}{10} \right\rfloor_5 = \sum_{i=-1}^{0} s_i 5^i = 4 \cdot 5^{-1},\\ r_2 &= \alpha_2 - a_2 = \frac{33}{10} - \frac{4}{5} = \frac{5}{2},\\ \alpha_3 &= \frac{1}{r_3} = \frac{2}{5}.\end{aligned}$$

Pak je p-adický rozvoj α_3 roven $2 \cdot 5^{-1}$. Pak

$$\begin{aligned}a_3 &= \left\lfloor \frac{2}{5} \right\rfloor_5 = \frac{2}{5},\\ r_3 &= \alpha_3 - a_3 = \frac{2}{5} - \frac{2}{5} = 0.\end{aligned}$$

Rubanův rozvoj $\frac{281}{116}$ do řetězového zlomku je tedy konečný, je tvaru $1, \frac{2}{5}, \frac{4}{5}, \frac{2}{5}$ a platí $\frac{281}{116} = \left[1, \frac{2}{5}, \frac{4}{5}, \frac{2}{5}\right]$.

K rozhodnutí o konečnosti rozvoje je dle věty 37 potřeba udělat maximálně $\max\{2, \lceil \frac{\log 116}{\log 5} \rceil\} = \lceil \frac{\log 110}{\log 5} \rceil = 3$ kroky. Rozvoj je konečný právě tehdy, když se v některém z těchto kroků ve výpočtu objeví záporné α_i. To v tomto případě nenastalo a jak jsme spočetli, Rubanův rozvoj je opravdu konečný.

Příklad 2. $\alpha = \frac{19}{110}$
Stejně jako v příkladě 1. spočteme Rubanův rozvoj do řetězového zlomku:

$$\alpha = \frac{19}{110} = 2 \cdot 5^{-1} + 2 \cdot 5 + \ldots, \qquad a_0 = \left\lfloor \frac{19}{110} \right\rfloor_5 = 2 \cdot 5^{-1},$$
$$r_0 = \frac{19}{110} - 2 \cdot 5^{-1} = -\frac{5}{22},$$
$$\alpha_1 = -\frac{22}{5} = 3 \cdot 5^{-1} + 4 \cdot 5 + \ldots, \qquad a_1 = \left\lfloor -\frac{22}{5} \right\rfloor_5 = \frac{3}{5},$$
$$r_1 = -\frac{22}{5} - \frac{3}{5} = -5,$$
$$\alpha_2 = -\frac{1}{5} = 4 \cdot 5^{-1} + 4 + 4 \cdot 5 + \ldots, \qquad a_2 = \left\lfloor -\frac{1}{5} \right\rfloor_5 = 4 \cdot 5^{-1} + 4 = \frac{24}{5},$$
$$r_2 = -\frac{1}{5} - \frac{24}{5} = -5,$$
$$\alpha_3 = -\frac{1}{5} = \alpha_2,$$
$$\vdots$$

Rubanův rozvoj čísla $\frac{19}{110}$ do řetězového zlomku je tvaru $\frac{2}{5}, \frac{3}{5}, \frac{24}{5}, \frac{24}{5}, \frac{24}{5}, \ldots$.

K rozhodnutí o konečnosti Rubanova rozvoje (tedy maximální nutný počet kroků, ve kterých ověřujeme, zda se ve výpočtu objevilo záporné α_i) bylo potřeba udělat 2 kroky, což odpovídá větě 37, dle které se záporné α_i objeví nejpozději v kroku $\max\{2, \left\lceil \frac{\log 110}{\log 5} \right\rceil\} = \left\lceil \frac{\log 110}{\log 5} \right\rceil = 3$. Navíc délka předperiodické části je $2 < 32 \cdot 5 \cdot H(\frac{19}{110}) = 160 \cdot 110$.

Příklad 3. $\alpha = \frac{19}{110}$
Spočteme Browkinův rozvoj do řetězového zlomku. Postup výpočtu je stále stejný, jen v tomto případě $s_i \in \{-2, -1, 0, 1, 2\}$:

$$\alpha = \frac{19}{110} = 2 \cdot 5^{-1} + 2 \cdot 5 + \ldots, \qquad b_0 = \left\langle \frac{19}{110} \right\rangle_5 = 2 \cdot 5^{-1},$$
$$r_0 = \frac{19}{110} - 2 \cdot 5^{-1} = -\frac{5}{22},$$
$$\alpha_1 = -\frac{22}{5} = -2 \cdot 5^{-1} + 1 - 1 \cdot 5, \qquad b_1 = \left\langle -\frac{22}{5} \right\rangle_5 = -2 \cdot 5^{-1} + 1 = \frac{3}{5},$$
$$r_1 = -\frac{22}{5} - \frac{3}{5} = -5,$$
$$\alpha_2 = -\frac{1}{5} = -1 \cdot 5^{-1}, \qquad b_2 = \left\langle -\frac{1}{5} \right\rangle_5 = -\frac{1}{5},$$
$$r_2 = -\frac{1}{5} - \frac{-1}{5} = 0.$$

Browkinův rozvoj čísla $\frac{19}{110}$ do řetězového zlomku je tvaru $\frac{2}{5}, \frac{3}{5}, -\frac{1}{5}$ a platí $\frac{19}{110} = \left[\frac{2}{5}, \frac{3}{5}, -\frac{1}{5}\right]$. Můžeme si všimnout, že pro $\alpha = \frac{19}{110}$ je Browkinův rozvoj konečný, kdežto rozvoj Rubanův je periodický.

Příklad 4. $\alpha = \frac{701}{255}$

Nejprve spočteme Rubanův rozvoj do řetězového zlomku:

$$\begin{aligned}
\alpha &= \frac{701}{255} = 1\cdot 5^{-1} + 1\cdot 5 + \ldots, & a_0 &= \left\lfloor \frac{701}{255} \right\rfloor_5 = \frac{1}{5},\\
r_0 &= \frac{701}{255} - 1\cdot 5^{-1} = \frac{130}{51},\\
\alpha_1 &= \frac{51}{130} = 1\cdot 5^{-1} + 1\cdot 5 + \ldots, & a_1 &= \left\lfloor \frac{51}{130} \right\rfloor_5 = \frac{1}{5},\\
r_1 &= \frac{51}{130} - \frac{1}{5} = \frac{5}{26},\\
\alpha_2 &= \frac{26}{5} = 1\cdot 5^{-1} + 1\cdot 5, & a_2 &= \left\lfloor \frac{26}{5} \right\rfloor_5 = \frac{1}{5},\\
r_2 &= \frac{26}{5} - \frac{1}{5} = 5,\\
\alpha_3 &= \frac{1}{5} = 1\cdot 5^{-1}, & a_3 &= \left\lfloor \frac{1}{5} \right\rfloor_5 = \frac{1}{5},\\
r_3 &= \frac{1}{5} - \frac{1}{5} = 0.
\end{aligned}$$

Rubanův rozvoj čísla $\frac{701}{255}$ do řetězového zlomku je tvaru $\frac{1}{5}, \frac{1}{5}, \frac{1}{5}, \frac{1}{5}$ a platí $\frac{701}{255} = \left[\frac{1}{5}, \frac{1}{5}, \frac{1}{5}, \frac{1}{5}\right]$. Můžeme si všimnout, že všechny počátky p-adických rozvojů budou stejné i pro Browkinův rozvoj. Tedy platí

$$\begin{aligned}
b_0 &= \left\langle \frac{701}{255} \right\rangle_5 = \frac{1}{5},\\
b_1 &= \left\langle \frac{51}{130} \right\rangle_5 = \frac{1}{5},\\
b_2 &= \left\langle \frac{26}{5} \right\rangle_5 = \frac{1}{5},\\
b_3 &= \left\langle \frac{1}{5} \right\rangle_5 = \frac{1}{5},
\end{aligned}$$

a Browkinův rozvoj je stejný jako rozvoj Rubanův.

Závěr

V této práci byla popsaná teorie potřebná k zavedení p-adických čísel a rozvojů do řetězových zlomků. Zaměřili jsme se na rozvoje Rubanův a Browkinův. Dokázali jsme, že v $\mathbb{Q}_p$ Rubanův rozvoj konverguje pro libovolné p-adické číslo, a tedy všechna $\alpha \in \mathbb{Q}_p$ lze jako Rubanův rozvoj do řetězového zlomku vyjádřit. Oproti tomu v $\mathbb{R}$ Rubanův rozvoj do řetězového zlomku $[a_0,a_1,\dots]$ konverguje právě tehdy, když $\sum_{i=1}^{\infty} a_i = \infty$, což je ekvivalentní tomu, že q_i jsou neomezené. $\frac{p_i}{q_i}$ jsou v tomto případě konvergenty řetězového zlomku.

Dále pro Rubanův rozvoj nezáporného čísla $\alpha \in \mathbb{Q}$ neplatí ohledně konečnosti totéž, co pro řetězové zlomky v reálných číslech. Ukázali jsme, že rozhodnout, zda je příslušný Rubanův rozvoj do řetězového zlomku konečný, lze algoritmicky v konečném počtu kroků. Algoritmus spočívá v tom, že v každém kroku spočteme α_i a ověříme, zda je nezáporné. Rubanův rozvoj je pak nekonečný právě tehdy, když je libovolné α_i záporné. Těchto kroků stačí udělat $\max\{2, \lceil \frac{\log b}{\log p} \rceil\}$, kde $\alpha = \frac{a}{b}$ pro $a, b \in \mathbb{Z}$ takové, že $gcd(a, b) = 1$. Pro Rubanův rozvoj dále platí, že je-li nekonečný, pak je periodický s délkou periody 1 a všechny členy periody jsou rovny $p - p^{-1}$. Předperiodickou část lze navíc spočítat efektivně - její délka je omezena hodnotou $H(\alpha)2p$, kde $H(\alpha)$ je multiplikativní výška.

Dokázali jsme také, že oproti tomu Browkinův rozvoj do řetězového zlomku pro racionální čísla konečnost zachovává.

Dále je možné studovat řetězové rozvoje $\sqrt{m}, m \in \mathbb{N}$. Například Lagrangerova věta říká, že v reálných číslech má každé reálné číslo nekonečný periodický řetězový zlomek právě tehdy, když se jedná o algebraické číslo stupně 2 (Hardy a kol. (2008), Věta 177). V p-adických číslech toto ovšem neplatí. Pro Rubanův i Browkinův rozvoj platí jen jisté podobnosti (více informací lze nalézt v článku Capuano a kol. (Capuano a kol. (2019)) nebo článku Browkina (Browkin (2001))). Problém rozhodnout, zda je rozvoj p-adického algebraického čísla stupně 2 do řetězového zlomku periodický, se zdá být stále otevřený.

V současně době neexistuje standardní algoritmus pro zavedení řetězových zlomků v tělese p-adických čísel. Vlastnosti mnoha rozvojů se liší ať už konečností nebo periodicitou. Není proto snadné určit, který rozvoj je nejvhodnější k zachování co nejvíce vlastností jako v reálných číslech.

Seznam použité literatury

Baker, A. An Introduction to p-adic Numbers and p-adic Analysis. School of Mathematics & Statistics, University of Glasgow, Glasgow G12 8QQ, Scotland, pages 15-27, URL: `https://web.archive.org/web/20161213093839/http://www.maths.gla.ac.uk/~ajb/dvi-ps/padicnotes.pdf`, Last visited on 28/03/2023,.

Bombieri, E. (2007 - 2006). *Heights in diophantine geometry*. New mathematical monographs ; 4. Cambridge University Press, Cambridge, reprinted with corrections edition. ISBN 978-0-521-71229-3.

Browkin, J. (1978). Continued fractions in local fields, I. *Demonstratio Mathematica*, **XI**, 67–82.

Browkin, J. (2001). Continued fractions in local fields, ii. *Mathematics of computation*, **70**(235), 1281–1292. ISSN 0025-5718.

Capuano, L., Veneziano, F. a Zannier, U. (2019). An effective criterion for periodicity of ℓ-adic continued fractions. *Mathematics of computation*, **88** (318), 1851–1861. ISSN 0025-5718.

Hardy, G., Wright, E., Heath-Brown, D., Heath-Brown, R., Silverman, J. a Wiles, A. (2008). *An Introduction to the Theory of Numbers*. Oxford mathematics. OUP Oxford. ISBN 9780199219865.

Ruban, A. A. (1970). Some metric properties of p-adic numbers. *Siberian Mathematical Journal*, **11**(1), 176–180. ISSN 1573-9260. doi: 10.1007/BF00970247. URL `https://doi.org/10.1007/BF00970247`.