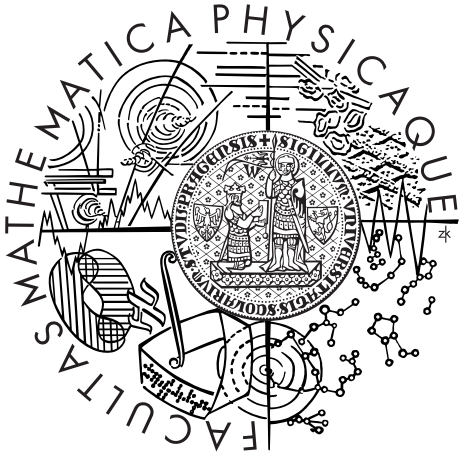
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

**BAKALÁŘSKÁ PRÁCE**




Richard Dubiel

# p-adická čísla

Katedra algebry

Vedoucí bakalářské práce: Mgr. Jan Šťovíček, Ph.D.

Studijní program: Matematika
Studijní obor: obecná matematika

Praha 2013

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

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 v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne .....  Podpis autora

Název práce: p-adická čísla

Autor: Richard Dubiel

Katedra: Katedra algebry

Vedoucí bakalářské práce: Mgr. Jan Šťovíček, Ph.D.

Abstrakt: Tato práce se zabývá konstrukcí tělesa p-adických čísel, jako zúplnění tělesa čísel racionálních a následně představí některé důležité vlastnosti tohoto tělesa. Představí pojmy absolutní hodnoty, metriky, ultrametriky a zúplnění tělesa vzhledem k absolutní hodnotě. Následně zavedeme speciální p-adickou absolutní hodnotu a metriku - takovou, která měří, „jak moc"je dané číslo dělitelné prvočíslem $p$. Skonstruujeme zúplnění tělesa racionálních čísel vzhledem k takové absolutní hodnotě - těleso p-adických čísel. Uvedeme, jak je možno tato čísla reprezentovat. Na závěr představíme dva z nejdůležitějších výsledku teorie p-adických čísel - Henselovo lemma a Hasse-Minkowského větu.

Klíčová slova: absolutní hodnota, zúplnění těles, dělitelnost, prvočísla

Title: p-Adic numbers

Author: Richard Dubiel

Department: Department of Algebra

Supervisor: Mgr. Jan Šťovíček, Ph.D.

Abstract: This thesis deals with construction of the field of p-adic numbers as a completion of rational numbers field and introduces several important properties of this field. It will introduce concepts of an absolute value, metric, ultrametric and completion of field with respect to absolute value. Then we introduce a p-adic absolute value - one that measures "how much" is a number divisible by a prime number $p$. Then we construct the completion of the field of rational numbers with respect to this absolute value - field of p-adic numbers. We show, how can one represent these numbers. At last, we introduce two of the most important results of the theory of p-adic numbers - Hensel lemma and Hasse-Minkowski theorem.

Keywords: absolute value, completion of fields, divisibility, prime numbers

Názov práce: p-adické čísla

Autor: Richard Dubiel

Katedra: Katedra algebry

Vedúci bakalárskej práce: Mgr. Jan Šťovíček, Ph.D.

Abstrakt: Táto práca sa zameriava na konštrukciu telesa p-adických čísel, ako zúplnenia telesa čísel racionálnych a následne predstaví niektoré dôležité vlastnosti tohoto telesa. Predstaví pojmy absolútnej hodnoty, metriky, ultrametriky a zúplnenia telesa vzhľadom k absolútnej hodnote. Následne zavedieme špeciálnu p-adickú absolútnu hodnotu a metriku - takú, ktorá meria, „ako veľmi"je dané číslo deliteľné prvočíslom $p$. Skonštruujeme zúplnenie telesa racionálnych čísel vzhľadom k tejto absolútnej hodnote - teleso p-adických čísel. Uvedieme, ako je tieto čísla možné reprezentovať. Na záver predstavíme dva z najdôležitejších výsledkov teórie p-adických čísel - Henselovo lemma a Hasse-Minkowského vetu.

Kľúčové slová: absolútna hodnota, zúplnenie telies, delitelnosť, prvočísla

# Obsah

# Kapitola 1

# Úvod

Pojmy ako absolútna hodnota, teleso úplne vzhľadom k danej absolútnej hodnote, prípadne zúplnenie neúplého telesa vzľadom k danej absolútnej hodnote sú známe zo základného kurzu matematickej analýzy. Tam sa môžeme stretnúť s telesom čísel racionálnych a jeho zúplnením vzhľadom k štandardnej absolútnej hodnote - číslami reálnymi. Ak hovoríme štandardná absolútna hodnota, myslíme tým takú, ktorá meria „vzdialenosť" od nuly. To ale nie je jediná absolútna hodnota, ktorú je možné zaviesť na racionálnych číslach, a reálne čísla nie sú ich jediné možné zúplnenie - a presne to je predmetom tejto práce. Ukážeme si, že na racionálnych číslach sa dá zaviesť úplne iná absolútna hodnota, než na akú sme „zvyknutí" - taká, ktorá meria, „ako veľmi"je dané racionálne číslo deliteľné nejakým pevne zvoleným prvočíslom. Následne skonštruujeme zúplnenie racionálnych čísel vzľadom k tejto nami zadefinovanej absolútnej hodnote - tzv. p-adické čísla, ktoré sa, ako uvidíme, od čísel reálnych v mnohom líšia. Ukážeme si aj niektoré vlastnosti tohto úplného telesa, ale väčšia časť tejto práce sa sústredí na jeho konštrukciu.

P-adické čísla boli prvýkrat popísané Kurtom Henselom v roku 1897 v snahe zapracovať do teórie čísel techniky používané pri práci s mocninnými radami. Jedná sa o silný nástroj, ktorý napríklad použil aj Andrew Wiles pri dokazovaní Veľkej Fermatovej vety. V súčasnosti sa využívajú napr. ako nástroj pri kryptografii eliptickými krivkami, alebo v tzv. p-adickej kvantovej mechanike - modernom prístupe k snahe porozumieť fundamentálnej fyzike.

# Kapitola 2

# Ochutnávka

Celý nasledujúci text, ak nie je uvedené inak, nasleduje knihu Fernanda Q. Gouveu - *p-adic Numbers: an Introduction*, uvádza dôkazy v podobe, v akej sú uvedené v tejto knihe, prípadne ponúka riešenie tzv. Problems - spravidla dôkazov pomocných tvrdení a viet, ktoré sú v spomínanej knihe prenechané na čitateľa. Predmetom tejto práce sú takzvané p-adické čísla - ich podrobnú a matematicky korektnú konštrukciu si ukážeme v nasledujúcej kapitole, spolu s niektorými významnými vlastnosťami tejto štruktúry. Na začiatok si teda neformálne ukážeme, čo si môžeme pod týmto pojmom predstaviť a k čomu celá práca smeruje.

Vieme, že ľubovoľné prirodzené číslo $m$ vieme zapísať „v bázi $p$", $p$ uvažujeme ľubovoľné prvočíslo:

$$m = a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n,$$

kde $a_i \in \mathbb{Z}$, $0 \leq a_i \leq p-1$ pre všetky $i = 1, \ldots, n$. Napríklad pre $m = 65$ a $p = 3$ máme:

$$65 = 2 + 0 \times 3 + 1 \times 3^2 + 2 \times 3^3$$

Skúsme teraz, čisto formálne, prejsť od kladných celých čísel ku kladným racionálnym. Budeme postupovať nasledovne: majme racionálne číslo $r = \frac{a}{b}$, kde $a, b$ sú kladné celé čísla. Aj menovateľ zapíšeme v bázi $p$, ako sme si ukázali vyššie a následne tieto výrazy formálne vydelíme. Priblížme si to na príklade:

$$p = 5$$

$$a = 9 = 4 + p$$

$$b = 17 = 2 + 3p$$

Máme teda:

$$\frac{9}{17} = \frac{4+p}{2+3p},$$

a po formálnom vydelení dostávame:

$$\frac{9}{17} = \frac{4+p}{2+3p} = 2 + 2p^2 + 4p^3 + p^5 + 3p^6 + \cdots$$

Správnosť výsledku overíme - jednoducho ho prenásobíme p-rozvojom čísla 17, a ak je všetko v poriadku, potom by sme mali dostať práve p-rozvoj čísla 9.

$$(2+3p)(2+2p^2+4p^3+p^5+3p^6+\cdots=$$

$$=4+\underbrace{6p}_{=p+5p=p+p^2}+4p^2+6p^3+8p^3+12p^4+2p^5+3p^6+6p^6+9p^7+\cdots$$

$$=4+p+\underbrace{p^2+4p^2}_{=5p^2=p^3}+6p^3+8p^3+12p^4+2p^5+3p^6+6p^6+9p^7+\cdots$$

$$=4+p+\underbrace{p^3+6p^3+8p^3}_{=15p^3=3p^4}+12p^4+2p^5+3p^6+6p^6+9p^7+\cdots$$

$$=4+p+\underbrace{3p^4+12p^4}_{=15p^4=3p^5}+2p^5+3p^6+6p^6+9p^7+\cdots$$

$$=4+p+\underbrace{3p^5+2p^5}_{=5p^5=p^6}+3p^6+6p^6+9p^7+\cdots$$

$$=4+p+\underbrace{p^6+3p^6+6p^6}_{=10p^6=2p^7}+9p^7+\cdots$$

$$\vdots$$

$$=4+p,$$

Ako teda vidíme, všetky mocniny $p$ vyššie ako 2, nám „miznú doprava". Ostáva nám

$$4+p=9.$$

Chceli by sme ešte týmto p-rozvojom vedieť zapísať aj záporné racionálne čísla.

K tomu nám ale stačí nájsť p-rozvoj čísla -1, pretože mocninné rady s p, s ktorými tu formálne pracujeme, môžeme bez problémov medzi sebou násobiť.
Všimnime si, že:

$$\underbrace{1+(p-1)}_{=p}+(p-1)p+(p-1)p^2+(p-1)p^3+\cdots=$$

$$= \underbrace{p + (p-1)p}_{=p^2} + (p-1)p^2 + (p-1)p^3 + \cdots =$$

$$= \underbrace{p^2 + (p-1)p^2}_{=p^3} + (p-1)p^3 + \cdots =$$

$$\vdots$$

$$= 0$$

Dostávame tak hľadaný p-rozvoj čísla -1:

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + (p-1)p^3 + \cdots$$

Teraz už vieme zapísať ľubovoľné racionálne číslo $x$ v tvare

$$x = \sum_{n \geq n_0} a_n p^n,$$

kde $n_0$ je celé číslo. (Presnejšie: $n_0$ je práve číslo spĺňajúce:

$$x = p^{n_0} \frac{a'}{b'},$$

kde $p \nmid a'$ a $p \nmid b'$. ) Takýto zápis čísla $x$ budeme nazývať (zatiaľ nič nedefinujeme - pripomínam, že s mocninnými radami zatiaľ pracujeme iba formálne) *p-adický rozvoj x.*

Nie je ťažké ukázať, že množina všetkých mocninných rád tvaru

$$\sum_{n \geq n_0} a_n p^n,$$

spolu s operáciami ich násobenia a sčítania, tvorí teleso.
Toto teleso označíme $\mathbb{Q}_p$ a nazveme ho *teleso p-adických čísel.*
V nasledujúcej kapitole pristúpime k tejto problematike poctivejšie: zadefinujeme

na telese $\mathbb{Q}$ absolútnu hodnotu (odlišnú od štandardnej, na akú sme zvyknutí), ňou indukovanú metriku a následne skonštruujeme teleso $\mathbb{Q}_p$ ako zúplnenie $\mathbb{Q}$ vzhľadom k nami zadefinovanej absolútnej hodnote.

# Kapitola 3

# Teoretická príprava

## 3.1 P-valuácia. P-adická absolútna hodnota.

Dobre poznáme absolútnu hodnotu na $\mathbb{R}$, resp. $\mathbb{Q}$, ktorá meria „vzdialenosť od 0", a taktiež vieme, že $\mathbb{R}$ je zúplnením $\mathbb{Q}$ vzhľadom k metrike indukovanej touto absolútnou hodnotou (tzn., že $\mathbb{R}$ je úplný vzľadom k tejto metrike v zmysle, že každá Cauchyovská postupnosť prvkov z $\mathbb{R}$ má taktiež limitu v $\mathbb{R}$ a $\mathbb{R}$ obsahuje $\mathbb{Q}$ ako hustú podmnožinu).

My si na začiatok na $\mathbb{Q}$ zavedieme novú absolútnu hodnotu - narozdiel od vyššie spomínanej, táto nová absolútna hodnota bude merať, „ako veľmi je dané čislo deliteľné prvočíslom $p$", pre $p$ ľubovoľné, pevne zvolené.

**Definícia 3.1.1.** *Nech* $\mathbf{F}$ *je teleso. Absolútna hodnota na* $\mathbf{F}$ *je funkcia*

$$|\ \ | : \mathbf{F} \longrightarrow [0, \infty),$$

*spĺňajúca:*

*i)* $|x| = 0$ *vtedy a len vtedy, ak* $x = 0$

*ii)* $|xy| = |x||y|$ *pre všetky* $x, y \in \mathbf{F}$

*iii)* $|x + y| \leq |x| + |y|$ *pre všetky* $x, y \in \mathbf{F}$

*Absolútnu hodnotu nazveme nearchimedovskou, ak spĺňa silnejšiu podmienku*

*iv)* $|x + y| \leq max\{|x|, |y|\}$ *pre všetky* $x, y \in \mathbf{F}$

*V opačnom prípade hovoríme o archimedovskej absolútnej hodnote.*

Vidíme, že podmienka *iv)* implikuje podmienku *iii).*

**Definícia 3.1.2.** *Pre pevne zvolené prvočíslo $p$ a $a \in \mathbb{Z} \setminus 0$ definujeme p-valuáciu čísla $a$ ako:*

$$v_p(a) = max\,\{r \in \mathbb{N} \cup \{0\} : p^r \mid a\}$$

*Pre nenulové racionálne číslo $\frac{a}{b}$ potom definujeme jeho p-valuáciu ako*

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b).$$

*Nakoniec položíme*

$$v_p(0) = \infty.$$

**Lemma 3.1.3.** *Nech $x, y \in \mathbb{Q}$. Potom $v_p$ má nasledujúce vlastnosti:*

1. *$v_p(x) = \infty$ vtedy a len vtedy, ak $x = 0$*
2. *$v_p(xy) = v_p(x) + v_p(y)$*
3. *$v_p(x + y) \geq min\,\{v_p(x), v_p(y)\}$.*

*Dôkaz.*
1) Implikácia sprava doľava je priamo definíciou p-valuácie pre $x = 0$. Naopak, ak $v_p(x) = \infty$. pre nejaké $x = \frac{a}{b}$, potom iste musí platiť $v_p(a) = \infty$., čo žiadne nenulové prirodzené číslo nesplňuje - teda nutne $a = 0$.
2) Majme nenulové racionálne čísla $x, y$, pre ktoré platí $v_p(x) = n, v_p(y) = m$, potom $x = p^n \frac{a}{b}, y = p^m \frac{c}{d}$ pre nejaké $a, b, c, d$ celé, také, že $p \nmid abcd$ (teda $p$ nedelí $a, b, c,$ ani $d$). Potom

$$v_p(xy) = v_p(p^n\,\frac{a}{b}\,p^m\,\frac{c}{d}) = v_p(p^{m+n}\frac{ac}{bd}) = n + m = v_p(x) + v_p(y).$$

3) Opäť majme nenulové racionálne čísla $x, y$, $x = p^n \frac{a}{b}, y = p^m \frac{c}{d}$, $p \nmid abcd$. Najprv ak $n = m$, dostávame:

$$x + y = p^n\,\left(\frac{a}{b} + \frac{c}{d}\right) = p^n\,\frac{ad + bc}{bd},$$

a keďže $p \nmid bd$, dostávame $v_p(x + y) \geq n$.

Teraz nech $n \neq m$, BÚNO $m > n$. Potom

$$x + y = p^n\left(\frac{a}{b} + p^{m-n}\frac{c}{d}\right)$$

$$= p^n\,\frac{ad + p^{m-n}bc}{bd},$$

a keďže $m - n > 0$ a $p \nmid ad$, dostávame, že

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

□

**Definícia 3.1.4.** *Pre ľubovoľné nenulové $x \in \mathbb{Q}$ definujeme jeho p-adickú absolútnu hodnotu nasledovne:*

$$|x|_p = p^{-v_p(x)}.$$

*Navyše položíme*

$$|0|_p = 0.$$

**Tvrdenie 3.1.5.** *Funkcia $|\ |_p$ je nearchimedovská absolútna hodnota na $\mathbb{Q}$.*

*Dôkaz.*
Správnosť tvrdenia okamžite plynie z Lemmy 3.1.3.

□

## 3.2 Metrika, ultrametrika. Princíp rovnoramennosti trojuholníkov.

**Definícia 3.2.1.** *Nech $X$ je množina, metrikou nazveme funkciu*

$$\rho : X \times X \longrightarrow \mathbb{R},$$

*spĺňajúcu pre všetky $x, y, z \in X$.:*

1. $\rho(x, y) \geq 0$
2. $\rho(x, y) = 0$ *práve vtedy, keď* $x = y$
3. $\rho(x, y) = \rho(y, x)$
4. $\rho(x, z) \leq \rho(x, y) + \rho(y, z)$

*Navyše $\rho$ nazveme ultrametrikou, ak namiesto podmienky* 4)*, spĺňa silnejšiu podmienku:*
*Pre všetky $x, y, z \in X$,*

$$\rho(x, z) \leq max\,\{\rho(x, y), \rho(y, z)\}.$$

**Definícia 3.2.2.** *Nech* $\mathbf{F}$ *je teleso a $|\ \ |$ je absolútna hodnota na* $\mathbf{F}$*. Definujeme vzdialenosť medzi dvoma prvkami $x, y \in \mathbf{F}$ ako*

$$d(x, y) = |x - y|.$$

.

**Veta 3.2.3.** *Nech* $|\ \ |$ *je nearchimedovská absolútna hodnota na telese* $\mathbf{F}$*. Potom funkcia* $d(x, y)$ *je ultrametrika.*

*Dôkaz.*
Vlastnosti 1. a 2. z definície metriky plynú bezprostredne z definície absolútnej hodnoty.
Ďalej si všimnime, že platí:

$$|1| = |1^2| = |1 \times 1| = |1||1| = |1|^2,$$

pričom jediné pozitívne reálne číslo, ktoré toto spĺňa (tj. že pre $a$ platí: $a = a^2$), je číslo 1, a teda musí platiť, že $|1| = 1$.
Ďalej si všimnime, že

$$1 = |1| = |(-1)(-1)| = |-1||-1|,$$

a rovnako, ako v predchádzajúcej úvahe, dostávame, že $|-1| = 1$. (vďaka tomu, že absolútna hodnota je nezáporné číslo.)
Teraz už nám nič nebráni ukázať, že pre ľubovoľné $x \in \mathbf{F}$ platí :

$$|-x| = |(-1)x| = |-1||x| = |x|,$$

čo nám okamžite dáva platnosť 3. vlastnosti z definície metriky. Nakoniec použijeme vlastnosť nearchimedovskej absolútnej hodnoty $|x + y| \leq \max\{|x|, |y|\}$ na rovnosť $(x - y) = (x - z) + (z - y)$:

$$|x - y| \leq max\,\{|x - z|, |z - y|\},$$

a teda $d(x, y)$ je skutočne ultrametrika. Takúto metriku (resp. ultrametriku) nazývame metrika (resp. ultrametrika) indukovaná absolútnou hodnotou.

□

**Tvrdenie 3.2.4.** *V ultrametrickom priestore (tj. na množine s ultrametrikou) platí takzvaný princíp rovnoramennosti trojuholníkov, tj. že každý „trojuholník"je v tomto priestore rovoramenný.*

*Dôkaz.*
Majme tri body $x, y, z$ - vrcholy nášho trojuholníka v ultrametrickom priestore s ultrametrikou $\rho$. Z definície ultrametriky vidíme že:

$$\rho(x, y) \leq max\{\rho(x, z), \rho(z, y)\}.$$

Bez újmy na obecnosti, nech je $\rho(x, z) > \rho(z, y)$ (v prípade, že $\rho(x, z) = \rho(z, y)$ už máme rovnoramenný trojuholník). Teda $\rho(x, y) \leq \rho(x, z)$. Zároveň ale musí platiť, že

$$\rho(x, z) \leq max\{\rho(x, y), \rho(y, z)\}.$$

Predpokladali sme $\rho(x, z) > \rho(z, y)$, takže nutne musí už byť $\rho(x, z) \leq \rho(x, y)$, takže dostávame rovnosť

$$\rho(x, y) = \rho(x, z).$$

Obecne teda platí, že ak $\rho(x,z) \neq \rho(z,y)$, potom nutne

$$\rho(x,y) = max\{\rho(x,z), \rho(z,y)\},$$

čiže každý trojuholník v ultrametrickom priestore je skutočne rovnoramenný.

□

P-adická absolútna hodnota je, ako sme ukázali, nearchimedovská, a teda je ňou indukovaná metrika samozrejme ultrametrikou, takže práve dokázaný princíp rovnoramennosti trojuholníkov je v priestore s p-adickou metrikou v platnosti, čo neskôr využijeme.

## 3.3 Zúplnenie telies.

Pripomenieme si pojmy Cauchyovskej postupnosti, úplného telesa a hustej podmnožiny - jedná sa o obdoby daných pojmov, ako ich poznáme zo základného kurzu analýzy, rozdiel spočíva len v tom, že pracujeme s telesom, nie obecným metrickým priestorom (tj. obecnou množinou a na nej zavedenou metrikou). Potom už budeme pripravený zostrojiť teleso p-adických čísel $\mathbb{Q}_p$.

**Definícia 3.3.1.** *Hovoríme, že postupnosť $(a_n)$ prvkov telesa $\mathbf{F}$ má limitu $a \in \mathbf{F}$ vzhľadom k absolútnej hodnote $|\ |$, ak platí*

$$\forall \epsilon > 0\ \exists n_0 \in \mathbb{N} : \forall n \geq n_0 \text{ platí, že } |a - a_n| < \epsilon.$$

**Definícia 3.3.2.** *Hovoríme, že postupnosť $(a_n)$ prvkov telesa $\mathbf{F}$ je cauchyovská vzhľadom k absolútnej hodnote $|\ |$, ak platí*

$$\forall \epsilon > 0\ \exists n_0 \in \mathbb{N} : \forall m, n \geq n_0 \text{ platí, že } |a_m - a_n| < \epsilon.$$

**Definícia 3.3.3.** *Hovoríme, že teleso $\mathbf{F}$ je úplné vzhľadom k absolútnej hodnote $|\ |$, ak každá cauchyovská postupnosť prvkov $\mathbf{F}$ má limitu v $\mathbf{F}$ vzhľadom k $|\ |$.*

**Definícia 3.3.4.** *Hovoríme, že $\mathbf{S} \subset \mathbf{F}$ je hustá v $\mathbf{F}$ vzhľadom k absolútnej hodnote $|\ |$ , ak*

$$\forall \epsilon > 0 \forall x \in \mathbb{F} : \ \ \mathbf{B}(x,\epsilon) \cap S \neq \emptyset,$$

*kde $\mathbf{B}(x,\epsilon)$ je otvorená guľa o polomere $\epsilon$ so stredom v $x$, tj.*

$$\mathbf{B}(x,\epsilon) = \{a \in \mathbf{F} : \ |a - x| < \epsilon\}.$$

Teraz si už môžeme riadne zadefinovať zúplnenie telesa vzhľadom k danej absolútnej hodnote, (resp. vzľadom k metrike ňou indukovanej).

**Definícia 3.3.5.** *Nech* $\mathbf{A}, \mathbf{B}$ *sú telesá,* $|\ |$ *je absolútna hodnota na* $\mathbf{A}$ *a existuje vnorenie* $\mathbf{A} \hookrightarrow \mathbf{B}$ *spĺňajúce nasledujúce podmienky:*

- *abolútna hodnota sa dá rozšíriť na* $\mathbf{B}$
- $\mathbf{B}$ *je úplné vzhľadom k absolútnej hodnote* $|\ |$ *(resp. vzhľadom k metrike ňou indukovanej)*
- $\mathbf{A}$ *je hustá v* $\mathbf{B}$ *(vzľadom k* $|\ |$ *),*

*potom* $\mathbf{B}$ *nazveme zúplnenie telesa* $\mathbf{A}$*.*

Zo základného kurzu analýzy vieme, že v tomto zmysle je $\mathbb{R}$ teleso reálnych čísel zúplnením $\mathbb{Q}$ vzhľadom k štandartnej metrike. Naším cieľom je zostrojiť zúplnenie vzhľadom k p-adickej metrike, danej p-adickou absolútnou hodnotou, pre ľubovoľné prvočíslo $p$. Najprv si teda ukážeme, že $\mathbb{Q}$ skutočne nie je vzhľadom k $|\ |_p$ úplné (a teda že naša snaha nie je zbytočná).

**Lemma 3.3.6.** *Postupnosť* $(x_n)$ *čísel z* $\mathbb{Q}$ *je cauchyovská vzhľadom k nearchimedovskej absolútnej hodnote* $|\ |$ *práve vtedy, keď platí*

$$lim_{n\to\infty}|x_{n+1} - x_n| = 0.$$

*Dôkaz.*

Pre $m = n + k$ dostávame:

$$|x_m - x_n| = |x_{n+k} - x_{n+k-1} + x_{n+k-1} + \cdots + x_{n+1} - x_n|,$$

a keďže ide o nearchimedovskú normu, dostávame

$$|x_m - x_n| \leq max\,\{|x_{n+k} - x_{n+k-1}|, |x_{n+k-1} - x_{n+k-2}|, \ldots, |x_{n+1} - x_n|\},$$

čo nám dáva správnosť tvrdenia.

□

**Veta 3.3.7.** *Teleso racionálnych čísel* $\mathbb{Q}$ *nie je úplné vzhľadom k absolútnej hodnote* $|\ |_p$ *pre žiadne prvočíslo* $p$*.*

*Dôkaz.*

Vetu dokážeme zvlášť pre nepárne prvočísla a pre $p = 2$. Najprv nech $p$ je nepárne prvočíslo. Skonštruujeme cauchyovskú postupnosť racionálnych čísel, ktorá ale v racionálnych číslach nebude mať limitu. Zvoľme najprv celé číslo $a$ také, že $a$ nie je štvorcom v $\mathbb{Q}$, súčasne nie je deliteľné prvočíslom $p$ a kongruencia $X^2 \equiv a \ (mod\ p)$ má riešenie (tomu sa hovorí aj, že $a$ je kvadratický zvyšok modulo $p$). Také $a$ iste existuje - stačí napríklad vziať nejaký štvorec v celých číslach, a pripočítať/odpočítať vhodný násobok čísla $p$. Teraz skonštruujeme nasledovnú postupnosť $(x_n)$: Položíme $x_0$ rovné nejakému riešeniu kongruencie, ktorú sme uviedli, tzn. bude platiť, že

$$x_0^2 \equiv a \ (mod\ p).$$

Následne zvolíme $x_1$ také, že $x_1 \equiv x_0 \ (mod\ p)$ a zároveň $x_1^2 \equiv a \ (mod\ p^2)$. Obecne v $n$-tom kroku volíme $x_n$ pre ktoré platí:

$$x_n \equiv x_{n-1} \ (mod\ p^n),$$

a zároveň

$$x_n^2 \equiv a \ (mod\ p^{n+1}).$$

Nahliadnime ešte, že takéto $x_n$ vieme vždy nájsť. Ak položíme $x_n = x_{n-1} + kp^n$, potom prvá podmienka je iste splnená. Druhú podmienku si teraz prepíšeme ako

$$(x_{n-1} + kp^n)^2 \equiv a \ (mod\ p^{n+1}).$$

Po umocnení zátvorky môžeme posledný člen ignorovať, keďže $p$ v ňom figuruje v mocnine $2n$ a teda modulo $p^{n+1}$ nezohráva žiadnu rolu. Dostávame tak

$$x_{n-1}^2 + 2x_{n-1}kp^n \equiv a \ (mod\ p^{n+1}).$$

Vieme ale, že $x_{n-1}^2$ je modulo $p^n$ rovné $a$, inak povedané $x_{n-1}^2 - a = lp^n$ pre nejaké $l$, takže po odčítaní $x_{n-1}$ na oboch stranách môžeme celú kongruenciu predeliť $p^n$, čím dostaneme

$$2x_{n-1}k \equiv -l \ (mod\ p).$$

Avšak vieme, že $p \neq 2$, takže $p$ nedelí $2x_{n-1}$ (všimnime si, ako sme volili čísla $(x_n)$), takže nech je $l$ akékoľvek, vždy vieme nájsť $k$ také, aby kongruencia bola splnená.

Teraz si všimnime, že

$$|x_{n+1} - x_n|_p = |kp^{n+1}|_p \leq p^{-(n+1)},$$

a teda podľa predchádzajúcej Lemmy 3.3.6 je nami skonštruovaná postupnosť skutočne cauchyovská. Zároveň ale

$$|x_n^2 - a|_p = |lp^{n+1}|_p \leq p^{-(n+1)},$$

takže limita postupnosti, ak existuje, musí byť rovná odmocnine z $a$, to ale nie je štvorcom v $\mathbb{Q}$, takže sme našli cauchyovskú postupnosť prvkov $\mathbb{Q}$, ktorá v $\mathbb{Q}$

nemá limitu, čo je presne to, čo sme chceli.

V prípade, že $p = 2$ použijeme rovnaký postup, s tým rozdielom, že budeme chcieť, aby $x_0^3 \equiv 3 \ (mod\ 2)$ (takže napr. $x_0 = 1$) a požadujeme, aby pre člen $x_n$ platila pozmenená podmienka $x_n^3 \equiv 3 \ (mod\ 2^{n+1})$. Ten potom volíme ako

$$x_n = x_{n-1} + 2^n,$$

potom po dosadení do podmienky a „odignorovaní" príliš vysokých mocnín čísla 2 dostávame

$$3x_{n-1}^2 k \equiv -l \ (mod\ 2),$$

a iste nie je problém položiť $k$ tak aby bola kongruencia splnená. Obdobne ako v predchádzajúcom prípade potom dostávame, že limita takejto postupnosti, ak existuje, by musela byť rovná tretej odmocnine z čísla 3, ktorú ale v racionálnych číslach nenájdeme.

□

# Kapitola 4

# Konštrukcia $\mathbb{Q}_p$

## 4.1 Od $\mathbb{Q}$ ku $\mathbb{Q}_p$

Konečne môžeme pristúpiť k samotnej konštrukcii zúplnenia. Ako sme si už viackrát povedali, potrebujeme, aby každá cauchyovská postupnosť v $\mathbb{Q}$ mala v tomto zúplnení limitu. Limity, ktoré nám v $\mathbb{Q}$ „chýbajú", nahradíme samotnými postupnosťami. Problém je, že dve postupnosti, ktoré „by mali mať"rovnakú limitu (intuitívne môžeme chápať tak, že ich „rozdiel"konverguje k 0), budú stále dvoma rôznymi objektami. Všetky takéto postupnosti preto stotožníme. Tomu zodpovedá konštrukcia faktorového okruhu všetkých cauchyovských (vzhľadom k p-adickej metrike) postupností racionálnych čísel, podľa jeho ideálu tvoreného postupnosťami s nulovou limitou.

**Definícia 4.1.1.** *Buď $\mathbb{Q}$ teleso racionálnych čísel a $|\ |_p$ p-adická absolútna hodnota. Označíme*

$$\mathbf{CP} = \mathbf{CP}_p(\mathbb{Q}) = \{(x_n) : \ (x_n) \textit{ je cauchyovská vzhľadom k } |\ |_p\}.$$

*Na* **CP** *zavedieme operácie sčítania a násobenia nasledovne:*

$$(x_n) + (y_n) = (x_n + y_n),$$

$$(x_n)(y_n) = (x_n y_n).$$

**Tvrdenie 4.1.2.** **CP** *spolu s takto zadefinovanými operáciami sčítania a násobenia tvorí komutatívny okruh s jednotkou.*

*Dôkaz.*

Potrebujeme ukázať, že takto definovaný súčet i súčin dvoch cauchyovských postupností je opäť cauchyovská postupnosť. Sčítanie:

$$|x_n + y_n - x_m - y_m|_p \leq |x_n - x_m|_p + |y_n - y_m|_p$$

z trojuholníkovej nerovnosti.
Pozn.: $|\ |_p$ je nearchimedovská, takže v skutočnosti dokonca

$$|x_n + y_n - x_m - y_m|_p \leq max\,\{|x_n - x_m|_p, |y_n - y_m|_p\}.$$

Keďže $(x_n)$ a $(y_n)$ sú cauchyovské, dostávame cauchyovskosť ich súčtu.

Čo sa týka súčinu, máme

$$\begin{aligned} |x_n y_n - x_m y_m| &= |x_n y_n - x_n y_m + x_n y_m - x_m y_m| \\ &\leq |x_n y_n - x_n y_m| + |x_n y_m - x_m y_m| \\ &= |x_n||y_n - y_m| + |y_m||x_n - x_m| \end{aligned}$$

Z cauchyovskosti $(x_n)$ a $(y_n)$ je jasné, že $|x_n|$ aj $|y_n|$ sú ohraničené nejakou (spoločnou) konštantou (cauchyovská postupnosť samozrejme musí byť ohraničená), a z toho už dostávame cauchyovskosť súčinu.

□

(Pozn.: **CP** ale nie je teleso. Ak vezmeme cauchyovské postupnosti

$$(x_n) = 0, p, 0, p^2, \ldots,$$

$$(y_n) = p, 0, p^2, 0, \ldots,$$

vidíme, že ich súčin je nulová postupnosť (tj. nulový prvok v **CP**), a teda **CP** nie je dokonca ani obor integrity.)

**Definícia 4.1.3.** *Buď $\mathbb{Q}$ teleso racionálnych čísel a $|\ |_p$ p-adická absolútna hodnota. Definujeme*

$$\mathbf{CP} \supset \mathbf{NP} = \mathbf{NP}_p(\mathbb{Q}) = \{(x_n) :\ lim_{n\longrightarrow\infty}|x_n|_p = 0\},$$

*množinu všetkých cauchyovských postupností, ktorých limita je rovná* 0.

**Tvrdenie 4.1.4.** **NP** *je maximálny ideál okruhu* **CP**.

*Dôkaz.*

Pre dve postupnosti z **NP** je určite aj ich súčet v **NP**, takisto pre $(x_n) \in \mathbf{NP}$ aj $-(x_n) \in \mathbf{NP}$. (To okamžite vidno z nearchimedovskej vlastnosti p-adickej absolútnej hodnoty. Samozrejme nám ju v skutočnosti vôbec netreba - stačí archimedovské $|x + y| \leq |x| + |y|$). Pre $(x_n) \in \mathbf{NP}$ a $(y_n) \in \mathbf{CP}$ máme

$$(x_n y_n) = (x_n)(y_n) \in \mathbf{NP},$$

čo vidíme z toho, že (ako sme si už povedali) členy cauchyovskej postupnosti $(y_n)$ musia byť ohraničené.

**NP** je teda ideál v **CP**. Ostáva ukázať, že je maximálny. To spravíme tak, že ukážeme, že ideál $I$ generovaný **NP** a ľubovoľnou $(x_n) \in \mathbf{CP}$, ktorá ale nemá nulovú limitu, už nutne musí byť celý okruh **CP**. K tomu využijeme znalosti toho, že ideál okruhu obsahujúci jednotku, je už celý okruh. Naším cieľom teda bude ukázať, že v ideále $I$ sa nachádza jednotkový prvok okruhu **CP** (tj. konštantná jednotková postupnosť (1)).

Majme teda cauchyovskú postupnosť $(x_n)$, ktorej limita nie je 0. Potom pre ňu iste existuje $n_0 \in \mathbb{N}$ a konštanta $c$, také že pre

$$\forall n \geq n_0 : \ |x_n|_p \geq c > 0.$$

(V opačnom prípade by buď musela $(x_n)$ konvergovať k 0, alebo by nebola cachyovská.) To okrem iného znamená, že od indexu $n_0$ vyššie sú všetky členy postupnosti $(x_n)$ nenulové. Môžeme definovať postupnosť $(y_n) = 0$ ak $n < n_0$ a $(y_n) = 1/x_n$ ak $n \geq n_0$. Potom pre $n \geq n_0$ platí:

$$|y_{n+1} - y_n| = |\frac{1}{x_{n+1}} - \frac{1}{x_n}| = \frac{|x_{n+1} - x_n|}{|x_n x_{n+1}|} \leq \frac{|x_{n+1} - x_n|}{c^2} \longrightarrow 0,$$

pracujeme samozrejme s p-adickou absolútnou hodnotou, ktorá je nearchimedovská, takže (opäť s použitím Lemmy 3.3.6) dostávame, že $(y_n) \in \mathbf{CP}$.

Pozrime sa teraz, ako vyzerá postupnosť $(x_n y_n)$. Prvých $n_0 - 1$ členov je nulových a nasledujú samé jednotky. Potom postupnosť $z_n = (1) - (x_n y_n)$ je prvkom **NP**. Inak povedané, postupnosť (1) vieme dostať ako súčet $(z_n) \in \mathbf{NP} \subset I$ a násobku $(x_n) \in I$, takže aj $(1) \in I$, čo sme chceli ukázať.

□

Teraz už konečne dostávame to, k čomu sme celý čas smerovali - definícia p-adických čísel. V okruhu **CP** chceme navzájom stotožniť prvky, ktoré „by mali mať rovnakú limitu". Tomu zodpovedá faktorový okruh **CP** podľa **NP**, navyše zo základného kurzu algebry vieme, že faktor komutatívneho okruhu podľa jeho maximálneho ideálu je teleso.

(Pozn.: Toto je mimochodom obecný návod, ako možno postupovať pri zúplňovaní obecného telesa vzhľadom k nejakej absolútnej hodnote na ňom definovanej.)

**Definícia 4.1.5.** *Definujeme teleso p-adických čísel ako faktorový okruh* **CP** *podľa* **NP**, *tj.*

$$\mathbb{Q}_p = \mathbf{CP}/\mathbf{NP}.$$

## 4.2 Je všetko v poriadku?

Zadefinovali sme teleso p-adických čísel $\mathbb{Q}_p$, no ostáva ešte ukázať, že je skutočne tým, čím sme chceli aby bolo - zúplnením telesa $\mathbb{Q}$ vzhľadom k p-adickej absolútnej hodnote $|\ |_p$.
Potrebujeme teda odpovedať na nasledujúce otázky:

- Existuje inklúzia (homomorfizmus) $\mathbb{Q}$ do $\mathbb{Q}_p$?
- Dá sa p-adická absolútna hodnota $|\ |_p$ rozšíriť na $\mathbb{Q}_p$?
- Je $\mathbb{Q}_p$ úplné vzhľadom k $|\ |_p$?
- Je $\mathbb{Q}$ hustá v $\mathbb{Q}_p$ vzľadom k $|\ |_p$?

Ukážeme si teraz, že na všetky tieto otázky môžeme odpovedať kladne, a teda naša snaha nebola zbytočná.

**Otázka 4.2.1.** *Existuje inklúzia (homomorfizmus) $\mathbb{Q}$ do $\mathbb{Q}_p$.*

Samozrejme priradíme číslu $x \in \mathbb{Q}$ konštantnú postupnosť $(x) = x, x, x, \ldots$. To je očividne cauchyovská postupnosť. (Presnejšie povedané, priradíme mu *triedu ekvivalencie* postupnosti $(x)$!) Dostávame inklúziu $\mathbb{Q}$ do $\mathbb{Q}_p$.

**Otázka 4.2.2.** *Dá sa p-adická absolútna hodnota $|\ |_p$ rozšíriť na $\mathbb{Q}_p$?*

Najprv dodefinujeme $|\ |_p$ tak, ako nám káže intuícia. Pre $\alpha \in \mathbb{Q}_p$ položíme

$$|\alpha|_p = lim_{n\longrightarrow\infty}|x_n|_p,$$

kde $(x_n)$ je ľubovoľný reprezentant rozkladovej triedy $\alpha$.
V prípade, že $\alpha = 0$, $(x_n) \in \mathbf{NP}$ (tzn., že $(x_n)$ konverguje k 0), konverguje $|x_n|_p$ k nule, takže $|\alpha|_p = 0$, presne ako by sme čakali.
Ak $\alpha \neq 0$, využijeme nasledujúce pozorovanie:
Ak $(x_n)$ je cauchyovská postupnosť, ktorá nekonverguje k 0, existuje (ako sme už raz využili) konštanta $c$ a prirodzené číslo $n_1$ také, že

$$\forall n \geq n_1 :\ |x_n|_p \geq c > 0.$$

Z cauchyovskosti ale samozrejme máme aj existenciu $n_2$, takého, že

$$\forall m, n \geq n_2 :\ |x_n - x_m|_p < c.$$

Takže ak položíme $n_0 = max\,\{n_1, n_2\}$, potom pre $\forall m, n \geq n_0$ je jednak $|x_m|_p, |x_n|_p \geq c$ a $|x_n - x_m| < c$.
Teraz si spomeňme na princíp rovnoramennosti „trojuholníkov"v ultrametrike; v tomto prípade „trojuholník"je tvorený „vrcholmi"$0, x_n, x_m$. A keďže veľkosť „hrany"$x_nx_m$ je menšia ako veľkosť obidvoch hrán $0x_n, 0x_m$ (tieto veľkosti sú totiž rovné $|x_n|_p$, resp. $|x_m|_p$), dostávame tak, že nutne musí byť

$$|x_n|_p = |x_m|_p.$$

Ak sa pozrieme, čím celá táto úvaha začala, vidíme, že sme vlastne ukázali, že ak $(x_n)$ je cauchyovská (pričom nekonverguje k 0), tak postupnosť $(|x_n|_p)$ nutne musí byť od určitého indexu konštantná.
Pre nás to znamená predovšetkým to, že pre nenulové $\alpha \in \mathbb{Q}_p$ existuje $|\alpha|_p$ tak

ako sme ju definovali.

Hodnota $|\alpha|_p$ bude iste rovnká, nech už za reprezentanta danej triedy ekvivalencie vyberieme akúkoľvek postpnosť z danej triedy ekvivalencie - ak totiž $(y_n)$ je nejaká iná postupnosť z triedy ekvivalencie s reprezentantom $(x_n)$, potom postupnosť $(x_n - y_n)$ konverguje k 0 (veď práve na základe toho sme stotožňovali jednotlivé postupnosti), teda aj postupnosť čísel $|x_n - y_n|_p$ konverguje k 0, ale potom aj $(|x_n|_p - |y_n|_p)$ iste konverguje k 0, takže limity noriem ľubovoľných dvoch postupností z rovnakej triedy ekvivalencie sú rovnaké, inak povedané, hodnota $|\alpha|_p$ nie je závislá na voľbe reprezentanta triedy ekvivalencie.

Nakoniec ešte overíme, že takto dodefinovaná absolútna hodnota je skutočne absolútnou hodnotou: Ak $|\alpha|_p = 0$, znamená to, že $|\alpha|$ je triedou ekvivalencie postupností, ktorých limity postupností absolútnych hodnôt ich členov, sú rovné 0, teda aj limity samotných postupností sú rovné 0 - a samozrejme táto trieda ekvivalencie je práve nulou v $\mathbb{Q}_p$.
Naopak, ak $\alpha = 0$, vezmime za jeho reprezentanta konštantnú nulovú postupnosť (ako sme ukázali, na výbere reprezentanta nezáleží) - takže $|\alpha|_p = 0$.
Ďalej

$$|\alpha\beta|_p = lim_{n\longrightarrow\infty}|x_n y_n|_p = lim_{n\longrightarrow\infty}|x_n|_p lim_{n\longrightarrow\infty}|y_n|_p = |\alpha|_p|\beta|_p,$$

kde $(x_n), (y_n)$ sú nejaké reprezentanty tried $\alpha, \beta$.
Nakoniec ešte nahliadneme, že

$$|\alpha + \beta|_p = lim_{n\longrightarrow\infty}|x_n + y_n|_p \leq lim_{n\longrightarrow\infty} max\left\{|x_n|_p, |y_n|_p|\right\}$$

$$= max\left\{lim_{n\longrightarrow\infty}|x_n|_p, lim_{n\longrightarrow\infty}|y_n|_p\right\} = max\left\{|\alpha|_p, |\beta|_p\right\}.$$

Podarilo sa nám teda korektne rozšíriť nearchimedovskú p-adickú absolútnu hodnotu na celé $\mathbb{Q}_p$.

**Otázka 4.2.3.** *Je* obraz $\mathbb{Q}$ *hustá množina v* $\mathbb{Q}_p$ *vzľadom k* $|\ |_p$*?*

Aby toto bola pravda, musí platiť, že pre ľubovoľné $\alpha \in \mathbb{Q}_p$ a ľubovoľne malé $\epsilon$ kladné, nachádza sa v otvorenej guli

$$\mathbf{B}(\alpha, \epsilon)$$

nejaká konštantná postupnosť prvkov $\mathbb{Q}$. Buď teda $(x_n)$ nejaký reprezentant $\alpha$ a $0 < \epsilon' < \epsilon$. Postupnosť $(x_n)$ je cauchyovská, takže existuje $n_0$ také, že pre

$$\forall m, n \geq n_0 :\ |x_n - x_m|_p < \epsilon'.$$

Položíme $y = x_{n_0}$ a uvažujme konštantnú postupnosť $(y)$. Takže

$$|\alpha - (y)|_p = |(x_n - y)|_p = lim_{n\longrightarrow\infty}|x_n - y|_p \leq \epsilon' < \epsilon,$$

pre všetky $n \geq n_0$, čiže skutočne $(y) \in \mathbf{B}(\alpha, \epsilon)$.

**Otázka 4.2.4.** *Je $\mathbb{Q}_p$ úplné vzľadom k $|\ |_p$?*

Nech je $\lambda_1, ..., \lambda_n, ...$ cauchyovská postupnosť prvkov $\mathbb{Q}_p$ (tj. cauchyovská postupnosť cauchyovských postupností). Chceme ukázať, že v $\mathbb{Q}_p$ má limitu. Množina $\mathbb{Q}$ je hustá v $\mathbb{Q}_p$, a tak pre každé $n$ vieme nájsť $(y_n)$ konštantnú postupnosť racionálnych čísel, takú, že $|\lambda_n - (y_n)|_p < 1/n$. Nech teraz $\epsilon > 0$ a $N$ je celé číslo, $N \geq 1/\epsilon$. Potom dostávame pre všetky $n \geq N$:

$$|\lambda_n - (y_n)|_p < 1/n \leq 1/N \leq \epsilon.$$

Teda postupnosť $(\lambda_n - (y_n))$ konverguje k 0, nutne teda musí byť cauchyovská. Máme $(y_n) = \lambda_n - (\lambda_n - (y_n)$, takže aj $(y_n)$ je cauchyovská (v $\mathbb{Q}_p$ a týmpádom aj v $\mathbb{Q}$.) Položme teraz $\lambda = y_1, ..., y_n, ...$ a ukážeme, že $\lambda$ je limitou postupnosti $\lambda_n$. V prvom rade zvoľme $\epsilon$ a $N$ také, že pre všetky $m, n \geq N$ bude $|y_m - y_n| < \epsilon$. Potom pre všetky $n \geq N$ je $|\lambda - (y_n)| = \lim_{m\to\infty} |y_m - y_n| < \epsilon$. Takže $|\lambda - (y_n)|$ konverguje k nule, a z toho už dostávame, že $(\lambda - \lambda_n) = (\lambda - (y_n)) - (\lambda_n - (y_n))$ konverguje k 0, čo je presne to, čo sme chceli.

# Kapitola 5

# Reprezentácia prvkov $\mathbb{Q}_p$

Teraz sa konečne vraciame späť k prvej kapitole, kde sme čisto formálne pracovali s p-adickými číslami ako s „mocninnými radami v p", bez toho, aby sme sa trápili niečím, ako je ich konvergencia. Teraz si ukážeme, že to, čo sme v kapitole jedna načrtli, je riadna reprezentácia p-adických čísel (nazveme ju kanonická reprezentácia), teda že každý prvok $\mathbb{Q}_p$, tj. trieda ekvivalencie cauchyovských postupností z $\mathbb{Q}$ v sebe obsahuje aj cauchyovskú postupnosť práve v tvare, o ktorom sme sa zmienili na začiatku tejto práce, a teda že každý prvok $\mathbb{Q}_p$ môžeme reprezentovať práve takouto postupnosťou. A nielen to - ukážeme, že narozdiel od napríklad štandardnej reprezentácie reálnych čísel (tj. napríklad v desiatkovej sústave), je táto reprezentácia jednoznačná.

## 5.1 Kanonická reprezentácia p-adických čísel

V nasledujúcej kapitole si uvedieme najbežnejšiu z možných reprezentácií p-adických čísel, spolu s pomocnými tvrdeniami, ako je uvedené v texte [2]

**Lemma 5.1.1.** *Nech $x \in \mathbb{Q}$ a $|x|_p \leq 1$. Potom pre ľubovoľné $i$ existuje celé číslo $\lambda$ také, že $|\lambda - x|_p \leq p^{-i}$. Navyše $\lambda$ je možné vybrať z množiny $\{1, 2, \ldots, p^i - 1\}$ a v takom prípade je určené jednoznačne.*

*Dôkaz.*

Nech $x = \frac{a}{b}, a, b$ nesúdeliteľné. Z predpokladu vety $|x|_p \leq 1$, takže $p$ nemôže deliť $b$. Potom aj $b$ a $p^i$ sú nesúdeliteľné, tzn. existujú celé čísla $m, n$ také, že

$$mb + np^i = 1.$$

Položme $\lambda = am$. Potom dostávame:

$$|\lambda - x|_p = |am - \frac{a}{b}|_p = |\frac{a}{b}|_p |mb - 1|_p$$

$$\leq |mb - 1|_p = |np^i|_p \leq p^{-i}.$$

Nakoniec nájdime $\alpha$ také, aby $\lambda + \alpha p^i \in \{1, 2, ...p^i - 1\}$. Potom ale nearchimedovská vlastnosť p-adickej absolútnej hodnoty (resp. metriky) zaistí, že

$$|\lambda + \alpha p^i - x|_p \leq max\,\{|\lambda - x|_p, |\alpha p^i|_p\},$$

čiže nerovnosť $|\lambda + \alpha p^i - x|_p \leq p^{-i}$ bude platiť.

□

**Veta 5.1.2.** *Pre každý prvok $\alpha \in \mathbb{Q}_p$ taký, že $|\alpha|_p \leq 1$ existuje práve jeden jeho reprezentant (tj. cauchyovská postupnosť $(a_n)$) pre ktorý platí:*

- $a_i \in \mathbb{Z}, 0 \leq a_i < p^i$ *pre* $i = 1, 2, \ldots$
- $a_i \equiv a_{i+1}$ *(mod* $p_i$*) pre* $i = 1, 2, \ldots$.

*Dôkaz.*

Nech $(b_n)$ je nejaká cauchyovská postupnosť reprezentujúca $\alpha$. Chceme nájsť postupnosť $(a_n) \in \alpha$, ktorá spĺňa obidve podmienky zo znenia vety.
BUNO predpokladajme, že $|b_i|_p \leq 1$ pre $\forall i$. (Vieme totiž, že $lim_{n\longrightarrow\infty}|b_n|_p = lim_{n\longrightarrow\infty}|a_n|_p$ a $|\alpha|_p \leq 1$, takže v prípade potreby vieme „vyškrtnúť" prvých toľko členov postupnosti $(b_n)$ aby nerovnosť $|b_i|_p \leq 1$ bola splnená).
Postupnosť $(b_n)$ je cauchyovská, takže pre kažé $j \in \mathbb{N}$ vieme nájsť $n_j \in \mathbb{N}$ také, že

$$|b_i - b_j|_p \leq p^{-j},\ \forall i, j \geq n_j.$$

Postupnosť čísel $n_j$ iste vieme voliť tak, aby bola rýdzorastúca, tj. vieme zaistiť aby $n_j \geq j$.
Veta vraví, že vieme nájsť postupnosť $(a_j)$ pre ktorú platí:

$$|a_j - b_{n_j}|_p \leq p^{-j}.$$

Píšme

$$\begin{aligned} |a_{j+1} - a_j|_p &= |a_{j+1} - b_{n_{j+1}} + b_{n_{j+1}} - b_{n_j} - (a_j - b_{n_j})|_p \\ &\leq max\,\{|a_{j+1} - b_{n_{j+1}}|_p, |b_{n_{j+1}} - b_{n_j}|_p, |a_j - b_{n_j}|_p\} \\ &\leq max\,\{1/p^{j+1}, 1/p^j, 1/p^j\} = p^{-j}, \end{aligned}$$

čo nie je nič iné, ako že po vydelení $p^j$ sa $a_{j+1}, a_j$ nelíšia, tj.
$a_j \equiv a_{j+1}$ (mod $p_j$).
Zároveň ale platí, že pre ľubovoľné $j$, $\forall i \geq n_j$

$$\begin{aligned} |a_i - b_i|_p &= |a_i - a_j + a_j - b_{n_j} - (b_i - b_{n_j})|_p \\ &\leq max\,\{||a_i - a_j|_p, |a_j - b_{n_j}|_p, |b_i - b_{n_j}|_p\} \\ &\leq max\,\{1/p^j, 1/p^j, 1/p^j\}, \end{aligned}$$

takže $lim_{i\longrightarrow\infty}|a_i - b_i|_p = 0$, tzn. $(a_n)$ skutočne náleží $\alpha$.

Dokázali sme teda existenciu postupnosti zo znenia vety. Ostáva jednoznačnosť. Buď $(\tilde{a}_n)$ postupnosť spĺňajúca podmienky vety, taká, že $\tilde{a}_{n_0} \neq a_{n_0}$ pre nejaké $n_0$. Potom ale $a_{n_0}$ nie je kongruentné s $\tilde{a}_{n_0}$ modulo $p^{i_0}$. Z podmienky vety ale musí zároveň platiť, že

$$a_n \equiv a_{n_0} \neq \tilde{a}_{n_0} \equiv \tilde{a}_n \pmod{p^{i_0}},$$

pre všetky $n \geq n_0$.
To ale neznamená nič iné, ako že

$$|a_n - \tilde{a}_n|_p > p^{-i_0}.$$

Potom ale postupnosti $(\tilde{a}_n)$ a $(a_n)$ nemôžu byť z rovnakej triedy ekvivalencie $\alpha$.

□

Konečne sa dostávame k zápisu p-adického čísla z prvej kapitoly. Ak teraz za reprezentanta $\alpha \in \mathbb{Q}_p$, $|\alpha|_p \leq 1$, zvolíme postupnosť čiastočných súčtov $(a_n)$, kde $i$-tý člen má tvar

$$a_i = b_0 + b_1 p + b_2 p^2 + \cdots + b_{n-1} p^{n-1},$$

kde $\forall i \quad d_i \in \{1, \ldots, p-1\}$, je to práve postupnosť vyhovujúca zneniu práve dokázanej vety.
Prvok $\alpha$ tak môžeme reprezentovať (v p-adickej norme) konvergentnou radou

$$\sum_{n=0}^{\infty} d_n p^n.$$

Na túto radu môžeme pozerať ako na „zápis čísla v bázi $p$", môžeme teda písať

$$\alpha = \ldots d_n \ldots d_2 d_1 d_0.$$

Vidíme, že sa jedná o analógiu zápisu reálneho čísla, na aký sme zvyknutý, s tým rozdielom, že v našom prípade je zápis konečný „doprava", zato môže byť nekonečný „doľava".
V prípade, že $|\alpha|_p > 1$, prenásobením $\alpha$ číslom $|\alpha|_p = p^m$ dostaneme p-adické číslo $\alpha' = \alpha p^m$, ktoré už spĺňa $|\alpha'|_p \leq 1$ (presnejšie $|\alpha'|_p = 1$). Potom môžeme písať

$$\alpha = \sum_{n=-m}^{\infty} d_n p^n,$$

alebo

$$\alpha = \ldots d_n \ldots d_2 d_1 d_0, d_{-1}, d_{-2} \ldots d_{-m}.$$

Takejto reprezentácii budem hovoriť *kanonická reprezentácia p-adického čísla* $\alpha$. Číslam $d_i$ budeme hovoriť *p-adické cifry* $\alpha$. To nás vedie k definícii p-adických celých čísel.

**Definícia 5.1.3.** *Prvku $\alpha \in \mathbb{Q}_p$ hovoríme p-adické celé číslo, ak v jeho kanonickej reprezentácii sú iba nezáporné mocniny p. Množinu všetkých p-adických celých čísel značíme $\mathbb{Z}_p$.*

Poznámka: P-adické celé čísla, sú práve čísla, ktorých p-adická absolútna hodnota je menšia alebo rovná 1, tj. $\mathbb{Z}_p$ tvorí v $\mathbb{Q}_p$ jednotkovú guľu.
Na záver si uvedieme malý ilustračný príklad.

*Príklad:*

Pre $p = 5$ a $x = \frac{76}{625}$ máme:

$$x = 1 \cdot 5^{-4} + 0 \cdot 5^{-3} + 3 \cdot 5^{-2} + 0 \cdot 5^{-1} + 0 \cdot 5^{0} + 0 \cdot 5^{1} + \dots .$$

Pre p-adickú absolútnu hodnotu $|x|_p$ platí

$$|x|_p = |76/625|_p = |5^{-4} \cdot 76|_p = 5^{-(-4)} \cdot 5^0 = 625.$$

Poznamenajme ešte, že zatiaľ čo každé celé číslo je aj p-adickým celým číslom, existujú racionálne zlomky, ktoré sú v telese p-adických čísel celými p-adickými číslami. Spomeňme si napríklad na rozvoj čísla 9/17 v kapitole 2. Dá sa ľahko nahliadnuť, že obecne každé racionálne číslo tvaru $a/b$, kde $p$ nedelí $b$ je celým p-adickým číslom.

# Kapitola 6

# Niektoré dôležité výsledky

## 6.1 Henselovo lemma

Na záver si uvedieme dva z najdôležitejších výsledkov teorie p-adických čísel: Prvým je Henselovo lemma, hovoriace o existencii koreňov polynómu, ktorého koeficienty sú p-adické celé čísla, v znení a s dôkazom ako je uvedené v texte [2].

**Veta 6.1.1.** *(Henselovo lemma):*
*Nech*

$$F(x) = b_0 + b_1x + b_2x^2 + \ldots + b_nx^n,$$

*je polynóm, ktorého koeficienty sú p-adické celé čísla a nech*

$$F'(x) = b_1 + 2b_2x + \ldots + nb_nx^{n-1},$$

*je formálna derivácia $F(x)$. Nech $\tilde{a}$ je celé p-adické číslo spĺňajúce $F(\tilde{a}) \equiv 0$ (mod p) a $F'(\tilde{a}) \neq 0$ (mod p). Potom existuje jednoznačne určené p-adické číslo $a$ také, že $F(a) = 0$ a $a \equiv \tilde{a}$ (mod p).*

*Dôkaz.*

Tvrdenie dokážeme induktívnym konštruovaním kanonickej reprezentácie p-adického čísla $a$, ktorého existenciu chceme dokázať. V k-tom kroku nájdeme $a_k = d_0 + d_1p + \cdots + d_kp^k$. Jednotlivé $a_k$ síce nebudú korene polynómu $F(x)$, no bude pre nich platiť $F(a_k) \equiv 0 \pmod{p^{k+1}}$. Limitným prechodom $k \longrightarrow \infty$ dostaneme hľadané $a$, ktoré už bude koreňom $F(x)$.
Chceme teda dokázať indukciou, že $\forall k \in \mathbb{N}$ existuje celé p-adické číslo tvaru

$$a_k = d_0 + d_1p + \cdots + d_kp^k,$$

ktoré spĺňa:

- $\forall i: \quad d_i \in \{1, \ldots, p-1\}$
- $F(a_k) \equiv 0 \pmod{p^{k+1}}$

- $a_k \equiv \tilde{a} \pmod{p}$

V nultom kroku položíme $a_0 = d_0$ rovné prvej p-adickej cifre čísla $\tilde{a}$. Potom iste $a_0 \equiv \tilde{a} \pmod{p}$ a $F(a_0) = 0 \pmod{p}$.
Prevedieme indukčný krok $k-1 \longrightarrow k$. Položíme $a_k = a_{k-1} + c_k p^k$, kde $0 \leq c_k < p$ zatiaľ nepoznáme. Teraz dosadíme $a_k$ do $F(x)$, pričom si členy, ktoré sú deliteľné $p^{k+1}$ nebudeme všímať (sú rovné 0 modulo $p^{k+1}$).

$$F(a_k) = F(a_{k-1} + c_k p^k) = \sum_{i=0}^{n} b_i (a_{k-1} + c_k p^k)^i.$$

V sume napravo teraz „odignorujeme"všetky členy deliteľné $p^{k+1}$, lebo modulo $p^{k+1}$ nehrajú žiadnu rolu. To znamená, že z binomického rozvoja zátvorky pre každé $i$ nám ostanú len tie členy, v ktorých je $c_k p^k$ nanajvýš v prvej mocnine. Dostávame

$$F(a_k) = b_0 + \sum_{i=1}^{n} b_i (a_{k-1}^i + a_{k-1}^{i-1} i c_k p^k \equiv F(a_{k-1}) + c_k p^k F'(a_{k-1}) \pmod{p^{k+1}}.$$

Z indukčného predpokladu je $F(a_{k-1}) \equiv 0 \pmod{p^k}$, takže existuje nejaké celé číslo $0 \leq \lambda_k < p-1$, že

$$F(a_{k-1}) = \lambda_k p^k.$$

Dostávame tak, že

$$F(a_k) \equiv \lambda_k p^k + c_k p^k F'(ak-1) \pmod{p^{k+1}}.$$

Po predelení $p^k$ tak dostávame kongruenciu

$$\lambda_k + c_k F'(a_{k-1}) \equiv 0 \pmod{p},$$

pre neznámu $c_k$. Pripomeňme si teraz, že $a_{k-1} \equiv \tilde{a}$ modulo $p$, takže aj $F'(ak-1)$ je kongruentné s $F'(\tilde{a})$ modulo $p$ (všeky členy okrem absolútnych sú deliteľné $p$). Z predpokladu vety ale $p$ nedelí $F'(\tilde{a})$, takže nedelí ani $F'(ak-1)$. Týmpádom môžme z kongruencie

$$\lambda_k + c_k F'(a_{k-1}) \equiv 0 \pmod{p},$$

vyjadriť $c_k$ ako

$$c_k \equiv \frac{-\lambda_k}{F'(a_{k-1})} \pmod{p},$$

ktoré zaistí, že $F(a_k) \equiv 0 \pmod{p^{k+1}}$.

Nakoniec teda položme

$$a = c_0 + c_1 p + c_2 p^2 + \cdots.$$

Pre všetky $k$ je

$$F(a) \equiv F(a_k) \equiv 0 \pmod{p^{k+1}},$$

takže $F(a) = 0$.
Jednoznačnosť $a$ plynie z jednoznačnosti postupnosti $(a_n)$.

□

Poznámka: Predpoklad $F'(\tilde{a}) \neq 0 \pmod p$ z nami uvedeného znenia Henselovho lemma, môžeme v skutočnosti nahradiť predpokladom slabším - a to, že $|F(\tilde{a})| < |F'(\tilde{a})|^2$ (pričom záver, že $a \equiv \tilde{a} \pmod p$ bude nahradený záverom, že $|a - \tilde{a}| < |F'(\tilde{a})|$). Dôkaz Henselovho lemma v tejto jeho silnejšej podobe nájdeme napr. v knihe J.W.S. Cassels, *Local Fields,* Cambridge University Press, Cambridge, 1986.

## 6.2 Lokálny-globálny princíp

Poznámka:
V tejto podkapitole, budeme používať značenie $\mathbb{Q}_p$ pre $p \leq \infty$, kde pre $p = \infty$ budeme príslušnou p-adickou absolútnou hodnotou rozumieť štandardnú absolútnu hodnotu. Samozrejme potom telesom $\mathbb{Q}_p$ rozumieme teleso reálnych čísel.

Prostredníctvom Henselovho lemma, sme si ukázali, že nie je ťažké zistiť, či polynóm má korene v $\mathbb{Z}_p$ - stačí totiž nájsť korene modulo $p$. Pozrime sa teraz na inú úlohu - čo ak chceme zistiť, či daný polynóm má korene v $\mathbb{Q}$? Určite vieme povedať, že ak nemá žiadny koreň v $\mathbb{Q}_p$, pre nejaké $p \leq \infty$, nemôže mať koreň ani v $\mathbb{Q}$. Každé teleso $\mathbb{Q}_p$ pre rôzne $p$, nám dáva „lokálne" informácie „blízko"prvočísla $p$. Korene z $\mathbb{Q}$ (uvažujme o nich ako o "globálnych") sú samozrejme koreňmi v každom $\mathbb{Q}_p$ (tj. „lokálnymi"koreňmi). Oveľa zaujímavejšie a užitočnejšie by ale bolo, keby sme sa naopak od „lokálnych"koreňov v $\mathbb{Q}_p$, pre všetky $p \leq \infty$, vedeli dostať ku „globálnym". Táto metóda sa často používa napríklad pri hľadaní riešení (alebo rozhodovaní o ich existencii) diofantických rovníc. Samozrejme, nie je vždy úspešná - existujú diofantické rovnice s koreňmi v $\mathbb{Q}_p$ pre všetky $p \leq \infty$, ktoré nemajú žiadne racionálne korene. Nasledujúca Hasse-Minkowského veta, ktorú si uvedieme bez dôkazu, je príkladom, kedy taktika „od lokálnych koreňov ku globálnym"úspešná je.

**Veta 6.2.1.** *(Hasse-Minkowského veta):*
*Nech*

$$F(X_1, X_2 \ldots, X_n) \in \mathbb{Q}(X_1, X_2 \ldots X_n)$$

*je kvadratická forma. Potom rovnica*

$$F(X_1, X_2 \ldots, X_n) = 0$$

*má netriviálne riešenie v $\mathbb{Q}$ vtedy a len vtedy, ak má netriviálne riešenie v $\mathbb{Q}_p$, pre všetky $p \leq \infty$.*

Namiesto dôkazu Hasse-Minkowského vety, si teda uvedieme jej aplikáciu na príklade s riešením, ako je uvedené v texte [1]. Ukážeme si, kedy má rovnica

$$aX^2 + bY^2 + cZ^2 = 0,$$

kde $a, b, c$ sú racionálne čísla, netriviálne racionálne riešenie, resp. riešenia. Máme teda rovnicu

$$aX^2 + bY^2 + cZ^2 = 0.$$

Tú určite môžeme prenásobiť najmenším spoločným násobkom menovateľov čísel $a, b, c$, takže $a, b, c$ môžeme predpokladať celé. Navyše, ak je najväčší spoločný deliteľ $a, b, c$ väčší ako 1, môžeme celú rovnicu týmto číslom predeliť, a teda $a, b, c$ môžeme predpokladať nesúdeliteľné. Všimnime si tiež, že ak

$$a = An^2,$$

pre nejaké $A, n$ celé čísla, potom riešenie $(x, y, z)$ rovnice

$$aX^2 + bY^2 + cZ^2 = 0,$$

zodpovedá riešeniu $(nx, y, z)$ rovnice

$$AX^2 + bY^2 + cZ^2 = 0.$$

To znamená, že $a, b, c$ môžeme predpokladať „bezštvorcové"(tj. v ich prvočíselnom rozklade nie je žiadna druhá mocnina)- môžme totiž predpokladať, že každý takýto štvorec „absorbuje"príslušná neznáma. To nám umožnuje učiniť ešte jeden predpoklad - že $a, b, c$ sú dokonca po dvoch nesúdeliteľné. Dôvod je nasledovný: položme $k$ rovné $NSD(a, b)$ a predpokladáme, že $k > 1$. Toto $k$ iste nedelí $c$ (predpokladáme $NSD(a, b, c) = 1$). Môžme písať:

$$kAX^2 + kB^2 + cZ^2 = 0,$$

pre nejaké $A, B$ celé, z čoho okamžite vidíme, že $k$ musí deliť aj $cZ^2$, ale $k$ nedelí $c$, teda $k$ delí $Z^2$. Navyše kedže $k$ je bezštvorcové, $k$ musí nutne deliť $Z$. Potom je ale možné celú rovnicu predeliť číslom $k$. Čísla $a, b, c$ teda skutočne smieme predpokladať po dvoch nesúdeliteľné (čo tiež znamená, že súčin $abc$ je bezštvorcový).

Hasse-Minkowského veta nám hovorí, že vieme rozhodnúť, či rovnica zo zadania má, alebo nemá riešenie v racionálnych číslach, podľa toho, či tá istá rovnicá má, alebo nemá riešenie vo všetkých $\mathbb{Q}_p$ pre $p \leq \infty$. Poďme teda zistiť, či existujú a ak áno, tak za akých podmienok, riešenia rovnice v jednotlivých telesách $\mathbb{Q}_p$.

*1. Nech $p$ je nepárne prvočíslo, ktoré nedelí žiaden z koeficientov $a, b, c$.* Budeme najprv študovať riešenia modulo $p$, aby sme potom, za pomoci Henselovho lemmatu rozhodli o existencii riešenia v $\mathbb{Q}_p$. Predpokladajme totiž, že vieme, že existuje nejaké netriviálne riešenie modulo $p$, $(x_0, y_0, z_0)$, rovnice zo zadania také, že $p$ nedelí aspoň jedno z čísel $x_0, y_0, z_0$ (bez újmy na obecnosti, nech $p$ nedelí $x_0$). Potom ale polynóm

$$F(X) = aX^2 + by_0^2 + cz_0^2$$

spĺňa podmienky Henselovho lemmatu - $F(x_0)$ je rovné 0 modulo $p$ (predpokladáme, že $x_0$ je jeho koreň), a $p$ nedelí $F'(x_0) = 2ax_0$ (nezabudnime, že sme predpokladali, že $p$ je nielen nepárne a nedelí $x_0$, ale nedelí ani $a$.) Takže vieme, že existuje (jednoznačne určené) p-adické číslo $x$, ktoré je koreňom polynómu $F(x)$, čiže trojica $(x, y_0, z_0)$ je nami vytúženým riešením rovnice zo zadania. Ostáva ale ukázať, že náš prvotný predpoklad bol naozaj správny, tj. že pre všetky nepárne prvočísla $p$ a celé čísla $a, b, c$ po dvoch nesúdeliteľné a nedeliteľné číslom $p$, existuje trojica celých čísel $(x_0, y_0, z_0)$, v ktorej aspoň jedno číslo nie je deliteľné číslom $p$ taká, že platí

$$ax_0^2 + by_0^2 + cz_0^2 \equiv 0 \pmod{p}.$$

Skúsme teda spočítať, koľko trojíc $(x, y, z)$ z celkového počtu $p^3$ možností (pracujeme totiž modulo $p$, teda pre každú z neznámych pripadá do úvahy $p$ hodnôt - od 0 do $p-1$), je riešením tejto kongruencie (zatiaľ nás nezaujíma, či je to riešenie, v ktorom aspoň jedna z hodnôt neznámej je nedeliteľná $p$). Ak $(x, y, z)$ je riešením, potom iste platí

$$(ax^2 + by^2 + cz^2)^{p-1} \equiv 0 \pmod{p}.$$

V opačnom prípade vďaka malej Fermatovej vete vieme, že

$$(ax^2 + by^2 + cz^2)^{p-1} \equiv 1 \pmod{p}.$$

Počet takýchto trojíc, ktoré riešením nie sú, označme $n$. Potom pre toto $n$ platí

$$n \equiv \sum_{(x,y,z)} (ax^2 + by^2 + cz^2)^{p-1} \pmod{p}.$$

Po umocnení jednotlivých sčítancov dostávame $n$ ako sumu súm nasledovného tvaru:

$$\sum_{(x,y,z)} \alpha a x^{2i} b y^{2j} c z^{2k},$$

kde $2i + 2j + 2k = 2(p-1)$ a $\alpha$ je celé číslo. Aspoň jeden z exponentov $2i, 2j, 2k$ je ostro menší ako $p-1$ (v opačnom prípade by ich suma bola väčšia alebo rovná $3(p-1)$). Bez újmy na obecnosti predpokladajme, že $2i < p-1$. Jednotlivé sumy teraz môžeme prepísať v tvare

$$\sum_{(y,z)} (\alpha y^{2j} z^{2k} \sum_{x} x^{2i}).$$

Pozrime sa bližšie na sumu $\sum_x x^{2i}$), resp. na jej obecnejšiu podobu $\sum_x x^n$), kde $n < p-1$. Ak prenásobíme všetky prvky konečného $p-$prvkového telesa ľubovoľným nenulovým, pevne zvoleným prvkom toho istého telesa, dostaneme opäť všetky prvky tohto telesa (prepermutované). (Pre spor predpokladajme, že existujú nejaké dva rôzne prvky $x, y$ a nenulové $a$ také, že $ax$ a $ay$ dávajú modulo $p$ rovnaký zvyšok. Potom ale $ax - ay = a(x-y)$ je modulo $p$ rovné nula, a teda $p$ by muselo deliť $a$, alebo $(x-y)$, čo je spor.) Potom ale aj zoznam prvkov $a^n x^n$ pre $a$ nenulové je prepermutovaný zoznam prvkov $x^n$ (pozor - nie nutne všetkých prvkov telesa!) To ale znamená, že

$$\sum_{x=0}^{p-1} x^n \equiv \sum_{x=0}^{p-1} a^n x^n \pmod{p},$$

a teda

$$0 \equiv \sum_{x=0}^{p-1} x^n - \sum_{x=0}^{p-1} a^n x^n \equiv (1-a^n) \sum_{x=0}^{p-1} x^n \pmod{p}.$$

Ak navyše nezvolíme $a$ ako ľubovoľný nenulový prvok telesa, ale ako nejaký jeho primitívny prvok, potom určite bude vždy $a^n$ modulo $p$ rôzne od 1 (čo je okamžite vidieť z toho, že primitívny prvok je vlastne generátor cyklickej grupy telesa a Malá fermatova veta nám hovorí, že $a^{p-1} = 1 \pmod{p}$, zatiaľčo $n$ môže byť rovné nanajvýš $p-2$, a kedže $a$ je generátor, nemôže nadobudnúť hodnotu 1 modulo $p$ aj v nejakej nižšej mocnine ako je $p-1$.) Ale potom sme už hotoví - suma $\sum_{x=0}^{p-1} x^n$ musí byť nutne rovná nule modulo $p$, teda aj všetky sumy

$$\sum_{(y,z)} (\alpha y^{2j} z^{2k} \sum_{x} x^{2i})$$

sú rovné nule modulo $p$, takže aj počet všetkých ne-riešení, ktorý sme chceli pôvodne určiť, je rovný nule modulo $p$, inak povedané, tento počet je prvočíslom $p$ deliteľný, a teda musí ním byť deliteľný aj počet riešení (nezabudnime, že počet riešení + počet neriešení je rovný $p^3$.) Jedno riešenie je nám ale iste známe - a to triviálne $x = y = z = 0$. Počet riešení je teda určite väčší ako 1 (musí byť predsa deliteľný $p$!), takže nutne existuje riešenie $(x, y, z)$, kde aspoň jedno číslo z trojice nie je deliteľné prvočíslom $p$, čo sme chceli ukázať.

*2. Nech p=2 a $a, b, c$ sú nepárne.* Predpokladajme, že nejaké riešenie $(x, y, z)$ v $\mathbb{Q}_2$ existuje. Potom môžme $x, y, z$ prenásobiť takou mocninou dvojky, aby $x, y$ aj $z$ boli celé p-adické čísla, a aby aspoň jedno z čísel malo v kanonickom zápise poslednú cifru (myslené samozrejme tú „najviac vpravo") nenulovú (inak povedané, aby to bola p-adická jednotka) - jedná sa vlastne len o prenásobenie celej rovnice príslušnou mocninou dvojky. No $a, b$ i $c$ sú všetky nepárne, takže v skutočnosti musia byť medzi $x, y$ a $z$ p-adické jednotky práve dve - v inom prípade by sa nemohlo jednať o riešenie rovnice (po dosadení by sme totiž dostali p-adickú jednotku.) Bez újmy na obecnosti, nech $y$ a $z$ sú dve p-adické jednotky, a $x$ je celá p-adická nejednotka - teda $x$ leží v ideále $2\mathbb{Z}_2$ (čo neznamená nič iné, ako že posledná cifra $x$ je nula). Potom $x^2$ náleží $4\mathbb{Z}_2$ a $y^2, z^2$ náležia $1+4\mathbb{Z}_2$. Potom ak vezmeme celú rovnicu modulo 4, dostávame nutnú podmienku, že $b + c = 0 \pmod{p}$. (Obdobne, ak by nejednotka bola $y$ alebo $z$, dostaneme podmienku pre zvyšné dva koeficienty). Na nájdenie postačujúcej podmienky pre existenciu riešenia použijeme opäť Henselovo lemma, presne ako v predchádzajúcom prípade. Problém je, že tentoraz máme $p = 2$, takže derivácia bude iste vždy deliteľná $p$. Spomeňme si ale na slabšiu podmienku, z poznámky za dôkazom Henselovho lemmatu! V našom konkrétnom prípade, aby táto podmienka bola splnená, musí platiť:

$$|ax_0^2 + by_0^2 + cz_0^2| < |2ax_0|^2$$

$$|ax_0^2 + by_0^2 + cz_0^2| < 1/4|x_0^2|$$

pre nejaké počiatočné $x_0$. Skúsme položiť $x_0 = 1$. Potom už vidíme, že ľavá strana nerovnosti musí byť menšia ako 1/4, teda musí byť rovná minimálne 1/8 (pracujeme s p-adickou absolútnou hodnotou), inak povedané, musí platiť

$$|ax_0^2 + by_0^2 + cz_0^2| \equiv 0 \pmod 8.$$

Vieme už tiež, že pre dva z koeficientov, bez újmy na obecnosti nech sú to $a, b$, platí $a+b \equiv 0 \pmod 4$. Takže buď $a+b \equiv 0 \pmod 8$ a potom ak položíme $y_0 = 1$ a $z_0 = 0$ Henselovo lemma nám už dáva existenciu riešenia, tak ako v predchádzajúcom prípade. To isté platí aj ak $a + b \equiv 4 \pmod 8$ - položíme $y_0 = 1$ a $z_0 = 2$. Teda nutná podmienka je zároveň aj postačujúca, tzn. pre 2 z koeficientov musí platiť, že ich súčet je deliteľný 4.

*3. Nech p=2 a jeden z koeficientov $a, b, c$ je párny.* Predpokladajme, že párnym koeficientom je $a$. (Stále predpokladáme, že $x, y, z$ sú p-adické celé čísla, a aspoň jedno z nich je p-adická jednotka). Nech najprv $x \in 2\mathbb{Z}_2$, Potom ($a$ je párne) $ax^2 \in 8\mathbb{Z}_2$, a $y$ alebo $z$ je 2-adická jednotka, nutne teda už takými jednotkami musia byť obidve. Ich štvorce teda iste ležia v $1 + 8\mathbb{Z}_2$ (to vidno okamžite, ak si 2-adickú jednotku zapíšeme v tvare $1+2x$ a umocníme na druhú). Dostávame tak nutnú podmienku $b+c \equiv 0 \pmod 8$. Naopak, ak $x$ je 2-adická jednotka, musianimi opäť byť aj $y$ a $z$. Ak by totiž napr. $y \in 2\mathbb{Z}_2$, potom by bolo dvomi deliteľné aj $ax^2+by^2$ a teda nutne aj $cz^2$, $c$ však predpokladáme nepárne, tzn. muselo by plati5, že $z \in 2\mathbb{Z}_2$. To by ale znamenalo, že $by^2 + cz^2 \in 4\mathbb{Z}_2$ a teda by tam muselo patriť aj $ax^2$, čo pravda byť nemusí. Všetky tri členy teda iste náležia $1 + 8\mathbb{Z}_2$, z čoho dostávame podmienku $a + b + c \equiv 0 \pmod 8$. To, že táto podmienka je zároveň postačujúca, dostaneme úplne tak isto, ako v predchádzajúcom prípade (tentoraz napr. ako polynóm v premennej $y$, aby sme sa nemuseli trápiť s párnosťou koeficientu $a$) - navyše už máme informácie o koeficientoch $a, b, c$ modulo 8 (na ľavej strane nerovnosti z prepokladu Henselovho lemmatu teda bude maximálne 1/16).

*4. Nech p je nepárne prvočíslo a jeden z koeficientov $a, b, c$ je deliteľný p.* Nech je takým koeficientom napríklad $a$. Potom môžeme písať

$$by^2 + cz^2 \equiv 0 \pmod p.$$

Stále predpokladáme, že jedno z čísel je p-adická jednotka. Opäť ňou teda musia byť obe (inak by sa nám „nevynulovali"), teda k obom existuje inverzný prvok, a my môžeme rovnicu prepísať ako

$$b + c(z/y)^2 \equiv 0 \pmod p.$$

Ak pre nutnú podmienku teraz predpokladáme, že takéto p-adické číslo existuje, existuje iste aj číslo celé, ktoré splňuje to isté (stačí zobrať konečný počet cifier z jeho zápisu), a teda iste platí, že

$$b + cr^2 \equiv 0 \pmod p,$$

pre nejaké $r$ celé. Použitím Henselovho lemmatu rovnako ako v predchádzajúcich prípadoch, dostaneme opäť, že je to aj podmienka postačujúca.

*5. Teleso reálnych čísel so štandartnou metrikou.* Je okamžite vidieť, že rovnica bude mať netriviálne riešenie práve vtedy, ak $a, b, c$ nebudú mať všetky to isté znamienko.

Tým sme získali všetky podmienky pre koeficienty v závislosti od jednotlivých hodnôt $p$ - ak teda budú všetky tieto podmienky splnené súčasne, Hasse-Minkowského veta nám dáva existenciu netriviálneho riešenia v $\mathbb{Q}$. Môžeme tak vysloviť nasledovné zhrnutie:

Rovnica $aX^2 + bY^2 + cZ^2 = 0$ zo zadania, má v $\mathbb{Q}$ netriviálne riešenie práve vtedy, keď koeficienty $a, b, c$ spĺňajú nasledujúce podmienky:

- Pre každé nepárne prvočíslo, ktoré delí $a$ (a obdobne pre nepárne prvočísla, ktoré delia $b, c$) existuje celé číslo $r$ také, že $b + r^2 c \equiv 0 \pmod{p}$.
- Ak $a, b, c$ sú nepárne, potom súčet niektorých dvoch z nich je deliteľný číslom 4.
- Ak $a$ je párne (a obdobne, ak $b$ alebo $c$ je párne) potom buď súčet $b + c$ alebo súčet $a + b + c$ je deliteľný číslom 8.
- Čísla $a, b, c$ nemajú všetky to isté znamienko.

# Kapitola 7

# Záver

Stručne sme si teda predstavili teleso p-adických čísel. Ukázali sme si, že absolútna hodnota môže mať skutočné rôzne podoby, tak ako aj koncept „vzdialenosti" dvoch prvkov telesa, v dôsledku čoho môže mať rôzne podoby aj zúplnenie neúplného telesa, v závislosti od toho, vzhľadom k akej absolútnej hodnote ho zúplňujeme. Okrem samotnej konštrukcie telesa p-adických čísel sme si aj načrtli ich možnú reprezentáciu. Iste by stálo za to ukázať si, ako je to s aritmetikou týchto čísel - to aj mnoho ďalších zaujímavých informácií nájde čitateľ napríklad v knihe [2]. Samostatnou kapitolou by iste bolo hľadanie rozšírenia telesa p-adických čísel analogicky k tomu, ako je teleso komplexných čísel rozšírením reálnych - teda telesa ktoré je nielen úplné, ale aj algebraicky uzavreté (jedná sa o zložitejší problém ako v prípade reálnych/komplexných čísel - tvorí samostatnú kapitolu v knihe [1]).

# Literatúra

[1] Fernando Quadros Gouvea, *p-adic Numbers: An Introduction, Second Edition, Corrected 3rd Printing, Universitext, Springer 1997*

[2] Svetlana Katok, *p-adic Analysis Compared with Real, Pennsylvania State University - AMS, 2007*

[3] Çetin Kaya Koç, *A Tutorial on p-adic Arithmetic, Technical Report, Electrical and Computer Engineering, Oregon State University, 2002*